UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y COMUNICACIONES

TEMA:

SISTEMA DE GESTIÓN DE REDES PARA EL CONTROL Y DISTRIBUCIÓN DEL TRÁFICO EN LA RED LAN DE LA UNIDAD EDUCATIVA BAÑOS DEL CANTÓN BAÑOS

Trabajo de Graduación. Modalidad: TEMI. Trabajo Estructurado de Manera Independiente, presentado previo la obtención del título de Ingeniero en Electrónica y Comunicaciones

LÍNEA DE INVESTIGACIÓN:

Administración de Redes

AUTOR: Carlos Andrés Sánchez Izurieta
TUTOR: Ing. David Guevara, Mg

Ambato - Ecuador
Agosto, 2014

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del Trabajo de Investigación sobre el Tema:

"Sistema de gestión de redes para el control y distribución del tráfico en la red LAN de la Unidad Educativa Baños del cantón Baños", del señor Carlos Andrés Sánchez Izurieta, estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los trámites y consiguiente aprobación de conformidad con el Art. 16 del Capítulo II, del Reglamento de Graduación para Obtener el Título Terminal de Tercer Nivel de la Universidad Técnica de Ambato

Ambato, Agosto del 2014

EL TUTOR

Ing. David Guevara, Mg

AUTORÍA

El presente trabajo de investigación titulado: "Sistema de gestión de redes para el control y distribución del tráfico en la red LAN de la Unidad Educativa Baños del cantón Baños". Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, Agosto del 2014

Carlos Andrés Sánchez Izurieta

CC: 180475602-9

APROBACIÓN COMISIÓN CALIFICADORES

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing. Mg. José Vicente Morales Lozada, Ing. Mg. Edgar Freddy Robalino Peña y Ing. Mg. Santiago Altamirano Meléndez, revisó y aprobó el Informe Final del trabajo de graduación titulado "Sistema de gestión de redes para el control y distribución del tráfico en la red LAN de la Unidad Educativa Baños del cantón Baños", presentado por el señor Carlos Andrés Sánchez Izurieta de acuerdo al Art. 17 del Reglamento de Graduación para obtener el título Terminal de tercer nivel de la Universidad Técnica de Ambato.

Ing. José Vicente Morales Lozada, Mg.

PRESIDENTE DEL TRIBUNAL

Ing. Edgar Freddy Robalino Peña, Mg

DOCENTE CALIFICADOR

Ing. Santiago Altamirano Meléndez, Mg

DOCENTE CALIFICADOR

DEDICATORIA

El presente trabajo de tesis está dedicado a Dios quien ha guiado mi camino y cuidado siempre; A mis padres, por haberme brindado amor y comprensión, enseñándome siempre el valor de la humildad, esfuerzo y sacrificio, quienes me han dado su fuerza y apoyo incondicional.
A mi esposa e hijo quienes me han sabido apoyar incondicionalmente en los momentos más difíciles de mi carrera estudiantil, así como también en los momentos tristes de mi vida, en los cuales me han dado la fortaleza para continuar esforzándome sin decaer, y poder ser un modelo a seguir.

Carlos Sánchez

AGRADECIMIENTO

Agradezco a Dios quien ha sido mi guía y ha iluminado cada paso que he dado en la vida llenándome de bendiciones.

A mis padres y familiares, quienes en toda mi vida me han apoyado en mi formación académica, creyendo en mí en todo momento.

A mi tutor, Ing. David Guevara, profesores, quienes han compartido su conocimiento y a todas las personas que de una u otra manera han colaborado para la realización de este trabajo de investigación.

A mis amigos y compañeros de la Universidad, por el apoyo y compañía brindada todo este tiempo.

A la Unidad Educativa Baños por abrirme sus puertas para la realización de este proyecto.

Finalmente un eterno agradecimiento a la Universidad Técnica de Ambato y la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

Carlos Sánchez

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

La Unidad Educativa Baños es una institución de educación superior con liderazgo, el cual provee un bachillerato unificado enfocado en los nuevos reglamentos para la educación secundaria. La cual cuenta con una infraestructura de red amplia que se distribuye para todo el sector administrativo, educativo y de servicios. La institución cuenta con un enlace de tres megas la cual se distribuye para la parte de laboratorios y red inalámbrica así como también hacia algunas estancias administrativas. El problema que presentaba en la Unidad Educativa Baños es la falta de control y monitoreo de los servicios de comunicación, dando lugar al objetivo principal que es el de presentar un diseño de un sistema de gestión de red para el control y distribución del tráfico en la red LAN de la institución. El propósito del presente proyecto es establecer las bases del funcionamiento de un sistema de gestión de red utilizando la tecnología existente en la institución y lograr proporcionar el servicio de red de una manera rápida, eficiente y segura, como una alternativa para el mejoramiento del funcionamiento de los servicios de comunicación de dicha institución, con el cual se logrará tener control total sobre la red en un tiempo extremadamente pequeño. Con el avance de la tecnología de redes, los responsables del control a nivel institucional ahora pueden tener una verdadera solución integrada y altamente rentable que ayude a garantizar calidad del servicio y control total de la distribución de estos servicios.

ABSTRACT

The Baños Education Unit is an institution of higher education leadership, which provides a unified school focused on new regulations for secondary education. This has a wide network infrastructure that is distributed to administrative sector, educational and service sector. The institution has a link three MB which is distributed to the part of laboratories and wireless network as well as to some administrative stay. The problem presented in the Baños Education Unit is the lack of control and monitoring of communications services, leading to the main objective is to present a design of a system network management for the control and distribution of traffic LAN network of the institution. The purpose of this project is to establish the basis of the functioning of a network management system using existing technology in the institution and achieve network service providing a fast, efficient and safe manner, as an alternative for improving the functioning of communication services of the institution, with which it achieved full control over the network in an extremely small time. With the advancement of network technology, the controllers at the institutional level can now have a real help to ensure service quality and total control of the distribution of these services highly integrated and cost effective solution.

Glosario de términos y acrónimos

MikroTik RouterOS.- es el sistema operativo y software del router el cual convierte a una PC Intel ó un MikroTik RouterBOARD™ en un router dedicado.

CENTOS(acrónimo de Community Enterprise OperatingSystem) es un clón a nivel binario de la distribución Red Hat Enterprise Linux, compilado por voluntarios a partir del código fuente liberado por Red Hat, empresa desarrolladora de RHEL.

DHCP.- (Protocolo de Comunicación de Host Dinámico), este protocolo, te permite comunicarte en este caso con un Servidor (Host), que te asigna una dirección IP dinámica, para que tu puedas comunicarte con otros equipos en la red.

SSH (Secure Shell).- es el nombre de un protocolo y del programa que lo implementa, y sirve para acceder a través de una red. Permite manejar por completo la computadora mediante un intérprete de comandos, y también puede redirigir el tráfico de X para poder ejecutar programas gráficos si tenemos un Servidor X (en sistemas Unix y Windows) corriendo.

DNS (DomainNameSystem).- es un sistema de nomenclatura jerárquica para computadoras, servicios o cualquier recurso conectado a Internet o a una red privada. Este sistema asocia información variada con nombres de dominios asignado a cada uno de los participantes.

UTC.- que significa que el reloj del sistema utilizará UTC (Tiempo Universal Coordinado), que es el sucesor de GMT (b>Greenwich Mean Time, que significa Tiempo Promedio de Greenwich).

ROOT.- súper usuario en las distribuciones de Linux, el cual tiene todos los permisos necesario para copiar, borrar o modificar todo un sistema desde su raíz.

SERVIDOR PROXY.- es un equipo intermediario situado entre el sistema del usuario e Internet. Puede utilizarse para registrar el uso de Internet y también para bloquear el acceso a una sede Web

RRDtool (Round Robin Database Tool).- Es una herramienta que funciona con una base de datos que controla la planificación según Round-Robin. La función principal es el tratamiento de datos temporales y datos seriales como temperaturas, transferencias en redes, cargas del procesador, etc.

F/oss (Software libre y de código abierto) .- Es el software que está licenciado de tal manera que los usuarios poseen la capacidad de estudiar, modificar y mejorar su diseño mediante la disponibilidad de su código fuente.

MIBs .- Base de Información Gestionada (Management Information Base o MIB) es un tipo de base de datos que contiene información jerárquica, estructurada en forma de árbol, de todos los dispositivos gestionados en una red de comunicaciones.

OIDs .- (Identificador único de objeto) Es un valor único global asociado con un objeto que lo identifica definida por el estándar de la ITU y de la Organización Internacional para la Normalización (ISO). Los OID son utilizados por múltiples protocolos para identificar autoridades de asignación y registros. Una autoridad de asignación, definida por un OID, es un sistema capaz de nombrar objetos.

GNU/GLP.- La Licencia Pública General de GNU o más conocida por su nombre en inglés GNU General Public License es la licencia más ampliamente usada en el mundo del software y garantiza a los usuarios finales la libertad de usar, estudiar, compartir y modificar el software.

ISP.- (Proveedor de Servicios de Internet) Es una empresa que brinda conexión a Internet a sus clientes. Un ISP conecta a sus usuarios a Internet a través de diferentes tecnologías tales como ADSL, DSL Dial -up, GSM, etc.

NAT.- (Network Address Translation - Traducción de Dirección de Red) es un mecanismo utilizado por routers IP para intercambiar paquetes entre dos redes que asignan mutuamente direcciones incompatibles.

RFC 1918.- Es un estandar internacional donde se define el rango de direciones disponibles para redes privadas clase A, B y C.

VLSM.- Es el resultado del proceso por el cual se divide una red o subred en subredes más pequeñas cuyas máscaras son diferentes según se adaptan a las necesidades de hosts por subred

VNC.- Son las siglas en inglés de Virtual Network Computing. VNC es un programa de software libre basado en una estructura cliente-servidor el cual permite tomar el control del ordenador servidor remotamente a través de un ordenador cliente..

MV.- Son las siglas de máquina virtual y es un software que simula a una computadora y puede ejecutar programas como si fuese una computadora real.

INTRODUCCIÓN

Las redes cableadas e inalámbricas son de naturaleza dinámica y auto-configurables, presentan recursos limitados como ancho de banda, conectividad, capacidad de procesamiento, entre otros. La arquitectura de las redes son varias y están basadas en el estándar IEEE 802.3 y 802.11.

Los modelos de gestión para redes inalámbricas existentes no cubren todas las necesidades que presentan este tipo de redes y conservación de recursos garantizando la calidad de servicio en la red al igual que para redes cableadas el cual esta descrito por el estándar mencionado.

Con la finalidad de cubrir algunas de las deficiencias notables que presentan los modelos de gestión ya existentes se desarrolló la presente investigación para proponer un modelo de gestión que permita cubrir la mayoría de las necesidades para así maximizar la disponibilidad, mejorar la rapidez, eficacia y eficiencia de la red.

La investigación inicia desde lo propuesto en donde se utilizan técnicas de routing y switching para la segmentación de la red; esto es complementado con la propuesta de adherir de técnicas innovadoras basadas en una herramienta de inteligencia artificial como lo es los servidores Linux o software libre.

Este modelo se basa en técnicas de routing y switching para controlar la movilidad, el cambio de topología debido a la entrada y salida de equipos en la red, y para segmentar la red llevando la gestión de mejor manera en grupos.

Dentro del modelo se definen varias interfaces entre las cuales consta la comunicación entre un nodo y otro a través de dos tecnologías diferentes como lo es las redes inalámbricas y las LAN cableadas. Controladas directamente desde un servidor CentOS que es el software controlador del tráfico que sale a la web complementado con software libre que proporciona servicios de correo, mensajería instantánea, telefonía IP entre los servicios adicionales.

Las redes inalámbricas son una herramienta fundamental en una institución que propone adherir a su sistema un servicio de calidad a partir de los recursos existentes en la institución las cuales son un servidor HP Proliant ML 150 G, un

router MikroTik, switch 8 puertos Dlink, los cuales nos ayudaran en el transcurso del desarrollo de la investigación, aparte que se utilizara CentOS como servidor principal.

Con la finalidad de unificar todas las teorías de la presente investigación, se propone incrementar dentro de la fase de implementación técnicas para la optimización de las redes, distribuyendo de una mejor manera el ancho de banda que se dispone en el nodo principal de la red, determinando si es necesario o no la instalación de un nodo adicional que garantice la calidad del sistema reduciendo así los posibles errores y pérdidas de conexión y obtener mejores resultados manteniendo la red por más tiempo evitando el desgaste de recursos, esto a través de la utilización de un modelo de confianza que permita decidir a los nodos con que nodo cooperar y con cuál no. Es decir que se tendría un nodo auxiliar que proporcione estabilidad en el sistema.

Después de investigar, analizar y estudiar los diferentes métodos de redes que se aplicarían en la propuesta utilizaremos las técnicas descritas para la implementación con el fin de mejorar la calidad de servicios para mejorar la gestión de la red y maximizar su rendimiento de los nodos, se propone un modelo unificando estas dos técnicas a base de software libre.

CAPÍTULO 1

El problema

1.1. Tema de Investigación

Sistema de gestión de redes para el control y distribución del tráfico en la red LAN de la Unidad Educativa Baños del cantón Baños.

1.2. Planteamiento del problema

A nivel nacional la gestión de redes es aplicada en la mayoría de instituciones, empresas públicas y privadas con el único fin de garantizar la calidad de los servicios de telecomunicaciones. La integración del software y Hardware con el elemento humano se conjuga para garantizar la funcionalidad de los sistemas de redes obteniendo como resultado un nivel tecnológico acorde a las exigencias nacionales e internacionales.

A nivel de Tungurahua las empresas e instituciones utilizan sistemas de gestión con la capacidad de organizar, desplegar y controlar todos los recursos de red necesarios para conseguir un fin pre-establecido que garantice el bien institucional, fomentando la aplicación de tecnologías actuales que proporcionan la integración de servicios como voz sobre IP, video conferencias y trasmisión de datos a altas velocidades.

En la unidad educativa Baños el sistema funciona en base a las configuraciones por defecto de los equipos de red, subutilizando el Software y Hardware los cuales son diseñados para brindar servicios óptimos en la red.

Con el aumento de la tecnología y a la vez de servicios que se aplican sobre una red, inician los problemas de control de acceso. Las redes se saturan por la cantidad de terminales transmitiendo información, y la pérdida de datos es más probable si no se realiza un control de cada una de las áreas de trabajo, ya que de igual forma existen usuarios con privilegios tales como los departamentos administrativos que necesitan una conexión permanente a la red. Todas estas normas serían las políticas

de acceso que se aplicarán sobre el sistema.

1.3. Delimitación

Área Académica: Programación y Redes

Línea de Investigación: Programación y Redes

Sublínea de investigación: Administración de Redes.

Delimitación espacial: Tungurahua, Baños de Agua Santa, Matriz, Unidad Educativa Baños, avenida Amazonas y vía El Salado

Delimitación Temporal: El presente proyecto de investigación tendrá una duración de 6 meses, a partir de que éste sea aprobado por el Honorable Consejo Directivo de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial.

1.4. Justificación

La gestión de redes es un complemento importante ya que es la combinación de Software y Hardware para conseguir el mayor rendimiento a la red de datos. Integrar más servicios es una de las metas de las comunicaciones avanzadas, sin descartar el control de los recursos de red como un punto fundamental en la generación de conocimientos educativos.

La tecnología que existe en la actualidad es la premisa más importante en el desarrollo de la investigación, ya que se analizaran las mejores técnicas para el manejo de la información sobre redes de datos basadas en software libre.

El proyecto es factible ya que no representa un gran costo de inversión y se dispone de Hardware de red en la institución, se cuenta con el aval y apoyo institucional para realizarlo, ayudando así cada vez más al crecimiento del nivel académico, por medio de este a sus numerosos estudiantes, maestros, personal administrativo y de servicios.

Los beneficiarios serán todos los usuarios de los laboratorios, departamentos administrativos y los estudiantes que registren sus dispositivos móviles justificando sus necesidades de acceso a la red inalámbrica de la institución, estos contaran con el acceso a la red según las normas establecidas en las políticas de control mejorando así la calidad del servicio.

Por lo cual la aplicación de este tipo de investigación se traduce en un avance no solo para la institución sino también a nivel tecnológico, ya que se analizara los diferentes tipos de software Hardware y protocolos de administración existentes, los cuales serán parte del estudio mejorando la calidad del servicio.

1.5. Objetivos

1.5.1. General

Diseñar un sistema de gestión de redes para el control y distribución del tráfico en la red LAN de la Unidad Educativa Baños de cantón Baños.

1.5.2. Específicos

- Analizar la red de datos de la institución para determinar fallos y deficiencia de la red.
- Determinar las herramientas de software y Hardware necesarias para la aplicación de las políticas de control de acceso
- Analizar los métodos existentes de control y distribución del tráfico en redes de datos.
- Diseñar el sistema de gestión de red aplicando las políticas de acceso determinadas para la institución.

CAPÍTULO 2

Marco Teórico

2.1. Antecedentes Investigativos

Revisando los repositorios digitales de las diferentes Universidades y Politécnicas, se encontró un tema similar a la investigación donde a través de un análisis pormenorizado del software libre se logra una administración zonal, en este estudio se determinó los tipos de gestión existentes y luego se escogió el más idóneo para la aplicación. Entre los software libre que estudio están el nagios, ntop, openNMS, webmin tomando sus principales características técnicas, logrando así dar una amplia gama de soluciones a la administración de redes. [1] De igual manera se encontró otra investigación en donde a través del análisis del software libre combinado con el estudio del protocolo SNMP se realizó una gestión eficiente en la empresa aplicada, entre los software analizados se encuentran CACTI, ZENOSS, ZABBIX, de los cuales se utilizó ZENOSS como opensource de administración logrando establecer los parámetros establecidos y mejorando la calidad del servicio tanto para el proveedor como para los usuarios. [2]

La aplicación de software libre en las instituciones en la actualidad se dio gracias a la intervención del ejecutivo con la aplicación de la resolución 1014 en donde se obliga a las instituciones públicas a migrar al software libre como base tecnológica en la enseñanza diaria. Esto lleva a la actualización general de todos los sistemas, sin embargo no se han aplicado del todo ya que se utiliza en la administración de redes, pero a través de las investigación se dará un giro total en la gestión de redes, este tipo de investigaciones ayudan al ser humano a darse cuenta de los alcances de las tecnologías actuales, integrando varios conceptos nunca antes aplicados, las comunicaciones avanzadas inician las premisas necesarias para la unificación de los servicios, es decir que no es necesario estar personalmente en el sitio de falla, sino más bien desde cualquier punto acceder al control total de los dispositivos de redes utilizados.

Al unir varios conceptos se logra unificar las redes, ya que no existe un solo software que nos garantice la coexistencia total de todos los equipos de una red, esto se debe a los derechos de autor de cada uno de los dispositivos, ya que en ninguna red se logrará tener un solo tipo de Hardware por el costo que representaría, es decir de la misma marca, por lo que se estudia el protocolo de gestión SNMP que es compatible con la mayoría de las marcas de equipos utilizadas en las redes de datos.

2.2. Fundamentación teórica

La gestión de redes incluye varios factores tales como la integración y coordinación del Hardware, software y factores humanos para monitorear, probar, configurar, evaluar y controlar los recursos de la red y conseguir los requerimientos en tiempo real con un buen desempeño, a un precio accesible para la institución en la que se aplicara esta gestión.

Este conjunto de actividades están dedicadas a un solo fin el de gestionar, controlar y distribuir de una manera eficiente los recursos de toda red de comunicaciones, con el objetivo general de garantizar un nivel de servicio confiable con las mejores prestaciones. Y proporciona una amplia gama de software, Hardware para la gestión hacia dentro de la red y hacia la nube garantizando la navegación de una manera confiable con las debidas seguridades del sistema.

A continuación se realizara un análisis de los tipos de gestión existentes, software y Hardware relacionados a la gestión con sus respectivos cuadros de características para luego concluir el estado del arte con una descripción general de otro tipo de investigación con un fin semejante además de una descripción de la ley de educación en donde exige la utilización de software libre para instituciones [3].

2.3. GESTIÓN DE RED

La gestión de redes según varios autores se define como un proceso en el que involucra varios factores tales como los mencionados por [4] en donde dice La gestión de redes incluye el despliegue, integración y coordinación del Hardware, software y los elementos humanos para monitorear, probar, sondear, configurar, analizar, evaluar y controlar los recursos de la red para conseguir los requerimientos de tiempo real, desempeño operacional, calidad de servicio a un precio razonable. Por lo que se determinó que la gestión de red es una de las partes más importantes para una institución que utiliza las tecnologías actuales.

2.4. GESTIÓN INTEGRADA

Es la solución a la gestión heterogénea ya que permite enlazar distintos dispositivos y generar un solo sistema de gestión integrado para toda la red y con una sola interfaz de usuario, esto nos da la posibilidad normalizar las comunicaciones mediante la utilización de protocolos de comunicación entre los elementos de la red y el centro de gestión (SNMP). Otra de sus características se destacan la normalización de la información para la gestión de redes lo que proporciona conectividad entre toda una red.

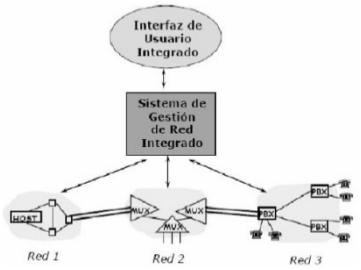


Figura 2.1: Gestión de Red Integrada
Fuente: Proyecto de Investigación – Gestión de Redes [5]

Se observa en la figura Nº 1 un sistema de gestión integrada, en donde existe la normalización de la información. El centro de gestión debe conocer a los elementos pertenecientes a la red mediante un nombre o identificación y sus propiedades deben estar visibles al gestor, es decir que desde el centro de control se debe poder acceder a cualquier punto de la red de comunicación, para controlar i/o corregir posibles fallos del sistema sin un desplazamiento previo al punto [5].

2.5. SNMP (Simple Network Management Protocol)

Dado que la tendencia natural de una red [6] es crecer constantemente conforme se añade nuevas aplicaciones o nuevos usuarios, los sistemas de gestión deben ser lo más flexibles al incremento o cambios en su entorno sin tener que realizar cambios drásticos en su sistema original. Este punto es uno de los más relevantes de la teleinformática, ya que prácticamente no existe una solución única, sino más bien varias soluciones de tipo propietarios, es decir creada por cada fabricante como por ejemplo Netview de IBM, OpenView de HP, etc.

Según la revista [7] SNMP es un conjunto de aplicaciones de gestión de red que emplea servicios ofrecidos por TCP/IP, Protocolo de mundo UNIX que ha llegado a convertirse en un estándar para la gestión de red, surge a raíz del interés mostrado por IAB (Internet Activities Board) que quería encontrar un protocolo compatible

con las red más grande del mundo el Internet. Inicialmente se tenía tres grupos de trabajo que desarrollaron este protocolo llegando cada uno a distintas conclusiones, siendo adoptado el SNMP (RFC 1098), incluyendo algunos aspectos relevantes de las otras investigaciones. En la Figura Nº 2 se observa las capas para la transmisión de información a través de este protocolo de gestión de redes desde un punto hacia otro.

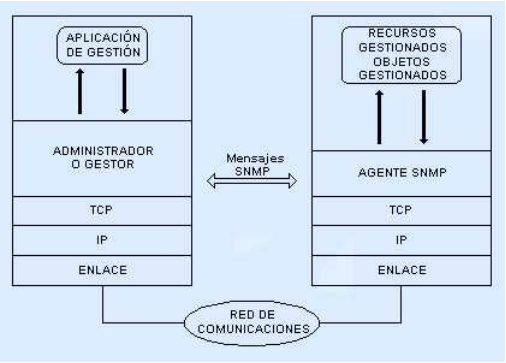


Figura 2.2: Protocolo de Gestión SNMP
Fuente: SNMP, Un Protocolo Simple de Gestión [6]

Para el protocolo SNMP la red constituye un grupo de elementos básicos Administradores o Management Stations ubicados en los equipos de gestión y los gestores o agentes (elementos pasivos tales como host, routers, modems) que son los que envían información a los administradores de la situación de la red.
Su principal inconveniente es el exceso de tráfico que se genera en el sistema, lo que puede ocasionar incompatibilidad a los entornos amplios de red; por lo que los protocolos CMIS/CMIP (Common Management Information Service/Protocol) de OSI ofrece un mejor rendimiento y seguridad en la red, estado estos orientados a la administración de entornos amplios.

2.5.1. MIB (Management Information Base)

Se define como una amplia base de datos contenida de la gestión, memoria interna del dispositivo usado, es una base de datos completa y bien definida. Con una estructura en árbol adecuada para manejar diversos grupos de objetos, detallada en RFC 1066 (Base de información de gestión para la gestión de redes sobre TCP/IP) [8].

2.6. OPENFLOW

OpenFlow es un protocolo que permite al servidor tener plena comunicación con cada dispositivos de la red ya sea conmutador o host. En un conmutador convencional la transferencia de paquetes y el enrutamiento de alto nivel suceden el mismo dispositivo, en un conmutador OpenFlow separa la trayectoria de datos de la de control. La trayectoria de datos yace en el mismo conmutador; un conmutador separado realiza el enrutamiento de alto nivel en donde el conmutador y el controlador se comunican por el protocolo OpenFlow. Esto permite a la red el uso efectivo de sus recursos y es posible aplicarlo sobre redes tradicionales esta metodología se denomina SDN que son redes definidas por software, es decir que el control de la red se desprende del Hardware y el software es el encargado de dominar los servicios de red, a este software se lo denomina controlador. En la figura Nº 3 se presenta los alcances del protocolo opensource para la administración de redes.

Figura 2.3: Open Flow
Fuente: OpenFlow [9]

La preferencia por este protocolo ha incrementado en aplicaciones como movilidad de máquina virtual, redes críticas para misión y redes móviles basadas en IP de nueva generación. Muchas empresas establecidas como IBM, Google y HP han utilizado completamente o han anunciado su intención de soportar este protocolo ya que también funcionan sobre redes tradicionales, lo que hace posible colocar máquinas virtuales en cualquier punto dentro del centro datos para recuperar la capacidad de computación varada [9].

2.7. SEGURIDAD DE REDES

El aspecto de la seguridad en las redes y ordenadores es un tema prioritario en la actualidad para la mayoría de las empresas, ya que los incidentes de seguridad se traducen en numerosas ocasiones en pérdidas millonarias o en pérdidas de confianza por parte de los usuarios de dichas redes [10].

La protección de las redes de computadores no es una tarea sencilla ya que reúne en si todos los elementos de la red. Las áreas fundamentales de la seguridad son:

- Protección de computadores.
- Protección de redes
- Cifrado y autenticación de la información.

2.8. SOFTWARE PROPIETARIO

Es aquel software informático en el cual el usuario tiene varias restricciones tales como el poder copiarlo, modificarlo y compartirlo, y no se tiene acceso al código fuente del programa, es decir que cualquiera que tenga acceso a este programa no puede redistribuirlo por los derechos del autor que se otorga al creador del programa o empresa que lo publica, para poder acceder al código fuente y hacerle mejoras se necesita una autorización previa del autor por lo que al publicar estas mejoras sigue perteneciendo el software al propietario original y todos sus derechos[11].

2.9. SOFTWARE LIBRE

En [12] dice El software respeta la libertad de los usuarios y la comunidad, es decir que los usuarios tienen la libertad de copiar, modificar, estudiar, distribuir y mejorar el software, con estas libertades el programador controla lo que hace el programa no el programa al usuario.

Un programa se considera software libre si cumplen las cuatro libertades esenciales:

1. Libertad de ejecutar el programa para cualquier propósito.
2. Libertad de estudiar cómo funciona el programa y cambiarlo para que haga lo que quiera (el acceso al código fuente es una condición necesaria).
3. Libertad de redistribuir copias para ayudar a su prójimo.
4. Libertad de distribuir copias de sus versiones modificadas a terceros (permite a la comunidad beneficiarse se las mejoras).

2.10. 2.10 CALIDAD DE SERVICIO (QoS)

El QoS es uno de los puntos más importantes en las aplicaciones de redes ya que dependiendo de las aplicaciones se considerara la importancia de la rapidez del

servicio ósea en aplicaciones en tiempo real no se pueden ocasionar interrupciones o pérdidas del enlace ya que esto significaría un mala calidad del servicio lo que ocasiona molestias por parte de los usuarios, como consecuencia una mala reputación ser administrador en los estudios realizados por el estándar 802 para los diferentes tipos de redes se han establecido muchos parámetros tales como velocidades, arquitecturas, dimensionamiento entre otras. Una de las características más importantes para el correcto funcionamiento de redes es la calidad del servicio que para redes Ethernet se establece por el estándar 802.1p en donde se establece como clases de servicios otorgados. En redes de Internet se considera "best effort" es decir sin ninguna garantía de calidad del servicio que con el paso de los años se ha ido mejorando y cambiando este paradigma a través de diversas técnicas [13].

Algunas aplicaciones como voz y video, son sensibles al retardo pero insensibles a la pérdida de datos; otras como transferencia de ficheros y el correo electrónico son insensibles al retardo pero sensible a las pérdidas; otras más como los gráficos interactivos o aplicaciones de computo interactivo, son sensibles tanto al retardo como a las pérdidas. Por otra parte, hay que señalar que flujos de tráfico distintos tienen prioridades diferentes; por ejemplo, el tráfico de gestión de red, en particular durante la ocurrencia de congestión o fallos es mucho más importante que el tráfico de aplicación [14].

2.11. Propuesta de Solución

De acuerdo a lo analizado anteriormente se logrará obtener un control total de la red de la institución, aplicando las políticas de acceso establecidas para cada una de las áreas y usuarios de la red, a través del software y Hardware.

CAPÍTULO 3

Metodología

3.1. Modalidad Básica de la investigación

El desarrollo de la investigación tiene la premisa necesaria para la fundamentación metodológica a través de una investigación aplicada que garantizo de manera transparente los procesos a realizar, y así alcanzar las metas establecidas. Esta se la realizo mediante el análisis de teorías aplicadas, proponiendo de mejor manera nuevos procesos que representa la mejora contínua o en un desarrollo exponencial de las nuevas tecnologías.

El tema requirió de la investigación de campo porque permitió recopilar la información desde donde se está produciendo el problema, la misma que permitió manejar los datos fidedignos y reales, los cuales oriento al análisis concreto del problema. Facilito el contacto directo con la realidad de la que se obtuvo los datos necesarios para el análisis del problema.

Se concurrió a la investigación bibliográfica, que facilitará ampliar y profundizar la información, y orientar a la aplicación de leyes y principios en los que se baso la parte técnica para dar la solución al problema, con el cual se logró cumplir con los objetivos propuestos.

La investigación se desarrollo con un enfoque cuali-cuantitativa en la cual la recopilación de información se realizo mediante la técnica de observación directa que permitió al investigador estar en contacto con el problema, y recopilar datos de manera estructurada.

3.2. Plan de recolección de información

La recolección de información se inicio previa a la visita de reconocimiento y presentación del proyecto de investigación, utilizando como recurso tablas comparativas, entrevista y fichas de observación.

3.3. Procesamiento y análisis de la información

Una vez que se ha obtenido la información apropiada de la investigación, esta formará parte de un proceso estadístico, el cual consiste en la tabulación de los datos, de forma ordenada y sistemática. El análisis de los resultados se presentará en cuadros estadísticos pastel destacando las tendencias o relaciones fundamentadas de acuerdo a los objetivos La revisión y la codificación de los resultados permitirán detectar los errores, omisiones y eliminar respuestas contradictorias y organizando para facilitar la tabulación.

3.4. Desarrollo del Proyecto

Para el desarrollo de la investigación se efectuaron los siguientes pasos:

- Análisis del estado actual de la red de la Unidad Educativa Baños.
- Determinación de los requerimientos a partir de los problemas encontrados en los sistemas de gestión actuales.
- Análisis de los métodos y alternativas de solución que se encontraron a partir de las necesidades.
- Selección de la mejor alternativa para mejorar el control y distribución del tráfico de red LAN de la institución.
- Diseño del sistema de gestión para el control y distribución del tráfico en la red del instituto aplicado.
- Implementación y configuración los dispositivos de red para que reconozca las diferentes rutas y capacidades asignadas a cada una de las áreas controladas.
- Evaluación del sistema de gestión mediante pruebas de funcionamiento.

CAPÍTULO 4

Desarrollo de la propuesta

4.1. Datos Informativos

4.1.1. Tema de la Propuesta

"Sistema de Gestión de redes para el control y distribución del tráfico en la red LAN de la Unidad Educativa Baños del cantón Baños"

4.1.2. Institución Ejecutora

- **Institución Educativa:** Unidad Educativa Baños
- **Tipo de Organización:** Pública
- **Departamento:** Administración de Redes

4.1.3. Beneficiarios

- Unidad Educativa Baños
- Profesores, Estudiantes
- Personal administrativo y de servicio de la institución.

4.1.4. Ubicación

- **Provincia:** Tungurahua
- **Cantón:** Baños de Agua Santa
- **Dirección:** Av. Amazonas y El Salado
- **Teléfono:** 032740408

4.2. Objetivos

4.2.1. General

Diseñar el sistema de gestión de redes para el control y distribución del tráfico en la red LAN en la unidad educativa Baños.

4.2.2. Específicos

- Analizar el estado actual de la red LAN para determinar fallos y deficiencias.
- Determinar las herramientas de Hardware y Software necesarios para la aplicación de la propuesta
- Establecer las Políticas de control acceso a la red LAN.
- Diseñar el sistema de gestión de red aplicando las políticas de acceso determinadas para la institución.
- Realizar las pruebas de funcionamiento en la red LAN.

4.3. Análisis de Factibilidad

Un estudio de factibilidad permite determinar si se cuenta con los recursos suficientes para cumplir las objetivos de la investigación por lo que es necesario analizar la factibilidad:

- Institucional
- Técnica
- Operativa
- y Económica

4.3.1. Factibilidad Institucional

El implementar un proyecto el cual brinde una re-estructuración de la red LAN institucional es de gran utilidad ya que permite al administrador tener un mayor control sobre los servicios de red, el acceso a la tecnología representa una necesidad básica para el proceso de enseñanza aprendizaje de la Unidad Educativa Baños. Tanto profesores, estudiantes, personal administrativo y de servicio utilizan el servicio de Internet ya sea en los laboratorios o a través de la red inalámbrica por lo que renovar el sistema es primordial para el crecimiento institucional.

4.3.2. Factibilidad Técnica

La implementación del presente proyecto de investigación es factible técnicamente, ya que se basa en mecanismos de configuración avanzados para el control del tráfico en la red LAN, se enfoca en el uso de recursos básicos en una red por lo que se puede decir que el proyecto es una alternativa de uso para cualquier institución con recursos limitados, fomentando el estudio de alternativas tecnológicas.

4.3.3. Factibilidad Operativa

En este punto el proyecto es factible ya que se cuenta con el aval de la institución para la utilización de la infraestructura física y los equipos existentes, además se dispone de los recursos humanos y tecnológicos para la aplicación de teorías como base fundamental para la investigación.

4.3.4. Factibilidad Económica

El presente proyecto de investigación es factible económicamente ya que se dispone del Hardware perteneciente a la institución y además debido existencia del software libre como un recurso accesible de manera gratuita. Los recursos adicionales que se requieran se encuentran cubiertos por el investigador.

4.4. Etapas para el desarrollo de la propuesta

Las etapas para el desarrollo de la investigación se plantean en base a los objetivos que se deben cumplir.

4.4.1. Analizar el estado actual de la red LAN para determinar fallos y deficiencias

- Análisis del Hardware y Software existentes
- Descripción del esquema de red institucional.
- Análisis del estado actual de la red LAN.
- Determinación de los problemas detectados en la red.

4.4.2. Determinar las herramientas de Hardware y Software necesarios para la aplicación de la propuesta

- Determinar los requerimientos de Hardware

- Análisis de distribuciones GNU/Linux para la aplicación sobre el servidor HP Proliant ML150.
- Establecer y analizar los requerimientos del Software.
- Analizar la virtualización de los servicios de red con sistemas de respaldo.
- Análisis de los servicios necesarios para la gestión de redes LAN
- Analizar Software de monitoreo de redes LAN

4.4.3. Establecer las Políticas de control acceso a la red LAN

- Establecer las Políticas Generales en base a estándares de gestión de redes.
- Establecer las Políticas específicas aplicadas en la red.

4.4.4. Diseño del sistema de gestión en base a las políticas de control de acceso

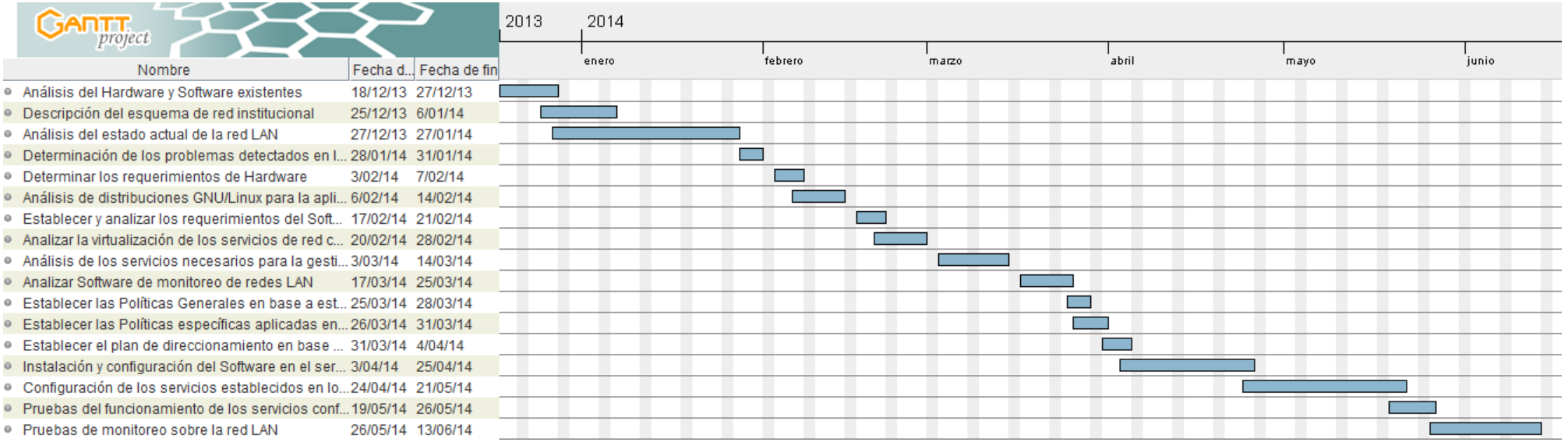
- Establecer el plan de direccionamiento en base a las necesidades de la red LAN.
- Instalación y configuración del Software en el servidor HP Proliant ML 150
- Configuración de los servicios establecidos en los equipos de red.

4.4.5. Pruebas de Funcionamiento

- Pruebas del funcionamiento de los servicios configurados.
- Pruebas de monitoreo sobre la red LAN.

4.4.5.1. Diagrama de Gantt

Para el desarrollo de las etapas del proyecto es necesarios establecer un diagrama en base a los tiempos de ejecución de la propuesta con fecha desde 18/12/2013 hasta 18/06/2014.



Nombre	Fecha d...	Fecha de fin
Análisis del Hardware y Software existentes	18/12/13	27/12/13
Descripción del esquema de red institucional	25/12/13	6/01/14
Análisis del estado actual de la red LAN	27/12/13	27/01/14
Determinación de los problemas detectados en l...	28/01/14	31/01/14
Determinar los requerimientos de Hardware	3/02/14	7/02/14
Análisis de distribuciones GNU/Linux para la apli...	6/02/14	14/02/14
Establecer y analizar los requerimientos del Soft...	17/02/14	21/02/14
Analizar la virtualización de los servicios de red c...	20/02/14	28/02/14
Análisis de los servicios necesarios para la gesti...	3/03/14	14/03/14
Analizar Software de monitoreo de redes LAN	17/03/14	25/03/14
Establecer las Políticas Generales en base a est...	25/03/14	28/03/14
Establecer las Políticas específicas aplicadas en...	26/03/14	31/03/14
Establecer el plan de direccionamiento en base ...	31/03/14	4/04/14
Instalación y configuración del Software en el ser...	3/04/14	25/04/14
Configuración de los servicios establecidos en lo...	24/04/14	21/05/14
Pruebas del funcionamiento de los servicios conf...	19/05/14	26/05/14
Pruebas de monitoreo sobre la red LAN	26/05/14	13/06/14

Figura 4.1: Diagrama de Gantt para el desarrollo de la propuesta
Elaborado por: El investigador

4.5. Análisis del estado actual de la red Institucional

4.5.1. Análisis de Hardware y Software existente

Es necesario conocer el estado de los equipos de red existentes, para entender el modo de operación y encaminar de mejor manera la investigación.

4.5.1.1. Hardware existente en la red Institucional

La Institución cuenta con una conexión de 3 a 1 MB asimétricos proporcionado por el ISP de CNT a través de un módem ADSL.

Para esto se verifica las especificaciones generales del Hardware de red existente:

Equipo	Descripción General	Estado del Equipo
MikroTik RB751U-2HND	Cuenta con 5 interfaces de red 10/100 y un procesador de 400 MHz, logra un rendimiento (throghput) de hasta 450 Mbps en total y hasta 92000 paquetes por segundo con frames de 64 bytes	Funcionando con dos subredes clase C privadas.
Modem CNT	Modem ADSL con una conexión de 3 a1 Mbps	Modo NAT
2 Switch Dlink DES-1008D	Posee 8 puertos no administrados, switch Fast Ethernet de D-Link permite enchufar cualquier puerto de una Ethernet de 10 Mbps o 100 Mbps.	Interconexión LAN
Nano Station 2 Ubiquiti	Ubiquiti NANOSTATION 2 2.4GHz. 10dBi	Access Point
2 Switch Dlink DES-1024D	El DES-1024D de 24 puertos Fast Ethernet Switch no administrado, este dispositivo entrega puertos a una red de 10Mbps o 100Mbps para multiplicar los anchos de banda. Con velocidades de hasta 200 Mbps por puerto en modo full-duplex.	Laboratorio 1 Laboratorio 2
Servidor HP Proliant ML 150	ML150 G6: Quad-Core Intel Xeon E5504, soporta hasta 2 procesadores 10GB PC3-10600E DDR3. HP Smart Array P410 controller w Zero Memory cache RAID (0/1/0+1) Embedded HP NC107i PCI Express Gigabit Server Adapter iLO100i Half-Height SATA DVD-ROM	Inactivo

Tabla 4.1: Hardware Disponible

Elaborado por: El Investigador

Una vez realizado el análisis de Hardware se determino que la instutución cuenta con un equipo servidor el cual no realiza ninguna actividad en la red.

Armario de Comunicaciones existente

La institución cuenta con una área específica para la colocación del Hardware de red, la cual no tiene una distribución adecuada. En la siguiente imagen se muestra

la realidad física del armario de communicaciones existente en la institución.

Figura 4.2: Armario de comunicaciones existente
Elaborado por: El investigador

Como se observa en la imagen la disposición de los equipos de red no cumple con ningun estandar establecido para la gestión de redes.

4.5.1.2. Software Existente en la red Institucional

En donde se describe el tipo de software que incorpora los equipos principales de la red.

Equipo	Software Utilizado	Licencia
MikroTik RB751U-2HND	MikroTik RouterOS la versión 7.x	Nivel 4
Servidor HP Proliant ML 150	Windows Server 2008	Obsoleto
Nano Station 2 Ubiquiti	AirOS v 5.0	Activo

Tabla 4.2: Software Usado

Elaborado por: El Investigador

4.5.1.3. Servicios disponibles

Los servicios que dispone la red son:

- Servidor DNS configurado en la MikroTik

- Limitación del ancho de banda por usuarios
- Registro de usuarios con Queue List en la MikroTik

4.5.2. Estructura de la Red Institucional

Esquema sintetizado de la red de datos institucional con todos los equipos disponibles para la investigación.

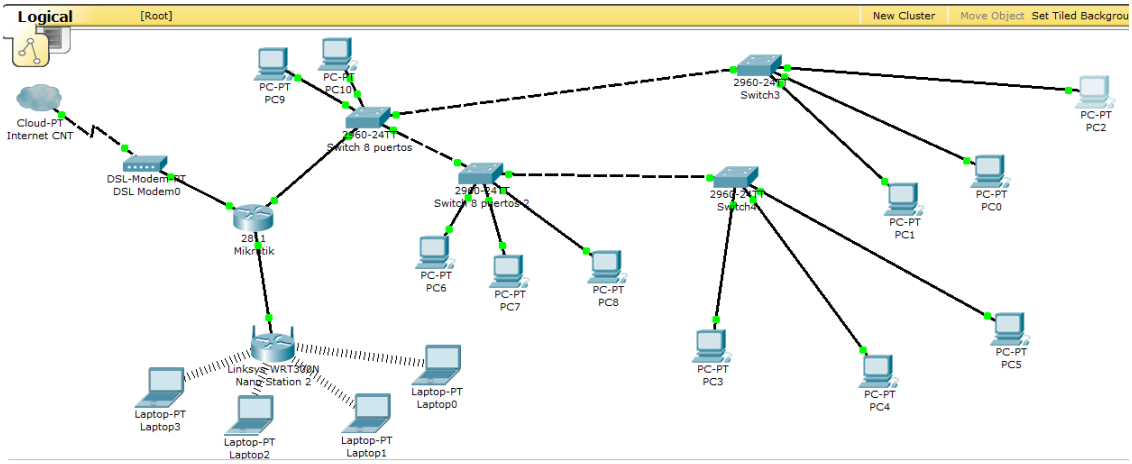


Figura 4.3: Descripción de la Red Institucional
Elaborado por: El investigador

La imagen muestra la realidad actual de la red que utiliza dos subredes, la 192.168.100.0/24 para la red Inalámbrica y la 192.168.10.0/24 para la red cableada a partir de estos datos se analiza el estado de la red LAN.

4.5.3. Análisis del estado actual de la red

Para analizar el estado de la red es necesario utilizar un software de monitoreo el cual capture información para posteriormente determinar los problemas existentes.

4.5.3.1. Software de Análisis WIRESHARK

En informática es un programa especializado en monitoreo y análisis que captura tramas o paquetes de una red de datos. El software informático que puede interceptar y registrar tráfico de paquetes sobre una red de datos. Tiene varios usos como por ejemplo detección de cuello de botella, análisis de falencias en la red, o fines maliciosos.

Figura 4.4: Wireshark
Elaborado por: El investigador

Características Generales

- Pertenece a los analizadores de red de software libre.
- Posee una interfaz agradable al usuario, tiene muchas opciones de organización y filtrado de la información.
- Es compatible con otros tipos de redes no solo LAN.
- Examina datos en tiempo real y de capturas anteriores.
- Da detalles, sumarios y un lenguaje completo para el filtrado y análisis de los paquetes.

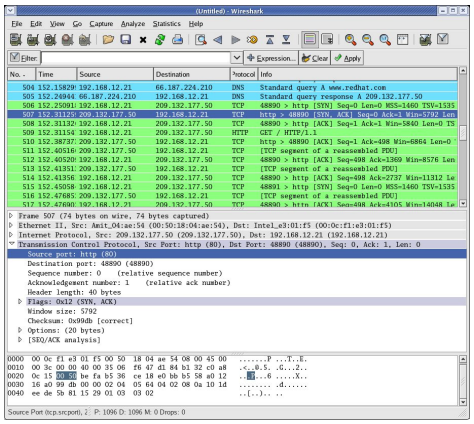


Figura 4.5: Entorno Wireshark
Elaborado por: El investigador

4.5.3.2. Distribución de equipos para el análisis de la red LAN

Esquema en donde se visualiza el análisis de tráfico a través de un HUB intermedio entre la MikroTik y la Nano Station 2 para la red inalámbrica. Para la red cableada se coloca el HUB entre la MikroTik y el switch de distribución en diferentes horarios.

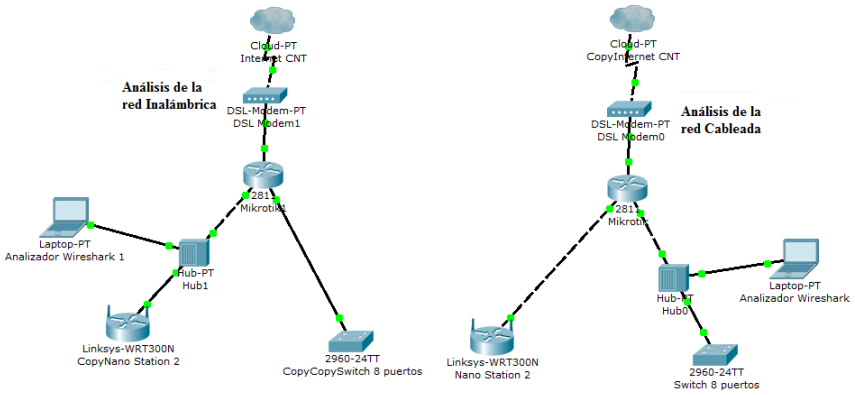


Figura 4.6: Descripción de la red al analizar la red
Elaborado por: El investigador

4.5.3.3. Horario de Captura de la Información

RED	Intervalo de Tiempo	Día 1	Día 2	Día 3	Día 4	Día 5
Cableada	7:45 > 8:15	72189	14846	170706	10846	36172
Cableada	8:15 > 8:45	72189	43480	45261	14624	52302
Inalámbrica	12:09 > 12:39	16706	53238	15468	65901	52338
Inalámbrica	14:05 > 14:35	48390	34160	14846	19584	16484

Tabla 4.3: Horario de Captura de Información

Elaborado por: El investigador

Describe de forma detallada los horarios de captura realizado en la toma de información sobre la red Cableada e Inalámbrica durante cinco días con un tiempo de captura de 30 minutos.

4.5.3.4. Red Cableada

Red Cableada					
Captura	Día 1	Día 2	Día 3	Día 4	Día 5
Problemas encontrados	6	2	8	0	6
Advertencias	7	3	7	1	8
Tráfico Superior	UDP	UDP	TCP	UDP	TCP – UDP
Porcentaje tráfico UDP	98,38	85,12	21,1	47,63	12,84
Porcentaje tráfico UDP	12,84	77,09	90,38	37,06	59,39
Porcentaje tráfico TCP	5,58	7,1	56,59	8,64	80,19
Porcentaje tráfico TCP	80,19	3,04	5,58	15,34	26,94

Tabla 4.4: Descripción del Análisis de la red Cableada

Elaborado por: El investigador

Es un resumen de las herramientas usadas en la detección de errores en la red a continuación se presentara el procesamiento de los datos para definir las causas de dichos problemas.

Figura 4.7: Análisis Estadísticos de los Problemas Detectados
Elaborado por: El investigador

El número de errores encontrados es equivalente al número de advertencias los cuales se producen por el tipo de tráfico existente en la red ocasionando pérdidas de datos, peticiones incompletas, entre otros inconvenientes.

Presentación de la herramienta Protocol Hierarchy Stadistics

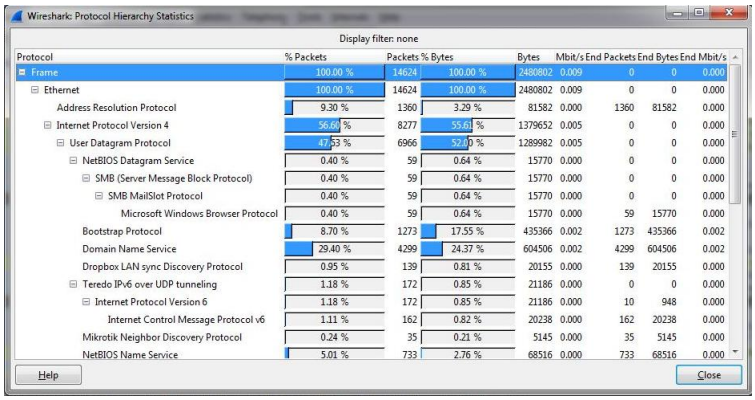


Figura 4.8: Uso de la Herramienta Protocol Hierarchy Statistics de Wireshark
Elaborado por: El investigador

Al analizar cada una de las capturas en los diferentes horarios se obtiene los siguientes resultados.

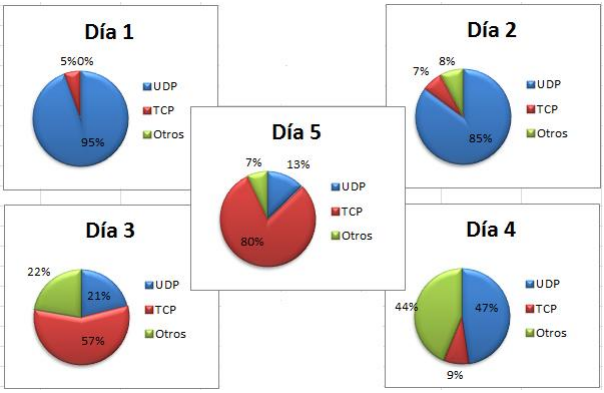


Figura 4.9: Presentación del Análisis de datos Red Cableada
Elaborado por: El investigador

El tráfico varía dependiendo del día en algunos casos se obtiene tráfico UDP excedente el cual ocasiona lentitud a la red y en otros casos el tráfico TCP lidera la red por lo que se concluye que existen horas y días en los cuales la red tiene un funcionamiento normal y en otros casos se tiene problemas de congestión los cuales se pueden corregir determinando cuales son los host que envían trafico UDP sin control. El trafico UDP además de ocasionar estos problemas saturan la red provocando lentitud al sistema.

Herramienta HTTP/load Distribution

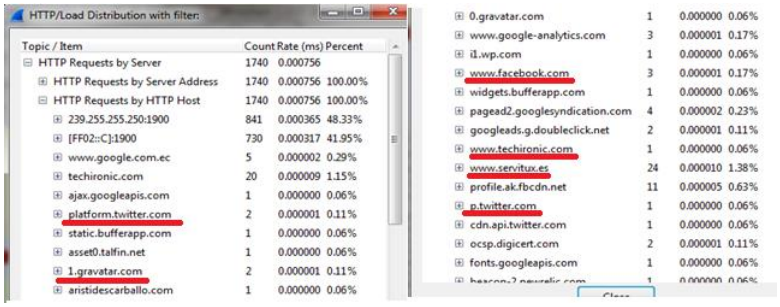


Figura 4.10: Uso de la Herramienta HTTP/Load Distribution.
Elaborado por: El investigador

La cual determina que páginas han sido visitadas por los usuarios de la red en donde se detectó acceso ilimitado a cualquier página ya sea redes sociales, servicios tecnológicos, y servicios de compras en Internet, e incluso acceso a páginas de adultos contraponiéndose al objetivo del servicio que es de carácter educativo comprobando la inexistencia de un servidor Proxy y Firewall que controle y limite el acceso a dichos sitios web.

Herramienta IO Graphs

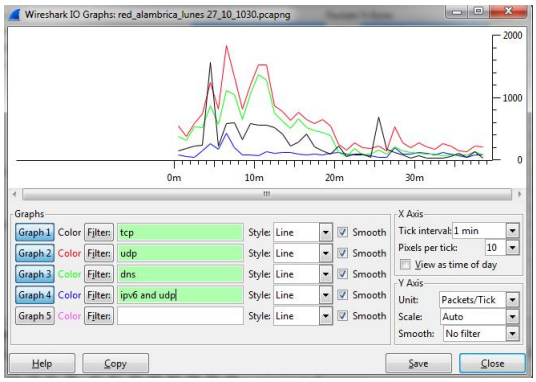


Figura 4.11: Uso de la Herramienta IO Graphs
Elaborado por: El investigador

Con esta se gráfica el tráfico generado en la captura de información filtrando los paquetes para determinar si el flujo existente en la red institucional es normal o existen anomalías como se observa el trafico UDP supera a la navegación cotidiana de la red ocasionando lentitud a la red una vez encontrado este problema se realiza un filtrado de paquetes para determinar los host que ocasionan este tráfico innecesario.

4.5.3.5. Red Inalámbrica

Red Inalámbrica					
Captura	Día 1	Día 2	Día 3	Día 4	Día 5
Problemas encontrados	8	22	4	23	10
Advertencias	3	6	2	13	7
Tráfico Superior	UDP	UDP	UDP	TCP	UDP
Porcentaje tráfico UDP	51,4	62,81	57,84	37,21	54,31
Porcentaje tráfico UDP	62,65	40,66	55,14	35,75	62,18
Porcentaje tráfico TCP	16,38	12,64	13,93	54,31	30,12
Porcentaje tráfico TCP	11,27	10,32	3,04	26,73	25,46

Tabla 4.5: Descripción del Análisis de la red Inalámbrica

Elaborado por: El investigador

En la cual se describe de manera ordenada los errores de la red, que tipo de tráfico prevalece y cuáles son sus porcentajes. En un resumen general el tráfico que lidera la red es UDP ocasionando congestión en la red.

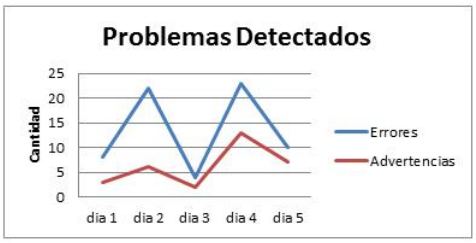


Figura 4.12: Análisis estadísticos de los problemas detectados
Elaborado por: El investigador

El número de errores encontrados es superior a las advertencia tales como datos perdidos, peticiones incompletas, entre otras.

Presentación de la herramienta Protocol Hierarchy Statistics

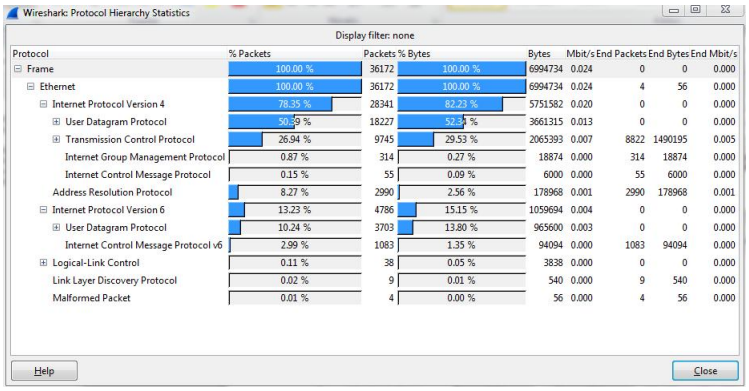


Figura 4.13: Presentación de la herramienta Protocol Hierarchy Statistics
Elaborado por: El investigador

Una vez analizado cada una de las capturas en los diferentes horarios se obtuvo los siguientes resultados.

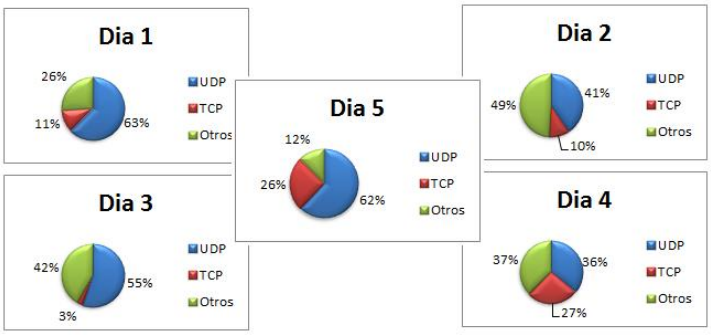


Figura 4.14: Presentación del Análisis de datos Red Inalámbrica
Elaborado por: El investigador

En la cual existe demasiado tráfico UDP lo que ocasiona errores y advertencias ya que UDP es un protocolo de envió sin respuesta y no se puede determinar si una paquete llego incompleto o no. Esto a nivel de datos tales como emails, y navegación web no representa mayor problema porque se entenderá el mensaje pero en aplicaciones tales como voz sobre IP, video conferencia es un gran problema. El trafico UDP además de ocasionar estos problemas saturan la red provocando lentitud al sistema.

Herramienta HTTP/load Distribution

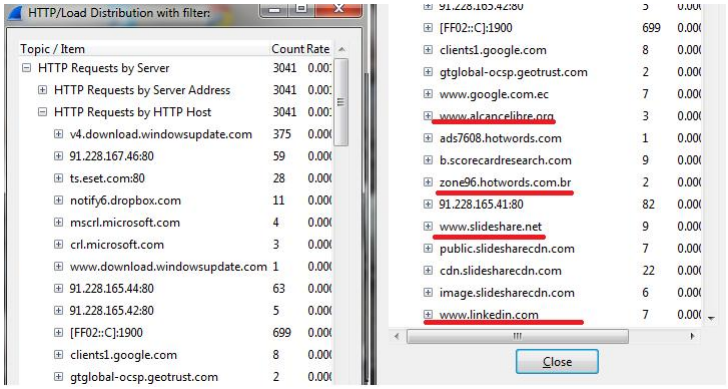


Figura 4.15: Uso de la Herramienta HTTP/Load Distribution
Elaborado por: El investigador

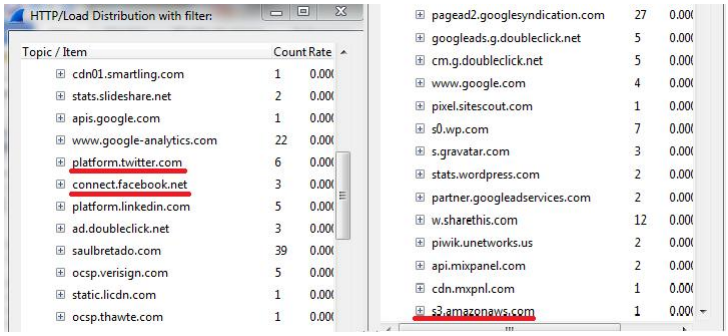


Figura 4.16: Herramienta HTTP/Load Distribution
Elaborado por: El investigador

Esta ayuda a determinar que páginas han sido visitadas por los usuarios de la red en donde se detectó acceso ilimitado a cualquier página ya sea redes sociales, servicios tecnológicos, y servicios de compras en Internet, e incluso acceso a páginas de adultos contraponiéndose al objetivo del servicio que es de carácter educativo comprobando la inexistencia de un servidor PROXY y Firewall que controle y limite el acceso a dichos sitios web.

Herramienta IO Graphs

Figura 4.17: Herramienta IO/Graphs en la red Inalámbrica
Elaborado por: El investigador

Con la cual se gráfica el tráfico generado en la captura de información filtrando los paquetes para determinar si el flujo existente en la red institucional es normal o existen anomalías como se observa el trafico UDP supera a la navegación cotidiana de la red ocasionando lentitud a la red una vez encontrado este problema se realiza un filtrado de paquetes para determinar los host que ocasionan este tráfico innecesario.

4.5.3.6. Análisis de tiempos de retardo en la conexión

Una vez analizado el tráfico de la red procedemos a realizar pruebas de conexión en host diferentes de la red en donde se ha tomado tiempos de conexión realizados en tiempo real y directamente de la fuente de información. Descripción de la prueba: En un host conectado a la red inalámbrica se procederá a conectarse a una página web y tomar el tiempo que se demora en mostrar el contenido, como prueba se tomó la siguiente página http://www.educacion.gob.ec/docentes la cual es una de las paginas más usadas por los profesores de la institución para fines académicos y de información en este caso con la IP 192.168.100.127 en un PC Lenovo con sistema operativo Windows 8 perteneciente a un docente de la institución.

Obteniendo los siguientes resultados:

Toma de información Nº1

	URL	Requests	Load time (seg)	Page Size (KB)
4	http://www.educacion.gob.ec/docentes/	55	47,79	407,1
5	http://www.educacion.gob.ec/docentes/	55	40,17	407,1
6	http://www.educacion.gob.ec/docentes/	55	313,2	407,1
7	http://www.educacion.gob.ec/docentes/	55	308,4	407,1
8	http://www.educacion.gob.ec/docentes/	55	319,2	407,1
9	http://www.educacion.gob.ec/docentes/	55	60	407,1
10	http://www.educacion.gob.ec/docentes/	55	54	407,1
11	http://www.educacion.gob.ec/docentes/	55	66	407,1
12	http://www.educacion.gob.ec/docentes/	55	436,8	407,1
13	http://www.educacion.gob.ec/docentes/	55	81,6	407,1

Figura 4.18: Captura del Proceso estadístico para el análisis de tiempos de respuesta
Elaborado por: El investigador

Datos tomados en cuenta:

- Request: Que son las peticiones enviadas o el número de elementos que contiene la página.
- Load Time: Es el tiempo de carga de la página web.
- Page size: Es el peso de la página en KB

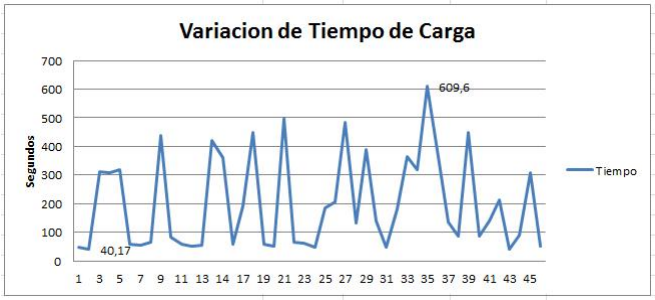


Figura 4.19: Presentación de la Variación del tiempo de Carga
Elaborado por: El investigador

En donde se observa que se tiene mucha variación en el tiempo de carga realizado en los cuales existen más picos altos que bajos de tiempo superando los 609,6 segundos como tiempo máximo de carga y 40,17 segundos tiempo mínimo de carga.

Toma de información Nº2

URL	Peso Pagina (KB)	Tiempo de Carga (Seg)	Sistema Operativo
www.español.yahoo.com	328	27	Windows 8 Pro
www.español.yahoo.com	328	60	Windows 8 Pro
www.español.yahoo.com	328	19	Windows 8 Pro
www.español.yahoo.com	328	18	Windows 8 Pro
www.español.yahoo.com	328	16	Windows 8 Pro
www.español.yahoo.com	328	12	Windows 8 Pro
www.español.yahoo.com	328	29	Windows 8 Pro
www.español.yahoo.com	328	18	Windows 8 Pro
www.español.yahoo.com	328	47	Windows 8 Pro
www.español.yahoo.com	328	17	Windows 8 Pro

Figura 4.20: Captura del Proceso estadístico para el análisis de tiempos de respuesta 2

Elaborado por: El investigador

Donde se tomó tres tipos de datos tales como: peso de la página, tiempo de carga y tipo de sistema operativo en el cual se realizó la prueba obteniendo los siguientes resultados.

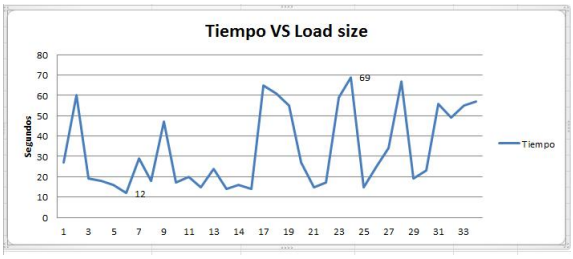


Figura 4.21: Presentación Tiempo VS Load size

Elaborado por: El investigador

En donde se tiene una variación en el tiempo de carga con picos superiores a los 60 segundos y pocos tiempos mínimos inferiores a 20 segundos donde se tiene excedente de tiempo de carga de la página usada reflejada en la información obtenida.

Toma de información Nº3

URL	page size (KB)	load size (min)	Request	S. Operativo
www.educacion.gob.ec	407	3,24	55	Windows 7
www.educacion.gob.ec	407	5	55	Windows 8
www.educacion.gob.ec	407	5,03	55	Windows 7
www.educacion.gob.ec	407	1,06	55	Ubuntu
www.educacion.gob.ec	407	2,46	55	Windows 7
www.educacion.gob.ec	407	5,14	55	Windows 8
www.educacion.gob.ec	407	2,34	55	Windows 8
www.educacion.gob.ec	407	1	55	Windows 8
www.educacion.gob.ec	407	2,58	55	Windows 8
www.educacion.gob.ec	407	7,22	55	Ubuntu

Figura 4.22: Captura del Proceso estadístico para el análisis de tiempos de respuesta 3

Elaborado por: El investigador

Considerando distintos sistemas operativos se obtiene los siguientes resultados:

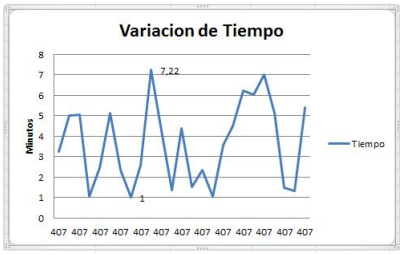


Figura 4.23: Presentación de la variación de tiempo de la captura 3
Elaborado por: El Investigador

En esta captura se observa como varía el tiempo de carga de una página que pesa 407 KB y obtenemos como resultado tiempos superiores a los 6 minutos y como mínimo un minuto que se traduce a demasiado tiempo de carga y lentitud de la red. Tomando en cuenta que en estos casos se logró cargar la página ya que en casos intermedios se excedió el tiempo de carga permitido por el navegador y sin obtener resultados.

4.5.3.7. Análisis de las tablas ARP

Otro de los problemas encontrados se localiza en la tabla ARP proporcionado por la MikroTik ya que se posee una lista de usuarios registrados en el sistema por el administrador y la tabla ARP nos proporciona información en tiempo real los dispositivos que se conectan a la red de la institución con su debida MAC Address.

IP Address	MAC Address	Interface
181.112.56.173	08:D0:9F:DB:79:40	ingre_inter-1
192.168.10.22	E8:40:F2:3E:17:37	laboratorios-3
192.168.10.25	B8:97:5A:3F:C8:B7	laboratorios-3
192.168.10.100	00:30:67:DB:96:BA	laboratorios-3
192.168.10.202	00:08:A1:A5:4F:FB	laboratorios-3
192.168.10.250	00:19:D1:B4:D5:DF	laboratorios-3
192.168.100.5	C4:17:FE:A2:D6:7E	bridge1
192.168.100.91	00:1E:64:77:5F:20	bridge1
192.168.100.101	00:24:2C:A0:88:75	bridge1
192.168.100.124	84:4B:F5:C2:87:5F	bridge1
192.168.100.127	00:21:5C:00:82:1F	bridge1
192.168.100.140	00:23:4D:A0:76:B4	bridge1
192.168.100.163	70:F3:95:6F:AC:C7	bridge1
192.168.100.169	24:EC:99:0F:3D:39	bridge1
192.168.100.172	94:39:E5:A0:41:5E	bridge1
192.168.100.178	88:9F:FA:42:40:9F	bridge1
192.168.100.190	AC:3C:0B:C1:88:BA	bridge1
192.168.100.193	74:E5:0B:09:1B:52	bridge1
192.168.100.197	00:27:22:02:F3:EB	bridge1
192.168.100.250	CC:08:E0:A1:7C:2F	bridge1
192.168.100.253	E0:63:E5:58:38:6D	bridge1

Figura 4.24: Tabla ARP en la MikroTik
Elaborado por: El Investigador

Donde se localizan IPs que no están registradas tales como la IP 192.168.100.5, IP 192.168.100.140, IP 192.168.100.190, IP 192.168.100.193, IP 192.168.100.197, IP 192.168.100.253 ya que estas IPs pertenecen a la red Inalámbrica de la Institución.

Este tipo de inconvenientes se traducen en tráfico ilegal de la red ya que no se tiene un control sobre las IPs utilizadas en la red. Otro de los inconvenientes se localiza cuando un usuario suplanta una dirección IP existente en la tabla ARP creando un conflicto o duplicados en el servicio de red saturando el sistema.

Al analizar las tablas ARP en horas pico se determino que existe un número aproximado de 60 usuarios recurrentes sobrecargando la capacidad de la MikroTik RB751U.

4.5.3.8. Análisis del Ancho de Banda existente

Considerando que le ancho de banda es la velocidad con que los datos son transferidos por una red, se debe realizar un cálculo del ancho de banda tomando en cuenta los siguientes factores:

- Ancho de Banda total necesario para la red.
- Ancho de banda asignado para cada usuario.
- Número de usuarios simultáneos

De donde se tiene la relación:

$$AB_{usuario} = \frac{AB_{disponible}}{Número\ de\ usuarios\ simultáneos}$$

Considerando que el número de usuarios recurrentes es 60 aproximadamente y además tomando el valor de 128 Kbps como un valor mínimo pero considerable para la navegación de los usuarios en la red, se determina que el ancho de banda mínimo necesario es:

$$AB_{necesario} = AB_{usuario} * \ Número\ de\ usuarios\ simultáneos$$

$$AB_{necesario} = 128\ Kbps * 60$$

$$AB_{necesario} = 7680\ Kbps \rightarrow 8192\ \text{Kbps}$$

Por lo que se comprueba que el ancho de banda utilizado no cubre las necesidades mínimas de la red institucional, lo cual se convierte en un inconveniente de rendimiento.

4.5.4. Resumen de problemas detectados en la red institucional

- Se tiene un acceso ilimitado a cualquier sitio web a través de la red institucional.
- Existen máquinas en la red que están generando excesivo tráfico UDP causando cuellos de botella y lentitud al sistema.
- Los tiempos de carga de páginas web exceden o se caducan en su gran mayoría debido a la limitación del ancho de banda por usuario configurado en la MikroTik.
- Existen dispositivos finales que no están registrados en la red institucional y tienen acceso a Internet.
- No existen reglas de Firewall establecidas para un correcto filtrado de tráfico en la red, incrementado las vulnerabilidades de la red.
- No existen políticas de control de acceso a la red institucional por lo que provoca congestión.
- No existe QoS ni seguridad en la red Institucional.
- No existe un ancho de banda suficiente para cubrir las necesidades de la red institucional.
- No existe un esquema de direccionamiento para la red inalámbrica y cableada.
- El armario de comunicaciones existente no cumple con normas de infraestructura básicas.

4.6. Determinar las herramientas de Hardware y Software para la aplicación de la propuesta

Una vez detectado los problemas generados en la red institucional, se procede a analizar los requerimientos necesarios para la ejecución de la propuesta, esto involucra el Hardware y software. La Unidad Educativa Baños cuenta con un servidor HP Proliant ML150 el cual no esta siendo utilizado y con un router MikroTik el cual imparte el servicio de Internet hacia laboratorios, administrativos y red Wifi a través de una topología en estrella extendida con switches de capa 2.

4.6.1. Establecer los Requerimientos de Hardware

Para corregir los problemas existentes en la red es necesario establecer los requerimientos tanto a nivel de Hardware como de Software. Entre los requerimientos de Hardware se incluye una rack para mejorar el armario de comunicaciones y cumplir con el estandar TIA/EIA 568-A de la infraestructura mínima de una red.

4.6.1.1. Armario de Comunicaciones (RACK 6U)

Es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. Las medidas de la anchura están normalizadas para que sea compatibles con equipamiento de cualquier fabricante. También son llamados bastidores, cabinas, cabinets o armarios. [15]

Tomando en cuenta el espacio y los equipos que se dispone se considera una Rack 6U con las siguientes características:

Figura 4.25: Armario de distribución Rack 6U
Fuente: Internet [15]

Información general

Soporte de pared gabinetes reducen los requisitos de espacio de piso y son la mejor opción para las oficinas lleno de gente y donde el tamaño no justifican una sala de telecomunicaciones dedicada

- Estructura de doble sección
- Puerta lateral Removible, fácil instalación y mantenimiento
- Entradas de cable opcionales de la placa superior e inferior
- Los ventiladores de refrigeración se pueden instalar para el requisito especial
- ESPESOR: Rieles de montaje 0.08 "(2.0 mm), otros 0.05" (1.2 mm)

Características del producto

- Estructura de la sección doble puerta lateral extraíble, fácil instalación y mantenimiento de entradas de cables opcionales de la placa superior e inferior.
- Los ventiladores se pueden instalar para ESPESOR requisito especial: Rieles de montaje 0.08 "(2.0mm), otros 0.05" (1.2 mm).
- Estructura de trama, la carga máxima de 132 libras (60 kg).
- Puerta lateral Quick abierto fácil de instalar y mantener.
- Camino superior e inferior del alambre.
- Pared y de pie tipo de instalación.
- Un ventilador de 4,7 "(120 mm) 110v motor axial.
- Montaje en la pared Conveniente y rápido.
- A 11 bandeja "(280mm)
- 4 Parantes
- Cumple con la norma ANSI / EIA RS-310-D, IEC297-2, DIN41491, PARTE 1, DIN41494; PART7, GB/T3047.2-92 estándar; whit Compatible 6U stantard Internacional y métrica estándar y estándar ETSI. [15]

4.6.1.2. Patch Panel AW190NXT06 CAT5e 24 Puertos

Se define como paneles donde se ubican los puertos de una red, normalmente localizados en un bastidor o rack de telecomunicaciones. Todas las líneas de entrada y salida de los equipos (routers, switches y servidores, etc.) tendrán su conexión a uno de estos paneles.

Figura 4.26: Pach Panel AW190NXT06 Cat5e
Fuente: Internet [15]

Descripción General

Este panel de interconexión de categoría 5E está diseñado para instalaciones de alta densidad. Supera los estándares ANSI/TIA/EIA-568 C.2, permite conexiones con conductores calibre 22 a 26 según la escala americana (AWG), e incluye contactos de bronce fosforoso. Todoslos paneles de conexión están hechos para su instalación directa en bastidores de 6U y existen configuraciones de 12, 24, y 48 puertos con puntos de anclaje integrados para mejorar la organización y la seguridad de los cables. La asignación de colores a los puertos permite la interconexión universal de los cables. Una terminación tipo 110 garantiza la conexión segura y fiable para maximizar el desempeño. Cuenta con certificación de seguridad UL (Underwriters Laboratories).

Especificaciones

- **Red:** Cantidad de puertos 24
- **Color del producto:** Negro

4.6.1.3. Patch Cord

Patch Cord o cable se usa en una red para conectar un dispositivo electrónico con otro. Se producen en muchos colores para facilitar su identificación. En cuanto a longitud, los cables de red pueden ser desde muy cortos para los componentes apilados, o tener hasta 100 metros como máximo y mientras mas largos son apantallados para evitar el ruido.

Figura 4.27: Patch Cord
Fuente: Internet [15]

Estándares de Cable par trensado

El estándar se refiere a las convenciones y protocolos que se acordó utilizar para el correcto funcionamiento entre redes de datos de área local, en el caso del cable

se utiliza en base a su categoría Se muestra en la siguiente tabla los estándares básicos de acuerdo a su mayor uso, recordando que la combinación de tales factores, generará diferentes precios en los productos e instalaciones.

Categoría	Ancho de Banda	Velocidad	Características
CAT 4	20 MHz	16 Mbps	Usos en redes Token Ring
CAT 5	100 MHz	100 Mbps	100 BASE-TX 1000 BASE-T
CAT 5e	100 MHz	100 Mbps	Ethernet 100BASE-TX y 1000 BASE-T, soporte Ethernet Gigabit
CAT 6	250 MHz	1000 Mbps	Ethernet Gigabit
CAT 6a	500 MHz	10000 Mbps	Ethernet 10 Gigabit

Tabla 4.6: Estandares de Cables par trensado

Fuente: Internet [15]

Se utiliza cable par trensado categoria 5e el cual existe en la institución organizando de mejor manera el armario de comunicaciones.

4.6.2. Análisis de distribuciones GNU/Linux para la aplicación sobre el servidor HP Proliant ML150

4.6.2.1. Descripción del Servidor HP Proliant ML150

Para analizar que Software se debe aplicar sobre el servidor es necesario especificar la capacidad que posee el servidor HP Proliant ML 150.

En la siguiente tabla se enumera las características y funciones del servidor.

Características Principales	Funciones adicionales
Procesador: Intel® Xeon®E5504 (2.0 GHz, 4 MB L3, 80W, DDR3-800), soporta hasta 2 procesadores. **Memoria Ram:** 10 GB PC3-10600 (Soporta hasta 48 GB con protección Advanced ECC). **Almacenamiento**: 2 discos de 150 GB (Soporta hasta 4TB discos SATA ó SAS) **Adaptador de red:** Embedded HP NC107i PCI Express Gigabit Server. **Dimensiones Físicas**: 20 x 42.4 x 61.68 cm (alto x ancho x fondo). **Protección de energía y ventilación**: 512327-B21 HP 750W Redundant Power Supply kit (por 2 unidades) + 508544-B21 HP RPS Enablement Kit (por 1 unidad). **Base para RACK:** 417705-B21 HP Tower to Rack Conversion Tray, Universal Kit.	• Soporta virtualización • Expansión de disco duro opciones para controladora y seguridad • Soporta sistemas de respaldo de datos RAID (0/1/0+1) • Soporta Microsoft Windows Server 2003, Microsoft Windows Server 2008, Hyper-V, RHEL, SLES, OEL, Solaris, VMware, y Citrix Essentials para XenServer y distribuciones GNU Lunix. • Administración remota avanzada • Protección de energía y ventilación • Base para rack 5u.

Tabla 4.7: Capacidad del Servidor HP Proliant ML 150

Elaborado por: El investigador

Entre las caracteríticas del Servidor físico se establece que admite virtualización por lo se sugiere separar los servicios de red como medida preventiva a posible fallos o ataques de Software malicióso, ademas que representa ventajas al mantenimiento de los servicios de red, ya que cada servicio operara de manera independiente aprovechando al máximo las capacidades de Servidor HP Proliant ML150. [16]

4.6.2.2. Análisis de distribuciones GNU/Linux para el servidor

Una vez determinado las capacidades del Hardware se procede a solventar las necesidades de Software considerando la utilización de Software de código abierto debido a que estos sistemas requieren mínimos recursos de Hardware por lo que se estudia tres tipos de distribuciones Linux que se detallan a continuación:

Características	CentOS	ClearOS	Zentyal
Especificaciones de Hardware	Memoria RAM: 64 MB mínimo en modo consola. Memoria RAM: 2GB mínimo en modo Gráfico. Espacio en Disco Duro: 1024 MB (mínimo) - 2 GB (recomendado). Procesador: Intel x86-compatible (32 bit) (Intel Pentium I/II/III/IV/ Celeron/Xeon, AMD K6/K7/K8, AMD Duron, Athlon/XP/MP). AMD64(Athlon 64, etc) e Intel EM64T (64 bit).	Procesadores/CPU Hasta 16 procesadores Memoria RAM 512 MB recomendado Disco Duro 2 GB recomendado CD-ROM Drive Requerido para instalación Tarjeta de Video Cualquier tipo de tarjeta de video Periféricos Monitor y Teclado Tarjeta de Red: 1 Tarjeta de Red ó 2 Tarjetas de Red en Modo Gateway	Los requerimientos de hardware para un servidor Zentyal dependen de los módulos que se instalen, de cuántos usuarios utilizan los servicios y de sus hábitos de uso. Algunos módulos tienen bajos requerimientos, como Cortafuegos, DHCP o DNS, pero otros como el Filtrado de correo o el Antivirus necesitan más memoria RAM y CPU.
Soporte de Software	7 Años de soporte oficial	18 meses de soporte oficial	Zentyal ofrece 4.5 años de soporte técnico oficial
Documentación (Existente desde)	2004	2010	2004
Estabilidad del Sistema	Alta	Media	Media
Servicios	SSH, TELNET, SMTP, DNS, DHCP, TFTP, HTTP, NETBIOS-NS, NETBIOS-SSN, IMAP, IMAP3, LDAP, HTTPS, SQUID, MYSQL, WEBCACHE, VPN.	Anti-virus, anti-spam, VPN, filtrado de contenidos, gestor de ancho de banda, servicios de archivos, los servicios SMTP, servicios de impresión, la certificación SSL, y servicios web.	NAT, PPPoE, DHCP, DNS, NTP, VLAN 802.1Q, RADIUS, Proxy HTTP, POP3, IMAP, Webmail, Antivirus, Jabber/XMMP
Valoración del Software en Seguridad.	10/10	8/10	9/10
Interfaz de Usuario	Modo Consola Modo Escritorio	Interfaz basada en web Basada en Red Hart Enterprise Linux	Interfaz Basada en web bajo Ubuntu server

Tabla 4.8: Análisis de Software de código abierto para la aplicación sobre el servidor HP Proliant ML150

Elaborado por: El investigador

Al analizar las distintas distribuciones GNU/Linux existentes se consideró tres tipos de software los cuales cumplen con los parámetros requeridos para el desarrollo de la investigación. Eligiendo CentOS como un sistema robusto, confiable y capaz de levantar todos los servicios requeridos en la investigación a la vez que se puede proyectar a más servicios adicionales que contribuyan al crecimiento productivo de la institución en la cual se aplicará las políticas para el control y distribución del tráfico de red. CentOS es una variación de Red Hart Enterprise Linux una versión de software comercial de carácter profesional, liberado para la utilización como software

de código abierto, proporcionando ventajas similares a las del software original y un soporte más duradero, además que se puede acoplar a ambientes con pocos recursos de Hardware. Posee mejor estabilidad, seguridad y escalabilidad.

4.6.3. Establecer y Analizar los requerimientos del Software

4.6.3.1. Requerimientos de Software

Para solventar las necesidades de la red LAN es necesario la investigación de los siguientes servicios:

- **Virtualización de servidores**.- El cuál permitirá separar los servicios de red optimizando el funcionamiento colectivo del sistema.
- **Servidor Firewall.**- El cual permite crear reglas de filtrado, bloqueos de puertos, direccionamiento de tráfico y más.
- **Servidor Proxy.-** Este ayudará a crear reglas de acceso a los servicios de Internet tales como bloqueos de dominios y descargas.
- **Servidor DNS cache .-** La aplicación de dns cache ayudará a mínimizar los tiempos de carga de páginas recurrentes.
- **Servidor DHCP.-** Este permitirá la configuración dinámica de los equipos finales disminuyendo los tiempos de configuración.
- **MikroTik RB751U.**- Permite impartir un servicio inalámbrico controlado aplicando conceptos de Firewall, DHCP, DNS y Hotspot.
- **Software de Monitoreo.-** Sirve para mantener un control permanente de los puntos de red .

4.6.4. Analizar la virtualización de los servicios de red con sistemas de respaldo

La virtualización divide los recursos de un equipo informático o Hardware para crear distintas máquinas virtuales que funcionan de manera independiente aunque no existan físicamente. Se trata de crear distintos entornos informáticos virtuales en un mismo Hardware o servidor.

4.6.4.1. Virtualización Completa

Se denominan aquellas soluciones que permiten ejecutar sistemas operativos huésped (Guest), sin tener que modificarlos, sobre un sistema anfitrión (Host), utilizando en medio un Hypervisor o Virtual Machine Monitor que permite compartir el Hardware real. Esta capa intermedia es la encargada de monitoriar los sistemas huésped con el fin de capturar determinadas instrucciones protegidas de acceso al Hardware, que no pueden realizar de forma nativa al no tener acceso directo.

Su principal ventaja es que los sistemas operativos pueden ejecutarse sin ninguna modificación sobre la plataforma, aunque como inconveniente frente a la emulación, el sistema operativo debe estar soportado en la arquitectura virtualizada.

Existen herramientas para poder hacer una virtualización completa XEN, KVM, Local Domains y VMWARE. Hay que tener en cuenta también que la virtualización completa no se refiere a todo el conjunto de Hardware disponible en un equipo, sino a sus componentes principales, básicamente el procesador y memoria. [17]

4.6.4.2. Kernel Based Virtual Machine (KVM)

La virtualización de los servicios de red proporciona un aislamiento, seguridad, flexibilidad, agilidad y portabilidad es decir que al virtualizar los servidores se garantiza el funcionamiento individual, generando un entorno seguro y flexible ya que permite descentralizar los servicios, es decir que si uno de los servidores deja de funcionar no afecta al resto de los equipos. Los archivos de configuración residen en uno a varios ficheros lo cual permite migrar los servicios hacia otros servidores disminuyendo el tiempo de recuperación del sistema. La creación de nuevos servidores virtuales se hace a través de un solo comando disminuyendo los tiempos de instalación y configuración.

Por lo que es necesario el estudio de la virtualización como premisa en el desarrollo de la investigación. En la virtualización existen múltiples tipos de herramientas, pero todos poseen algo en común, se trata de programas o herramientas que hacen creer a otros programas que son Hardware. [17]

La virtualización permite:

- Ahorra en reinicio en caso de que tengamos que cambiar habitualmente de S.O.
- Permite lanzar varios sistemas operativos diferentes en una misma computadora.
- Facilita la administración de los sistemas operativos virtualizados.

- Migración dinámica de aplicaciones.

La virtualización favorece en los siguientes puntos:

- Ahorro de costes de Hardware y alojamiento de equipos.
- Mantenimiento de cada servidor.
- Sistemas centralizados.
- Aprovechamiento de recursos.
- Sistemas de prueba.
- Simplicidad, Compatibilidad, Seguridad y ahorro en el consumo de energía.

Instalación de KVM

Antes de poder instalar es necesario ver los requisitos:

- Como mínimo un 1 GB de memoria.
- Disco duro con buena capacidad.
- Procesador con soporte virtualización.
- Particiones independientes para el sistema de forma clásica o LVM:

Se necesita los siguientes paquetes:

- kvm: El paquete KVM instala el modulo para el kernel en el cual permitirá tener máquina virtuales huésped.
- libvirt-bin: La librería libvirt-bin es la encargada de la virtualizar las máquinas huésped.
- virtinst: La herramienta virtinst permite la instalación, administración y configuración de las máquinas huésped.

Loguear como super usuario para realizar la instalación y configuración. su ==> clave root

Digitar el comando:

```
# yum -y groupinstall kvm libvirt-bin virtinst
```

Crear un usuario perteneciente al grupo libvirtd:

```
# adduser user libvirtd
```

el cual se encargara de la administración de las máquinas virtuales. [17]

Configuración de la Interface de red en modo Bridge

Este modo es configurado por defecto cuando se crea una máquina virtual. Es un término en redes que describe la extensión de una red sin utilizar otro router. Cuando se establece el modo bridge en una tarjeta de red virtual, la red local es extendida hacia tu máquina virtual. Aunque el equipo se conecte a la red local usando el Hardware del ordenador físico, la máquina virtual es totalmente independiente en la red como un equipo más.

También cabe destacar que en el modo bridge, si el equipo físico está configurado para recibir una IP por DHCP, la máquina virtual recibirá la IP del mismo servidor DHCP. [18]

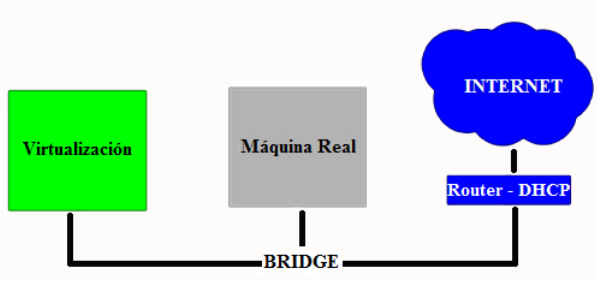


Figura 4.28: Modo Bridge
Fuente: Internet [18]

4.6.4.3. Sistema de respaldo RAID 1

Redundant Array of Inexpensive Disk. (En español: matriz redundante de discos independientes) Es utilizado para garantizar la integridad de los datos: en caso de fallo de un disco duro, es posible continuar las operaciones en el otro disco duro sin ningún problema. No se mejora el rendimiento y los otros discos duros son ocultos. Es necesario tener al menos dos discos duros. El RAID 1 hace una simple copia del primer disco (por lo que para 2 discos de igual tamaño, obtenemos un espacio de almacenamiento igual al espacio de un solo disco). [19]

Según el estándar ISO 17799 inciso 10.5 el respaldo de la información o backup tiene como objetivo mantener la integridad y disponibilidad de la información como una política de respaldo por lo que se considera la utilización de RAID 1 para garantizar un backup de los servicios de red. El servidor HP Proliant ML150 permite realizar Raid (0/1/0+1) por lo que es factible aplicar este concepto.

Al aplicar el concepto de RAID 1se crea un espejo de la información en dos discos duros lo que produce un gran aumento en la velocidad de lectura, pues permite leer múltiples sectores de datos de cada disco duro al mismo tiempo utilizando canales de

transferencia de datos distintos. Una de las principales ventajas es la seguridad de la información. Al romperse un disco duro la información sigue estando duplicada en otro disco duro de forma correcta lo que proporciona versatilidad en la recuperación del sistema.

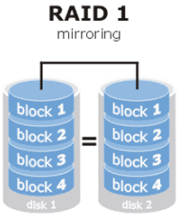


Figura 4.29: Demostración gráfica de RAID1
Fuente: Internet [19]

4.6.5. Análisis de los servicios necesarios para la gestión de redes LAN

En este punto se analiza las configuraciones de los servicios de red que se aplican en el desarrollo de la propuesta, tomando en cuenta el Hardware y Software disponible.

Los servicios necesarios y básicos en la gestión de redes son:

- Servidor Proxy
- Servidor Firewall
- Servidor DNS
- Servidor DHCP
- Hotspot en MikroTik

4.6.5.1. Servidor PROXY

Es un Servidor Intermediario que se define como una computadora o dispositivo que ofrece un servicio de red, consiste en permitir a los clientes realizar conexiones de red indirectas hacia otros servicios de red. Durante el proceso ocurre lo siguiente:

- Cliente se conecta hacia un Servidor Proxy.
- Cliente solicita una conexión, archivo u otro recurso disponible en un servidor distinto.
- Servidor Intermediario proporciona el recurso ya sea conectándose hacia el servidor especificado o sirviendo éste desde un caché.

- En algunos casos el Servidor Intermediario puede alterar la solicitud del cliente o bien la respuesta del servidor para diversos propósitos.

Los Servidores Proxy generalmente trabajan simultáneamente como muro cortafuegos operando en el Nivel de Red, actuando como filtro de paquetes, como en el caso de iptables o bien operando en el Nivel de Aplicación, controlando diversos servicios. [20]

Tipos de Servidores Proxy

Los diferentes tipos de Proxy son:

- Servicio Proxy o Proxy Web
- Proxy Caché.
- Praxis transparentes.
- Reverse Proxy / Proxy inverso.
- Proxy NAT (Network Address Translation) / Enmascaramiento.
- Proxy abierto.
- Cross-Domain Proxy.

Proxy transparente

Son transparentes en los términos que su dirección IP está expuesto, sino mas bien en los términos que no se sabe que se lo está utilizando. Combina un servidor Proxy con NAT (Network Address Translation) de manera que las conexiones son enrutadas dentro del Proxy sin configuración por parte del usuario. Este es el tipo de Proxy que utilizan los proveedores de servicios de Internet (ISP). [20]

SQUID

Es un Servidor Intermediario de alto desempeño que se ha desarrollado desde hace varios años, es ampliamente utilizado entre los sistemas operativos como GNU/Linux y derivados de Unix. Es muy confiable, robusto y versátil y se distribuye bajo los términos de la Licencia Pública General GNU (GNU/GPL). Siendo equipamiento lógico libre, está disponible el código fuente para quien así lo requiera.

Squid consiste de un programa principal como servidor, un programa para búsqueda en servidores DNS, programas opcionales para reescribir solicitudes,

realizar autenticación, algunas herramientas para administración y herramientas para clientes. Al iniciar Squid da origen a un número configurable de procesos de búsqueda en servidores DNS, cada uno de los cuales realiza una búsqueda única en servidores DNS. [20]

Configuración de Squid

Squid utiliza el archivo de configuración localizado en /etc/squid/squid.conf y se podrá trabajar sobre este utilizando su editor de texto. Existen un gran número de opciones, de los cuales se configura las siguientes:

- Listas de Control de Acceso
- Reglas de Control de Acceso
- http_port
- cache_dir

Estas son las principales opciones necesarias para la aplicación de la propuesta, antes de realizar algún cambio es recomendable realizar copias de seguridad del archivo de configuración sin cambios.

Listas de Controles de acceso

Para poder controlar el tráfico de los clientes hacia Internet, es necesario establecer Listas de Control de Acceso que definan una red o bien ciertos anfitriones en particular. A cada lista se le asignará una Regla de Control de Acceso que permitirá o denegará el acceso a Squid.

De modo predeterminado en CentOS 6, Squid habilita el acceso a todas las redes locales, definidas en el RFC1918. Es decir, permite el acceso a 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16, fc00::/7 y fe80::/10. Por lo que es necesario eliminar esta configuración y establecer solo los parámetros específicos. [20]

Sintaxis

Regularmente una lista de control de acceso se establece con la siguiente sintaxis:
acl [Nombre de la lista] src [lo que compone a la lista]
Ejemplo:

```
acl localnet src 192.168.10.0/24
```

También puede definirse una Lista de Control de Acceso especificando un archivo localizado en cualquier parte del disco duro y la cual contiene una lista de direcciones IP.

Ejemplo:

```
acl nombre_archivo src "/etc/squid/listas/nombre_archivo"
```

El archivo /etc/squid/listas/nombre_archivo tendrá un contenido similar al siguiente:

```
192.168.10.1
192.168.10.2
192.168.10.3
192.168.10.4…
```

Figura 4.30: Listas de redes Locales para Squid por archivo
Elaborado por: El investigador

Lo anterior define que la lista de control de acceso denominada nombre_archivo estará compuesta de las direcciones IP incluidas en el archivo /etc/squid/listas/nombre_archivo.

Reglas de Control de Acceso.

Estas definen si se permite o deniega acceso hacia Squid. Se aplican a las Listas de Control de Acceso. Deben colocarse en la sección de reglas de control de acceso definidas por el administrador.

Sintaxis

La sintaxis básica de una regla de control de acceso es la siguiente:

```
http_access [deny o allow] [lista de control de acceso]
```

Ejemplos:

En la siguiente línea se considera una regla que establece acceso permitido a Squid a la Lista de Control de Acceso denominada localnet:

```
http_access allow localnet
```

También pueden definirse reglas valiéndose de la expresión !, la cual significa no.

```
http_access allow localnet ¡deniedsites
```

Lo que significa que existe acceso a squid por parte de localnet y deniega el acceso a la deniedsites. Este tipo de reglas son útiles cuando se tiene un gran grupo de IP dentro de un rango de red al que se debe permitir acceso y otro grupo dentro de la misma red al que se debe denegar el acceso. [20]

Opción http_port

Esta opción es utilizada para indicar el puerto a través del cual escuchará peticiones Squid. EL valor predeterminado es 3128, es decir, Squid escuchará peticiones a través del puerto 3128/tcp.

```
http_port 3128
```

Para configurar el servidor Proxy en modo transparente, sólo es necesario añadir la opción transparent.

Ejemplo:

```
http_port 192.168.1.1:3128 transparent
```

Opción cache_dir

Esta opción se utiliza para establecer el tamaño que utiliza Squid para almacenamiento de caché en el disco duro. De modo predeterminado Squid utiliza el formato ufs para crear en el directorio /var/spool/squid un caché de 100 MB, dividido en jerarquías de 16 directorios subordinados, hasta 256 niveles cada uno:

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

Aquí se puede incrementar el tamaño del caché, mientras más grande sea el caché, más objetos se almacenarán en éste y por lo tanto se consumirá menos el ancho de banda. La siguiente línea establece un caché de 2 GB.

```
cache_dir ufs /var/spool/squid 2048 16 256
```

El formato de cache ufs puede llegar a bloquear el proceso principal de Squid en operaciones de entrada/salida sobre el sistema de archivos cuando hay muchos clientes conectados. Para evitar que esto ocurra, se utilizar aufs, que utiliza el mismo formato de ufs, pero funciona de manera asincrónica, consiguiéndose un mejor desempeño. [20]

```
cache_dir aufs /var/spool/squid 2048 16 256
```

Opción maximum_object_size

Esta opción se utiliza para definir el tamaño máximo de los objetos en el caché. Es aconsejable establecerla en escenarios con alta carga de trabajo, puesto que permite evitar desperdiciar recursos de sistema almacenando en el caché objetos de gran tamaño que probablemente sólo sean aprovechados por unos pocos usuarios, optimizando el uso del caché con objetos pequeños que de otro modo generarían una gran cantidad de peticiones hacia las redes públicas o Internet. [20]

Ejemplo:

De la siguiente manera se establece un límite de 48 MB para los objetos del caché.

```
máximum_object_size 64 MB
```

Opciones cache_swap_low y cache_swap_high

Es posible realizar una limpieza automática del caché de Squid cuando éste llegue a cierta capacidad. La opción cache_swap_low establece el porcentaje a partir del cual se empezara a limpiar el cache.

Ejemplo:

A continuación se establece que el cache se empezará a limpiar cuando se llegue al 90 % de su capacidad.

```
cache_swap_low 90
```

La opción cache_swap_high establece el porcentaje a partir del cual se comenzará a limpiar de manera agresiva el cache. [20]

Ejemplo:

Aquí se establece que el cache se empezará a limpiar de manera agresiva cuando se llegue al 95 % de su capacidad.

```
cache_swap_high 95
```

4.6.5.2. Servidor FIREWALL

Un Firewall es un sistema ubicado entre dos redes y que ejerce la una política de seguridad establecida. Es el mecanismo encargado de proteger una red confiable de una que no lo es como el Internet.

Puede consistir en distintos dispositivos, que deben cumplir los siguientes objetivos:

- Todo el tráfico desde dentro hacia fuera, y viceversa, debe pasar a través de él.

- Sólo el tráfico autorizado, definido por la política local de seguridad, es permitido.

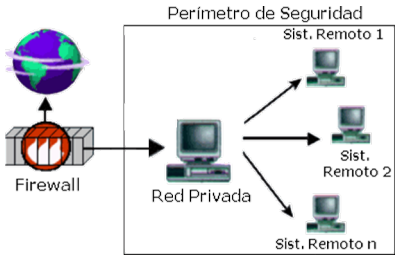


Figura 4.31: Perímetro de Seguridad del Firewall
Fuente: Internet [21]

Como puede observarse, el Firewall, sólo sirven de defensa perimetral de las redes, no defienden de ataques o errores provenientes del interior, como tampoco puede ofrecer protección una vez que el intruso lo traspasa.

Algunos Firewalls aprovechan esta capacidad de que toda la información entrante y saliente debe pasar a través de ellos para proveer servicios de seguridad adicionales como la encriptación del tráfico de la red. [21]

Tipos de Firewall

Existen tres tipos de firewalls:

- Firewalls de Software
- Enrutadores de Hardware
- Firewalls de Hardware

Firewall de Software

Se caracterizan por ser de bajo costo y son una buena elección cuando sólo se utiliza una PC. La instalación y actualización es sencilla, pues se trata de una aplicación de seguridad, como lo sería un antivirus; de hecho, muchos antivirus poseen firewalls en sus sistemas.

Este tipo de Firewalls se basa en el principio de que cada paquete que circula por la red es inspeccionado, así como también su procedencia y destino. Se aplican desde la capa de Red hasta la de Aplicaciones. [21]

NETFILTER

Es un Firewall de software basado en host para los sistemas operativos Linux. Está incluido como parte de la distribución de Linux y se activa por defecto. Este Firewall es controlado por el programa llamado iptables. El filtrado Netfilter tiene lugar a nivel del núcleo, antes de que un programa pueda incluso procesar los datos de los paquetes de red. [22]

Aplicación

Normalmente estos son utilizados con los servidores Proxy. En este caso no es posible el pasaje de datos de manera directa entre redes, ya que hay un monitoreo de los datos. Estos sistemas son utilizados para poder traducir ciertas direcciones de la red, pero siempre escondiendo el lugar donde se origina el tráfico.

El Firewall tiene la capacidad de cumplir las siguientes funciones:

- Protección de información privada: Define que usuarios de la red y que información va a obtener cada uno de ellos.
- Optimización de acceso: Define de manera directa los protocolos a utilizarse.
- Protección de intrusos: Protege de intrusos externos restringiendo los accesos a la red. [22]

4.6.5.3. Servidor DNS

Es el encargado de traducir el nombres de dominio en la direcciones IP de un servidor y viceversa. En primera instancia la resolución de cada nombre de dominio es delegado al servidor DNS del ISP del usuario.

Cuando se registra un dominio en nic.ec, la resolución de cada nombre de dominio es delegada al servidor DNS del ISP designado como administrador por la entidad registrante.

Los servidores DNS distribuidos en la red resuelven los pedidos de información, convirtiendo los nombres en una dirección IP. Si un servidor DNS no contiene la información, genera una consulta a otro servidor DNS y así sucesivamente hasta encontrar la dirección IP, o bien llega hasta un servidor DNS Raíz que le indica la dirección IP del servidor DNS que resuelve el pedido. [23]

Existen tres elementos indispensables que son: **Servidor web, Dominio y Servidor DNS** y su funcionamiento es:

1. Se realiza una petición hacia un dominio publico o privado en el navegador.

2. Se consulta en Internet la configuración del dominio.

3. El Servidor DNS direcciona la información hacia el servidor web.

Todo esto pasa en cuestión de milésimas de segundo. [23]

Ejemplo:

En la imagen se demuestra el funcionamineto del servidor DNS.

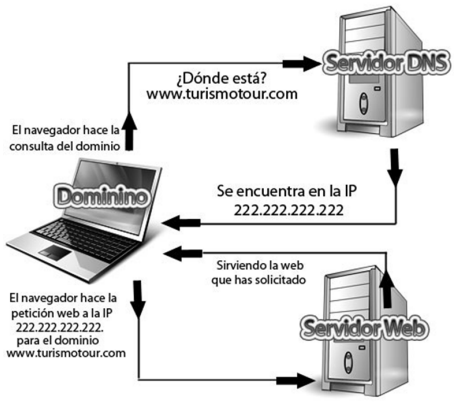


Figura 4.32: Funcionamiento del DNS
Fuente: Internet [23]

Tipos de Servidores DNS:

- **Servidor Primario/Principal/Maestro.** Mantiene de forma oficial la información de la zona sobre la que tiene autoridad. Responde a las peticiones de resolución consultando sus propios archivos de zona.
- **Servidor Secundario/Esclavo.** Obtiene la información de la zona pidiendosela constantemente al servidor primario.
- **Servidor Cache.** Se utilizan para acelerar las consultas de resolución de nombres de dominio frecuentemente utilizados. Suelen emplearse en redes de área local.

DNS cache

Un servidor DNS CACHE sirve para "cachar" las peticiones que los clientes de una red hacen a un servidor de nombres de dominio (DNS SERVER) que en la mayoría de los casos esta fuera de la propia LAN y que proporciona el proveedor de Internet (ISP - Internet Service Provider). Es decir, una red de por ejemplo 30 equipos conectados a Internet a través de un servidor Linux por un lado y por la otra parte, una tarjeta de red esta conectado a un modem ADSL. Quien resuelve los nombres de dominio a su

correspondiente IP, sería el DNS del proveedor, pero se implementa un DNS Caché, entonces el equipo Linux sería el que estaría resolviendo las direcciones. La primera vez utiliza el DNS de proveedor o cuando necesita renovarse una dirección IP de un dominio, pero posteriormente el Caché server conserva esa IP y el siguiente usuario que solicite la página, el mismo servidor local Linux lo resolverá, sin necesidad de hacer conectarse al proveedor, reduciendo enormemente los tiempos de consulta. Ese el funcionamiento de un DNS Caché. Y es bastante fácil implementarlo en Linux. [24]

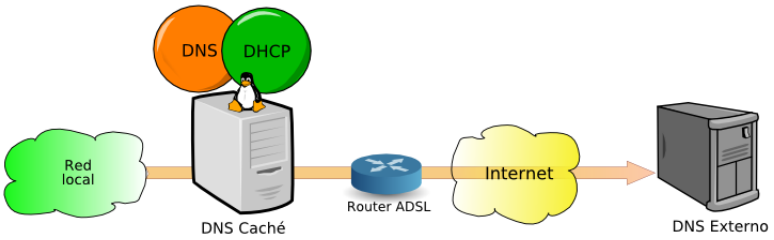


Figura 4.33: Esquema del DNS Caché
Fuente: Internet [24]

DNSMASQ

El paquete dnsmasq permite poner en marcha un servidor DNS y un servidor DHCP de una forma muy sencilla. Simplemente instalando y arrancando el servicio dnsmasq, sin realizar ningún tipo de configuración adicional, nuestro PC se convertirá en un servidor caché DNS y además, resolverá los nombres que tengamos configurados en el archivo /etc/hosts de nuestro servidor. La resolución funcionará tanto en sentido directo como en sentido inverso, es decir, resolverá la IP dado un nombre de PC y el nombre del PC dada la IP.

Adicionalmente, dnsmasq dispone de servidor DHCP y permite resolver los nombres de los PCs a los que les ha asignado dirección IP dinámica. Es posible configurar el servidor DHCP añadiendo simplemente una única línea al archivo de configuración, para indicar el rango de sesión. [24]

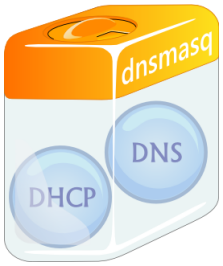


Figura 4.34: Esquema del DNSMASQ
Fuente: Internet [24]

4.6.5.4. SERVIDOR DHCP

Es aquel que recibe peticiones de clientes solicitando una configuración de red IP. El servidor responde a dichas peticiones entregando los parámetros que permitan a los clientes autoconfigurarse. Para que un host pueda acceder al servidor DHCP, en la configuración de red es necesario seleccionar la opción 'Obtener dirección IP automáticamente'.

DHCP (DYNAMIC HOST CONFIGURATION PROTOCOL)

Es el protocolo de configuración dinámica de host es un estándar TCP/IP diseñado para simplificar la administración de la configuración IP de los equipos de red.

Si se dispone de un servidor DHCP, la configuración IP de los PCs puede hacerse de forma automática, evitando así la necesidad de tener que realizar manualmente uno por uno la configuración TCP/IP de cada equipo. [25]

El servidor proporcionará al cliente al menos los siguientes parámetros:

- Dirección IP
- Máscara de subred

Opcionalmente, el servidor DHCP podrá proporcionar otros parámetros de configuración tales como:

- Puerta de enlace
- Servidores DNS
- Muchos otros parámetros más

El servidor DHCP proporciona una configuración de red TCP/IP segura y evita conflictos de direcciones repetidas. Utiliza un modelo cliente-servidor en el que el servidor DHCP mantiene una administración centralizada de las direcciones IP

utilizadas en la red. Los clientes podrán solicitar al servidor una dirección IP y así poder integrarse en la red.

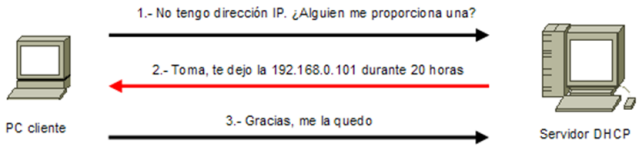


Figura 4.35: Funcionamiento del DHCP
Fuente: Internet [25]

Parámetros Necesarios

El servidor solo asigna direcciones dentro de un rango prefijado en la configuración del servicio por lo que se debe especificar los siguientes parámetros:

- Dirección IP del segmento de red
- Dirección IP de difusión
- Máscara de sub-red
- Puerta de enlace
- Servidor de nombres DNS
- Rango de direcciones IP a asignar de modo dinámico

Cuando se arrancamos de nuevo un PC cuya configuración IP se determina por DHCP, pueden darse dos situaciones:

- Si la concesión de alquiler de licencia ha caducado, el cliente solicitará una nueva licencia al servidor DHCP (la asignación del servidor podría o no, coincidir con la anterior).
- Si la concesión de alquiler no ha caducado en el momento del inicio, el cliente intentará renovar su concesión en el servidor DHCP, es decir, que le sea asignada la misma dirección IP. [26]

4.6.5.5. HOTSPOT en MikroTik RB751U

HOTSPOT

Un hotspot (en inglés un punto caliente) es un punto geográfico de acceso inalámbrico de carácter público mediante el cual los usuarios pueden conectarse a Internet.

Los Hotspot son los lugares que ofrecen acceso Wifi, que pueden ser aprovechados especialmente por dispositivos portátiles como notebooks, PDAs, consolas, etc. Estos generalmente son un servicio que brindan los restaurantes, hoteles, aeropuertos, shoppings, supermercados, universidades y otros lugares públicos.

Los hotspot Wifii fueron propuestos por Brett Stewart en la conferencia NetWorld/InterOp en San Francisco en agosto de 1993. Si bien Stewart no empleó el término "hotspot", sí se refirió al acceso público a redes LAN inalámbricas.

El término "Hotspot" posiblemente haya sido propuesto por Nokia unos cinco años después de que Stewart proponga el concepto. En la actualidad, los hotspot libres crecen exponencialmente, incluso extendiéndose a áreas metropolitanas de todo el mundo. Un hotspot puede crearse empleando un router Wifi. [27]

Tipos de Hotspot

Se pueden diferenciar dos tipos que son:

- Hotspot Público
- Hotspot Privado

HOTSPOT PRIVADO

Se pueden situar en un lugar de trabajo, o tener un grupo privado de usuarios que deciden crear y compartir un hotspot, es decir que su característica principal es no estar disponible al publico en general sino a un grupo específico de usuarios.

Para poder instalar un hotspot se necesita:

- Un punto de acceso inalámbrico abierto.
- Un servidor DHCP para asignar las diferentes IP de los clientes de forma automática.
- Un servidor de página web (apache) con un portal cautivo en el que los clientes deben autentificarse en el sistema para acceder a Internet.
- Una página de autenticación de usuarios.
- Un servidor de base de datos para poder administrar los datos del portal (usuarios y conexiones).

Y finalmente, para que los usuarios que se autentifican en el sistema pueden navegar por Internet es necesario un servidor radius permite autentificar a los equipos de una red a través de la dirección MAC del equipo. [27]

Configurar MikroTik como Hotspot

Un Portal Cautivo es un sistema que permite capturar el tráfico http (web) de nuestros clientes y re direccionarlo a un Portal para fines de autenticación. Una vez el cliente es autenticado, este puede acceder a todos los servicios de Internet con "normalidad".

La configuración estándar de MikroTik Hotspot es muy fácil de configurar, pero hay que hacer ciertas modificaciones para evitar tener problemas en la red si es que se utiliza AP's o Routers modo cliente. Se toma en cuenta que un hotspot está pensado para ser utilizado en lugares relativamente "pequeños", y que además los clientes NO se conectarán a través de AP's o Routers modo cliente. Un punto donde todas las personas que se conecten ahí, lo harán directamente con laptops, iPod, PDA, smartphones, etc.

Muchos usan MikroTik Hotspot en redes wireless extensas como único sistema de seguridad, dejando la señal abierta (sin encriptación), teniendo la creencia que este sistema es inviolable, lo que es bastante falso. Sin contar que estamos dejando la puerta abierta para que cualquier persona malintencionada haga un gran alboroto en la red. [27]

MIKROTIK RB751U

Es el RB más completo del mercado para las redes de bajo nivel de tráfico debido a las velocidad del CPU, se lo puede utilizar para balanceo de carga de hasta 5 WANs y distribuirlo de manera inalámbrica, además se lo puede utilizar como Firewall para la protección de redes internas. [28]

Descripción

- Cuenta con 5 interfaces de red 10/100 y un procesador de 400Mhz, y según las pruebas realizadas por MikroTik logra un throughput de hasta 450 Mbps en total.

- Cuenta con un puerto USB, el cual se puede usar para conectar un módem GSM y tener avisos/alertas por GSM. También se lo puede usar como un dispositivo de almacenamiento externo y hacer caché ahí mismo.

- Es un RouterBOARD de bajo costo, por la incorporación de una placa inalámbrica, que cuenta con una tarjeta en 2.4GHz que soporta los estándares 802.11 b/g/n con 1 W de potencia máxima y una antena incorporada de 2.5 dBi

y un conector externo MMCX para agregarle una antena de mayor potencia. [28]

Aplicaciones de seguridad de MikroTik RouterOS

Figura 4.36: MikroTik RB751U
Fuente: Internet [28]

- **Seguridad Wireless.** La seguridad siempre ha de ser una prioridad en Internet, MikroTik RouterOS ofrece las máximas posibilidades en este campo.
- **Firewall NAT.** Evidentemente MikroTik ofrece aplicaciones de última tecnología para impedir que alguien pueda entrar en la red.
- **Control de prioridad P2P.** Para evitar tener problemas en tu red esta aplicación permitirá controlar el tráfico P2P. [28]

4.6.5.6. Análisis del Software de monitoreo

Para determinar el mejor método de monitoreo de redes de datos se debe establecer un proceso para el análisis de distintas soluciones y escoger la que mejor se adapte a esta investigación.

Este proceso contempla tres etapas principales que son:

1. Identificación de los requerimientos de la red.
2. Investigar qué tipo de software cumple con los requerimientos.
3. Seleccionar un sistema apropiado de un conjunto de soluciones.

Etapa 1 Requerimientos de la red

Aquí se establece los requerimientos que debe cumplir el software que debe aplicarse, estos se definen en base a las necesidades de la red LAN de la institución.

- Debe ser un sistema F/oss

- Debe funcionar sobre la plataforma CentOS 6.5 de Linux.
- Debe ser fácil la instalación de todos los paquetes y dependencias.
- El software debe monitorear constantemente los dispositivos de red; servidors, routers y switches.
- Debe generar informes y estadísticas del estado de la red.
- Debe generar alertas cuando se presentes problemas.
- Enviar mensajes de error o advertencia al administrador de la red.
- Permite configurar umbrales de referencia al comportamiento normal de la red.
- Admite el monitoreo a través del protocolo de administración de redes SNMP

Etapa 2 Lista de sistemas F/oss

En esta etapa se realiza la búsqueda de los diferentes sistemas disponibles.

NAGIOS

Figura 4.37: Nagios
Fuente: http://www.k4ch0.org/tag/nagios/

Es el sistema de monitorización de red de código abierto mas popular disponible en la nube. Fue creado originalmente para ejecutarse en Linux, pero existen otras variantes de Unix que soportan este software. Nagios proporciona supervisión de los servicios de red (SMTP, POP3, HTTP, NNTP, ICMP, SNMP, FTP, SSH) y recursos de host (carga del procesador, uso de disco, los registros del sistema), entre otros. El control remoto se maneja a través de túneles SSH o SSL cifrado. Nagios posee un diseño simple pero eficaz que ofrece a los usuarios la libertad para desarrollar varios chequeos de servicio sin esfuerzo propio basado en las necesidades y mediante el uso de cualquiera de las herramientas de apoyo que existen. Para detectar y diferenciar entre hosts que están en subniveles y los que son inalcanzables, Nagios permite definir una jerarquía de la red con los hosts "padre". Cuando los servicios o los problemas de acogida se plantean, la notificación será enviada a la persona que está a cargo de la red a través del correo electrónico, SMS. [29]

ZABBIX

Figura 4.38: Zabbix
Fuente: http://www.zabbix.com/logo_download.php

Es un mecanismo de vigilancia tipo empresarial que está completamente equipado y posee soporte comercial. Es capaz de monitorear y dar seguimiento de la situación de los servicios de red, servidores y otro Hardware de red. Zabbix tiene una interface amigable con grandes funcionalidades de visualización incluidas las vistas definidas por el usuario, zoom, y la cartografía. Posee un método de comunicación versátil que permite una configuración rápida y sencilla de los diferentes tipos de notificaciones de eventos predefinidos. Zabbix cuenta con tres módulos principales: el servidor, los agentes, y el usuario. Como base de datos de seguimiento, puede utilizar MySQL, PostgreSQL, Oracle o SQLite. No es necesario instalar ningún software en los host monitoreados, Zabbix admite una comprobación de disponibilidad y capacidad de respuesta al servicio SNMP o HTTP. Para supervisar las estadísticas de la red a través de un host, es necesario instalar un agentes Zabbix para visualizar la carga de la CPU, utilización de la red y espacio en disco, etc. Zabbix incluye soporte para el monitoreo a través de SNMP, TCP y controles ICMP, IPMI y parámetros personalizados como una opción para instalar un agente en los hosts. [29]

CACTI

Figura 4.39: Cacti
Fuente: http://www.cacti.net/

Este software es una herramienta web de gráficas que está diseñada como una interfaz completa para el almacenamiento de datos en RRDtool y la utilidad gráfica que permite a los usuarios monitorear y graficar la carga de la CPU, la utilización de ancho de banda de red, el tráfico de red, y mucho más. Puede ser utilizado para configurar la recopilación de datos en sí, lo que permite configuraciones particulares, a controlar sin ningún tipo de configuración manual de RRDtool. Cacti permite monitorear los servicios en un período preestablecido y el gráfico de los datos

resultantes. Es utilizada principalmente para representar los datos a través de gráficas, de la carga del CPU y la utilización de ancho de banda de red. Cacti puede controlar cualquier fuente a través del uso de scripts de shell y ejecutables. Es completamente compatible con arquitectura de plugins, tiene una amplia comunidad que se ha reunido en torno a los foros de Cacti para proporcionar scripts, plantillas y consejos sobre creación de plugins. [29]

ZENOSS

Figura 4.40: Zenoss
Fuente: http://siliconangle.com/

Es un software basado en el servidor de aplicaciones Zope y escrito en Python, Zenoss (Zenoss Core) es un servidor que combina una programación original y varios proyectos de codigo abierto para integrar un sistema operativo y una plataforma de gestión de red que permite el almacenamiento de datos a través de la interfaz Web. Zenoss permite a los usuarios supervisar la disponibilidad, inventario y configuración, desempeño y los acontecimientos. Zenoss Core es capaz de supervisar a través de SNMP, SSH, WMI, servicios de red tales como (HTTP, POP3, NNTP, SNMP, FTP) y los recursos del host en la mayoría de sistemas operativos de red. Una arquitectura plug-in creada por ZenPacks permite a los miembros de la comunidad para ampliar su funcionalidad. ZenPacks están encapsulados en Python y la instrumentación de suministros y los informes. [29]

MUNIN

Figura 4.41: Munin
Fuente: http://munin-monitoring.org/

Munin utiliza RRDtool como base para representar los resultados gráficamente a través de una interfaz web. Este posee una arquitectura de maestro/nodo en la cual el maestro enlaza a todos los nodos a intervalos regulares. Al usar Munin, se puede supervisar el rendimiento de los equipos, redes y aplicaciones de una manera rápida

y fácil. Esto hace que la detección de problemas se más fácil, el rendimiento mejora y permite visualizar claramente el uso de los recursos de todos los puntos de red. Para el plugin Munin, la prioridad principal es la arquitectura plug and play. Posee una variedad de plugins de control disponibles que facilitarán su utilización. [29]

Etapa 3 Selección del Software

Para la selección del software se realiza una tabla de valoración en la cual se plantea los siguientes parámetros:

Indicadores	Valor
Preconfigurado	1
Requiere Plugins	0.5
No, permite	0

Tabla 4.9: Valoración del software

Elaborado por: Carlos Sánchez

En base a este cuadro se califica al software dependiendo de si cumple o no con los requerimientos establecidos:

Requerimientos	Nagios	Zabbix	Cacti	Zenoss	Munin
Sistema F/oss	1	1	1	1	1
Plataforma CentOS 6.5	1	0.5	1	0.5	0.5
Facilidad de Instalación	0.5	0.5	1	0.5	0.5
Monitoreo constante	1	1	1	1	1
Generan informes y estadísticas	1	1	1	1	1
Poseen alertas a problemas de red	1	0.5	1	0.5	1
Envía mensajes de errores o adventencias	1	0.5	1	0.5	0.5
Permite configurar umbrales de referencia	1	1	1	1	1
Monitoreo de servidores y routers	1	1	1	1	1
Admite el protocolo SNMP	1	1	1	1	1
Total	9.5	8.0	10	8.0	8.5

Tabla 4.10: Calificación del Software de monitoreo

Elaborado por: Carlos Sánchez

Aquí se realiza un cuadro comparativo de los distintos software encontrados para seleccionar el que mejor se acopla a las necesidades del sistema.

Software	NAGIOS	ZABBIX	CACTI	ZENOSS	MUNIN
Descripción General	Proporciona supervisión de los servicios de red y recursos de host.	Diseñado para monitorear y registrar el estado de varios servicios de red, servidores y hardware de red.	Diseñado como una completa interface para almacenar datos de RRDTool y la utilidad gráfica.	Es un servidor y plataforma de gestión de red.	Utiliza RRDtool para presentar resultados gráficos a través de su interface.
Requisitos del Software	Sistema Operativo CentOS 5 y 6 Apache PHP GCC Compiler GD Development libraries	Apache 1.3.12 o superior. PHP 4.3 o superior. Mysql 3.22 o superior php-mysql net-snmp-devel (para soporte SNMP)	RRDtool Mysql PHP HTTPD SNMP	python-dev libmysqlclient15-dev mysql-server build-essential binutils make swig h.autoconf	Epel Repository RRDtool Apache servidor LAMP Apache2 MySQL
Soporte de software	Si	Si	Si	Si	Si
Documentación	http://www.nagios.org/documentation	http://www.zabbix.com/es/documentation.php	http://docs.cacti.net/	http://www.zenoss.com/resources/documentation	http://munin-monitoring.org/wiki/Documentation
Experiencia	12 años	9 años	13 años	12 años	8 años
Protocolos soportados	SMTP POP3 HTTP NNTP ICMP SNMP FTP SSH	SNMP TCP ICMP IPMI	SNMP ICMP UDP TCP	HTTP POP3 NNTP SNMP FTP	SNMP
Valoración del software	9.5	8.0	10	8.0	8.5
Interface de usuario	Interface web	Interface web	Interface Web	Interface Web	Interface Web

Tabla 4.11: Análisis del Software de monitoreo F/oos

Elaborado por: Carlos Sánchez

Se determinó que existe una gran variedad de software que cumple con lo requerimientos del sistema de gestión, de los cuales se elige Cacti como software para el monitoreo de la red, ya que este proporciona varios servicios con una plataforma sencilla, además que proporciona un amplio soporte y experiencia en el desarrollo de software, las dependencias no son complicadas de instalar y soporta el protocolo snmp que permite el monitoreo de todos los nodos de la red existentes.

4.6.5.7. CACTI

Es una solución gráfica completa de la red diseñada para aprovechar el poder de RRDtool almacenamiento de datos y la funcionalidad gráfica. Cacti ofrece una rápida variedad y avanzada de plantillas gráficas, múltiples métodos de adquisición

de datos, y las características de administración de usuarios fuera de la caja. Todo esto está envuelto en una intuitiva interfaz de fácil uso, que tenga sentido para las instalaciones LAN de tamaño hasta redes complejas con cientos de dispositivos. [30]

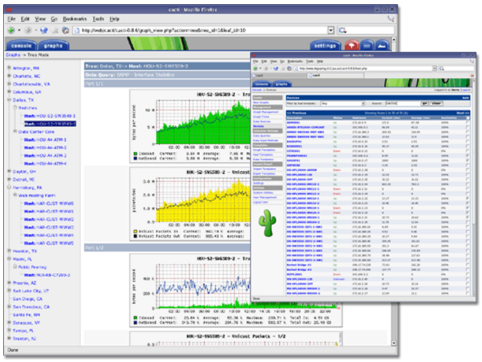


Figura 4.42: Cacti Pagina Oficial
Fuente: http://www.cacti.net/

Esta herramienta permite monitorizar y visualizar gráficas y estadísticas de dispositivos conectados a una red y que tengan habilitado el protocolo SNMP. Esta permite visualizar gráficas del estado de nuestra red, ancho de banda consumido, detectar congestiones o picos de tráfico o monitorizar determinados puertos de un equipo de red.

Con Cacti se puede monitorizar cualquier equipo de red que soporte el protocolo SNMP, ya sea un switch, un router o un servidor Linux. Siempre que tengan activado el protocolo SNMP y se conozcan las MIBs con los distintos OIDs (identificadores de objeto) que se puede monitorizar y visualizar, además programar la colección de gráficas con las que se desea realizar el seguimiento. Cacti es una aplicación que funciona bajo entornos Apache + PHP + MySQL, por tanto, permite una visualización y gestión de la herramienta a través del navegador web. La herramienta utiliza RRDtool, que captura los datos y los almacena en una base de datos circular, permitiendo visualizar de forma gráfica los datos capturados mediante MRTG (Multi Router Traffic Grapher).

La instalación es sencilla ya que se encuentra como paquete en la mayoría de los repositorios de distribuciones Linux. Es decir que al digitar **yum install cacti** en CentOS, se instala la aplicación y todas las dependencias necesarias, tales como MySQL, Apache, PHP. La instalación básica de Cacti incluye una aplicación basado en php, que es suficiente para una red con 10 o12 hosts de red, pero que con muchos dispositivos empieza a aumentar la carga del sistema de forma preocupante.

El funcionamiento de Cacti es muy sencillo, la aplicación revisa a cada uno de los hosts que tiene configurados solicitando los valores de los parámetros OIDs. El

período de sondeo es configurable por el administrador, éste determina la precisión de la información a visualizar, ya que un período bajo aumenta la cantidad de datos capturados y, por tanto, la resolución de la representación gráfica. Y en un período corto de muestreo aumenta la carga del sistema.

Cacti es una herramienta versátil en la que existen bastantes templates hechos para diferentes equipos y fabricantes, si no se encuentra lo algún templates este permite construir a medida siempre y cuando se posea los MIBs de los fabricantes, por lo que la flexibilidad de uso es alta. [30]

4.7. POLÍTICAS DE ACCESO A LA RED INSTITUCIONAL

Según las normas ISO 17799 inciso 11.4 del control del acceso a la red se establecen las políticas para el uso de los servicios de red bajo la premisas establecidas en dicho documento.

Conjuntamente y respetando el Reglamento se establece las siguientes políticas de acceso a los servicios de red e Internet de la institución.

4.7.1. Políticas Generales

- Es responsabilidad del centro educativo promover el uso de las Tecnologías de la Información y la Comunicación en el ámbito educativo entre el alumnado y el profesorado.
- La red de la institución constituye un apoyo de la actividad educativa Baños estableciendo un apoyo metodológico del proceso enseñanza aprendizaje por lo que el servicio es exclusivo para la comunidad educativa.
- Se autorizara el acceso al servicio a quien lo solicite bajo supervisión y monitoreo del docente y el encargado de la red.
- La red permitirá la reproducción de videos y descarga de archivos exclusivos para el campo educativo solo a Autoridades y docentes.
- Todos los usuarios de la Institución tienen acceso a Internet con los equipos asignados para su trabajo o equipos identificados en el departamento de administración de redes.
- Los usuarios podrán ver los equipos de la red y compartir archivos entre sí, mas no con los usuarios de otras redes.

- Se determinará que ancho de banda mínimo requerido se asignara a cada usuario y procesos distribuyendo de una manera equitativa para todos los usuarios.
- Se monitoreará constantemente el tráfico de red, el acceso a sitios web y el uso de ancho de banda.
- Para el ingreso a la red los dispositivos finales deben registrarse en la administración de redes para posteriormente ser autorizadas.
- Los equipos utilizados para la conexión de la intranet, contaran con una autenticación WPA o WPA2 para su acceso.
- Establecer el plan de direccionamiento de las subredes pertenecientes a la institución.

4.7.2. Políticas del Servidor Proxy

- El departamento de administración de redes controlara el acceso a páginas con contenido pornográfico, farándula, juegos online o en red y el acceso a motores de descarga tomando en cuenta que el uso de Internet es netamente académico en horarios establecidos.
- El administrador limitara el acceso a páginas de ventas por Internet dependiendo del usuario y propósito de la misma.
- La administración controlara el acceso a redes sociales de acuerdo a la hora establecida por el reglamento institucional.
- El departamento de administración de redes controlara el acceso a páginas con contenido de videos, películas, series o afines limitando el acceso a información de carácter educativo o con fines justificables.

4.7.3. Políticas de Firewall

- Añadir una regla que permita acceder a los servicios de administración del Firewall desde las direcciones IP de administración 192.168.10.208/28.
- Negar el acceso a los servicios de administración desde cualquier otra IP perteneciente a la red.
- Establecer reglas de conexión entre las subredes internas de ser necesario.

- Establecer una regla que envié las peticiones HTTP y HTTPS hacia el servidor Proxy.
- Establecer una regla que permita al servidor Proxy salir hacia el Internet una vez filtrado el tráfico HTTP y HTTPS.
- Habilitar el trafico ssh, dns a través de la intranet y la red interna de la institución.
- Habilitar un puerto seguro para acceso remoto a través del protocolo ssh desde la subred de equipos administradores hacia la intranet.

4.8. Diseño del sistema de gestión en base a las políticas de acceso

Una vez determinado las políticas de acceso a la red institucional, se aplica los conceptos estudiados para el sistema de gestión sobre la red LAN.

4.8.1. Plan de direccionamiento de la red institucional

En el cuál se presenta el esquema de direccionamiento de las subredes que necesita la institución con los diferentes fines, se aplica el concepto de VLSM para optimizar la subred, logrando así distribuir de mejor manera los servicios de red.

Plan de Direcionamiento de la red Institucional								
	Nº Máquinas	Direcion de Red	Rango de direcionamiento	Gateway	Dir. De Broadcast	Mascara de Red	CIDR	Dir. Disponibles
Estudiantes Inalámbrica	50	192.168.10.0	192.168.10.2 - 192.168.10.62	192.168.10.1	192.168.10.63	255.255.255.192	/26	10
Docentes de Red Inalámbrica	40	192.168.10.64	192.168.10.66 - 192.168.10.126	192.168.10.65	192.168.10.127	255.255.255.192	/26	20
Laboratorio 1	24	192.168.10.128	192.168.10.130 - 192.168.10.158	192.168.10.129	192.168.10.159	255.255.255.224	/27	4
Laboratorio 2	24	192.168.10.160	192.168.10.162 - 192.168.10.190	192.168.10.161	192.168.10.191	255.255.255.224	/27	4
Área Administrativa	10	192.168.10.192	192.168.10.194 - 192.168.10.206	192.168.10.195	192.168.10.207	255.255.255.240	/28	2
Dep. Redes	10	192.168.10.208	192.168.10.210 - 192.168.10.222	192.168.10.209	192.168.10.223	255.255.255.240	/28	2
Invitados	6	192.168.10.224	192.168.10.226 - 192.168.10.230	192.168.10.225	192.168.10.231	255.255.255.248	/29	0
Total de Host	164							42

Tabla 4.12: Plan de Direccionamiento de red

Elaborado por: El investigador

Tomando en cuenta que el crecimiento de las redes es aproximadamente un 25 % cada tres años se posee 42 direcciones disponibles las cuales ayudaran a solventar el crecimiento en cada una de las subredes.

4.8.1.1. Esquema de red Propuesto

El siguiente esquema de red se propone como una solución alternativa al diagrama existente usado actualmente por la institución.

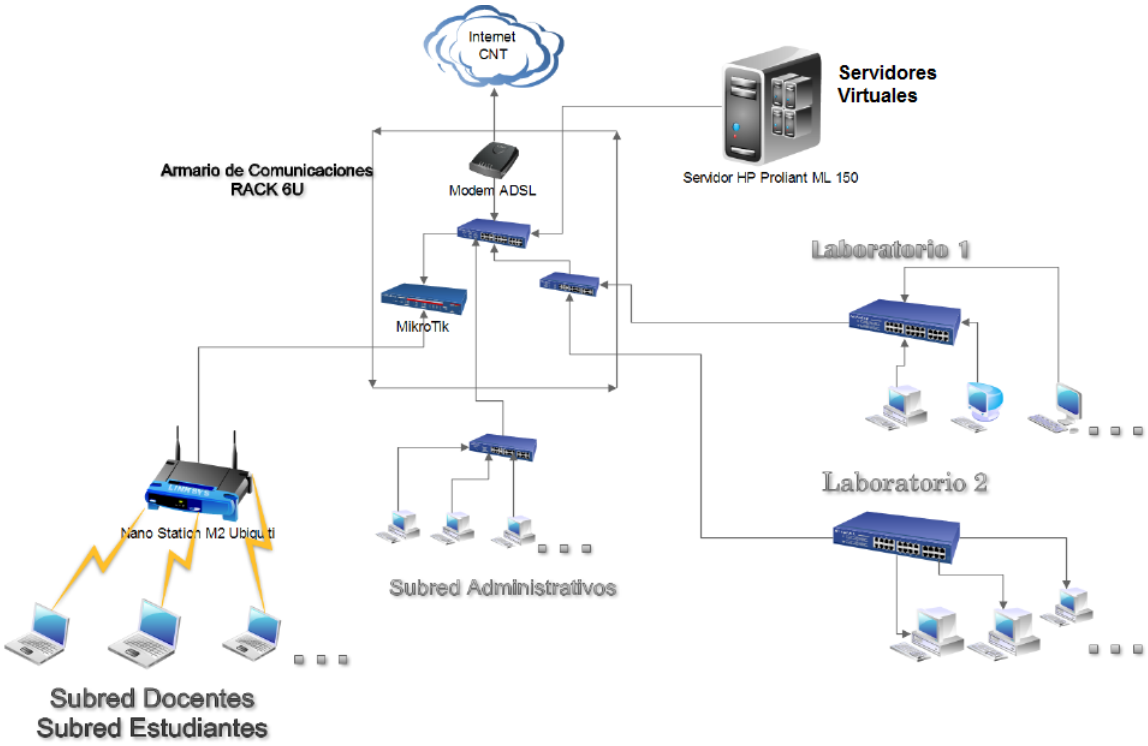


Figura 4.43: Esquema de red de la Propuesta
Elaborado por: El Investigador

4.8.2. Instalación y configuración de CentOS en el Servidor HP Proliant ML 150

4.8.2.1. Creación de RAID 1

Descargar de la página oficial de CentOS, la versión más reciente que es CentOS 6.5. El archivo ISO descargado ocupa 4,16 Gbytes, por lo que se puede grabar en un DVD para proceder a la instalación del servidor.

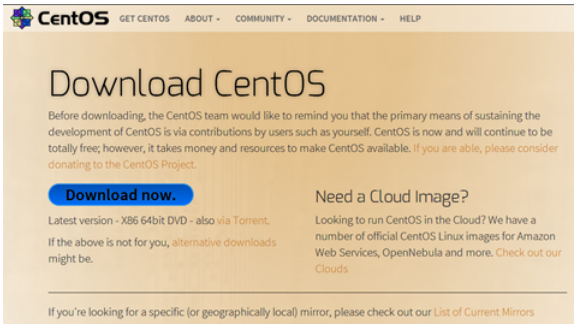


Figura 4.44: Página Oficial CentOS
Elaborado por: El investigador

Bootear desde DVD

Se Introduce el DVD grabado en el servidor. Encender y arrancar desde la unidad de DVD donde aparecerá una pantalla de bienvenida que nos permite instalar, actualizar o entrar en modo rescate.

Se va a instalar desde cero, por lo que se selecciona la primera opción y se salta la verificación del disco. En los siguientes pasos, se elige el idioma, la distribución de teclado, hasta elegir una instalación de CentOS nueva.

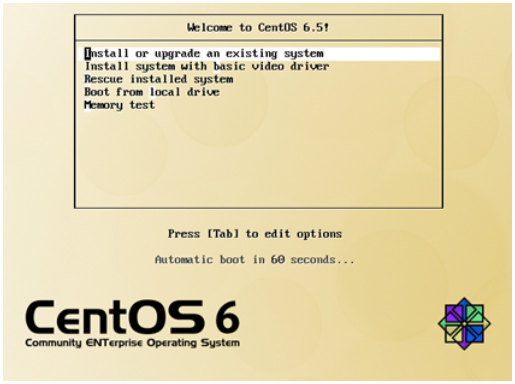


Figura 4.45: Instalación de CentOS
Elaborado por: El investigador

Selección de instalación

Seleccionar una instalación personalizada para poder modificar las particiones de los discos.

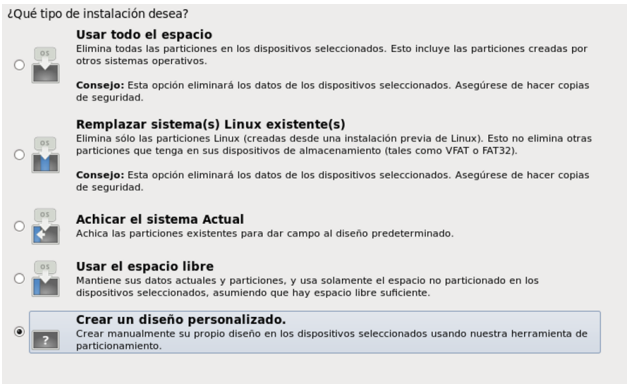


Figura 4.46: Selección del tipo de instalación CentOS
Elaborado por: El investigador

Selección y modificación de particiones

Teniendo las particiones en blanco empezamos a crear nuevas particiones en donde se elige partición Raid.

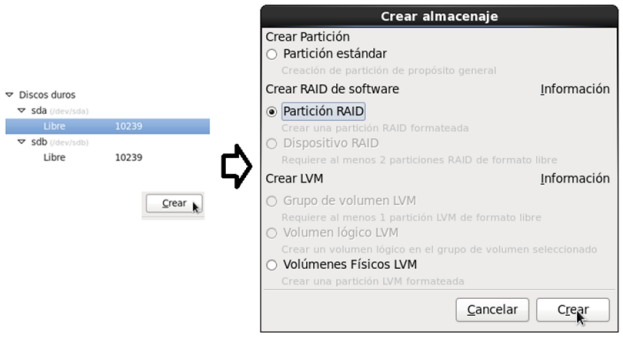


Figura 4.47: Creación de particiones Raid
Elaborado por: El investigador

Crear RAID 1

Seleccionar el sda, ajustar el tamaño al mínimo requerido en este caso 2 GB, como tamaño fijo y forzar a partición primaria y aceptar.

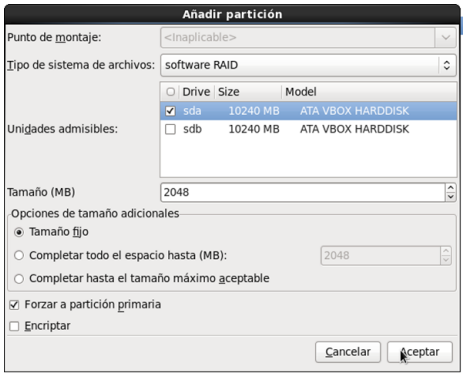


Figura 4.48: Creación de particiones Raid Primaria
Elaborado por: El investigador

Repetir el proceso para el resto de espacio en el mismo disco 1 pero con la variación de que no será un disco primario como se muestra en la siguiente imagen.

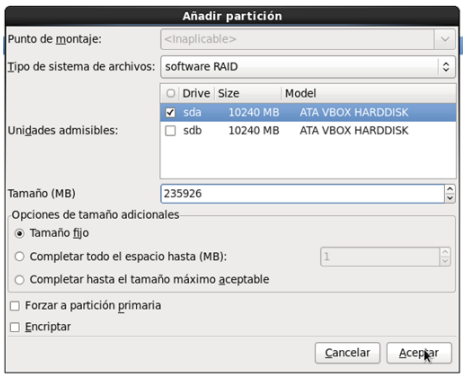


Figura 4.49: Creación de particiones Raid Secundaria
Elaborado por: El investigador

Realizar el mismo proceso en el disco 2 para tener una distribución de la siguiente manera.

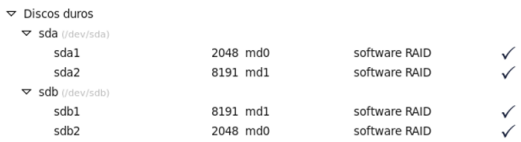


Figura 4.50: Visualización de particiones RAID
Elaborado por: El investigador

En donde el software Raid tiene las mismas capacidades en este caso existen dos de 2GB y 2 del resto del espacio del disco en donde se crea.

Crear Particiones Lógicas Raid

Seleccionar la primera partición RAID del disco 1 que será /dev/sda1 oprimir el botón crear y seleccionar dispositivo RAID y crear.

Figura 4.51: Creación de almacenaje dispositivos RAID
Elaborado por: El investigador

Una vez ingresado en el asistente de creación de dispositivo RAID teclear los siguientes datos:

Punto de Montaje: /boot

Tipo de Sistema de Ficheros: ext3

Dispositivo RAID: md0

Nivel RAID: RAID1

Miembros del RAID: Seleccionar los sda1 de 2GB y sdb2 de 2GB.

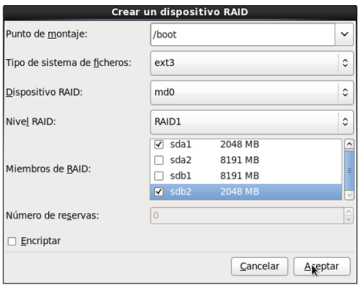


Figura 4.52: Creación de dispositivo RAID md0
Elaborado por: El investigador

Seleccionar la segunda partición RAID del disco 1 que será /dev/sda2 oprimir el botón crear y seleccionar dispositivo RAID y crear. Repetir el proceso de creación de dispositivo RAID con los siguientes datos:

Punto de Montaje: Sin nada

Tipo de Sistema de Ficheros: physical volumen (LVM)

Dispositivo RAID: md1

Nivel RAID: RAID1

Miembros del RAID: Seleccionar los sda2 y sdb1

Figura 4.53: Creación de dispositivo RAID md1
Elaborado por: El investigador

Crear de los Puntos de montaje

Seleccionar la partición creada en dispositivos RAID md1 y oprimir el botón crear, una vez abierto el asistente en el campo Crear LVM seleccionar Grupo de Volumen LVM y crear.

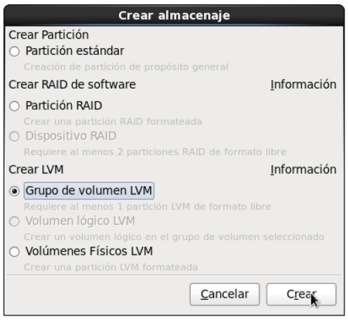


Figura 4.54: Creación de Volumen LVM
Elaborado por: El investigador

En la siguiente pantalla modificar los parámetros así:

1. **Nombre del Grupo:** Por defecto
2. **Extensión física:** 32
3. **Pulsar Añadir**

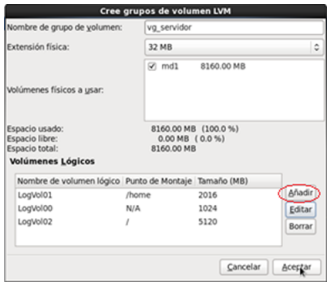


Figura 4.55: Creación de Grupos LVM
Elaborado por: El investigador

Crear los volúmenes lógicos para swap, home y /. Con los siguientes parámetros:
Swap:

- a) Punto de Montaje: Vacío
- b) Tipo de sistema de ficheros: swap
- c) Nombre del volumen lógico: logVol00
- d) Tamaño(MB): 15000 (debe ser Igual o mayor a la Memoria RAM del equipo)
- e) Presionar aceptar

Figura 4.56: Creación de Volumen para swap
Elaborado por: El investigador

/HOME:

- a) **Punto de Montaje:** /home
- b) **Tipo de sistema de ficheros:** ext3
- c) **Nombre del volumen lógico:** logVol01
- d) **Tamaño(MB):** 20000 (Unos 20 GB)
- e) **Presionar aceptar**

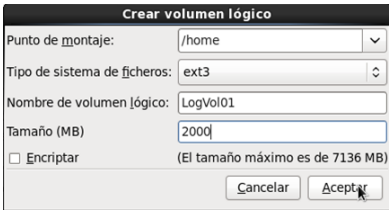


Figura 4.57: Creación de Volumen para /home
Elaborado por: El investigador

/:

- a) **Punto de Montaje**: /
- b) **Tipo de sistema de ficheros:** ext3
- c) **Nombre del volumen lógico:** logVol02
- d) **Tamaño(MB):** Resto del Tamaño del Disco
- e) **Presionar aceptar**

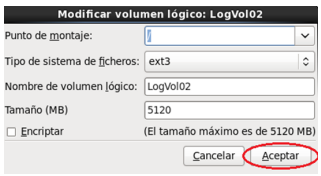


Figura 4.58: Creación de Volumen para /
Elaborado por: El investigador

Una vez terminado la creación de volúmenes la distribución de los discos será de la siguiente manera:

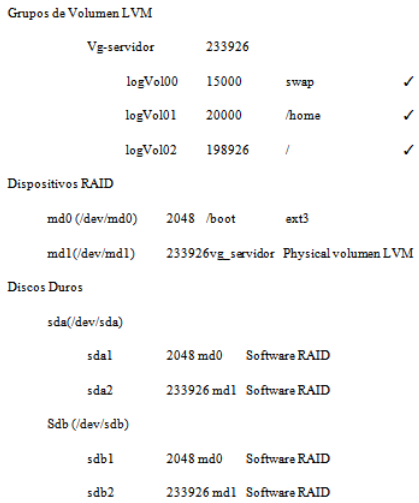


Figura 4.59: Resumen de modificación de las Particiones
Elaborado por: El investigador

4.8.2.2. Instalación CentOS 6.5

Confirmar los cambios realizados en los discos y continuar la instalación de CentOS.

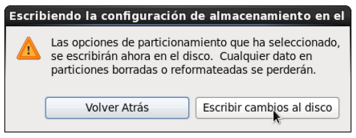


Figura 4.60: Confirmación de seguridad para cambios en los discos
Elaborado por: El investigador

Una vez terminado continuamos y elegimos el tipo de instalación que se desea realizar de las cuales elegimos un servidor básico.

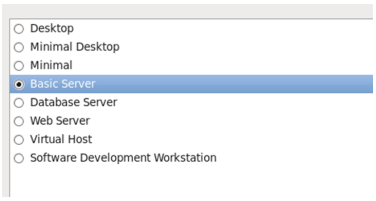


Figura 4.61: Selección del tipo de instalación
Elaborado por: El investigador

Terminar la instalación CentOS

Una vez concluido la configuración el software calcula automáticamente el número de paquetes necesarios para la instalación e inicia el proceso. Una vez culminado el

proceso reiniciamos y está concluida la instalación del servidor.

4.8.2.3. Instalación y configuración de KVM

Para empezar la instalación del servidor de máquinas virtuales KVM es necesario realizar algunos cambios antes de configurar la plataforma de virtualización.

Para empezar se verifica si el cpu soporta virtualización con el siguiente comando:

```
egrep '(vmx | svm)' - color = Siempre / proc / cpuinfo
```

Obteniendo los siguientes resultados:

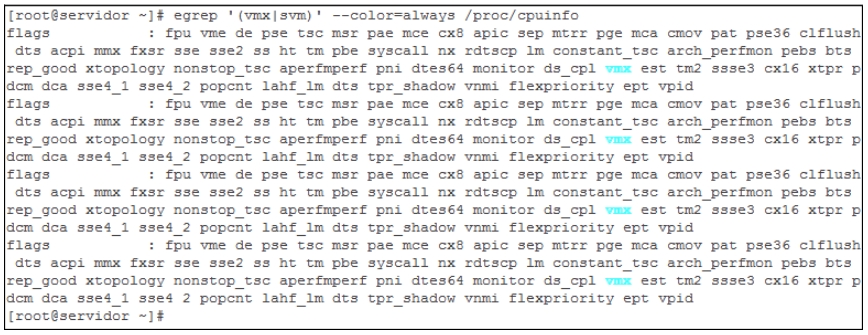


Figura 4.62: Verificación del CPU para virtualización
Elaborado por: El investigador

Es decir que el CPU admite cuatro virtualizaciones que es ideal para aplicar el concepto de KVM para una virtualización completa.

Antes de instalar es necesario obtener las claves GPG para los paquetes de software a través del siguiente comando:

```
rpm - import / etc / pki / rpm-gpg / RPM-GPG-KEY *
```

Para instalar KVM y virtinst (herramienta para crear máquinas virtuales), se ejecuta el comando:

```
yum -y groupinstall kvm libvirt-python virtinst qemu-kvm
```

A continuación, inicie el demonio libvirt:

```
# service libvirtd start
```

Para comprobar si KVM se ha instalado correctamente, se ejecuta

```
# virsh -c qemu :///system list
```

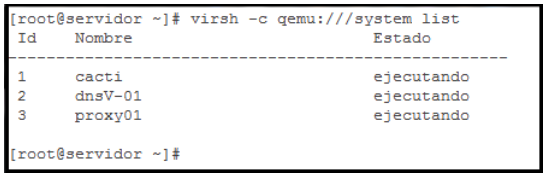


Figura 4.63: virsh list
Elaborado por: El investigador

Lo siguiente es establecer un puente de red en el servidor para que las máquinas virtuales se pueda acceder desde otros hosts como si fueran sistemas físicos de la red.

Para ello, es necesario instalar el paquete bridge-utils por lo que se ejecuta:

```
# yum install bridge-utils
```

Se acepta la instalación de los paquetes y se procede a configurar el puente de red.

Configuración del MODO BRIDGE

Este tipo de configuración nos permite crear un puente entre la tarjeta de red física y las virtuales, permitiéndonos conectarnos a la red local de la institución como si fuera otra máquina que estuviera en la red local. Para poder tener este tipo de configuración es necesario instalar el siguiente paquete.

```
servidor:~# yum -y install bridge-utils
```

Al estar utilizando la distribución CentOS para configurar el puente en la interface de red abrir el archivo con el editor vi. Al archivo /etc/sysconfig/network-scripts/ifcfg-eth0.

```
servidor:~# vi /etc/sysconfig/network-scripts/ifcfg-eth0
```

Donde se modifica de la siguiente manera:

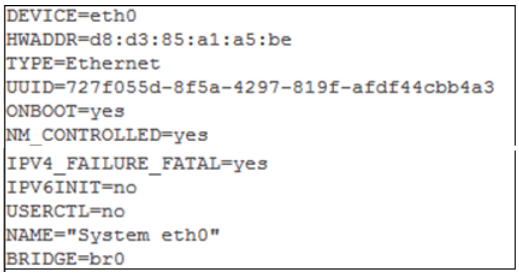


Figura 4.64: Interface eth0
Elaborado por: El investigador

Una vez terminado la modificación guardar la configuración del archivo para poder copiarlo y modificarlo en la nueva interface tipo bridge:

```
servidor:~# cp /etc/sysconfig/network-scripts/ifcfg-eth0 /etc
/sysconfig/network-scripts/ifcfg-br0
```

y se edita de la siguiente manera.

```
servidor:~# vi /etc/sysconfig/network-scripts/ifcfg-br0
```

```
DEVICE=br0
TYPE=Bridge
ONBOOT=yes
NM_CONTROLLED=yes
BOOTPROTO=none
IPADDR=192.168.1.3
NETMASK=255.255.255.248
DNS2=8.8.8.8
GATEWAY=192.168.1.1
DNS1=192.168.1.1
DEFROUTE=yes
IPV4_FAILURE_FATAL=yes

IPV6INIT=no
USERCTL=no
STP=yes
DELAY=0
```

Figura 4.65: Interface br0
Elaborado por: El investigador

Una vez terminado el proceso reiniciar el servicio de red:

```
servidor:~# service network restart
```

Escribir la regla de Firewall que permita la conexión en modo bridge:

```
servidor:~# iptables -I FORWARD -m physdev --physdev-is-bridged
-j ACCEPT
servidor:~# service iptables save
servidor:~# service iptables restart
```

4.8.2.4. Creación de una MV con KVM por consola

Para poder hacer la instalación desde consola de una máquina virtual, se ejecuta el comando virt-install.

virt-install [conexión][opciones]

En tipo de conexión siempre va hacer –connect qemu:/system y en opciones podremos poner los siguientes parámetros:

Parámetro	Descripción
-n	**Nombre la máquina virtual**
-r	**Memoria RAM virtual**
-f	**Ruta del Disco Duro Virtual**
-s	**Tamaño del disco duro**
-c	**Unidad DVD/CDRom o imagen ISO.**
-l	**Indica que la instalación es por medio de http, ftp o nfs**
–network=br0	**Modo de conexión a la red física en puente.**
-w network=default	**Modo de conexión a la red virtual en NAT**
-vcpus	**Número de CPU virtuales.**
–vnc	**Conexión tipo VNC**

Tabla 4.13: Opciones de virt-install

Elaborado por: El investigador

Instalación por línea de comandos:

```
virt-install --connect qemu:///system -n dnsV-01 -r 512 -f /vm
/dnsV-01.img -s 10 -c /usr/centos/CentOS-6.5-i386-bin-DVD.iso
--network=bridge:br0
```

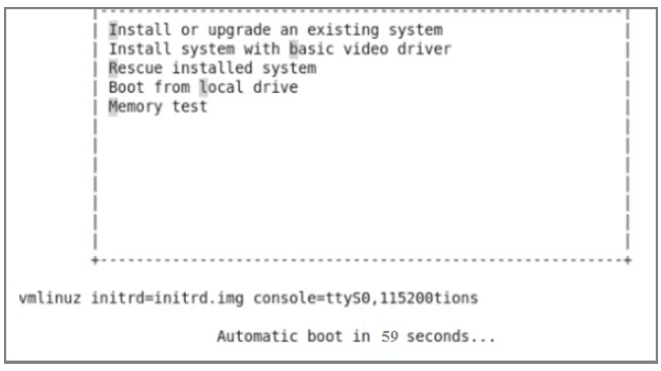


Figura 4.66: Instalación de una máquina virtual con KVM console
Elaborado por: El investigador

Una vez iniciado editar la instalación con la tecla TAB y digitar “vmlinuz initrd=initrd.img console=ttyS0,115200” y continuar la instalación de forma normal.

4.8.2.5. Clonación de Máquinas Virtuales

Una vez creado la máquina virtual antes de realizar cualquier modificación proceder a clonar la máquina virtual con el siguiente comando. Esto evitará una nueva instalación y se podrá clonar las máquinas virtuales que se requieran.

```
virt-clone -o dnsV-01 -n server-clone -f /vm/server_clone.img
```

Una vez clonada la máquina virtual proceder a configurar la interface eth0 o la que ha sido asignada de la siguiente manera.

```
# vi /etc/udev/rules.d/70-persistent-net.rules
```

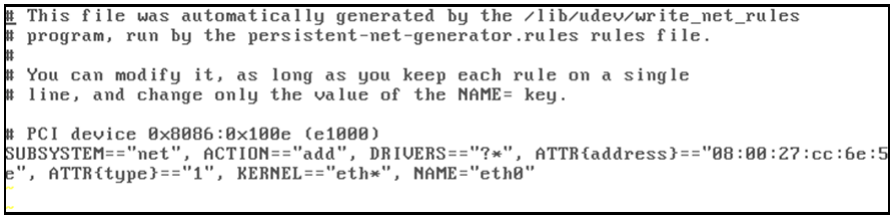


Figura 4.67: Instalación de una máquina virtual con KVM consola
Elaborado por: El investigador

Donde se confirma la interface que se está utilizando y la MAC address asignada. Estos datos deben coincidir con la configuración de la interface en vi /etc/sysconfig/network-scripts/ifcfg-eth0.

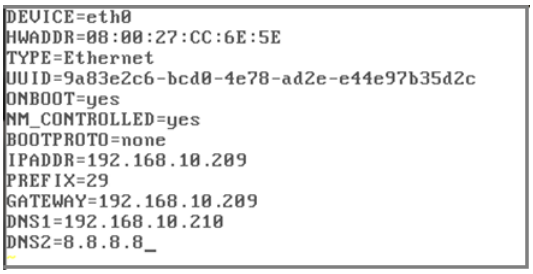


Figura 4.68: Interface Eth0 de la máquina virtual proxy01
Elaborado por: El investigador

Este proceso se realiza para cada una de las máquinas virtuales que se ocuparan.

4.8.3. Configuración de los servicios establecidos en los equipos de red

A continuación se precede a configurar los siguientes servicios:

- Configuración del servidor Proxy con squid
- Configuración del servidor Firewall con Netfilter
- Configuración del servidor DNS con DNSMASQ
- Configuración del servidor DHCP con el servicio dhcpd

4.8.3.1. Configuración del Servidor PROXY con SQUID

Una vez iniciado el servidor Proxy se instala los servicios squid y httpd.
Digitar el comando:

```
# yum -y install squid httpd
```

Al completarse la instalación se puede iniciar con la configuración.

Políticas del Proxy

La función del Proxy en la red institucional será para filtrar el trafico http que contenga pornografía, farándula, juegos online, limitar el acceso a motores de descarga, ventas por Internet, redes sociales, videos, películas o series que no tengan un carácter educativo por lo que se creara tres tipos de archivos en los cuales se establecerán estos parámetros de bloqueo.

Parámetros de Configuración Básicos

Una vez clara la función principal del servidor se procede a la configuración de los parámetros iniciales:

```
acl manager proto cache_object
acl localhost src 127.0.0.1/32 ::1
acl to_localhost dst 127.0.0.0/8 0.0.0.0/32 ::1

# Example rule allowing access from your local networks.
# Adapt to list your (internal) IP networks from where browsing
# should be allowed

acl localnet src 192.168.10.0/24
acl block url_regex -i "/etc/squid/listas/block.squid"
acl deniedsites url_regex -i "/etc/squid/listas/deniedsites"
acl extensions urlpath_regex "/etc/squid/listas/extensions"


acl SSL_ports port 443
acl Safe_ports port 80          # http
```

Figura 4.69: Descripción del archivo squid.conf
Elaborado por: El investigador

Donde se da acceso a localhost y se define como subred local a 192.168.10.0/24 es decir que esta red puede acceder al servidor Proxy. También se define el archivo deniedsites, block y extensions la cual ayuda a definir cuáles son los sitios bloqueados.

Una vez realizado este proceso se permite o se deniega el acceso de la siguiente manera:

```
#
# INSERT YOUR OWN RULE(S) HERE TO ALLOW ACCESS FROM YOUR CLIENTS
#

# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
http_access allow localhost
http_access allow localnet !block !deniedsites !extensions
#http_access deny all


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

Figura 4.70: Permitir acceso a la red local y filtrado de sitios
Elaborado por: El investigador

Reglas de Control de Acceso.

Las líneas que se definen a continuación son las reglas que permiten acceder la red LAN hacia el Proxy.

```
# Example rule allowing access from your local networks.
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
#http_access allow localnet
http_access allow localhost
```

Figura 4.71: Listas de redes Locales para Squid por archivo
Elaborado por: El investigador

En la siguiente línea se establece la regla que permite a Squid acceder a la lista denominada localnet:

```
http_access allow localnet
```

También se define de la siguiente manera:

```
http_access allow localnet ¡deniedsites
```

Donde existe acceso a squid por parte de localnet y deniega el acceso a la deniedsites.

Esto se aplica para reducir el número de acl y hacer más rápido el funcionamiento del squid.

Opción http_port.

Si se necesita configurar el servidor Proxy en modo transparente, por lo que es necesario añadir la opción transparent así:

```
http_port 192.168.10.209:3128 transparent
```

Opción cache_dir.

La opción que nos permitirá que squid tenga un mayor desempeño trabajando de manera asíncrona será:

```
cache_dir aufs /var/spool/squid 512 16 256
```

Donde se establece 2 GB para almacenaje del cache del Proxy y los demás valores son los niveles de subdirectorios admitidos.

Opción maximum_object_size.

```
máximum_object_size 64 MB
```

Donde se define el tamaño máximo de los objetos del caché generando un mejor desempeño al cache del Proxy.

Opciones cache_swap_low y cache_swap_high.

```
cache_swap_low 90
cache_swap_high 95
```

Lo anterior permite tener un caché saludable que se limpia automáticamente al llegar a un 90 % de uso.

Creación de los Archivos de configuración

Primero para crear los archivos de configuración es necesario crear un directorio llamado listas dentro el directorio squid de la siguiente manera:

```
# mkdir /etc/squid/listas
```

Una vez creado el directorio se empieza a crear los archivos de configuración del squid.

```
#nano /etc/squid/listas/deniedsites
```

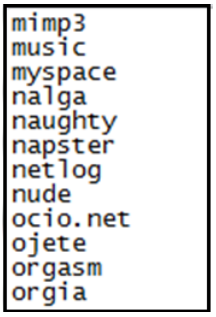


Figura 4.72: Archivo deniedsites
Elaborado por: El investigador

Donde se escribe los sitios bloqueados por el Proxy los cuales se definen como pornografía, farándula y juegos online.

Ahora se crea el directorio block que contiene páginas en la cuales se realizan descargas, se ven videos, películas o series.

```
#nano /etc/squid/listas/block
```

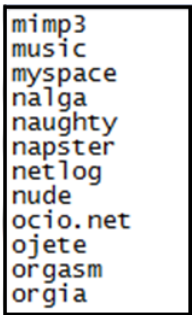


Figura 4.73: Archivo deniedsites
Elaborado por: El investigador

Aquí se describe los sitios bloqueados por el Proxy los cuales se definen como películas, series, motores de descarga.

Archivo de extensiones bloqueadas

```
#nano /etc/squid/listas/extensions
```

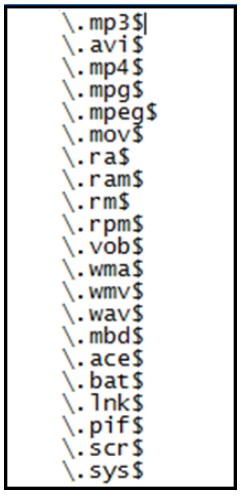


Figura 4.74: Archivo deniedsites
Elaborado por: El investigador

El archivo contiene una descripción de las extensiones de archivos los cuales son innecesarios y no se desea utilizar en el campo educativo.

Descripción del archivo final de squid

```
acl localnet src 192.168.10.0/24
acl block url_regex -i "/etc/squid/listas/block.squid"
acl deniedsites url_regex -i "/etc/squid/listas/deniedsites"
acl extensions urlpath_regex "/etc/squid/listas/extensions"


acl SSL_ports port 443
acl Safe_ports port 80          # http
acl Safe_ports port 21          # ftp
acl Safe_ports port 222         #ssh
acl Safe_ports port 443         # https
acl Safe_ports port 70          # gopher
acl Safe_ports port 210         # wais
acl Safe_ports port 1025-65535  # unregistered ports
acl Safe_ports port 280         # http-mgmt
acl Safe_ports port 488         # gss-http
acl Safe_ports port 591         # filemaker
```

Figura 4.75: Configuración Final del Squid 1
Elaborado por: El investigador

```
# Adapt localnet in the ACL section to list your (internal) IP networks
# from where browsing should be allowed
#http_access allow localhost
#http_access allow innocent
http_access allow localnet !block !deniedsites !extensions
#http_access deny  ipblocked
#http_access deny all


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

# Squid normally listens to port 3128
#http_port 3128
http_port 192.168.10.209:3128 transparent


# We recommend you to use at least the following line.
 ierarchy stoplist cgi-bin ?
```

Figura 4.76: Configuración Final del Squid 2
Elaborado por: El investigador

4.8.3.2. Instalación y configuración de NETFILTER (iptables)

Este servicio se instala con el servidor en caso de no hacerlo es posible instalarlo con la siguiente expresión:

```
# yum -y install iptables
```

Una vez instalado el servicio se procede a configurar editando el archivo.

```
# vi /etc/sysconfig/iptables
```

En donde se especifica qué tipo de tráfico es permitido y cual es bloqueado además en este caso va a servir para realizar rutas hacia el servidor Proxy y poder usarlo en una configuración transparente.

Políticas del Firewall

Las principales acciones del Firewall serán permitir un acceso total entre la LAN, dar Internet al Proxy a través de la interfaz eth1 WAN, habilitar el tráfico ssh y dns y filtrar el tráfico del puerto 443 https.

Iniciando la Configuración de iptables

Al conocer las funciones que desempeñara el Proxy se procede primero a limpiar las configuraciones de iptables antiguas o por defecto.

```
# iptables -F
# iptables -X
# iptables -t nat -F
# iptables -t nat -X
# iptables -t mangle -F
# iptables -t mangle -X
```

Esto borra toda configuración previa o por defecto a partir de aquí se empieza la configuración total de la red:

Lo principal es poder acceder al servidor Firewall desde la red interna por lo que se aplica los siguientes parámetros:

Aceptar el tráfico entrante del localhost

```
# iptables -A INPUT -i lo -j ACCEPT
```

Aceptar el tráfico saliente del localhost

```
# iptables -A OUTPUT -o lo -j ACCEPT
```

Aceptar el tráfico entrante de la red LAN

```
# iptables -A INPUT -i eth0 -j ACCEPT
```

Aceptar el tráfico saliente de la red LAN

```
# iptables -A OUTPUT -o eth0 -j ACCEPT
```

Una vez habilitado el acceso desde localhost y la red LAN permitimos acceso remoto hacia el servidor por ssh a través del puerto configurado en este caso el puerto 22(cabe recalcar que se puede modificar el número de puerto de ser necesario).

```
# iptables -A INPUT -i eth1 -p tcp --dport 22 -j ACCEPT
# iptables -A OUTPUT -o eth1 -p tcp --sport 22 -j ACCEPT
```

Esto es temporal para fines de configuración posteriormente se eliminan comentando con el símbolo numeral. Para permitir conectar vía SSH desde mi red LAN al servidor de Firewall y Proxy.

```
# iptables -A INPUT -i eth0 -p tcp --dport 22 -j ACCEPT
# iptables -A OUTPUT -o eth0 -p tcp --sport 22 -j ACCEPT
```

Permitir conectar mi servidor al Internet, depende de servicio de DNS

```
# iptables -A OUTPUT -o eth1 -p tcp --dport 80 -j ACCEPT
# iptables -A INPUT -i eth1 -p tcp --sport 80 -j ACCEPT
```

Permitir al servidor conectarse a otros servidores de DNS.

```
# iptables -A OUTPUT -o eth1 -p udp --dport 53 -j ACCEPT
# iptables -A INPUT -i eth1 -p udp --sport 53 -j ACCEPT
```

Permitir hacer ping desde el servidor Aceptar ICMP request hacia fuera

```
# iptables -A OUTPUT -o eth1 -p icmp --icmp-type
echo-request -j ACCEPT
```

Aceptar ICMP reply hacia dentro

```
# iptables -A INPUT -i eth1 -p icmp --icmp-type
echo-reply -j ACCEPT
```

PROXY TRANSPARENTE

Para ejecutar Proxy transparente se define reglas en la tabla nat de la siguiente manera.

```
# iptables -A PREROUTING -i eth0 -p tcp -m tcp --dport 80 -j DNAT
--to-destination 192.168.10.209:3128
```

En donde se direcciona todo lo que sale por el puerto 80 de la LAN hacia el servidor Proxy con la dirección 192.168.10.209:3128 y el puerto 3128 y se refuerza con:

```
# iptables -A PREROUTING -p tcp -m tcp --dport 80 -j REDIRECT
--to-ports 3128
```

Con esto esta direccionado el tráfico hacia el Proxy transparente por lo que la siguiente regla se encarga de direccionar a la red LAN para que salga a Internet por el Proxy.

```
# iptables -A POSTROUTING -s 192.168.10.0/24 -o eth1 -j SNAT
-to-source 192.168.1.3
```

Es decir que todo lo que provenga de la LAN saldrá a Internet a través de la eth1 y específicamente de la dirección 192.168.1.3 que es la del servidor Proxy.

Direccionar el tráfico HTTPS hacia el Proxy al igual que el tráfico tcp por el puerto 80 direccionamos el tráfico HTTPS para que salga a través de la interfaz eth1 que posee el Proxy. En este caso es solo para obtener acceso a Internet por el puerto 443 ya que el Proxy no entenderá que se está enviando y se debe aplicar otras reglas para bloquear trafico HTTPS innecesario.

```
# iptables -A FORWARD -s 192.168.10.0/24 -o eth1 -p tcp -m tcp
-dport 443 -j ACCEPT
```

Bloquear FACEBOOK con Iptables

Recordando que squid no entiende el tráfico recibido por el puerto 443 ya que es encriptado y en la actualidad las redes sociales utilizan este puerto para dar sus servicios. La única manera de bloquear este tráfico es negando el dominio y la ip o grupos de ip usadas de la siguiente manera.

Se bloquea el dominio de facebook

```
#iptables -A FORWARD -p tcp -m string --string "es-la.facebook.com"
--algo bm --to 65535 -m tcp --dport 443 -j DROP
```

Se bloquea el rango de direcciones IP públicas usadas por facebook.

```
# iptables -A FORWARD -p tcp -m tcp --dport 443 -m iprange
--dst-range 31.13.0.0-31.13.80.255 -j DROP
```

Se bloquea el dominio de meebo.com y facebook.com

```
# iptables -A FORWARD -p tcp -m string --string "www.meebo.com"
--algo bm --to 65535 -m tcp --dport 443 -j DROP
# iptables -A FORWARD -p tcp -m string --string "www.facebook.com"
--algo bm --to 65535 -m tcp --dport 443 -j DROP
```

Resumen de reglas en iptables:

```
[root@wpad ~]# iptables -nL
Chain INPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp spt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:80
LOG        tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22 flags:0x
3F/0x02 LOG flags 0 level 4
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:22
LOG        all  --  0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 4

ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0           icmp type 0
ACCEPT     udp  --  192.168.1.0/29       0.0.0.0/0           udp spt:53
ACCEPT     udp  --  192.168.10.0/24      0.0.0.0/0           udp spt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:161
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:161
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp spt:53
DROP       all  --  0.0.0.0/0            0.0.0.0/0

Chain FORWARD (policy ACCEPT)
target     prot opt source               destination
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           STRING match "es-la
.facebook.com" ALGO name bm TO 65535 tcp dpt:443
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:443 destina
tion IP range 31.13.0.0-31.13.80.255
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           STRING match "www.m
eebo.com" ALGO name bm TO 65535 tcp dpt:443
DROP       tcp  --  0.0.0.0/0            0.0.0.0/0           STRING match "www.f
acebook.com" ALGO name bm TO 65535 tcp dpt:443
ACCEPT     tcp  --  192.168.10.0/24      0.0.0.0/0           tcp dpt:443
ACCEPT     tcp  --  192.168.10.0/24      0.0.0.0/0           tcp dpt:80
LOG        all  --  0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 4

Chain OUTPUT (policy ACCEPT)
target     prot opt source               destination
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     all  --  0.0.0.0/0            0.0.0.0/0
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:22
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp dpt:80
ACCEPT     icmp --  0.0.0.0/0            0.0.0.0/0           icmp type 8
LOG        all  --  0.0.0.0/0            0.0.0.0/0           LOG flags 0 level 4

ACCEPT     udp  --  0.0.0.0/0            192.168.1.0/29      udp spt:53
ACCEPT     udp  --  0.0.0.0/0            192.168.10.0/24     udp spt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:22
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp dpt:53
ACCEPT     tcp  --  0.0.0.0/0            0.0.0.0/0           tcp spt:161
ACCEPT     udp  --  0.0.0.0/0            0.0.0.0/0           udp spt:161
DROP       all  --  0.0.0.0/0            0.0.0.0/0

Chain HTTPS_BLOQUEO (0 references)
target     prot opt source               destination
```

Figura 4.77: Resumen de la configuración de iptables
Elaborado por: El investigador

4.8.3.3. Instalación y configuración del servidor DNS

En este punto se configura el servidor DNS que ayuda a resolver paginas web ya sea de forma directa o inversa con dnsmasq.

Instalar DNSMASQ en CentOS

```
#yum -y install dnsmasq*
```

Una vez terminada la instalación se inicia la configuración editando el archivo con:

```
# nano /etc/resolv.conf
```

En donde se debe ingresar la ip del servidor dns caché y la ip del dns externo a utilizarse en este caso la 8.8.8.8 que es el servidor DNS de google.

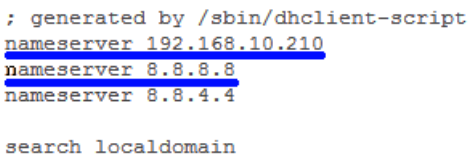


Figura 4.78: Archivo resolv.conf para el dns
Elaborado por: El investigador

Es necesarios también configurar la dirección ip en el archivo hosts:

```
# nano /etc/hosts
```

Donde se ingresa la ip del servidor dns y el nombre del equipo así:

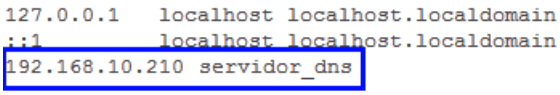


Figura 4.79: Configuración del archivo hosts
Elaborado por: El investigador

Una vez realizado estos cambios iniciar el servicio y luego añadirlo al inicio del sistema así:

```
# service dnsmasq restart
# chkconfig dnsmasq on
```

Listo

4.8.3.4. Instalación y configuración del servidor DHCP

Ejecutar lo siguiente para instalar o actualizar todos los paquetes necesarios:

```
# yum -y install dhcp
```

Modificaciones necesarias en el muro cortafuegos

Por lo general, jamás se abren puertos de DHCP a las redes públicas. Es necesario abrir los puerto 67 y 68 (BOOTPS yBOOTPC) por UDP, tanto para tráfico entrante como saliente.

Servicio IPTABLES

Como el servicio funciona a través de la interfaz eth0, puede utilizar el mandato IPTABLES del siguiente modo:

```
# iptables -A INPUT -i eth0 -p udp -m state -state NEW -m udp
-sport 67:68 -dport 67:68 -j ACCEPT
# service iptables save
```

Reiniciar el servicio IPTABLES a fin de que surtan efecto los cambios.

```
# service iptables restart
```

SELinux y el Servicio dhcpd.

Se desactivo el SELinux por lo que no necesita cambios.

Iniciar, detener y reiniciar, el servicio dhcpd.

Para agregar el servicio de dhcpd al inicio del sistema, en todos los niveles de ejecución, se digita:

```
# chkconfig dhcpd on
```

Para iniciar por primera vez el servicio dhcpd:

```
# service dhcpd start
```

Para que los cambios surtan efecto se reinicia el servicio de la siguiente manera:

```
#service dhcpd restart
```

Para detener el servicio dhcpd:

```
# service dhcpd stop
```

PROCEDIMIENTO DE CONFIGURACIÓN DHCP

Archivo de configuración /etc/sysconfig/dhcpd

El servicio DHCP funciona solo sobre la RED LAN a través de la interface eth0 por lo que se edita el archivo /etc/sysconfig/dhcpd y se agrega el valor eth0, como argumento de la opción DHCPDARGS de la interfaz utilizada por la red local.

Se edita el archivo /etc/sysconfig/dhcpd:

```
# nano /etc/sysconfig/dhcpd
# Command line options here
DHCPDARGS=eth0
```

ARCHIVO DE CONFIGURACIÓN dhcpd.conf

Una vez realizado esta configuración con los datos de la red LAN se procede a configurar con las siguientes características:

Para la Subred del Laboratorio 1

- Dirección IP del segmento de red: 192.168.10.128
- Dirección IP de difusión: 192.168.10.159
- Máscara de sub-red: 255.255.255.224 (27 bits)
- Puerta de enlace: 192.168.10.129
- Servidor de nombres: 192.168.10.210
- Rango de direcciones IP a asignar de modo dinámico: 192.168.10.130 hasta 192.168.10.158

Para la Subred del Laboratorio 2

- Dirección IP del segmento de red: 192.168.10.160
- Dirección IP de difusión: 192.168.10.191
- Máscara de sub-red: 255.255.255.224 (27 bits)
- Puerta de enlace: 192.168.10.161
- Servidor de nombres: 192.168.10.210
- Rango de direcciones IP a asignar de modo dinámico: 192.168.10.162 hasta 192.168.10.190

CONFIGURACIÓN BÁSICA

Para iniciar la configuración primero se debe sacar una copia de seguridad del archivo original del servicio dhcpd así:

```
# cd /etc/dhcp/
# cp dhcpd.conf dhcpd.conf.original
# cd
```

Como se utiliza CentOS 6, se edita el archivo /etc/dhcp/dhcpd.conf.

```
#nano /etc/dhcp/dhcpd.conf
```

Una vez ingresado modificar todos los parámetros descritos a continuación para las subredes:

```
ddns-update-style interim;
ignore client-updates;
authoritative;
default-lease-time 900;
max-lease-time 7200;
option domain-name "192.168.10.210";
option ntp-servers 0.pool.ntp.org, 1.pool.ntp.org, 2.pool.ntp.org;
subnet 192.168.10.128 netmask 255.255.255.224 {
        option routers 192.168.10.129;
        option subnet-mask 255.255.255.224;
        option broadcast-address 192.168.10.159;
        option domain-name-servers 192.168.10.210;
        range 192.168.10.130 192.168.10.158;

}                                                              4
subnet 192.168.10.160 netmask 255.255.255.224 {
        option routers 192.168.10.161;
        option subnet-mask 255.255.255.224;
        option broadcast-address 192.168.10.191;
        option domain-name-servers 192.168.10.210;
        range 192.168.10.162 192.168.10.190;

}
```

Figura 4.80: Configuración del archivo dhcpd.conf
Elaborado por: El investigador

Lo anterior corresponde a la configuración para el servidor DHCP de la red LAN institucional.

Una vez terminada la configuración, para iniciar el servicio ejecutar:

```
# service dhcpd start
```

4.8.3.5. Configuración del Hotspot en la MikroTik RB751U

Configuración de la interfaces LAN y WAN en la MikroTik Para iniciar la configuración de la MikroTik se procede a resetear todos los valores configurados por defecto.

Se ingresa en new terminal system reset-configuration.

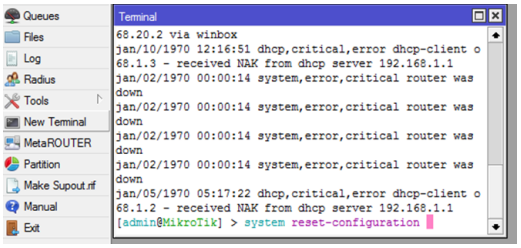


Figura 4.81: Reseteo de la Mikrotik
Elaborado por: El investigador

Al resetear completamente se pierde la conexión con la MikroTik y se procede a ingresar nuevamente y aceptar el reset completo de la MikroTik.

En este punto se puede acceder solo por MAC address en la cual se inicia la configuración de las interfaces. Como primer punto se crea las direcciones de red para cada interface en la dirección ip => addresses.

Interface LAN Inalámbrica

Dirección de Red	192.168.10.0/26
Gateway	192.168.10.1
Interface	Ether2

Tabla 4.14: Configuración de la Interface LAN Inalámbrica

Elaborado por: El investigador

Interface WAN

Dirección de Red	192.168.1.0/29
Gateway	192.168.1.1
Interface	Ether1

Tabla 4.15: Configuración de la Interface WAN

Elaborado por: El investigador

Mostrado en la siguiente imagen.

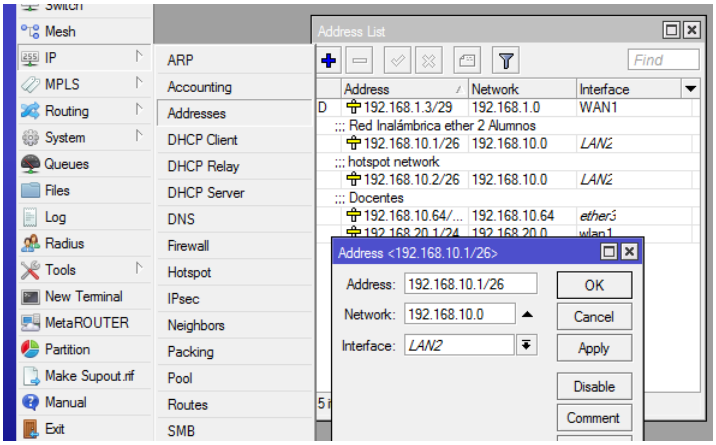


Figura 4.82: Configuración de la dirección de red Inalámbrica
Elaborado por: El investigador

Interface subred docentes => ether3

Dirección de Red	192.168.10.64/26
Gateway	192.168.10.65
Interface	Ether3
Comentario	Docentes

Tabla 4.16: Configuración de la Interface LAN 1

Elaborado por: El investigador

Es necesario la creación de un bridge accediendo a la pestaña bridge => nuevo bridge (+) y a continuación se acepta la configuración con la interface INALÁMBRICA con el bridge.

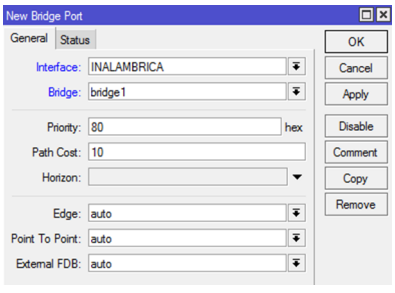


Figura 4.83: Entorno MikroTik para la configuración del bridge
Elaborado por: El investigador

Es necesario enmascarar las redes por lo que se ingresa al menú IP => Firewall => pestaña NAT.

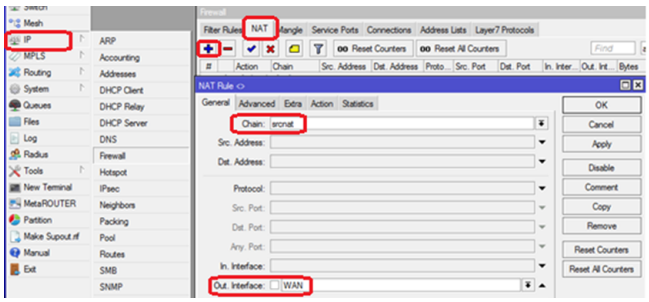


Figura 4.84: Entorno MikroTik para la configuración del NAT Firewall
Elaborado por: El investigador

Definir los parámetros de la regla nat:

- **Chain** srcnat
- **Out Interface** WAN

Y en la pestaña Accion seleccionar Masquerade como lo indica la imagen.

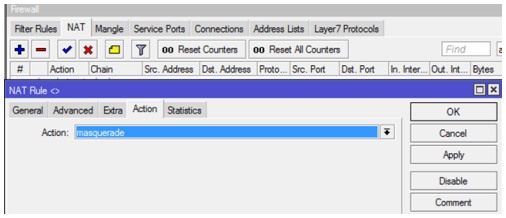


Figura 4.85: Entorno MikroTik para la configuración NAT Firewall masquerade
Elaborado por: El investigador

Se configura un DHCP client para la Interface WAN que accede el servicio a través un modem ADSL con los siguientes parámetros.

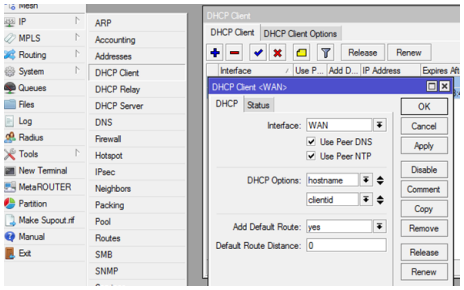


Figura 4.86: Entorno MikroTik para la configuración del DHCP client
Elaborado por: El investigador

Los datos de la red se configuran automáticamente.

Servidor DHCP en la MikroTik

Como siguiente punto se configura un servidor DHCP para la red Inalámbrica a través de asistente de configuración, estableciendo el rango de IPs requeridos para la subred de estudiantes.

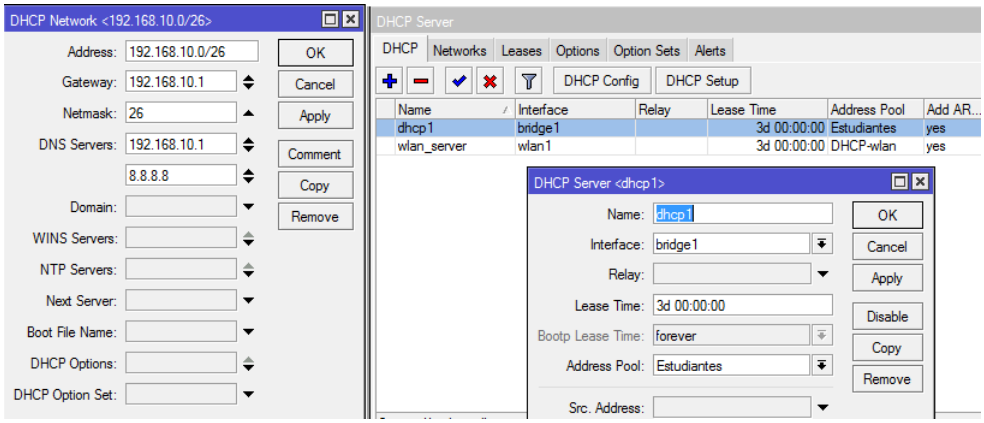


Figura 4.87: Entorno MikroTik para el DHCP server
Elaborado por: El investigador

Repetir el proceso para la subred docentes.

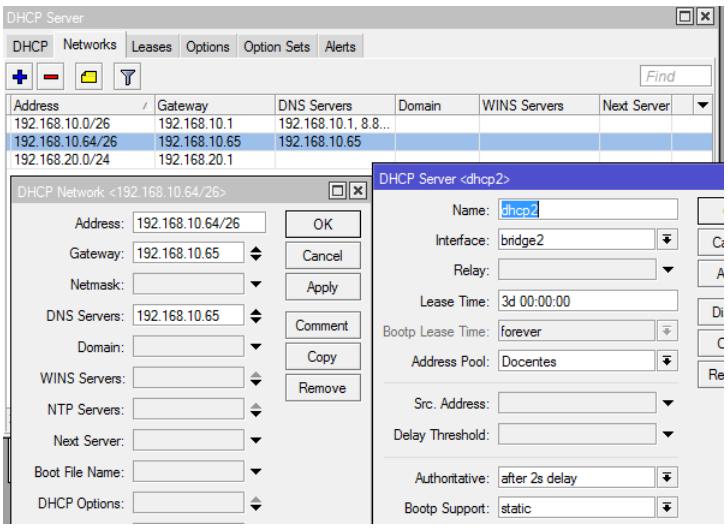


Figura 4.88: Entorno MikroTik para el DHCP server
Elaborado por: El investigador

Es necesario configurar los DNS en el menú IP => DNS

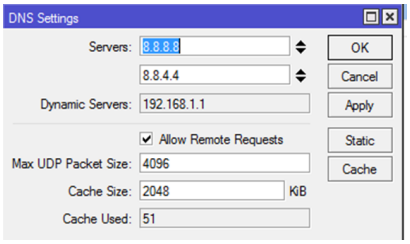


Figura 4.89: Configuración del DNS
Elaborado por: El investigador

En donde se establecen los DNS de google como regla general esto en un futuro se puede modificar de ser necesario.

Configuración del servidor Hotspot el MikroTik

Para empezar ingresar a IP => Hotspot => pestaña Servers => botón Hotspot Setup, para iniciar con el asistente de configuración de Hotspot Server.

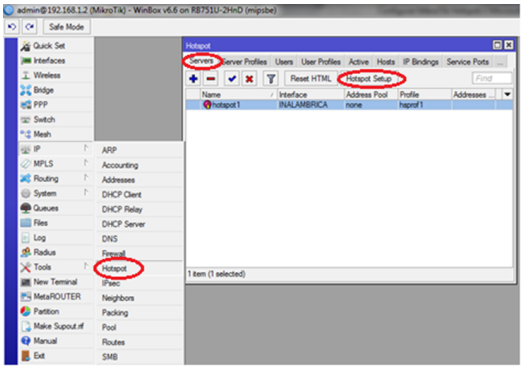


Figura 4.90: Instalación de Hotspot server en MikroTik
Elaborado por: El investigador

La instalación del hotspot es como cualquier instalación tomando en cuantas los parámetros necesarios ya que posee un asistente de ayuda.

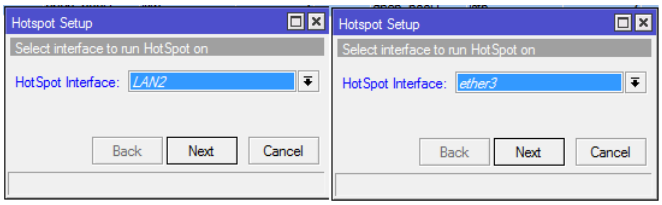


Figura 4.91: Select interface to run hotspot on
Elaborado por: El investigador

Hotspot Interface, se especifica la interfaz donde se configura el Hotspot server,

en este caso se escoge la interface de la red inalámbrica de la interface red LAN ether 2 y ether 3 respectivamente.

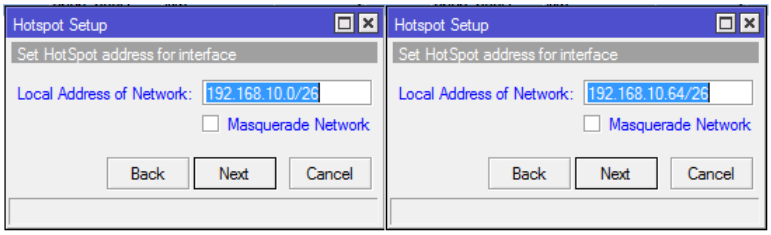


Figura 4.92: Set Hotspot address for interface
Elaborado por: El investigador

Local Address of Network, aparecerá automáticamente la puerta de enlace de los clientes, que en este caso es 192.168.10.1 y la 192.168.10.65; tomado de los datos del IP de ether2 y ether3 que se especificó anteriormente.

Masquerade Network, en este caso desmarcado ya que en un paso anterior se enmascaro todas la interfaces de red.

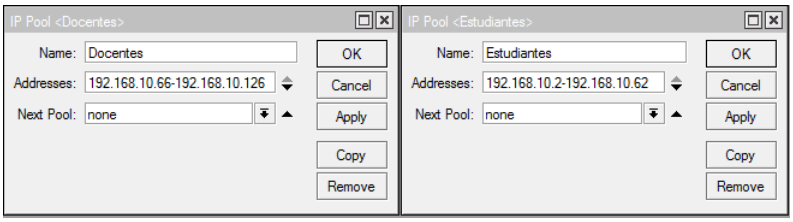


Figura 4.93: Set pool for Hotspot addresses
Elaborado por: El investigador

Address Pool of Network, donde se especifica el rango de IP's que serán asignados a los clientes para que así obtengan un IP automáticamente.

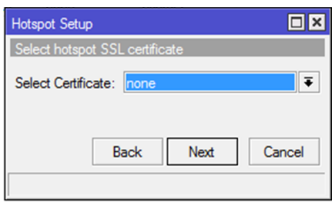


Figura 4.94: Select Hotspot ssl certificate
Elaborado por: El investigador

Select Certificate, se elige **none**, ya que no se cuenta con un certificado SSL. Estos certificados son utilizados para validar una página web cuando se utiliza el protocolo https y así encriptar las conexiones entre el cliente y servidor.

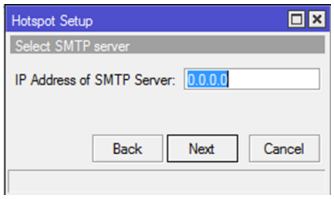


Figura 4.95: Select Hotspot ssl certificate
Elaborado por: El investigador

IP Address of SMTP Server, se lo deja tal como está: 0.0.0.0 ya que no se cuenta con un servidor SMTP (protocolo de transferencia de correo electrónico simple).

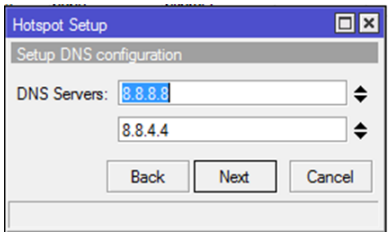


Figura 4.96: Setup DNS configuration
Elaborado por: El investigador

DNS Servers, los dns que se configuró son universales pertenecientes a google por lo que no se necesita ninguna configuración adicional.

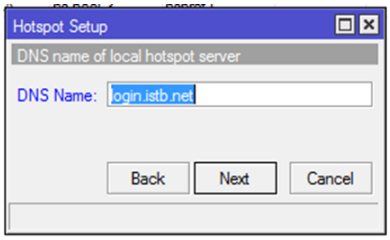


Figura 4.97: DNS name para el hotspot
Elaborado por: El investigador

DNS Name, Aquí se especifica el nombre de dominio al cual se redirigirá el tráfico de la red hacia el hotspot; es decir que al ingresar a una página web por parte de un usuario se re direcciona al portal cautivo para que el cliente se autentique con el nombre de usuario y contraseña, ese portal tendrá dirección **http://login.istb.net/**

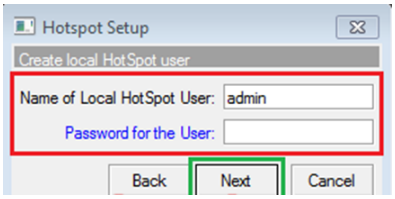


Figura 4.98: Setup DNS configuration
Elaborado por: El investigador

Name of Local Hotspot User, por defecto, el nombre del usuario administrador para el logueo en el hotspot es admin, y se conserva para no tener ningún inconveniente, y con ese nombre se autentica al hotspot por primera vez.

Password for the User, el password de logueo, en este caso el password será andres, hasta que el administrador de la red lo decida cambiar pero es necesario recordarlo.

El servidor hotspot está configurado y listo para ejecutarse como la conexión a la MikroTik era por ip se desconectó y es necesario volver a conectarnos por MAC.

Una vez conectado se ingresa a una página web para verificar el funcionamiento y se tiene el siguiente resultado.

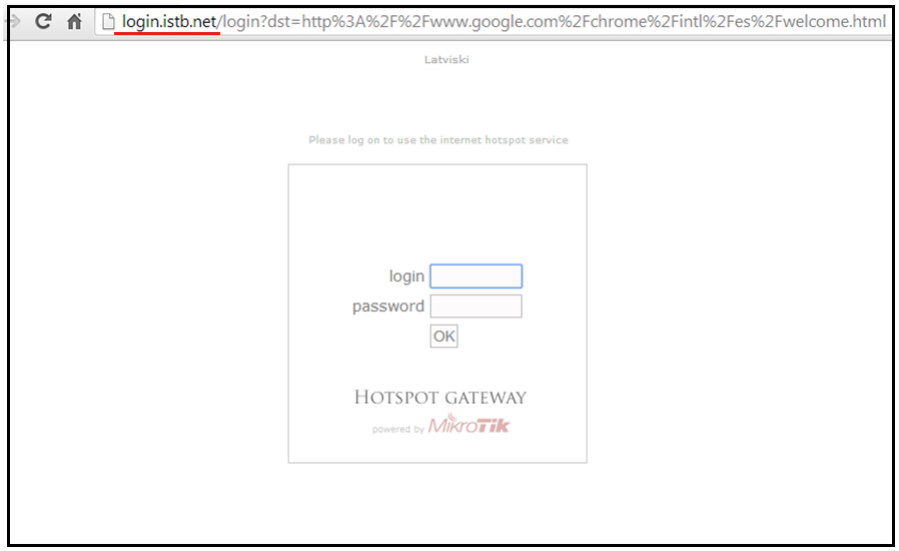


Figura 4.99: Petición de usuario hotspot
Elaborado por: El investigador

En donde se debe ingresar el usuario y la contraseña para poder acceder a todos los servicios de la red.

Una vez que se visualice el portal cautivo, se debe autenticar con el user y password que se configuró en la instalación en este caso el login es **admin** y el password es andres. Una vez autenticado, hotspot dará un mensaje de bienvenida y habrá acceso

a Internet normalmente (sin esta autenticación no hay absolutamente ningún servicio disponible).

Modificaciones finales del Hotspot

Hasta aquí funciona normal pero se debe hacer algunas configuraciones para evitar problemas posteriores.

Empezar la configuración abriendo la regla hotspot1 y así poder editar sus opciones.

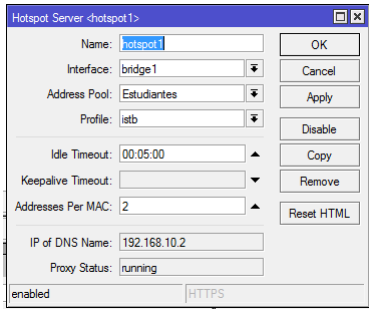


Figura 4.100: Configuración del hotspot server
Elaborado por: El investigador

Name, es el nombre del servidor hotspot.

Interface, es la interfaz de red INALÁMBRICA o ether3.

Address Pool, como se conecta a la nanostation2 inalámbrica se debe especificar como dhcp_pool1 caso contrario none.

Profile, es el perfil de del servidor hotspot mostrado a continuación.

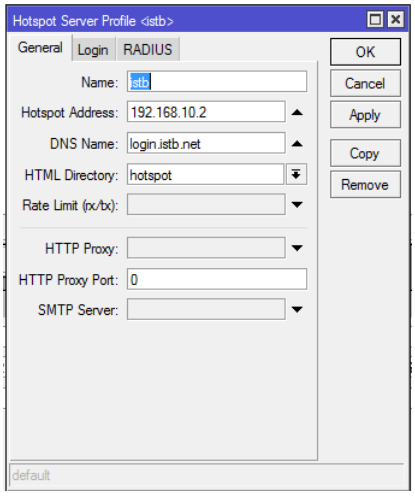


Figura 4.101: Perfil del Hotspot server
Elaborado por: El investigador

Donde se especifica las configuraciones que aplicara el servidor.

Tipo de autenticación.

Existen tres tipos de autenticación principales que son:

1. Escribiendo usuario y clave.
2. Autenticándose por MAC.
3. Siendo un usuario trial (de prueba).

Abrir IP => Hotspot => pestaña Server Profiles y abrir la regla istb => pestaña Login, donde se observa todas las opciones de autenticación.

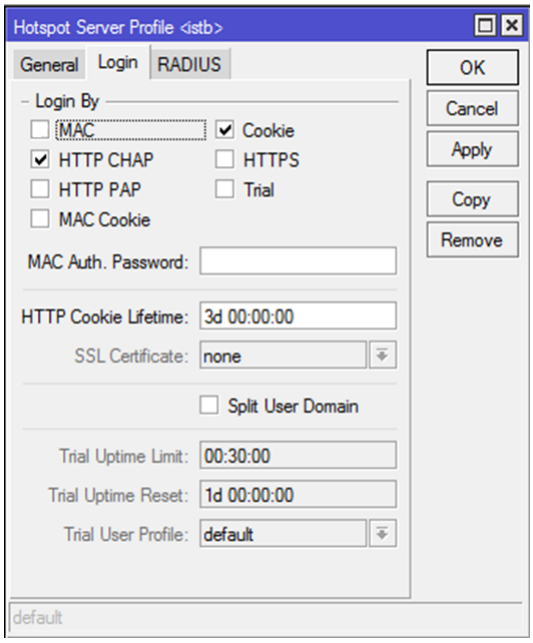


Figura 4.102: Hotspot server Profile
Elaborado por: El investigador

Donde se utiliza la autenticación por usuario evitando así que otros usuarios no autorizados ingresen al servicio de red inalámbrica.

Creación de usuarios para autenticación

Crear cuenta para autenticación por usuario y contraseña.
Ir a IP => Hotspot => Users y abrimos una nueva regla (+)

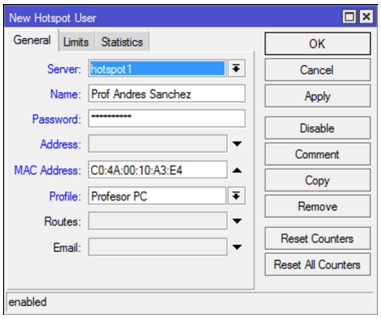


Figura 4.103: New Hotspot User
Elaborado por: El investigador

En donde se especifica los parámetros del usuario este proceso se realizará para el total de usuarios de la red:

Usuario Profesor

- **Name**: Prof Andrés Sánchez
- **Password**: istbandres
- **Address**: Blanco
- **MAC Address:** C0:4A:00:10:A3:E4
- **Profile**: Profesor PC

Usuario Estudiante

- **Name**: Est Juan Pérez
- **Password**: estu_istb1
- **Address**: Blanco
- **MAC Address:** C1:43:10:19:C3:D4
- **Profile:** Estudiante PC

Usuario Autenticado por MAC address

- **Name:** C0:4A:00:10:A3:E4
- **Profile**: Profesor DP

En donde se especifica el usuarios con la MAC address C0:4A:00:10:A3:E4 con el perfil del profesor dispositivo final como se muestra en la imagen.

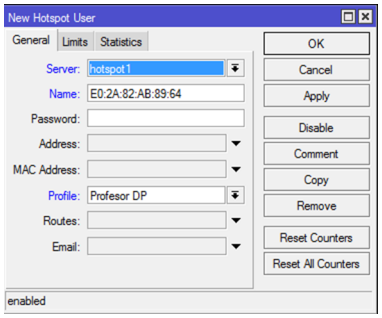


Figura 4.104: New Hotspot user MAC
Elaborado por: El investigador

Este proceso se realiza para todos los usuarios con los diferentes perfiles que se describen a continuación.

Creación de perfiles de usuario

Abrir IP => Hotspot => Users Profiles y crear una nueva regla (+)

Perfil Profesor PC

- **Name:** Profesor PC
- **Address Pool:** hs-pool-3
- **Rate limit (rx/tx):** 512k/1000k
- **MAC cookie timeout:** 3dias

Perfil Profesor DP

- **Name:** Profesor DP
- **Address Pool:** hs-pool-3
- **Rate limit (rx/tx):** 256k/512k
- **MAC cookie timeout:** 1dia

Perfil Estudiante PC

- **Name:** Estudiante PC
- **Address Pool:** hs-pool-3
- **Rate limit (rx/tx):** 256k/512k

- **MAC cookie timeout:** 3dias

Perfil Estudiante DP

- **Name:** Estudiante DP
- **Address Pool:** hs-pool-3
- **Rate limit (rx/tx):** 128k/256k
- **MAC cookie timeout:** 1dia

Perfil Invitado

- **Name:** Invitado
- **Address Pool:** hs-pool-3
- **Sessions timeout:** 00:30:00
- **Rate limit (rx/tx):** 128k/256k
- **MAC cookie timeout:** 02:00:00

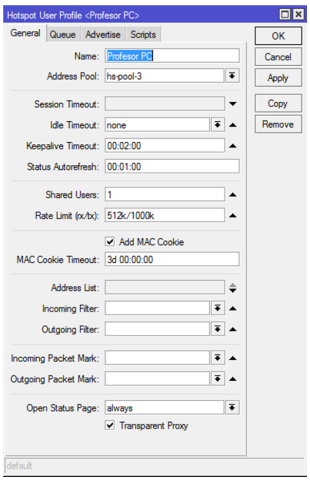


Figura 4.105: Perfil Profesor PC
Elaborado por: El investigador

Estos parámetros se utilizan en la creación de usuarios hotspot concluyendo las configuraciones.

Bloqueo de tráfico P2P en la red Inalámbrica

El tráfico p2p siempre es causal de saturación en redes inalámbricas por lo que a través del Firewall de la MikroTik se negara este tipo de tráfico.

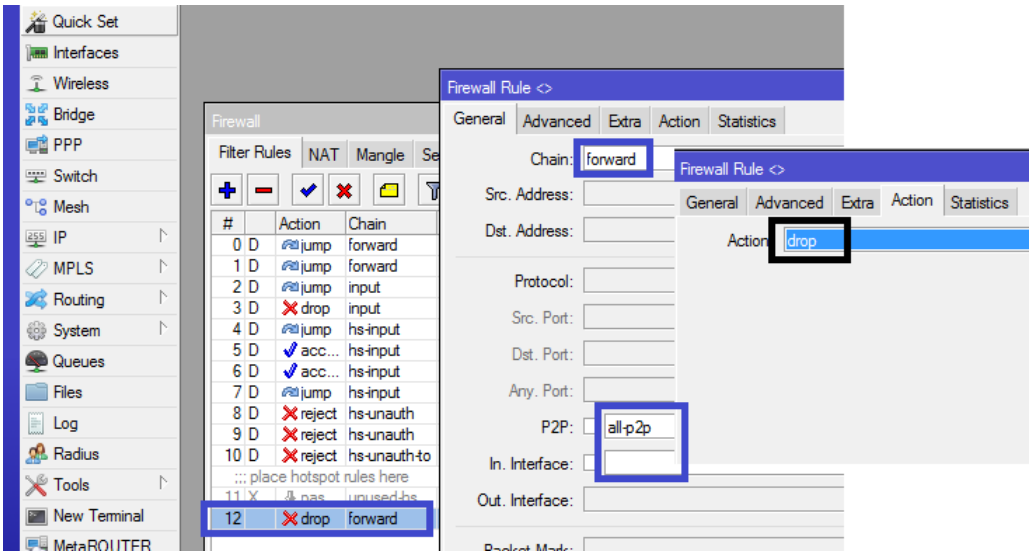


Figura 4.106: Bloqueo de tráfico P2P
Elaborado por: El investigador

El Firewall permite bloquear este tipo de tráfico para la interface ether3 que es la red Inalámbrica de la institución.

4.8.3.6. Instalación y configuración de CACTI

Para poder instalar Cacti en el servidor es necesario seguir los siguientes pasos:

Dependencias de Cacti

Es necesario Instalar las siguientes dependencias necesarias para el buen funcionamiento de cacti.

yum install vim-enhanced net-snmp net-snmp-utils php-snmp initscripts ruby

Instalación RRDTOOL

Para instalar rrdtool se digita el comando:

yum install rrdtool

Instalación y Configuración MySQL y PHP

Cacti requiere de una Base de Datos como MySQL por lo cual se instala.

yum -y install mysql mysql-server

Como también se debe instalar PHP y el conector hacia la Base de Datos MySQL.

yum install php php-mysql php-cli php-common httpd

Iniciar el servidor de MySQL

service mysqld start

Se crea un password al administrador de MySQL.

mysqladmin -u root password andres

Crear la Base de Datos Cacti

Conectarse a la consola de administración de MySQL.

mysql -u root -p

Crear la Base de Datos para cacti.

mysql> create database cacti;

Configurando usuario admincacti con los permisos con su contraseña.

mysql> GRANT ALL PRIVILEGES ON cacti.* TO “admincacti”@”localhost” IDENTIFIED BY “andres”;

Instalación y Configuración la herramienta CACTI

Para poder instalar Cacti hay que agregar un nuevo repositorio llamado dag wieers, de la siguiente manera.

rpm -Uhv http://apt.sw.be/redhat/el5/en/i386/rpmforge/RPMS/rpmforge-release-0.3.6-1.el5.rf.i386.rpm

Instalar la herramienta de monitoreo de redes Cacti

yum install cacti

Crear la estructura de Base Datos Cacti

Para crear toda la estructura de la Base de Datos de Cacti.

mysql -u admincacti -p cacti < /var/www/cacti/cacti.sql

Enter password: andres

Configurar la Conexión a MySQL

Se debe configurar dentro de Cacti el archivo config.php que se encuentra dentro del portal del mismo.

vim /var/www/cacti/include/config.php

Solamente hay que modificar algunos parámetros de la conexión a MySQL.

$database_type = "mysql";
$database_default = "cacti";
$database_hostname = "localhost";
$database_username = "admincacti";
$database_password = "andres";
$database_port = "3306";
Con esto ya se tiene todo configurado en Cacti.

Configuración Apache

Hay que configurar el servidor Apache para que permita visualizar el cacti desde cualquier equipo editando el archivo:

vim /etc/httpd/conf.d/cacti.conf
Dentro de este archivo contiene los siguientes parámetros:
Alias /cacti/ /var/www/cacti/
<Directory /var/www/cacti/>
DirectoryIndex index.php
Options –Indexes
AllowOverride all
order deny,allow
deny from all
allow from 127.0.0.1
AddType application/x-httpd-php .php
php_flag magic_quotes_gpc on
php_flag track_vars on
</Directory>
Aquí es necesario comentar con un # el parámetro deny from all.
#deny from all
Con esto ya existe conexión a Cacti por medio de cualquier equipo de la red local.

Iniciando servicios necesarios Cacti

Reiniciar los servicios necesarios para Cacti.
service httpd restart
service mysqld restart
service crond restart
Para terminar la instalación de Cacti es necesario abrir el navegador favorito y teclear la siguiente url http://localhost/cacti/install o http://192.168.1.201/cacti/install.

Si no tiene acceso es necesario bajar los servicios iptables del servidor con el comando:

#service iptables stop

Post-Instalación Cacti

Para terminar la instalación de Cacti seguir los siguientes pasos:

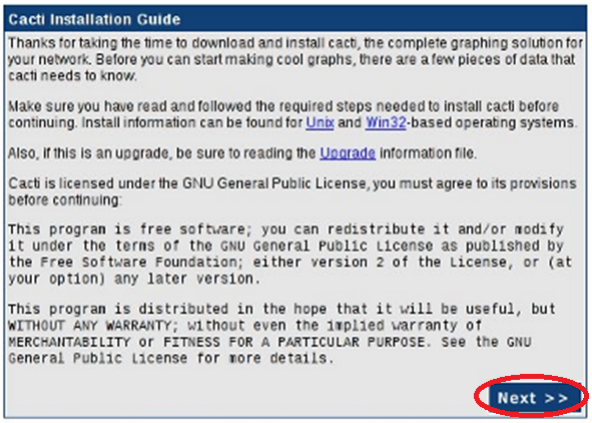


Figura 4.107: Licencia y características de Cacti.
Elaborado por: El investigador

Elegir el tipo de instalación:

- Nueva: Instalación limpia dentro del sistema.

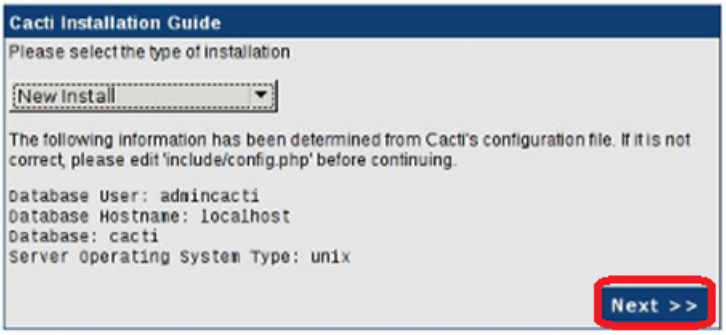


Figura 4.108: Cacti Installation Guide
Elaborado por: El investigador

Donde se especifica el tipo de instalación en este caso una nueva.

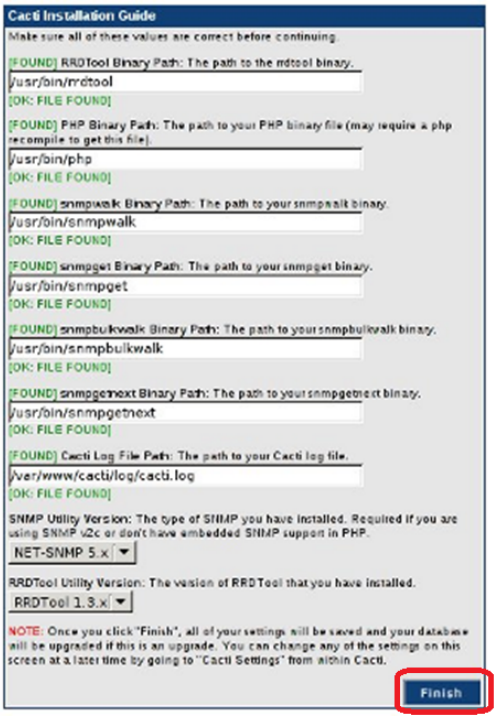


Figura 4.109: Verificando Dependencias de Cacti
Elaborado por: El investigador

Al Terminar este proceso acceder al sitio por default el usuario es admin y contraseña admin.

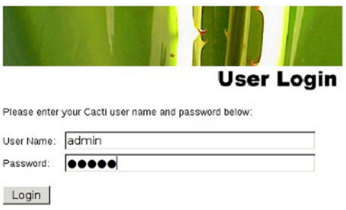


Figura 4.110: Accediendo al aplicación de Cacti.
Elaborado por: El investigador

Al momento de acceder al sitio este indica que es necesario cambiar el password del admin de Cacti, ya que es una contraseña muy débil.

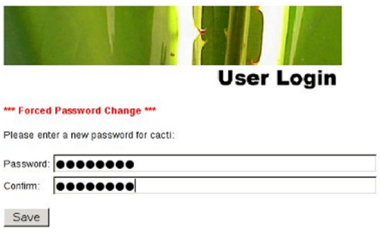


Figura 4.111: Cambiando contraseña del admin en cacti
Elaborado por: El investigador

Analizar Clientes en la red

Para poder analizar a los clientes en la red se requiere que tengan instalado y configurado el SNMP en las máquinas para que Cacti pueda obtener la información de los equipo en tiempo real.

Configurando Cliente

Para agregar clientes y ser analizados, en cacti se puede agregar de la siguiente manera, existe un menú llamado Management el cual tiene la opción de Devices.

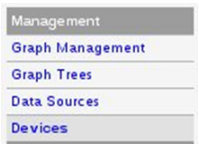


Figura 4.112: Menú de Managent en Cacti
Elaborado por: El investigador

En esta opción muestra los equipos ya configurados por default como localhost, y donde se puede agregar más equipos con la opción Add.

Figura 4.113: Agregando Maquinas a Cacti
Elaborado por: El investigador

Configuración Dispositivo.

En la configuración del dispositivo o server que se desee analizar por medio cacti, se tiene que llenar los siguientes parámetros.

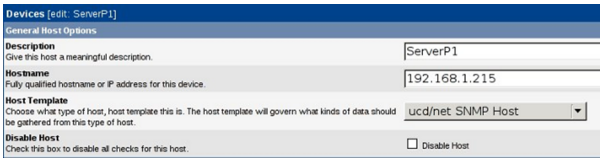


Figura 4.114: Configurando las opciones de Devices del dispositivo o cliente de la red.
Elaborado por: El investigador

Configuración Detectando el dispositivo.

Es necesario configurar el método de detección del dispositivo de la red local que por lo general se lo hace con el comando ping así:

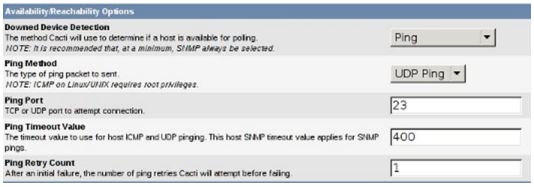


Figura 4.115: Configurando la detección del cliente Cacti.
Elaborado por: El investigador

Configuración SNMP

El tipo de conexión SNMP para conectarse a los clientes SNMP se configura de la siguiente manera.

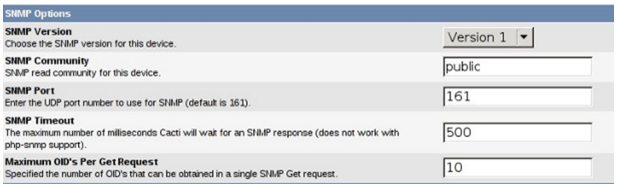


Figura 4.116: Configurando las opciones de conexión con los cliente Cacti.
Elaborado por: El investigador

Templates de gráficas

En esta parte se selecciona los templates de tipo gráficas para algunos servicios o recursos del servidor.

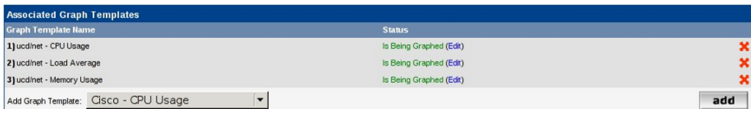


Figura 4.117: Seleccionando gráficas para algunos servicios
Elaborado por: El investigador

Visualizar Clientes.

Para visualizar los clientes que cacti ya tiene registrados hay que ir al menú Management => Device.

Figura 4.118: Visualizando los clientes configurados en cacti
Elaborado por: El investigador

Visualizar reportes.

Para visualizar las gráficas de un cliente, es necesario ir a la pestaña de graphs.

Figura 4.119: Menu de Selección Cacti
Elaborado por: El investigador

Para visualizar las gráficas de los clientes Cacti

Al momento de entrar a los reportes este muestra todas las gráficas que existen en cacti de todos los clientes, donde se selecciona las gráficas necesarias.

Figura 4.120: Opciones adicionales de cacti
Elaborado por: El investigador

Con esto se puede obtener el reporte de un solo cliente y obtener toda la información necesaria por horas, días fechas o intervalos de fechas de la siguiente manera.

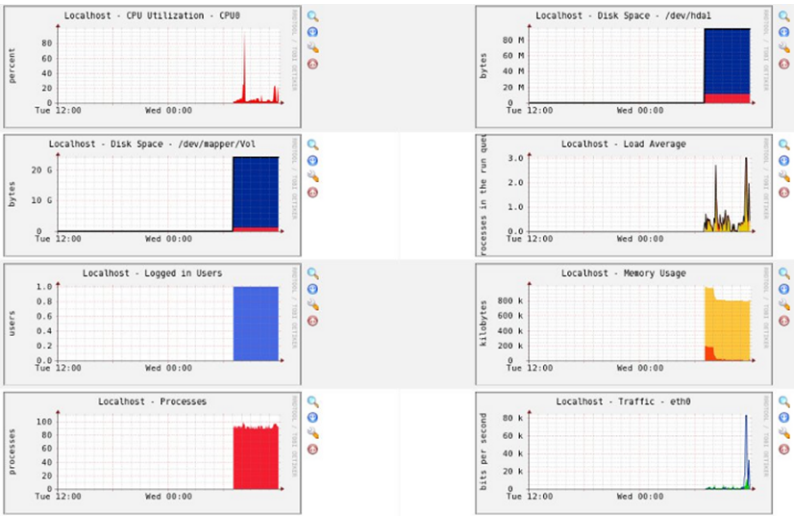


Figura 4.121: Visualizando información de un servidor.
Elaborado por: El investigador

4.9. Pruebas de Funcionamiento

4.9.1. Funcionamiento del servidor PROXY

El servidor Proxy no permite acceder a páginas web de sitios pornográficos, farándula, juegos, series y películas las cuales están restringidos para la red de la institución.

Se conecta un PC al switch, en base al siguiente esquema.

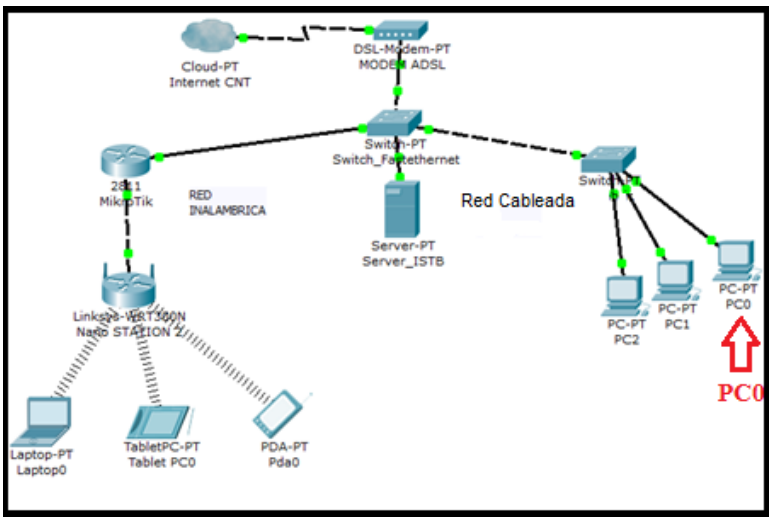


Figura 4.122: Esquema final de la Red LAN institucional
Elaborado por: El investigador

El PC0 adquiere la una IP automáticamente a través del servidor DHCP con las siguientes características.

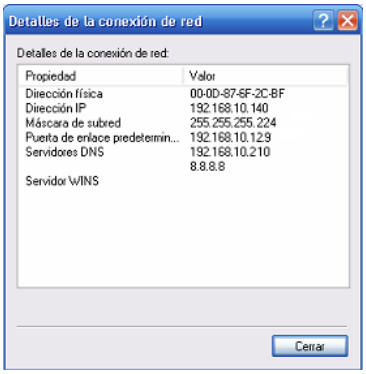


Figura 4.123: Detalles de la conexión a la red PC0
Elaborado por: El investigador

PRUEBA Nº 1

Se ingresa al servidor de búsqueda de google, y se escribe una palabra que este en el archivo de configuración del Proxy obteniendo varios resultados.

Figura 4.124: Imagen del navegador en prueba de Proxy
Elaborado por: El investigador

En este punto se tiene acceso a través del buscador de google, al seleccionar uno de los resultados entra en acción la regla del Proxy que bloquea el acceso como se muestra en la figura:

Figura 4.125: Proxy Bloqueando acceso
Elaborado por: El investigador

En donde se observa que la regla del Proxy que bloquea este tipo de contenido, no permite visualizar los resultados cumpliendo así con la política del uso del servicio de Internet.

PRUEBA Nº 2

Esta conciste en descargar un archivo con la extensión mp3 la cual no es aceptado por el servidor Proxy, al ingresar a la página www.tusmp3.net y se busca una canción.

Figura 4.126: Imagen del navegador en prueba de Proxy Nº 2
Elaborado por: El investigador

Al intentar descargar una canción en formato mp3 se obtiene el siguiente resultado:

Figura 4.127: Proxy Bloqueando descargas de extensions
Elaborado por: El investigador

En donde se observa que el Proxy deniega la descarga cumpliendo con la acl extensions urlpath_regex -i "/etc/squid/listas/extensions" y http_access deny extensions.

4.9.2. Funcionamiento del servidor FIREWALL

El servidor Firewall cumple varias funciones en la red, entre las más importantes permitir el tráfico sobre la red LAN cableada, permitir acceso remoto ssh, enviar el tráfico del puerto 80 hacia el Proxy y bloquear acceso al servidor HTTPs de Facebook, entre otros. Para demostrar el funcionamiento se realiza un intento por acceder a este servidor a través del navegador.

Figura 4.128: Captura del navegador buscando facebook
Elaborado por: El investigador

Como se observa en la imagen el navegador encuentra el servidor de facebook en el cual se procede a ingresar:

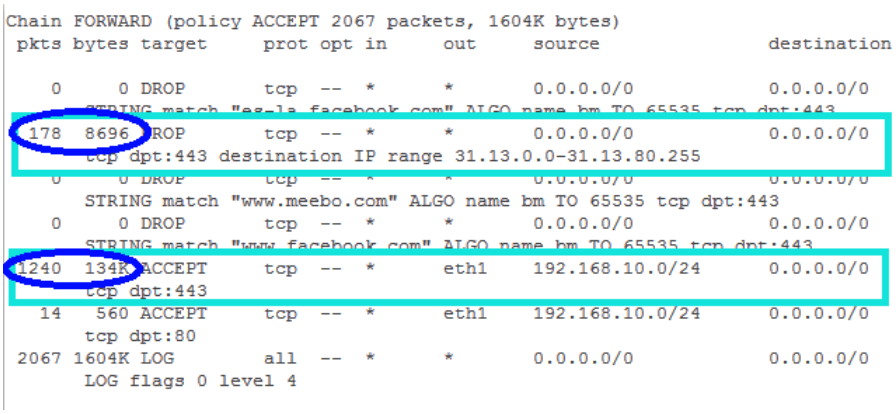


Figura 4.130: Captura del archivo de configuración del Firewall
Elaborado por: El investigador

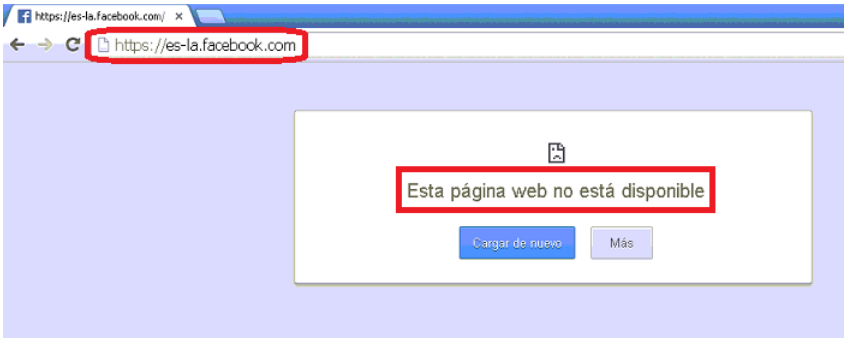


Figura 4.129: Captura del navegador al intentar acceder al servidor de facebook
Elaborado por: El investigador

En donde se observa que no existe acceso a este servidor y se genera tráfico sobre la regla que limita el acceso a este servicio.

En donde se observa que al intentar establecer una conexión con el servidor de facebook se genera tráfico sobre la regla de Firewall que lo bloquea.

4.9.3. Funcionamiento del servidor DNS cache

El servicio DNS se comprueba a través del comando **nslookup** en consola, que obtiene la información utilizada por el servidor dns para resolver páginas web.

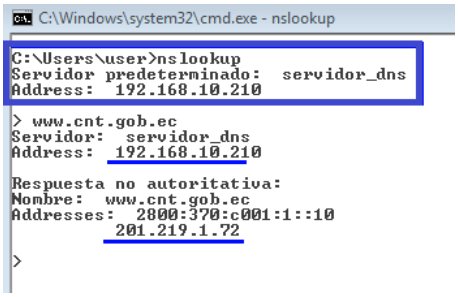


Figura 4.131: Captura de la navegación
Elaborado por: El investigador

Con lo que se comprueba que la dirección IP del servidor DNS es la 192.168.10.210 y esta resolviendo las direcciones web.

4.9.4. Funcionamiento del servidor DHCP

La subred utilizada es la 192.168.10.128/27 y la 192.168.10.160/27 para la red cableada de los 2 laboratorios, el acceso a la red LAN se debe obtener una ip automáticamente a través de este servidor.

imagen

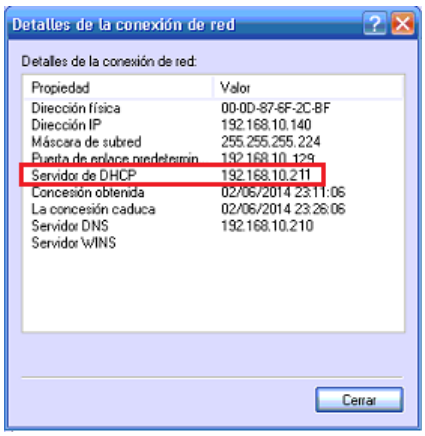


Figura 4.132: Captura de los detalles de la conexión a la red institucional
Elaborado por: El investigador

Para la red inalámbrica se utiliza la red 192.168.10.0/26 para estudiantes y la 192.168.10.64/26 para docentes que imparte el servidor DHCP de la MikroTik automáticamente.

4.9.5. Funcionamiento del Hotspot en MikroTik

Para demostrar el funcionamiento del servidor hotspot se accede a la red mediante un host y se verifica la autenticación de usuario.

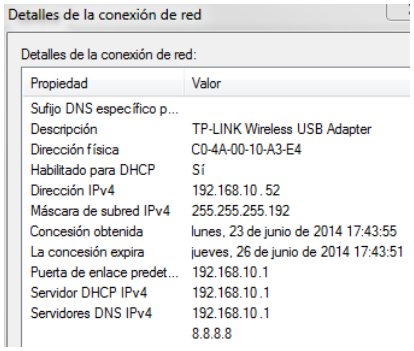
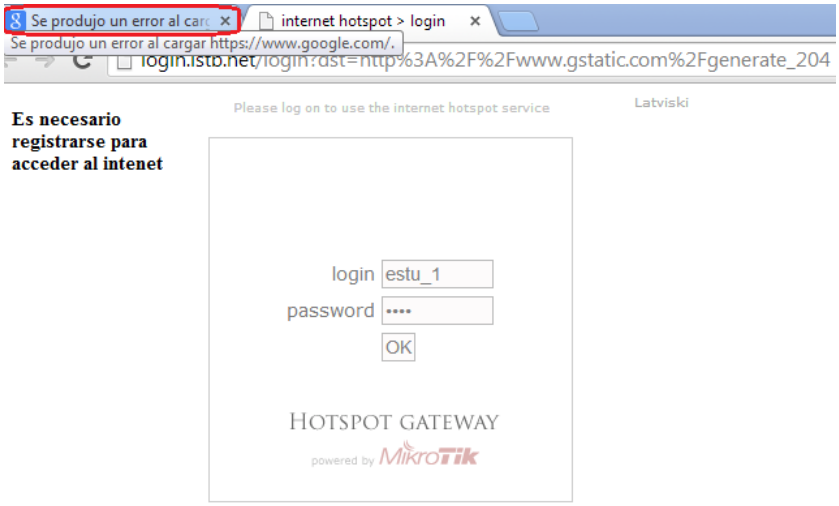


Figura 4.133: Captura de los detalles de la conexión a la red institucional Inalámbrica
Elaborado por: El investigador



Al ingresar el nombre de usuario y contraseña se tiene acceso así:

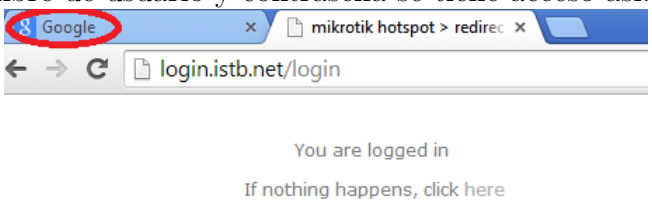


Figura 4.134: Accediendo a la red inalámbrica hotspot
Elaborado por: El investigador

Como se muestra en la imagen al ingresar ya como un usuario del hotspot, se tiene acceso al Internet.

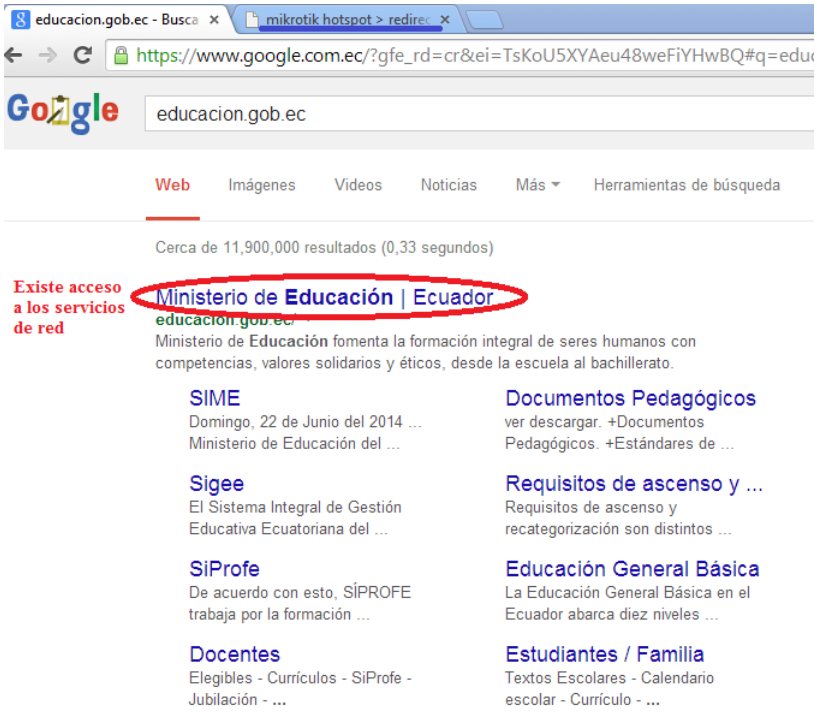


Figura 4.135: Acceso a la red inalámbrica a través del Hotspot
Elaborado por: El investigador

Ya con el acceso a los servicio de red se procede a verificar el funcionamiento de la regla del Firewall para bloquear el tráfico P2P en la red Inalámbrica:

Prueba del bloqueo P2P

Para esta prueba se utiliza cualquier software que genere tráfico P2P desde un host de la red inalámbrica de la siguiente manera:

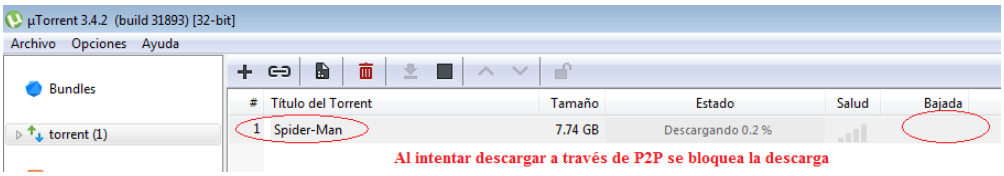


Figura 4.136: Generar tráfico P2P para prueba de funcionamiento
Elaborado por: El investigador

Luego se visualiza a través de winbox la regla que bloquea p2p.

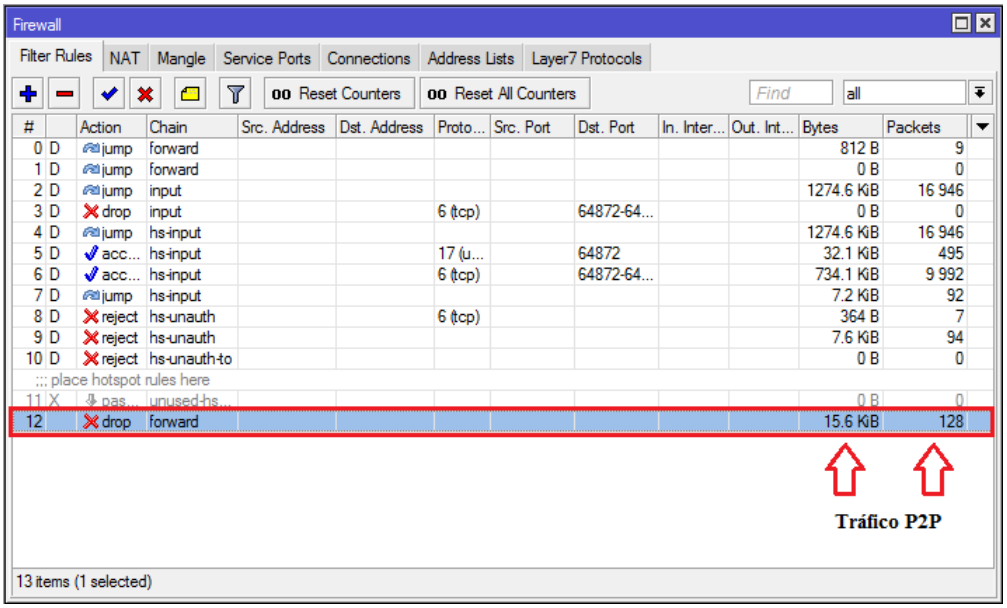


Figura 4.137: Bloqueo del tráfico P2P
Elaborado por: El investigador

En donde se observa que al general tráfico P2P desde un host de la red, este genera tráfico sobre la regla que lo bloquea.

4.9.6. Pruebas del monitoreo a través de CACTI

En este servidor se utiliza para visualizar el estado de los dispositivos de la red.

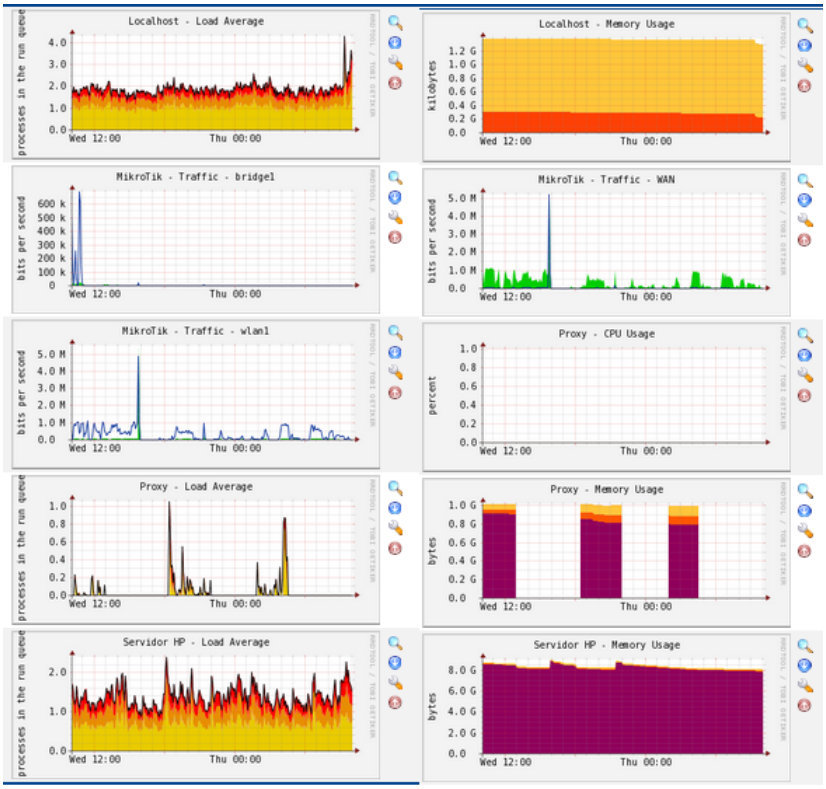


Figura 4.138: Resultado de Cacti 1
Elaborado por: El investigador

En donde se observa las gráficas generadas por los servidores y dispositivos de Red.

CAPÍTULO 5

Conclusiones y Recomendaciones

CONCLUSIONES

- El ancho de banda disponible no cubre las necesidades mínimas de la red institucional.
- La virtualización ha permitido aislar servicios de red proporcionando independencia al funcionamiento.
- Al aplicar el concepto de RAID 1 se posee alta disponibilidad de los servicios instalados y de la información.
- La implementación de nuevos esquemas han contribuido al crecimiento de la red institucional, lo que ha optimizado notablemente el desempeño de la red LAN.
- Al aplicar el concepto de Proxy transparente se ayuda a minimizar el tiempo de configuración de los host pertenecientes a la red LAN cableada, lo que ofrece un acceso más dinámico y controlado.
- El monitoreo a través de la herramienta cacti ofrece facilidad para la toma de decisiones sobre toda la red LAN institucional.

RECOMENDACIONES

- Aumentar el ancho de banda a 8 MB para cubrir las necesidades mínimas requeridas.
- Crear usuarios con autenticación individual para evitar posibles problemas en la red que ocasionaría conflicto en el funcionamiento de la misma.
- Vigilar constantemente los servicios a través de la herramienta cacti sobre el estado de la red institucional, para tomar decisiones administrativas a tiempo.
- Proporcionar el servicio de Internet a usuarios temporales con la debida autorización, limitando el mismo al darle un usuario con el perfil de invitado.
- Chequear regularmente los equipos institucionales para verificar que se cumplan con el reglamento del uso de las NTIC.

Bibliografia

[1] Crhistian Guerrero “evaluación de sistemas de gestión bajo software libre de la administración zonal norte Eugenio Espejo”. Universidad Politecnica Salesiana. [online]. Quito, julio 2011 Disponible en: http://dspace.ups.edu.ec/handle/123456789/1678

[2] José Iván Freire Bonilla “herramienta opensource de administración y monitoreo basado en SNMP para el mejoramiento del funcionamiento de la red en Speddy COM. CIA. LTDA.”. UNIVERSIDAD TÉCNICA DE AMBATO [En línea]. Biblioteca Facultad de Ingenieria en Sistemas, Electronica e Industrial, abril del 2013 Sección Tesis Numero t802ec.

[3] José A. Domínguez “Introducción a la Gestión de Redes” Universidad de Oregón 2007. Disponible en: http://lacnic.net/documentos/lacnicx/Intro_Gestion_Redes.pdf

[4] Fundación Universitaria Iberoamericana, “Gestión de Redes” Publicado en: 2013 Disponible en: http://www.funiber.org/areas-de-conocimiento/tecnologias-de-la-informacion/gestion-de-redes/

[5] Elizabeth Andrea Catata Nina, Claudio Cesar Gonzáles Mamani , Nereida Celina Llerena Valdivia “Proyecto de Investigación – Gestión de Redes - Autodema” Arequipa Agosto del 2008 Publicado por: Universidad Católica de San Pablo, Marzo del 2010.

[6] J Manuel Huidobro “SNMP, Un Protocolo Simple de Gestión” Revista BIT de las Tecnologías de la información Autor Ingeniero Superior de Telecomunicaciones y Responsable del Centro de Información al Cliente en Ericsson Comunicaciones de Empresa, Marzo-Abril de 1997 disponible en: http://www.coit.es/publicac/publbit/bit102/quees.htm

[7] Ing. Rosales Briceño Caryuly “PROTOCOLO SNMP” Universidad Rafael Belloso Chacín. Publicado el 2004. Disponible en: http://www.publicaciones.urbe.edu-/index.php/telematique/article/viewArticle/782/1886.

[8] Craig Zacker ; Capítulo 31: Herramientas de administracion de red y de solucion de problemas; REDES; McGraw-Hill/Interamericana; 2002; Aravaca (Madrid);

#pag.970

[9] Margaret Rouse “OpenFlow” publicado en Noviembre del 2012 Disponible en: http://searchdatacenter.techtarget.com/es/definicion/OpenFlow

[10] Jesús Sánchez Allende, Joaquín López Lérida; Capítulo 8: Gestion de Red y Seguridad; REDES; McGraw-Hill/Interamericana; 2004; España; #pag.203

[11]APC (Asociación para el Progreso de las Comunidades), “Software Propietario”, 2013 disponible en: http://www.apc.org/es/glossary/term/241

[12] Traducción: Luis Miguel Arteaga Mejía, 2001. Revisiones: Hernán Giovagnoli. “¿QUE ES SOFTWARE LIBRE?” Última actualización: $Date: 2013/08/31 20:12:01 disponible en http://www.gnu.org/philosophy/free-sw.es.html

[13] Cristian G “CALIDAD DE SERVICIO (QOS)” publicado el primero de abril del 2013 y disponible en: http://www.uv.es/~montanan/ampliacion/ampli_6.pdf

[14] William Stallings; Capítulo 13: Congestion en Redes de Datos; Comunicaciones y Redes de Computadores; Persons Educación S.A.; 2004; Madrid (España); #pag.417

[15] Mario Enrique Cedeño Toledo, “COMPUGAMER abinete - Rack cerrado de pared, Connection 6UR” Disponible en: http://www.compugamer.com.ec/v3/gabinete-rack-cerrado-de-pared-connection-6ur-30-profundidad.html

[16] Pagina Oficial de HP, “HP ProLiant ML150 G6 E5504”, publicado en el 2009. Disponible en: http://www.hp.com/latam/catalogo/co/ml100_smb/sp/466132-001.html

[17] HOWTOFORGE Linux tutorials “Virtualization With KVM On A CentOS 6.4 Server” 2013-04-16 13:54 Disponible en: http://www.howtoforge.com/virtualization-with-kvm-on-a-centos-6.4-server

[18] Hosting CHILE “Como instalar KVM en CentOS 6” Publicado el Martes 24 de Octubre del 2011. Disponible en: http://tutoriales-cpanel.blogspot.com/2011/10/como-instalar-kvm-en-centos-6.html

[19] nytros, “How to configure Software RAID1 with CentOS 6.x” Noviembre 24 del 2012. Disponible en: http://infoliser.com/how-to-configure-software-raid1-with-centos-6-x/

[20] Joel Barrios Dueñas, “Configuración de Squid: Opciones básicas” Publicado el 13/12/2013, 23:48. Disponible en: http://www.alcancelibre.org/staticpages/index-.php/19-0-como-squid-general

[21] Pello Xabier Altadill Izura, Ingeniero en Informática por la UPV−EHU Seguridad de IBERCOM, “IPTABLES”, disponible en: http://es.tldp.org/Manuales-LuCAS/doc-iptables-firewall/doc-iptables-firewall.pdf

[22] Bluder Garcia, “Firewall e IPTables”, Publicado en el 2009. Disponible en: http://bluder10.blogspot.com/2009/03/firewall-e-iptables.html

[23]TurismoTour.com, Julio “Que son los servidores DNS”, publicado el Viernes, 3 de junio de 2011 a las 06:56. Disponible en: http://www.turismotour.com/ %C2 %BF-que-son-los-servidores-dns/

[24] intef (Instituto Nacional de Tecnologías Educativas y Formación del Profesorado), “Servidor DNS y DHCP sencillo con DNSMASQ” Disponible en: http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m2/servidor_dns ___dhcp_sencillo_con_dnsmasq.html

[25] Ernesto Ariganelo y Enrique Barrientos Sevilla; Capítulo 5: DHCP; REDES CISCO. CCPN a Fondo; RA-MA Editorial; 2010; Madrid - España; #pags.195-200

[26] Margaret Rouse, “DHCP (Dynamic Host Configuration Protocol)”, publicado en Marzo del 2008. Disponible en: http://searchunifiedcommunications.techtarget-.com/definition/DHCP.

[27] Julio Gómez López; Capítulo 10: Hostpot; Redes Wifi, Guía de Campo de WIFI; RA-MA Editorial; 2008; Madrid (España); #pag.219

[28] MikroTik routerboard “RB751U-2HnD” Publicado el . Disponible en: http://routerboard.com/RB751U-2HnD

[29] TechSource, “5 Aplicaciones Libres para Monitoreo de Redes y Servidores”, publicado el jueves 16 de Diciembre del 2012. Disponible en: http://fraterneo.blogs-pot.com/2010/12/5-aplicaciones-libres-para-monitoreo-de.html

[30] The cacti group “About Cacti”, Publicado en el 2014. Disponible en: http://www.cacti.net/ y JJ Velasco, Bitelia “Monitoriza el estado de tu red con Cacti”, Publicado el 24 de septiembre del 2010. Disponible en: http://bitelia.com/2010/09/monitoriza-el-estado-de-tu-red-con-cacti

Anexos y Apéndices

Anexo A

Reglamento del Uso de las NTIC's

El disponer de un reglamento permite a la intitución crear normas para el uso del equipo informático por lo que se plantea un modelo aplicable a la institución.

UNIDAD EDUCATIVA BAÑOS

RECTORÍA

"Por la cual se establece el Reglamento de Usuarios de las Aulas de Informática de la Institución Educativa"

El rector (e) de la UNIDAD EDUCATIVA BAÑOS, en uso de sus atribuciones estatutarias,

RESUELVE

ARTICULO ÚNICO. - Establecer el Reglamento de Usuarios de las Aulas de Informática de la Institución Educativa así:

Capítulo I. Usuarios y servicios de las Aulas de Informática

Artículo 1. Se consideran Aulas de Informática todos los espacios físicos y recursos de Hardware, software y conectividad que la Institución Educativa ofrece como apoyo a las actividades de enseñanza/aprendizaje.

Artículo 2. Se consideran cuatro tipos de posibles usuarios de las Aulas de Informática a) estudiantes que se encuentren debidamente matriculados; b) profesores, coordinadores y directivos; c) empleados de la institución cuya vinculación con la IE se encuentre vigente; d) padres de familia y vecinos de la Institución Educativa; y e) usuarios del aula diferentes a los anteriores (capacitaciones específicas, cursos de educación continuada, usuarios individuales, etc). Los usuarios tipo c deben contar con autorización de la rectoría para hacer uso

de las Aulas de Informática. Los usuarios tipo d y e solo podrán hacer uso de las Aulas de Informática en los horarios establecidos por la Institución Educativa.

Artículo 3. La institución ofrecerá a los usuarios de las Aulas de Informática los recursos de Hardware, software y conectividad disponibles, para que sirvan como apoyo en sus actividades académicas. El uso académico prima sobre cualquier otra utilización.

Artículo 4. La administración de los recursos de las Aulas de Informática es responsabilidad del Departamento de Informática de la Institución Educativa. Las Aulas de Informática deben estar en todo momento bajo la responsabilidad del Coordinador Informático, o de un docente de informática, o de un docente de área o del monitor del Aula.

Artículo 5. La utilización por parte de los usuarios de las Aulas de Informática se hará de acuerdo con las condiciones establecidas en el presente reglamento.

Capítulo II. Normas básicas para la utilización de las Aulas de Informática

Artículo 6. Los usuarios únicamente pueden utilizar los servicios para los cuales están autorizados. Sin la debida autorización, no se permite tener acceso directo a los servidores de las salas, copiar software o modificar los archivos que se encuentren allí. Para el uso de servicios especiales como sacar impresiones, grabar un CD/DVD o utilizar el escáner, se debe solicitar permiso al monitor o al docente responsable de la sala.

Artículo 7. Bajo ninguna circunstancia se podrá utilizar el nombre (login), código o clave de acceso (password) de otro usuario. Cada usuario debe permitir su plena identificación en la Red de la Institución.

Artículo 8. Los usuarios de los recursos de las Aulas de Informática, deben tener presente que sus acciones pueden afectar a la institución y a otros usuarios. Un usuario no podrá interferir en los procesos computacionales de la Institución con acciones deliberadas que puedan afectar el desempeño y seguridad de los recursos informáticos o de la información.

Artículo 9. Las clases que requieran el uso permanente de un Aula de Informática durante todo el año lectivo, serán solicitadas directamente por el jefe de departamento o por el coordinador académico y se asignarán en el orden riguroso a la recepción de dicha solicitud, dando prelación a las asignaturas en las que se trabaja con integración de las TIC.

Artículo 10. El uso de las Aulas de Informática y de los servicios de Red serán para fines exclusivamente académicos. Está prohibido usar los equipos de las Aulas

y los servicios de Red para jugar, enviar o recibir información pornográfica o de propósito netamente comercial. Por comodidad de los usuarios, sólo se permite el uso simultáneo de un computador a un máximo de dos (2) personas.

Artículo 11. El horario de servicio será establecido y dado a conocer a todos los usuarios por el Departamento de Informática. La utilización de los recursos de las Aulas de Informática en horario diferente al escolar debe estar debidamente autorizadas por el personal administrativo de la Institución Educativa.

Artículo 12. En caso de pérdida, daño o deterioro de los equipos usados, el usuario debe reportar inmediatamente esta situación al monitor de la Sala para proceder a su reparación. Si se determina que el daño fue causado por mal manejo o maltrato del equipo, el usuario responsable debe encargarse de la reparación del mismo.

Capítulo III. De los deberes y derechos de los usuarios

Artículo 13. Son deberes de los usuarios:

1. Hacer reserva de los equipos o de las salas con la debida anticipación, de conformidad con las políticas establecidas por la Institución. La asignación de equipos se ajustará a la disponibilidad de equipos y a la atención de los usos prioritarios de las Aulas.

2. Reservar equipos de las Aulas de Informática para trabajo individual. Un usuario podrá reservar un máximo de 2 horas a la semana para trabajo individual. Este tipo de reserva solo podrá hacerse para realizar trabajos académicos o relacionados con la Institución Educativa.

3. El docente o responsable de una clase no debe abandonar en ningún momento el Aula de Informática sin dar aviso previo al encargado o monitor de la misma. Si el profesor no va a estar presente durante la clase en el Aula debe especificarlo en el momento de reservarla.

4. En caso de requerir algún software especial, el profesor debe solicitar su instalación con la debida anticipación indicando en cuántos y en cuáles equipos del Aula de Informática se requiere.

5. Cumplir puntualmente con los horarios de servicio establecidos para trabajar en las Aulas de Informática.

6. Cuidar los recursos de Hardware y software así como los muebles y demás materiales que se encuentran disponibles para su uso en las Aulas de Informática.

7. Informar inmediatamente al encargado de la sala sobre cualquier irregularidad en el funcionamiento del equipo asignado (Hardware, software o conectividad).

8. Acatar las instrucciones y procedimientos especiales establecidos por la Institución para hacer uso de los recursos de las Aulas de Informática.

9. Abstenerse de fumar y consumir alimentos y/o bebidas al interior de las Aulas de Informática.

10. Mantener la disciplina y no interferir con el trabajo de los demás usuarios de las Aulas de Informática.

11. Los usuarios tipo a (estudiantes) que requieran salir del Aula durante la clase, deberán solicitar autorización al profesor que esté a cargo en ese momento.

12. Procurar el debido orden, limpieza y cuidado de los equipos al terminar el uso, esto incluye apagar los equipos adecuadamente y dejar el puesto de trabajo limpio y ordenado.

13. En caso de práctica de grupo, el profesor debe responder por el cuidado general y el buen manejo de la sala y sus equipos durante la clase.

14. Almacenar correctamente su información y hacerlo únicamente en las carpetas destinadas para ese fin.

15. Cuidar sus objetos personales, ya que los encargados de las Aulas de informática no se responsabilizan por la pérdida de los mismos.

Artículo 14. Son derechos de los usuarios:

1. Recibir tratamiento respetuoso por parte del personal a cargo del Aula de Informática.

2. Recibir asistencia técnica en cuanto a Hardware, software y conectividad se refiera, de acuerdo con las disposiciones definidas por la Institución.

3. Disponer de equipos en pleno funcionamiento en las Aulas de Informática.

4. Hacer uso del Hardware, software y conectividad que se le haya asignado durante la totalidad del tiempo que se le haya acordado.

Capítulo V. Sanciones

Artículo 15. La Institución UNIDAD EDUCATIVA BAÑOS podrá imponer a los usuarios que incurran en algunas de las acciones enumeradas en el Artículo 16 del presente reglamento, las siguientes sanciones:

1. Amonestación verbal. Será impuesta por el encargado de la Sala de Informática, dependiendo de la gravedad de la falta.

2. Amonestación escrita. La harán los Coordinadores Académicos o de Disciplina mediante comunicación escrita, de la cual quedará copia en la hoja de vida del usuario.

3. Suspensión de clases por uno o más días a usuarios en calidad de estudiantes. La impondrá el Rector a solicitud del Coordinador Académico o de Disciplina.

4. Matrícula condicional a usuarios en calidad de estudiantes. La impondrá el Rector, dependiendo de la gravedad de la falta.

5. Cancelación temporal. Será impuesta a los usuarios tipo d y e (Artículo 2) por el encargado de las Aulas de Informática, dependiendo de la gravedad de la falta.

Artículo 17. El procedimiento para la aplicación de las sanciones mencionadas a los estudiantes, se regirá por el Manual de Convivencia de la Institución.

Artículo 18. Cualquier situación no prevista en el presente reglamento, la resolverá el Rector de acuerdo con el Manual de Convivencia de la Institución.

Anexo B

Proveedores de Internet (ISP)

La investigación determinó que el ancho de banda mínimo necesario para la red de la institución es de 8 MB por lo que se analiza las tarifas de diferentes ISPs.

Proveedores de Internet	Descripción del Servicio	Medio de Transmisión	Velocidad de subida/bajada	Costo Mensual	Costo de Instalación
CNT	**Plan PYMES Asimétrico (Compartido 2 a 1)**	**Fibra Óptica**	**Hasta 15 x 7 Mbps**	**200 USD**	**380 USD**
Claro	PYMES PACK 9000 (4 a 1)	Depende de localización	9024 Kbps Simétricos	135 USD	Depende de Localización
Speedy	Gold 3 Megas Compartido 2 a 1	Depende de localización	Hasta 3 x 3 Mbps	420 USD	Depende de Localización
@NET	8 megas Dedicado	Inalámbrico vía Radio	8x8 Mbps	800 USD	50 USD

Los precios establecidos en los planes de internet los precios están sujetos al IVA en una 12% por lo cual se considera que CNT tiene el plan PYMES asimétrico que cumple con los requerimientos de la red.

Anexo C

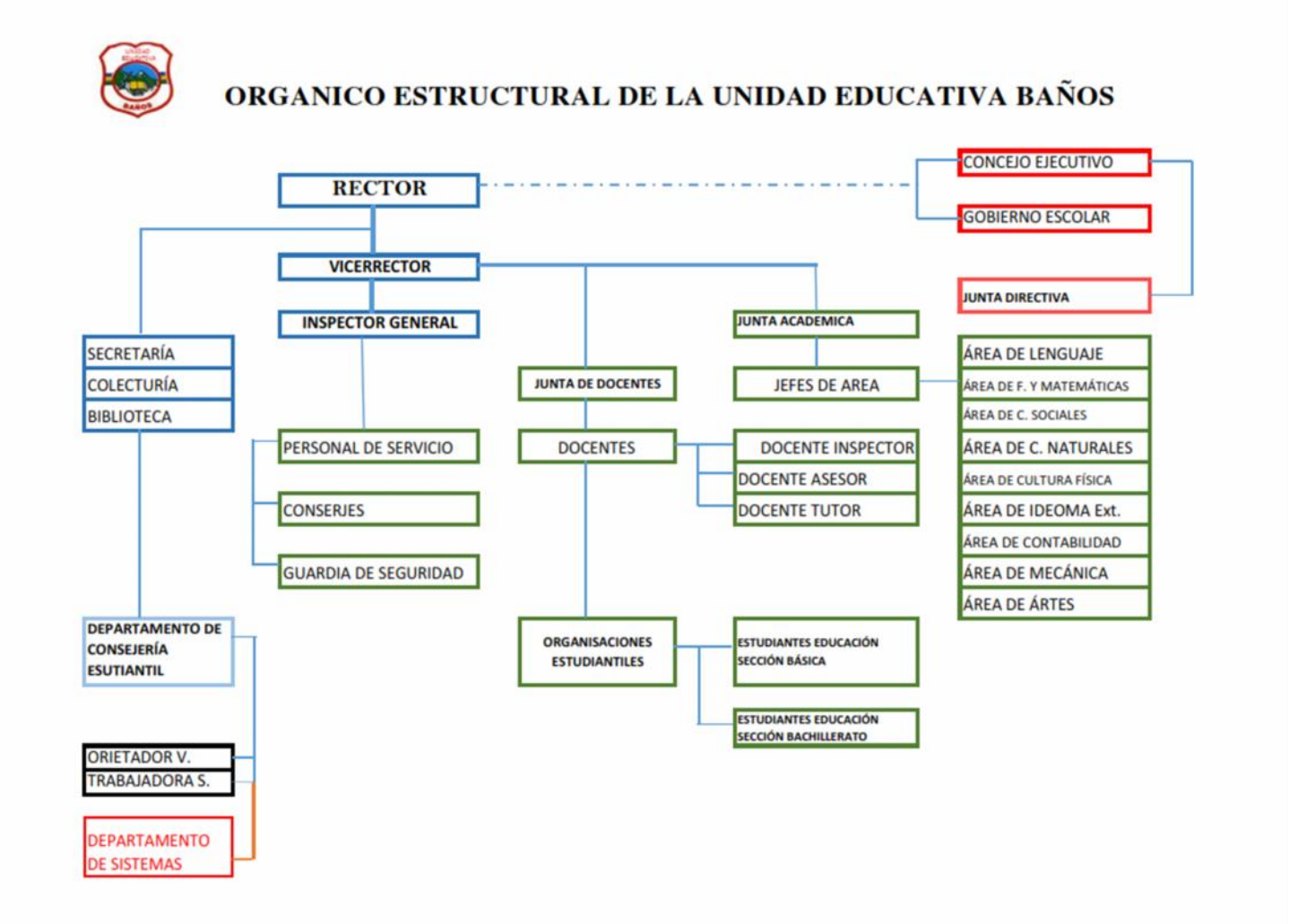
Partida Presupuestal

N	Descripción	Unidad	Cantidad	Valor Unitario ($)	Valor del Rubro ($)
1	Resmas de hojas	c/u	4	4.5	18
2	Carga de tinta B/N	c/u	2	12	24
3	Cartucho color	c/u	3	12	36
4	Anillados	c/u	6	2.0	12
5	DVD-R	c/u	5	0.5	2.50
6	Transporte	c/u	60	1.48	88.80
7	Disco Duro externo	c/u	1	100	100
8	Armario de Comunicaciones RACK	c/u	1	180	180
9	Patch Panel 24 Puertos Cat 5e	c/u	1	80	80
10	Patch Core Cat 5e	c/u	5	2.0	10
11	Herramienta Ponchadora	c/u	1	15	15
		Subtotal, USD $			475
		Imprevistos (5%), USD $			23.75
		TOTAL, USD $			498.75

El costo del proyecto de investigación fue cubierto por el investigador con los parámetros descritos en el presupuesto.

Anexo D

ORGANIGRAMA INSTITUCIONAL



Anexo E

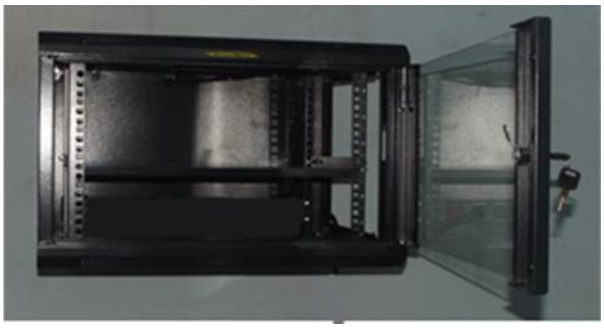
INSTALACIÓN DEL ARMARIO DE COMUNICACIONES

Para la instalación se necesita los siguientes elementos:

- Rack 6U
- Patch Panel 24 Puertos Cat 5e
- Patch Cord Cat 5e
- Herramienta Ponchadora
- Crimpadora
- Tester cable de red
- Cable UTP Cat 5e
- Conectores RJ45
- Regleta de enchufes para Rack

Procedimiento:

1. Montaje del Rack en la pared



2. Colocar la regleta de enchufes

3. Colocar los equipos de red

4. Montaje del Patch Panel y Patch Cord

5. Presentación Final