UNIVERSIDAD NACIONAL DE LOJA

Área de la Energía, las Industrias y los Recursos Naturales No Renovables

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y TELECOMUNICACIONES

Título:

"ANÁLISIS DEL REQUERIMIENTO DE UN SEGMENTADOR DE ANCHO DE BANDA PARA LA RED LAN DE LA UNIVERSIDAD NACIONAL DE LOJA E IMPLEMENTACIÓN EN EL ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES"

"TESIS PREVIA A LA OBTENCIÓN DEL TÍTULO EN INGENIERA EN ELECTRÓNICA Y TELECOMUNICACIONES"

Autora:
EVELIN GABRIELA ALVARADO OTERO

Director de Tesis:
Ing. Juan Pablo Cabrera Samaniego, M.Sc.

LOJA – ECUADOR

2013

CERTIFICACIÓN

Ing. Juan Pablo Cabrera Samaniego, M.Sc.

DIRECTOR DE TESIS

Haber dirigido, asesorado, revisado y corregido el presente trabajo de tesis de grado, en su proceso de investigación cuyo tema versa en **"Análisis del Requerimiento de un Segmentador de Ancho de Banda para la Red LAN de la Universidad Nacional de Loja e Implementación en el Área de la Energía, las Industrias y los Recursos Naturales No Renovables"** previa a la obtención del título de Ingeniero (a) en Electrónica y Telecomunicaciones, realizado por la señorita egresada: **Evelin Gabriela Alvarado Otero**, la misma que cumple con la reglamentación y políticas de investigación, por lo que autorizo su presentación y posterior sustentación y defensa.

Loja, Octubre del 2013

Ing. Juan Pablo Cabrera Samaniego M.Sc.

DIRECTOR DE TESIS

AUTORÍA

Yo, Évelin Gabriela Alvarado Otero, declaro ser la autora del presente trabajo de tesis y eximo expresamente a la Universidad Nacional de Loja y a sus representantes jurídicos de posibles reclamos o acciones legales, por el contenido de la misma.

Adicionalmente acepto y autorizo a la Universidad Nacional de Loja, la publicación de mi tesis en el Repositorio Institucional-Biblioteca Virtual.

Autora: Évelin Gabriela Alvarado Otero

Firma:.....

Cédula: 1104200538.

Fecha: 5 de Diciembre del 2013

CARTA DE AUTORIZACIÓN DE TESIS POR PARTE DEL AUTOR, PARA LA CONSULTA, REPRODUCCIÓN PARCIAL O TOTAL, Y PUBLICACIÓN ELECTRÓNICA DEL TEXTO COMPLETO.

Yo Évelin Gabriela Alvarado Otero, declaro ser autora de la tesis titulada: "Análisis del Requerimiento de un Segmentador de Ancho de Banda para la RED LAN de la Universidad Nacional de Loja e Implementación en el Área de la Energía, las Industrias y los Recursos Naturales No Renovales", como requisito para optar al grado de: Ingeniera en Electrónica y Telecomunicaciones; autorizo al Sistema Bibliotecario de la Universidad Nacional de Loja para que con fines académicos, muestre al mundo la producción intelectual de la Universidad, a través de la visibilidad de su contenido de la siguiente manera en el repositorio digital Institucional:

Los usuarios pueden consultar el contenido de este trabajo en el RDI, en las redes de información del país y del exterior, con las cuales tenga convenio la Universidad.

La Universidad Nacional de Loja, no se responsabiliza por el plagio o copia de la tesis que realice un tercero.

Para constancia de esta autorización, en la ciudad de Loja, a los cinco días del mes de diciembre del dos mil trece, firma la autora.

Firma: ……

Autora: Évelin Gabriela Alvarado Otero
Cédula: 1104200538
Dirección: Cdla. Zamora **Correo Electrónico:** egalvarado.o@gmail.com
Teléfonos: 2570617 **Celular:** 593-984129532

DATOS COMPLEMENTARIOS

Director de Tesis: Ing. Juan Pablo Cabrera Samaniego, M.Sc.

Tribunal de Grado: Ing. Diego Vinicio Orellana Villavicencio.
Ing. Marcelo Fernando Valdiviezo Condolo.
Ing. Julio César Guamán Segarra.

DEDICATORIA

Ángel, Blanquita, Andrea y Fiorella,

con mucho cariño.

AGRADECIMIENTO

Deseo expresar mis más sinceros agradecimientos a todos quienes hicieron posible la culminación de la presente tesis:

Mi agradecimiento muy especial al Ing. Juan Pablo Cabrera, M.Sc., quien me apoyó en todo momento, con sugerencias en el desarrollo de la fase de campo, análisis de datos y en la dirección y revisión de este trabajo.

A la Universidad Nacional de Loja, al Área de Energía y de Recurso Naturales No Renovables, a través de la Carrera de Ingeniería Electrónica y Telecomunicaciones, donde obtuve los conocimientos técnicos que han contribuido a mi formación profesional.

A todas las áreas de la UNL en donde me apoyaron técnicamente y esto hizo posible la ejecución de la tesis.

También quiero dejar constancia de mi agradecimiento a la Unidad de Telecomunicaciones e Información/Sección Redes, por haberme brindado su ayuda y valiosas sugerencias en el desarrollo de presente trabajo.

LA AUTORA

TABLA DE CONTENIDOS

CONTENIDO **Página**

ÍNDICE DE TABLAS

Nº DESCRIPCIÓN Página

ÍNDICE DE FIGURAS

a. TÍTULO

ANÁLISIS DEL REQUERIMIENTO DE UN SEGMENTADOR DE ANCHO DE BANDA PARA LA RED LAN DE LA UNIVERSIDAD NACIONAL DE LOJA E IMPLEMENTACIÓN EN EL ÁREA DE LA ENERGÍA, LAS INDUSTRIAS Y LOS RECURSOS NATURALES NO RENOVABLES

b. RESUMEN

El presente proyecto de tesis contiene información sobre el requerimiento de un segmentador de ancho de banda para la red LAN de la Universidad Nacional de Loja e implementación en el Área de la Energía, las Industrias y los Recursos Naturales No Renovables. Este estudio está basado en la situación actual de la Universidad, en las cinco áreas que componen el campus universitario.

En la sección **d. Revisión de Literatura**, se desarrolla el marco teórico del proyecto, el cual comprende conceptos de los temas centrales del proyecto de tesis, tales como: Redes de área local, tecnologías Ethernet, ancho de banda, concepto de segmentación y calidad de servicio, así como una breve descripción del escenario de estudio.

En la sección **e. Materiales y Métodos**, se hace mención al equipo para la implementación; también se desarrolla la metodología general de la tesis que va desde el análisis de la situación actual de la red de datos de la Universidad Nacional de Loja, en donde se realiza una descripción de las áreas que comprenden el campus universitario, la descripción de los equipos principales con los que cuenta la red de área local, información acerca de su direccionamiento IP, así como también el sistema de control de acceso a Internet.

En la sección **f. Resultados**, se analiza el consumo de ancho de banda de la universidad, se describen las herramientas que se utilizaron para el análisis; además contiene un estudio relevante acerca del área de energía, el consumo de ancho de banda del área, un reporte de la navegación web que generan sus usuarios, también se detalla la herramienta que se utilizó para la asignación de ancho de banda fijo para cada área. También se analizó el sistema RouterOS, sus características y funciones, también se detallan las configuraciones relacionas con la gestión de redes, tales como: configuración TCP/IP, configuración DHCP, enmascaramiento, establecimiento de puertos, firewall, el de la segmentación del ancho de banda, aplicaciones P2P, servicios de capa 7, etc. Además se

muestran los resultados de las pruebas que se realizaron para la implementación del equipo en la biblioteca del área de energía.

En la sección **g. Discusión**, se describe un análisis relacionado a los puntos importantes abordados en la tesis, así como también la comparación de Mikrotik frente a otras tecnologías para gestionar de una manera más eficiente el ancho de banda. Proceso que se siguió para la implementación del equipo Mikrotik en la biblioteca del área de energía de la UNL.

SUMARY

This thesis contains information about the requirement of a segmenter bandwidth to the data network of the National University of Loja and implementation in the area of Energy, Industry and Non-Renewable Natural Resources. This study is based on the current state of the University, in the five areas that make up the campus.

In section **d. Literature Review**, develops the theoretical framework of the project, which includes concepts of the central themes of the thesis project, such as local area networks, Ethernet technologies, bandwidth segmentation concept and quality of service as well as a brief description of the study setting.

In section **e. Materials and Methods**, references to the device for the implementation; develops the general methodology of the thesis that goes from the current situation analysis of the data network of the National University of Loja, where a description of the areas that comprise the university campus, the description main equipment with which account the local area network, information about its IP address, as well as the access control system to the Internet.

In section **f. Results**, analyzes the bandwidth consumption of the university, describes the tools used for analysis and also contains a relevant study about the energy area, the bandwidth consumption of the area, a report of generating web browsing users, also detailed the tool that was used to allocate fixed bandwidth for each area. Also analyzed RouterOS system, its features and functions, configurations are also relate to network management , such as TCP/IP, DHCP settings, masking, setting ports, firewall, segmentation width band, P2P applications, layer 7 services, etc.. Also shows the results of the tests that were performed for the implementation of the device at library in the area of energy.

In section **g. Discussion**, describes an analysis related to the important points discussed in the thesis, as well as Mikrotik comparison over other technologies to manage more efficiently the bandwidth. Process followed for the implementation of the Mikrotik device at library in the energy area at UNL.

c. INTRODUCCIÓN

Una red, vista en su nivel más básico, es la interconexión entre dos equipos, mediante un medio físico; con el fin de permitir el intercambio de información entre ellos. Hoy en día, sin tener en cuenta la sofisticación que pueden presentar todas las redes, parten de este sencillo sistema; y aunque esta interconexión no parezca extraordinaria, analizado en el tiempo, este sin duda ha sido el mayor y más importante logro en el mundo de las comunicaciones.

Las comunicaciones, y su principal red Internet, en la actualidad es el recurso más imprescindible en la mayor parte de las esferas de la sociedad, consintiendo el progreso de herramientas que ayudan a las personas al mejor desarrollo en su ámbito personal y profesional. Los avances de Internet han traído un sin número de desafíos en los campos: científico, tecnológico y humano, medidas sobre los cuales crecerán y se formarán las sociedades futuras.

Las sociedades actuales, conocedoras de la realidad tecnológica y la necesidad de tener protegido su más preciado bien como lo es la información, se han visto involucradas en los avances que han cambiado completamente la perspectiva del mundo informático. La buena elección de una plataforma de comunicaciones hará que una sociedad tenga más posibilidades de asegurar una posición exitosa; en su implementación se consideran aspectos que permiten optimizar rendimiento y fiabilidad de toda la red.

El presente trabajo surge de la necesidad de la Universidad Nacional de Loja, en investigar la importancia de tener totalmente administrada su red de datos, en términos de segmentación del ancho de banda. Sin dejar de lado parámetros tales como: fiabilidad, flexibilidad en la arquitectura de red, seguridad en los canales de transmisión y que además cumpla con la característica principal que es de permitir la segmentación del ancho de banda, se plantea para éste proyecto la implementación un equipo RouterOS Mikrotik para la biblioteca del área.

Este proyecto expone, sin descuidar la capacidad y velocidades de transmisión en Internet, la importancia de incorporar una herramienta que permita una mejor administración del ancho de banda para beneficio de las personas que trabajan, investigan y que se preparan, en esta institución educativa de tercer nivel.

Esta investigación fue diseñada e implementada mediante el cumplimiento de los siguientes objetivos:

OBJETIVO GENERAL

Analizar el requerimiento de un segmentador de ancho de banda para la red LAN de la Universidad Nacional de Loja e implementar una red para el área de la energía con la aplicación de un equipo segmentador de ancho de banda, para demostrar que se optimizará el uso de los servicios de Internet reflejado en la velocidad de transmisión de datos.

OBJETIVO ESPECÍFICO

1. Levantamiento de línea base sobre el tráfico existente en la red LAN de la Universidad Nacional de Loja y conocer los diferentes parámetros que influyen en la misma.

2. Determinar el número de usuarios que acceden al Internet en el área de energía, en el caso alámbrico e inalámbrico.

3. Implementar un segmentador de ancho de banda que funcione para la biblioteca del área de energía.

4. Realizar las pruebas necesarias para la verificación del funcionamiento del segmentador para la biblioteca del área de energía.

d. REVISIÓN DE LITERATURA

d.1 CAPÍTULO I: Redes de Área Local

Las redes de área local también conocidas como LANs, son redes privadas que se encuentran dentro de un mismo edificio o locación de poca distancia (Km.). Su función es conectar computadores de distintas estaciones de trabajo, en una empresa, con el fin de compartir recursos (impresoras por ejemplo) e intercambiar información. Difieren de otras redes en: topología, tecnología de transmisión y en el tamaño.

Las redes de área local se encuentran limitadas por su longitud máxima, es decir, dependiendo de la longitud máxima que posea la red LAN, dependerá el tiempo de transmisión y las pérdidas de la información.

La conexión de una LAN se da mediante cable, típicamente cable UTP, esto con el fin de interconectar muchas máquinas. Las LANs se ejecutan de 10 a 100 Mbps, con retardo bajo (µs o ns) cometiendo pocos errores. En la actualidad, las LANs funcionan hasta 10 Gbps. Son posibles varias topologías de red, pero las más comunes son: la de red de bus, estrella, anillo y malla.

d.1.1 Ethernet

Ethernet es un estándar que define los lineamientos para la transmisión de datos. Especifica características de cableado, señalización de nivel físico y los formatos de tramas de datos del modelo de Interconexión de Sistemas Abiertos (OSI) por sus siglas en inglés. <<En 1985, el comité de estándares para Redes Metropolitanas y Locales del Instituto de Ingenieros Eléctricos y Electrónicos (IEEE) publicó los estándares para las LAN. Estos estándares comienzan con el número 802. El estándar para Ethernet es el 802.3. El IEEE quería asegurar que sus estándares fueran compatibles con los del modelo OSI de la Organización Internacional para la Estandarización (ISO)>>[6]. El estándar IEEE 802.3 funciona en las capas 1 y 2 del modelo OSI, para autenticar la compatibilidad.

d.1.2 Modelo de Referencia OSI

Una de las necesidades con mayor influencia dentro de un sistema de comunicaciones es el establecimiento de estándares, sin estos sólo se podrían comunicar entre sí los equipos de una misma marca y que utilizaran la misma tecnología. <<La ISO ha generado una gran variedad de estándares, siendo uno de ellos la norma ISO-7494 que define el modelo OSI, este modelo nos ayudará a comprender mejor el funcionamiento de las redes de ordenadores>> [7]. Este modelo es más bien conocido como el modelo de referencia OSI, no asegura la comunicación entre equipos, sino que aporta bases para una mejor estructuración de protocolos de comunicación. Describe siete niveles que permiten la conexión entre sistemas abiertos, cumpliéndose de abajo hacia arriba, en la tabla 1, se resumen las 7 capas con su respectiva función, unidad y protocolos.

Tabla 1. Capas del Modelo de Referencia OSI

	CAPAS	FUNCIÓN	PDU	PROTOCOLOS
7	Aplicación	Servicios de red a aplicaciones	Datos	HTTP, FTP, SMTP, SNMP, DHCP, NTP, DNS, POP, SSH, Telnet
6	Presentación	Representación de los datos.	Datos	JPEG, GIF, MPEG
5	Sesión	Comunicación entre dispositivos de la red	Datos	Apple Talk, Winsock
4	Transporte	Conexión extremo–a–extremo y fiabilidad de los datos	Segmento	TCP, UDP, SPX.
3	Red	Determinación de ruta e IP (Direccionamiento lógico)	Paquete	IP, ICMP. (Router)
2	Enlace de datos	Direccionamiento físico (MAC y LLC)	Trama	LLC, MAC, PPP, HDLC, Frame Relay, ATM.(Switch, Bridge)
1	Física	Se ocupa de la transmisión del flujo de bits a través del medio.	Bit	Ethernet, Token Ring, Token Bus. (Hub, Repetidor)
Elaborado por: Évelin Alvarado Otero				

En otras palabras, al ser recibido un paquete desde otro sistema con modelo OSI, dicho paquete, a medida que va ascendiendo de la capa 1 a la 7, deja en cada capa los datos añadidos por la capa equivalente del otro sistema, hasta quedar únicamente los datos a transmitir; en resumen, se forman las denominadas tramas por capa.

d.1.3 Modelo TCP/IP

El modelo TCP/IP, es el modelo que se pone en práctica en la vida real. El modelo de referencia OSI es universalmente reconocido, pero, el estándar que se utiliza en la práctica para Internet, desde el punto de vista técnico, es el Protocolo de Control de Transmisión/Protocolo Internet (TCP/IP). El modelo de referencia TCP/IP y su pila de protocolos, permiten que la comunicación entre dos o más dispositivos de red sea posible, desde cualquier lugar del mundo. A continuación en la tabla 2, se detalla en resumen las 4 capas con su respectiva función y protocolos.

Tabla 2. Capas del Modelo de Referencia TCP/IP

CAPAS		FUNCIÓN	PROTOCOLOS
4	Aplicación	Maneja protocolos de alto nivel, aspectos de representación, codificación y control de diálogo.	HTTP, Telnet, FTP, TFTP, SNMP, DNS, SMTP, X Windows y otros protocolos de aplicación
3	Transporte	Aspectos de calidad del servicio con respecto a la confiabilidad, el control de flujo y la corrección de errores.	TCP, UDP, RTP
2	Internet	Envía paquetes origen desde cualquier red en Internetwork de redes y que estos paquetes lleguen a su destino independientemente de la ruta y de las redes que se utilizaron para llegar hasta allí.	IP, ICMP, ARP, RARP
1	Acceso a la red	Es la capa que se ocupa de todos los aspectos que requiere un paquete IP para realizar realmente un enlace físico y luego realizar otro enlace físico.	Ethernet, Token Ring, FDDI, X.25, Frame Relay, RS-232, v.35
Elaborado por: Évelin Alvarado Otero			

Las capas del modelo TCP/IP cumplen iguales funciones que las capas del modelo OSI, en la figura 1, se muestra qué capas del modelo TCP/IP cumplen igual responsabilidad que en el modelo OSI.

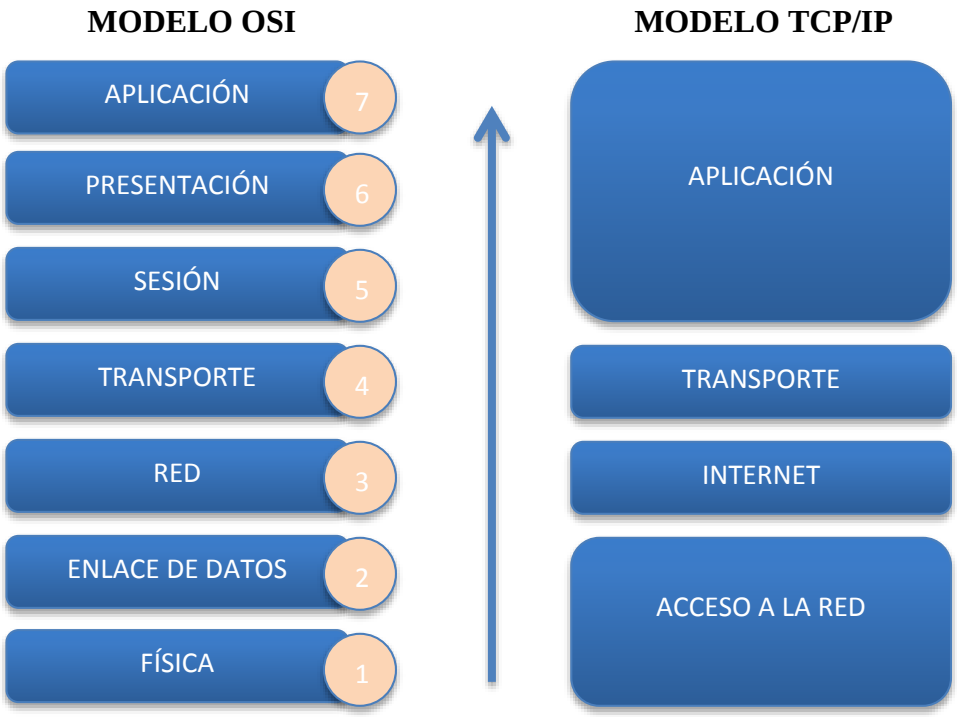


Figura 1. Modelo de Referencia TCP/IP y OSI

d.1.3.1 Protocolos TCP/IP

Al referirse a TCP/IP, se habla instintivamente como el protocolo que rige el funcionamiento de Internet. De cierta manera esto es verdad, porque se le llama TCP/IP, al conjunto de protocolos que permite estar siempre conectado a Internet. Los dos protocolos fundamentales que lo conforman son:

- **Protocolo de control de transmisión TCP:** trabaja en la capa de transporte del modelo de referencia OSI, facilitando el transporte fiable de datos.
- **Protocolo Internet IP:** trabaja en la capa de red del modelo de referencia OSI, permite llevar los datos hacia otros *host*.

Este protocolo maneja errores en la transmisión, administra el enrutamiento y entrega de los datos, también controla la transmisión real mediante señales de estado. En la figura 2, se muestra la pila de protocolos que funcionan por capa.

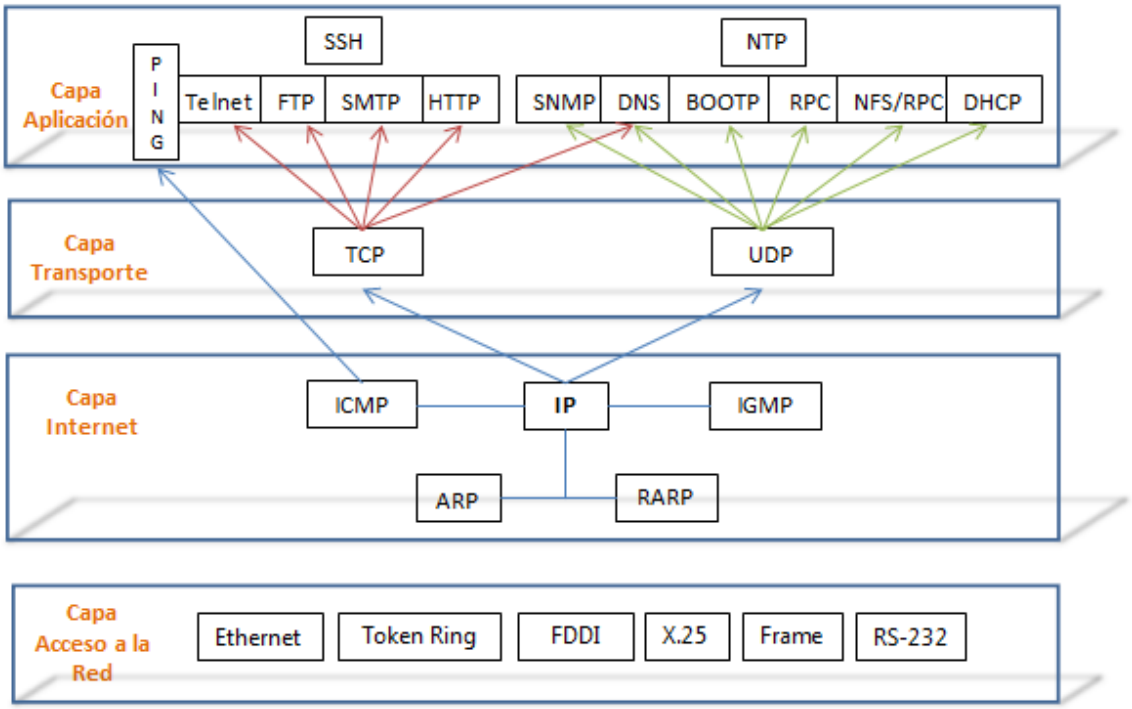


Figura 2. **Protocolos del modelo TCP/IP**

Protocolos de alto nivel:

a) Protocolos basados en ICMP:

- **PING:** se utiliza para realizar una solicitud de eco

b) Protocolos basados en TCP:

- **Telnet**: terminal remoto, proporciona capacidad de registro de entrada remoto.
- **FTP:** (*File Transfer Protocol*) o Protocolo de Transferencia de Archivos proporciona una interfaz y servicio para la transferencia de archivos de un servidor a otro, desde cualquier parte en la que se encuentre el usuario.
- **SMTP:** (*Simple Mail Transfer Protocol*) o Protocolo Simple de Transferencia de Correo brinda servicios de correo electrónico en las redes de Internet.
- **HTTP:** (HyperText Transfer Protocol: encargado de dar funcionalidad a las páginas web.

c) Protocolos basados en UDP:

- **SNMP**: (*Simple Network Management Protocol*) o Protocolo Simple de Administración de Red, utiliza procesos distintos de TCP/IP, tal es el caso de

administradores y agentes en vez de clientes y servidores. Es un protocolo que permite tener supervisada una red desde software que soporte ICMP.

- **BOOTP:** arranque remoto.
- **DNS:** (*Domain Name System*) o Sistema de nombres de dominio, convierte una dirección lógica a una dirección de nombre, entendible para el usuario.
- **RPC**: (*Remote Procedure Call*) o ejecución de procesos remotos.

d) **Protocolo TCP**: (*Transport Control Protocol*) o Protocolo de Control de Transporte es un protocolo orientado a la conexión. Gestiona la conexión entre las computadoras emisora y receptora de forma parecida al desarrollo de las llamadas telefónicas.

e) **Protocolo UDP:** (*User Datagrama Protocol*) o Protocolo de Datagrama de Usuario es un protocolo de transporte no orientado a conexión que proporciona servicios en colaboración con TCP.

f) **Protocolo IP:** (Internet Protocol) o Protocolo de Internet es la base para todo el direccionamiento que se produce en las redes TCP/IP y proporciona un protocolo orientado a la capa de red sin conexión. Análogamente es semejante al mecanismo de envío de cartas, desde un remitente hacia un destinatario.

g) **Protocolo ICMP:** (*Internet Control Message Protocol*) protocolo de la familia Internet, este protocolo es un gestor de errores, que permite la comunicación de información de control y de errores entre computadoras intermedias y/o dispositivos activos de red, por las que viajan los paquetes de datos.

h) **Protocolo IGMP:** (*Internet Group Management Protocol*) es un protocolo de la familia Internet, que permite a computadores pertenecer a grupos multicast. El IP multicast es una variante de IP, permite emplear datagramas con múltiples destinatarios.

i) **Protocolo ARP:** (*Address Resolution Protocol*) o Protocolo de Resolución de Direcciones, relaciona una dirección IP con una dirección MAC.

j) **Protocolo RARP:** (*Reverse Address Resolution Protocol*) este protocolo tiene la finalidad de proporcionar la dirección lógica de un computador, ya que este por si solo puede conocer su dirección MAC únicamente.

d.2 CAPÍTULO II: Ancho de Banda

No es hasta hace algún tiempo atrás que transmisiones de televisión, radio, y hasta el mismo teléfono ya se enviaban por un medio no guiado, y mucho más remotamente mediante cables utilizando ondas electromagnéticas. <<El ancho de banda analógico se mide en función de la cantidad de espectro magnético ocupada por cada señal. o ciclos por segundo. Por lo general, se usan múltiplos de esta unidad de medida básica para anchos de banda analógicos>>[14]. Esta unidad permite definir frecuencias del espacio radioeléctrico para televisión, radio, y teléfonos inalámbricos que por ejemplo operan a 900 MHz o a 2,4 GHz. <<También son las unidades que se usan para describir las frecuencias de las redes inalámbricas 802.11a y 802.11b, que operan a 5GHz y 2,4 GHz>>[14].

Las nuevas tecnologías de la información y la comunicación, son el boom de las telecomunicaciones, y es que desde la aparición de su potencial integrante la red Internet, en el cual se introdujo la transmisión de audio, video y datos (que fue principalmente para lo que fue creado), fue necesaria la aparición de un nuevo concepto de ancho de banda, ya que el lenguaje con las señales analógicas no sería el mismo. El término red digital aparece en la comunicación de datos por medio de internet. <<En la señalización digital, toda la información se envía como bits, independientemente del tipo de información del cual se trate. Voz, video y datos se convierten todos en corrientes de bits al ser preparados para su transmisión a través de medios digitales. >>[14]. Este nuevo tipo de transmisión es el de ancho de banda digital. Gracias al nuevo concepto de ancho de banda digital, fue posible enviar grandes cantidades de información por medio de un canal digital. <<Independientemente de lo que la información digital demore en llegar a su destino y reensamblarse, para que pueda ser vista, oída, leída o procesada en su forma original>>[14].

Sin duda alguna que el medio de información más popular es la Internet, para poder acceder a este, los computadores también fueron evolucionando a la par. El ancho de banda como tal, es una propiedad física del medio de transmisión y su concepto es uno de los más importantes y actuales en el campo de las telecomunicaciones. De la siguiente manera

queda definido ancho de banda digital: <<En conexiones a Internet el ancho de banda digital, ancho de banda de red o simplemente ancho de banda, es la cantidad de información o de datos que se puede enviar a través de una conexión de red en un período de tiempo dado. El ancho de banda se indica generalmente en bites por segundo (bps), kilo bites por segundo (Kbps), o mega bites por segundo (Mbps).>> [24]

El término ancho de banda también se refiere a la capacidad de ancho de banda disponible en bit/s, lo cual representa un rango neto de bits en un sistema de comunicación digital. Desde un punto de vista más general, aquella conexión de ancho de banda digital es la que permite transportar suficiente cantidad de información. Está claro que, en esencia, una buena comunicación consiste totalmente en una sucesión de conexiones, cada cual con su propio ancho de banda.

La decisión de incrementar el ancho de banda disponible en una red, es única y exclusiva del administrador de red, al determinar que las capacidades de transferencia de la red comprometen la disponibilidad de los servicios. <<Esta decisión se sustenta en estudios que consideran: la topología de la red, la capacidad de los enlaces, las características de los equipos de red instalados actualmente, las necesidades de los usuarios y los servicios ofrecidos. Acerca de la capacidad de transferencia de la red, esto se puede entender como que el flujo de datos es tan grande, que ocupa todo el ancho de banda disponible y compromete el envío del resto de la información en la red proveniente de todos los usuarios>>[3].

Incrementar el ancho de banda innecesariamente es el resultado de una inversión económica considerable; los parámetros antes mencionados, son un punto muy importante para tomar la decisión de incrementar o no el ancho de banda. Si se tiene una cantidad de usuarios inadecuada para el ancho de banda contratado, la red presentará caídas; para cálculos de ancho de banda, independientemente de las aplicaciones más utilizadas y más bien como un dato referencial y mínimo, por usuario, se considera en términos de eficiencia, una cantidad de 250 kbps por *host*.

<<Se puede dar el caso de que un usuario siempre este acaparando la mayor parte del ancho de banda. Si se eligiera incrementar el ancho de banda en la red, y la cuestión de este usuario que gana la competencia por el recurso se pasara por alto, el resultado sería que este usuario seguiría ganando la mayoría del ancho de banda disponible y peor aún, el ancho de banda ganado sería más grande que el que originalmente utilizaba>>[3].

d.3 CAPÍTULO III: Segmentador

La mayor parte de los *hosts* tiene la capacidad de utilizar el ancho de banda que el usuario necesite, pero, cuando el volumen de tráfico en la red crece debido a un inadecuado uso del servicio, surgen técnicas para que este problema sea controlado. Por ejemplo, si varios usuarios de una misma red local empiezan a descargar simultáneamente películas, llegando hasta el 90% de la capacidad de descarga y de subida total, los demás usuarios de la red se tendrían un mal servicio.

La solución más popular que ha producido un mejoramiento considerable en el rendimiento de la red, es implementar un sistema que se encargue de limitar el ancho de banda. Para evitar este tipo de inconveniente con el uso del ancho de banda en Internet, los administradores de red hacen uso de un equipo segmentador de ancho de banda.

Un segmentador es sinónimo de una planeación estratégica y táctica del ancho de banda, operaciones y mantenimiento de una red y sus servicios, con el fin de asegurar que los usuarios de una red reciban un servicio con la calidad que ellos esperan y asegurar que la información se mueva a través de ella con la máxima eficiencia y transparencia para los usuarios. Esta es la estructura en la que deben fijarse las labores de administración de una red.

Un administrador de red debe tener en cuenta cuáles son los parámetros fundamentales para la administración de una red y tener en cuenta cuales le servirán para una asignación futura. En la figura 3, se detallan modelos básicos.

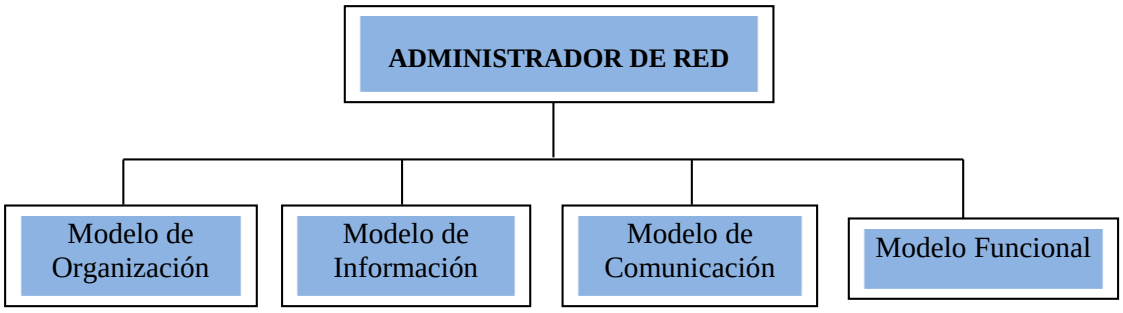


Figura 3. Modelo Administrador de Red

d.3.1 Segmentación del ancho de banda

En una red que presente una mala calidad de servicio, significa que puede tener algunos problemas tales como: el mal uso del ancho de banda contratado, por no lograr asignar el recurso de en forma dinámica a tipos de tráfico específicos; distintos tipos de congestión en los enlaces de datos, descarte de tráfico de alta prioridad, ya que ciertos flujos pueden estar utilizando el ancho de banda en forma desmedida; falta de disponibilidad del ancho de banda en aplicaciones que requieren la participación del usuario; entrega de información inoportuna de mensajería o correo electrónico. <<Todos estos inconvenientes afectan directa o indirectamente a los usuarios y por consiguiente la productividad de una organización>>[13].

La segmentación del ancho de banda permite asignar ancho de banda ya sea en forma dinámica o manual, según lo permitan las características del equipo implementado, controlar la congestión, o establecer prioridades en el tráfico. Manejar de una forma eficiente el ancho de banda, se conoce también como calidad y servicio, <<Para disponer de una calidad de servicio aceptable en redes IP, se han diseñado herramientas a medida como el protocolo de reservación Protocolo de Reserva de Recursos (RSVP), mediante Calidad de Servicio (QoS) se pueden preservar datos con características relevantes>>[13].

d.3.2 Calidad de Servicio – QoS

La Calidad de Servicio suele ser definida como un conjunto de tecnologías que permiten a los administradores de red manejar los efectos de la congestión del tráfico,

usando óptimamente los diferentes recursos de la red, en lugar de ir aumentando continuamente capacidad. "Es el efecto colectivo del rendimiento de un servicio que determina el grado de satisfacción del usuario de dicho servicio"

ITU-T Recomendación E-800 (0894) (1994)

d.3.2.1 Parámetros o atributos que definen la QoS

Reserva de Ancho de Banda:

Garantiza la transmisión de cierta cantidad de datos en un tiempo determinado. Este resultado se obtiene mediante identificadores de cabecera de los paquetes dando prioridad al tráfico de un determinado tipo de archivos (video, sonido, voz, etc.), de esta manera, se asegura un determinado ancho de banda para estos archivos, siempre que el usuario los utilice.

Importancia de la QoS

La QoS tiene cuatro situaciones a tomar en cuenta para determinar un QoS eficiente:

1. La QoS que el usuario espera.
2. La QoS que el proveedor entrega.
3. La QoS que el proveedor de servicio de internet obtiene imparcialmente.
4. La QoS que finalmente el usuario percibe.

Se dice que una red o proveedor ofrecen "Calidad de Servicio" cuando se le garantiza al usuario el cumplimiento de uno o varios parámetros que ofrece Internet. Si no, se concluye que lo que ofrece un servicio "*best effort*" (mejor esfuerzo), que es muy parecido a QoS pero no es una garantía de calidad de servicio.

d.3.2.2 QoS en los Routers

El QoS se convierte en una disciplina de colas para dar preferencia a los paquetes según la QoS establecida. También es la selección de ruta según las características de QoS de cada posible ruta, y lo más importante invocar tratamiento QoS en la subred del siguiente salto. Entre otras características tenemos que:

- QoS es la tentativa de utilizar recursos existentes razonablemente (no se necesita utilizar todo el ancho de banda disponible para decir que el servicio es excelente).
- QoS balancea y prioriza el flujo de datos, cerciorándose de ofrecer la mejor velocidad posible y previniendo el "monopolio" del canal de datos.
- QoS no es únicamente limitación.
- QoS popularmente es implementado por mecanismos de *queueing* (en el caso de los *Mikrotik*). El Queuing controla la forma en que los paquetes esperan en cola para salir de la interface.

d.4 CAPÍTULO IV: Descripción del escenario de estudio: Red de datos de la Universidad Nacional de Loja

d.4.1 Infraestructura

El campus universitario se encuentra ubicado en la Ciudadela Universitaria Guillermo Falconí Espinoza, entre las calles Avenida Reinaldo Espinosa y la Avenida Pío Jaramillo Alvarado, en esta parte del campus universitario se encuentran funcionando cuatro de las cinco áreas que forman parte de la Universidad Nacional de Loja (UNL), estas áreas son: el Área de la Educación el Arte y la Comunicación; el Área Jurídica, Social y Administrativa; el Área Agropecuaria y de Recursos Naturales Renovables; y el Área de la Energía, las Industrias y los Recursos Naturales no Renovables. La quinta área que conforma la Universidad Nacional de Loja, se encuentra en el centro noroccidental de la misma ciudad, ubicada en el barrio Sevilla de Oro en la parte posterior al Hospital Isidro Ayora, ubicado en las calles Manuel Monteros y Carlos Román, esta área es: el Área de la Salud Humana.

Para la conexión entre el campus principal y el área de la Salud, se hace uso de una red de retorno (Backhaul), conformado por un equipo *Canopy Motorola Wireless Internet Plataform* a una frecuencia de enlace de 5.7 GHz, entre enlace punto-punto. En las figuras 4 y 5 respectivamente se puede observar la ubicación del campus universitario al sur de la ciudad de Loja y la ubicación del Área de la Salud Humana en el centro noroccidental de la ciudad.

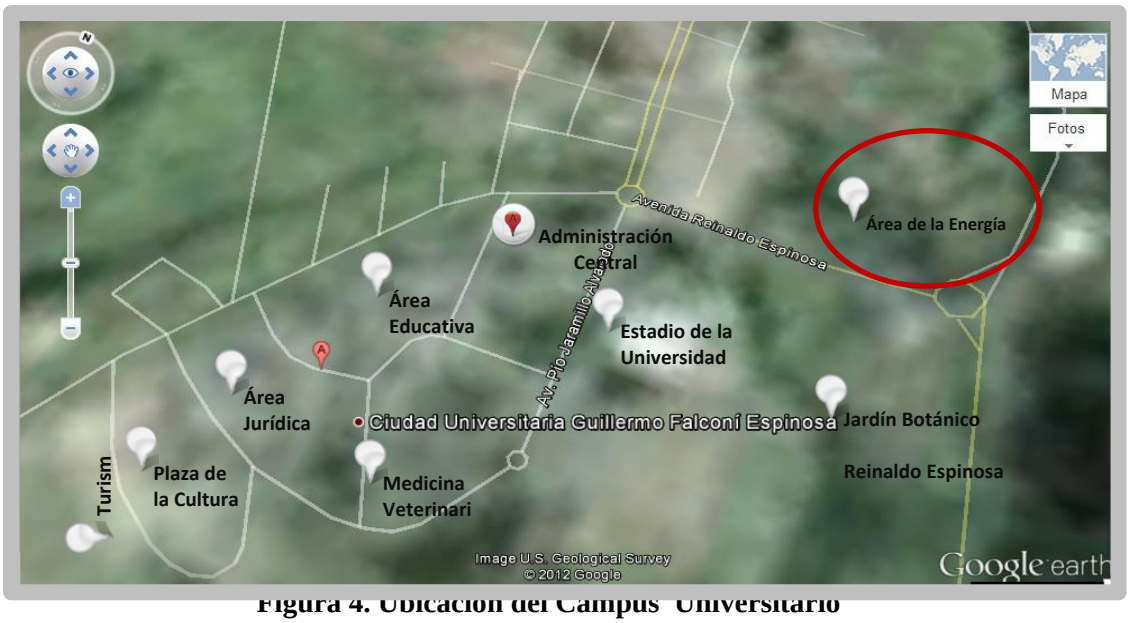


Figura 4. Ubicación del Campus Universitario

Figura 5. Ubicación del Área de Salud

d.4.2 Área de la Educación Arte y Comunicación

Se encuentra ubicada al Noroccidente de la ciudadela Universitaria es una de las más grandes con la que cuenta la Universidad, su estructura física en su mayoría compuesta de edificios de dos pisos, a diferencia del edificio de la Carrera de Comunicación Social, la cual actualmente está ubicada en una construcción antigua; es parte de esta área el colegio Universitario Manuel Cabrera Lozano, en este bloque se encuentra la biblioteca del área,

siendo este el lugar donde se encuentra un servidor proxy, el cual da acceso a la red a dicha área, cuenta con switchs de acceso para la red cableada, las carreras de Comunicación social, Informática Educativa, Ingles, Químico Biológicas, Físico Matemáticas, Artes Plásticas, Música, Educación Física, Psicología, y Posgrado de Educativa forman parte de esta área.

d.4.3 Área Jurídica Social y Administrativa

Es el área más grande dentro de la Universidad, ubicada al Noroccidente de la misma contigua al Área Educativa, dispone de edificios en su mayoría de dos pisos, es la que cuenta con el mayor número de estudiantes, tiene aproximadamente diez bloques en los que se distribuyen las diferentes carreras, al igual que todas las áreas dispone de una biblioteca que es el lugar donde se encuentra ubicado el servidor proxy que permite el acceso a la red. Forman parte del área Jurídica las carreras de: Derecho, Banca y Finanzas, Administración Publica, Turismo, Posgrado de Derecho, Administración de Empresas, Economía, Trabajo Social, Contabilidad y Auditoría.

d.4.4 Área Agropecuaria

Ubicada al Sur del campus Universitario, compuesta por edificios en su mayoría actuales, cuenta con aproximadamente con dieciséis edificios entre uno y dos pisos, tiene la biblioteca perteneciente al área que es el lugar donde se encuentra un servidor proxy para dar acceso a la red. Forman parte de esta área las carreras de: Ingeniería Agrícola, Ingeniería Agronómica, Ingeniería en Manejo y Conservación del Medio Ambiente, Ingeniería en Producción, Ingeniería Forestal, Medicina Veterinaria y los Programas de Posgrado.

d.4.5 Área de la Energía, las Industria y los Recursos Naturales no Renovables (AEIRNNR)

El área de la Energía como se la denomina usualmente se encuentra ubicada al Nororiente del Campus Universitario, forman parte de esta área los edificios de la Modalidad de Estudios a Distancia (MED), en su mayoría está compuesta por edificios

nuevos, aquí se encuentran cuatro laboratorios virtuales, cuenta con siete edificios que conforman esta área, uno de los edificios con más concentración de usuarios de la red de datos es la biblioteca, al igual que con el resto de áreas también dispone de un servidor proxy para dar acceso a los usuarios de la red cableada, cuenta con 9 puntos de acceso que se encuentran distribuidos en los diferentes bloques. Forman parte de esta área las carreras de: Ingeniería en Sistemas, Ingeniería Electromecánica, Ingeniería en Geología, Ingeniería en Electrónica y Telecomunicaciones.

d.4.6 Área de la Salud Humana

Esta área se encuentra ubicada al Norte de la ciudadela Universitaria, junto al hospital Isidro Ayora, cuenta en su mayoría con edificaciones nuevas, a diferencia de las otras áreas la conexión con la red de datos se la hace de manera inalámbrica, contando también con un servidor proxy para el acceso a la red, cuenta con aproximadamente siete edificios entre la parte administrativa y los que se utilizan para dar clases, cuenta con cuatro puntos de acceso los cuales les permiten la comunicación inalámbrica a los usuarios de la red de datos, forman parte de esta área las carreras de: Laboratorio clínico, Odontología, Medicina, Psicología Clínica, Enfermería y su nivel de posgrado con especialidades Médicas y Maestría.

d.4.7 Administración Central

El edificio de administración central se encuentra ubicado en el lado Norte de la UNL dividido en dos bloques. En este edificio se encuentran localizados la mayoría de los departamentos administrativos de la Universidad en el bloque uno encontramos departamentos como son, el Rectorado, Vicerrectorado, Secretaria General, Jefatura de Bibliotecas Auditoria Interna, Procuraduría General, Tesorería, Documentación y Archivo, Venta de Derechos Especiales y Construcciones, mientras tanto en el bloque dos tenemos los departamentos de Recursos Humanos, Bienestar Estudiantil, Compras Públicas, Sucursal del Banco de Loja , Contabilidad General, Dirección Financiera, Nominas, Sistema de Gestión Académico, Centro de Investigaciones y Apoyo al Desarrollo Universitario y la Unidad de Redes Telecomunicaciones e Información, sección redes que

es el encargado del control de la red de datos de la UNL, se encuentra ubicado en este edificio en la planta alta, donde se ubica además el cuarto frío que es donde están los equipos como son servidores principales, los Switchs de acceso, UPS de los equipos, etc.

e. MATERIALES Y MÉTODOS

e.1 Materiales

Para la implementación del proyecto de tesis se utilizó un equipo Mikrotik RouterBOARD 750, figura 6, cuyo sistema operativo está basado en el Kernel de Linux y es muy estable. Se adopta la utilización de este equipo primeramente por cumplir con las características de un equipo controlador de ancho de banda y poseer similares características al de un equipo segmentador más robusto, además de brindar buena seguridad y flexibilidad, es un equipo adecuado para el número de usuarios que forman parte de la biblioteca, debido a que soporta un máximo de 60 usuarios; es adecuado también para trabajar con el ancho de banda asignado a la biblioteca ya que el equipo soporta hasta 10 Mbps. En el anexo 1 se presenta información de su ficha técnica.

Figura 6. Equipo Mikrotik RouterBOARD RB750

<u>Características principales del equipo Mikrotik</u> [4]

- ✓ Puede ejecutarse desde discos IDE o módulos de memoria flash.
- ✓ Diseño modular de 113x89x28mm.

- ✓ Módulos actualizables
- ✓ Peso sin embalaje y cables: 129g

Características de ruteo [4]

- ✓ Políticas de enrutamiento. Ruteo estático o dinámico.
- ✓ Bridging, protocolo spanning tree, interfaces multiples bridge, firewall en el
- ✓ bridge.
- ✓ Servidores y clientes: DHCP, PPPoE, PPTP, PPP, Relay de DHCP.
- ✓ Cache: web-proxy, DNS.
- ✓ Gateway de HotSpot.
- ✓ Lenguaje interno de scripts.

Características del RouterOS [4]

- ✓ Filtrado de paquetes por:
- ✓ Origen, IP de destino.
- ✓ Protocolos, puertos.
- ✓ Contenidos (seguimiento de conexiones P2P).
- ✓ Puede detectar ataques de denegación de servicio (DoS)
- ✓ Permite solamente cierto número de paquetes por periodo de tiempo.

Calidad de servicio (QoS) [4]

- ✓ **Tipos de colas**
  - RED
  - BFIFO
  - PFIFO
  - PCQ
- ✓ **Colas simples**
  - Por origen/destino de red.
  - Dirección IP de cliente.
  - Interface

- ✓ **Árboles de colas**
  - Por protocolo.
  - Por puerto.
  - Por tipo de conexión.

Interfaces del RouterOS [4]

- ✓ Ethernet 10/100/1000 Mbit.
- ✓ Inalámbrica (Atheros, Prism, CISCO/Airones)
- ✓ Punto de acceso o modo estación/cliente, WDS.
- ✓ Síncronas: V35, E1, Frame Relay.
- ✓ Asíncronas: Onboard serial, 8-port PCI.
- ✓ ISDN
- ✓ xDSL
- ✓ Virtual LAN (VLAN)

Herramientas de manejo de red [4]

- ✓ Ping, traceroute.
- ✓ Medidor de ancho de banda.
- ✓ Contabilización de tráfico.
- ✓ SNMP.
- ✓ Torch.
- ✓ Sniffer de paquetes.

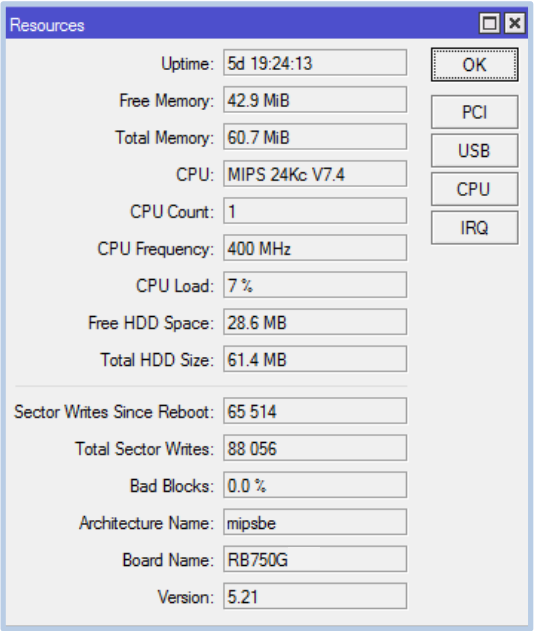


Figura 7. Características del equipo Mikrotik 750

En la figura 7 se muestran las principales características del sistema operativo y software Mikrotik RB750. Costo del equipo para la implementación: 70 USD.

e.2 Métodos

e.2.1 Análisis de la red de datos de la Universidad Nacional de Loja

En la actualidad la Universidad dentro de su estructura funcional cuenta con la Unidad de Telecomunicaciones e Información (UTI), la cual está dividida en cuatro secciones importantes las cuales son: sección de desarrollo de software, sección de mantenimiento y equipos electrónicos, sección de telecomunicaciones y la sección de redes y equipos informáticos. La sección de redes y equipos informáticos es el responsable de la administración y gestión de la Red de datos en la Universidad Nacional de Loja (UNL).

El Proveedor de Servicios de Internet (ISP) con el que cuenta la UNL es el Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado (CEDIA), quienes en convenio con la empresa TELCONET S.A, provee un ancho de banda de 99Mbps.

El número de usuarios finales con los que cuenta la red LAN de la UNL comprende un estimado de: 2000 a 2500 puntos; y para el caso de los usuarios inalámbricos, un estimado de: 800 usuarios.

Backbone de la Universidad Nacional de Loja

En la figura 8, se muestra el backbone de la infraestructura de la red de datos, donde se observan las principales conexiones troncales de la intranet como de la extranet.

El backbone de la Universidad está compuesto de un gran número de switches interconectados, los cuales llevan los datos a través de las distintas dependencias, utilizando tres tipos de medio de transmisión según la necesidad: fibra óptica, cable UTP (*Unshielded twisted pair*) cat. 5e y enlaces inalámbricos.

e.2.2 Tecnología Ethernet

Bajo el estándar IEEE 802.3 desarrollado para tecnología Ethernet para redes LAN, la Universidad trabaja con tecnologías 100 Fast Ethernet (100 Mbps) y Gigabit Ethernet (1000 Mbps) para conexiones a internet. Fast Ethernet es una red de comunicación de datos en serie, a través de pares de cobre o Fibra Óptica. Para la Red de Área Local Inalámbrica (WLAN), utilizando el estándar IEEE 802.11b (2,4GHz) y 802.11n (2,4GHz -5,4 GHz).

Como medio más utilizado para la transmisión de datos se utiliza el Cable UTP categoría 5e bajo la norma EIA/TIA 568-A-B, siendo el más utilizado el estándar B para conectorización; este cable está compuesto de 8 hilos (4 pares), es de tipo par trenzado sin protección, viene trenzado para evitar pérdida de datos a causa de la diafonía, este cable permite transmitir datos sin pérdida de bits hasta los 90 metros.

Para la distribución de Internet a las distintas áreas se realizan conexiones mediante Fibra Óptica multimodo, en modo de transmisión Full Duplex. Los enlaces de fibra entre los distintos nodos Fasth Ethernet de la red informática, son de fibra óptica multimodo 62.5 /125 micrones (μm) de seis hilos con una cubierta buferizada. Gracias a las grandes velocidades a las que permite trabajar, hace posible una comunicación Full-Dúplex.

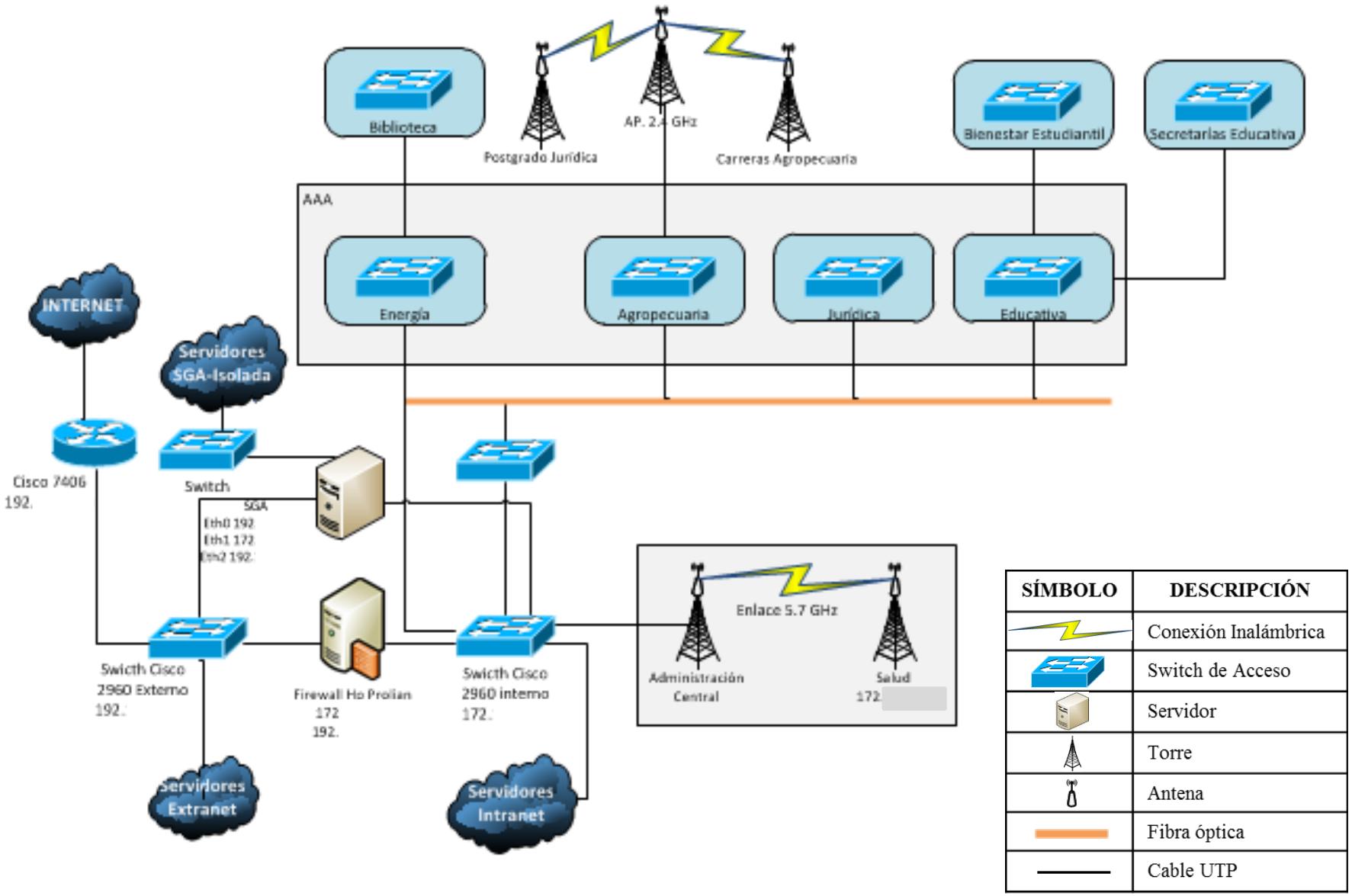


Figura 8. Backbone de la Universidad Nacional de Loja

e.2.3 Topología

La Universidad cuenta con una topología de red de estrella jerarquizada, la propia topología de la red proporciona puntos de concentración para el control y el envío de la información a los siguientes nodos. Cada nodo se conecta de forma independiente a un nodo central o de mayor jerarquía. La ventaja de tener este tipo de topología es que en caso de fallo de alguno de los nodos, no se pierde la conexión de toda la universidad, sino la conexión de los usuarios que están jerárquicamente por debajo del nodo principal afectado, es el producto de tener una conexión en cascada. La distribución inicia desde el Cuarto de Telecomunicaciones hacia las distintas áreas o bloques donde se requiere el servicio de Internet.

La tecnología con que trabaja la red actualmente permite velocidades de 10 Mbps y 100 Mbps, la cual no necesita repetidores o amplificadores intermedios, debido a que trabaja con las distancias necesarias para el campus universitario.

En los bloques de Administración Central la red de datos se compone de un backbone que usa como medio de transmisión fibra óptica de 6 hilos, en su mayoría ocupando dos hilos para la interconexión la que comunica las AAA: Jurídica, Educativa, Agropecuaria y Energía y los dispositivos de networking activos para las comunicaciones.

Las distancias de transmisión de este tipo de fibra esta alrededor de los 1,604 km y se utilizan a diferentes velocidades: 10 Mbps, 100 Mbps. Cada terminación de fibra en cada edificio, se encuentra distribuido en el campus universitario, llega a su respectiva bandeja de fibra que se encuentra empalmada con conectores del tipo SC, y estos a los switch que poseen puertos para fibra.

Este cableado troncal es el que soporta todo el tráfico de información entre las áreas, permitiendo de esta manera hacer uso de los diferentes servicios de red que brinda la Universidad en todo el campus universitario como son: (servicio) Internet, Acceso

Inalámbrico, Correo Electrónico, Videoconferencias, Sistema de Gestión Académico etc.

Diagrama de la topología de la Intranet

En el diagrama de topología, figura 9, se describen todos los enlaces principales, servidores y dispositivos de *networking* que sirven para la comunicación en la red de datos de todo el campus universitario.

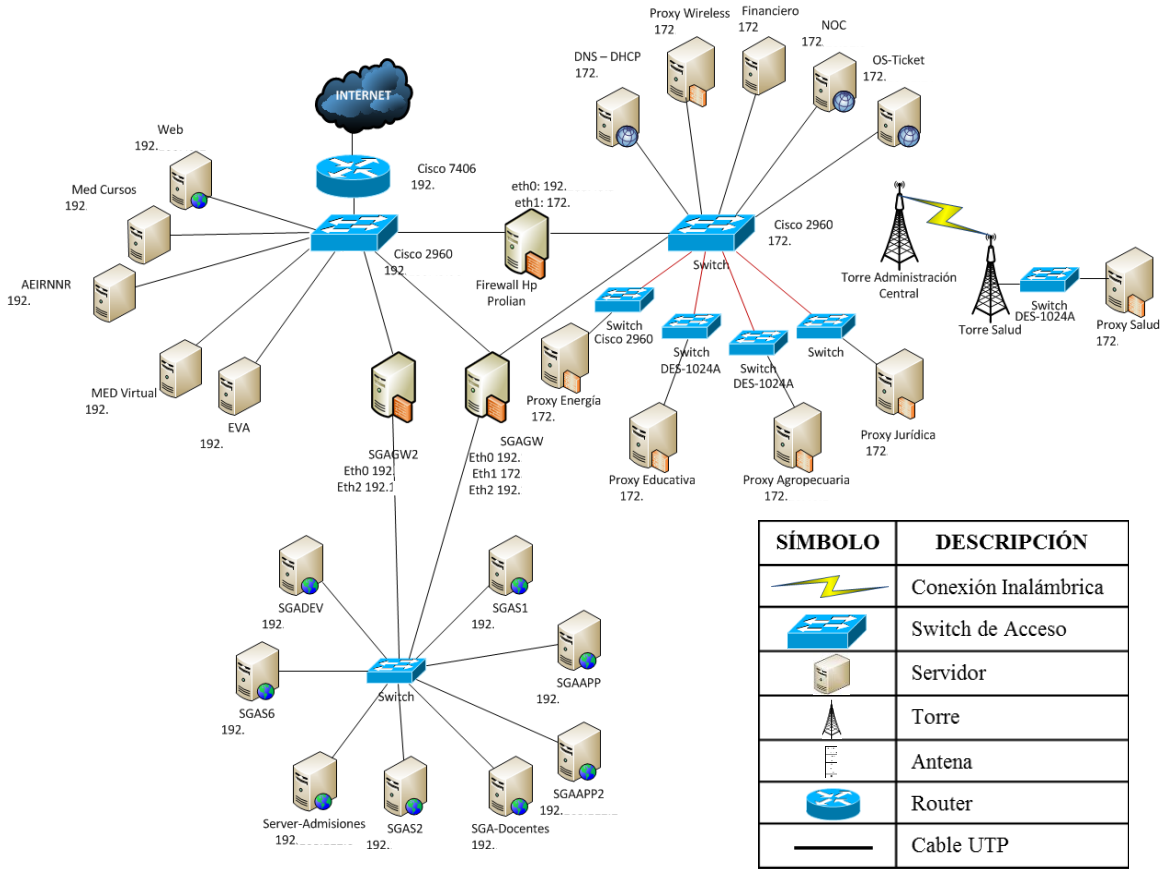


Figura 9. Topología de la Intranet de la Universidad Nacional de Loja

En la figura 9, se puede observar detalladamente los dispositivos de *networking* activos principales como son: Router cisco 7604, switch cisco 2960 externo, switch cisco 2960 interno, firewall HP *ProLiant*, los cuales se describen más adelante. También se visualiza los servidores públicos y privados, los cuales brindan servicios muy importantes en el campus universitario dentro de ellos están DNS, DHCP, Proxys etc.

Descripción de servidores públicos

Como se muestra en la figura 9, al Switch cisco 2960 están conectados los servidores públicos. Estos servidores son necesarios para acceder tanto desde afuera como desde la intranet de la universidad. A continuación se detallan los servidores que se encuentran implementados y en producción en la Unidad de Telecomunicaciones e Información.

- **Servidor Web:** este servidor tiene la función de brindar al usuario todas las actividades digitales de la Universidad a través de aplicaciones web dinámicas como son: blogs, cursos, etc. Aquí se encuentra información de cada una de las dependencias y áreas académico administrativas lo que permite la interacción de los usuarios con la página.
- **Sistema Académico:** el cuarto de telecomunicaciones contiene todos los servidores que cumplen la función de brindar un Sistema de Gestión Académico (SGA) de alto rendimiento y disponibilidad. Lo que permite la automatización de procesos académicos que se realizaban de forma manual. Este es un servicio que se encuentra disponible tanto para estudiantes como docentes en la página web de la universidad.
- **Modalidad a Distancia:** los servidores con los que cuenta la Modalidad de Estudios a Distancia (MED) ofrecen una educación a distancia virtualizada mediante las plataformas de *e-learning* (moodle) las cuales incorporan aplicación como: foros de discusión, blog personales, mensajería instantánea etc.

En la tabla 3, se detalla el hardware de los equipos donde están funcionando los diferentes servicios de internet en la red de datos pública de la Universidad Nacional de Loja.

Tabla 3. Descripción del hardware de los servidores públicos

Servidor	Marca / Modelo	Características
Web Universidad	HP Proliant ML150	• Procesador: Intel Xeon 3.2 Ghz • Memoria: 1GB • Disco Duro: 100 GB

MED 1 (Módulos)	HP Compaq	• Procesador: Core 2Duo Inside • Memoria: 5GB • Disco Duro: 500 GB
MED 2 (Evaluación)	HP Compaq	• Procesador: Core 2Duo Inside • Memoria: 4GB • Disco Duro: 250 GB
Sistema Académico 1	Aopen	• Procesador: Pentium 4, 2.0 Ghz • Memoria: 512 MB • Disco Duro: 60 GB
Sistema Académico 2	Compaq Presario	• Procesador: Intel Pentium 4, 3.6 GHZ • Memoria: 512 MB • Disco Duro: 160 GB
Correo Electrónico	HP Compaq 6000 Pro MT PC	• Procesador: Intel Core 2Duo, 2.9 Ghz • Memoria: 2GB • Disco Duro: 300 GB
Radio Universitaria	HP Compaq 6000 Pro MT PC	• Memoria: 1957 MB • Disco Duro: 295 GB
Firewall	HP Proliant ML370G5	• Procesador: Intel Xeon 1.8 Ghz • Memoria: 2GB • Disco Duro: 66 GB
Elaborado por: Évelin Alvarado Otero		

Descripción de los servidores privados

Como se muestra en la figura 9, los servidores de la intranet están interconectados con el Switch cisco 2960 y existe un segmento conectado para wireless Lan (WLan). Todos estos servidores son privados, por lo que solo pueden ser accedidos desde la intranet, es decir no se pueden visualizar los servicios de Internet desde afuera.

A continuación se detallan los servidores que se encuentran implementados y en funcionamiento en el cuarto de telecomunicaciones como son: Sistema de nombres (DNS), Asignación de direcciones IP (dhcp), proxy wireless, Sistema Académico (SGA). Etc.

- **Sistema de Nombres:** permite la resolución directa o inversa de las direcciones de Internet, se encuentra configurado como DNS primario haciendo uso del domino unl.edu.ec.

- **Asignación de direcciones IP:** este servidor asigna a los clientes (pc, entre otros) automáticamente por medio de direcciones MAC los parámetros de configuración de la red como son: IP, máscara de subred, puerta de enlace.
- **Proxy Wireless (uno solo):** equipo intermediario que intercepta peticiones de navegación de usuarios que utilizan cualquier dispositivo que se conecta de forma inalámbrica a la red de la Universidad.
- **Sistema de Gestión Académico:** el Sistema de Gestión Académico, facilita a los estudiantes, docentes y funcionarios cumplir sus actividades académicas de forma eficaz y eficiente.

En la tabla 4, se detalla el hardware de los equipos en donde están funcionando los diferentes servicios de internet en la red de datos de la intranet de la Universidad Nacional de Loja.

Tabla 4. Descripción del hardware de los servidores privados

Servidor	Marca / Modelo	Características
DNS- DHCP	HP Proliant ML150	• Procesador: Intel Xeon 3.2 Ghz • Memoria: 1GB • Disco Duro: 100 GB
Proxys	HP Compaq	• Procesador: Pentium D 3.4 Ghz • Memoria: 1GB • Disco Duro: 145 GB
Proxy Wireless (transparente)	HP Compaq	• Procesador: Pentium D 3.4 Ghz • Memoria: 2 GB • Disco Duro: 145 GB
Elaborado por: Évelin Alvarado Otero		

e.2.4 Cuarto de Telecomunicaciones

El cuarto de telecomunicaciones, figura 10, se encuentra ubicado en el cuarto piso del edificio de Administración Central bloque 2, y está a cargo de la UTI; el cuarto de telecomunicaciones se define como el espacio donde residen los equipos de telecomunicaciones, solo se admiten equipos directamente relacionados con los sistemas de telecomunicaciones, aquí se encuentran los equipos de manejo exclusivo del

administrador de red, como los routers, switchs, servidores. Su función principal es ser la base para una distribución organizada de lo que es cableado horizontal y vertical.

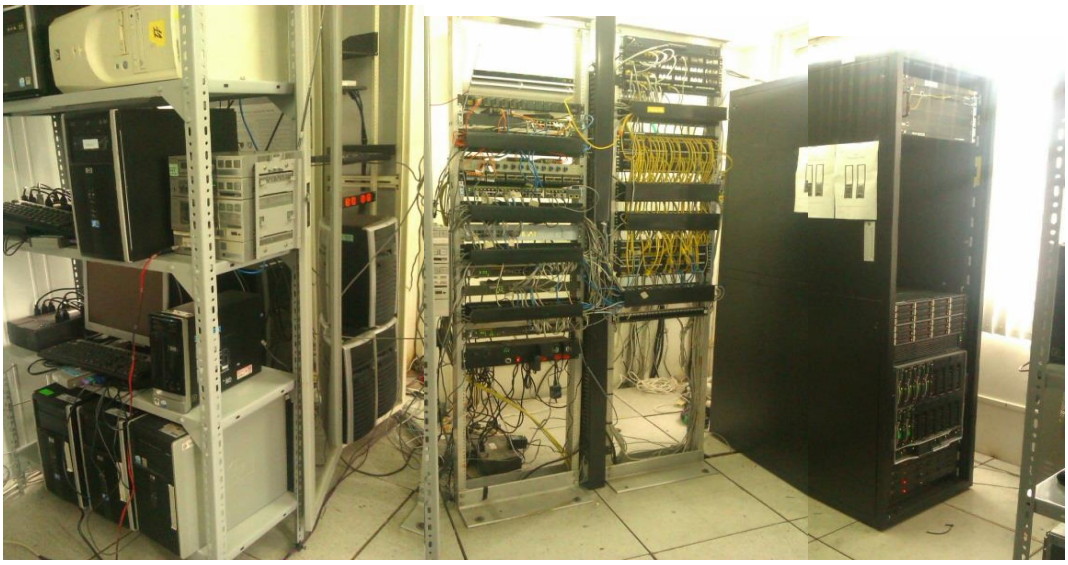


Figura 10. Cuarto de Telecomunicaciones de la Universidad

Descripción de los dispositivos de networking principales

En la tabla 5, se detalla los principales dispositivos de networking activos de la red de la Universidad Nacional de Loja con su respectiva descripción y funcionamiento.

Tabla 5. Descripción de los dispositivos de networking principales

Dispositivo	Descripción	Funcionamiento
Router Cisco 7604	Tiene la dirección IPv4 pública 192.xx.xx.xx/24	• Permite acceder a Internet comercial e Internet2 que brinda el CEDIA (Consorcio Ecuatoriano para el Desarrollo de Internet Avanzado).
Switch Cisco 2960 externo	Tiene la dirección IPv4 pública 192.xx.xx.xx/24	• Este dispositivo opera en la capa 2 del modelo OSI facilitando la interconexión de dos o más segmentos de red. • Una de las Interfaces Fast Ethernet 1000 Mbps se conecta al Router Cisco 7604. • Los puertos 10/100 Mbps se conectan con los servidores públicos (Firewall, MED, SGA, Web. Etc.)

Switch Cisco 2960 interno	Tiene la dirección IPv4 privada 172.xx.xx.xx/19	• Una de las interfaces Fast Ethernet 10/100 Mbps se conecta directamente con el Firewall HP Proliant facilitando el acceso al Internet. • Algunos puertos se conectan con los diferentes servicios de internet como lo son dns, dhcp, proxis, SGA. Etc.
Firewall HP Proliant	Tiene dos direcciones de red: Dirección IPv4 pública 192.xx.xx.xx Dirección IPv4 privada 172.xx.xx.xx	• Cada una de las interfaces Fast Ethernet 10/100 se conecta a los Switch 2960 interno y externo respectivamente. • Está configurado con NAT lo que permite a los equipos con direcciones IP privadas compartan una dirección IP enrutable (IP pública). • Este equipo posee las políticas de seguridad (iptables), enrutamiento hacia el exterior y VPN (Red Privada Virtual).
Elaborado por: Évelin Alvarado Otero		

e.2.5 Direccionamiento IPv4 público de la Universidad Nacional de Loja

La Universidad posee un rango de direcciones IPv4 públicas que ha sido asignada por NIC.EC (Registro de Nombres de Dominio del Ecuador), estas direcciones permiten a la universidad brindar sus servicios de internet al mundo entero, como lo son cursos, sistema de gestión académico, radio universitaria, etc. En la tabla 6, se detalla el direccionamiento IPv4 público de clase C.

Tabla 6. Descripción de parámetros IPv4 de la red pública

DESCRIPCIÓN	ESPECIFICACIÓN
Red Clase C	192.xx.xx.xx/24
Dominio	unl.edu.ec
Mascara de subred	255.255.255.0
Dirección de Broadcast	192.xx.xx.xx
Puerta de enlace	192.xx.xx.xx
Servidor DNS primario (proveedor)	200.xx.xx.xx
Servidor DNS secundario (proveedor)	200.xx.xx.xx
Elaborado por: Évelin Alvarado Otero	

e.2.6 Direccionamiento IPv4 de Intranet de la Universidad Nacional de Loja

La Universidad actualmente posee un direccionamiento IPv4 privado de clase B que se usa en los dispositivos de networking, equipos finales, servidores, puntos de acceso inalámbrico, etc. En la tabla 7, se detalla el direccionamiento IPv4 de la UNL.

Tabla 7. Descripción de parámetros IPv4 de la intranet

DESCRIPCIÓN	ESPECIFICACIÓN
Red Clase B	172.xx.xx.xx/16
Dominio	unl.edu.ec
Subred de la Universidad	172.xx.xx.xx/19
Máscara de subred	255.255.224.0
Dirección de Broadcast	172.xx.xx.xx
Puerta de enlace	172.xx.xx.xx
Servidor DNS	172.xx.xx.xx
Elaborado por: Évelin Alvarado Otero	

e.2.7 Situación actual de la Red LAN del AEIRNNR

Para llevar a cabo la implementación del segmentador en el área de energía fue necesario realizar un levantamiento de línea base general de datos, equipos y tráfico actual de la red en dicha área**.**

El tramo de fibra óptica (multimodo) va desde administración central hasta el ÁREA DE ENERGÍA, este llega al bloque 1 donde funciona la Dirección del Área, en el cual se conecta a un switch Cisco 2960 en el cual está conectado el servidor proxy, desde este switch se conecta mediante enlace de fibra óptica (el cual en la actualidad se encuentra dañado) al bloque de la carrera de geología (al Museo de Rocas) a un switch 3Com, igualmente mediante fibra hasta la ex secretaria del área bloque 4, desde ahí hasta el bloque 5 que es la biblioteca del área a un switch 3Com SuperStack 4500 de 24 puertos, para luego con cable UTP dirigirse en cascada al bloque 6, terminando así con la interconexión entre los bloques. Del mismo modo, del bloque de la dirección del área

se conecta a la MED a un switch D-Link de 24 puertos, del cual a su vez existe una cascada hacia Artes y el taller eléctrico.

El número actual de usuarios finales de la red LAN del área de Energía es de 250, y una capacidad de 137 usuarios para el Internet inalámbrico. Luego de una inspección al estado actual de la red en el área de energía, se pudo realizar un diagrama de cómo está conformada la red. En la figura 11, se muestra la interconexión de bloques del área.

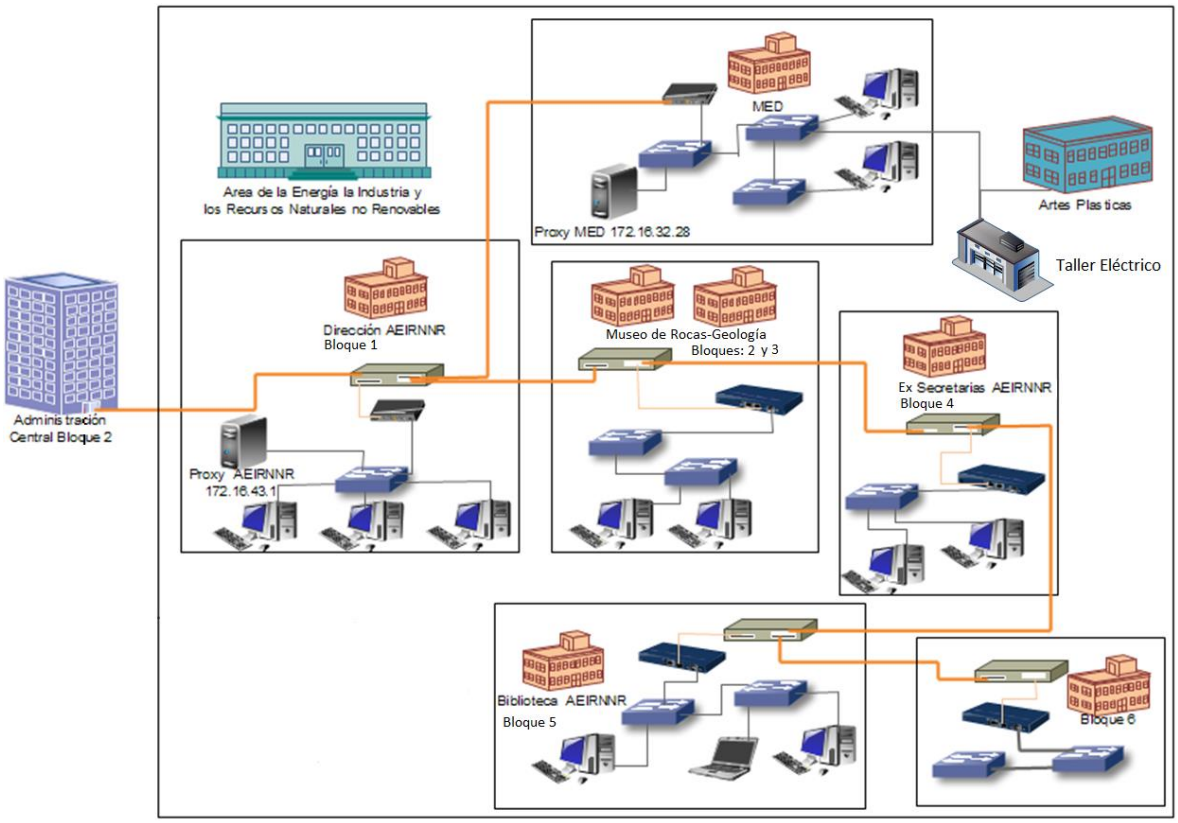


Figura 11. Distribución LAN área de Energía

e.2.7.1 Sistema Actual de Control a Páginas Web

El sistema actual de control a páginas web con el que cuenta la Universidad es el DansGuardian como un filtro de contenido de sitios web, su principal objetivo es filtrar páginas web en base a un conjunto de criterios, este a su vez trabaja conjuntamente con el servidor proxy SQUID , presente en la red local.

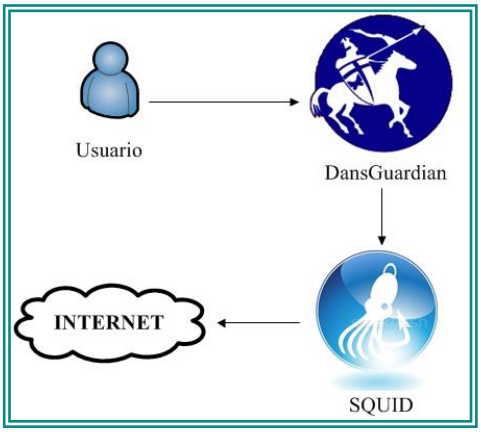


Figura 12. Esquema de funcionamiento de DansGuardian y Squid

DansGuardian trabaja en medio del proxy y del cliente, interceptando y modificando la comunicación entre ambos, tomando las medidas previas para facilitar el filtrado de páginas visitadas por el usuario, como se muestra en la figura 12; su utilización es de especial interés en centros educativos.

e.2.7.2 Características de DansGuardian

<<La herramienta DansGuardian es código abierto, está desarrollada en C++ y permite una configuración flexible adaptándose a las necesidades del usuario. Al instalar el paquete la configuración por defecto ya limita las visitas a páginas prohibidas, pero dispone de gran cantidad de archivos de configuración para llevar a cabo un ajuste del servicio más personalizado>>[15].

Así funciona el mecanismo: el usuario, mediante el navegador web, realiza peticiones de páginas, estas son interceptadas por DansGuardian, únicamente son redireccionadas al SQUID aquellas solicitudes que superan el filtrado, caso contrario aparecerá la siguiente pantalla mostrada en la figura 13.

Figura 13. Pantalla de acceso denegado en DansGuardian dentro del campus universitario

DansGuardian <<acepta peticiones en el puerto 8080 y las redirecciona al proxy SQUID, que escucha en el puerto 3128. Por lo tanto, cuando una petición entra por el puerto 8080, DansGuardian la filtra y la pasa al proxy SQUID por el puerto 3128>>[15], como se muestra en la figura 14. Por lo tanto, es de suma importancia que el puerto 8080 no esté siendo utilizado por ningún otro servicio.

Figura 14. Puertos de DansGuardian y Squid

Ministerio de Educación, Cultura y Deporte. *"DansGuardian: filtro de contenidos"*. Gobierno de España. Disponible en: <http://recursostic.educacion.es/observatorio/web/es/software/software-general/524-dansguardian-filtro-de-contenidos>. [En línea]. [Última actualización 20 de Noviembre del 2007]. Consulta: Agosto del 2012.

Si como resultado de filtrado se obtiene (obedeciendo a la configuración de los filtros) que una página web no pudo ser descargada, se muestra al usuario el mensaje correspondiente al "Acceso Denegado" tal como se muestra en la figura 13. Las páginas que son seguras, aquellas que utilizan el protocolo https (puerto 443), igualmente son redirigidas. Para evitar que los usuarios se salten el proceso de filtrado, el administrador de red asegura su funcionamiento con la aplicación de IPTABLES.

e.2.7.3 Métodos de Filtrado

Lo siguiente son los métodos de filtrado que DansGuardian utiliza para mejorar su objetivo de bloqueo:

1. Filtro comprobando que las extensiones de archivos y los tipos Extensiones Multipropósito de Correo de Internet prohibidos (MIME), no estén en una lista.
2. Filtrar de acuerdo con las (URLs) Localizador de Recursos Uniforme, incluyendo expresiones regulares.
3. Y el método adoptado por la Universidad, que es el de trabajar con listas blancas y listas negras.

Los tipos MIME <<son una serie de convenciones o especificaciones dirigidas al intercambio a través de Internet de todo tipo de archivos (texto, audio, vídeo, etc.) de forma transparente para el usuario>>[2].

Dentro de una lista con palabras prohibidas, DansGuardian lo que hace es comparar el contenido de las páginas web. En la lista se encuentran palabras relacionadas con la pornografía, terrorismo, alcohol y demás contenido no deseado. <<Todos estos métodos se apoyan en la utilización de unos archivos de filtros que almacenan frases, palabras, URLs, etc, cuyo acceso queda prohibido>>[22].

En la actualidad, la conciliación del DansGuardian con respecto a la libertad de comunicación tornan a la herramienta de protección, como obsoleta; las restricciones

impuestas por este filtro, sobre Internet, puede ser inoportuna en algunos casos, tal es el ejemplo de la situación actual en la Universidad cuando un usuario navega en Internet, debido a la rigurosidad del mecanismo de protección, la excesiva restricción al momento de realizar consultas, por parte de los estudiantes, docentes o personal administrativo, imposibilitan el desarrollo de la investigación.

f. RESULTADOS

f.1 Medición del Consumo de Ancho de Banda de la Universidad Nacional de Loja

Dentro de la operación de sistemas de información, un factor de medida muy importante es el de la disponibilidad de los servicios. Para poder brindar una alta disponibilidad, es necesario disponer de herramientas que permitan medirla y que ayuden al administrador a detectar posibles errores o fallos que la afecten. Para la medición del consumo de Ancho de Banda de la Universidad se hace uso de dos herramientas de software: Nagios y Cacti.

Nagios: software libre para monitorización que permite tener conocimiento en cada instancia del día del estado del sistema; genera alertas y alarmas cuando el funcionamiento de los mismos no es el esperado. La recepción de alarmas pueden recibirse mediante correo electrónico, donde consta una vista global con el estado de todos los servicios definidos para cada elemento, verde: (Up) arriba y rojo: (Down)caído. Cualquier sistema que soporte Protocolo Simple de Administración de Red (SNMP), es susceptible de ser monitorizado con Nagios (switches, routers, puntos de acceso, servidores de cualquier tipo, etc). La visualización y gestión de la herramienta es por medio de la web.

Cacti: software que monitoriza cualquier equipo de red que soporte el protocolo SNMP, ya sean estos *switch*, *router* o servidores Linux. Brinda la visualización de 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. La visualización y gestión de la herramienta se da mediante la web.

En la figura 15, se muestra toda la granja de servidores de la Universidad en el Nagios, indicando que el estado de los servidores estaba funcionando para el día de las mediciones de consumo de ancho de banda proporcionadas por el Cacti.

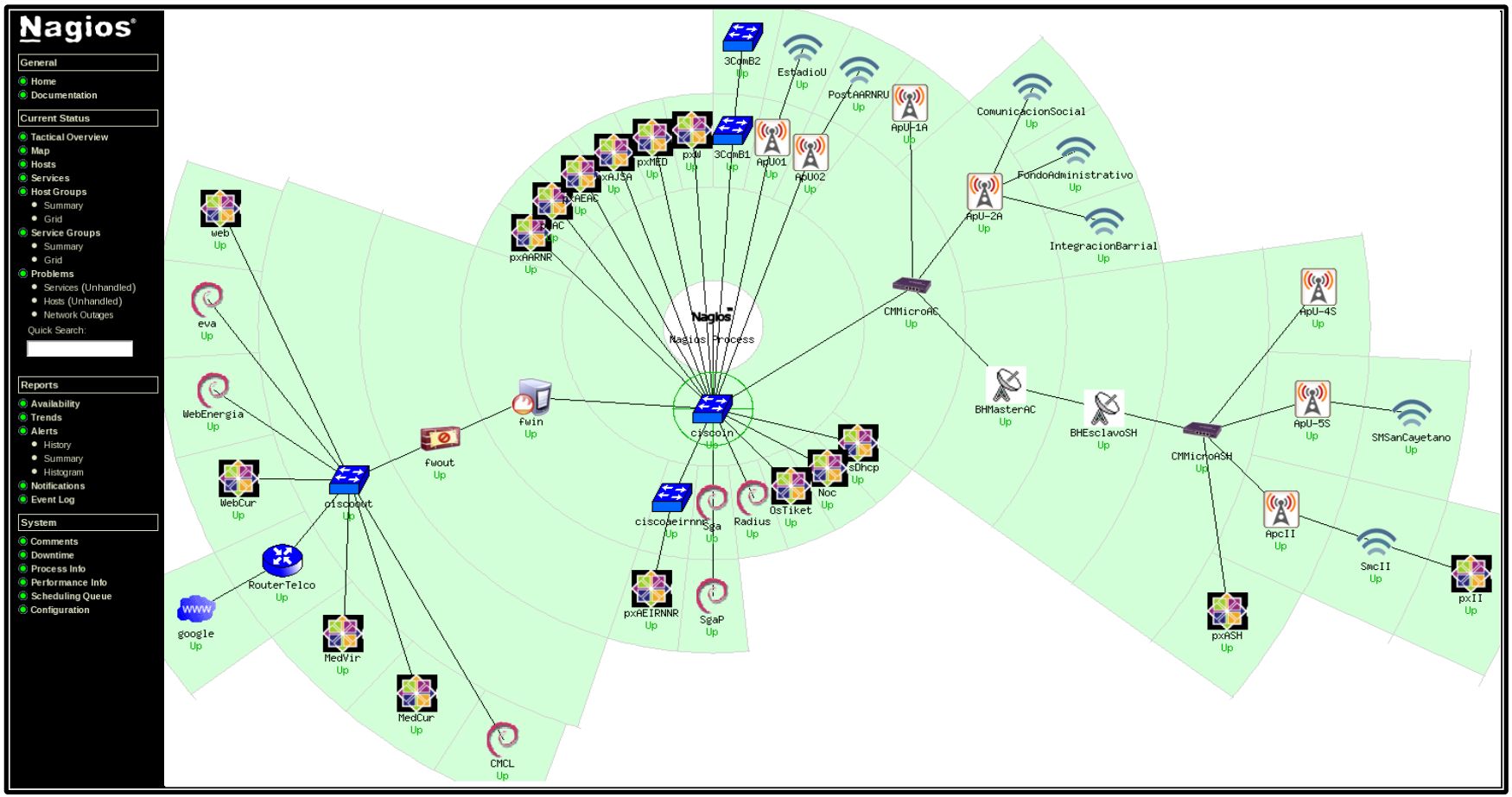


Figura 15. Red de la UNL monitoreada por Nagios

f.1.1 Consumo Ancho de Banda Firewall Principal

Una vez demostrado que los servidores estaban en funcionamiento, se procedió a la toma de la lectura del Firewall principal de la UNL, datos proporcionados por el Cacti, son datos en los cuales el sistema ha estado realizando dicho monitoreo, del resto de meses que se observan vacíos, el software no ha estado realizando monitoreo.

CONSUMO PROMEDIO DE 24 HORAS: (Miércoles 24, 12:00-Jueves 25, 12:00) Octubre 2012

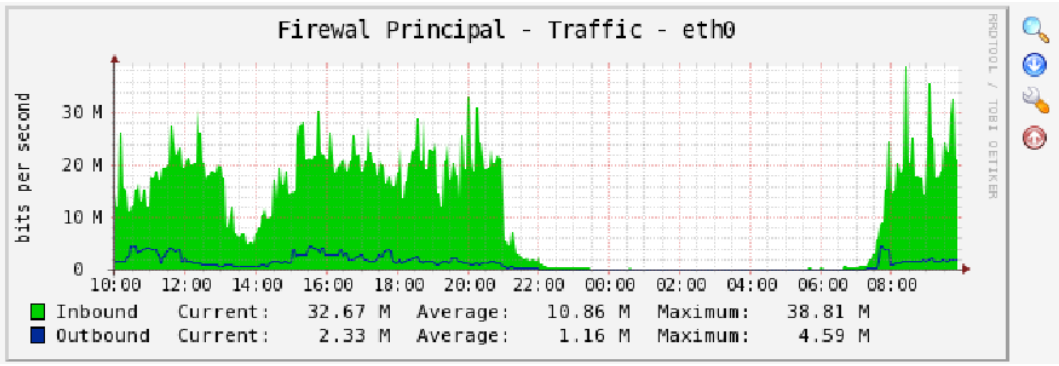


Figura 16. Firewall principal (Consumo AB: 24 horas)

En la figura 16, se observa el consumo de un día, en el caso del Firewall principal, podemos ver que existe un consumo máximo de 38.81Mbps de bajada y un máximo de 4.59Mbps de subida.

CONSUMO PROMEDIO DE UNA SEMANA: Semanas 42: (Jueves 18 y Viernes 19), 43(Lunes 22, Martes 23, Miércoles 24 y Jueves 25) Octubre 2012

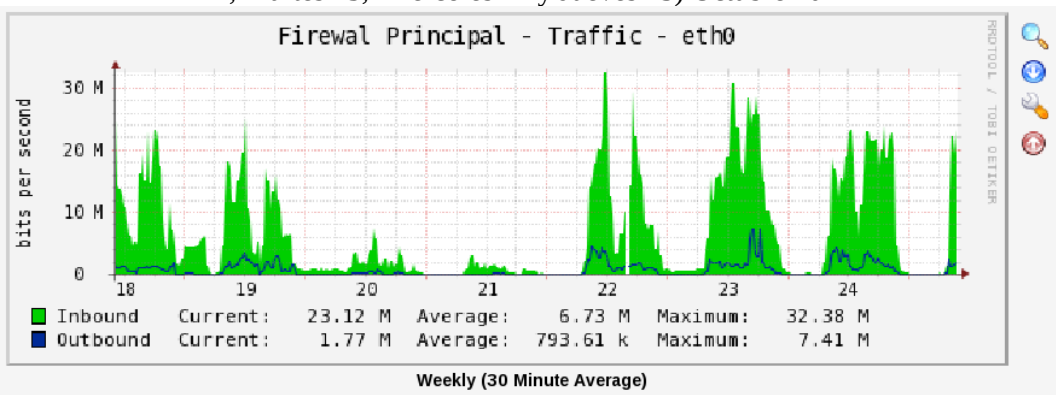


Figura 17. UNL Firewall principal (Consumo AB: 1 semana)

En la figura 17, se observa el consumo de una semana, en el caso del Firewall principal, podemos ver que existe un consumo máximo de 32.38 Mbps de bajada y un máximo de 7.41 Mbps de subida.

CONSUMO PROMEDIO DE 1 MES: Semanas 39-42 (24 Septiembre- 21 Octubre 2012)

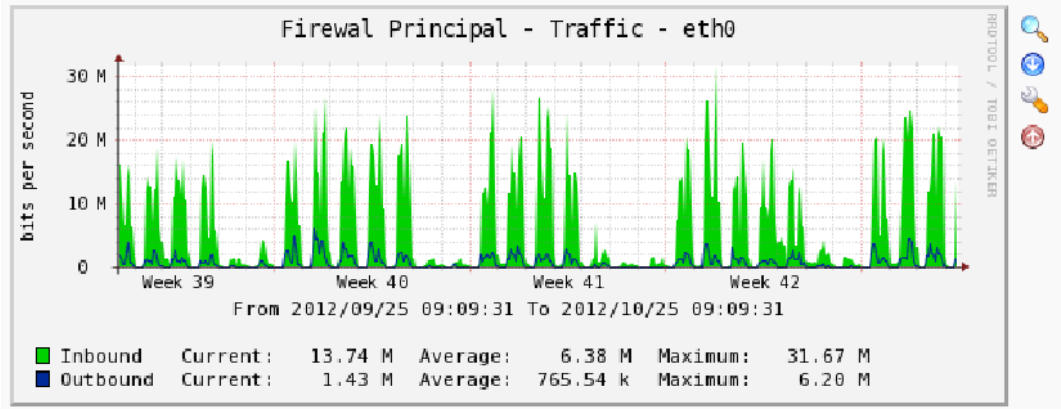


Figura 18. UNL Firewall principal (Consumo AB: 1 mes)

En la figura 18, se observa el consumo de un mes, en el caso del Firewall principal, podemos ver que existe un consumo máximo de 31.67 Mbps de bajada y un máximo de 6.20 Mbps de subida.

CONSUMO PROMEDIO DE 2 MESES: Semanas 35-42 (27 Agosto-21 Octubre 2012)

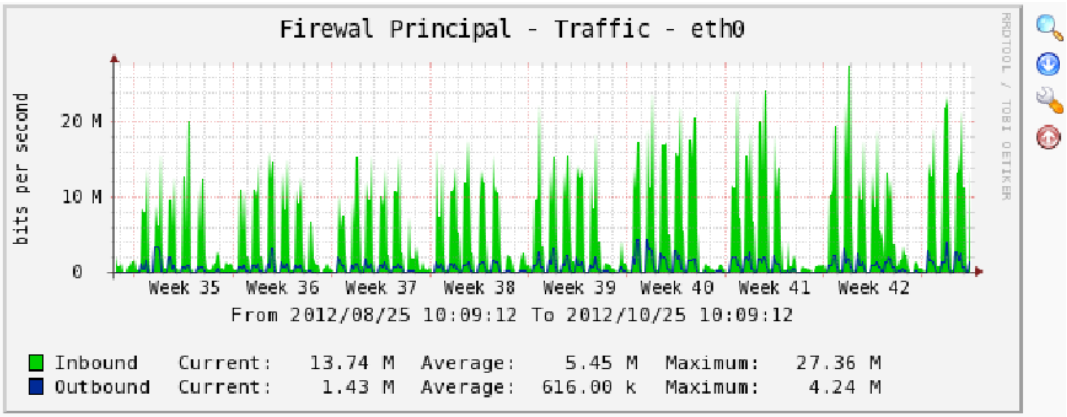


Figura 19. UNL Firewall principal (Consumo AB: 2 meses)

De la figura 19, se observa el consumo de dos meses, en el caso del Firewall principal, podemos ver que existe un consumo máximo de 27.36 Mbps de bajada y un máximo de 4.24 Mbps de subida.

CONSUMO PROMEDIO DE 1 AÑO: Octubre 2011/2012

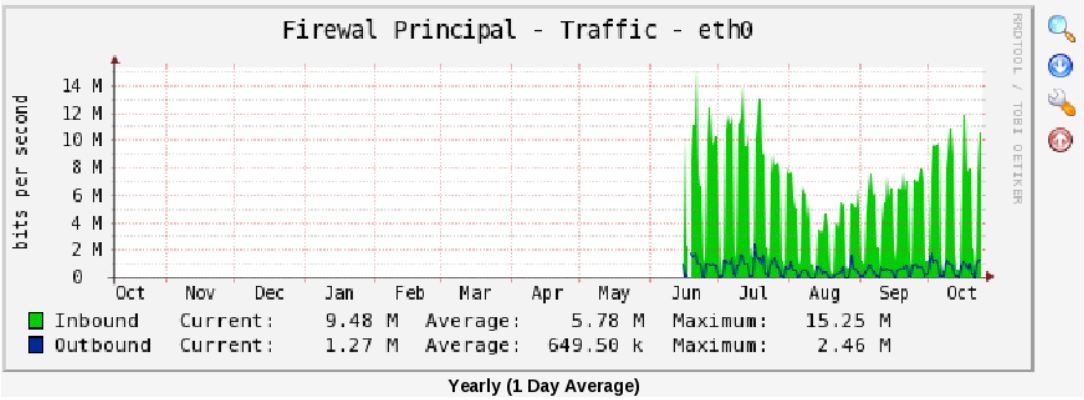


Figura 20. UNL Firewall principal (Consumo AB: 4 meses)

De la figura 20, se observa el consumo de un año, en el caso del Firewall principal, podemos ver que existe un consumo máximo de 15.25 Mbps de bajada y un máximo de 2.46 Mbps de subida.

En la tabla 8, se muestra el resumen de datos recopilados del consumo de AB (ancho de banda) del Firewall principal de la UNL.

Tabla 8. Resultados de Consumo de AB en UNL

UNL FIREWALL PRINCIPAL		
	AB (Mbps**) Bajada**	**AB (**Mbps**) Subida**
Consumo (24 horas)	38,81	4,59
Consumo (1 semana)	32,38	7,41
Consumo (1 mes)	31,67	6,20
Consumo (2 meses)	27,36	4,24
Consumo (4 meses)	15,25	2,46
Elaborado por: Évelin Alvarado Otero		

f.1.2 Consumo de ancho de banda por áreas

Una vez analizado el consumo de ancho de banda promedio de toda la Universidad del firewall principal, se procede a la lectura de los datos que proporciona cada proxy de las áreas. En vista de que el *Cacti* no ha sido activo en algunos meses, para el cálculo del ancho de banda asignado para cada área (como se verá más adelante), sólo se tomarán en cuenta los meses que se encuentran monitoreados. A manera de observación, los datos para los proxys de: Educativa, Jurídica, Agropecuaria, Salud, Energía, Med, Idiomas y Wireless respectivamente, no arrojan datos asimétricos, lo cual muestra que no se realiza un monitoreo calibrado al sistema. Siendo únicamente el dato de subida, un dato no real.

PROXY EDUCATIVA

CONSUMO PROMEDIO DE 24 HORAS: (Lunes 10 Diciembre 2012, 8:00-16:00)

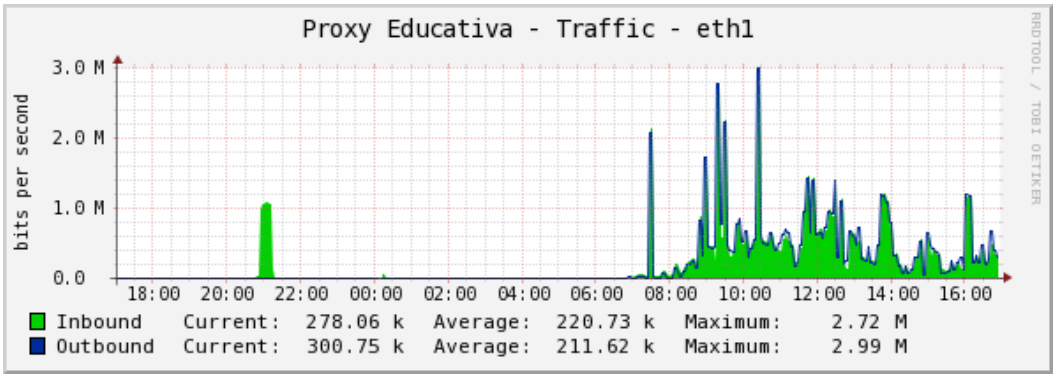


Figura 21. Proxy Educativa (Consumo AB: 24 horas)

En la figura 21, se observa el consumo de un día, en el caso del proxy educativa, podemos ver que existe un consumo máximo de 2.72 Mbps de bajada y un máximo de 2.99 Mbps de subida.

CONSUMO PROMEDIO DE UNA SEMANA: Semana 50: (Lunes 03-Lunes 10 Diciembre

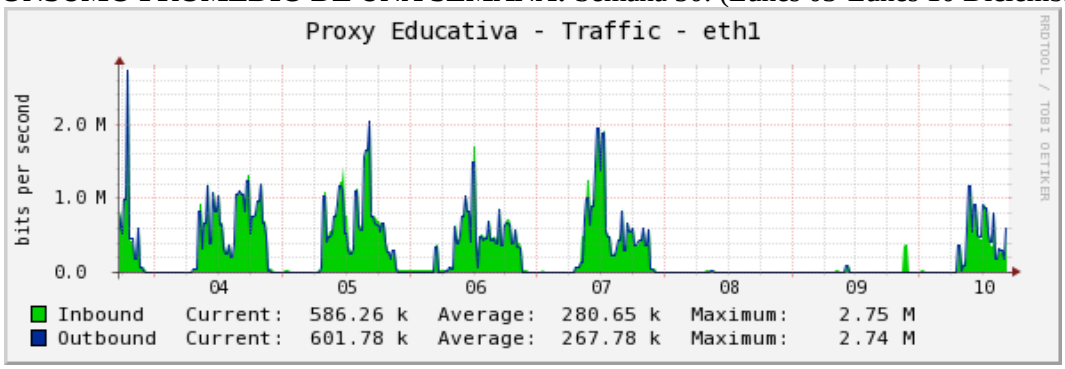


Figura 22. Proxy Educativa (Consumo AB: 1 semana)

En la figura 22, se observa el consumo de una semana, en el caso del proxy educativa, podemos ver que existe un consumo máximo de 2.75 Mbps de bajada y un máximo de 2.74 Mbps de subida.

CONSUMO PROMEDIO DE 1 MES: Semanas 48, 49, 50 (26 Noviembre- 10 Diciembre 2012)

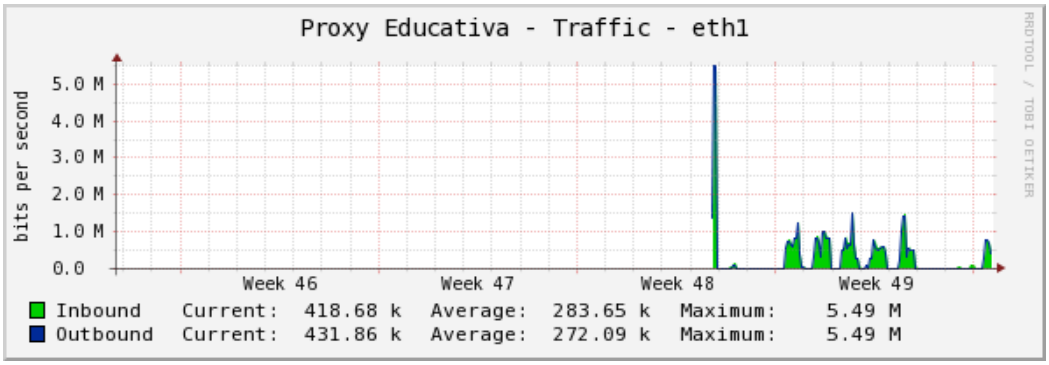


Figura 23. Proxy Educativa (Consumo AB: 1 mes)

En la figura 23, se observa el consumo de un mes, en el caso del proxy educativa, podemos ver que existe un consumo máximo de 5.49M de bajada y un máximo de 5.49M de subida.

En la tabla 9, se muestra el resumen de datos recopilados del consumo de ancho de banda del Proxy de Educativa.

Tabla 9. Resultados de Consumo de AB Educativa

PROXY EDUCATIVA		
	AB (Mbps**) Bajada**	**AB (**Mbps**) Subida**
Consumo (24 horas)	2,72	2,99
Consumo (1 semana)	2,75	2,74
Consumo (1 mes)	5,49	5,49
Elaborado por: Évelin Alvarado Otero		

PROXY JURÍDICA

CONSUMO PROMEDIO DE UNA SEMANA: Semana 49: (Lunes 03-Lunes 10 Diciembre de 2012)

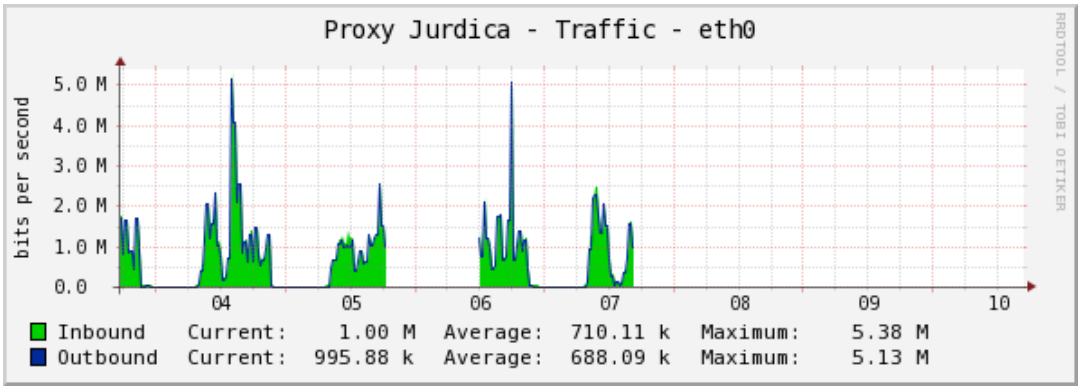


Figura 24. Proxy Jurídica (Consumo AB: 24 horas)

En la figura 24, se observa el consumo de una semana, en el caso del proxy jurídica, podemos ver que existe un consumo máximo de 5.38 Mbps de bajada y un máximo de 5.13 Mbps de subida.

CONSUMO PROMEDIO DE 1 MES: Semanas 46, 48, 49 (11 Noviembre- 7 Diciembre 2012)

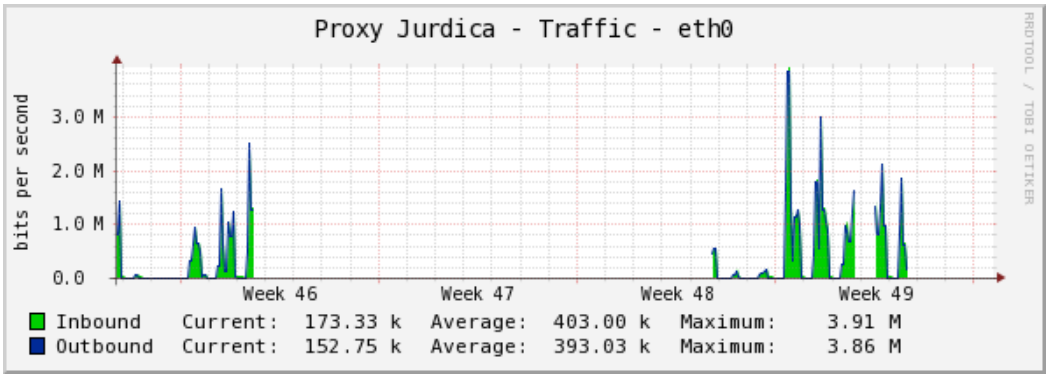


Figura 25. Proxy Jurídica (Consumo AB: 1 semana)

En la figura 25, se observa el consumo de un mes, en el caso del proxy jurídica, podemos ver que existe un consumo máximo de 3.91 Mbps de bajada y un máximo de 3.86 Mbps de subida.

CONSUMO PROMEDIO DE UN AÑO: Diciembre 2011-Diciembre 2012

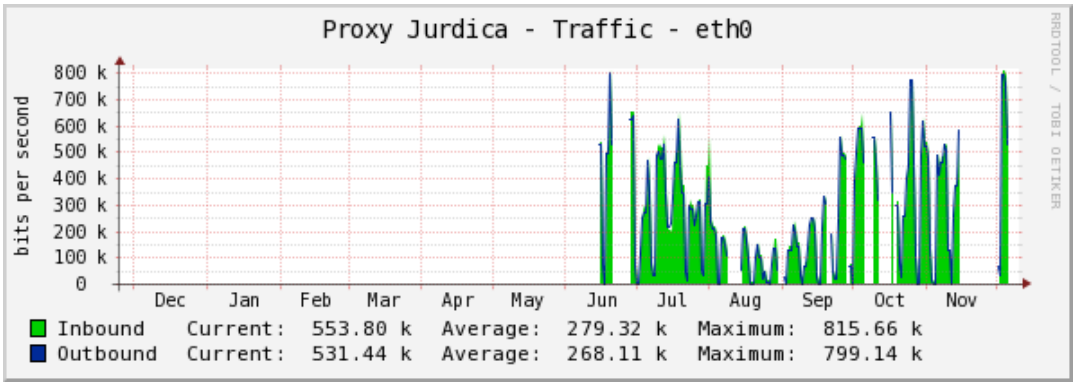


Figura 26. Proxy Jurídica (Consumo AB: 1 año)

En la figura 26, se observa el consumo de un año, en el caso del proxy jurídica, podemos ver que existe un consumo máximo de 815.66 kbps de bajada y un máximo de 799.14 kbps de subida.

En la tabla 10, se muestra el resumen de datos recopilados del consumo de AB (ancho de banda) del Proxy de Jurídica.

Tabla 10. Resultados de Consumo de AB Jurídica

PROXY JURÍDICA		
	AB (Mbps**) Bajada**	**AB (**Mbps**) Subida**
Consumo (1 semana)	5,38	5,13
Consumo (1 mes)	3,91	3,86
Consumo (1 año)	815,66 kbps	799,14 kbps
Elaborado por: Évelin Alvarado Otero		

PROXY AGROPECUARIA

CONSUMO PROMEDIO DE 24 HORAS: (Lunes 10 Diciembre 2012, 8:00-Lunes 10 Diciembre 2012, 16:00)

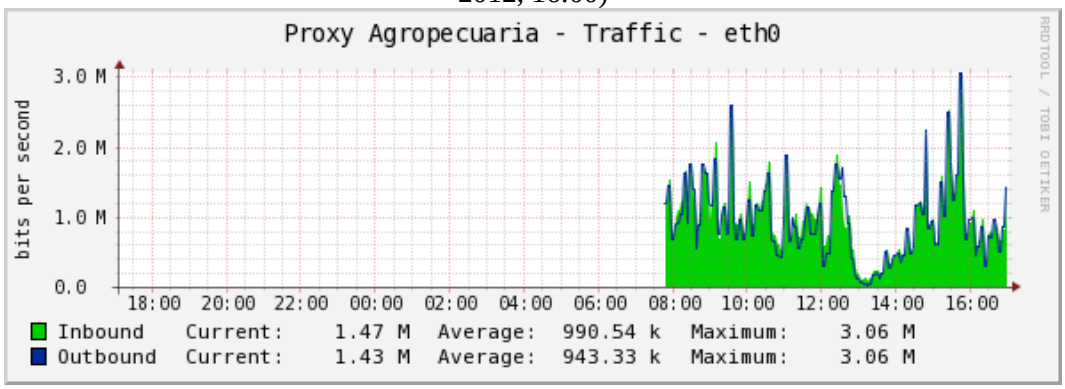


Figura 27. Proxy Agropecuaria (Consumo AB: 24 horas)

En la figura 27, se observa el consumo de un día, en el caso del proxy agropecuaria, podemos ver que existe un consumo máximo de 3.06 Mbps de bajada y un máximo de 3.06 Mbps de subida.

CONSUMO PROMEDIO DE UNA SEMANA: Semana 49: (Lunes 03-Lunes 10 Diciembre de 2012)

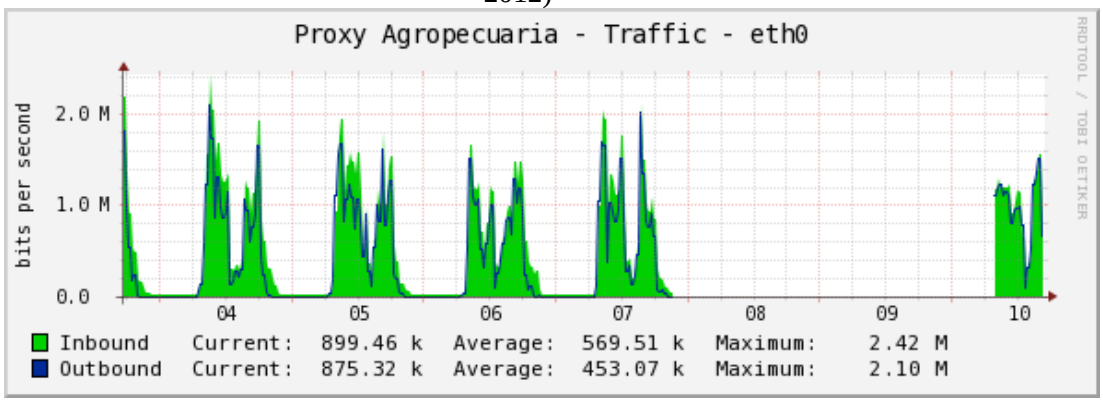


Figura 28. Proxy Agropecuaria (Consumo AB: 1 semana)

En la figura 28, se observa el consumo de una semana, en el caso del proxy agropecuaria, podemos ver que existe un consumo máximo de 2.42 Mbps de bajada y un máximo de 2.10 Mbps de subida.

CONSUMO PROMEDIO DE 1 MES: Semanas 46, 48, 49 (11 Noviembre- 7 Diciembre 2012)

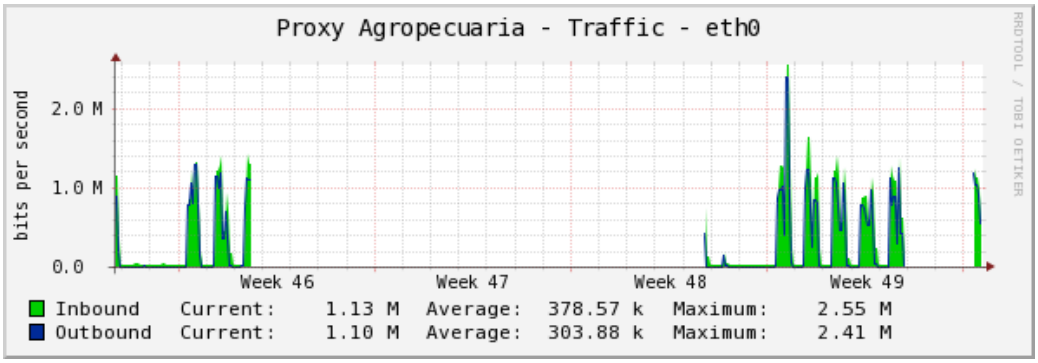


Figura 29. Proxy Agropecuaria (Consumo AB: 1 mes)

En la figura 29, se observa el consumo de un mes, en el caso del proxy agropecuaria, podemos ver que existe un consumo máximo de 2,55 Mbps de bajada y un máximo de 2,41 Mbps de subida.

CONSUMO PROMEDIO UN AÑO: Diciembre 2011-Diciembre 2012

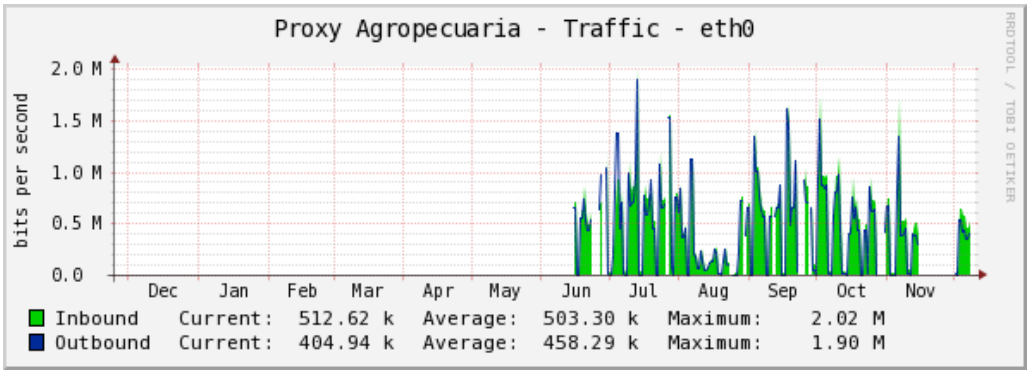


Figura 30. Proxy Agropecuaria (Consumo AB: 1 año)

En la figura 30, se observa el consumo de un año, en el caso del proxy agropecuaria, podemos ver que existe un consumo máximo de 2.02 Mbps de bajada y un máximo de 1.90 Mbps de subida.

En la tabla 11, se muestra el resumen de datos recopilados del consumo de AB (ancho de banda del Proxy de Agropecuaria.

Tabla 11. Resultados de Consumo de AB Agropecuaria

PROXY AGROPECUARIA		
	AB (Mbps**) Bajada**	**AB (**Mbps**) Subida**
Consumo (1 día)	3,06	3,06

Consumo (1 semana)	2,42	2,10
Consumo (1 mes)	2,55	2,41
Consumo (1 año)	2,02	1,90
Elaborado por: Évelin Alvarado Otero		

PROXY SALUD

CONSUMO PROMEDIO DE 24 HORAS: (Lunes 10 Diciembre 2012, 8:00-Lunes 10 Diciembre 2012, 16:00)

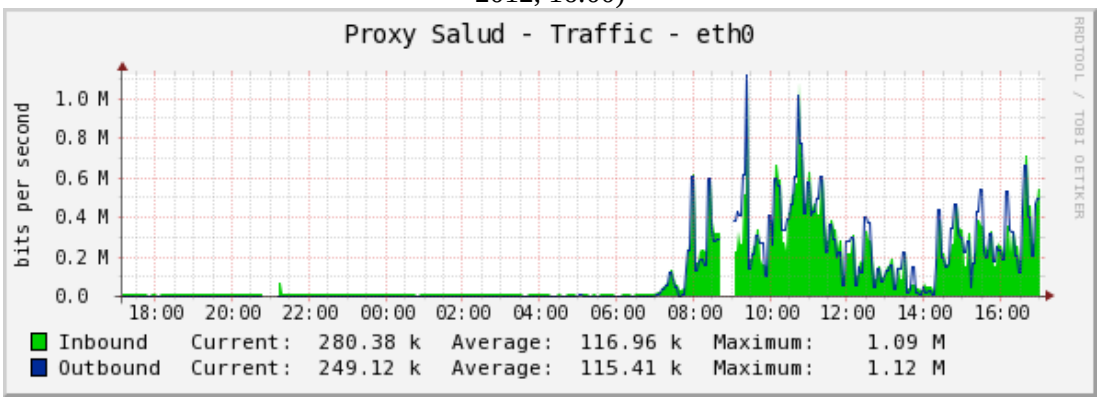


Figura 31. Proxy Salud (Consumo AB: 24 horas)

En la figura 31, se observa el consumo de un día, en el caso del proxy salud, podemos ver que existe un consumo máximo de 1.09 Mbps de bajada y un máximo de 1.12 Mbps de subida.

CONSUMO PROMEDIO DE UNA SEMANA: Semana 49: (Lunes 03-Lunes 10 Diciembre de 2012)

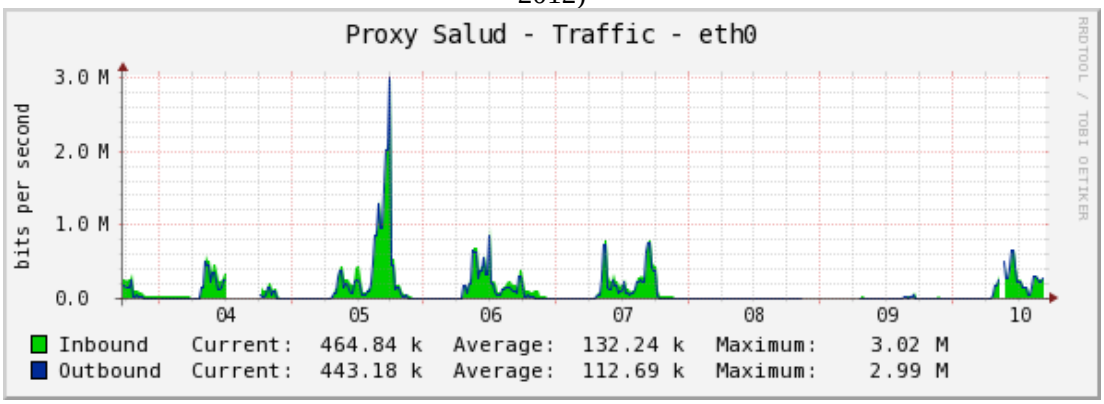


Figura 32. Proxy salud (Consumo AB: 1 semana)

En la figura 32, se observa el consumo de una semana, en el caso del proxy salud, podemos ver que existe un consumo máximo de 3.02 Mbps de bajada y un máximo de 2.99 Mbps de subida.

CONSUMO PROMEDIO DE 1 MES: Semanas 46, 48, 49 (11 Noviembre-7 Diciembre 2012)

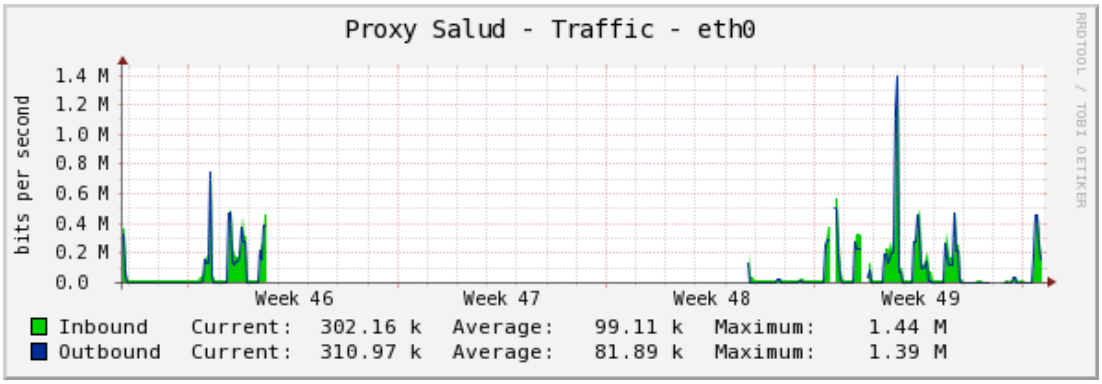


Figura 33. Proxy Salud (Consumo AB: 1 mes)

En la figura 33, se observa el consumo de un mes, en el caso del proxy salud, podemos ver que existe un consumo máximo de 1.44 Mbps de bajada y un máximo de 1.39 Mbps de subida.

CONSUMO PROMEDIO UN AÑO: Diciembre 2011-Diciembre 2012

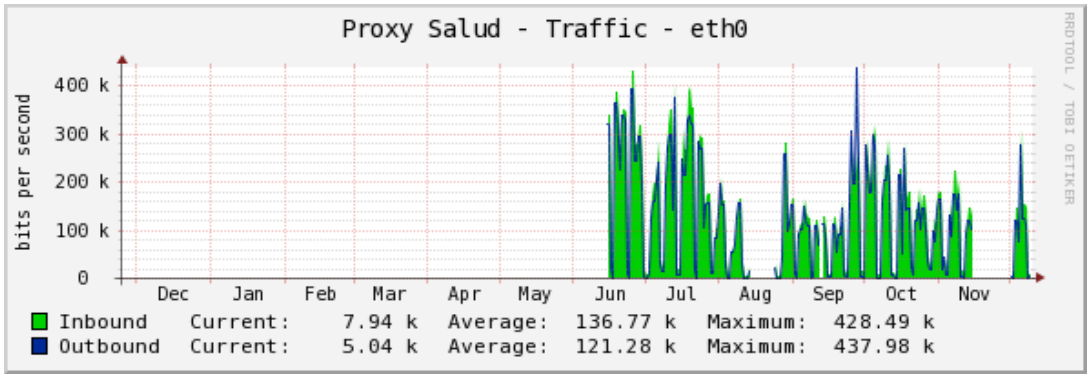


Figura 34. Proxy Salud (Consumo AB: 1 año)

En la figura 34, se observa el consumo de un año, en el caso del proxy salud, podemos ver que existe un consumo máximo de 428.49 Kbps de bajada y un máximo de 437.98 Kbps de subida.

En la tabla 12, se muestra el resumen de datos recopilados del consumo de ancho de banda del Proxy de Salud.

Tabla 12. Resultados de Consumo de AB Salud

PROXY SALUD		
	AB (Mbps**) Bajada**	**AB (**Mbps**) Subida**
Consumo (1 día)	1,09	1,12
Consumo (1 semana)	3,02	2,99
Consumo (1 mes)	1,44	1,39
Consumo (1 año)	428,49 kbps	437,98 kbps
Elaborado por: Évelin Alvarado Otero		

PROXY MED

CONSUMO PROMEDIO DE 24 HORAS: (Jueves 10 Enero 2013, 12:00-Viernes 11 Enero 2013, 10:00)

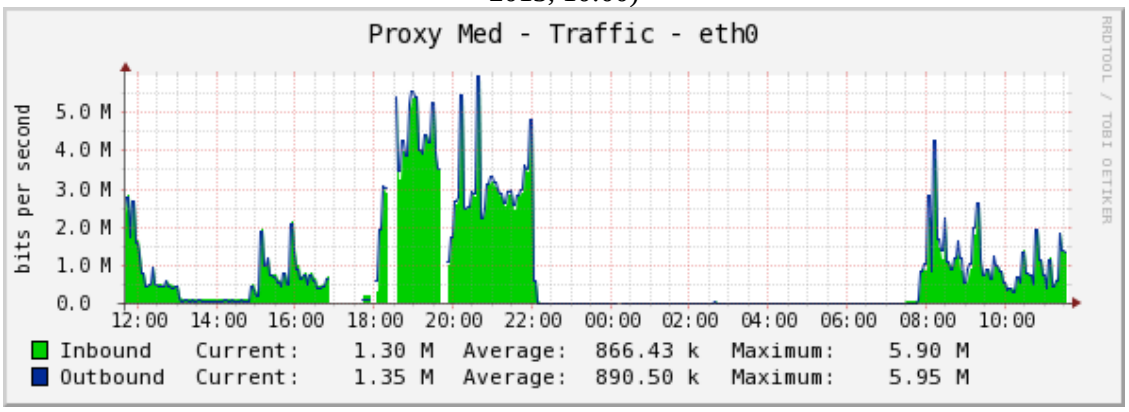


Figura 35. Proxy MED (Consumo AB: 24 horas)

En la figura 35, se observa el consumo de ancho de banda de un día, en el caso del proxy med, podemos ver que existe un consumo máximo de 5.90 Mbps de bajada y un máximo de 5.95 Mbps de subida.

CONSUMO PROMEDIO DE UNA SEMANA: Semana 02: (Viernes 04-Jueves 10 Enero 2013)

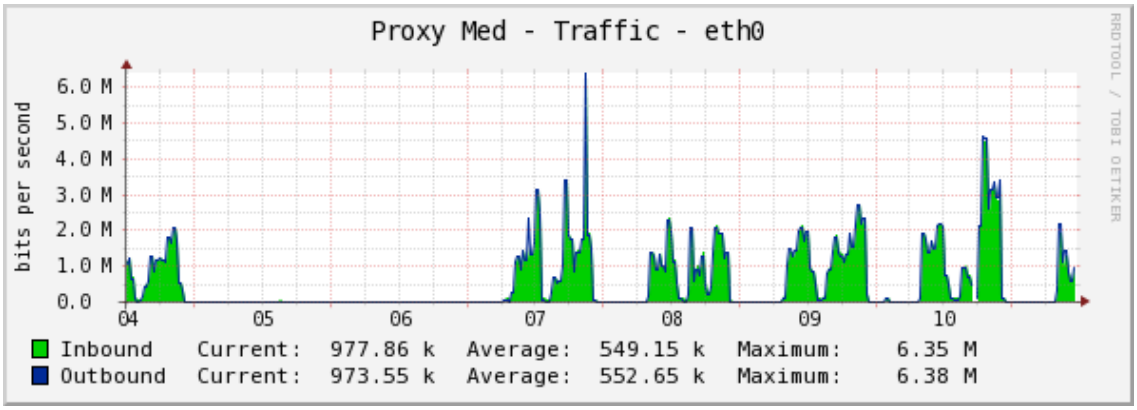


Figura 36. Proxy MED (Consumo AB: 1 semana)

En la figura 36, se observa el consumo de ancho de banda de una semana, en el caso del proxy med, podemos ver que existe un consumo máximo de 6.35 Mbps de bajada y un máximo de 6.38 Mbps de subida.

CONSUMO PROMEDIO DE 1 MES: Semanas 50, 51, 52-01, 02 (11 Diciembre 2012-10 Enero 2013)

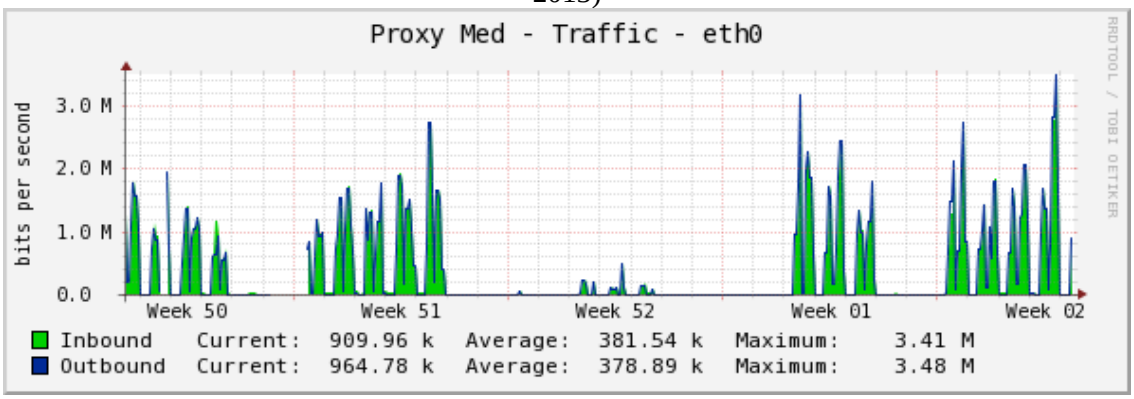


Figura 37. Proxy MED (Consumo AB: 1 mes)

En la figura 37, se observa el consumo de un mes, en el caso del proxy med, podemos ver que existe un consumo máximo de 3.41 Mbps de bajada y un máximo de 3.48 Mbps de subida.

CONSUMO PROMEDIO UN AÑO: Enero 2012-Diciembre 2012

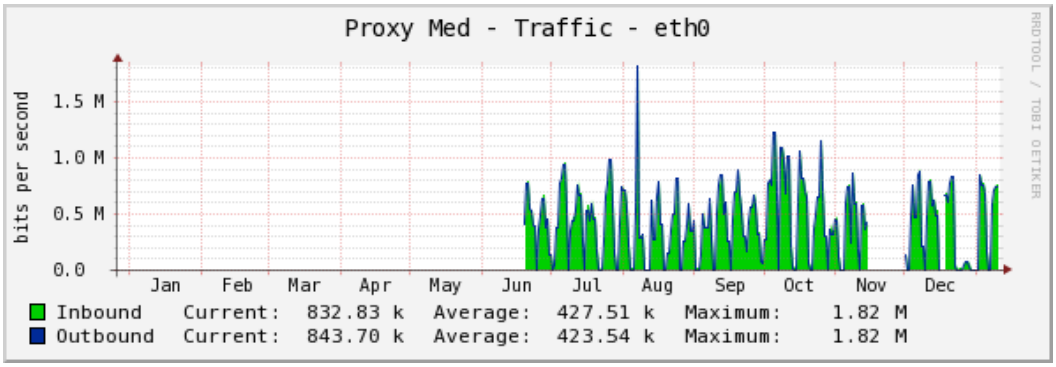


Figura 38. Proxy MED (Consumo AB: 1 año)

En la figura 38, se observa el consumo de un día, en el caso del proxy med, podemos ver que existe un consumo máximo de 1.82 Mbps de bajada y un máximo de 1.82 Mbps de subida.

En la tabla 13, se muestra el resumen de datos recopilados del consumo de ancho de banda del Proxy de la MED.

Tabla 13. Resultados de consumo MED

PROXY MED		
	AB (Mbps**) Bajada**	**AB (**Mbps**) Envío**
Consumo (1 día)	5,90	5,95
Consumo (1 semana)	6,35	6,38
Consumo (1 mes)	3,41	3,48
Consumo (1 año)	1,82	1,82
Elaborado por: Évelin Alvarado Otero		

PROXY IDIOMAS

CONSUMO PROMEDIO DE 24 HORAS: (Jueves 10 Enero 2013, 12:00-Viernes 11 Enero 2013, 10:00)

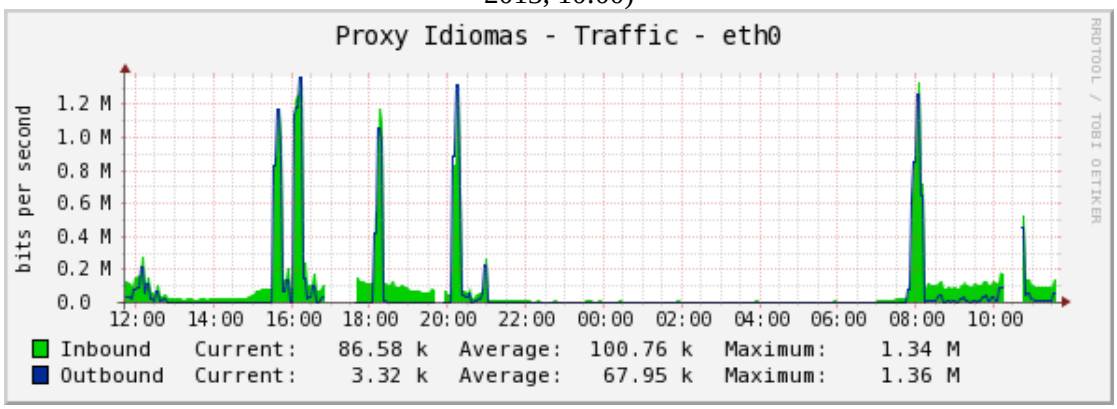


Figura 39. Proxy Idiomas (Consumo AB: 24 horas)

En la figura 39, se observa el consumo de un día, en el caso del proxy idiomas, podemos ver que existe un consumo máximo de 1.34 Mbps de bajada y un máximo de 1.36 Mbps de subida.

CONSUMO PROMEDIO DE UNA SEMANA: Semana 02: (Viernes 04-Jueves 10 Enero 2013)

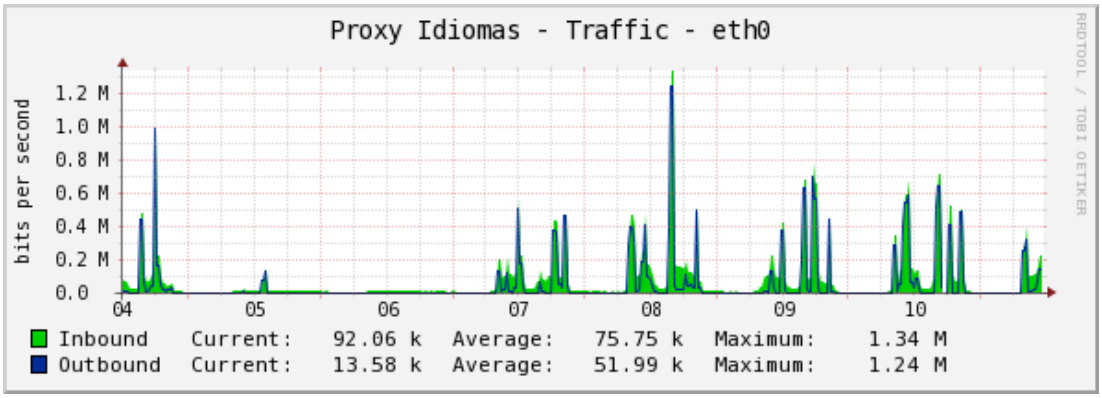


Figura 40. Proxy Idiomas (Consumo AB: 1 semana)

En la figura 40, se observa el consumo de una semana, en el caso del proxy idiomas, podemos ver que existe un consumo máximo de 1.34 Mbps de bajada y un máximo de 1.24 Mbps de subida.

CONSUMO PROMEDIO DE 1 MES: Semanas 50, 51, 52-01, 02 (11 Diciembre 2012-10 Enero 2013)

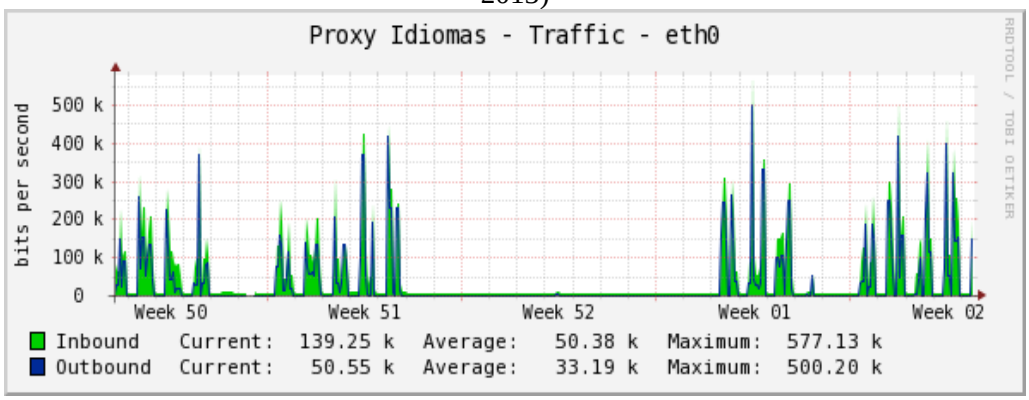


Figura 41. Proxy Idiomas (Consumo AB: 1 mes)

En la figura 41, se observa el consumo de un mes, en el caso del proxy idiomas, podemos ver que existe un consumo máximo de 577.13 Kbps de bajada y un máximo de 500.20 Kbps de subida.

CONSUMO PROMEDIO UN AÑO: Enero 2012-Diciembre 2012

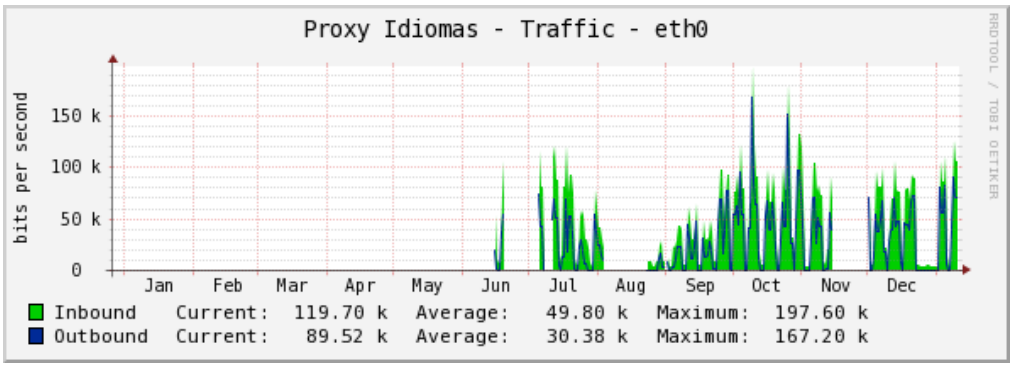


Figura 42. Proxy Idiomas (Consumo AB: 1 año)

En la figura 42, se observa el consumo de un año, en el caso del proxy idiomas, podemos ver que existe un consumo máximo de 197.60 Kbps de bajada y un máximo de 167.20 Kbps de subida.

En la tabla 14, se muestra el resumen de datos recopilados del consumo de ancho de banda del Proxy de Idiomas.

Tabla 14. Resultados de Consumo de AB Idiomas

PROXY IDIOMAS		
	AB (Mbps) Bajada	**AB (Mbps) Subida**
Consumo (1 día)	1,34	1,36
Consumo (1 semana)	1,34	1,24
Consumo (1 mes)	577,13 kbps	500,20 kbps
Consumo (1 año)	197,60 kbps	167,20 kbps
Elaborado por: Évelin Alvarado Otero		

PROXY WIRELESS

CONSUMO PROMEDIO DE 24 HORAS: (Jueves 10 Enero 2013, 12:00-Viernes 11 Enero 2013, 10:00)

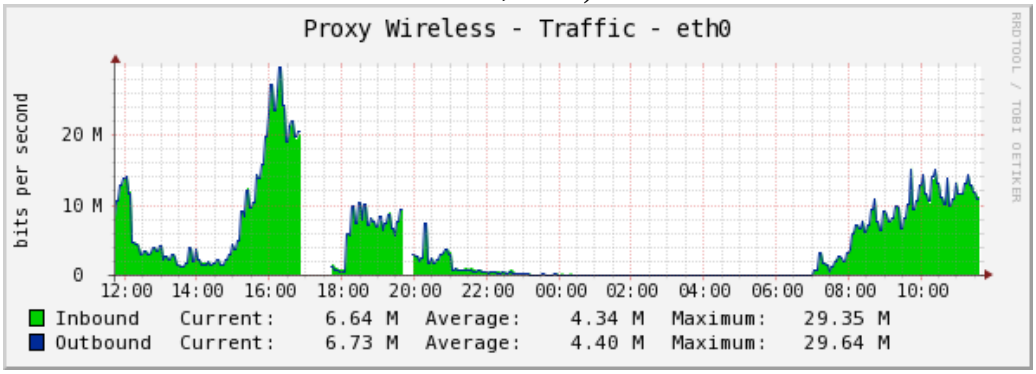


Figura 43. Proxy Wireless (Consumo AB: 24 horas)

En la figura 43, se observa el consumo de un día, en el caso del proxy wireless, podemos ver que existe un consumo máximo de 29.35 Mbps de bajada y un máximo de 29.64 Mbps de subida.

CONSUMO PROMEDIO DE UNA SEMANA: Semana 02: (Viernes 04-Jueves 10 Enero 2013)

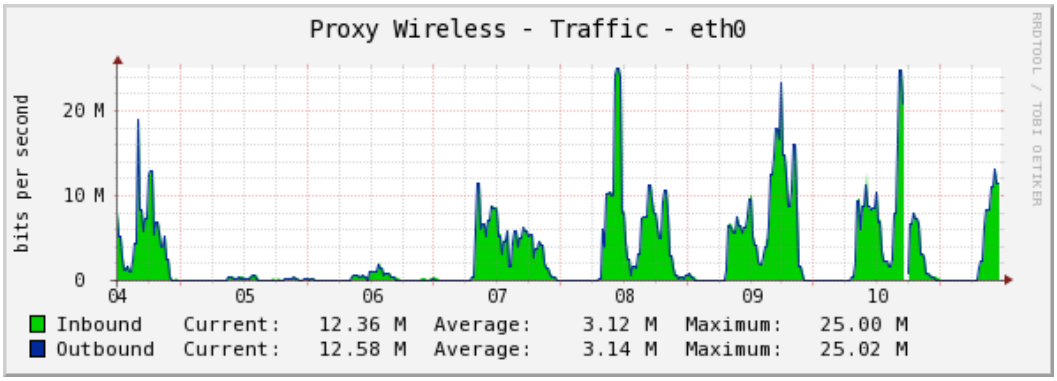


Figura 44. Proxy Wireless (Consumo AB: 1 semana)

En la figura 44, se observa el consumo de una semana, en el caso del proxy wireless, podemos ver que existe un consumo máximo de 25.00 Mbps de bajada y un máximo de 25.02 Mbps de subida.

CONSUMO PROMEDIO DE 1 MES: Semanas 50, 51, 52-01, 02 (11 Diciembre 2012-10 Enero 2013)

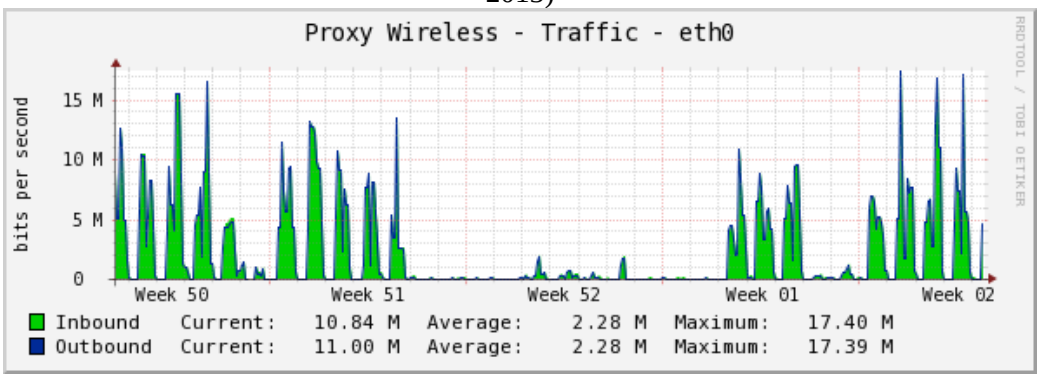


Figura 45. Proxy Wireless (Consumo AB: 1 mes)

En la figura 45, se observa el consumo de un mes, en el caso del proxy wireless, podemos ver que existe un consumo máximo de 17.40 Mbps de bajada y un máximo de 17.39 Mbps de subida.

CONSUMO PROMEDIO UN AÑO: Enero 2012-Diciembre 2012

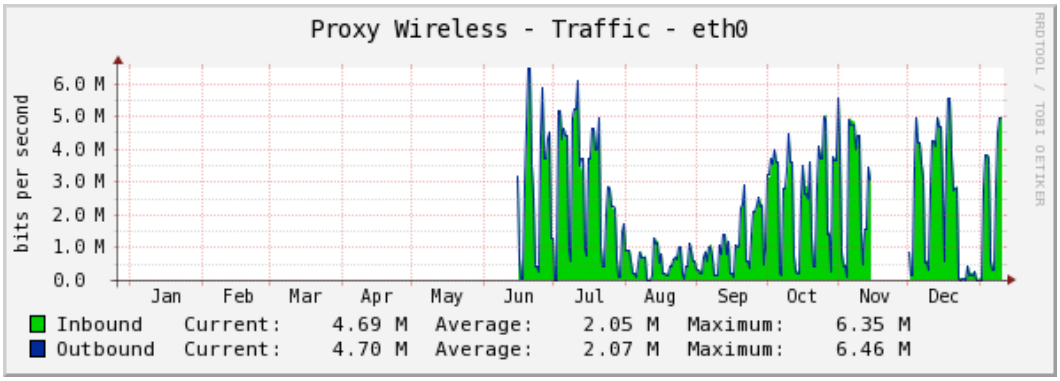


Figura 46. Proxy Wireless (Consumo AB: 1 año)

En la figura 46, se observa el consumo de un año, en el caso del proxy wireless, podemos ver que existe un consumo máximo de 6.35 Mbps de bajada y un máximo de 6.46 Mbps de subida.

En la tabla 15, se muestra el resumen de datos recopilados del consumo de ancho de banda del Proxy Wireless.

Tabla 15. Resultados de Consumo de AB Wireless

PROXY WIRELESS		
	AB (Mbps**) Bajada**	**AB (**Mbps**) Subida**
Consumo (1 día)	29,35	29,64
Consumo (1 semana)	25	25,02
Consumo (1 mes)	17,40	17,39
Consumo (1 año)	6,35	6,46
Elaborado por: Évelin Alvarado Otero		

f.2 Consumo Ancho de Banda AEIRNNR (Proxy ENERGÍA)

Se trata de manera individual al **área de energía** ya que es en esta área en la que se procederá con la implementación del equipo segmentador, aparte de tener el conocimiento del consumo real de ancho de banda que genera dicha área, se precisa la información de conocer a detalle la actividad en Internet que tienen todos los usuarios en la red LAN del área como se verá en la siguiente sección. Se procedió a la toma de datos proporcionados por el Cacti para el proxy energía. A manera de observación, al igual que en los proxys anteriores, el Cacti arroja datos de consumo simétricos; siendo únicamente el dato de subida, un dato no real.

CONSUMO PROMEDIO 24 HORAS: (Miércoles 24 Octubre 2012, 12:00-Jueves 25 Octubre 2012, 12:00)

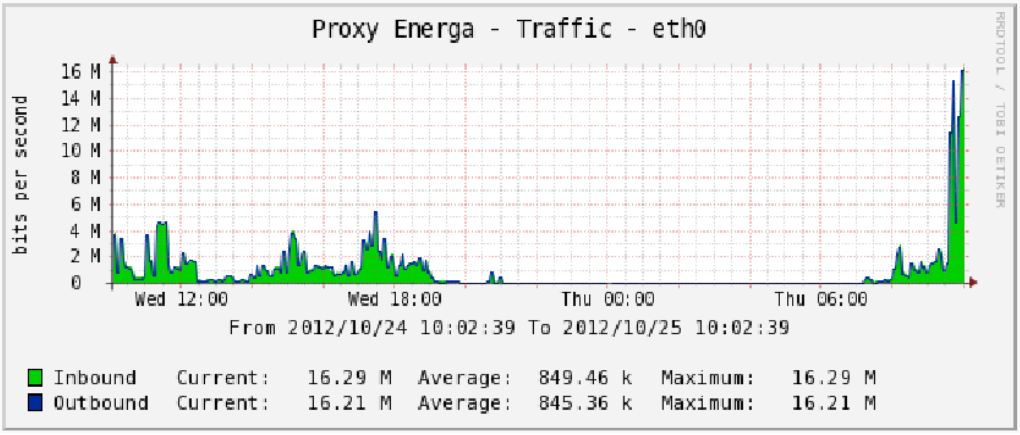


Figura 47. Proxy Energía (Consumo AB: 24 horas)

De la figura 47, se observa el consumo de un día, en el caso del proxy energía, podemos ver un consumo máximo de 16.29 Mbps de bajada y un máximo de 16.21 Mbps de subida.

CONSUMO PROMEDIO DE UNA SEMANA: Semanas: 42(Jueves 18 y Viernes 19), 43(Lunes 22, Martes 23, Miércoles 24 y Jueves 25) Octubre 2012

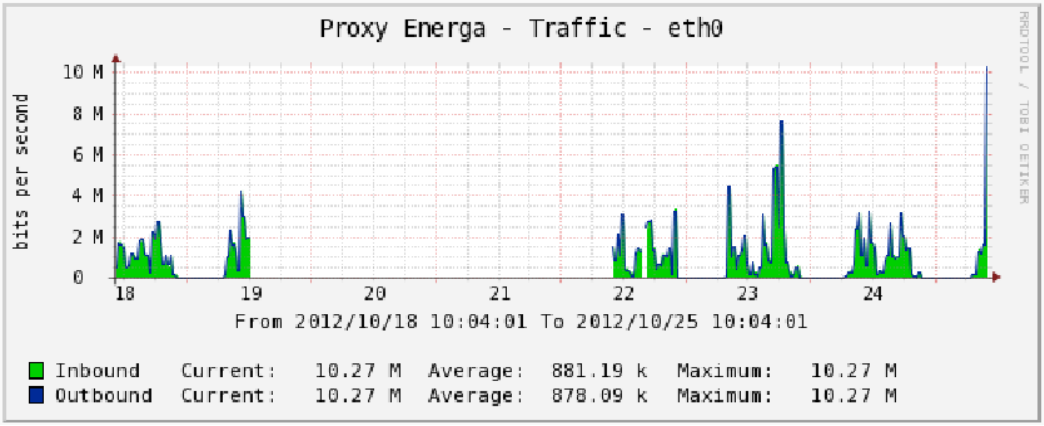


Figura 48. Proxy Energía (Consumo AB: 1 semana)

De la figura 48, se observa el consumo de una semana, en el caso del proxy energía, podemos ver un consumo máximo de 10.27 Mbps de bajada y un máximo de 10.27 Mbps de subida.

CONSUMO PROMEDIO DE 1 MES: Semanas 39-42 (24 Septiembre- 21 Octubre 2012)

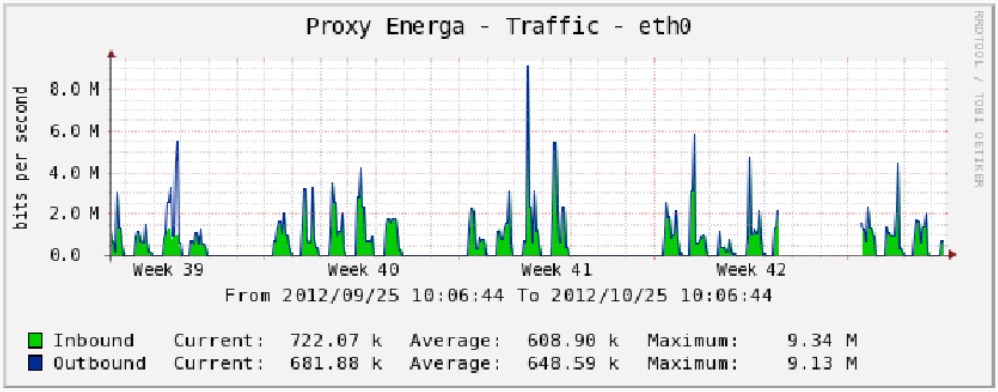


Figura 49. Proxy Energía (Consumo AB: 1 mes)

En la figura 49, se observa el consumo de un mes, en el caso del proxy energía, podemos ver un consumo máximo de 9.34 Mbps de bajada y un máximo de 9.13 Mbps de subida.

CONSUMO PROMEDIO DE 2 MESES: Semanas 35-42 (27 Agosto-21 Octubre 2012)

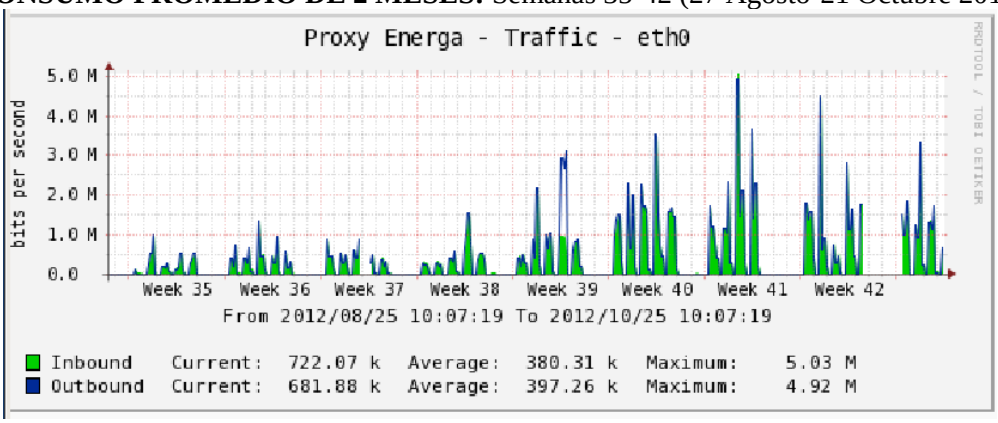


Figura 50. Proxy Energía (Consumo AB: 2 meses)

De la figura 50, se observa el consumo de dos meses, en el caso del proxy energía, podemos ver un consumo máximo de 5.03 Mbps de bajada y un máximo de 4.92 Mbps de subida.

En la tabla 16, se muestra el resumen de datos recopilados del consumo de ancho de banda del Proxy de Energía.

Tabla 16. Resultados de Consumo de AB de Energía

PROXY AEIRNNR		
	AB (Mbps**) Bajada**	**AB (**Mbps**) Subida**
Consumo (24 horas)	16,29	16,21
Consumo (1 semana)	10,27	10,27
Consumo (1 mes)	9,34	9,13
Consumo (2 meses)	5,03	4,92
Elaborado por: Évelin Alvarado Otero		

f.2.1 Reporte del contenido web del AEIRNNR

La importancia de conocer el contenido web del proxy del AEIRNNR, es permitir conocer las páginas que son más visitadas por el usuario, que tipos de servicios son los que más utilizan, para así tener conocimiento de que páginas y servicios segmentar de acuerdo a su prioridad, así como determinar cuáles son los usuarios que más utilizan la red.

Para determinar: IP's de los equipos que se han conectado a Internet, las páginas más visitadas por los usuarios, la cantidad de usuarios que accedieron y a qué hora accedieron, cuantos bytes han sido descargados, páginas denegadas, descargas que han realizado, como parámetros relevantes para el desarrollo del proyecto, los servidores de la Universidad cuentan con el software Generador de Reportes del Análisis de SQUID (SARG), gracias al fichero de log "access.log" del ya mencionado proxy Squid, nos permitirá analizar los parámetros citados. En la figura 51, se esquematiza en que parte de la red entra en función el SARG.

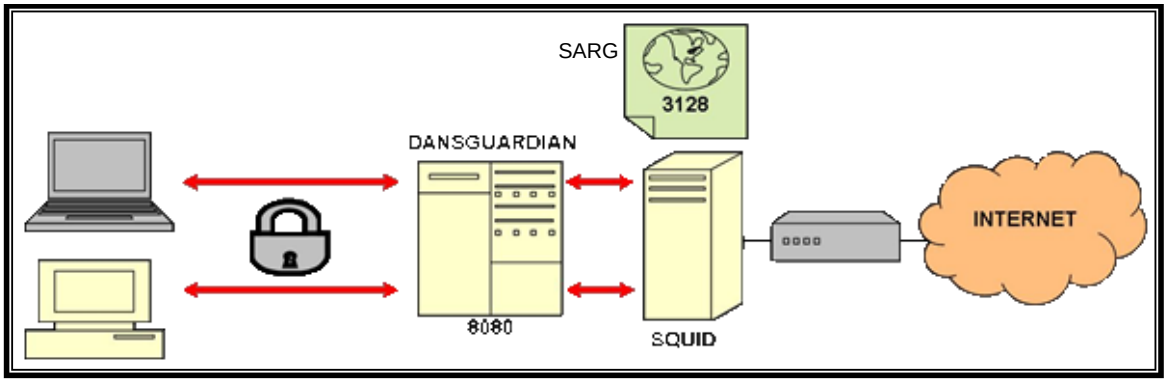


Figura 51. Software Squid Analysis Report Generator - SARG

<<El administrador de la red, mediante comandos *log* desde SQUID, genera la petición que realiza SARG, se pueden ver directamente desde la web en la que está corriendo el SQUID>>[9]. Para obtener los contenidos de navegación web, se tomó un mes de muestra, del 1 de Octubre al 1 de Noviembre de 2012. Una vez generados los reportes, SARG se presenta en la web como se muestra en la figura 52. De una lista de opciones tales

como: *Top sites*, *Sites & Users*, *Downloads* y *Denied accesses*, se consiguieron los siguientes datos.

Figura 52. Lista de reportes SARG

En base al reporte generado por SARG para el AEIRNNR, un *Top Sites* de las páginas más visitadas en el AEINNR se muestran en la figura 53; a continuación en la tabla 17, se muestra una pequeña lista de páginas que se marcarán en el equipo de manera independiente por ser páginas de alto consumo de ancho de banda como es el caso de youtube y por ser redes sociales como en el caso de facebook, también se marcará de manera independiente a los servicios como: Skype, Messenger, p2p, etc.

SARG Squid Analysis Report Generator

Reporte de navegacion del area de energia

Period: 01 oct 2012—01 nov 2012

Top 100 sites

NUM	ACCESSED SITE	CONNECT	BYTES	TIME
1	tb.gooofull.com	177.05K	37.67M	0:28:28
2	www.google.com.ec	17.79K	230.56M	2:33:57
3	clients1.google.com.ec	17.34K	16.23M	1:12:48
4	pagead2.googlesyndication.com	11.36K	5.70M	0:05:55
5	safebrowsing-cache.google.com	9.89K	649.41M	1:22:03
6	badoo.com	6.87K	80.35M	15:49:07
7	eva.unl.edu.ec	6.08K	196.98M	0:18:52
8	l.yimg.com	5.53K	112.82M	0:29:13
9	www.google.com	5.52K	21.35M	0:31:00
10	77.73.177.242	5.20K	1.34M	10:54:58
11	pubads.g.doubleclick.net	4.21K	16.80M	0:24:20
12	www.twoo.com	4.15K	111.72M	1:18:17
13	www.unl.edu.ec	3.47K	112.53M	0:12:33
14	mail.yimg.com	3.23K	32.16M	0:13:37
15	l1.yimg.com	3.21K	29.56M	0:22:13
16	us1.badoo.com	3.03K	31.49M	7:05:06
17	estudiantes.unl.edu.ec	2.97K	36.86M	0:15:28
18	www.facebook.com	2.91K	88.94M	9:33:12
19	172.16.32.10	2.88K	13.97M	0:30:40
20	aeirnnr.unl.edu.ec	2.84K	20.44M	0:07:03

Figura 53. Reporte SARG Top Site

Tabla 17. Páginas marcadas individualmente para asignación de ancho de banda

TOP 10 SITES			
NUM	**ACCESSED SITE**	**CONNECT (K)**	**BYTES (M)**
18	www.facebook.com	2.91K	88.94M
52	www.youtube.com	1.08K	1.17M
6	www.badoo.com	6.87K	80.35M
48	www.twitter.com	1.13K	33.30M
31	www.msn.com	1.64K	3.87M
POR SERVICIO			
1	Skype		
2	Messenger		
3	Audio		
4	Video		
	P2P		
Elaborado por: Évelin Alvarado Otero			

En la figura 54, por su parte se muestra el *Top Users*, y en la tabla 18, se determina que los usuarios que más utilizan internet son los usuarios de la biblioteca del área. El rango de las IPs de la biblioteca del área va desde la **172.16.50.125** a la **172.16.50.160**.

SARG Squid Analysis Report Generator

Reporte de navegacion del area de energia

Period: 01 oct 2012—01 nov 2012

Sort: bytes, reverse

Top users

NUM		USERID	CONNECT	BYTES	%BYTES	IN-CACHE-OUT		ELAPSED TIME	MILLISEC	%TIME
1		172.16.49.134	13.82K	685.43M	11,45%	0,00%	100,00%	48:12:53	173.573.668	9,17%
2		172.16.50.10	38.46K	519.15M	8,67%	23,48%	76,52%	37:22:17	134.537.433	7,11%
3		172.16.50.140	15.43K	385.47M	6,44%	6,21%	93,79%	20:26:21	73.581.363	3,89%
4		172.16.50.150	14.08K	316.14M	5,28%	5,84%	94,16%	20:53:36	75.216.965	3,97%
5		172.16.50.148	14.98K	262.11M	4,38%	8,45%	91,55%	28:38:08	103.088.132	5,45%
6		172.16.50.151	14.25K	261.24M	4,36%	5,27%	94,73%	27:54:13	100.453.292	5,31%
7		172.16.50.147	9.39K	200.80M	3,35%	4,59%	95,41%	13:48:15	49.695.764	2,63%
8		172.16.50.142	5.57K	193.95M	3,24%	3,47%	96,53%	18:10:56	65.456.514	3,46%
9		172.16.49.102	4.23K	193.38M	3,23%	0,00%	100,00%	12:57:53	46.673.905	2,47%
10		172.16.50.189	10.23K	161.90M	2,70%	2,46%	97,54%	04:00:49	14.449.088	0,76%
11		172.16.50.144	6.13K	145.71M	2,43%	5,76%	94,24%	12:01:07	43.267.276	2,29%
12		172.16.50.146	8.25K	138.45M	2,31%	11,22%	88,78%	07:33:08	27.188.248	1,44%
13		172.16.50.129	5.18K	128.97M	2,15%	2,88%	97,12%	04:51:24	17.484.247	0,92%
14		172.16.50.141	5.89K	112.78M	1,88%	7,78%	92,22%	07:32:00	27.120.717	1,43%
15		172.16.50.112	10.09K	104.80M	1,75%	10,89%	89,11%	06:39:31	23.971.282	1,27%
16		172.16.49.155	183.61K	104.28M	1,74%	45,87%	54,13%	12:42:30	45.750.868	2,42%
17		172.16.50.139	5.03K	91.40M	1,53%	5,73%	94,27%	09:10:15	33.015.746	1,74%
18		172.16.50.153	6.22K	88.38M	1,48%	6,12%	93,88%	31:10:31	112.231.067	5,93%
19		172.16.50.143	2.93K	81.94M	1,37%	4,33%	95,67%	10:53:21	39.201.703	2,07%
20		172.16.49.154	6.19K	79.55M	1,33%	8,14%	91,86%	03:39:38	13.178.978	0,70%

Figura 54. Reporte SARG Top Users

Tabla 18. Resultados del Top Users

TOP USERS				
NUM	**USERID**	**BYTES (M)**	**% BYTES**	**USER**
1	172.16.49.134	685.43M	11,45%	Carrera de Ing. en Sistemas
2	172.16.50.10	519.15M	8,67%	Lab. Programación
3	172.16.50.140	385.47M	6,44%	Biblioteca Energía
4	172.16.50.150	316.14M	5,28%	Biblioteca Energía
5	172.16.50.148	262.11M	4,38%	Biblioteca Energía
6	172.16.50.151	261.24M	4,36%	Biblioteca Energía
7	172.16.50.147	200.80M	3,35%	Biblioteca Energía
8	172.16.50.142	193.95M	3,24%	Biblioteca Energía
9	172.16.49.102	193.38M	3,23%	Dirección
10	172.16.50.189	161.90M	2,70%	Lab. Geología
11	172.16.50.144	145.71M	2,43%	Biblioteca Energía

12	172.16.50.146	138.45M	2,31%	Biblioteca Energía
13	172.16.50.129	128.97M	2,15%	Biblioteca Energía
14	172.16.50.141	112.78M	1,88%	Biblioteca Energía
15	172.16.50.112	104.80M	1,75%	Lab. Telecomunicaciones
16	172.16.49.155	104.28M	1,74%	Biblioteca Energía
17	172.16.50.139	91.40M	1,53%	Biblioteca Energía
18	172.16.50.153	88.38M	1,48%	Biblioteca Energía
19	172.16.50.143	81.94M	1,37%	Biblioteca Energía
20	172.16.49.154	79.55M	1,33%	Carrera de Ing. en Geología
Elaborado por: Évelin Alvarado Otero				

En la opción de *Downloads*, por su parte, muestra las descargas realizadas en el área. Cabe mencionar, que por lo extenso del reporte proporcionado por SARG para *Downloads*, se tomó en cuenta 2 IPs de la biblioteca del área, que son evaluadas en distintas horas del día. En base a lo expuesto en la figura 55, se puede notar que la mayor parte de descargas son actualizaciones para el sistema, y una minoría son la descarga por parte de peticiones. La flecha azul indica el inicio de uso y la flecha roja el fin de uso por parte de un usuario, evaluado en un solo día.

SARG Squid Analysis Report Generator

Reporte de navegacion del area de energia

Period: 01 oct 2012—01 nov 2012

Downloads

172.16.50.140	01/11/12-08:24:45	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	01/11/12-08:24:46	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	01/11/12-08:24:48	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	01/11/12-08:24:49	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	01/11/12-08:24:50	http://hotmail.com
	01/11/12-08:24:51	http://evsecure-ocsp.verisign.com
	01/11/12-08:24:54	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	01/11/12-08:24:56	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	01/11/12-08:24:57	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	01/11/12-08:24:58	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	01/11/12-08:24:59	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	01/11/12-08:25:00	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	01/11/12-08:25:01	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	01/11/12-08:25:02	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	01/11/12-08:25:04	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	01/11/12-08:25:04	http://fb.com
	01/11/12-08:25:05	http://www.facebook.com
	01/11/12-08:29:51	http://cache.pack.google.com/edgedl/chrome/win/22.0.1229.94_22.0.1229.79_chrome_updater.
	01/11/12-08:30:36	http://evsecure-ocsp.verisign.com
	01/11/12-08:34:09	http://google.com
	01/11/12-08:34:09	http://www.google.com
	01/11/12-09:15:47	http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.
	29/10/12-09:31:35	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	29/10/12-09:31:40	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	29/10/12-09:31:43	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	29/10/12-09:31:45	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	29/10/12-09:31:47	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	29/10/12-09:31:48	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	29/10/12-09:31:49	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	29/10/12-09:31:51	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	29/10/12-09:31:53	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	29/10/12-09:31:55	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	29/10/12-09:31:57	http://cache.pack.google.com/edgedl/update2/1.3.21.123/GoogleUpdateSetup.exe
	29/10/12-09:37:00	http://cache.pack.google.com/edgedl/chrome/win/22.0.1229.94_22.0.1229.79_chrome_updater.
172.16.50.141	29/10/12-10:32:11	http://www.google.com
	29/10/12-10:36:17	http://cache.pack.google.com/edgedl/chrome/win/22.0.1229.94_22.0.1229.79_chrome_updater.exe
	29/10/12-11:10:28	http://www.google.com
	29/10/12-11:10:37	http://hotmail.com
	29/10/12-11:10:37	http://www.google.com.ec/complete/search?sugexp=chrome,mod=0&client=chrome&hl=es&q=hotm
	29/10/12-11:10:41	http://www.download.windowsupdate.com/msdownload/update/v3/static/trustedr/en/authrootstl.cab
	29/10/12-11:13:00	http://people.directory.live.com/xmlProxy.htm?vn=9.090515.0&domain=live.com
	29/10/12-11:13:05	http://by2msg3020816.by2.gateway.edge.messenger.live.com/xmlProxy.htm?vn=9.090515.0&doma
	29/10/12-11:13:19	http://by2msg3010706.gateway.messenger.live.com/xmlProxy.htm?vn=9.090515.0&domain=live.co
	29/10/12-11:13:19	http://sn127w.snt127.mail.live.com/Handlers/WebIMPop.mvc?0&biciNoLDParse=1&V=12&domain=liv
	29/10/12-11:36:57	http://baymsg1010734.by2.gateway.edge.messenger.live.com/xmlProxy.htm?vn=9.090515.0&doma
	29/10/12-11:38:14	http://baymsg1020331.by2.gateway.edge.messenger.live.com/xmlProxy.htm?vn=9.090515.0&doma
	29/10/12-14:41:51	http://www.google.com
	29/10/12-14:41:56	http://www.facebook.com
	29/10/12-14:42:17	http://www.hotmail.com
	29/10/12-14:43:17	http://geo.messenger.services.live.com/xmlProxy.htm?vn=9.090515.0&domain=live.com
	29/10/12-14:43:20	http://bl169w.blu169.mail.live.com/Handlers/WebIMPop.mvc?0&biciNoLDParse=1&V=12&domain=liv
	29/10/12-14:43:21	http://baymsg1020416.gateway.messenger.live.com/xmlProxy.htm?vn=9.090515.0&domain=live.co
	29/10/12-14:50:39	http://www.facebook.com
	29/10/12-14:53:54	http://evsecure-ocsp.verisign.com
	29/10/12-15:17:54	http://www.google.com
	29/10/12-15:18:28	http://es.engadget.com
	29/10/12-16:38:03	http://www.google.com
	29/10/12-16:38:59	http://www.google.com.ec/complete/search?sugexp=chrome,mod=0&client=chrome&hl=es&q=imfic

Figura 55. Reporte SARG *Download*

En la opción de *Denied*, muestra las páginas que han sido negadas. En la figura 56, se toma en consideración 4 IPs de la biblioteca del área por lo extenso del reporte. En base a estas IPs se expone que, al negar algunas categorías de páginas web, niega descargas de actualizaciones, cuentas en youtube, etc., que se encuentran disponibles en estas.

SARG Squid Analysis Report Generator

Reporte de navegacion del area de energia

Period: 01 oct 2012—01 nov 2012

Denied

172.16.50.126	30/10/12-13:15:02	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.1/misc/AdbeRdrUpd951_all_incr.msp
	30/10/12-13:15:03	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.1/misc/AdbeRdrUpd951_all_incr.msp
	31/10/12-17:40:14	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.1/misc/AdbeRdrUpd951_all_incr.msp
	31/10/12-17:40:14	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.1/misc/AdbeRdrUpd951_all_incr.msp
	30/10/12-13:21:09	http://pagead2.googlesyndication.com/pagead/imgad/1723995/728x90Esp.swf?clickTag=http%3A%2F%2Fadclick.g.dou.
	30/10/12-13:21:07	http://pagead2.googlesyndication.com/pagead/imgad/879366/flashwrite_1_2.js
	30/10/12-13:30:04	http://pagead2.googlesyndication.com/pagead/imgad?id=CLmx8oGx0vfHtwEQARgBMgiqFvqXcJXFJw
	30/10/12-13:22:38	http://pagead2.googlesyndication.com/pagead/imgad?id=CNra_5fw8tv9ZRABGAEyCGZqBcmNIDxA
	30/10/12-13:21:15	http://pagead2.googlesyndication.com/pagead/imgad?id=CNXwj7Tn7LXW_QEQARgBMghoAo6nXTrHCw
	30/10/12-13:22:39	http://pagead2.googlesyndication.com/pagead/imgad?id=CNXwj7Tn7LXW_QEQARgBMghoAo6nXTrHCw
172.16.50.136	30/10/12-10:51:04	http://ads.adbrite.com/adserver/vdi/830697?r=http%3A%2F%2Fi.w55c.net%2Fm.gif%3Fid%3D8bb138bc0446417c9a
	29/10/12-17:05:15	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.1/misc/AdbeRdrUpd951_all_incr.msp
	29/10/12-17:11:48	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.1/misc/AdbeRdrUpd951_all_incr.msp
	29/10/12-17:14:04	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.1/misc/AdbeRdrUpd951_all_incr.msp
	29/10/12-17:28:11	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.1/misc/AdbeRdrUpd951_all_incr.msp
	29/10/12-17:29:18	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.1/misc/AdbeRdrUpd951_all_incr.msp
	29/10/12-17:29:22	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.1/misc/AdbeRdrUpd951_all_incr.msp
	30/10/12-10:46:47	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.1/misc/AdbeRdrUpd951_all_incr.msp
	30/10/12-10:47:55	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.1/misc/AdbeRdrUpd951_all_incr.msp
	30/10/12-10:48:42	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.1/misc/AdbeRdrUpd951_all_incr.msp
172.16.50.137	29/10/12-17:12:46	http://ads2.msads.net/CIS/17/000/000/000/022/424.swf?fd=latam.msn.com
	31/10/12-11:27:19	http://ads.adbrite.com/adserver/vdi/830697?r=http%3A%2F%2Fi.w55c.net%2Fm.gif%3Fid%3D8bb138bc0446417c9a
	29/10/12-17:04:14	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.1/misc/AdbeRdrUpd951_all_incr.msp
	29/10/12-17:04:14	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.1/misc/AdbeRdrUpd951_all_incr.msp
	30/10/12-10:47:06	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.1/misc/AdbeRdrUpd951_all_incr.msp
	30/10/12-10:47:07	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.1/misc/AdbeRdrUpd951_all_incr.msp
	30/10/12-10:53:44	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.1/misc/AdbeRdrUpd951_all_incr.msp
	30/10/12-10:53:44	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.1/misc/AdbeRdrUpd951_all_incr.msp
	31/10/12-11:22:04	http://armdl.adobe.com/pub/adobe/reader/win/9.x/9.5.1/misc/AdbeRdrUpd951_all_incr.msp
172.16.50.142	29/10/12-10:50:04	http://accounts.youtube.com:443
	29/10/12-10:50:04	http://accounts.youtube.com:443
	29/10/12-10:50:04	http://accounts.youtube.com:443
	29/10/12-10:50:04	http://accounts.youtube.com:443
	29/10/12-10:52:47	http://accounts.youtube.com:443
	29/10/12-10:52:47	http://accounts.youtube.com:443
	29/10/12-10:52:47	http://accounts.youtube.com:443
	29/10/12-10:39:57	http://ads2.msads.net/CIS/17/000/000/000/022/424.swf?fd=latam.msn.com
	29/10/12-14:39:18	http://ads2.msads.net/CIS/17/000/000/000/022/424.swf?fd=latam.msn.com
	31/10/12-18:27:32	http://ads2.msads.net/CIS/17/000/000/000/022/424.swf?fd=latam.msn.com

Figura 56. Reporte SARG Denied

f.3 Cálculo Ancho de Banda

Por el momento no existe hardware o software que permita hacer un uso correcto del ancho de banda destinado para la red de datos de la UNL; para hacer uso de los 99 Mbps de ancho de banda que dispone la Universidad, los usuarios al momento de conectarse a la red compiten por un segmento de ancho de banda, el mismo que le es asignado de manera inadecuada.

Como primera instancia para la aplicación a futuro de un segmentador en la Universidad, se procede al cálculo del ancho de banda que se debe asignar para cada área de la universidad. A partir de los datos proporcionados por el Cacti sobre el consumo de ancho de banda por parte de cada proxy, se hace uso del procedimiento de Muestreo y Estimación por Intervalos de confianza.

<<El diseño de muestras es uno de los temas más relevantes en la elaboración y desarrollo de una investigación científica, de la calidad de la muestra y de la adecuada selección de las unidades de análisis, depende en gran medida la utilidad de la investigación. Además, es la base para lograr obtener estimaciones de parámetros asertivamente y de lograr validar o confirmar hipótesis que es lo que se entiende en gran medida como inferencia estadística>>[18].

El código de la tabla 19, es una parte de un algoritmo implementado en el software de MatLab; <<este describe el comportamiento de una variable, a base de un conjunto de muestras (de preferencia muestras que abarquen el monitoreo de un año de corrido sobre un sistema), este programa puede proporcionar comportamientos pasados o predecir comportamientos de la variable en un sistema. En el caso de no tener datos de cualquier día "x", en base a los datos de los días anteriores y posteriores, el programa realiza un análisis y predice un posible comportamiento del sistema para el día del cual no se tiene datos>>[10].

Tabla 19. Código MatLab

CÓDIGO FUENTE (MATLAB)

```
>>function [fitresult,Max] = createFit(Tiempo, Objeto)
%% Ajuste
 T = 1:4;
[xData, yData] = prepareCurveData( T', Objeto );

ft = fittype( 'pchipinterp' );
opts = fitoptions( ft );
opts.Normalize = 'on';

[fitresult, ~] = fit( xData, yData, ft, opts );

figure( 'Name', 'Ancho de banda' );
h = plot( fitresult, xData, yData );
Legend (h, 'Ancho de banda vs. Tiempo', 'Ajuste', 'Location',
'NorthEast' );

xlabel( 'Tiempo' );
ylabel( 'Ancho de banda' );
grid on

DataLista = feval(fitresult,Tiempo);
m = bootstrp(31,@mean,DataLista);
s = std(m,0);
figure('Name','Ancho de banda')
plot(DataLista)
hold on
plot(DataLista+3*s,'--r')
plot(DataLista-3*s,'--r')
hold off
Max = max(DataLista+3*s);
disp(ceil(Max));
```

f.3.1 Procedimiento

De cada una de las áreas:

<<El cálculo de intervalos de confianza para la estimación de parámetros, son técnicas que nos permiten hacer declaraciones sobre qué valores podemos esperar para un parámetro>>[18]. El intervalo calculado dependerá de:

- El número de muestras.
- <<Lo estimado en la muestra (porcentaje, media,…) El intervalo de confianza está formado por valores ligeramente menores y mayores que la aproximación ofrecida por la muestra>>[18].
- La probabilidad (nivel de confianza) con la que el método dará una respuesta correcta, trabaja con niveles de confianza habituales para los intervalos de confianza de 95% (95% de acierto-5% de incertidumbre-tomados 2 intervalos de incertidumbre) y el 99% (99% de acierto-1% de incertidumbre-tomado 1 intervalo de incertidumbre).

Puede parecer ilógico que no se pretenda respuestas con una confianza del 100%, sucede que en estos casos, no servirían intervalos muy grandes. Hay que interpolar al nivel de confianza como que se dispone de un método para calcular intervalos. Para el presente proyecto, en nuestro cálculo se toman tres intervalos de confianza, por lo tanto, nuestro intervalo queda de la siguiente manera: 90%-10%.

Nuestro intervalo de confianza es para el dato más alto de la tabla, en nuestro caso, para el dato de consumo más alto de cuatro semanas. No es el dato más bajo porque no queremos asignar el ancho de banda suficiente, y no es a partir de la media porque no se pretende asignar un ancho de banda necesario, es a partir del dato más alto de consumo de ancho de banda que se generó en el mes, al que el programa le dará prioridad, ya que se desea asignar un ancho de banda favorable para la nueva navegación sin control de contenido.

PROXY EDUCATIVA

```
>> [fitresult, Max] = createFit (Tiempo, Educativa);
   AB= 7
```

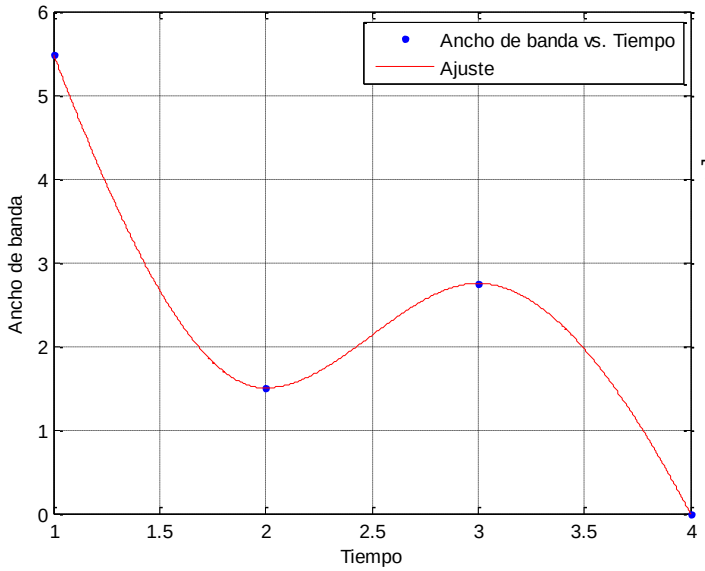


Figura 57. Gráfica datos proxy educativa

Tabla 20. Datos Proxy Educativa

PROXY EDUCATIVA	
Semanas	Mbps
1	5,49
2	1,5
3	2,75
4	0
Media	**2,43**

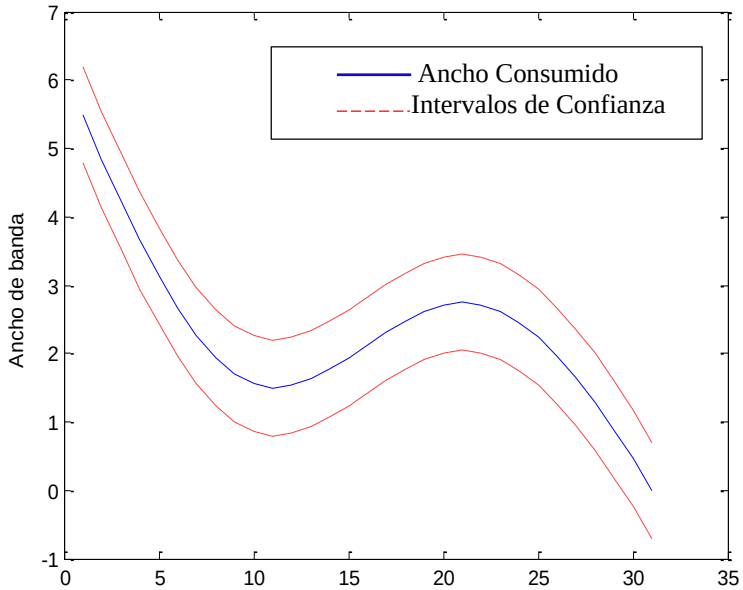


Figura 58. Gráfica para AB asignada educativa

Tabla 21. AB Educativa

AB Asignado	
Mbps	Mbps
5,49	± 0,75
TOTAL	**7**

PROXY JURÍDICA

```
>> [fitresult, Max] = createFit (Tiempo, Jurídica);
   AB= 7
```

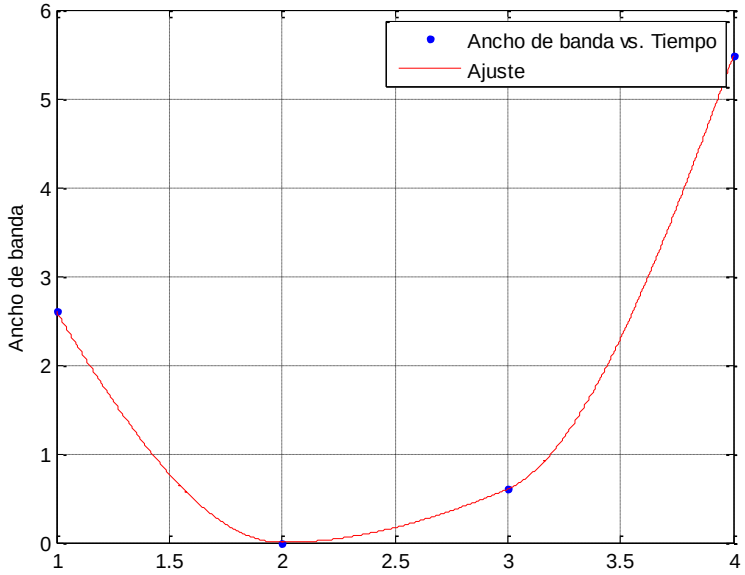


Figura 59. Gráfica datos proxy Jurídica

Tabla 22. Datos Proxy Jurídica

PROXY JURÍDICA	
Semanas	Mbps
1	2,6
2	0
3	0,8
4	5,38
Media	**2,19**

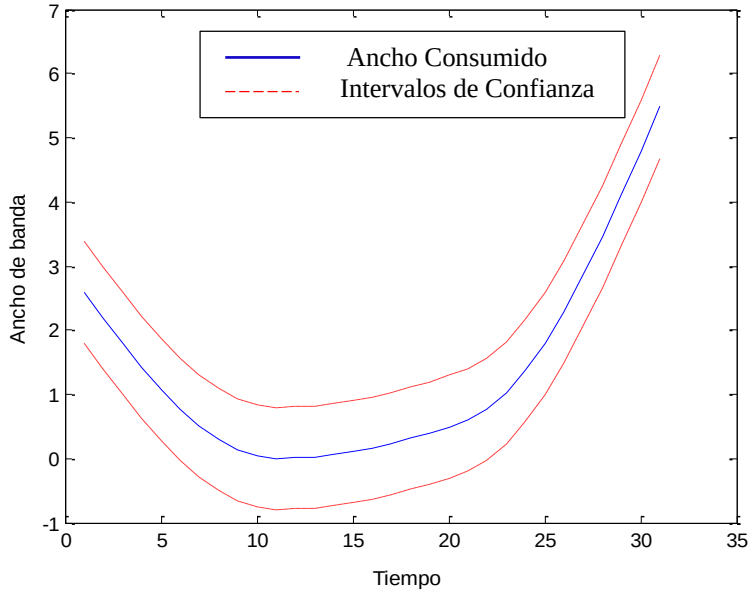


Figura 60. Gráfica para AB asignado Jurídica

Tabla 23. AB Jurídica

AB Asignado	
Mbps	Mbps
5,38	± 0,81
TOTAL	**7**

PROXY AGROPECUARIA

```
>> [fitresult, Max] = createFit (Tiempo, Agro);
   AB= 3
```

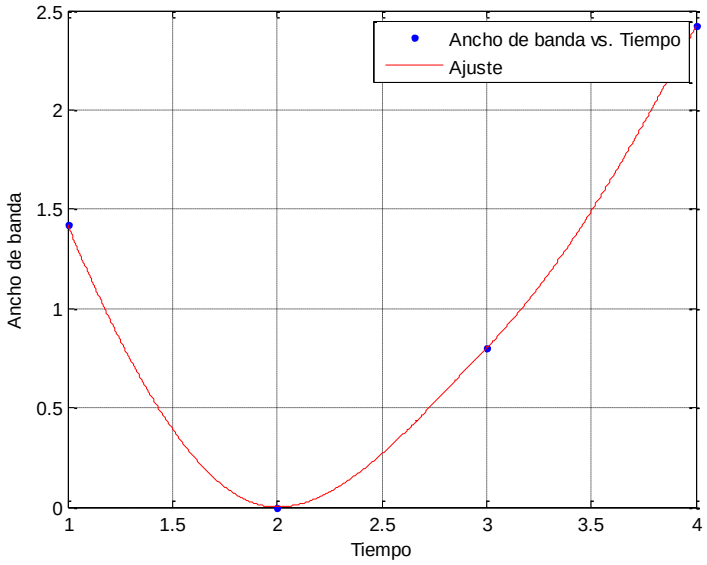


Figura 61. Gráfica datos proxy Agropecuaria

Tabla 24. Datos proxy Agrop.

PROXY AGROPECUARIA	
Semanas	Mbps
1	1,42
2	0
3	0,8
4	2,42
Media	**1,16**

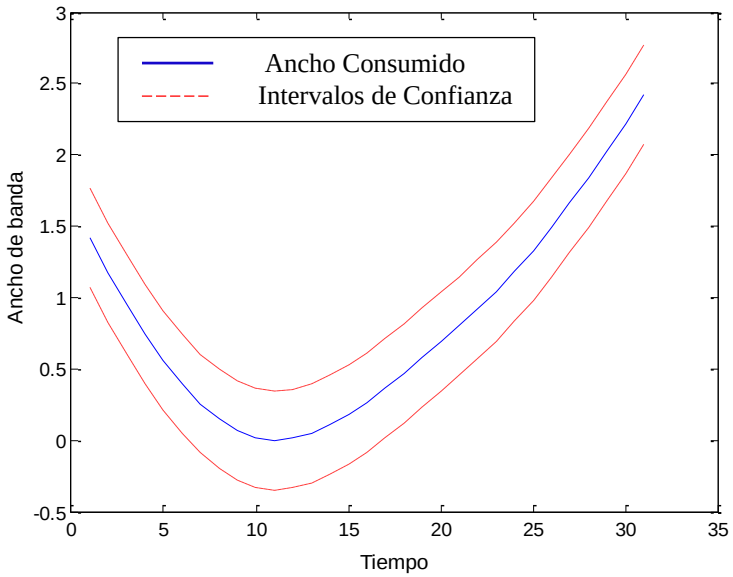


Figura 62. Gráfica para AB asignado Agropecuaria

Tabla 25. AB Agropecuaria

AB Asignado	
Mbps	Mbps
2,42	± 0,29
TOTAL	**3**

PROXY SALUD

```
>> [fitresult, Max] = createFit (Tiempo, Salud);
   AB= 4
```

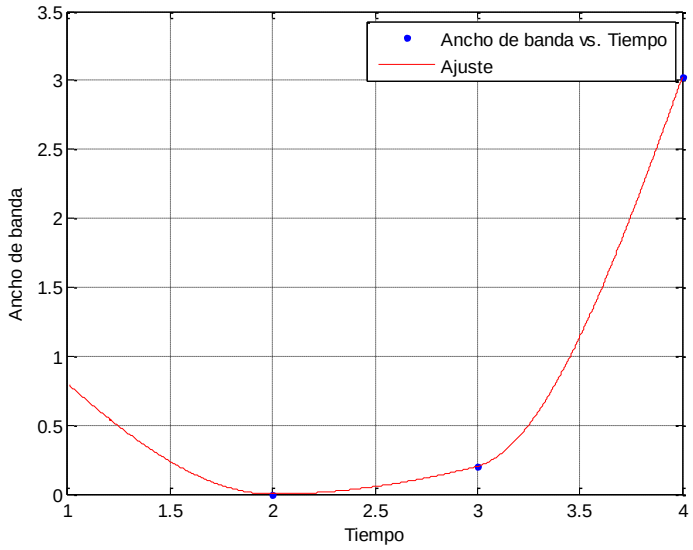


Figura 63. Gráfica datos proxy Salud

Tabla 26. Datos proxy Salud

PROXY SALUD	
Semanas	Mbps
1	0,8
2	0
3	0,2
4	3,02
Media	**1,01**

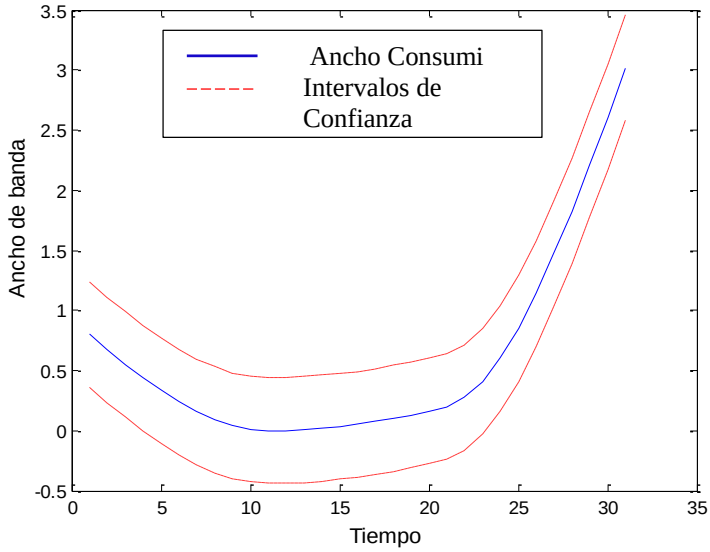


Figura 64. Gráfica para AB asignado Salud

Tabla 27. AB Salud

AB Asignado	
Mbps	Mbps
3,02	± 0,49
TOTAL	**4**

PROXY ENERGÍA

```
>> [fitresult, Max] = createFit (Tiempo, Energía);
   AB= 12
```

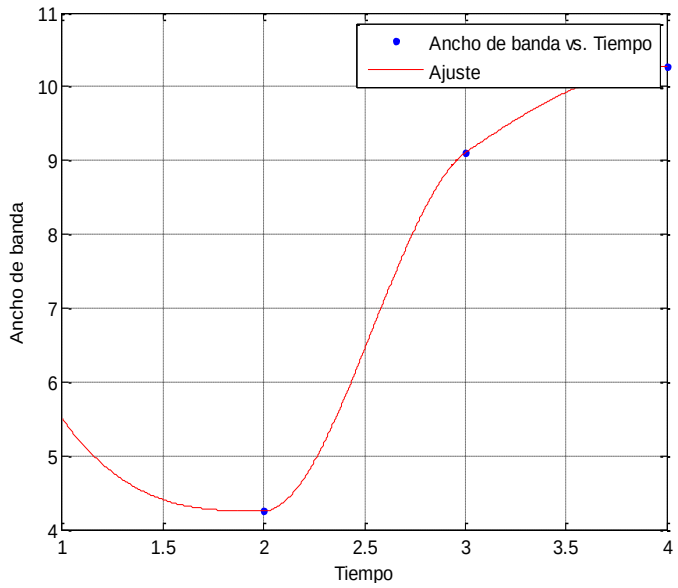


Figura 65. Gráfica datos proxy Energía

Tabla 28. Datos proxy Energía

PROXY ENERGÍA	
Semanas	Mbps
1	5,5
2	4,25
3	9,1
4	10,27
Media	**7,28**

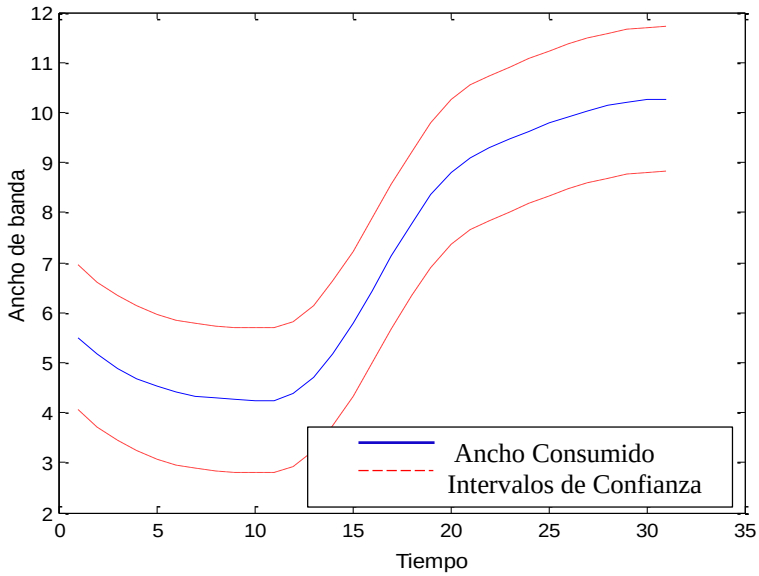


Figura 66. Gráfica para AB asignado Energía

Tabla 29. AB Energía

AB Asignado	
Mbps	Mbps
10,27	± 0,87
TOTAL	**12**

PROXY MED

```
>> [fitresult, Max] = createFit (Tiempo, Med);
   AB= 8
```

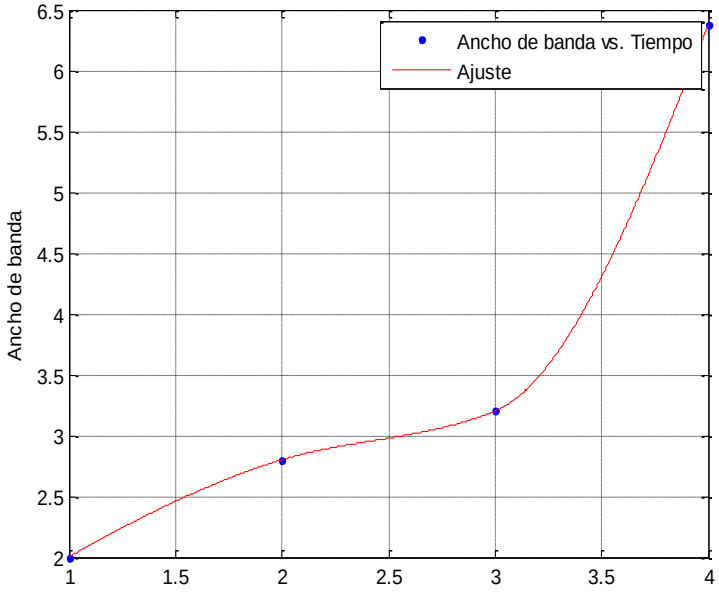


Figura 67. Gráfica datos proxy MED

Tabla 30. Datos proxy MED

PROXY MED	
Semanas	Mbps
1	0
2	2,8
3	3,2
4	6,38
Media	**3,6**

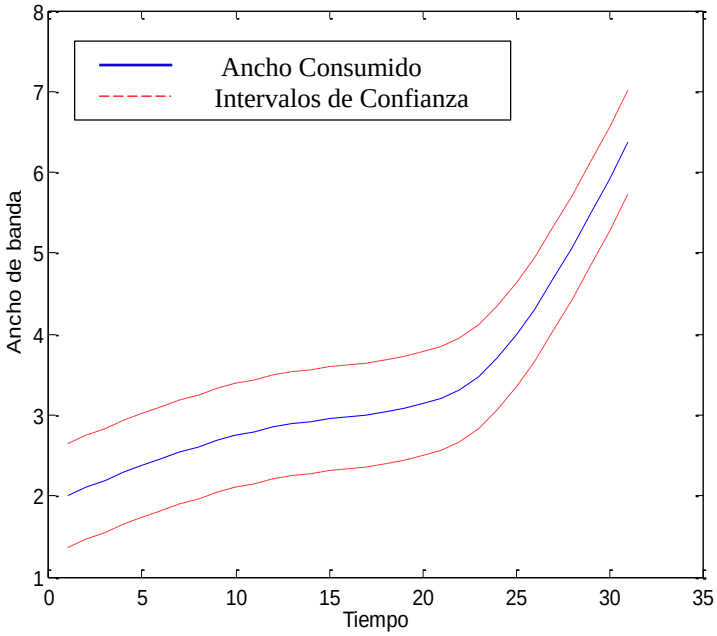


Figura 68. Gráfica para AB asignado MED

Tabla 31. AB MED

AB Asignado	
Mbps	Mbps
6,38	± 0,81
TOTAL	**8**

PROXY IDIOMAS

```
>> [fitresult, Max] = createFit (Tiempo, Idiomas);
AB= 2
```

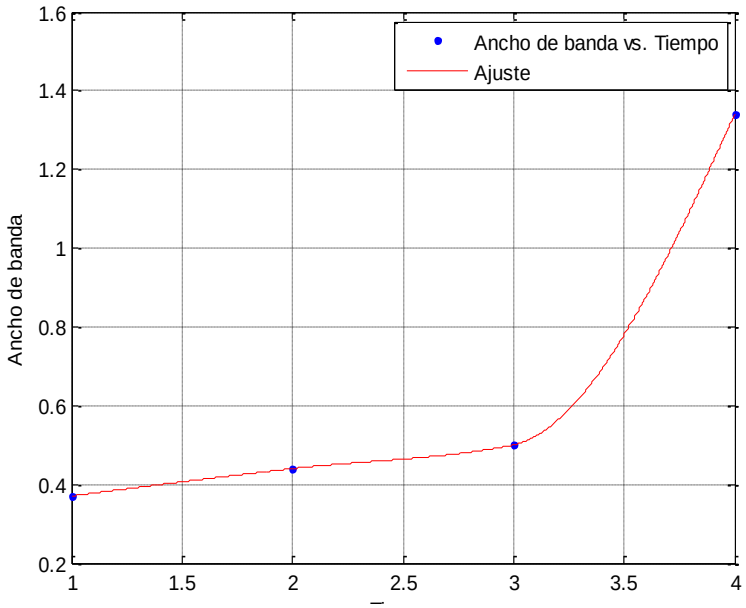


Figura 69. Gráfica datos proxy Idiomas

Tabla 32. Datos proxy Idiomas

PROXY IDIOMAS	
Semanas	Mbps
1	0,37
2	0,44
3	0,5
4	1,34
Media	**0,66**

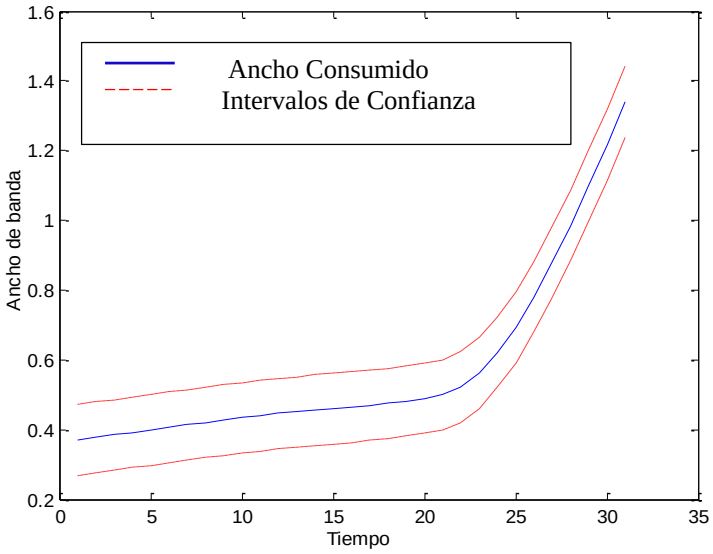


Figura 70. Gráfica para AB asignado Idiomas

Tabla 33. AB Idiomas

AB asignado	
Mbps	Mbps
1,34	± 0,33
TOTAL	**2**

PROXY WIRELESS

```
>> [fitresult, Max] = createFit (Tiempo, Wireless);
   AB= 20
```

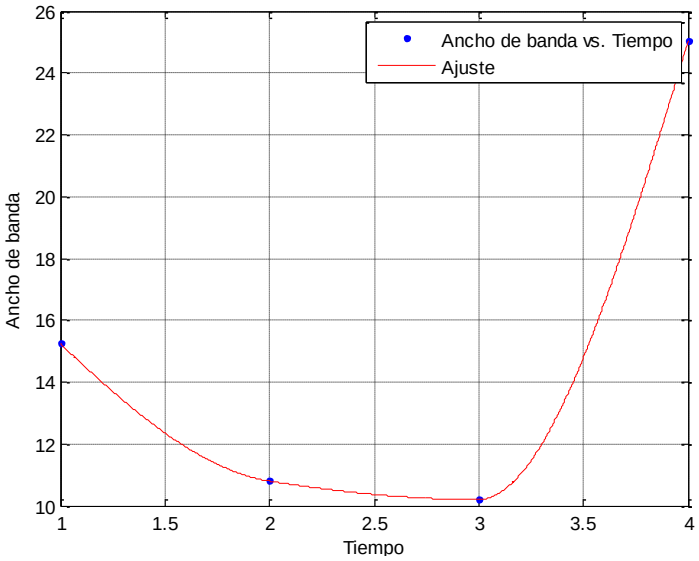


Figura 71. Gráfica datos proxy Wireless

Tabla 34. Datos proxy Wireless

PROXY WIRELESS	
Semanas	Mbps
1	15,25
2	10,8
3	10,2
4	17,4
Media	**13,41**

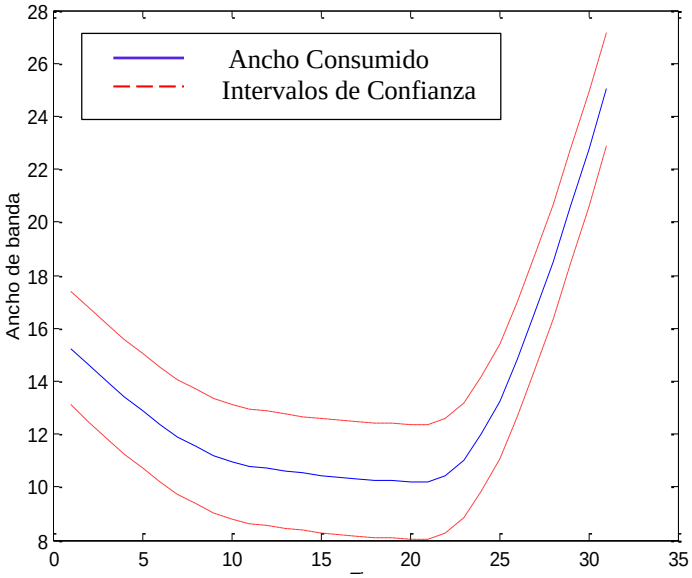


Figura 72. Gráfica para AB asignado Wireless

Tabla 35. AB Wireless

AB Asignado	
Mbps	Mbps
17,4	± 1,3
TOTAL	**20**

Con un ancho de banda asignado para cada área, la asignación de ancho de banda para la Universidad Nacional de Loja queda distribuida de la siguiente manera, tabla 36:

Tabla 36. Resumen de los AB asignados por proxy

DISTRIBUCIÓN DE ANCHO DE BANDA PARA LA UNL	
ÁREA	**ANCHO DE BANDA (Mbps)**
Educativa	7
Jurídica	7
Agropecuaria	3
Salud	4
Energía	12
Med	8
Idiomas	2
Wireless	20
TOTAL	**63**
Elaborado por: Évelin Alvarado Otero	

Los 36 Mbps de ancho de banda restantes, quedan a disposición para una asignación a Administración Central (no se pudo contar con información de consumo de ancho de banda de su proxy por falta de monitoreo) y para crecimiento futuro en la Universidad.

f.3.2 Cálculo ancho de banda para la Biblioteca del AEIRNNR

En virtud a la base de los datos proporcionados por el *SARG*, los usuarios potenciales del área de energía se encuentran en la biblioteca del área; para asignar un ancho de banda acorde a las necesidades del lugar y del estudiante, el proceso para la decisión de cuánto se le asigna a la biblioteca, se lo toma en función de eficiencia.

f.3.2.1 Designación del ancho de banda

El mal uso del ancho de banda, por parte de un usuario en particular, llega a comprometer el rendimiento de los servicios de la red y repercutir en la calidad del servicio. Es por esto que han surgido soluciones que implementan la asignación del ancho de banda por usuario.

Debido a que no existe información real en cuanto al uso de la red de la biblioteca del AEIRNNR que permita efectuar un análisis estadístico para posteriormente distribuir un ancho de banda adecuado para esta dependencia, dentro de los conceptos de eficiencia, para el presente proyecto se ha considerado aplicar una analogía entre el uso de una red de datos correspondiente a un cyber con la red de datos de la biblioteca, esto debido a la amplia similitud que se genera durante las visitas de los diferentes usuarios.

Al categorizar o clasificar al individuo dentro de un rango de eficiencia al momento de navegar, se le atribuye al usuario un ancho de banda asimétrico de entre 100Kbps a150Kbps. Indicadores institucionales, para la acreditación institucional, exigen 125kbps por alumno, para este proyecto se ha considerado un ancho de banda de 140 Kbps, manteniéndose cerca del valor del indicador; por lo tanto el ancho de banda para la biblioteca del área queda establecido de la siguiente manera:

$$AB = (140Kbps \cdot 36) \qquad \textbf{\textit{Ec. 1}}$$
$$AB = 5040\ Kbps$$

Siendo conscientes de las actuales aplicaciones y el respectivo peso que estas tienen en internet, en razón a los 36 puntos de accesos a Internet con los que se cuenta en la biblioteca, se determina, asignar un ancho de banda asimétrico de **5 Mbps** para su uso compartido, bajo parámetros de QoS descritos en el siguiente apartado.

f.4 Configuración y pruebas

RouterOS elegido para la implementación en la biblioteca del área, a continuación se muestra paso por paso la configuración del equipo según los requerimientos para las pruebas.

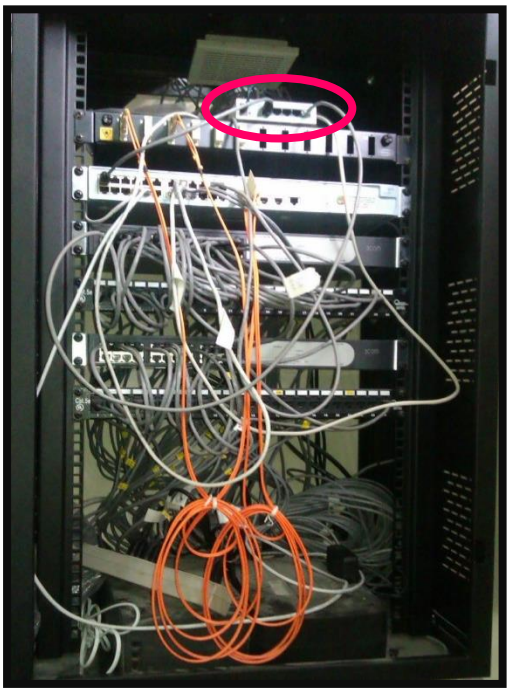


Figura 73. Ubicación del equipo en el armario de la biblioteca

f.4.1 Configuraciones básicas del equipo

f.4.1.1 Logueo al Mikrotik

Existen algunas formas de acceder al equipo al Mikrotik sin haber configurado nada previamente. Una manera es ingresando directamente desde la consola una vez finalizada la instalación, otro método es utilizando consola Telnet o SSH (Intérprete de Órdenes Segura) a través del puerto serie o Ethernet por mac o ip, o simplemente mediante la utilización del software winbox, del cual son dueños los mismos desarrolladores de Mikrotik. Se lo puede descargar desde la misma página web de mikrotik: www.mikrotik.com opción downloads, opción winbox.

Debido a la flexibilidad, rapidez y ventajas que presenta la utilización de winbox respecto a los otros métodos, esta fue la herramienta que se utilizó para la configuración del equipo. Desde una PC se ejecuta el soft Winbox, el cual nos despliega una ventana para loguearse al Mikrotik.

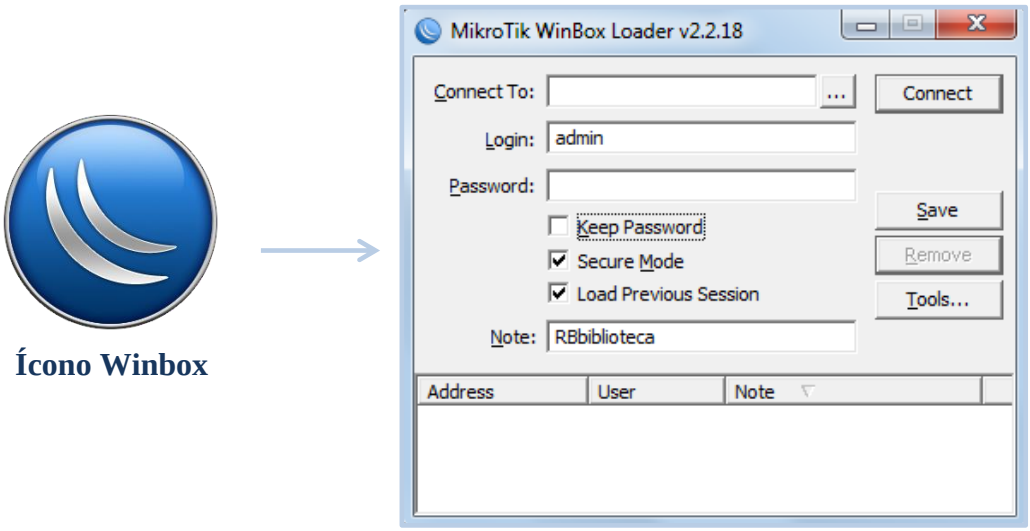


Figura 74. Herramientas Winbox para el logueo

En esta ventana, figura 74, se puede escribir las direcciones Mac o ip de la placa del Mikrotik a la cual estamos conectados. Hacer clic en (…) para que el mismo software escriba la dirección Mac de la interfaz al que se esté conectado al equipo. Cabe mencionar que cada uno de los cinco puertos del equipo tiene su respectiva dirección MAC, la dirección que muestre pertenecerá al puerto al que esté conectado al Mikrotik.

Una vez identificada la MAC de la interfaz, en Login escribir: admin y como Password: (en blanco). Al finalizar esta carga de datos hacemos clic en Connect. Luego de esto, el software inicia automáticamente una descarga de plugins, con el fin de tener los datos de lo configurado en el equipo para poder administrarlos remotamente.

Al finalizar la descarga aparece la pantalla de configuración del Mikrotik, figura 75. En la cual, en la parte superior encontramos información del estado del equipo tales como: la hora, espacio en la memoria, estado del procesador, el safe mode; a mano izquierda se encuentra el menú principal para configuración del equipo.

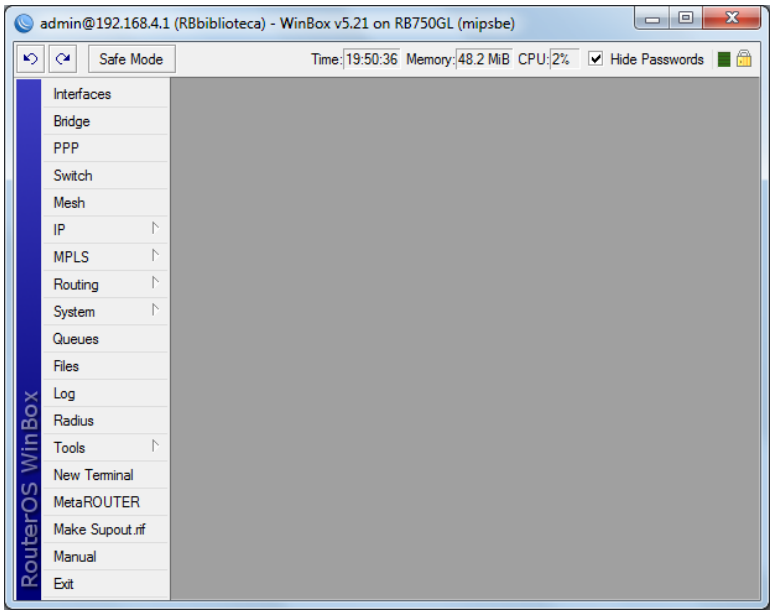


Figura 75. Pantalla principal de configuración

En el menú izquierdo muestra varias opciones de configuración, cada una de estas opciones despliega submenús que permiten acceder a cada una de las características de Mikrotik. Este menú varía dependiendo de la versión de versión y de equipo, las principales son:

Interface: Aquí se permite agregar, eliminar, habilitar, deshabilitar, definir diferentes tipos de interfaces a configurar. Se puede establecer Ethernet, *EoIP Tunnel*, *Mesh*, *Vlan*, etc.

Bridge: Administra conexiones tipo Bridge entre interfaces con diferentes opciones de filtrado para mejor manejo de tráfico.

Mesh: Permite configuración y administración de redes *Mesh*.

PPP: ya sea como cliente o como servidor, en el menú PPP se pueden habilitar túneles tipo: PPP *(Point to Point Protocol)*, PPTP *(Point to Point Tunneling Protocol)*, L2TP *(Layer 2*

Tunneling Protocol), OVPN *(Open Virtual Private Network)*, PPPOE *(Point to Point Over Ethernet*.

IP: contiene parámetros referentes a IP como por ejemplo: Addresses, Firewall, NAT, Hotspot, Routes, DHCP Server, DNS, Webproxy, etc.

MPLS: Permite la incorporación de MPLS *(Multiprotocol Label Switching)*, con la cual se puede administrar calidad de servicio QoS, ya que trabaja entre la capa 2 y capa 3 del modelo OSI.

Routing: <<Permite el uso de protocolos de enrutamiento como: OSPF (*Open Shortest Path First*), RIP (*Routing Information Protocol*), BGP (*Border Gateway Protocol*), MME *(Mesh Made Easy)*, este último utilizado para enrutar redes MESH, además permite la administración de filtros en el enrutamiento>>[15].

System: Permite administrar características internas del router como: el reloj, la velocidad del procesador, interfaces de administración, *passwords*, usuarios, etc., además de herramientas de diagnóstico de estado del router.

Queues: Permite la creación de estructuras de datos (colas), que ayudan una mejor gestión en la priorización de tráfico y control del mismo, limitación de velocidad.

Files: <<Ofrece la posibilidad del manejo de archivos de respaldo, actualización de paquetes RouterOS, o el manejo de script para funciones programadas del router>>[15].

Log: Permite visualizar un historial de cambios realizados sobre configuraciones del router, acceso de usuarios establecidos, errores suscitados y su hora respectiva.

Radius: Permite configurar la opción de autenticación a servidores Radius.

Tool: incorpora una serie de herramientas de diagnóstico y gestión de networking, como son: *Bandwidth Test* para pruebas de *throughput* del canal usado, IP Scan permite crear un registro ARP (*Address Resolution Protocol*) de los equipos conectados a una interface, Ping para pruebas ICMP de equipos remotos, Telnet usado para acceso y administración de otros equipos mediante capa 3 del modelo OSI, Torch permite visualizar el trafico ARP de las diferentes interface, así como el ancho de banda utilizado.

New Terminal: Permite la configuración y administración de todas las aplicaciones del router mediante línea de comandos.

f.4.1.2 Administración de usuarios

Crear un listado de usuarios que tendrán acceso para administración o simplemente lectura de las configuraciones es importante a la hora de implementar seguridades en nuestro router, permite establecer tres tipos de usuarios: full, de lectura y usuarios de escritura. En esta configuración están creados usuarios de full administración y de lectura.

Para crear un nuevo usuario, en el menú principal, damos clic en *System*, y dentro en el submenú se busca *User*. En la nueva ventana que aparece, figura 76, se da clic en el símbolo **(+)**, y en la nueva ventana se llena los campos con el nombre del usuario, el grupo al cual pertenecerá que puede ser: read, - grupo de lectura, full - opción para administración completa, y write – para modificar configuraciones pero no usuarios; y de ser necesario se puede definir las redes IP permitidas para la administración. Este usuario y clave le servirá para ingresar al equipo vía Winbox, vía web o vía SSH.

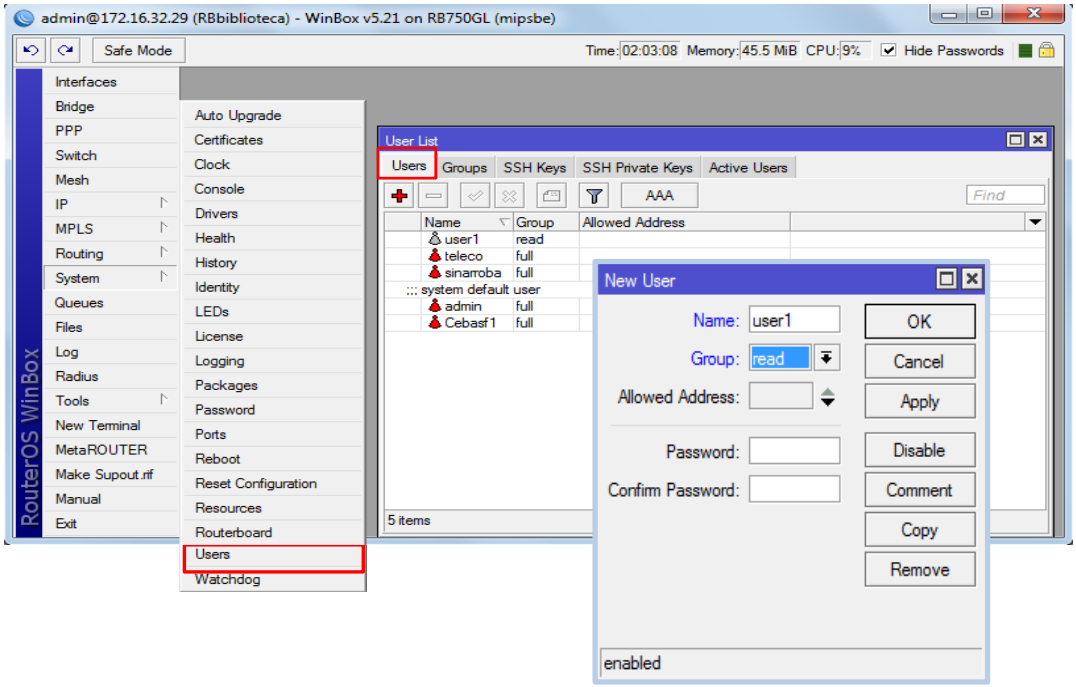


Figura 76. Lista de usuarios

Además es posible determinar que usuarios se encuentran activos dentro del equipo, en la pestaña *Active Users*, figura 77, aquí indica la dirección IP desde la que se ingresa al router, y la forma de acceso al equipo (WinBox, SSH, Web).

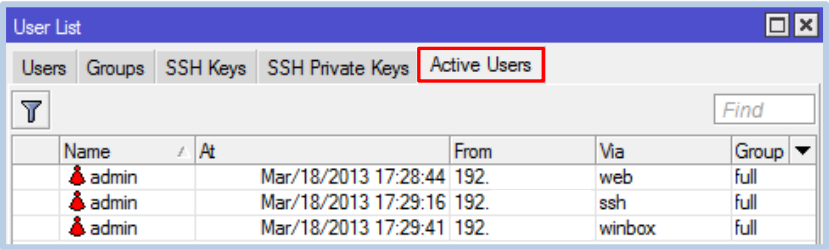


Figura 77. Lista de usuarios activos

f.4.1.3 Administración de los puertos para acceso al Mikrotik

La administración de los puertos que servirán para ingresar al equipo es muy importante definirlos desde el principio, para configurarlos nos dirigimos al menú principal y clic sobre IP, de los submenús que se despliegan seleccionamos *Services*, se abre una ventana, figura 78, en la que se muestra las posibles vías de acceso, en nuestro caso, quedarán habilitadas solamente ssh, winbox y www.

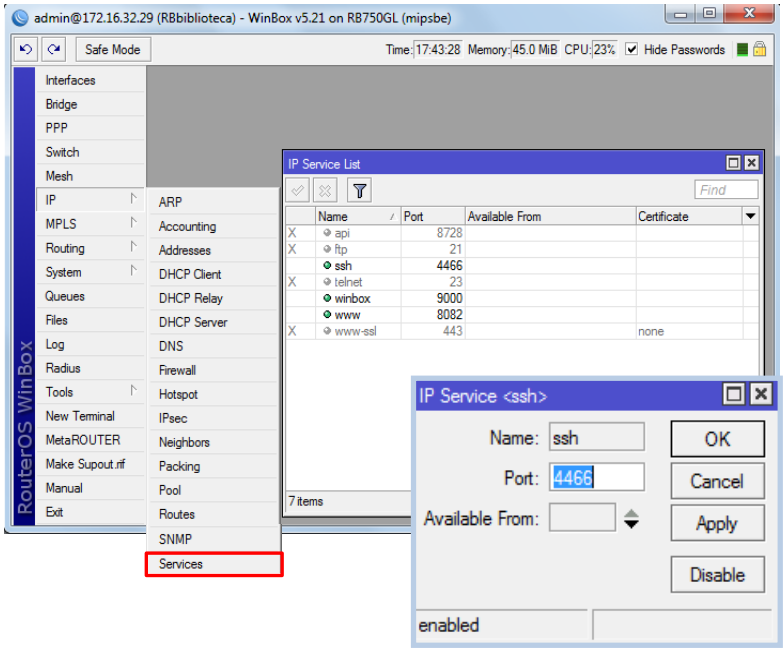


Figura 78. Administración de puertos de acceso

Haciendo doble clic sobre cualquiera de ellos, es posible cambiar el puerto que viene por defecto, por motivos de seguridad. En nuestro caso se ha configurado para ssh el puerto 4466, para web el puerto 5487 y para winbox el puerto 9000.

f.4.1.4 Definición y configuración de interfaces

El equipo cuenta con cinco interfaces ethernet, para configurarlas según nuestra necesidad; en la parte del menú principal, hacemos clic en el menú *Interfaces*, en donde se visualizarán las interfaces de las que dispone el equipo, figura 79. Inicialmente previo a cualquier configuración, las cinco interfaces que presenta el equipo son: ether1, ether2, ether3, ether4, ether5.

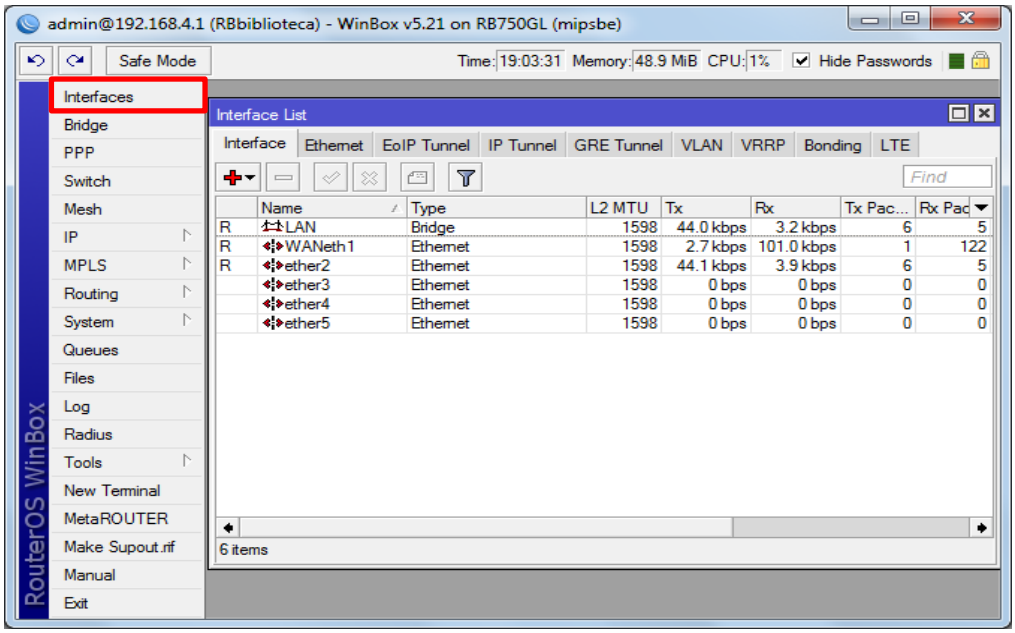


Figura 79. Pantalla Interfaces

En la figura 79, se visualizan ya las interfaces configuradas, a continuación la configuración de la ether1 como WANeth1, figura 80, que es la interface por la que se proveerá de internet al equipo. Doble clic sobre la interface ether1 y se configura los siguientes parámetros:

Pestaña *General*:

Name: WANeth1

MTU: 1500 (*Default*)

ARP: enabled (*Default*)

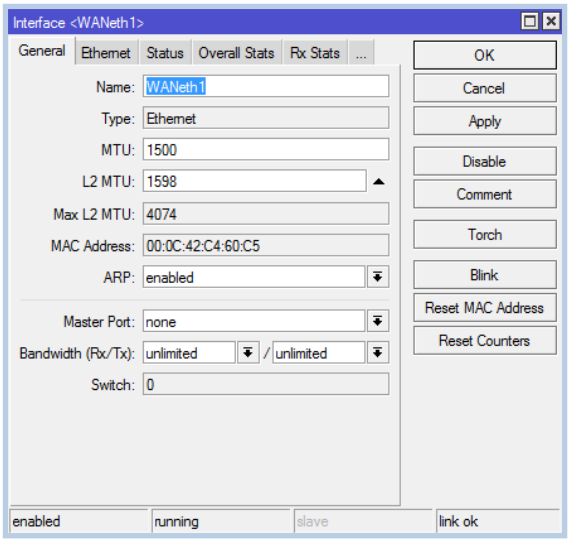


Figura 80. Ether1: Pestaña General

Pestaña *Ethernet*:

Speed: 100Mbps: seleccionado

Auto Negotiation: seleccionado (*Default*)

Full duplex: seleccionado (*Default*)
Clic Apply

Clic OK

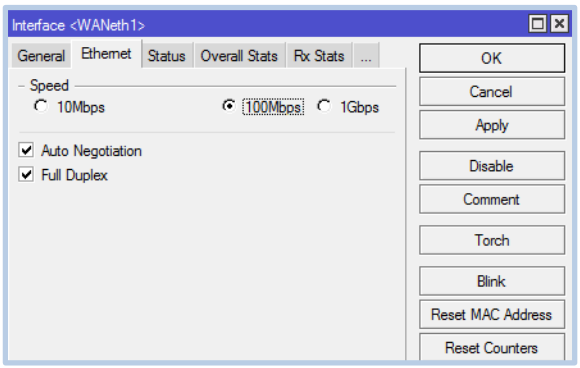


Figura 81. Ether1: Pestaña Ethernet

Pestaña *Status*:

- En esta ventana podemos ver el estatus la interface actual.

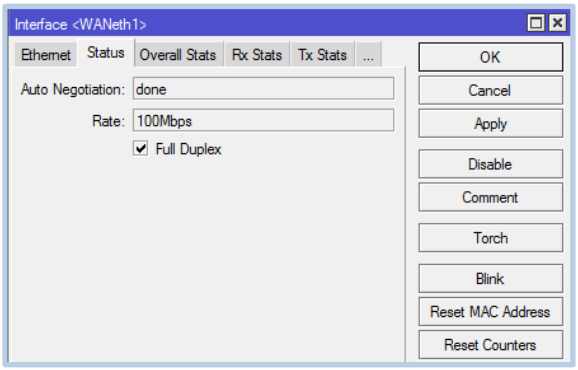


Figura 82. Ether1: Pestaña Status

Pestaña *Traffic*:

1. Vemos la gráfica de kbps enviados y recibidos por dicha interface.
2. Vemos la gráfica de p/s enviados y recibidos por la interface.

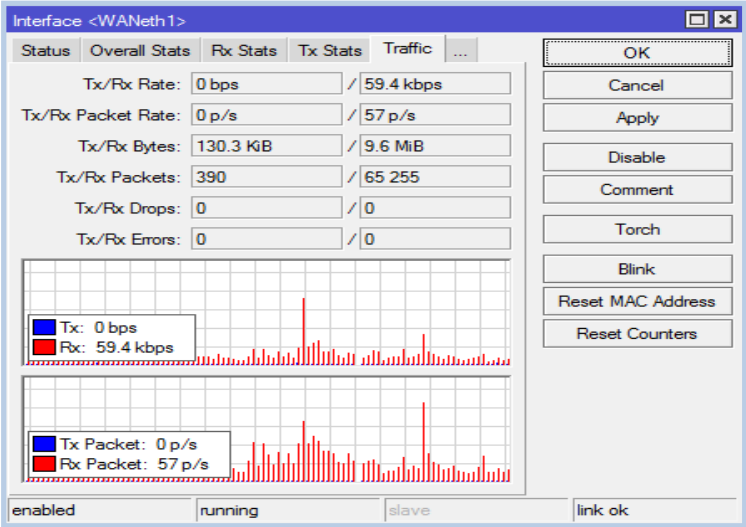


Figura 83. Ether1: Pestaña Traffic

Para la configuración de las ether 2, 3, 4, 5, no se realiza ningún cambio en los parámetros, vienen configuradas por *default*, en caso de necesitarlas para alguna otra tarea, se cambia los parámetros expuestos en la 80 y 81, según sea el requerimiento; para este caso no se necesitan configuraciones especiales.

En la figura 79, se observa una interface llamada LAN, esta interface es creada por el mismo administrador configurada en modo *Bridge* para los puertos ether 2, 3, 4, 5, para que exista una misma configuración en cualquiera de las interfaces al momento de conectarse al equipo. Para esta configuración, en la barra de menús de la parte izquierda, clic en *Bridge*, figura 84.

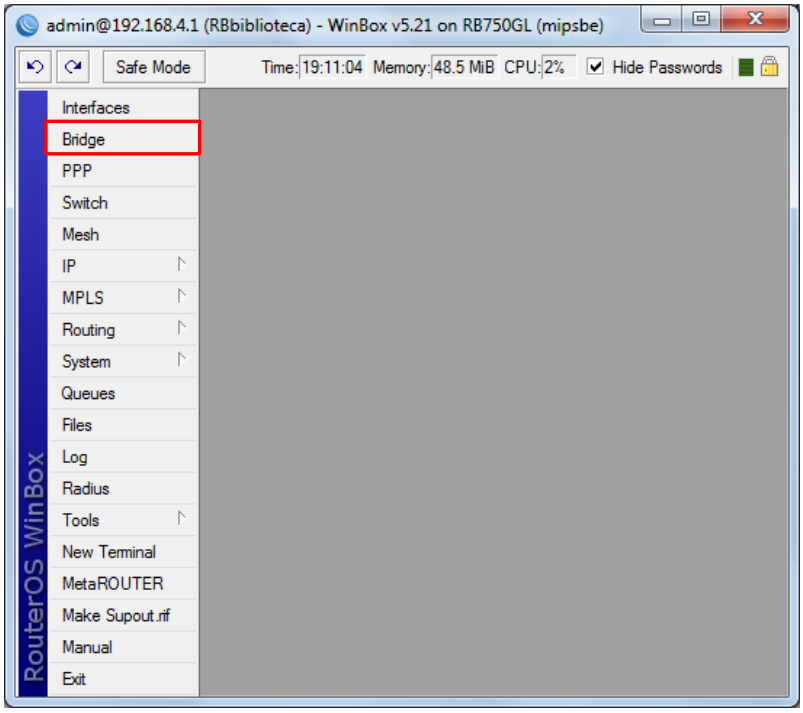


Figura 84. Configuración del Bridge

Aparecerá una venta Bridge, y se configura lo siguiente:

Pestaña *Bridge*:

1. **Clic en (+)**

   Name: LAN

   Type: Bride (*Default*)

   MTU: 1500 (*Default*)

   ARP: enabled (*Default*)

   Clic Apply

   Clic OK

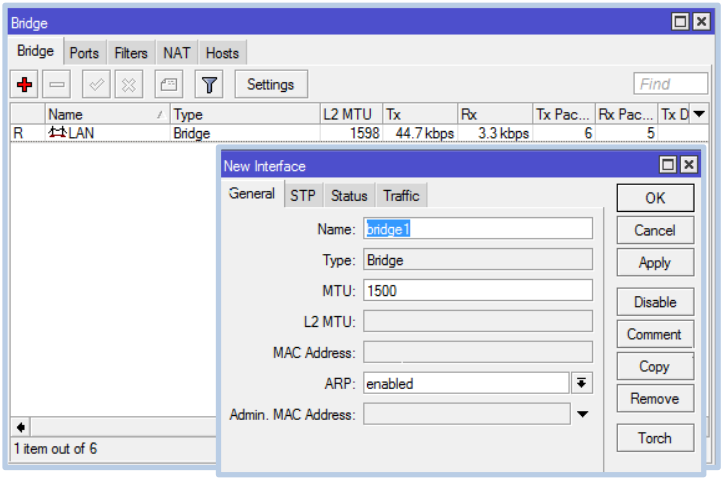


Figura 85. Bridge

Pestaña *Ports*:

1. **Clic en (+)**

   Interface: ether 2, 3, 4, 5

   Type: Seleccionar LAN

   Priority: 80 (*Default*)

   Path Cost: 10 (*Default*)

   Clic Apply

   Clic OK

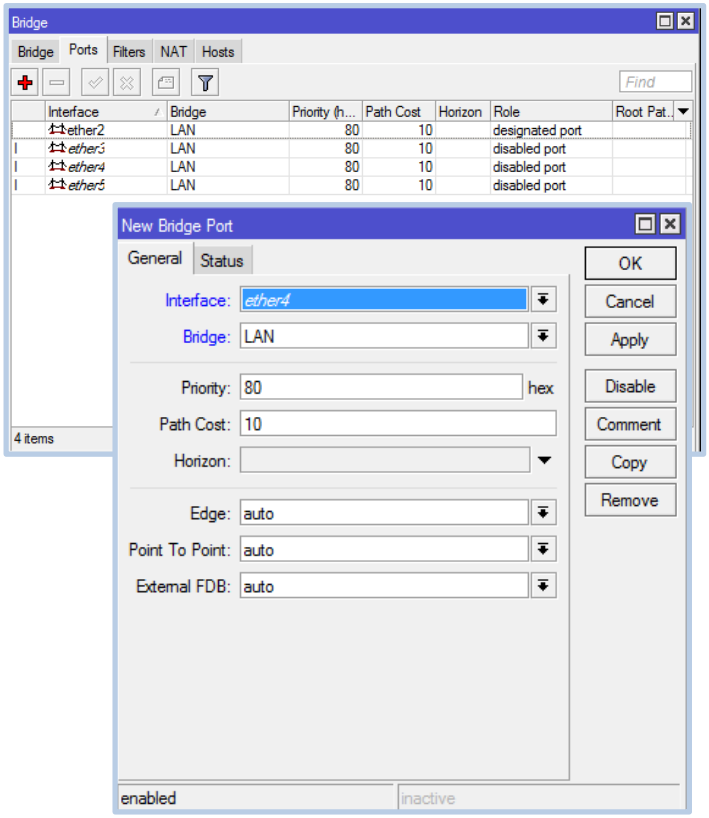


Figura 86. Bridge pestaña Ports

f.4.1.5 Configuración TCP/IP

Para el ingreso y configuración de cualquier tipo de router es necesaria la configuración de una dirección IP, para ingresarla nos dirigimos al menú principal, clic en el menú *IP*, y en el listado desplegado se escoge *Addresses*, se hace clic sobre el icono del signo **(+)**, figura 87; en la pantalla desplegada se indica cuatro campos: la dirección IP (Address), la máscara de subred, la dirección de red, y la interface que va a asumir dicha IP. Se ingresa los datos de la dirección IP, la red y la interface, ya que la dirección de *Network* es calculada automáticamente.

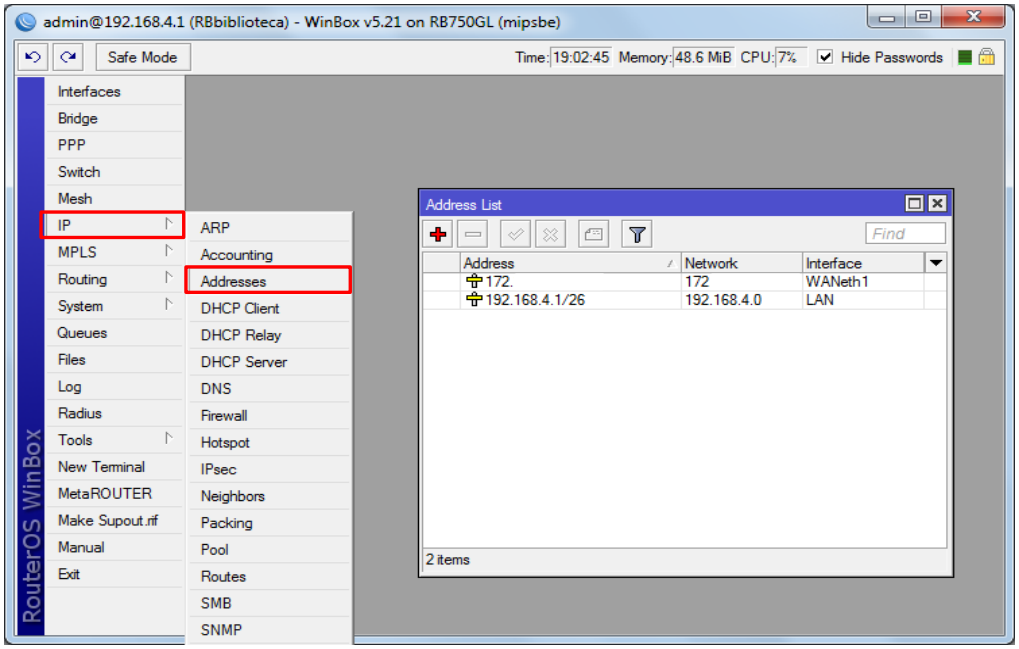


Figura 87. Addresses List

IP para internet (Interface WAN):

1. **Clic en (+)**

   Address: 172.xx.xx.xx/19

   Clic Apply

   Network: 172.xx.xx.xx

   Interface: WANeth1

   Clic OK

IP para red interna (Interface LAN):

1. **Clic en (+)**

   Address: 192.168.4.1/26

   Clic Apply

   Network: 192.168.4.0

   Interface: LAN

   Clic OK

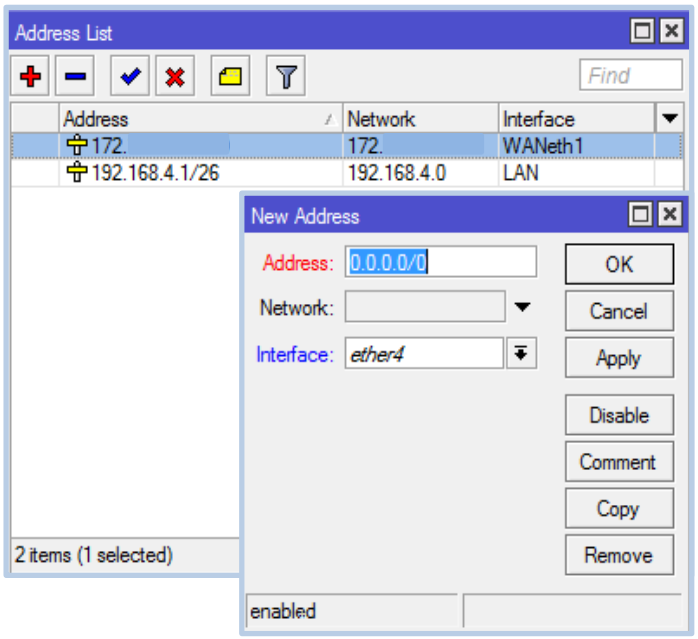


Figura 88. Configuración Address List

f.4.1.6 Puerta de enlace (*GATEWAY*)

La puerta de enlace permite la comunicación desde una red hacia otra red o grupo de redes, incluyendo Internet, especifica las rutas que deben seguir para alcanzar a un determinado host. Para configurar la dirección de Gateway, del menú principal, clic sobre IP y en los submenús que se despliegan, clic en *Routes*, figura 89, y configuramos lo siguiente.

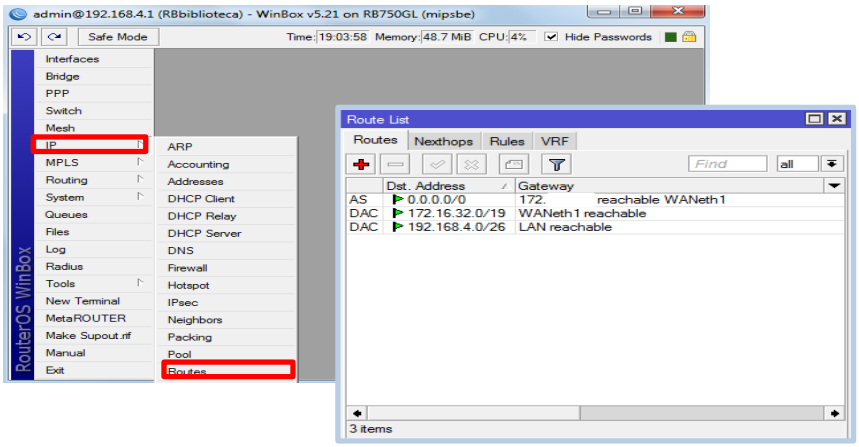


Figura 89. Gateway

Pestaña *Routes*:

1. **Clic en (+)**

Dst. Address: 0.0.0.0/0

Gateway: 172.xx.xx.xx

Type: unicast (*Default*)

Distance: 1 (*Default*)

Scope: 30, 10 (*Default*)

Clic Apply

Clic OK Figura

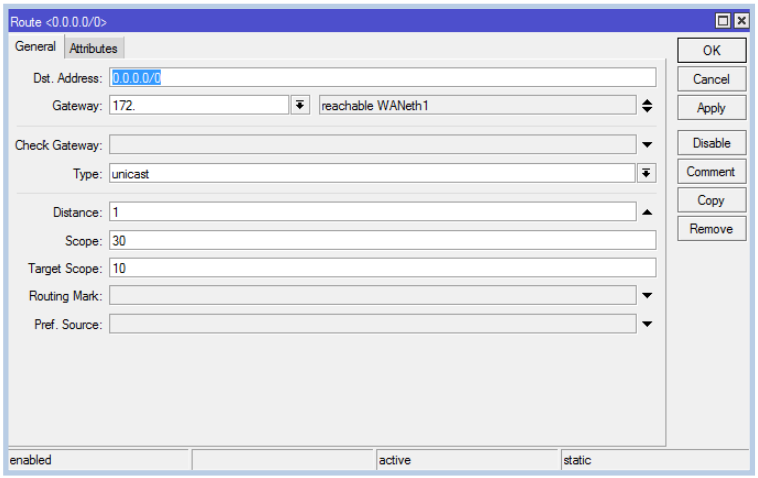


Figura 90. Configuración del Gateway

RouterOS utiliza un "*default destination-address*" 0.0.0.0/0, los ceros indican que todas las redes con cualquier máscara pueden ser alcanzadas por el equipo, mediante el *Gateway* especificado. Como se muestra en la figura 90, existen dos parámetros más:

WANeth1 reachable y LAN reachable, éstas dos se crean por *default* el momento que configuramos el submenú Address.

f.4.1.7 DNS

Los servidores DNS permiten la traducción de direcciones de red inteligibles para humanos a dígitos binarios asociados a servidores host. RouterOS permite hacer DNS Caching, esto significa que RouterOS utiliza una sola vez los DNS's del ISP, y para los equipos conectados a él los entrega directamente, esto significa que un equipo conectado detrás del router con RouterOS no necesita ir hasta un servidor DNS del ISP, sino que realiza el traslado directamente del equipo RouterOS, en un tiempo mucho menor. Para ingresar servidores DNS, en el menú principal se busca IP, se despliega un submenú y seleccionamos DNS, figura 91, se abre una ventana de configuración.

DNS *Settings*:

Servers: 172.xx.xx.xx

✓ **Allow Remote Requests**

Max UDP: 4096 (*Default*)

Cache Size: 2048

Cache Used: (*Default*)

Clic Apply

Clic OK

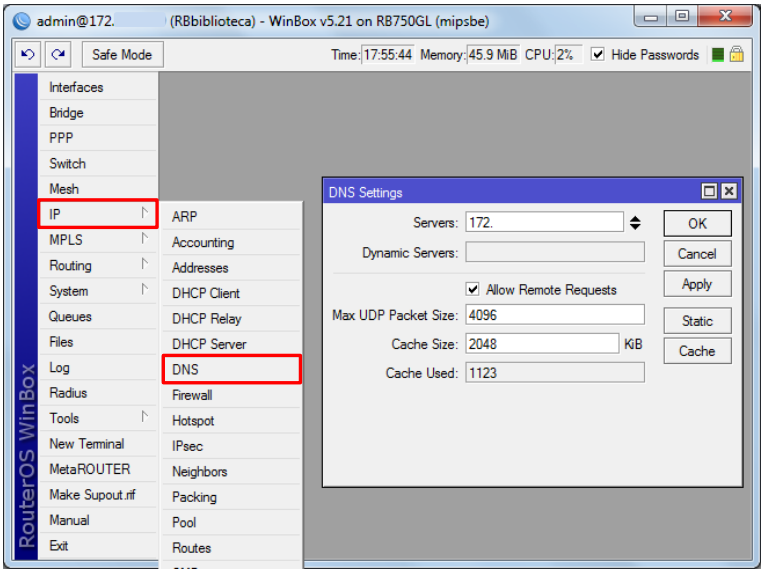


Figura 91. Configuración DNS

f.4.1.8 Configuración del DHCP Server.

Muchas veces los proveedores de Internet, permiten a sus clientes obtener direcciones IP automáticamente vía DHCP. Mikrotik tiene la capacidad de funcionar como un servidor DHCP, y administrar múltiples servidores DHCP con diferentes direcciones IP, esto

significa que se puede asignar toda la información necesaria a nuestros clientes de forma automática.

Para acceder al DHCP modo Server, del menú principal, clic sobre *IP*, de la lista que se despliegan seleccionamos *DHCP Server*, y se abre una ventana para la configuración; hacemos clic en *DHCP Setup*, figura 92, para ésta configuración se abrirán algunas ventanas; esta es una forma sencilla e intuitiva de configurar un servidor DHCP.

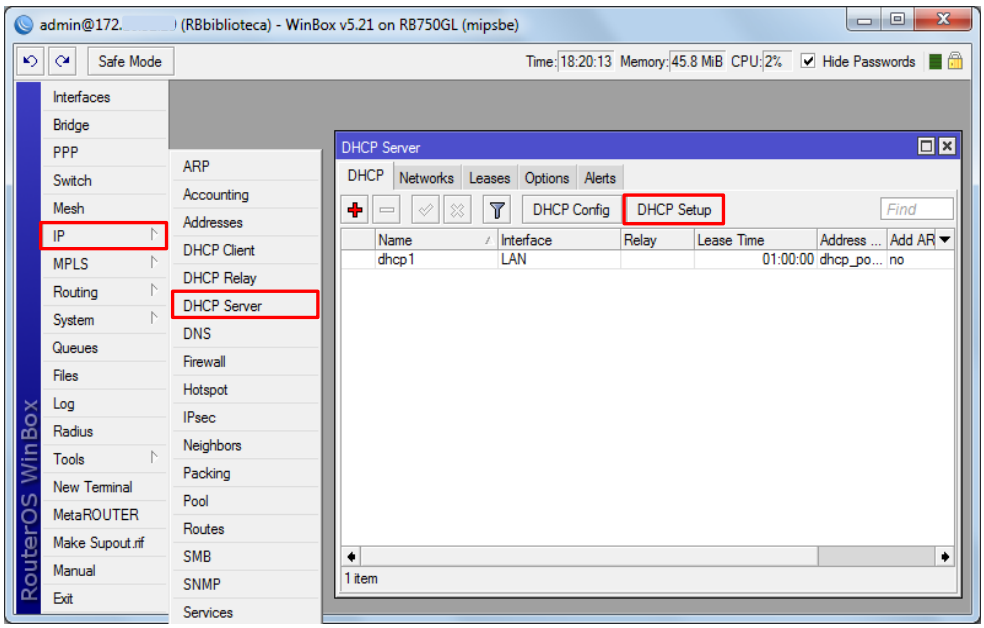


Figura 92. Configuración servidor DHCP

Aparecerá una pantalla solicitando la interface donde se va a crear el DHCP server, figura 93, es importante tener en cuenta que el DHCP correrá sobre una interface. Damos clic en la viñeta para desplegar y seleccionamos la interface LAN.

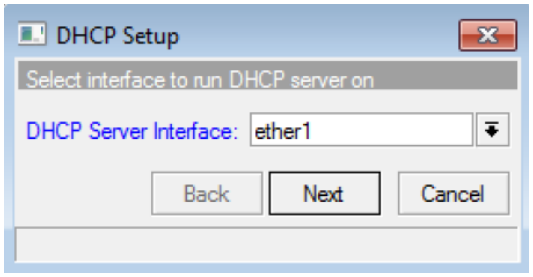


Figura 93. Interface DHCP servidor

A continuación preguntará la red de direcciones IP que administrará, esta deberá también ser incluida en la lista de direcciones como puerta de enlace de la subred DHCP, figura 94.

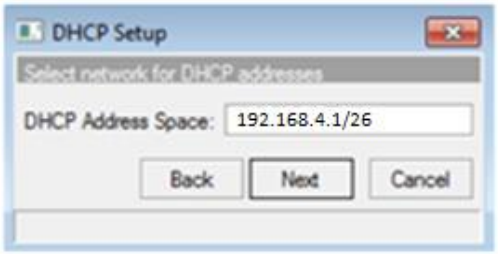


Figura 94. Asignación de red DHCP

Lo siguiente a configurar será el rango de IP's que serán designados. Figura 95.

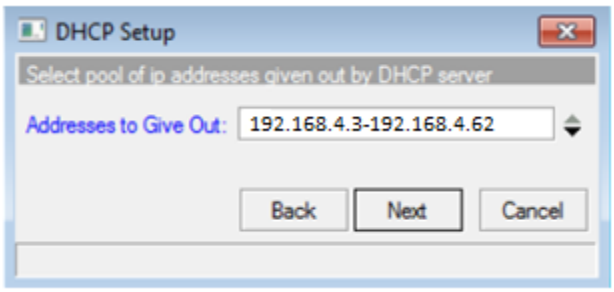


Figura 95. Configuración rango DHCP

Y al final el servidor DNS. Figura 96.

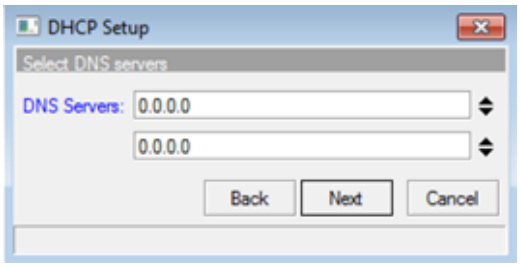


Figura 96. Configuración servidores DNS para DHCP

Finalmente se configurará el tiempo en *Leases Time*, que es el tiempo que se guardará la dirección IP antes de ser reasignada automáticamente hacia otro cliente, y con esto indicará que la configuración ha sido completada satisfactoriamente.

Una vez que se ha finalizado con la configuración, en la pestaña DHCP aparece la primera configuración, doble clic, y se despliega la ventana DHCP Server <dhcp1>, figura 97, con las configuraciones realizadas.

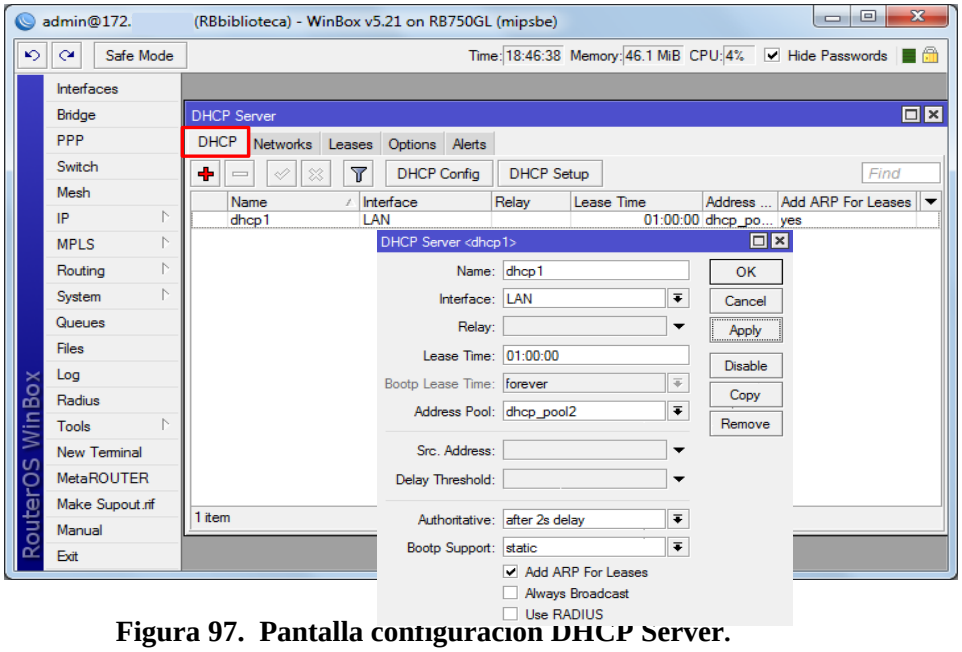


Figura 97. Pantalla configuración DHCP Server.

Para poder comprobar el pool de IPs o cambiarlo de rango, en el menú principal clic en IP y de los submenús que se despliegan clic sobre *Pool*, figura 98, se abre una ventana de *IP Pool*, en la pestaña Pools se encuentra ya creada el dhcp_pool2, que es la que corresponde al pool de IPs que se generó automáticamente al configurar el *DHCP Server*. Doble clic sobre dhcp_pool2 para que se despliegue la ventana de configuración en el caso de necesitar cambiar el rango.

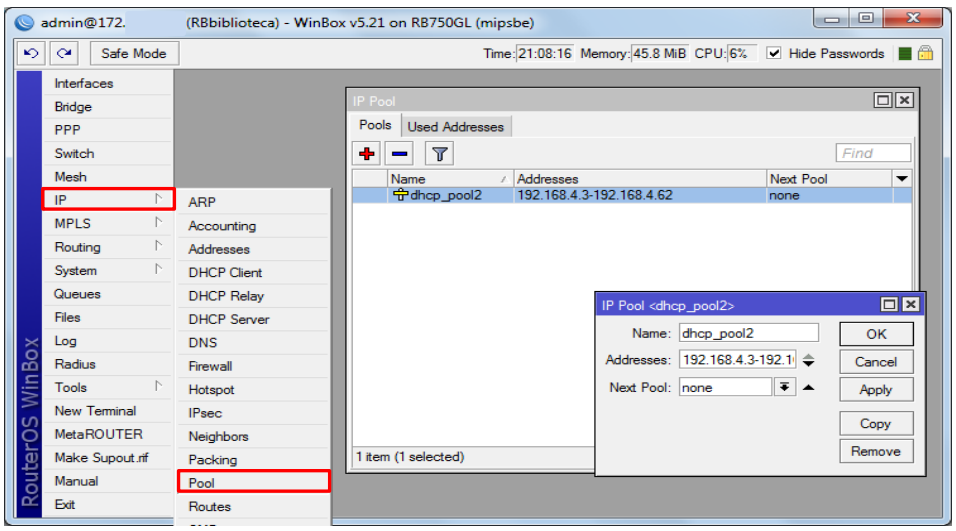


Figura 98. Ventana para visualizar el Pool de IPs.

Regresando a la revisión del *DHCP Server* creado, dentro de la pestaña *Networks* se crea también información del direccionamiento de la red interna, doble clic, y se despliega la ventana DHCP *Network* <192.168.4.0/26>, figura99, y se observan los parámetros que configuramos previamente; también es posible configurar DNS Domain, WINS en caso de trabajar con servidores de red internos, Domain para trabajar dentro de un dominio de red, NTP server para sincronizar la fecha en todos los equipos con asignación DHCP, etc.

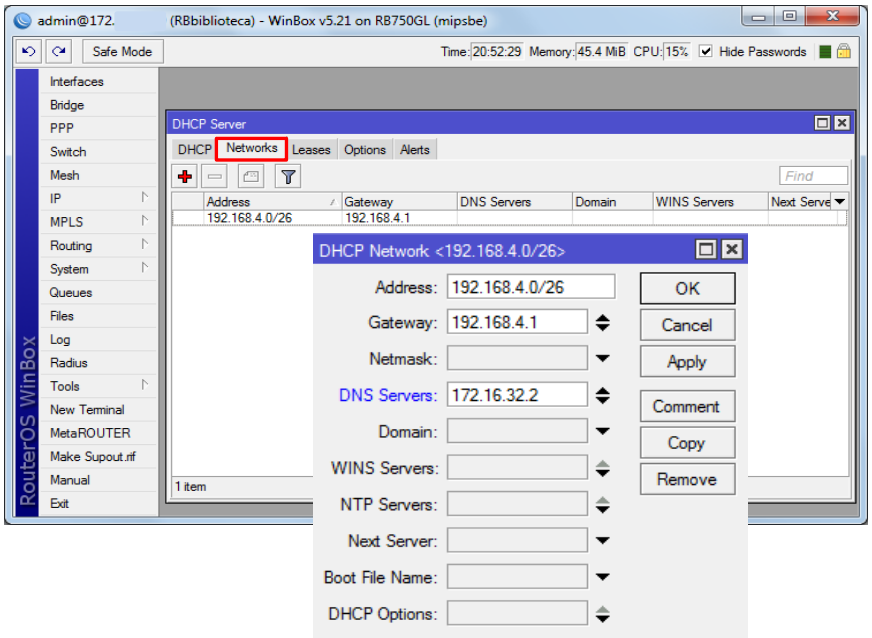


Figura 99. Pantalla configuración DHCP Network.

f.4.1.9 Servidor SNTP

Este es un protocolo utilizado para la sincronización de hora y fecha en servidores y equipos en general. Para configurar como cliente al SNTP, se ingresa al menú principal, clic en *System*, de los submenús que se despliegan se da clic en *SNTP Client*, figura 100. A continuación se habilita el servicio agregando un visto en la opción *Enabled*. En este modo se escoge la opción *unicast*, ya que se recibirá la información desde un servidor a un solo equipo router, y en los campos Primary NTP Server, y Secondary NTP Server se ingresará las direcciones IP de los servidores NTP que se usará.

Estos pueden ser servidores locales, o servidores públicos; en el caso del equipo están puestos direcciones de servidores públicos, por ejemplo server 1: 200.58.118.148, server 2: 146.164.53.65. El resto de parámetros tienen la función de *display* para indicar detalles de actualizaciones y operaciones del SNTP.

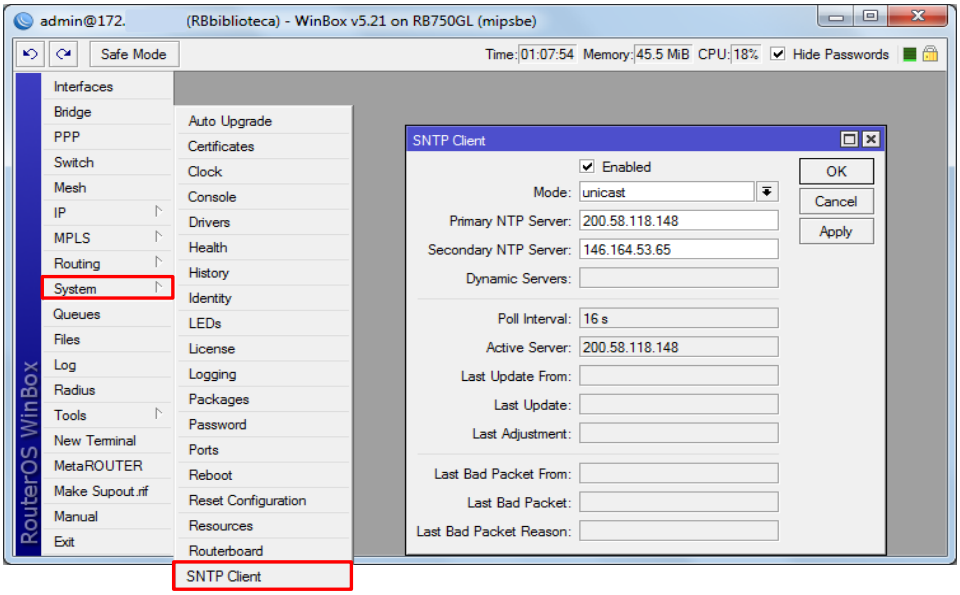
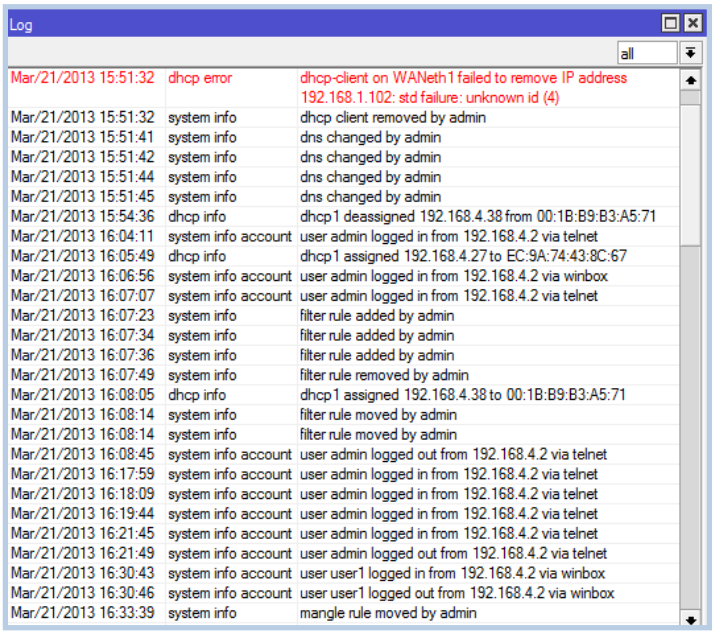


Figura 100. Configuración SNTP

f.4.1.10 Registros

Mikrotik tiene un sistema de registros que muestra cambios, errores del sistema, y ayuda a diagnosticar problemas que se generan en la configuración del router. Para acceder al registro, desde el menú principal se hace clic en Log, y abrirá una ventana que indica con fecha y hora la información del sistema, información del DHCP, información de qué cuenta se loguea al equipo, cambios realizados al equipo y por qué cuenta, etc. Figura 101.



Log

all

Mar/21/2013 15:51:32	dhcp error	dhcp-client on WANeth1 failed to remove IP address 192.168.1.102: std failure: unknown id (4)
Mar/21/2013 15:51:32	system info	dhcp client removed by admin
Mar/21/2013 15:51:41	system info	dns changed by admin
Mar/21/2013 15:51:42	system info	dns changed by admin
Mar/21/2013 15:51:44	system info	dns changed by admin
Mar/21/2013 15:51:45	system info	dns changed by admin
Mar/21/2013 15:54:36	dhcp info	dhcp1 deassigned 192.168.4.38 from 00:1B:B9:B3:A5:71
Mar/21/2013 16:04:11	system info account	user admin logged in from 192.168.4.2 via telnet
Mar/21/2013 16:05:49	dhcp info	dhcp1 assigned 192.168.4.27 to EC:9A:74:43:8C:67
Mar/21/2013 16:06:56	system info account	user admin logged in from 192.168.4.2 via winbox
Mar/21/2013 16:07:07	system info account	user admin logged in from 192.168.4.2 via telnet
Mar/21/2013 16:07:23	system info	filter rule added by admin
Mar/21/2013 16:07:34	system info	filter rule added by admin
Mar/21/2013 16:07:36	system info	filter rule added by admin
Mar/21/2013 16:07:49	system info	filter rule removed by admin
Mar/21/2013 16:08:05	dhcp info	dhcp1 assigned 192.168.4.38 to 00:1B:B9:B3:A5:71
Mar/21/2013 16:08:14	system info	filter rule moved by admin
Mar/21/2013 16:08:14	system info	filter rule moved by admin
Mar/21/2013 16:08:45	system info account	user admin logged out from 192.168.4.2 via telnet
Mar/21/2013 16:17:59	system info account	user admin logged in from 192.168.4.2 via telnet
Mar/21/2013 16:18:09	system info account	user admin logged in from 192.168.4.2 via telnet
Mar/21/2013 16:19:44	system info account	user admin logged in from 192.168.4.2 via telnet
Mar/21/2013 16:21:45	system info account	user admin logged in from 192.168.4.2 via telnet
Mar/21/2013 16:21:49	system info account	user admin logged out from 192.168.4.2 via telnet
Mar/21/2013 16:30:43	system info account	user user1 logged in from 192.168.4.2 via winbox
Mar/21/2013 16:30:46	system info account	user user1 logged out from 192.168.4.2 via winbox
Mar/21/2013 16:33:39	system info	mangle rule moved by admin

Figura 101. Registro del sistema

Mikrotik permite llevar un registro de varios tipos de aplicaciones que corren sobre él y pueden ser activados de forma individual en función de su requerimiento. Para activar de forma individual estos registros en el menú principal se busca System / Logging, se da un clic sobre el símbolo **(+)**, figura 102, en Topics se busca la aplicación de la que se necesita llevar registro. *Action*: memory (si se desea que se guarden los datos) o echo (sólo para tener conocimiento de la acción), clic en Apply, clic **OK.**

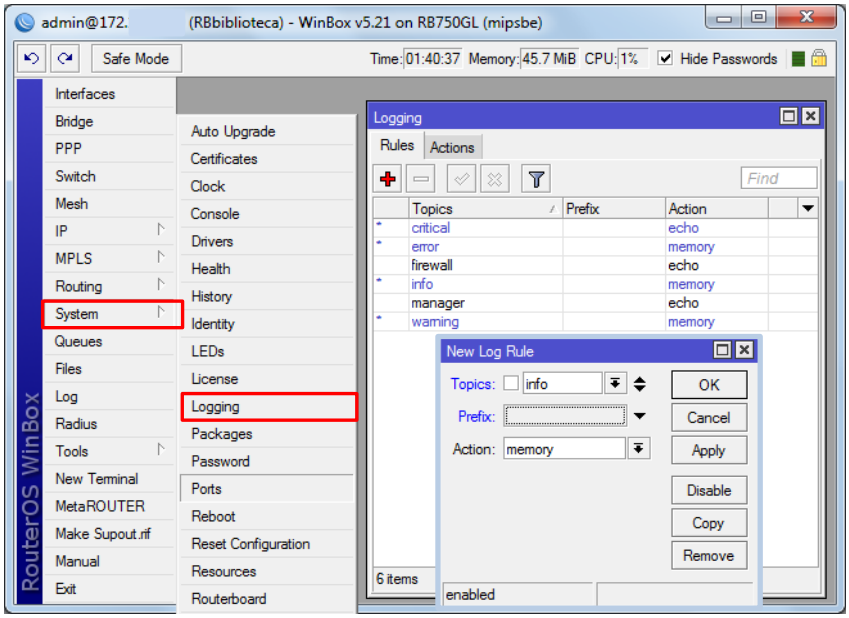


Figura 102. Temas del registro

En el equipo están configurada *manager*, que muestra configuraciones en el equipo por parte del administrador (*system info*), la asignación que el equipo realiza a los usuarios que se conectan (*dhcp info*), personas que ingresan al equipo Mikrotik (*system info account*).

f.4.2 Manejo de Archivos de Respaldo del Sistema (BACKUP)

f.4.2.1 Respaldo del Sistema

Mikrotik permite guardar las configuraciones o cambios realizados en su configuración; para guardar un respaldo, en el menú principal clic sobre Files, aparecerá una ventana de *File List*, se hace clic sobre el botón *Backup*, figura 103, esto crea un archivo MikroTik-xxxxxxxx-0000.backup, mediante el botón copiar, o arrastrando el archivo directamente a una carpeta en el escritorio de la PC, se guardará el respaldo generado.

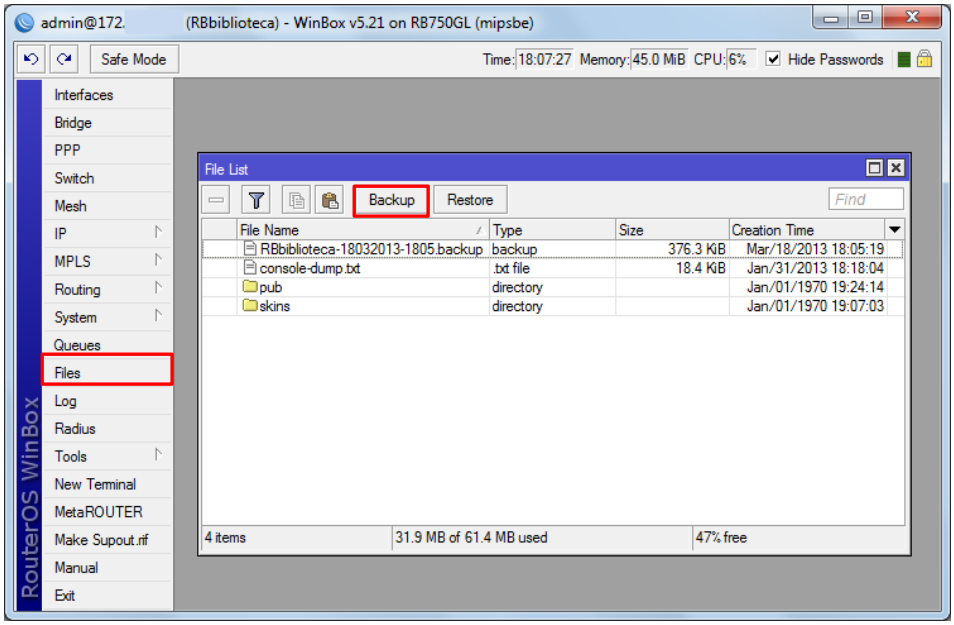


Figura 103. Respaldo de configuraciones

Para restaurar una configuración previamente guardada se copia el archivo guardado, dentro de la ventana *File List* se da un clic en el botón pegar, una vez se comprueba que el archivo fue copiado en el Mikrotik, clic sobre *Restore*; rápidamente indicará que es necesario reiniciar el equipo, finalmente clic sobre el botón yes.

f.4.3 Configuraciones IP/FIREWALL

El firewall, por defecto lee las reglas de arriba hacia abajo y sale con la primera que se encuentra configurada. Se usa la orden passthrough para obligar a que, luego de cumplirse una regla, se siga con las demás. Es muy similar a iptables. En el siguiente esquema, figura 104, se puede ver cómo se produce el flujo de los paquetes dentro del firewall de un Mikrotik.

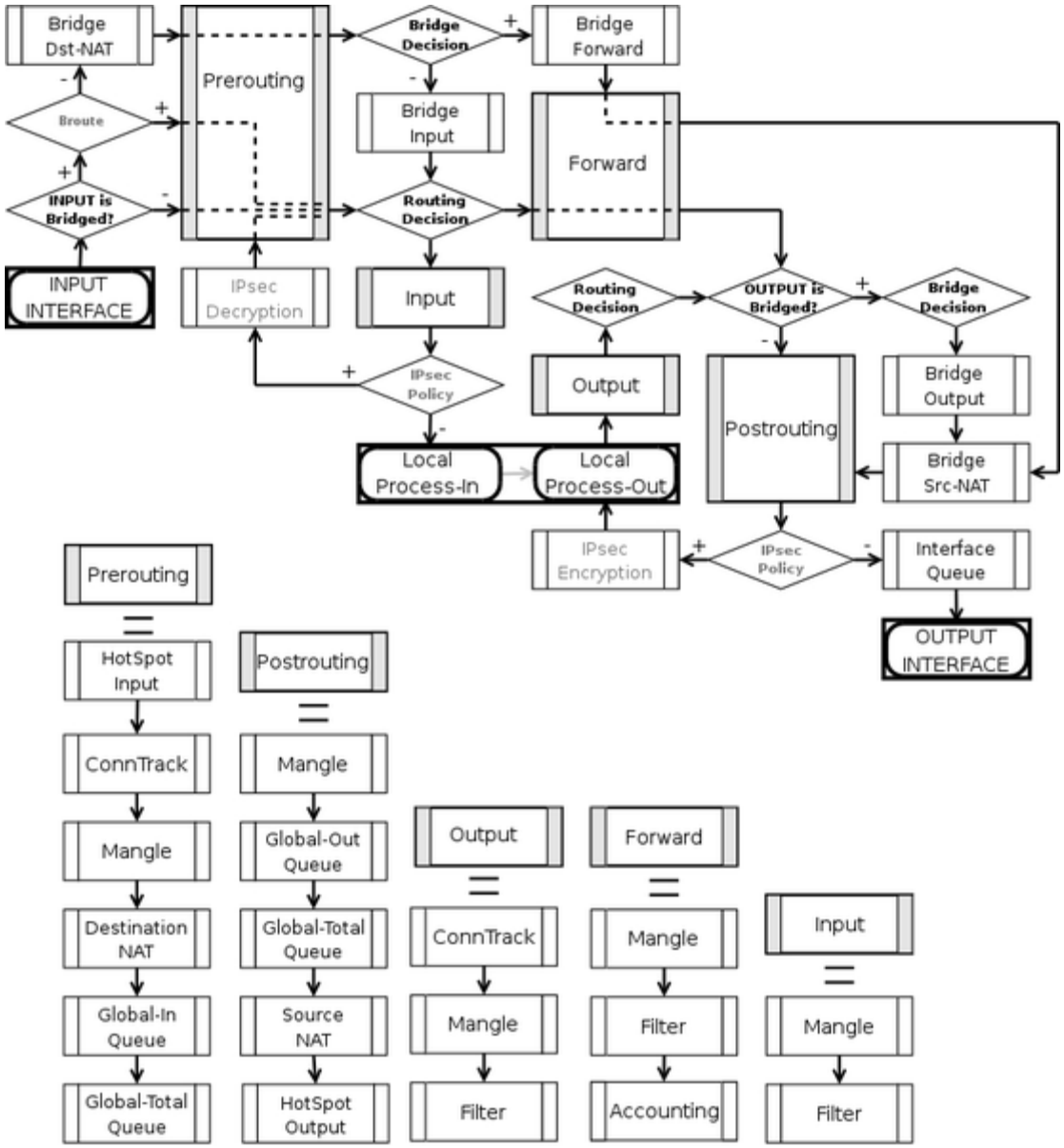


Figura 104. Proceso de flujo de paquetes [16]

HINOJOSA, Rod. *"Calidad de Servicio, Quality of Service"*. Año 2005. Disponible en: < http://www.slideshare.net/RodHinojosa/calidad-de-servicio-qoshttp://profesores.elo.utfsm.cl/~agv/publications/2006/senacitel/DenzerLopezGonzalezSubmitted.pdf>. [En línea].

Es conviene empezar configurando las reglas de estado, con el propósito de ahorrar procesamiento y acelerar los procesos para las conexiones ya establecidas y las relativas. Del menú principal clic sobre IP, luego de los submenús que se despliegan clic sobre *Firewall* y se abrirá una ventana llamada Firewall, figura 105, en este submenú se

configurará la mayor parte del equipo con lo concerniente a reglas de filtro, NAT, Mangle, Listas de direcciones y protocolos de capa 7.

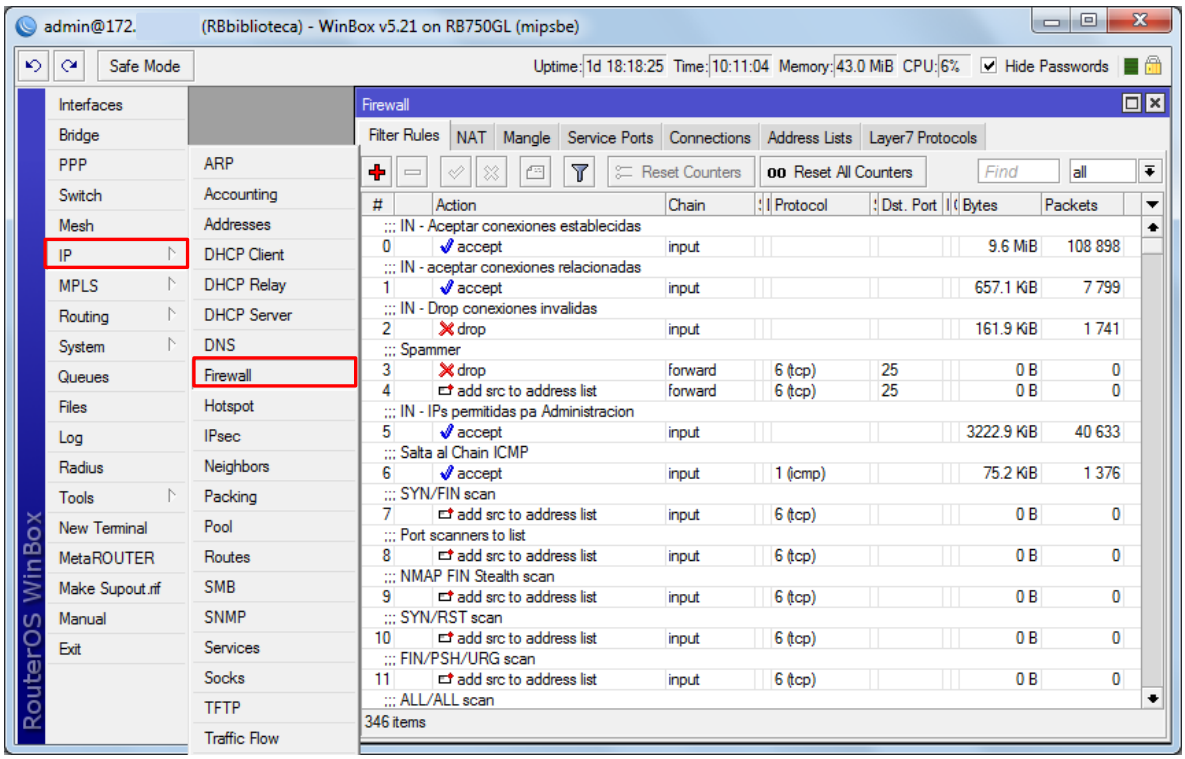


Figura 105. Ventana Firewall

f.4.3.1 Pestaña Address List

Las direcciones IP sirven para los propósitos de una identificación general de acogida en las redes IP. Las listas contienen direcciones IP para las que podemos tomar determinadas acciones.

Es posible añadir varias direcciones IP de acceso a una sola interfaz. En caso de tener en modo bridge las interfaces del equipo, la dirección IP del dispositivo se puede asignar a cualquier interfaz. Se utiliza ip/address *list* para crear listas de direcciones con un fin específico; ya sean estas de administración, para llamar un a conjunto de IPs desde una regla de configuración; aquí también se mostrará de manera automática, una lista negra de IPs que intenten un ataque al equipo con escaneo de puertos (esto siempre y cuando se

tenga configurada la regla en el Filter Rules como veremos más adelante). Para crear las listas se procede de la siguiente manera:

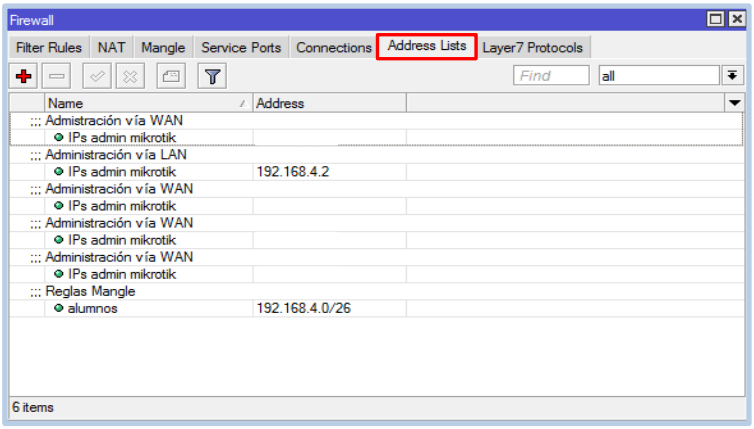


Figura 106. Pestaña Address List

En la figura 106, se observa dos tipos de listas: IPs admin mikrotik (Administración WAN) que contiene las direcciones IP permitidas para acceder al equipo ya sea SSH, Winbox o vía Web (configuraciones que se mostrarán más adelante), IPs admin mikrotik (Administración LAN) tiene una sola dirección IP que será la que nos permitirá ingresar al equipo mediante Winbox, y por último la lista alumnos (Reglas Mangle) que abarca el rango IP configurado para la LAN, esta lista nos permitirá llamar a todo el grupo de direcciones en vez de ir una por una. Para la configuración de las listas se realiza lo siguiente, clic en **(+):**

Address List:

Name: Escribimos: IPs admin Mikrotik.
(Una vez ingresado el nombre de la lista se crea automáticamente para futuras aplicaciones)
Address: 172.xx.xx.xx, 192.168.4.2
(Ingresar una por una)

Comment: Administración WAN
Administración LAN
Clic Apply
Clic OK

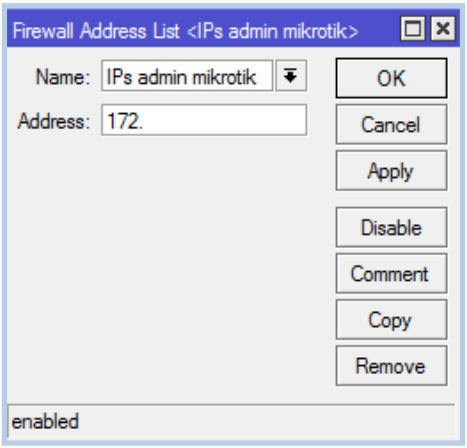


Figura 107. Configuración Address List

Para la creación de la lista alumnos:

Name: Escribir: alumnos
(Una vez ingresado el nombre de la lista se crea automáticamente para futuras aplicaciones)

Address: 192.168.4.0/26

Comment: Reglas Mangle

Clic Apply

Clic OK

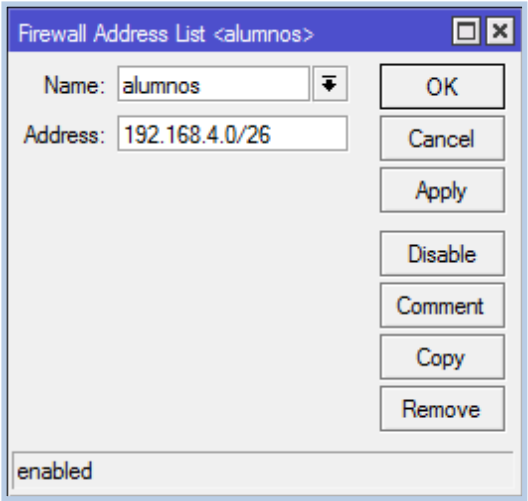


Figura 108. Configuración Address List-alumnos

f.4.3.2 Pestaña NAT-Configuración de Enmascaramiento IP

Esta característica permite mediante una dirección IP pública que tiene acceso a Internet, trasladar el acceso a Internet a varios equipos con direcciones IP privadas. Esto debido a la escasez de direcciones IPv4 los proveedores de Internet están limitados de entregar direcciones IP a todos los equipos de una red, pero mediante el uso de NAT o enmascaramiento se puede permitir que una red privada de equipos, pueda acceder a Internet a través de una única IP válida en Internet, de esta manera además se protege la red privada de ataques desde Internet.

Para habilitar el enmascaramiento clic en IP, se busca *Firewall*, dentro de la pantalla de Firewall se busca la pestaña de NAT, figura109, se da clic en el signo **(+)** y se configura el tipo de encadenamiento que se va a usar, las direcciones de red de fuente o la interface que se va a usar.

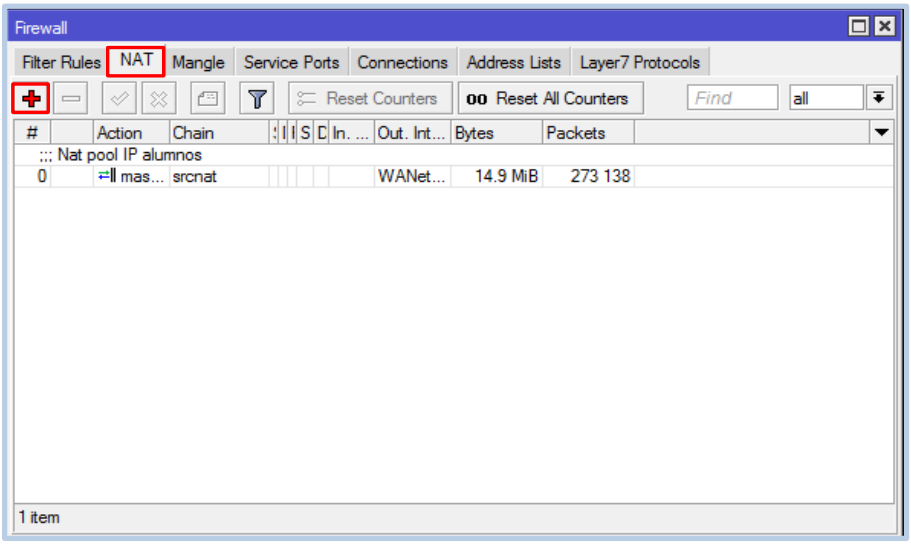


Figura 109. Pestaña NAT

Pestaña *General*:

Chain: srcnat

Out Interface: WANeth1

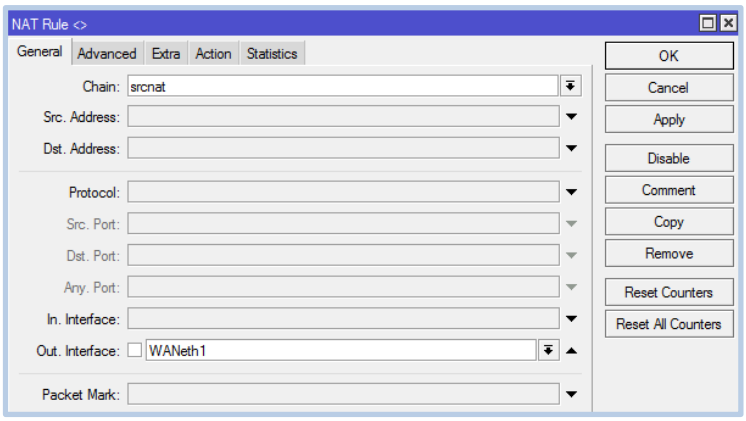


Figura 110. Configuración NAT-pestaña general

Pestaña *Advanced*:

Src Address List: alumnos

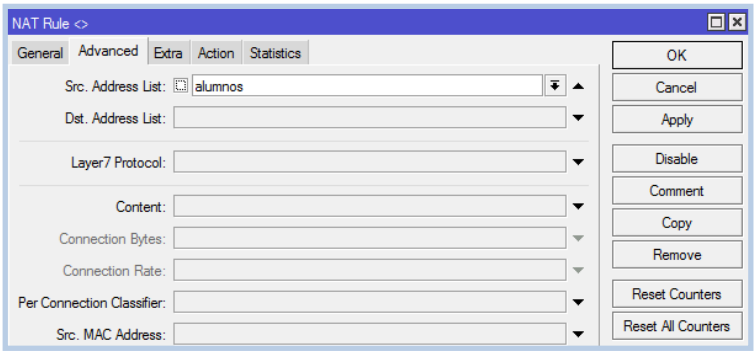


Figura 111. Configuración NAT-pestaña advanced

Pestaña *Action*:

Action: masquerade

Clic Apply

Clic OK

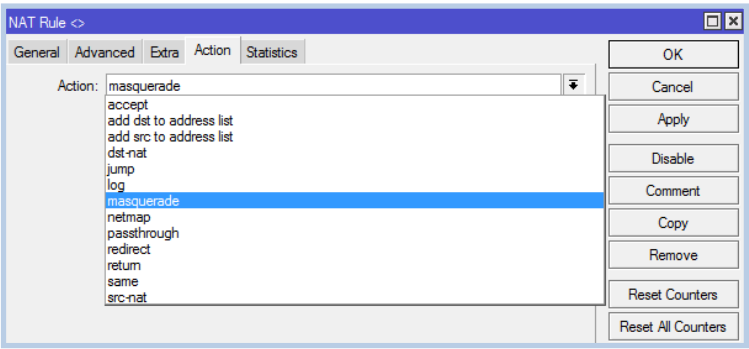


Figura 112. Configuración NAT-pestaña action: enmascaramiento

f.4.3.3 Pestaña Filter Rules

El firewall implementa paquetes de filtrado, por lo tanto proporciona funciones de seguridad que se utilizan para administrar el flujo de datos hacía, desde y a través del router. Junto con la traducción de direcciones de red que sirve como una herramienta para prevenir el acceso no autorizado a las redes directamente unidos y con el mismo router, así como un filtro para el tráfico saliente.

Los paquetes de filtrado ayudan a mantener las amenazas lejos de los datos disponibles dentro de la red. Siempre que las diferentes redes se conectan entre sí, existe la amenaza de que alguien desde fuera de nuestra red intente infringir nuestra LAN. El firewall se utiliza como un medio para prevenir o minimizar los riesgos de seguridad inherentes a la conexión a otras redes. Ya para la configuración una a una de las reglas del filtro, dentro de la pestaña *Filter Rules* clic sobre **(+)** para ir agregándolas. Figura 113.

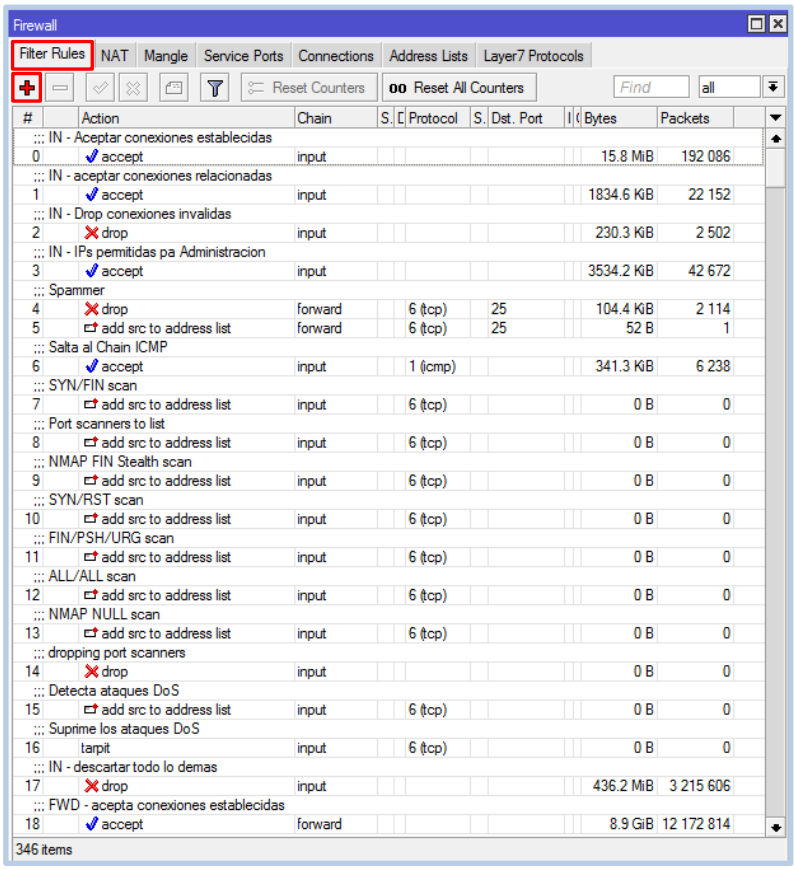


Figura 113. Pestaña filter rules

Para esta parte se consultó un paquete de filtro ya generado por los mismos desarrolladores de Mikrotik para sus usuarios; este paquete consta de 346 reglas (tabla 37), en una breve descripción contiene lo siguiente:

Tabla 37. Reglas del Filter Rule

1	IN	Aceptar Conexiones Establecidas	
2		Aceptar Conexiones Relacionadas	
3		Drop Conexiones Inválidas	
4		IPs permitidas para Administración	Las creadas en el Address List
5		Spammer	Regla que dropea el spam
6		Salta al Chain ICMP	Controla eventos que requieran ICMP.
7		SYN/FIN scan	También denominado "*inundación TCP/SYN*") consiste en saturar el tráfico de la red (denegación de servicio) para aprovechar el mecanismo de negociación de tres vías del protocolo TCP.

8		Port scanners to list	Pone en cuarentena IPs que están intentando atacar al equipo, mediante el escaneo de puertos.
9		NMAP FIN Stealth scan	Para el rastreo de puertos no permitido.
10		SYN/RST scan	Rastrea cualquier ataque de escaneo de puertos, más un bit RST.
11		FIN/PSH/URG scan	Tipo de combinación de banderas utilizadas por TCP/IP para la comunicación y control de datos, muy utilizado para el escaneo de puertos.
12		ALL/ALL scan	Se trata de un escaneo de puertos en busca de ordenadores en Internet que tienen los puertos abiertos que pueden ser atacados
13		NMAP NULL scan	
14		Dropping port scanners	Dropea todos los ataques descritos anteriormente que se puedan realizar mediante port scanners. Esta regla agrega una lista negra de las IPs que intentan hacer el scan de puertos. IP/Firewall/Addres List.
15		Detecta Ataques DoS	Detecta y bloquea ataques DoS.
16,17		Suprime Ataques DoS	
18	IN	Descarta todo lo demás	
19	FWD	Acepta conexiones establecidas	Refuerzo para el Chain IN para conexiones establecidas, relacionadas e inválidas.
20		Acepta conexiones relacionadas	
21		Descarta paquetes inválidos	
22,23,24		Saltar a virus	
25		Descartar todo lo demás	
26	ICMP	0:0 and limit for 5pac/s	Para detectar y bloquear ataques de ping flood.
27		3:3 and limit for 5pac/s	
28		3:4 and limit for 5pac/s	
29		8:0 and limit for 5pac/s	
30		11:0 and limit for 5pac/s	
31		Drop everything else	
DROP A LISTA DE VIRUS			
32-346	DROP		Bloquea puertos conocidos de virus.
Elaborado por: **Évelin Alvarado Otero**			

Para trasladar el archivo con las reglas hacia el equipo Mikrotik se hace lo siguiente, antes de nada, las reglas que serán copiadas en el equipo vienen en texto .txt, por lo tanto lo que se hace es copiar las reglas, luego de esto, en el equipo nos dirigimos hacia al menú

principal, clic sobre *New Terminal*, se abre la ventana de Terminal, figura 114, escribimos la dirección de donde queremos que se genere la información: ip firewall, damos enter y luego en la parte en blanco seguido de la dirección, clic derecho paste.

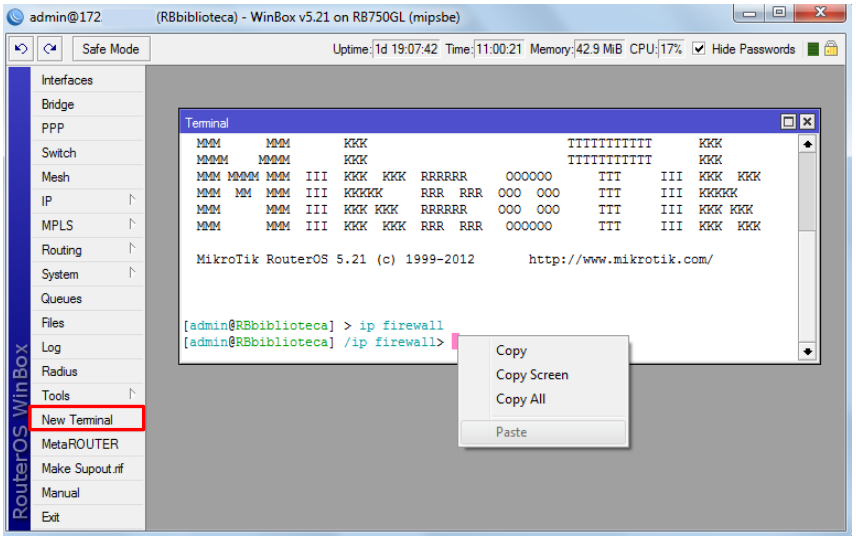
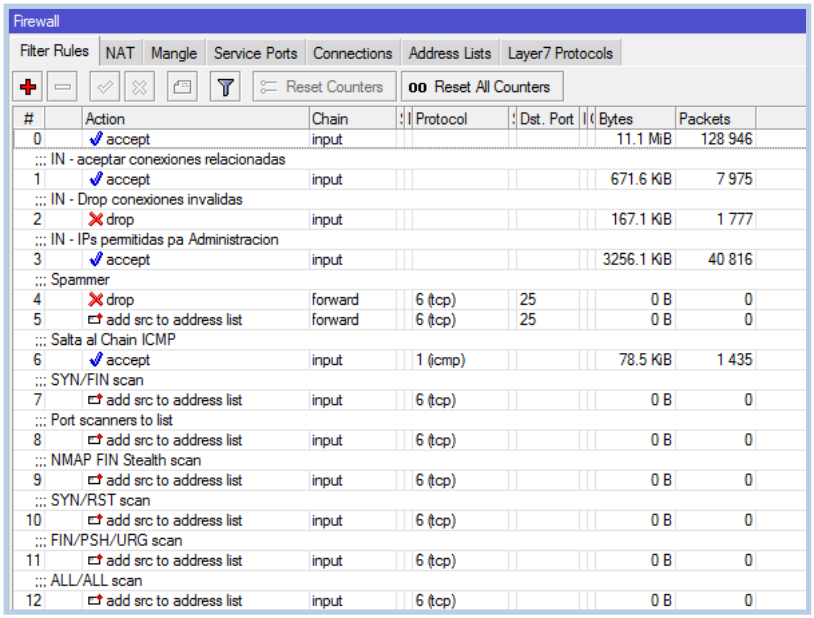


Figura 114. Proceso de copiado de reglas en el new terminal

Luego nos dirigimos hacia el filter rules y aparecerán ya las reglas configuradas, no está demás revisar que las reglas se hayan pegado en su totalidad, figura 115, es muy importante realizar las pruebas o ir verificando cómo éstas se cumplen.



Firewall

Filter Rules | NAT | Mangle | Service Ports | Connections | Address Lists | Layer7 Protocols

Reset Counters | Reset All Counters

#	Action	Chain	Protocol	Dst. Port	Bytes	Packets
0	accept	input			11.1 MiB	128 946
;;; IN - aceptar conexiones relacionadas						
1	accept	input			671.6 KiB	7 975
;;; IN - Drop conexiones invalidas						
2	drop	input			167.1 KiB	1 777
;;; IN - IPs permitidas pa Administracion						
3	accept	input			3256.1 KiB	40 816
;;; Spammer						
4	drop	forward	6 (tcp)	25	0 B	0
5	add src to address list	forward	6 (tcp)	25	0 B	0
;;; Salta al Chain ICMP						
6	accept	input	1 (icmp)		78.5 KiB	1 435
;;; SYN/FIN scan						
7	add src to address list	input	6 (tcp)		0 B	0
;;; Port scanners to list						
8	add src to address list	input	6 (tcp)		0 B	0
;;; NMAP FIN Stealth scan						
9	add src to address list	input	6 (tcp)		0 B	0
;;; SYN/RST scan						
10	add src to address list	input	6 (tcp)		0 B	0
;;; FIN/PSH/URG scan						
11	add src to address list	input	6 (tcp)		0 B	0
;;; ALL/ALL scan						
12	add src to address list	input	6 (tcp)		0 B	0

Figura 115. Paquete de reglas del filtro Mikrotik

f.4.3.4 Pestaña Layer 7 Protocols

El marcado de paquetes puede ser ya sea por: direcciones IP, rango de direcciones IP, por puerto, rango de puerto, protocolo IP, DSCP y otros parámetros, tal es el caso de características de capa 7 *(Layer7).*

Layer7 o L7 es la capa Aplicación del modelo OSI, permite al router Mikrotik analizar cada uno de los paquetes que ingresan a la red y decidir qué hacer con ellos; L7 es utilizado para categorizar paquetes IP con el fin de identificar de forma más efectiva a los programas peer to peer (P2P). De la guía de script para Layer7 disponibles en http://l7-filter.sourceforge.net/protocols se tomó en cuenta para controlar en el equipo los siguientes servicios: audio, facebook, msn, Skype y video.

Para configurar Layer7, de la pestaña Layer7 Protocols clic sobre **(+)**, figura 116**:**

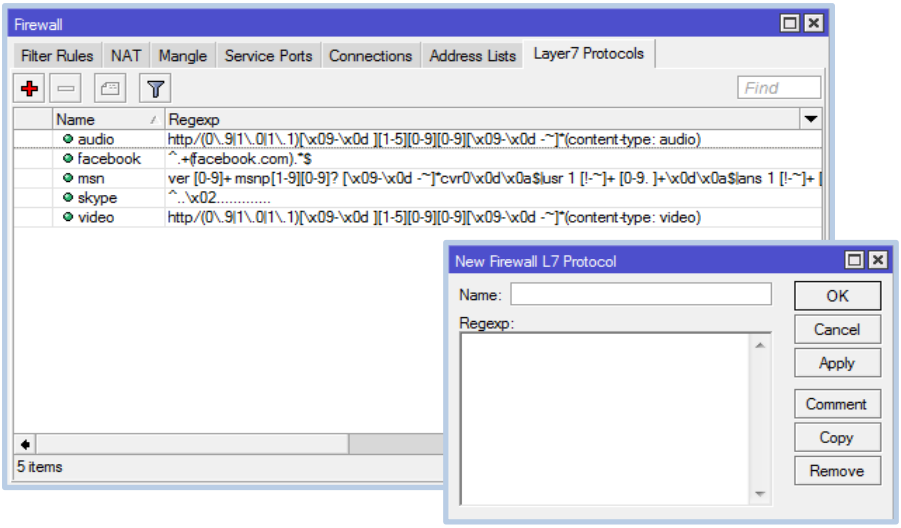


Figura 116. Pestaña Layer7

Pestaña *Layer7*:

Name: audio, facebook, msn, Skype, video.

Regexp: En el espacio en blanco se pega el script que controlará uno por uno a los servicios.

Clic Apply

Clic OK

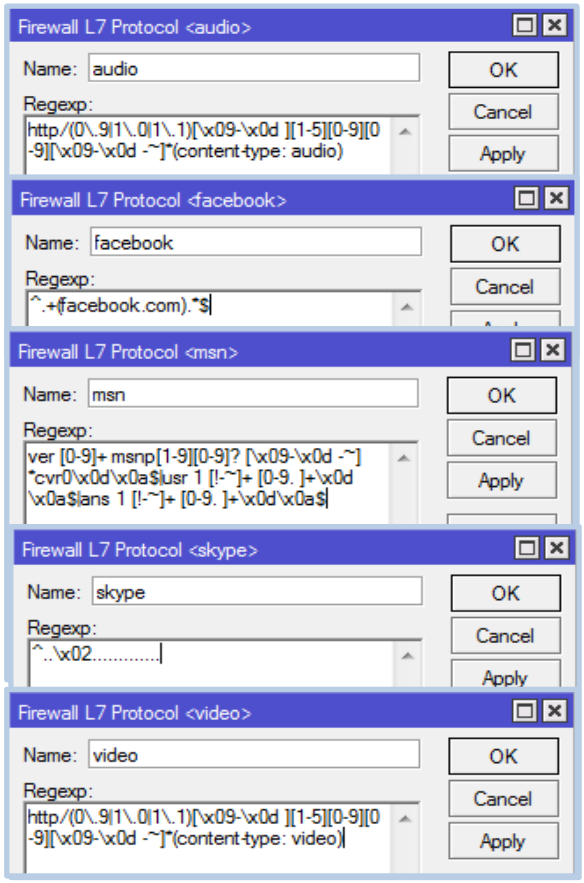


Figura 117. Configuración de servicios por Layer7

De esta manera quedan establecidos cuáles serán los servicios que en Mangle serán marcados por Layer7.

f.4.3.5 Pestaña Mangle

Mangle es una especie de "marcador" que marca los paquetes para su posterior procesamiento con características especiales. Muchas otras configuraciones en el equipo hacen uso de estas marcas, por ejemplo: *Queue Trees*, *NAT*, *Routing*, *Simple Queue*. Las reglas que aquí se configuran identifican un paquete basándose en su marca para procesarla adecuadamente. El marcado en mangle es sólo dentro del router, no se transmiten a través de la red. Como técnica de clasificación de tráfico, importante en la segmentación, se realiza el ruteo basado en reglas.

CADENAS

Además, la configuración de reglas mangle se utiliza para modificar algunos campos de la cabecera IP, como TOS (DSCP) y campos TTL. La administración se podrá hacer en las cadenas: prerouting, postrouting.

<<En el caso de PREROUTING podremos modificar los datos destino de la conexión según nos interese y antes de tomar la decisión de enrutamiento>>[8]. Sólo tiene sentido en el interfaz de entrada, controla bajada de paquetes.

<<Cuando utilizamos la cadena POSTROUTING podremos modificar los paquetes justo antes de devolverlos a la red. Podremos modificar los datos de origen, porque el destino ya se ha decidido en una de las cadenas previas FOWRARD u OUTPUT>>[8]. Controla subida de paquetes.

El mejor marcado es el de prerouting, porque lo que se puede controlar mejor tanto para la conexión y los paquetes.

MARCAS DE PAQUETES

Mark Connection: Permite monitorear IPs de los usuarios que se encuentran navegando, especialmente funciona para agregar modificadores especiales por conexión, *mark connection* es la antesala para luego marcar dichas conexiones con el *Mark Packet* en queue tree. En la pestaña *IP/Firewall/Connections* visualiza todo el *Mark Connections* configurado.

Mark Packet: permite trabajar con las conexiones marcadas en el Queue Tree para determinar la asignación de anchos de banda.

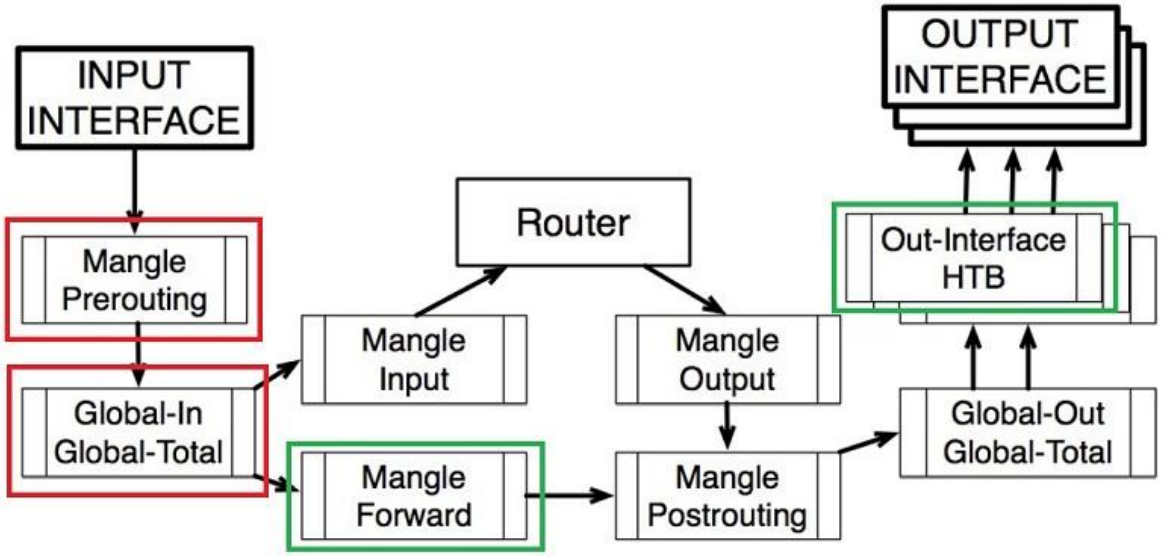


Figura 118. Lógica para el marcado de paquetes [18]

Mikrotik RouterOS. *"Workshop QoS Best Practice"*. Dallas/Fort worth MUM USA 2009. Disponible en: <http://mum.mikrotik.com/presentations/US09/megis_qos.pdf>. [En línea].

En la pestaña Mangle sin duda se encuentra la parte central de la configuración del equipo Mikrotik, es la base de segmentación del ancho de banda, de una buena configuración de este apartado dependerá el éxito de la segmentación. Para empezar con una configuración, damos clic sobre **(+)** para ir agregando una por una las reglas.

En la figura 119, se muestra las reglas que se tiene configuradas, para no hacer extensa la parte de configuración, las reglas están divididas de tres formas, las configuradas por: contenido, L7 y por puerto.

Firewall

Filter Rules | NAT | Mangle | Service Ports | Connections | Address Lists | Layer7 Protocols

00 Reset Counters | 00 Reset All Counters | Find | all

#	Action	Chain	Protocol	Src. Port	Dst. Port	In...	Out...	Connection Mark	Bytes	Packets
mark connection										
;;; youtube										
4	mark connection	prerouting							35.4 MiB	44 279
;;; messenger										
10	mark connection	prerouting							0 B	0
;;; badoo										
14	mark connection	prerouting							4222.1 KiB	4 906
;;; twitter										
16	mark connection	prerouting							6.2 MiB	11 216
;;; facebook										
18	mark connection	prerouting							182.4 MiB	331 257
;;; marcado general trafico lan										
20	mark connection	prerouting							798.0 MiB	7 082 749
;;; http_audio										
8	mark connection	prerouting							24.7 MiB	28 100
;;; http_video										
6	mark connection	prerouting							420.0 MiB	518 237
;;; Skype										
12	mark connection	prerouting							49.5 MiB	126 490
;;; redtube										
2	mark connection	prerouting							0 B	0
mark packet										
5	mark packet	prerouting						conn_youtube	3489.4 MiB	4 166 147
7	mark packet	prerouting						conn_video	420.0 MiB	518 237
9	mark packet	prerouting						conn_audio	24.7 MiB	28 100
11	mark packet	prerouting						conn_messenger	0 B	0
15	mark packet	prerouting						conn_badoo_in	18.7 MiB	29 853
17	mark packet	prerouting						conn_twitter_in	74.4 MiB	120 766
19	mark packet	prerouting						conn_facebook_in	182.5 MiB	331 346
31	mark packet	prerouting						conn_alumnos	30.5 KiB	256
33	mark packet	prerouting						conn_alumnos	1685.3 MiB	7 935 977
1	mark packet	postrouting	6 (tcp)		8291				0 B	0
13	mark packet	prerouting						conn_skype	49.5 MiB	126 524
3	mark packet	prerouting						conn_redtube	0 B	0
22	mark packet	postrouting	6 (tcp)		80,443			conn_alumnos	413.8 MiB	3 080 744
24	mark packet	postrouting	6 (tcp)		80,443			conn_alumnos	34.6 MiB	357 698
26	mark packet	postrouting	6 (tcp)		80,443			conn_alumnos	199.8 MiB	2 553 143
28	mark packet	postrouting	6 (tcp)		25,110,143,465,993,995			conn_alumnos	11.0 KiB	169
30	mark packet	postrouting	6 (tcp)		20,21,22			conn_alumnos	1215 B	19
32	mark packet	postrouting						conn_alumnos	0 B	0
29	mark packet	prerouting	6 (tcp)	20,21,22				conn_alumnos	1117 B	19
27	mark packet	prerouting	6 (tcp)	25,110,143,465,993,995				conn_alumnos	11.8 KiB	122
21	mark packet	prerouting	6 (tcp)	80,443				conn_alumnos	3556.3 MiB	3 876 807
23	mark packet	prerouting	6 (tcp)	80,443				conn_alumnos	685.6 MiB	538 346
25	mark packet	prerouting	6 (tcp)	80,443				conn_alumnos	5.6 GiB	4 322 061
;;; winbox										
0	mark packet	prerouting	6 (tcp)	8291					0 B	0

34 items (1 selected)

Figura 119. Pestaña Mangle

<u>Configuración por contenido:</u> están configuradas por contenido las páginas de youtube, badoo, twitter, redtube; a continuación se muestra una sola configuración ya que para todas son la misma, como ejemplo tomaremos youtube. Para esto en la pestaña de Mangle clic en (**+**), aparecerá una venta de New Mangle Rule con cinco pestañas, se configura las pestañas necesarias.

Pestaña *General*:

Chain: prerouting

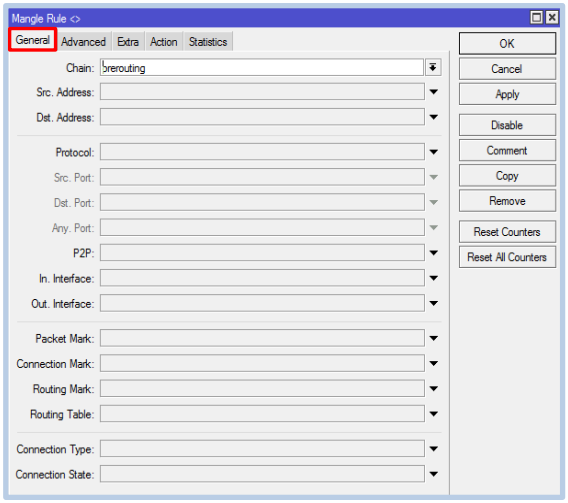


Figura 120. Mangle Configuración/pestaña general

Pestaña *Advanced*:

Content: youtube

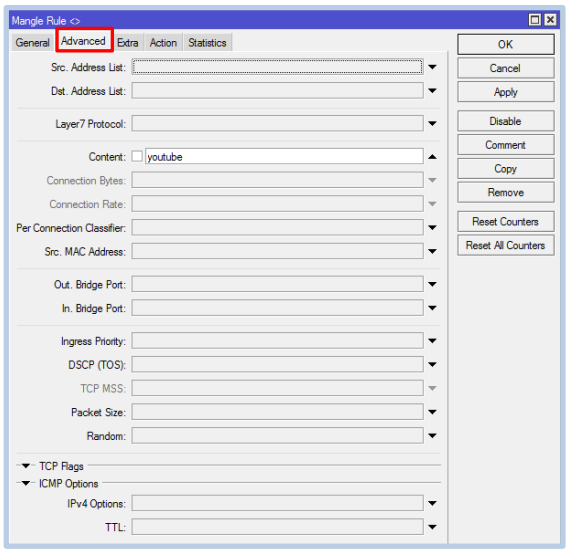


Figura 121. Mangle Configuración/pestaña advanced

Pestaña *Action*:

Action: mark connection

New Connection Mark: escribimos conn_youtube

- ✓ **Passthrough** (solo activo para mark connection)

Comment: youtube
Clic Apply
Clic OK

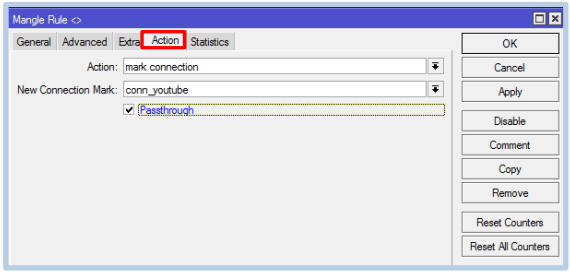


Figura 122. Mangle Configuración/pestaña action

La configuración hasta aquí, permite visualizar en *IP/Firewall/Connections*, la conexión que está siendo realizada; también es el paso para crear la regla de asignación de ancho de banda.

Click en (**+**):

Pestaña *General*:

Chain: prerouting
Connection Mark: buscamos conn_youtube

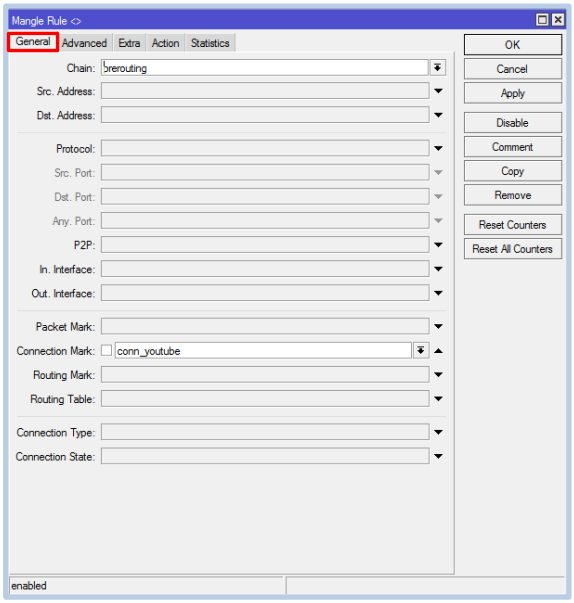


Figura 123. Mangle Configuración/pestaña general

Pestaña *Action*:

Action: mark packet

New Packet Mark: escribir pack_youtube
Clic Apply
Clic OK

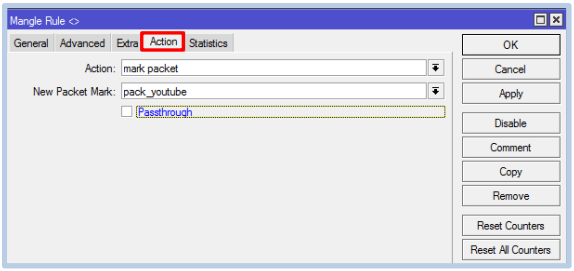


Figura 124. Mangle Configuración/pestaña action

Esta nueva regla de creación del *Mark Packet*, es la que da paso para realizar la asignación de ancho de banda de lo que estemos segmentando, al momento de configurar en el Queue Tree.

Configuración por L7: están configuradas por layer 7 los servicios de Skype, Messenger, la página de Facebook y las páginas de audio y video; a continuación se muestra una sola

configuración ya que para todas son la misma, como ejemplo tomaremos facebook. Para esto en la pestaña de Mangle clic en (+), aparecerá una venta de *New Mangle Rule*.

Pestaña *General*:

Chain: prerouting

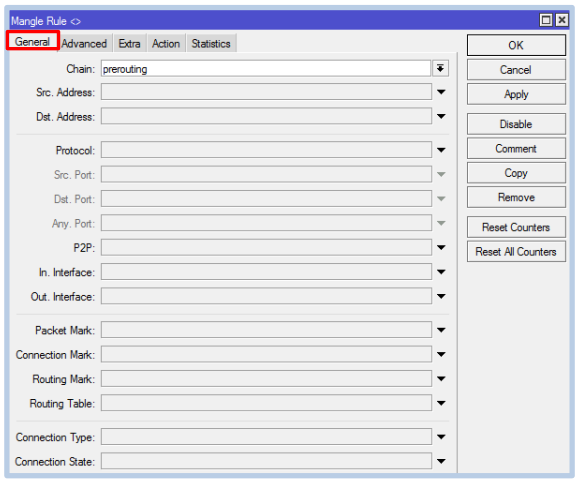


Figura 125. Mangle Configuración/pestaña general

Pestaña *Advanced*:

Layer7 Protocol: Buscar facebook, que ya configuramos previamente en la pestaña del Firewall/Layer7 Protocol.

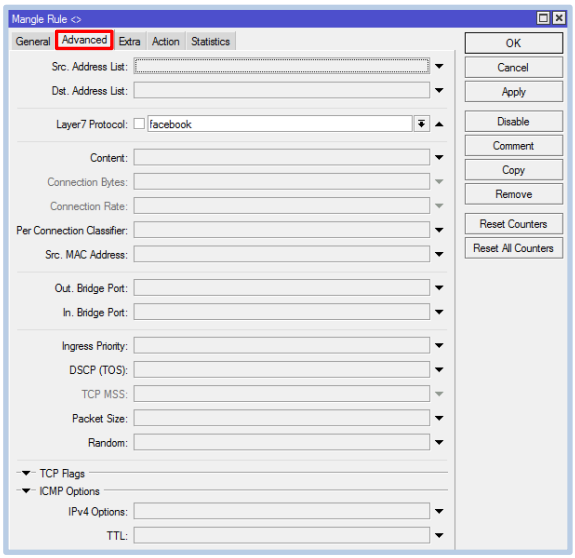


Figura 126. Mangle Configuración/pestaña advanced

Pestaña *Action*:

Action: mark connection

New Connection Mark: escribir conn_facebook_in

✓ **Passthrough** (solo activo para mark connection)

Comment: facebook

Clic Apply

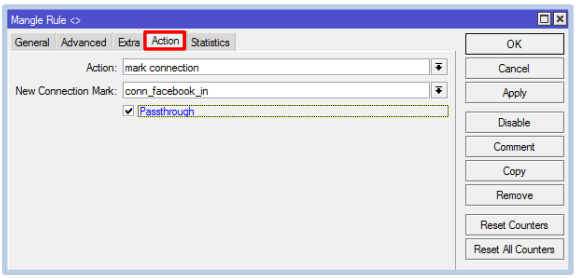


Figura 127. Mangle Configuración/pestaña action

Click en (+):

Pestaña *General*:

Chain: prerouting
Connection Mark: conn_facebook_in

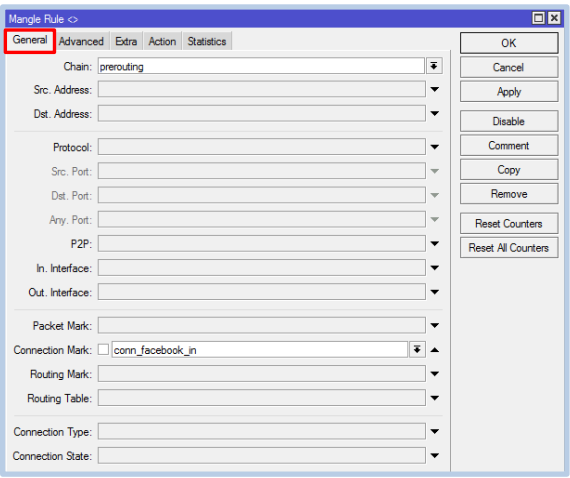


Figura 128. Mangle Configuración/pestaña general

Pestaña *Action*:

Action: mark packet

New Packet Mark: escribir pack_youtube
Clic Apply
Clic OK

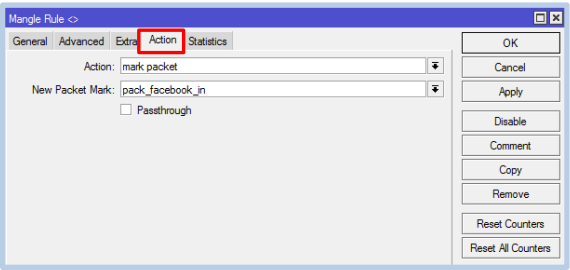


Figura 129. Mangle Configuración/pestaña action

Configuración por puerto: están configuradas por puerto los siguientes protocolos: http puerto 80, https puerto 443, ftp (datos) puerto 20, ftp (control) puerto 21, ssh/sftp puerto 22, smtp puerto 25, pop3 puerto 110, imap4 puerto 143, smtp/ssl puerto 465, imap4/ssl puerto 993, pop3/ssl puerto 995 y wimbox puerto 8291; a continuación se muestra una sola configuración ya que para todas son la misma, como ejemplo tomaremos http y https. Para esto en la pestaña de Mangle clic en (+), aparecerá una venta de *New Mangle Rule.*

Antes de comenzar con la configuración de las reglas por puertos, se configura un solo *mark connection* para todas las reglas de configuración por puerto. Esta regla obedece a la lista alumnos, y se crea una sola para no tener redundancia.

Pestaña *General*:

Chain: prerouting

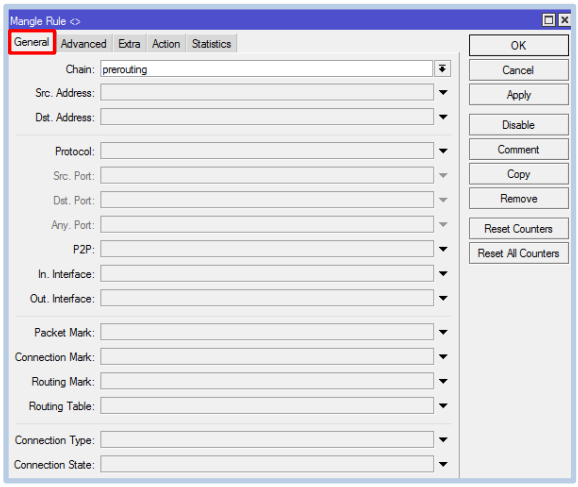


Figura 130. Mangle Configuración/pestaña general

Pestaña *Advanced*:

Src. Address List: Buscar alumnos, que ya configuramos previamente en la pestaña del Firewall/Address Lists.

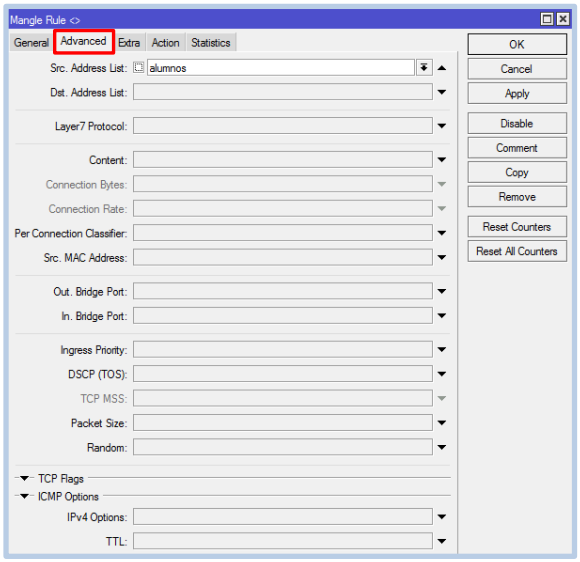


Figura 131. Mangle Configuración/pestaña advanced

Pestaña *Action*:

Action: mark connection

New Connection Mark: escribir conn_alumnos

✓ **Passthrough** (solo activo para mark connection)

Comment: marcado general tráfico lan

Clic Apply

Clic OK

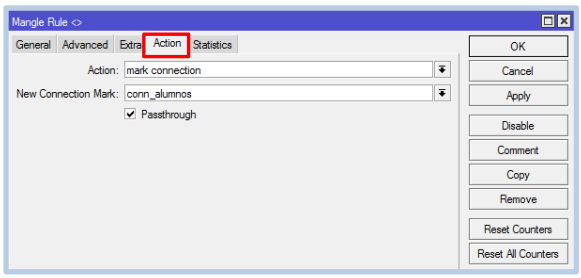


Figura 132. Mangle Configuración/pestaña action

La configuración por puerto tiene un trato especial, ya que es en estas reglas donde se hace diferencia entre páginas livianas, medianas y pesadas. Cabe mencionar que la configuración de la opción *Connection Bytes* es sólo para puerto 80 y 443, el resto de reglas tienen la misma configuración a excepción de esta.

Pestaña *General*:

Chain: prerouting
Protocol: 6 (tcp)
Src. Port: 80, 443
Connection Mark: escribimos conn_alumnos

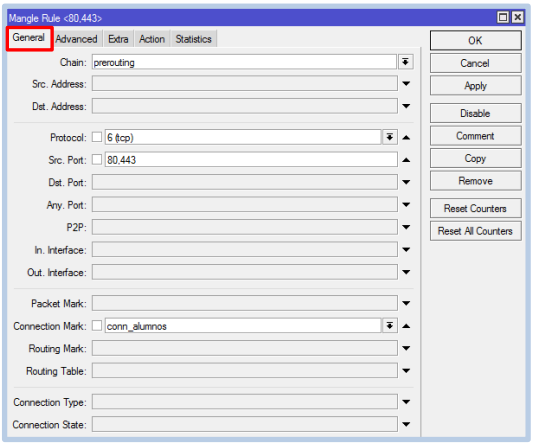


Figura 133. Mangle Configuración/pestaña general

Pestaña *Advanced*:

Connection Byte: 0-256000,
256000-512000,
512000-0
(se ingresa uno por uno).

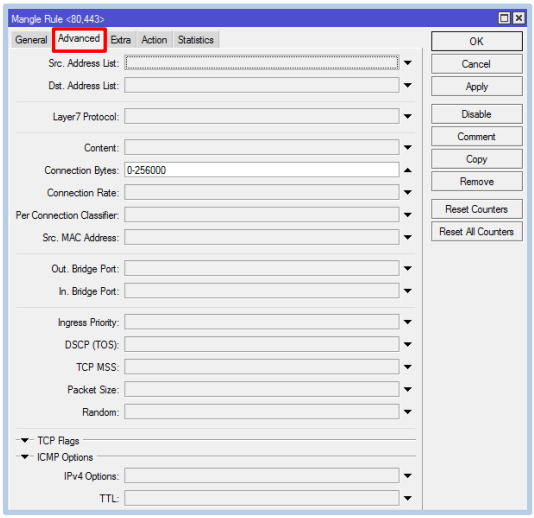


Figura 134. Mangle Configuración/pestaña advanced

Pestaña *Action*:

Action: mark packet

New Packet Mark: escribir pack_alumnos_smallin
Clic Apply
Clic OK

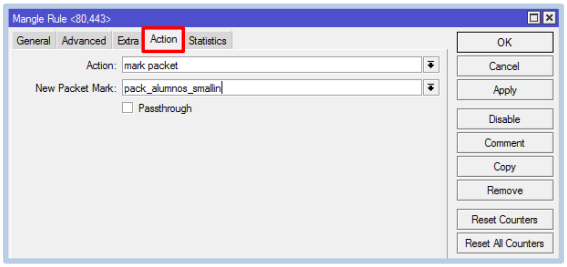


Figura 135. Mangle Configuración/pestaña action

Click en (**+**):

Chain: postrouting
Protocol: 6 (tcp)
Dst. Port: 80, 443
Connection Mark: escribimos conn_alumnos

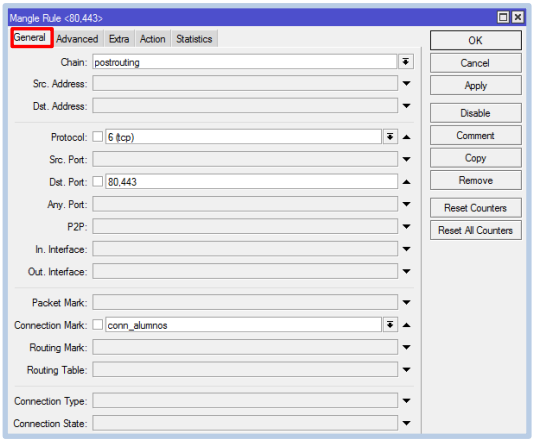


Figura 136. Mangle Configuración/pestaña general

Pestaña *Advanced*:

Connection Byte: 0-256000,
256000-512000,
512000-0
(Ingresamos uno por uno).

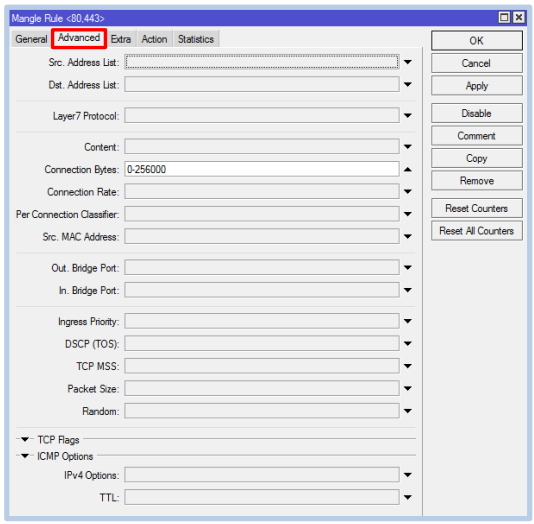


Figura 137. Mangle Configuración/pestaña advanced

Pestaña *Action*:

Action: mark packet

New Packet Mark: escribimos pack_alumnos_smallout
Clic Apply
Clic OK

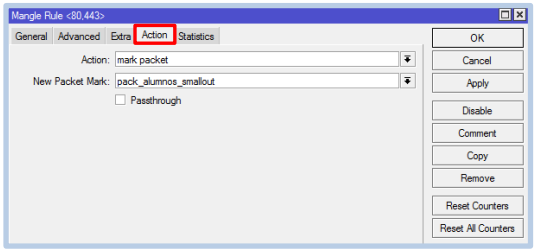


Figura 138. Mangle Configuración/pestaña action

Una configuración importante, es la configuración de una regla que llamaremos resto, para el caso de controlar el tráfico que no se esté marcando.

Pestaña *General*:

Chain: prerouting
Connection Mark: escribimos conn_alumnos

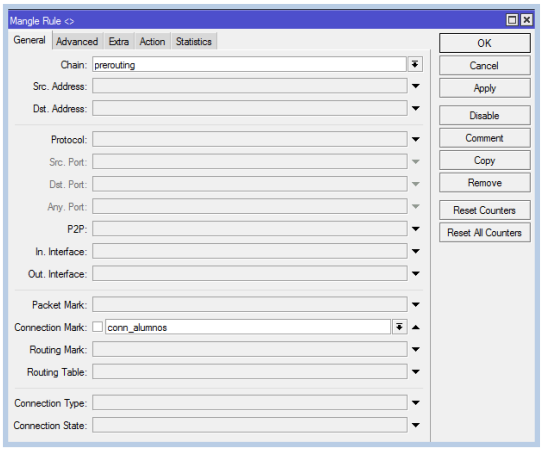


Figura 139. Mangle Configuración/pestaña general

Pestaña *Action*:

Action: mark packet
New Packet Mark: escribir pack_alumnos_restoin
Clic Apply
Clic OK

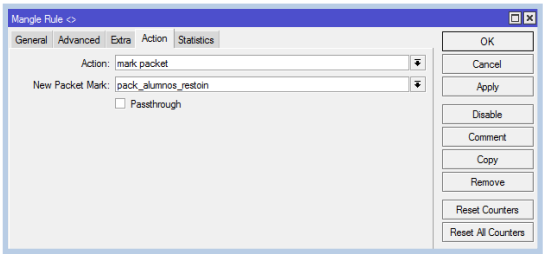


Figura 140. Mangle Configuración/pestaña action

Una regla que también necesita especial configuración es para aplicaciones p2p, para esto, tabla 38:

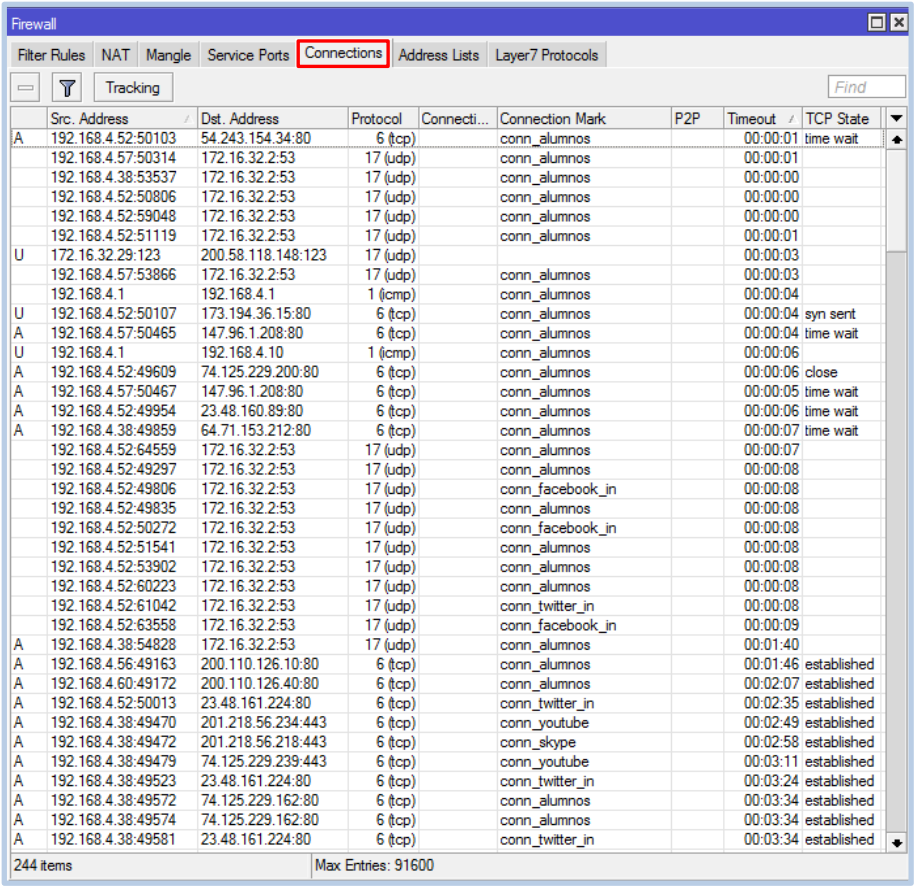
Tabla 38. P2P All

Pestaña *General*	**Chain:** prerouting
	P2P: Seleccionar all-p2p
	Connection Mark: Seleccionar con_alumnos
Pestaña *Action*	**Action:** Seleccionar mark packet
	New Packet Mark: escribir pack_alumnos_p2p
Clic Apply **Clic Ok**	
Elaborado por: **Évelin Alvarado Otero**	

f.4.3.6 Pestaña Connections

Para terminar con la configuración del submenú Firewall hablaremos acerca de la pestaña Connections. En las reglas de Mangle se configuró la opción **Action/ New**

Connection Mark, esto con el fin de poder ver qué conexiones están haciendo su camino a través del router, se puede visualizar las conexiones actuales a / desde / a través del router. Clic sobre Connections y aparecerá lo siguiente:



	Src. Address	Dst. Address	Protocol	Connecti...	Connection Mark	P2P	Timeout	TCP State
A	192.168.4.52:50103	54.243.154.34:80	6 (tcp)		conn_alumnos		00:00:01	time wait
	192.168.4.57:50314	172.16.32.2:53	17 (udp)		conn_alumnos		00:00:01	
	192.168.4.38:53537	172.16.32.2:53	17 (udp)		conn_alumnos		00:00:00	
	192.168.4.52:50806	172.16.32.2:53	17 (udp)		conn_alumnos		00:00:00	
	192.168.4.52:59048	172.16.32.2:53	17 (udp)		conn_alumnos		00:00:00	
	192.168.4.52:51119	172.16.32.2:53	17 (udp)		conn_alumnos		00:00:01	
U	172.16.32.29:123	200.58.118.148:123	17 (udp)				00:00:03	
	192.168.4.57:53866	172.16.32.2:53	17 (udp)		conn_alumnos		00:00:03	
	192.168.4.1	192.168.4.1	1 (icmp)		conn_alumnos		00:00:04	
U	192.168.4.52:50107	173.194.36.15:80	6 (tcp)		conn_alumnos		00:00:04	syn sent
A	192.168.4.57:50465	147.96.1.208:80	6 (tcp)		conn_alumnos		00:00:04	time wait
U	192.168.4.1	192.168.4.10	1 (icmp)		conn_alumnos		00:00:06	
A	192.168.4.52:49609	74.125.229.200:80	6 (tcp)		conn_alumnos		00:00:06	close
A	192.168.4.57:50467	147.96.1.208:80	6 (tcp)		conn_alumnos		00:00:05	time wait
A	192.168.4.52:49954	23.48.160.89:80	6 (tcp)		conn_alumnos		00:00:06	time wait
A	192.168.4.38:49859	64.71.153.212:80	6 (tcp)		conn_alumnos		00:00:07	time wait
	192.168.4.52:64559	172.16.32.2:53	17 (udp)		conn_alumnos		00:00:07	
	192.168.4.52:49297	172.16.32.2:53	17 (udp)		conn_alumnos		00:00:08	
	192.168.4.52:49806	172.16.32.2:53	17 (udp)		conn_facebook_in		00:00:08	
	192.168.4.52:49835	172.16.32.2:53	17 (udp)		conn_alumnos		00:00:08	
	192.168.4.52:50272	172.16.32.2:53	17 (udp)		conn_facebook_in		00:00:08	
	192.168.4.52:51541	172.16.32.2:53	17 (udp)		conn_alumnos		00:00:08	
	192.168.4.52:53902	172.16.32.2:53	17 (udp)		conn_alumnos		00:00:08	
	192.168.4.52:60223	172.16.32.2:53	17 (udp)		conn_alumnos		00:00:08	
	192.168.4.52:61042	172.16.32.2:53	17 (udp)		conn_twitter_in		00:00:08	
	192.168.4.52:63558	172.16.32.2:53	17 (udp)		conn_facebook_in		00:00:09	
A	192.168.4.38:54828	172.16.32.2:53	17 (udp)		conn_alumnos		00:01:40	
A	192.168.4.56:49163	200.110.126.10:80	6 (tcp)		conn_alumnos		00:01:46	established
A	192.168.4.60:49172	200.110.126.40:80	6 (tcp)		conn_alumnos		00:02:07	established
A	192.168.4.52:50013	23.48.161.224:80	6 (tcp)		conn_twitter_in		00:02:35	established
A	192.168.4.38:49470	201.218.56.234:443	6 (tcp)		conn_youtube		00:02:49	established
A	192.168.4.38:49472	201.218.56.218:443	6 (tcp)		conn_skype		00:02:58	established
A	192.168.4.38:49479	74.125.229.239:443	6 (tcp)		conn_youtube		00:03:11	established
A	192.168.4.38:49523	23.48.161.224:80	6 (tcp)		conn_twitter_in		00:03:24	established
A	192.168.4.38:49572	74.125.229.162:80	6 (tcp)		conn_alumnos		00:03:34	established
A	192.168.4.38:49574	74.125.229.162:80	6 (tcp)		conn_alumnos		00:03:34	established
A	192.168.4.38:49581	23.48.161.224:80	6 (tcp)		conn_twitter_in		00:03:34	established

Figura 141. Pestaña Connections

En la figura 141, se observa en primera instancia la *Src Address* que representa la dirección origen desde la que se realiza la petición; seguido se observa la *Dst. Address* que representa la dirección destino de la petición; luego observamos *Protocol* que significa el protocolo utilizado por la página o servicio; seguido a esto se encuentra *Connection Mark* que son las conexiones marcadas desde las reglas de mangle como fueron: youtube, facebook, Skype, alumnos para tráfico general LAN, etc. Seguidamente se observa el *timeout* que muestra los tiempos en el que la conexión se eliminará de la lista de conexiones (valores por *default*). Por último se observa *TCP State* que representa el estado actual de la conexión TCP, pueden ser: "*established*", "*time-wait*", "*close*", "*time-close*", "*syn-sent*".

f.4.4 Calidad de servicio (QOS)/QUEUES

QoS no solamente limita ancho de banda, también es un intento de utilizar recursos existentes de una manera eficiente (no utilizando todo el ancho de banda disponible), es balancear y priorizar el flujo de datos.

El QoS de mikrotik basa su funcionamiento de calidad y servicio en mecanismos de disciplinas queueing, <<estas controlan el orden y la velocidad de los paquetes de salida y de entrada en la interfaz; también delimita que paquetes deben esperar por su turno para ser enviados fuera de la interfaz y quienes deben ser descargados, siempre trabaja sobre la interfaz de salida. Solamente puede haber una disciplina de *queue* por cada interface>>[28].

f.4.4.1 Tipos de Disciplinas de Queues

Las disciplinas pueden ser clasificadas dentro de 2 grupos por su influencia en el flujo de datos: schedulers y shapers.

- Tipo Scheduler: <<reordena el flujo de paquetes. Este tipo de disciplinas limitan el número de paquetes esperando, no la velocidad>>. [28]
  - FIFO
  - RED
  - SFQ
- Tipo Shaper: <<controlan la velocidad del flujo de datos. Adicionalmente pueden hacer un trabajo programado>>. [28]
  - PCQ
  - HTB

Para la configuración del tipo de cola que se utilizará para la segmentación, se maneja PCQ (*Per Connection Queue*) del cual Mikrotik es propietario, ya que nos permitirá trabajar con el tipo de *Queue* que queremos implementar, y es el de *Queue Tree*. Es posible limitar la máxima velocidad dada para los paquetes enviados.

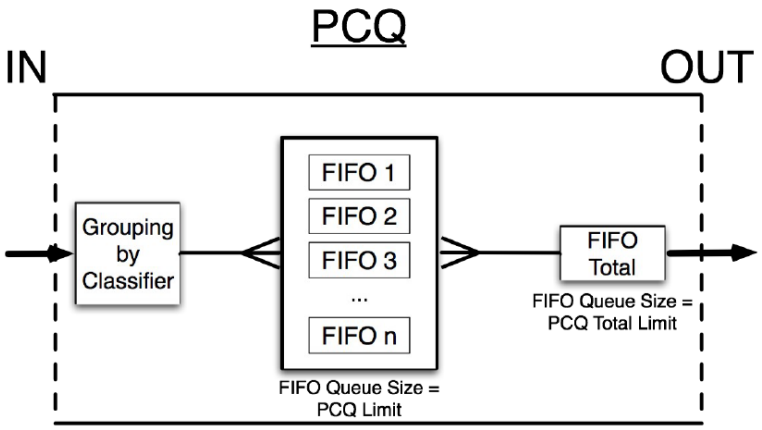


Figura 142. Arquitectura interna PCQ [18]

Mikrotik RouterOS. *"Workshop QoS Best Practice"*. Dallas/Fort worth MUM USA 2009. Disponible en: <http://mum.mikrotik.com/presentations/US09/megis_qos.pdf>. [En línea].

Con el fin de garantizar que cada subflujo de PCQ, figura 143, represente a cada cliente en particular, se crea 2 tipos diferentes PCQ: PCQ_upload, PCQ_download.

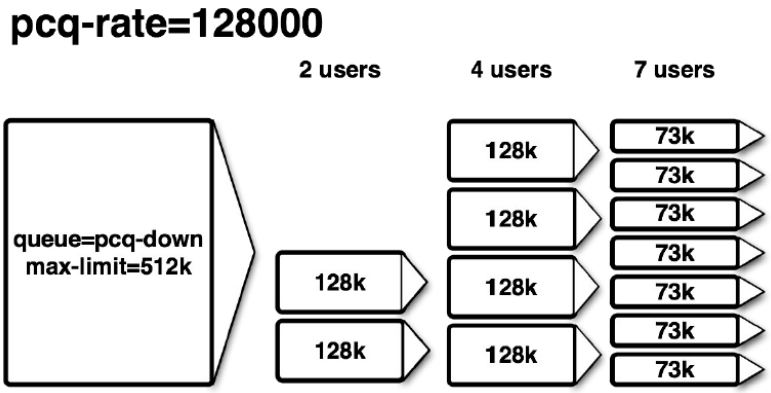


Figura 143. Ejemplo control del ancho de banda en PCQ [18]

MikroTik RouterOS. *"Workshop QoS Best Practice"*. Dallas/Fort worth MUM USA 2009. Disponible en: <http://mum.mikrotik.com/presentations/US09/megis_qos.pdf>. [En línea].

El Queue Tree es sólo unidireccional y puede ser utilizado en cualquiera de las disciplinas disponibles de Tipo *Shaper*. No tienen ningún orden, todo el tráfico se procesa simultáneamente. Los *subqueues* deben tener marcas de paquete o *mark packet* asignadas desde "IP/Firewall/Mangle". Para hacer uso de *Mangle* y *Queue Tree* se debe:

a. Marcar el tráfico por tipo de tráfico en el mangle con la cadena o chain PREROUTING.
b. Crear la variable global y luego las subvariables en el queue.
c. Limitar el tráfico por interfaz.
d. Priorizar y limitar el tráfico por tipo con Global-in.

Es necesario mantener la cantidad de reglas *Mangle* y las de *Queue* en el menor número posible, ya que tener demasiadas reglas ocasionan un desempeño lento del equipo.

f.4.4.2 Configuración del Queue

Del menú principal, clic sobre *Queues*, aparecerá una ventana llamada *Queue List*, aquí encontraremos los apartados que necesitamos configurar que son: *Queue Tree* y *Queue Type*.

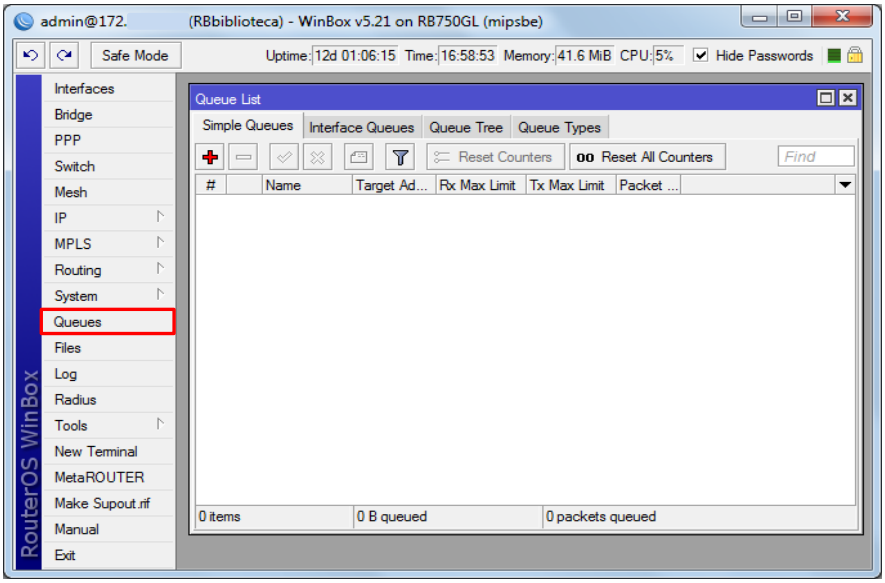


Figura 144. Configuración del Queue

Primeramente se configura el Queue Types, figura 144, clic sobre ésta pestaña y luego sobre (+).

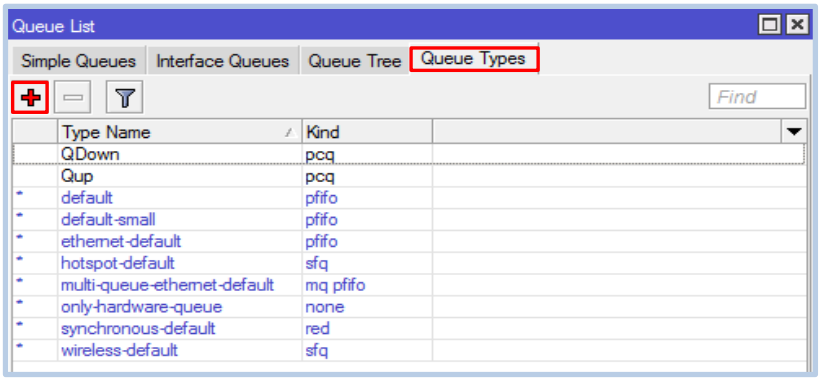


Figura 145. Pestaña Queue Type

Pestaña *Queue Types*:

Type Name: Ingresamos QDown

Kind: Seleccionar pcq
Classifier: ✓ Dst. Addess
Clic Apply
Clic OK

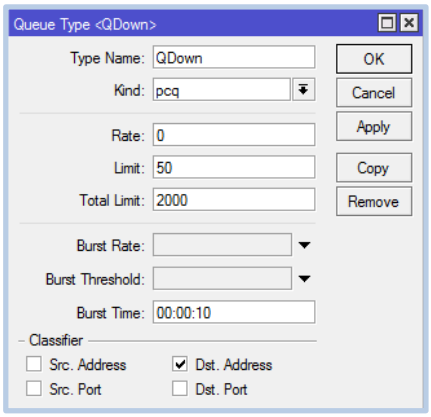


Figura 146. Configuración Queue Type Down

Type Name: Ingresamos Qup

Kind: Seleccionar pcq
Classifier: ✓ Src. Addess
Clic Apply
Clic OK

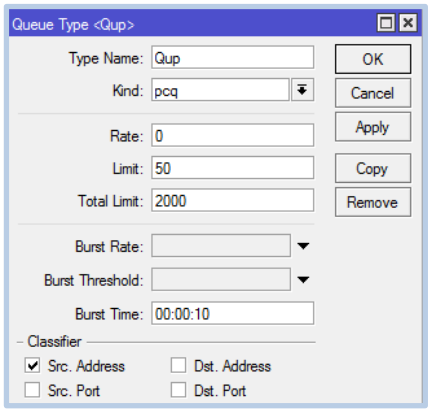
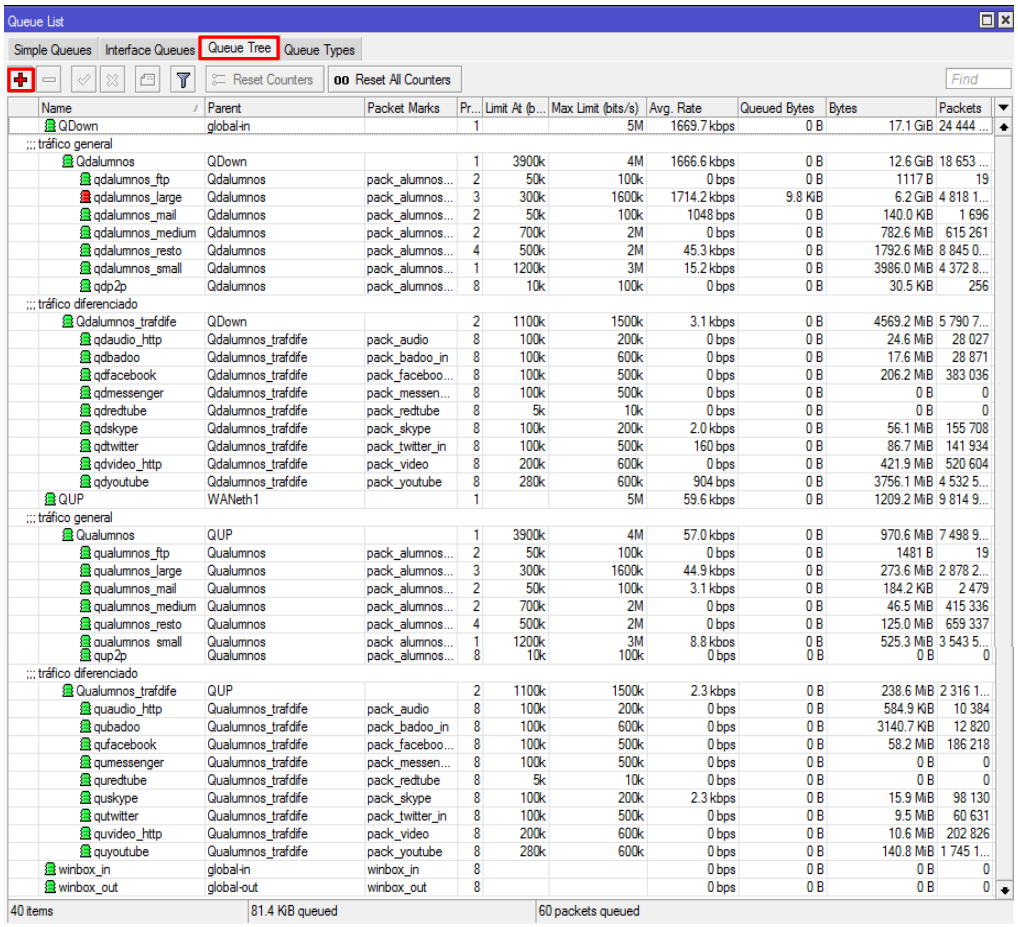


Figura 147. Configuración Queue Type Up

Ahora se configura la parte de la segmentación de ancho de banda para las distintas páginas y servicios que se marcaron previamente en las reglas de *Mangle* con *Mark Packet*, en el *Queue Tree*, figura 148, se las llama una por una.



Queue List

Simple Queues | Interface Queues | Queue Tree | Queue Types

Reset Counters | Reset All Counters | Find

Name	Parent	Packet Marks	Pr...	Limit At (b...	Max Limit (bits/s)	Avg. Rate	Queued Bytes	Bytes	Packets
QDown	global-in		1		5M	1669.7 kbps	0 B	17.1 GiB	24 444 ...
;;; tráfico general									
Qdalumnos	QDown		1	3900k	4M	1666.6 kbps	0 B	12.6 GiB	18 653 ...
qdalumnos_ftp	Qdalumnos	pack_alumnos...	2	50k	100k	0 bps	0 B	1117 B	19
qdalumnos_large	Qdalumnos	pack_alumnos...	3	300k	1600k	1714.2 kbps	9.8 KiB	6.2 GiB	4 818 1...
qdalumnos_mail	Qdalumnos	pack_alumnos...	2	50k	100k	1048 bps	0 B	140.0 KiB	1 696
qdalumnos_medium	Qdalumnos	pack_alumnos...	2	700k	2M	0 bps	0 B	782.6 MiB	615 261
qdalumnos_resto	Qdalumnos	pack_alumnos...	4	500k	2M	45.3 kbps	0 B	1792.6 MiB	8 845 0...
qdalumnos_small	Qdalumnos	pack_alumnos...	1	1200k	3M	15.2 kbps	0 B	3986.0 MiB	4 372 8...
qdp2p	Qdalumnos	pack_alumnos...	8	10k	100k	0 bps	0 B	30.5 KiB	256
;;; tráfico diferenciado									
Qdalumnos_trafdife	QDown		2	1100k	1500k	3.1 kbps	0 B	4569.2 MiB	5 790 7...
qdaudio_http	Qdalumnos_trafdife	pack_audio	8	100k	200k	0 bps	0 B	24.6 MiB	28 027
qdbadoo	Qdalumnos_trafdife	pack_badoo_in	8	100k	600k	0 bps	0 B	17.6 MiB	28 871
qdfacebook	Qdalumnos_trafdife	pack_faceboo...	8	100k	500k	0 bps	0 B	206.2 MiB	383 036
qdmessenger	Qdalumnos_trafdife	pack_messen...	8	100k	500k	0 bps	0 B	0 B	0
qdredtube	Qdalumnos_trafdife	pack_redtube	8	5k	10k	0 bps	0 B	0 B	0
qdskype	Qdalumnos_trafdife	pack_skype	8	100k	200k	2.0 kbps	0 B	56.1 MiB	155 708
qdtwitter	Qdalumnos_trafdife	pack_twitter_in	8	100k	500k	160 bps	0 B	86.7 MiB	141 934
qdvideo_http	Qdalumnos_trafdife	pack_video	8	200k	600k	0 bps	0 B	421.9 MiB	520 604
qdyoutube	Qdalumnos_trafdife	pack_youtube	8	280k	600k	904 bps	0 B	3756.1 MiB	4 532 5...
QUP	WANeth1		1		5M	59.6 kbps	0 B	1209.2 MiB	9 814 9...
;;; tráfico general									
Qualumnos	QUP		1	3900k	4M	57.0 kbps	0 B	970.6 MiB	7 498 9...
qualumnos_ftp	Qualumnos	pack_alumnos...	2	50k	100k	0 bps	0 B	1481 B	19
qualumnos_large	Qualumnos	pack_alumnos...	3	300k	1600k	44.9 kbps	0 B	273.6 MiB	2 878 2...
qualumnos_mail	Qualumnos	pack_alumnos...	2	50k	100k	3.1 kbps	0 B	184.2 KiB	2 479
qualumnos_medium	Qualumnos	pack_alumnos...	2	700k	2M	0 bps	0 B	46.5 MiB	415 336
qualumnos_resto	Qualumnos	pack_alumnos...	4	500k	2M	0 bps	0 B	125.0 MiB	659 337
qualumnos_small	Qualumnos	pack_alumnos...	1	1200k	3M	8.8 kbps	0 B	525.3 MiB	3 543 5...
qup2p	Qualumnos	pack_alumnos...	8	10k	100k	0 bps	0 B	0 B	0
;;; tráfico diferenciado									
Qualumnos_trafdife	QUP		2	1100k	1500k	2.3 kbps	0 B	238.6 MiB	2 316 1...
quaudio_http	Qualumnos_trafdife	pack_audio	8	100k	200k	0 bps	0 B	584.9 KiB	10 384
qubadoo	Qualumnos_trafdife	pack_badoo_in	8	100k	600k	0 bps	0 B	3140.7 KiB	12 820
qufacebook	Qualumnos_trafdife	pack_faceboo...	8	100k	500k	0 bps	0 B	58.2 MiB	186 218
qumessenger	Qualumnos_trafdife	pack_messen...	8	100k	500k	0 bps	0 B	0 B	0
quredtube	Qualumnos_trafdife	pack_redtube	8	5k	10k	0 bps	0 B	0 B	0
quskype	Qualumnos_trafdife	pack_skype	8	100k	200k	2.3 kbps	0 B	15.9 MiB	98 130
qutwitter	Qualumnos_trafdife	pack_twitter_in	8	100k	500k	0 bps	0 B	9.5 MiB	60 631
quvideo_http	Qualumnos_trafdife	pack_video	8	200k	600k	0 bps	0 B	10.6 MiB	202 826
quyoutube	Qualumnos_trafdife	pack_youtube	8	280k	600k	0 bps	0 B	140.8 MiB	1 745 1...
winbox_in	global-in	winbox_in	8			0 bps	0 B	0 B	0
winbox_out	global-out	winbox_out	8			0 bps	0 B	0 B	0

40 items | 81.4 KiB queued | 60 packets queued

Figura 148. Estructura final Queue Tree

El *Queue Tree* es una configuración en árbol, así que lo que se crea primeramente serán las variables globales, que son las que creamos en el Queue Type. Clic sobre (+) las creamos una por una: Qdown y QUP

*Las prioridades se cumplen del uno al ocho, siendo uno el más importante.

**Los rangos de ancho de banda son criterio del administrador y políticas internas de la institución.

Pestaña *General*:

Name: Ingresamos QDown

Parent: Seleccionar global-in
Queue Type: Seleccionar QDown
Priority: 1
Max Limit: 5M (AB acordado para la biblioteca)
Clic Apply
Clic OK

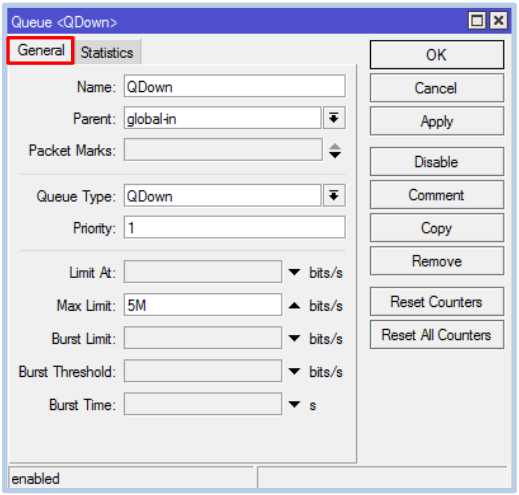


Figura 149. Configuración Queue/pestaña general

Pestaña *General*:

Name: Ingresamos QUP

Parent: Seleccionar global-in
Queue Type: Seleccionar Qup
Priority: 1
Max Limit: 5M (AB acordado para la biblioteca)
Clic Apply
Clic OK

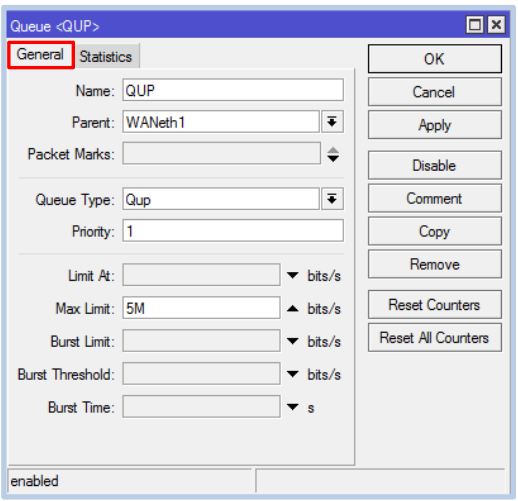


Figura 150. Configuración Queue/pestaña general

Para poder realizar una distribución ordena, a partir de las variables globales, se les creará dos variables secundarias para cada una, con el fin de diferenciar el tipo de tráfico marcado. Para esto nuevamente clic sobre (**+**) de la ventana Queue List.

Para QDown:

- Qdalumnos (tráfico general)
- Qdalumnos_trafdife (tráfico diferenciado).

Para QUP:

- Qualumnos (tráfico general)
- Qualumnos_trafdife (tráfico diferenciado).

Pestaña *General*:

Name: Ingresar Qdalumnos
Parent: Seleccionar QDown
Queue Type: Seleccionar QDown
Priority: 1
Limit At: 3900k
Max Limit: 4M
Comment: tráfico general
Clic Apply
Clic OK

Pestaña *General*:

Name: Ingresar Qdalumnos_trafdife
Parent: Seleccionar QDown
Priority: 2
Limit At: 1100k
Max Limit: 1500k
Comment: tráfico diferenciado
Clic Apply
Clic OK

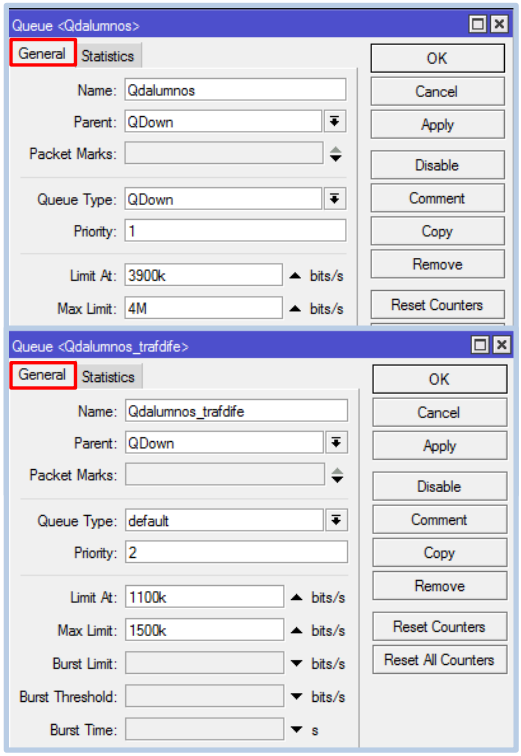


Figura 151. Configuración Queue/subvariables down

Pestaña *General*:

Name: Ingresar Qualumnos
Parent: Seleccionar QUP
Priority: 1
Limit At: 3900k
Max Limit: 4M
Comment: tráfico general
Clic Apply
Clic OK

Pestaña *General*:

Name: Ingresar Qualumnos_trafdife
Parent: Seleccionar QUP
Queue Type: Qup
Priority: 2
Limit At: 1100k
Max Limit: 1500k
Comment: tráfico diferenciado
Clic Apply
Clic OK

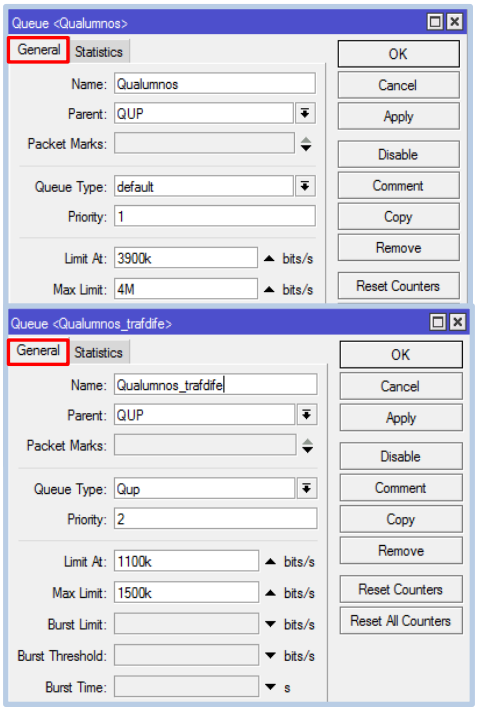


Figura 152. Configuración Queue/subvariables up

Para proceder a cumplir con el objetivo de segmentar el ancho de banda para las distintas páginas y servicios, se procede a llamar lo marcacado en mangle con mark packet. Por lo extenso que se haría la configuración se toma un ejemplo por cada variable secundaria tanto para download como para upload, para las demás reglas seria lo mismo. La configuración del árbol queda establecida de la siguiente manera, figura 153:

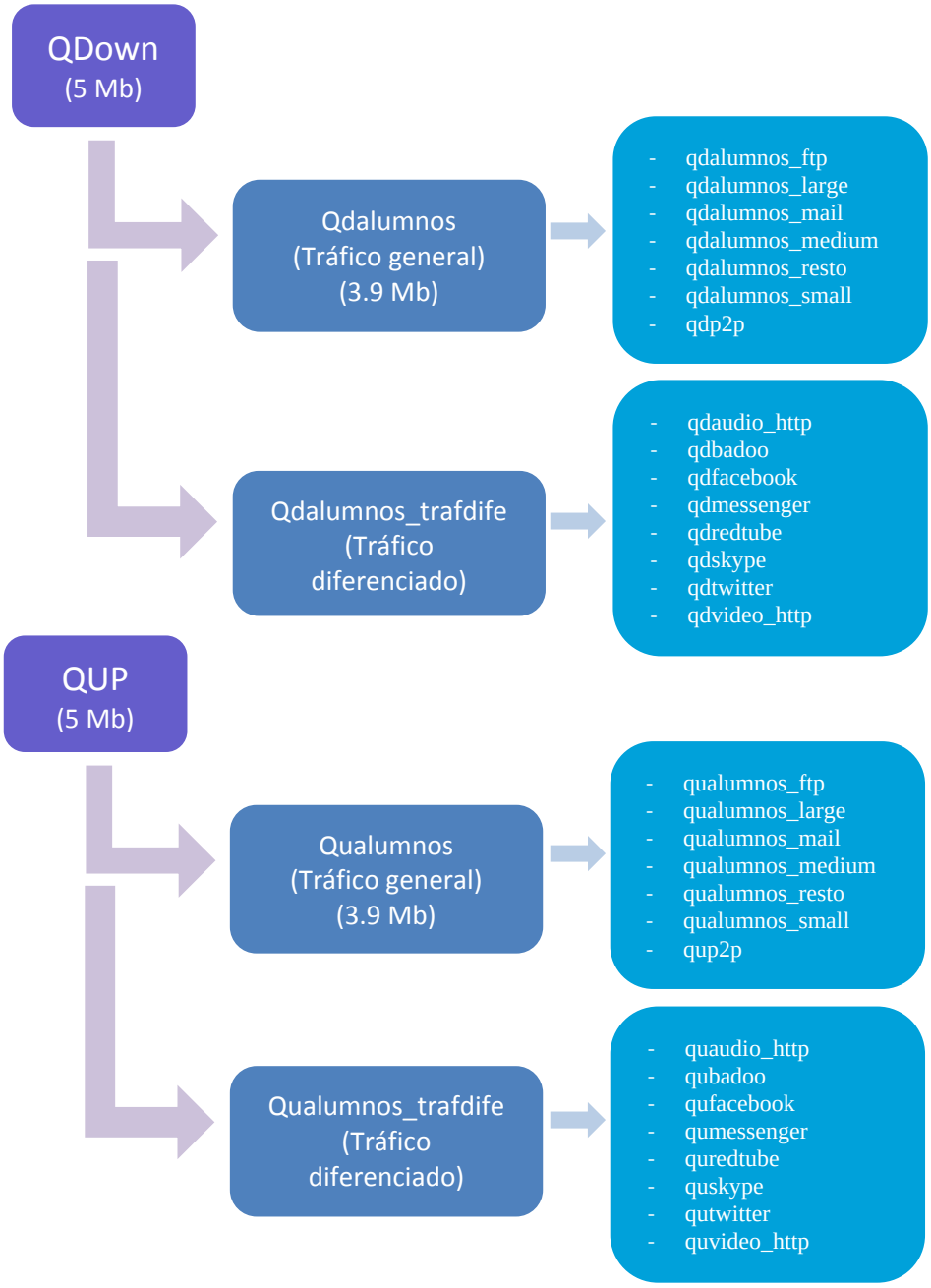


Figura 153. Estructura de la segmentación del servicio de internet en la biblioteca

Para la configuración de Qdalumnos_large, clic sobre (+).

Pestaña *General*:

Name: Ingresamos qdalumnos_large
Parent: Seleccionar Qdalumnos
Packet Marks: Seleccionar pack_alumnos_largein
Queue Type: QDown
Priority: 3
Limit At: 300k
Max Limit: 1600k
Clic Apply
Clic OK

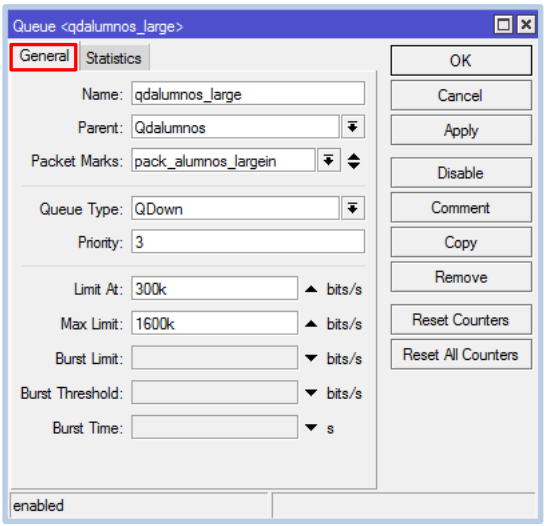


Figura 154. Configuración Queue/qdown páginas

Pestaña *General*:

Name: Ingresamos qualumnos_large
Parent: Seleccionar Qualumnos
Packet Marks: Seleccionar pack_alumnos_largeout
Queue Type: Qup
Priority: 3
Limit At: 300k
Max Limit: 1600k
Clic Apply
Clic OK

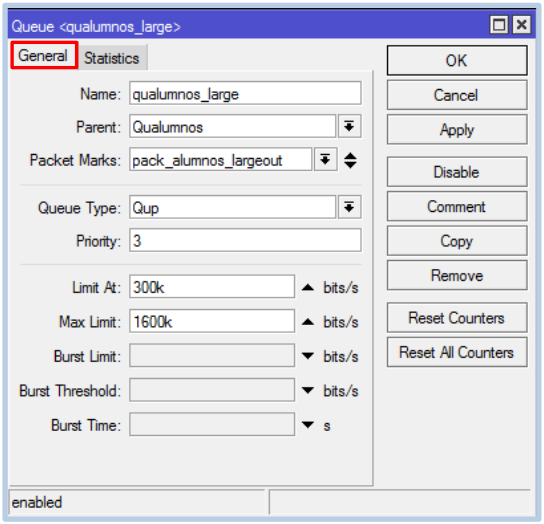


Figura 155. Configuración Queue/qup páginas

Para la configuración de qdyoutube, clic sobre (+).

Pestaña *General*:

Name: Ingresar qdyoutube
Parent: Seleccionar Qdalumnos_trafdife
Packet Marks: Seleccionar pack_youtube
Queue Type: QDown
Priority: 8
Limit At: 280k
Max Limit: 600k
Clic Apply
Clic OK

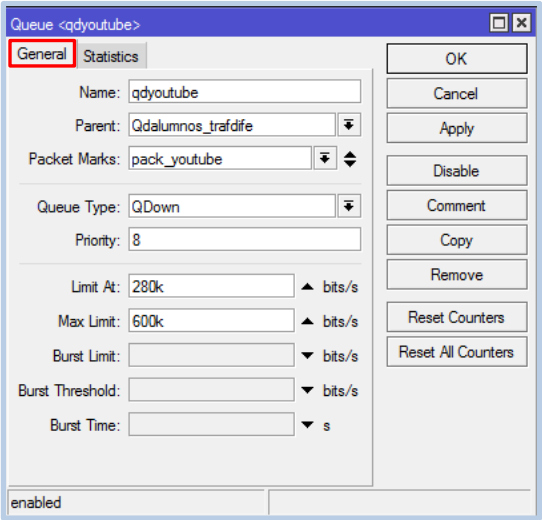


Figura 156. Configuración Queue/qdown youtube

Pestaña *General*:

Name: Ingresar quyoutube
Parent: Seleccionar Qualumnos_trafdife
Packet Marks: Seleccionar pack_youtube
Queue Type: Qup
Priority: 8
Limit At: 280k
Max Limit: 600k
Clic Apply
Clic OK

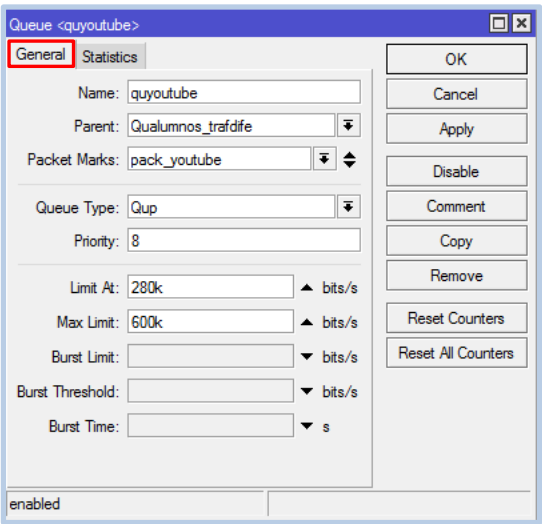


Figura 157. Configuración Queue/qup youtube

f.4.5 Otras Herramientas

f.4.5.1 Ingreso vía web

Para realizar cualquier configuración o sólo ingresar al equipo para observar su comportamiento, en caso de no tener instalado el programa winbox, también es posible acceder al mismo mediante la web. En caso de encontrarse fuera de la red del equipo, se

logra loguear con la dirección de WANeth0 IP 172.xx.xx.xx5487; en el caso de encontrarse en la red del equipo, se ingresa con la dirección IP 192.168.4.1:5487.

Figura 158. Interfaz para ingresar al equipo vía web

Se ingresa los datos que pide como son Login y Password, figura 158, clic en login y aparece la interfaz vía web, figura 159. Cabe mencionar que por este medio se ingresa con los mismos usuarios y contraseñas respectivas con los que se logea en el winbox.

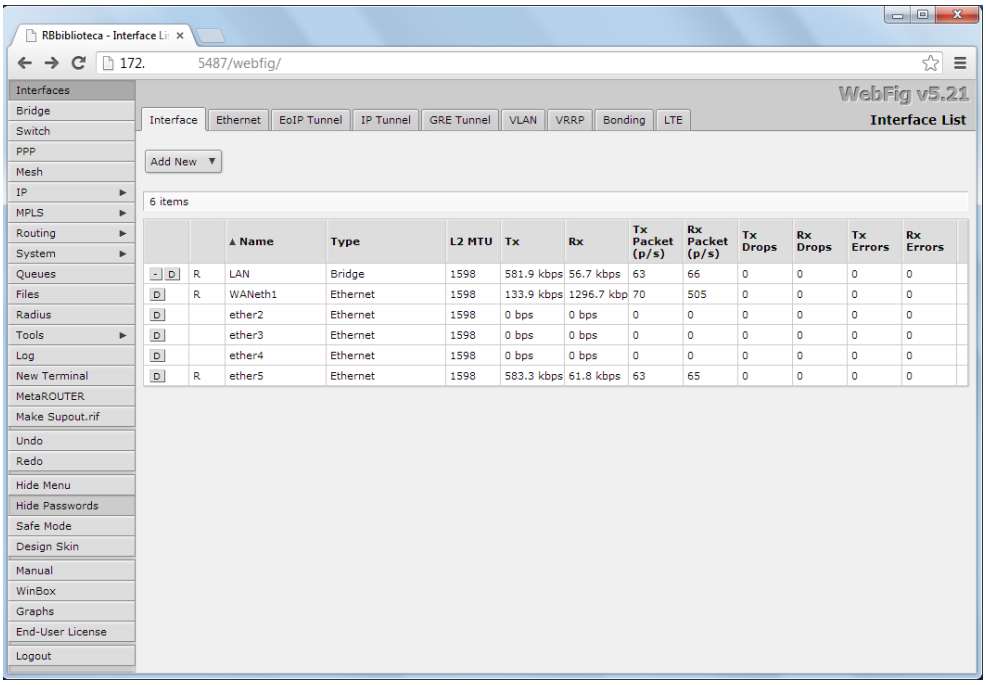


Figura 159. Interfaz web del Mikrotik

f.4.5.2 Graphing

Graphing es una herramienta para monitorear diversos parámetros de Mikrotik en tiempo real y presentar los datos recogidos en gráficos. Consta de dos partes - la primera parte recoge la información y la otra parte es la de muestrar los datos en una página Web.

Del menú principal, clic sobre el menú *Tools*, y se despliega una lista de submenús, seleccionamos *Graphing*. Aparecerá una ventana de Graphing, figura 160, clic sobre (+) y configuramos lo siguiente.

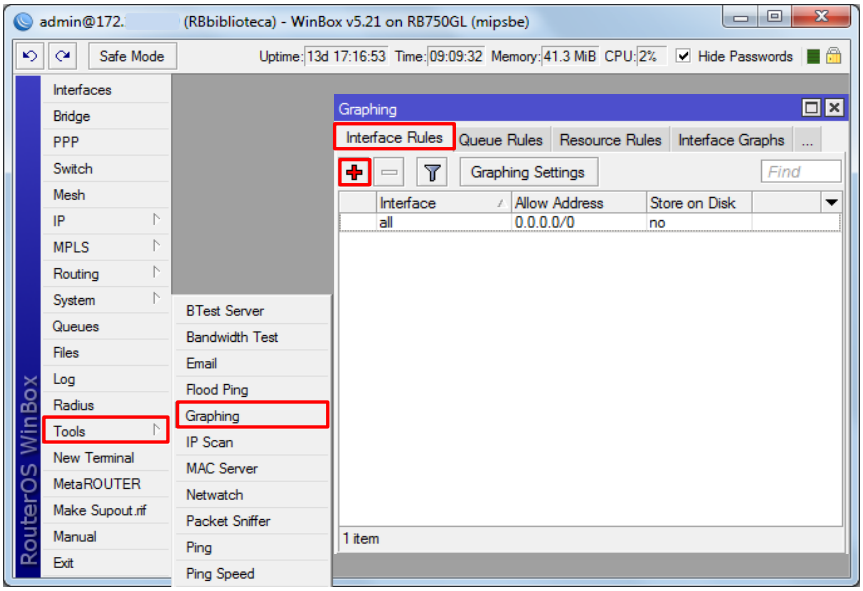


Figura 160. Herramienta Graphing

Ventana Interface Graphing Rule:

Interface: Seleccionar all
Allow Address: 0.0.0.0/0
Deshabilitado Store on Disk
Clic Apply
Clic OK

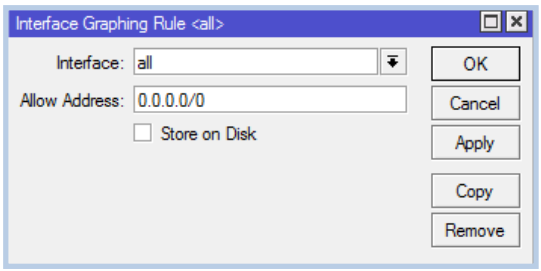


Figura 161. Configuración del Graphing

Ventana Graphing:

Clic Graphing Settings
Store Every: Seleccionar 5 min.
Clic Apply
Clic OK

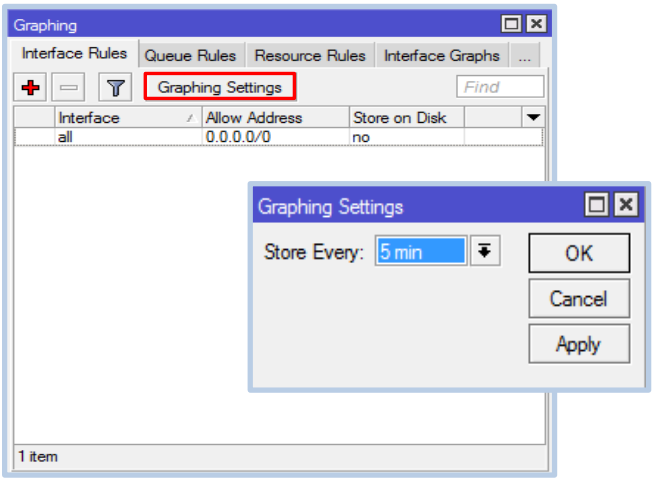


Figura 162. Configuración del intervalo de tiempo de actualización

Esta configuración ayuda a visualizar vía web el comportamiento del consumo de ancho de banda por parte de la LAN. Clic sobre *Graphs*, luego sobre la interfaz que desea vizualizar, figura 163.

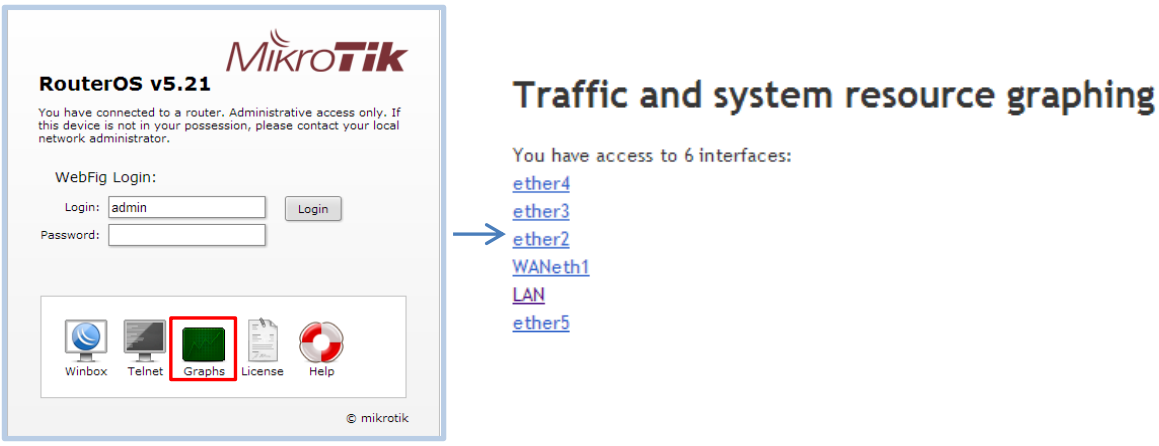


Figura 163. Interfaz para la visualización de las gráficas de consumo

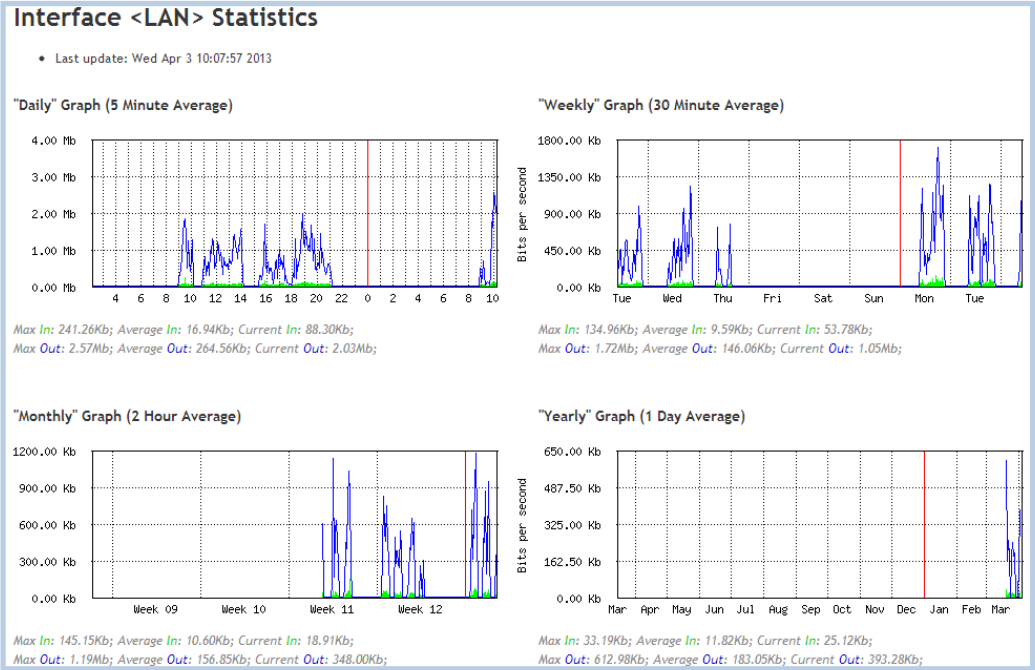


Figura 164. Gráficas de consumo

f.4.5.3 Torch

La herramienta *Torch* sirve para determinar puertos e IPs que están siendo utilizados por internet, esto ayuda a quien configura el equipo para determinar cuáles serán las páginas y puertos más utilizados para poder crear reglas para el marcado de paquetes, con esta herramienta también se puede conocer cuánto consume la interfaz que seleccione. Otra utilidad que tiene la herramienta es al momento de realizar pruebas de configuración, para ir revisando si es que los puertos están marcando bien. En resumen, con esta herramienta se logra monitorear todos los movimientos de los usuarios identificados con cierta IP.

Del menú principal, clic sobre *Tools*, de la lista que se despliega seleccionar *Torch*, figura 165, aparecerá una ventana en la que se seleccionará lo que se desee visualizar. De la gráfica 93, en Interfaz seleccionar LAN, activar: Protocol, Port, Src. Address y Dst. Address o lo que desee escanear. Clic sobre *Start* para empezar, clic *Stop* para detener.

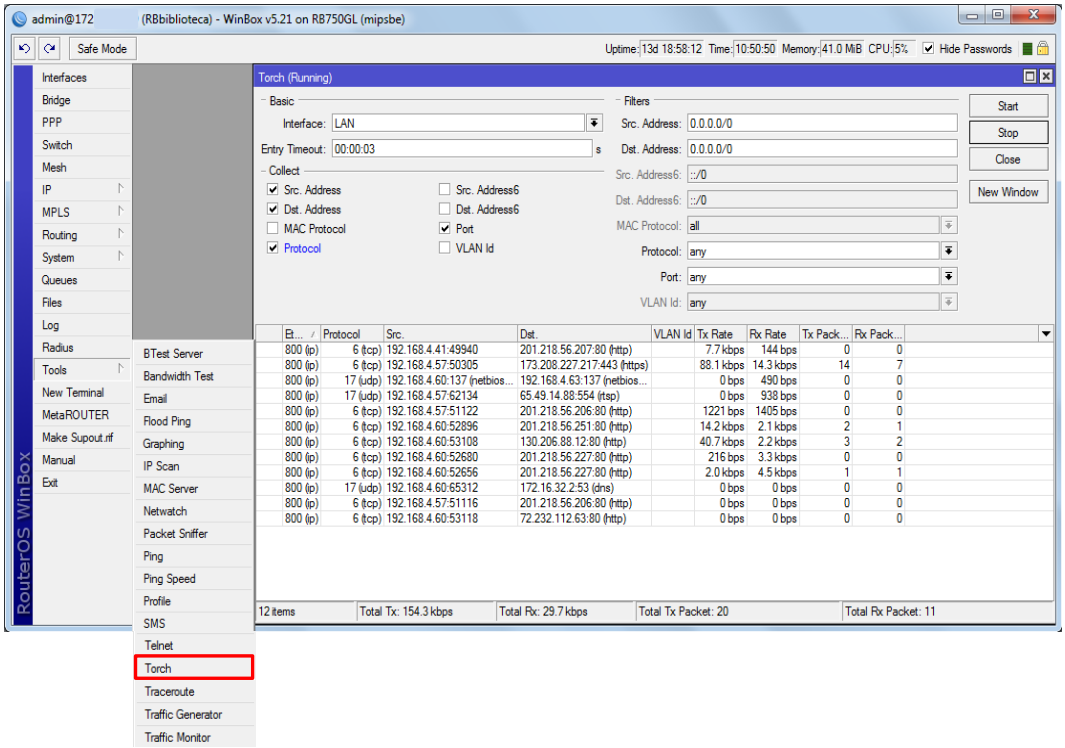


Figura 165. Herramienta Torch

f.4.5.4 IP Scan

La herramienta IP Scan permite al administrador escanear su red y saber cuáles IPs fueron asignadas y que están siendo utilizadas por determinado host en ese tiempo. Del menú principal, clic sobre *Tools* y de la lista que se despliega clic sobre *IP Scan*, figura 166. Se puede realizar el scan tanto por interfaz así como también por rango de IPs.

Ventana IP Scan:

Interface: LAN
Clic Start
Clic Stop

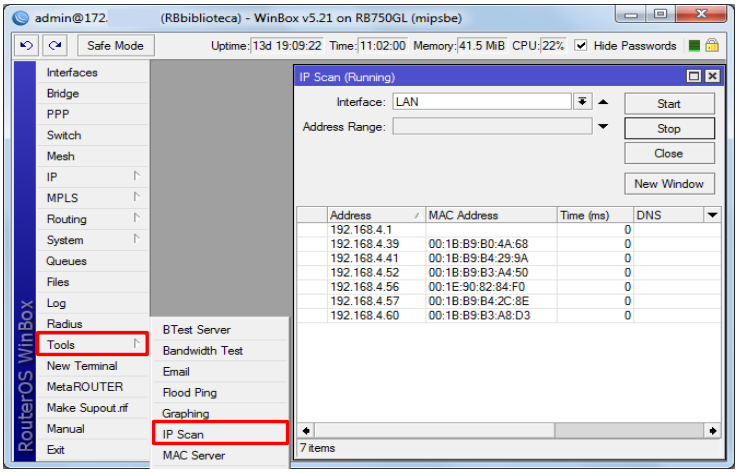


Figura 166. Herramienta IP Scan

f.5 Pruebas del sistema Mikrotik

f.5.1 New Terminal

El *New Terminal*, figura 167, se utiliza para acceder a la configuración del router Mikrotik y características de gestión que utilizan terminales de texto, es decir, clientes de terminales remotas, así como de monitor y teclado locales. Se utiliza para escribir guiones. Este manual describe los principios generales de la consola de operación. Para el buen manejo de esta herramienta es necesario conocer sobre cómo escribir scripts.

Figura 167. New Terminal

Resumen de funciones comunes

- ✓ Permite modificar la configuración del router utilizando comandos de texto. La estructura de mando es similar a la shell de Unix. Existe una gran cantidad de comandos disponibles, que están divididos en jerarquía. Por ejemplo, todos (bueno, casi todos) los comandos que trabajan con rutas comienzan con "ip route":

```
[admin@RBbiblioteca] > ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 A S  0.0.0.0/0                           172.xx.xx.xx              1
 1 ADC  172.xx.xx.xx/xx     172.xx.xx.xx    WANeth1                   0
 2 ADC  192.xx.xx.xx/xx     192.xx.xx.xx    LAN                       0
```

- ✓ En lugar de escribir "ip route" antes de cada mandato, se puede escribir una vez para "cambiar a" esa rama de la jerarquía. Así, el ejemplo anterior también podría ser ejecutado de esta manera:

```
[admin@RBbiblioteca] /ip route> print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
 #      DST-ADDRESS        PREF-SRC        GATEWAY            DISTANCE
 0 A S  0.0.0.0/0                           172.16.32.1               1
 1 ADC  172.xx.xx.xx/xx     172.xx.xx.xx    WANeth1                    0
 2 ADC  192.xx.x.x/xx       192.xx.xx.xx    LAN                        0
```

- ✓ Para cambiar de nivel en la jerarquía de mando que se encuentra en este momento escriba "/"

```
[drax] ip route> /
[drax]>
```

- ✓ Para subir un nivel de comandos, escriba ".."

```
[drax] ip route>..
[drax] ip>
```

- ✓ También puede utilizar "/" y ".." para ejecutar comandos de otros niveles sin cambiar el nivel actual:

```
[drax] ip route> /ping 10.0.0.10
timeout: ping reply not recieved after 1000 mss
timeout: ping reply not recieved after 1000 mss
2 packets transmitted, 0 packets received, 100% packet loss
```

- ✓ O bien, para volver al nivel de base se puede utilizar el ".." dos veces:

```
[admin@RBbiblioteca] > ip route
[admin@RBbiblioteca] /ip route>.. .. ping 192.xx.xx.xx
HOST                                      SIZE TTL TIME  STATUS
192.xx.xx.xx                                 56  64 0ms
192.xx.xx.xx                                 56  64 1ms
192.xx.xx.xx                                 56  64 3ms
    sent=3 received=3 packet-loss=0% min-rtt=0ms avg-rtt=1ms max-rtt=3ms
```

- ✓ Muchos de los comandos de nivel operan como matrices: interfaces, rutas, usuarios, etc. Estas matrices se muestran en listas. Todos los elementos de la lista tienen un número de orden seguido por los valores de sus parámetros. Por ejemplo:

```
[admin@RBbiblioteca] > interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
 #     NAME                          TYPE                MTU L2MTU  MAX-
L2MTU
 0     ether4                        ether              1500  1598
4074
 1     ether3                        ether              1500  1598
4074
 2     ether2                        ether              1500  1598
4074
 3  R  WANeth1                       ether              1500  1598
4074
 4  R  LAN                           bridge             1500  1598
 5  R  ether5                        ether              1500  1598
4074
```

- ✓ Para cambiar los parámetros de un elemento (configuración de una interfaz en particular), deberá especificar su número al comando "set", ejemplo:

```
[drax]> interface set 1 mtu=1460
[drax]> interface print
Flags: X - disabled, D - dynamic
  #   NAME                 MTU   TYPE
  0 X ether1               1500  ether
  1   ether2               1460  ether
  2 X pptp-in1                   pptp-in
  3   tunl                 1500  eoip-tunnel
```

Nota: Aunque los números pueden cambiar cada vez que se utiliza el comando "print", estos no cambiarán su configuración. Una vez asignado, seguirán siendo el mismo hasta que salga del modo consola o hasta que el próximo comando "print" se ejecute.

- ✓ Si lo que se desea es exportar reglas de las distintas configuraciones, basta con escribir primero la dirección del menú principal, luego la dirección del submenú (en caso de que sea ocupe) y al final "export", ejemplo:

```
[admin@RBbiblioteca] > ip firewall export
# apr/10/2013 16:07:15 by RouterOS 5.21
# software id = TU43-RF8Y
#
/ip firewall layer7-protocol
```

```
add name=msn regexp="ver [0-9] + msnp [1-9][0-9]\? [\\x09-\\x0d -
~]*cvr0\\x0d\
\x\......
```

El comando "export" imprime una secuencia de comandos que se puede utilizar para restaurar la configuración. Si tiene el argumento "from", entonces es posible exportar únicamente los elementos especificados. Además, si el argumento "from" está dado, "export" no desciende recursivamente en la jerarquía de mando. El comando "export" también tiene el argumento de "file", que le permite guardar el archivo de secuencia de comandos en el router para recuperarla más tarde.

- ✓ El modo consola cuenta con una ayuda integrada, que se puede acceder tecleando "?"'. La regla general es que la ayuda muestra lo que se puede escribir en la posición donde el '?' se ha ingresado (de manera similar al presionar la tecla TAB para completar comandos que no estamos seguros).

- ✓ El comando "find" tiene los mismos argumentos de "set", y el argumento "from" que funciona como el argumento "from" con el comando "print". El comando "find" devuelve números internos de todos los elementos que tienen los mismos valores de los argumentos de la forma especificada.

- ✓ El comando "ping" es muy útil al momento de comprobar la salida de internet desde el equipo, si al hacer "ping" desde dentro del equipo se obtiene una respuesta favorable quiere decir que la configuración está bien hecha, caso contrario habría que volver a revisar los parámetros principales tales como: ip/dns, ip/routes, ip/dhcp_server, ip/addresses.

f.5.2 Direccionamiento y Asignación IP

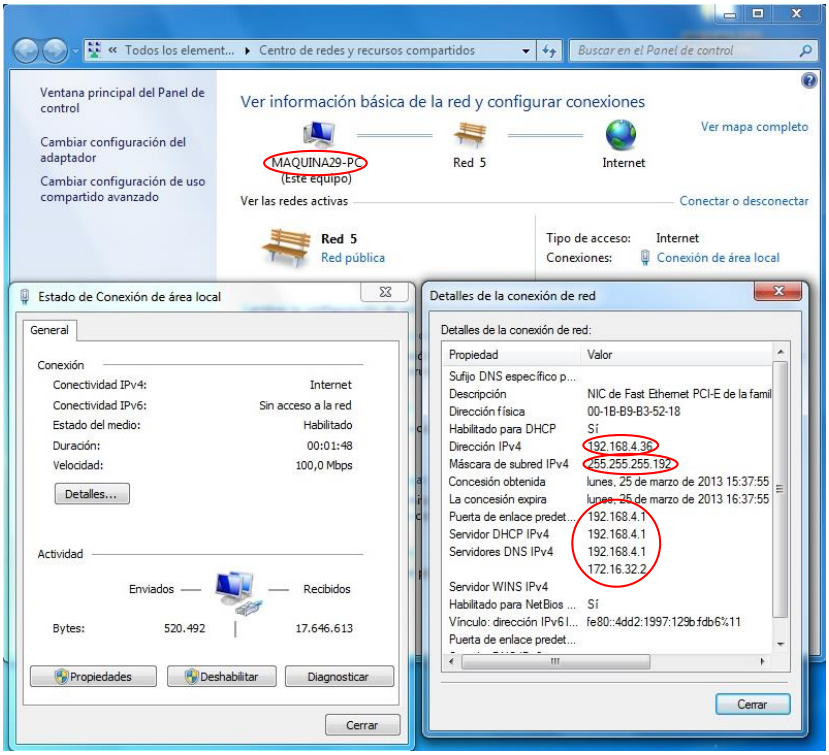


Figura 168. Demostración de direccionamiento IP

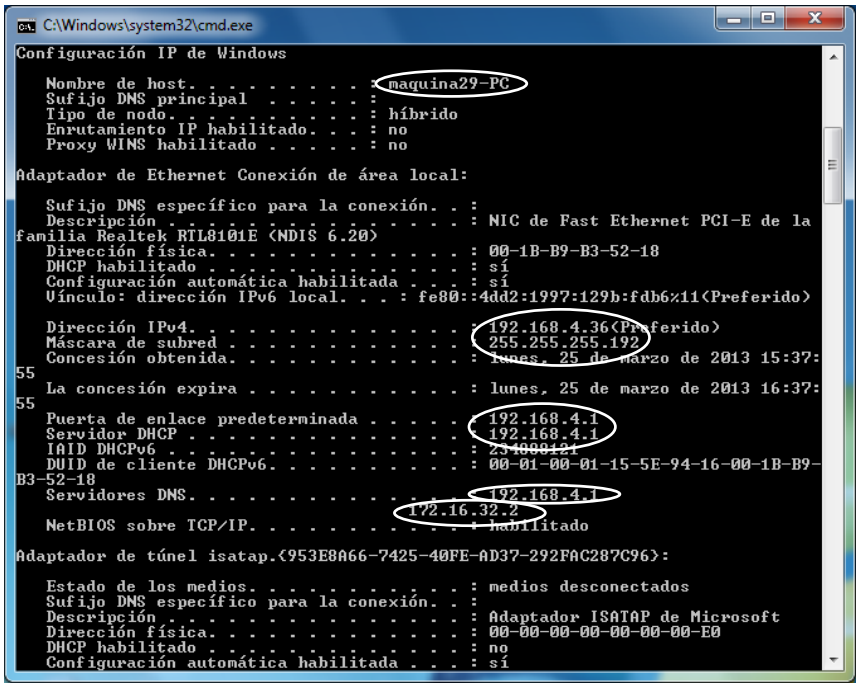


Figura 169. Ping demostración de direccionamiento IP

f.5.3 PING (salida a Internet)

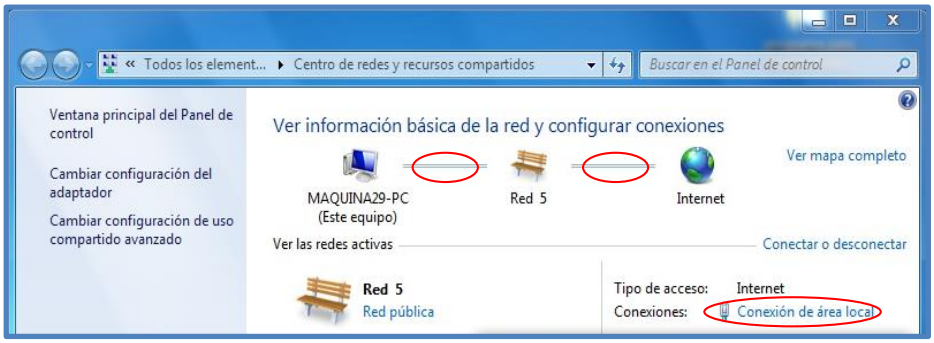


Figura 170. Demostración de enlace de interne

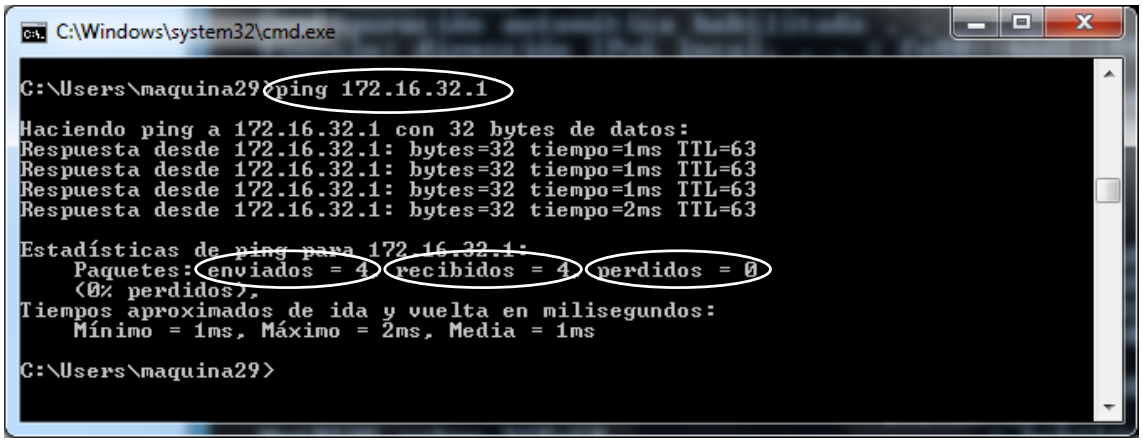


Figura 171. Ping a la puerta de enlace de la Universidad

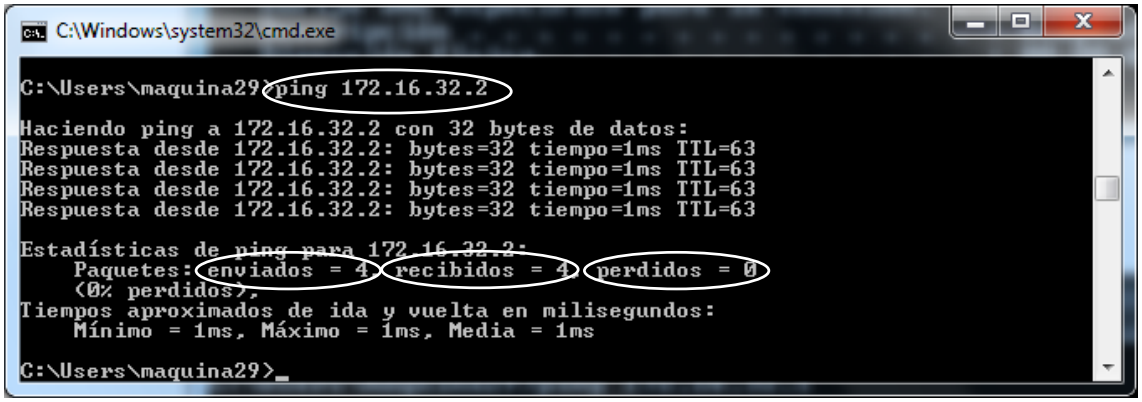


Figura 172. Ping al DNS de la Universidad

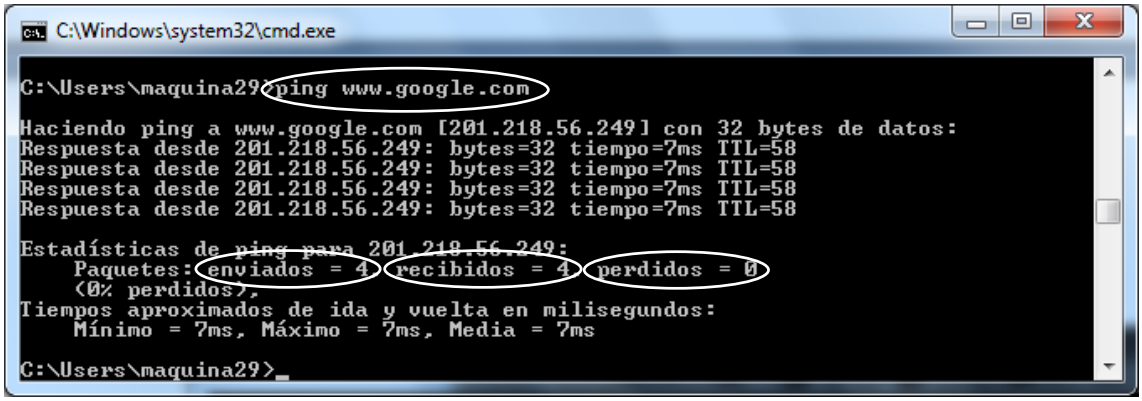
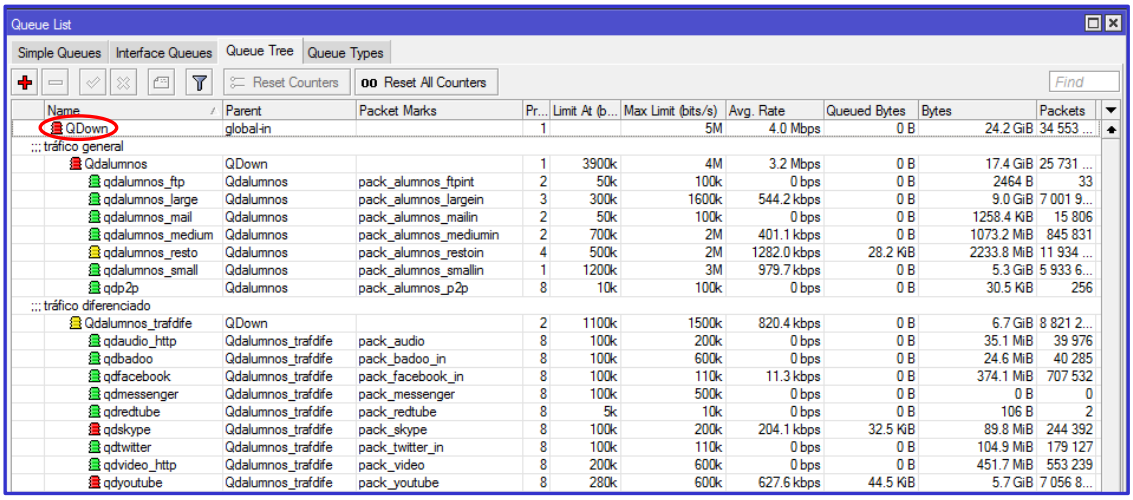


Figura 173. Ping a Google

f.5.4 Segmentación



Queue List

Simple Queues | Interface Queues | Queue Tree | Queue Types

Reset Counters | Reset All Counters | Find

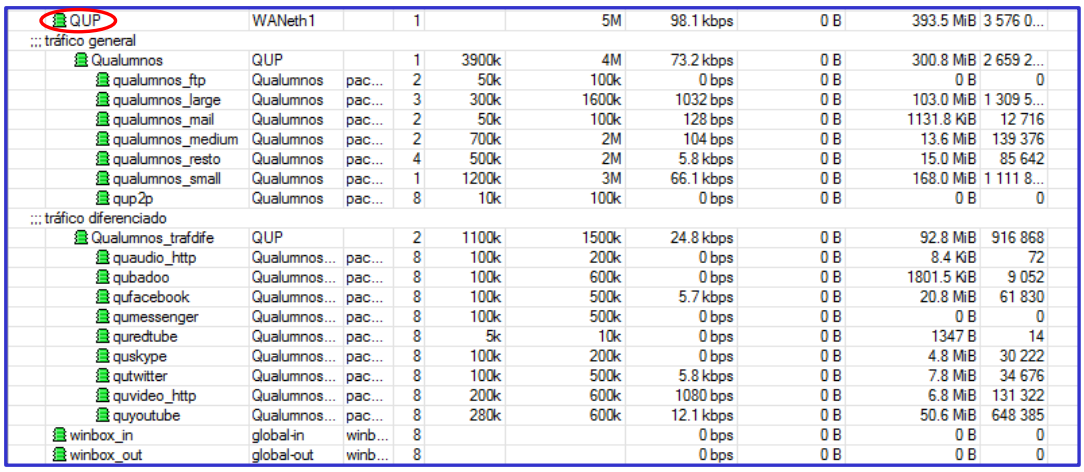
Name	Parent	Packet Marks	Pr...	Limit At (b...	Max Limit (bits/s)	Avg. Rate	Queued Bytes	Bytes	Packets
QDown	global-in		1		5M	4.0 Mbps	0 B	24.2 GiB	34 553 ...
;;; tráfico general									
Qdalumnos	QDown		1	3900k	4M	3.2 Mbps	0 B	17.4 GiB	25 731 ...
qdalumnos_ftp	Qdalumnos	pack_alumnos_ftpint	2	50k	100k	0 bps	0 B	2464 B	33
qdalumnos_large	Qdalumnos	pack_alumnos_largein	3	300k	1600k	544.2 kbps	0 B	9.0 GiB	7 001 9...
qdalumnos_mail	Qdalumnos	pack_alumnos_mailin	2	50k	100k	0 bps	0 B	1258.4 KiB	15 806
qdalumnos_medium	Qdalumnos	pack_alumnos_mediumin	2	700k	2M	401.1 kbps	0 B	1073.2 MiB	845 831
qdalumnos_resto	Qdalumnos	pack_alumnos_restoin	4	500k	2M	1282.0 kbps	28.2 KiB	2233.8 MiB	11 934 ...
qdalumnos_small	Qdalumnos	pack_alumnos_smallin	1	1200k	3M	979.7 kbps	0 B	5.3 GiB	5 933 6...
qdp2p	Qdalumnos	pack_alumnos_p2p	8	10k	100k	0 bps	0 B	30.5 KiB	256
;;; tráfico diferenciado									
Qdalumnos_trafdife	QDown		2	1100k	1500k	820.4 kbps	0 B	6.7 GiB	8 821 2...
qdaudio_http	Qdalumnos_trafdife	pack_audio	8	100k	200k	0 bps	0 B	35.1 MiB	39 976
qdbadoo	Qdalumnos_trafdife	pack_badoo_in	8	100k	600k	0 bps	0 B	24.6 MiB	40 285
qdfacebook	Qdalumnos_trafdife	pack_facebook_in	8	100k	110k	11.3 kbps	0 B	374.1 MiB	707 532
qdmessenger	Qdalumnos_trafdife	pack_messenger	8	100k	500k	0 bps	0 B	0 B	0
qdredtube	Qdalumnos_trafdife	pack_redtube	8	5k	10k	0 bps	0 B	106 B	2
qdskype	Qdalumnos_trafdife	pack_skype	8	100k	200k	204.1 kbps	32.5 KiB	89.8 MiB	244 392
qdtwitter	Qdalumnos_trafdife	pack_twitter_in	8	100k	110k	0 bps	0 B	104.9 MiB	179 127
qdvideo_http	Qdalumnos_trafdife	pack_video	8	200k	600k	0 bps	0 B	451.7 MiB	553 239
qdyoutube	Qdalumnos_trafdife	pack_youtube	8	280k	600k	627.6 kbps	44.5 KiB	5.7 GiB	7 056 8...

Figura 174. Demostración de marcado de paquetes en Queue List-QDown

*Color verde: Dentro del límite de ancho de banda asignado.

**Color amarillo: Aproximándose al límite máximo de ancho de banda asignado.

***Color Rojo: Ancho de banda saturado.



QUP	WANeth1		1		5M	98.1 kbps	0 B	393.5 MiB	3 576 0...
;;; tráfico general									
Qualumnos	QUP		1	3900k	4M	73.2 kbps	0 B	300.8 MiB	2 659 2...
qualumnos_ftp	Qualumnos	pac...	2	50k	100k	0 bps	0 B	0 B	0
qualumnos_large	Qualumnos	pac...	3	300k	1600k	1032 bps	0 B	103.0 MiB	1 309 5...
qualumnos_mail	Qualumnos	pac...	2	50k	100k	128 bps	0 B	1131.8 KiB	12 716
qualumnos_medium	Qualumnos	pac...	2	700k	2M	104 bps	0 B	13.6 MiB	139 376
qualumnos_resto	Qualumnos	pac...	4	500k	2M	5.8 kbps	0 B	15.0 MiB	85 642
qualumnos_small	Qualumnos	pac...	1	1200k	3M	66.1 kbps	0 B	168.0 MiB	1 111 8...
qup2p	Qualumnos	pac...	8	10k	100k	0 bps	0 B	0 B	0
;;; tráfico diferenciado									
Qualumnos_trafdife	QUP		2	1100k	1500k	24.8 kbps	0 B	92.8 MiB	916 868
quaudio_http	Qualumnos...	pac...	8	100k	200k	0 bps	0 B	8.4 KiB	72
qubadoo	Qualumnos...	pac...	8	100k	600k	0 bps	0 B	1801.5 KiB	9 052
qufacebook	Qualumnos...	pac...	8	100k	500k	5.7 kbps	0 B	20.8 MiB	61 830
qumessenger	Qualumnos...	pac...	8	100k	500k	0 bps	0 B	0 B	0
quredtube	Qualumnos...	pac...	8	5k	10k	0 bps	0 B	1347 B	14
quskype	Qualumnos...	pac...	8	100k	200k	0 bps	0 B	4.8 MiB	30 222
qutwitter	Qualumnos...	pac...	8	100k	500k	5.8 kbps	0 B	7.8 MiB	34 676
quvideo_http	Qualumnos...	pac...	8	200k	600k	1080 bps	0 B	6.8 MiB	131 322
quyoutube	Qualumnos...	pac...	8	280k	600k	12.1 kbps	0 B	50.6 MiB	648 385
winbox_in	global-in	winb...	8			0 bps	0 B	0 B	0
winbox_out	global-out	winb...	8			0 bps	0 B	0 B	0

Figura 175. Demostración de marcado de paquetes en Queue List-QUP

f.5.5 Generación de tráfico entrante y saliente

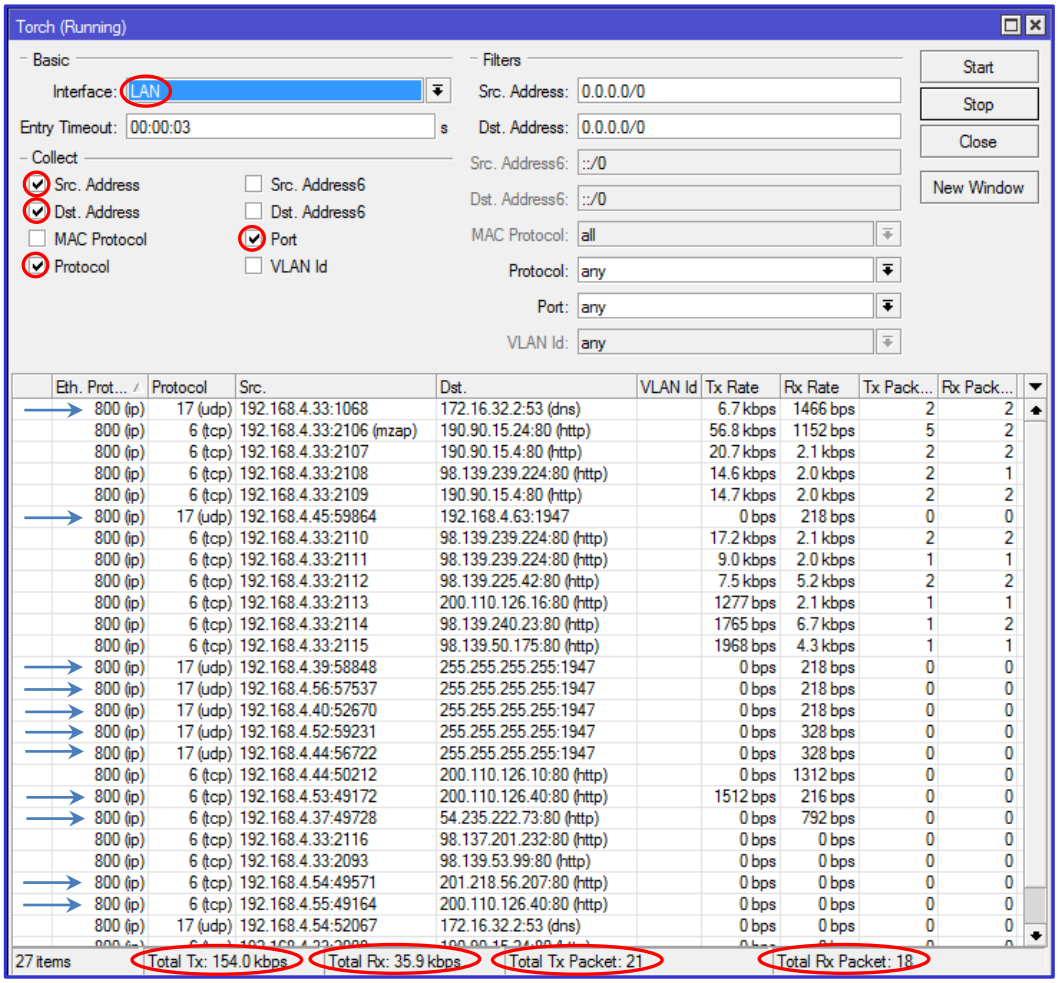


Figura 176. **Tráfico LAN genererado por los usuarios en la biblioteca**

f.5.6 Consumo de Ancho de Banda

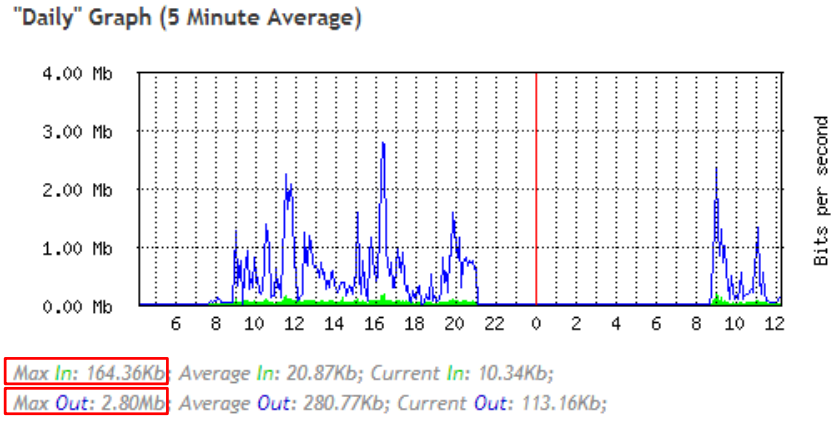


Figura 177. Consumo de ancho de banda 24 horas (26 de Marzo 2013)

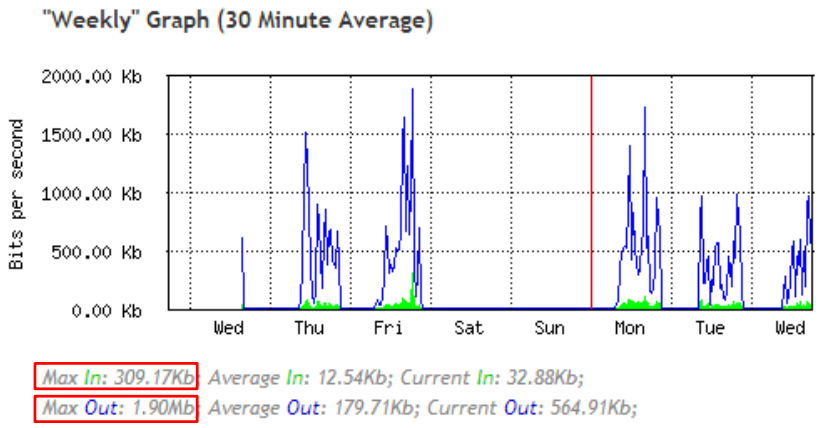


Figura 178. Consumo de ancho de banda una semana (20/27 de Marzo 2013

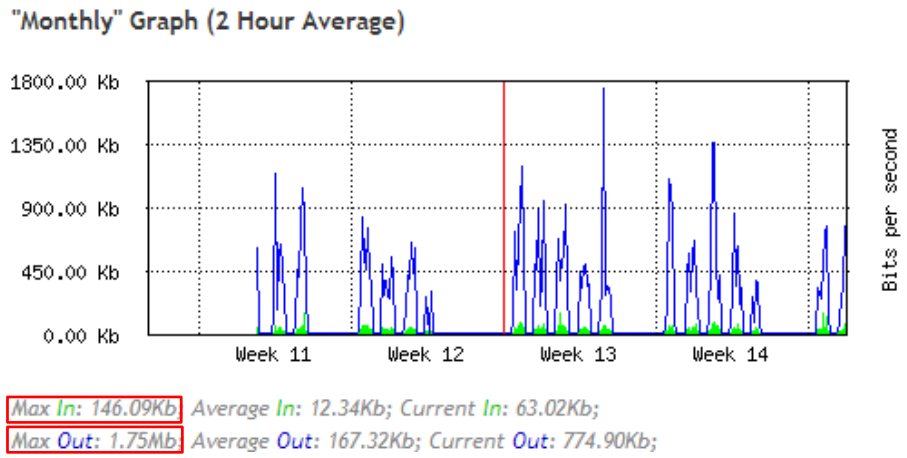


Figura 179. Consumo de ancho de banda de un mes (14 Marzo al 14 de Abril 2013)

f.6 Configuración para el Acceso Inalámbrico

Para la nueva distribución en el pool del mikrotik de la cual se va a disponer a partir de la conexión del AP, se realiza una tabla resumen con la función que se le dará a cada una de las IPs de la dirección de red 192.168.4.0/26. Tabla 39.

Tabla 39. Direccionamiento a partir de la inclusión del AP

FUNCIÓN	DIRECCIÓN IP
Dirección LAN equipo Mikrotik	192.168.4.1
Admin. Estática equipo Mikrotik	192.168.4.2
Crecimiento	192.168.4.3-192.168.4.5
Dirección LAN AP	192.168.4.6
DHCP/AP	192.168.4.7-192.168.4.26
DHCP/LAN equipo Mikrotik	192.168.4.27-192.168.4.62

f.6.1 Configuración del Pool en el equipo Mikrotik

Del menú principal seleccionar *IP* y de la lista de submenús que se despliega seleccionar *Pool*, aparecerá ya el pool que antiguamente se tenía configurado para el DHCP de la LAN, pero como se va a conectar el AP el rango de IPs va a cambiar. Doble clic sobre el pool, figura 180, y cambiamos a 192.168.4.27-192.168.4.62 el cual dispone de 36 direcciones IP para la conexión cableada.

.

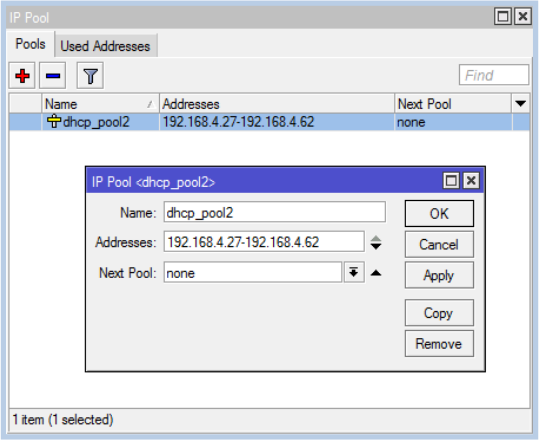


Figura 180. Pool de IPs

f.6.2 Configuración en el AP

En el menú LAN, pestaña Home:

IP address: 192.xx.xx.xx

Subnet Mask: 255.255.255.xx

Default Gateway: 192.xx.xx.xx

Clic en Apply

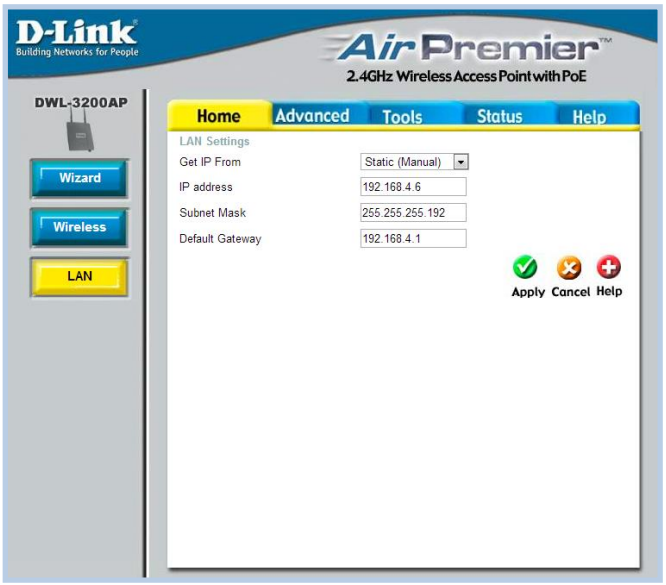


Figura 181. Configuración LAN

En el menú Wireless, pestaña Advanced:

IP Assigned From: 192.xx.xx.xx

The Range of Pool: 20

SubMask: 255.255.255.xx

Gateway: 192.xx.xx.xx

Wins: 192.xx.xx.xx

DNS: 172.xx.xx.xx

Status: On

Clic en Apply

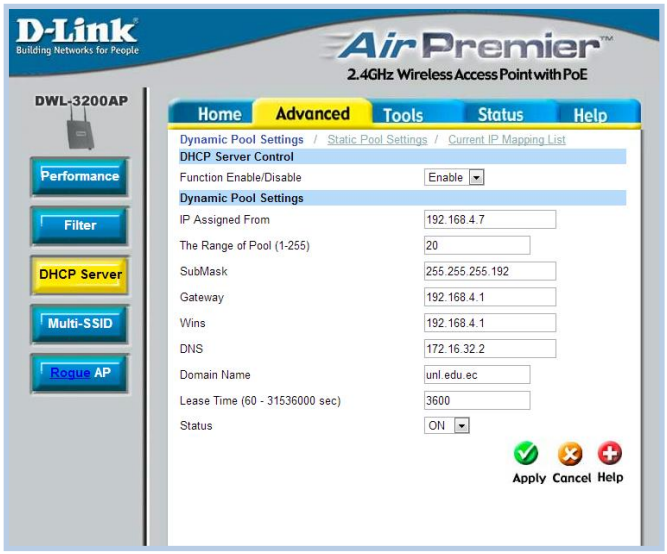
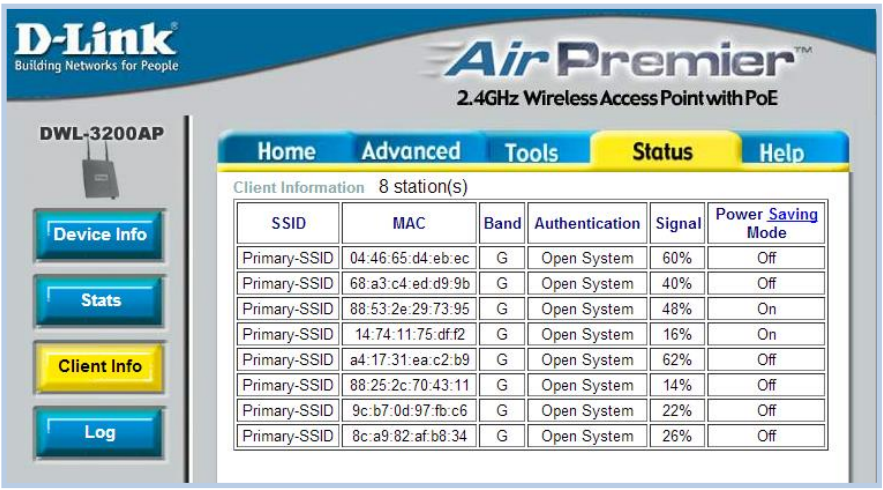


Figura 182. Configuración DCHP Server

En la pestaña Status se puede vizualizar información de los usuarios conectados, figura 183.



SSID	MAC	Band	Authentication	Signal	Power Saving Mode
Primary-SSID	04:46:65:d4:eb:ec	G	Open System	60%	Off
Primary-SSID	68:a3:c4:ed:d9:9b	G	Open System	40%	Off
Primary-SSID	88:53:2e:29:73:95	G	Open System	48%	On
Primary-SSID	14:74:11:75:df:f2	G	Open System	16%	On
Primary-SSID	a4:17:31:ea:c2:b9	G	Open System	62%	Off
Primary-SSID	88:25:2c:70:43:11	G	Open System	14%	Off
Primary-SSID	9c:b7:0d:97:fb:c6	G	Open System	22%	Off
Primary-SSID	8c:a9:82:af:b8:34	G	Open System	26%	Off

Figura 183. **Información del usuario**

Para poder ingresar al AP, desde fuera de la red privada, se le debe configurar la ruta. Del menú principal, clic sobre *IP* y luego de la lista que se despliega clic sobre *Firewall*. En la pestaña *NAT* se agrega la siguiente regla, figura 184 y 185, clic en (**+**):

Pestaña *General*:

Chain: dstnat

Dst. Address: 172.xx.xx.xx

Protocol: tcp

Dst. Port: 8xxx

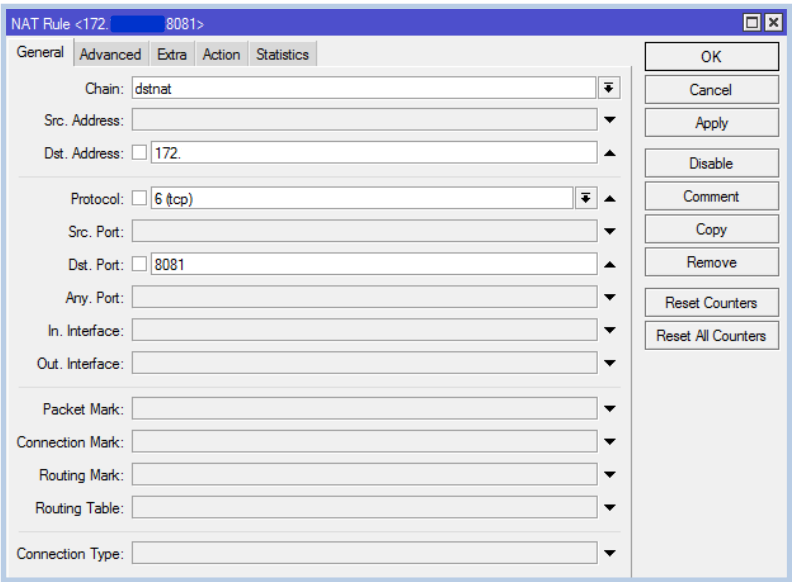


Figura 184. Pestaña General de NAT

Pestaña *Action*:

Action: dst-nat

To Addresses: 192.xx.xx.xx

To Ports: 80

Clic Apply

Clic OK

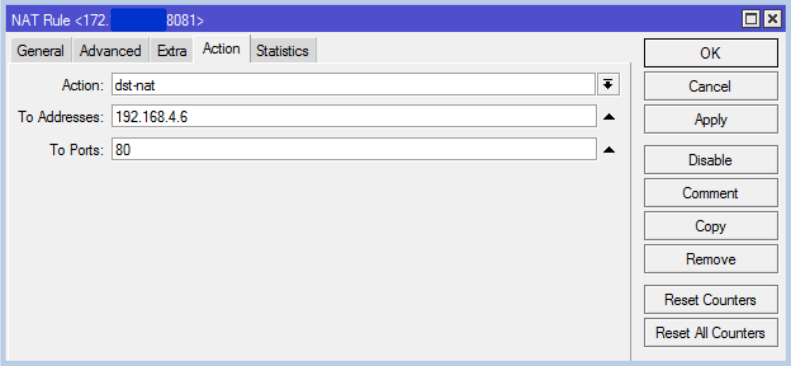


Figura 185. Pestaña Action de NAT

Para ingresar al AP desde fuera de la red privada, se ingresa con 172.xx.xx.xx:8081 y luego con el usuario y contraseña establecidos en el AP por el administrador.

g. DISCUSIÓN

g.1 Aspectos Metodológicos relacionados con el entorno de medición del consumo del ancho de banda

Para el desarrollo del presente trabajo **investigativo** se aplicó el método cualitativo, método en el cual utilizamos los siguientes elementos de observación:

- **Estudio exploratorio bibliográfico sobre el manual de referencia de Mikrotik**, elemento en el cual se buscó información en el manual de referencia, se tuvo en cuenta las normativas y capacidad del equipo en cuanto a memoria y procesamiento.
- **Estudio descriptivo de la Universidad Nacional de Loja. Unidad de análisis del entorno organizacional de la UNL:**

  Variables:

  - Todas las áreas que componen la Universidad.
  - Número Total de Usuarios.
  - Seguridad.
  - Topología.
  - Cantidad de Ancho de Banda.
  - Consumo de Ancho de Banda.

g.2 Mikrotik como una herramienta de control de ancho de banda

Controlar el ancho de banda según las ocupaciones de cada individuo, es algo que se puede hacer gracias a distintas herramientas. Lo lógico es utilizar aquella herramienta que se acople a nuestra necesidad. Se puede lograr controlando la calidad de servicio, ya que esta se puede configurar en base a las necesidades. Se puede lograr mediante la aplicación de reglas de firewall que den más o menos ancho de banda, por ejemplo, según en función de horarios pico. Sin duda alguna, el mejor método es el de conocer las necesidades exactas de los usuarios y dosificar el ancho de banda basándonos en su forma de navegación.

Dentro de los equipos para gestionar de una manera más eficiente el ancho de banda de cualquier institución o empresa, en el mercado se encuentran distintas marcas de equipos segmentadores, estas disponen de equipo ya sea robustos o sencillos dependiendo del número de conexiones que se vaya a tener en la red. En el mercado se encuentran marcas reconocidas como: CISCO, Cyberoam (Anexo 3), Blue Coat PacketShaper (Anexo 2), Ascenflow (Anexo 4), Mikrotik (Anexo 1). Todos con una característica en especial que es la de administrar el ancho de banda de una manera más eficiente; presentan la idea de que no es necesario adquirir cada vez más ancho de banda para mejorar el rendimiento de la red, sino de gestionarlo de mejor manera. La diferencia entre cada uno de estos equipos radica en el énfasis que le ponen al control de aplicaciones P2P, a la categorización de los elementos a administrar, a la prioridad y rigurosidad al momento de asignar ancho de banda.

Entre los equipos analizados se establecieron parámetros técnicos y operativos que permitirían la implementación. Se consideró el número de usuarios que se van a conectar, que no son más de 100 hosts, estudios relacionados con segmentación del ancho de banda a nivel del país por parte de tesistas de otras universidades, equipos más utilizados y reconocidos en el país, equipo sin el riesgo de demorar en su adquisición, y para llevar a cabo una demostración pequeña de lo que se pretende realizar a grosso modo con la segmentación del ancho de banda de la universidad, un equipo pequeño y de características económicas accesibles (sin descuidar los elementos principales de QoS), conduce a la elección de la marca Mikrotik; además como punto importante, en la ciudad de Loja se logra encontrar certificaciones en relación a esta tecnología; y, es mucho más accesible y fácil su compra.

Mikrotik es una tecnología nueva, y por ese mismo hecho ellos tienen precios más asequibles, en la actualidad se encuentran compitiendo con las más grandes marcas, innovando, sin descuidar sus características esenciales para el fin que persigue esta tecnología y estar a la par de sus potenciales competidores. Para la implementación en una biblioteca (una red pequeña) el sistema de RouterOS cumple con todas las características y

requerimientos para su funcionamiento. Y en el caso específico de la tesis pude hacer la configuración y pruebas de implementación sin ningún inconveniente.

g.3 Implementación del equipo Mikrotik para la biblioteca del área de Energía.

Los pasos y procedimientos para la implementación del Mikrotik fueron:

- Instalación Mikrotik
- Acceso al Mikrotik
- Configuraciones para salida a Internet
- Configuración servidor DHCP
- Declaración de reglas
- Control de ancho de banda en base a QoS

Para la recolección de la información relacionada a las actividades, problemas, causas y posibles alternativas de solución referentes a los elementos de observación se hizo uso del método deductivo. Se trabajó siempre con la consulta frecuente a un experto en configuración de equipos Mikrotik.

En la fase preliminar a la implementación del equipo se realizaron las siguientes actividades:

Inspección del lugar donde se iba a implementar el equipo, reconocimiento de los equipos que se encuentran en el armario ubicado en la biblioteca y la interconexión entre ellos, así como también un conteo de los puntos disponibles en la biblioteca. Una vez que se recopiló la información con la aplicación de los instrumentos seleccionados se procedió a la configuración e implementación del equipo.

Materiales que aportaron significativamente a la tesis:

- CACTI (software)
- Nagios (software)
- SARG (software)
- Router Mikrotik (hardware)
- Manuales Mikrotik.

h. CONCLUSIONES

- Luego del análisis realizado a la red de datos de la UNL, para disponer adecuadamente de los recursos que proporciona Internet, en términos de calidad de servicio, la Universidad necesita un equipo segmentador.

- Dentro del campus universitario existe un control de navegación web, sin embargo, por ser esta una institución educativa de tercer nivel, no es conveniente limitar por completo los servicios, sino que también se requiere la implementación de nuevas políticas para navegación web, que soporten el acceso a aplicaciones requeridas, siempre y cuando éstas no interfieran con el desarrollo de la misma Universidad.

- La falta de tener administrado el servicio de Internet, se convierte en un inconveniente, no sólo para los usuarios sino para el mismo administrador de la red de datos, ya que el no contar con un equipo que cumpla con las características necesarias, el ancho de banda por el que se está pagando, está siendo mal utilizado.

- Para el caso de la implementación, los usuarios en el AEIRNNR y su reporte de navegación web, son una pequeña muestra del campus universitario, que refleja, tal como se muestra en las figura 53, tabla 17, y las figuras 55 y 56 respectivamente, un reporte sin calidad de servicio.

- Una vez implementado el equipo segmentador en la biblioteca del área de energía, y luego de las configuraciones en términos de calidad y servicio, se comprobó la segmentación de las páginas y servicios propuestos en la tabla 17, tal como se muestra en las figuras 174 y 175 respectivamente.

- No fue la mejor distribución de ancho de banda que se obtuvo para las distintas áreas, ya que no se contaba con la cantidad necesaria de datos monitoreados por el CACTI, datos necesarios para el algoritmo utilizado para la predicción, debido a que se había dejado de monitorear la red por algún tiempo. Pero aun así, con los

datos disponibles, se logró cumplir con un cálculo muy aproximado a la realidad para poder justificar el porqué de cada ancho de banda por área.

i. RECOMENDACIONES

- En virtud a las pruebas y experiencias que se tuvo a lo largo del desarrollo del presente proyecto de tesis con respecto a la implementación del equipo segmentador en la biblioteca del área de energía, la Universidad Nacional de Loja necesita un equipo que cumpla satisfactoriamente con el trabajo de segmentar su ancho de banda. El p**roblema es que existen** pocos medios para monitorear, controlar y maximizar el rendimiento de las redes. Se recomienda implementar un sistema de gestión de tráfico de aplicaciones que proporcione visibilidad, control, gestión de la red y que garantice un rendimiento efectivo. En la búsqueda del equipo ideal a sugerir para que se implemente en la red de datos de la UNL, se considera pertinente la compra del equipo PacketShaper (Anexo 2).

- No se necesitan grandes cantidades de Ancho de Banda para demostrar que la herramienta Internet es eficiente, sino más bien para tenerla administrada de acuerdo a las necesidades de los usuarios, sin descuidar las políticas institucionales.

- Se recomienda al departamento de redes y telecomunicaciones, tener monitoreados todos los meses del año a la red, debido a que es muy importante contar con un respaldo de datos acerca del consumo de ancho de banda, así de esta manera, se tienen datos precisos para futuros cálculos o estadísticas que se requieran del servicio de Internet.

- Se recomienda tener bien configuradas las medidas de seguridad en términos de acceso a este equipo tan importante como lo es el segmentador, ya que como cualquier equipo en redes, está sujeto a posibles infiltraciones desde el mismo campus universitario.

- Se recomienda establecer las prioridades con las que va a contar cada categoría a segmentar en el equipo Mikrotik, ya que para ofrecer una óptima QoS es la

limitación por prioridad. Una vez establecidos los rangos de ancho de banda para cada regla, se debe establecer la prioridad es lo más importante en términos de QoS.

j. BIBLIOGRAFÍA

TESIS:

[1] **SARANGO, Washington.** "*IMPLEMENTACIÓN DE ENLACES BACKHAUL PARA BACK BONE DE UN WISP MEDIANTE EL USO DEL SISTEMA OPERATIVO ROUTEROS*". [Tesis] Tecnología en Electrónica y Telecomunicaciones. Escuela Politécnica Nacional. Año 2011. Quito, Ecuador. 144p. Disponible en repositorio digital: <http://bibdigital.epn.edu.ec/handle/15000/3956>. [En línea].

[2] **DONATE PRIETO, Francisco.** "*TRANSMISIÓN DE IMÁGENES DE VIDEO MEDIANTE SERVICIOS WEB XML SOBRE J2ME"*. [Tesis] Ingeniería de Telecomunicaciones. Universidad de Sevilla-Escuela Superior de Ingenieros. Año 2007. Sevilla, España. 318p. Disponible en repositorio digital: < http://bibing.us.es/proyectos/abreproy/11372/fichero/Memoria%252FMemoria+completa.pdf>. [En línea].

[3] **MORALES HERNÁNDEZ, Sergio Paulo.** *"ADMINISTRACIÓN DEL ANCHO DE BANDA EN UNA WLAN"*. [Tesis] Licenciatura. Ingeniería en Sistemas Computacionales. Departamento de Computación, Electrónica, Física e Innovación. Universidad de la Américas de Puebla. Año 2006. San Andrés Cholula, Puebla, México. 190p. Disponible en repositorio digital: < http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/morales_h_sp/indice.html>. [En línea]

[4] **DI RIENZO, Víctor. PICA, Gustavo. ROCHE, Emilio**. *"IMPLEMENTACION DE UNA RED PARA LA EMPRESA ROYAL TECH"*. [Tesis] Ingeniería en Telecomunicaciones. Universidad Blas Pascal. Año 2008. Córdoba, Argentina. 197p. Disponible en repositorio digital: <http://es.scribd.com/doc/16020012/Mikrotik-Tutorial>. [En línea].

[5] **LLERENA, Christian.** *"SISTEMAS ADMINISTRADORES DE ANCHO DE BANDA DE ENLACES WAN E INTERNET"*. [Tesis] Ingeniería Electrónica especialidad Telecomunicaciones. Escuela Politécnica del Ejército. Año 2005. Quito, Ecuador. 234p. Disponible en repositorio digital: <http://repositorio.espe.edu.ec/bitstream/21000/845/1/T-ESPE-020945.PDF>. [En línea].

RECURSOS ELECTRÓNICOS:

[6] **CISCO. Networking Academy.** "*Ethernet*". Disponible en: < http://blog.utp.edu.co/ee973/files/2012/04/capitulo09-ethernet.pdf>. Cap. 9. [En línea]. Consulta: Agosto del 2012.

[7] **BLUE COAT, Packet Guide**. *"PacketShaper 10000 Product Specifications"*. Disponible en: <https://bto.bluecoat.com/packetguide/9.1/products/specifications-10000.htm>. [En línea]. Consulta: Marzo del 2013.

[8] **Joomla.** *"Cortafuegos con IP Tables"*. Disponible en: <http://dns.bdat.net/blog/index.php/prueba/22-redes/cortafuegos/299-cortafuegos-con-iptables?showall=&start=6>. [En línea]. Consulta: Diciembre del 2012.

[9] **CISNEROS, Hugo.** *"SARG Generando Reportes de Squid"*. Disponible en: < http://ferrolmoda.com/ficheros/final/sarg/sarg-0.1-es-ES.pdf>. [En línea]. Consulta: Septiembre del 2012.

[10] **CABRERA, Juan Pablo**. *"Desarrollador del Algoritmo de Predicción en Sofware MATLab"*. Ingeniero en Electrónica y Telecomunicaciones, Docente Investigador en la Universidad Nacional de Loja. **Correo electrónico:** jpcabrera2@hotmail.com

[11] **Mikrotik RouterOS.** *"Workshop QoS Best Practice"*. Dallas/Fort worth MUM USA 2009. Disponible en: <http://mum.mikrotik.com/presentations/US09/megis_qos.pdf>. [En línea]. Consulta: Noviembre del 2012.

[12] **GNU General Public License**. *"L7-filter Supported Protocols"* [Última actualización 7 de Enero del 2009]. Disponible en: <http://nl7-filter.sourceforge.net/protocols>. [En línea]. Consulta: Febrero del 2013.

[13] **DENZER, Patricio. LÓPEZ, Waldo. GONZÁLEZ, Agustín.** "*Administración de Ancho de Banda Mediante un Router CISCO 3600*". Departamento de Electrónica. Universidad Técnica Federico Santa María. Disponible en: <http://profesores.elo.utfsm.cl/~agv/publications/2006/senacitel/DenzerLopezGonzalezSubmitted.pdf>. [En línea]. Consulta: Septiembre del 2012.

[14] **LÓPEZ, Pablo.** *"Ancho de Banda Digital versus el Analógico"*. Disponible en: < http://programoweb.com/214/ancho-de-banda-digital-versus-el-analogico/>. [En línea]. Consulta: Octubre del 2012.

[15] **Ministerio de Educación, Cultura y Deporte.** *"DansGuardian: filtro de contenidos"*. Gobierno de España. Disponible en: <http://recursostic.educacion.es/observatorio/web/es/software/software-general/524-dansguardian-filtro-de-contenidos>. [En línea]. [Última actualización 20 de Noviembre del 2007]. Consulta: Agosto del 2012.

[16] **ROUTERBOARD.** *"RB750"*. Disponible en: <http://routerboard.com/RB750>. [En línea]. Consulta: Diciembre del 2012.

[17] **MANUAL MIKROTIK**. *"Mikrotik, Manual Wiki"*. Official **MikroTik documentation**. [Última actualización 13 de Marzo del 2013]. Disponible en: <http://wiki.amikrotik.com/wiki/Category:Manual#list>. [En línea]. Consulta: Octubre del 2012.

[18] **BARÓN, F.J; MONTIEL TÉLLEZ, F.** *"Capítulo 2: Intervalos de Confianza"*. Disponible en: < http://www.bioestadistica.uma.es/baron/apuntes/ficheros/cap02.pdf>. [En línea]. Consulta: Febrero del 2013.

[19] **FOROS**. **"***QoS estático (Queue Tree + Mangle) para* Mikrotik". Disponible en: <http://www.bloodzone.net/forums/f21/qos-est%E1tico-queue-tree-mangle-para-mikrotik-97086/>. [En línea]. [Última actualización 2 de Septiembre del 2011, 15:36 PM]. Consulta: Noviembre del 2012.

[20] **CYBEROAM.** "Unified Threat Management". Tech Sheet. Disponible en: <http://www.cyberoam.com/downloads/Techsheet/CyberoamTechSheet.pdf >. [En línea]. Consulta: Febrero del 2013.

[21] **CYBEROAM.** *"Gestión de ancho de banda".* Disponible en: <http://www.cyberoam.com/es/bandwidthmanagement.html>. [En línea]. Consulta: Marzo del 2013.

[22] **BARRON, Daniel.** *"DansGuardian".* Disponible en: <http://www.ecured.cu/index.php/DansGuardian>. [En línea]. Consulta: Agosto del 2012.

[23] **XTRA**. "*Optimizando las Redes para hacer más eficientes las activad de las Organizaciones.* Año 2008. Disponible en: <http://www.idris.com.ar/pdf/AscenFlow.pdf>. [En línea]. Consulta: Enero del 2013.

[24] **Definición.** *"Concepto de ancho de banda"* Disponible en: <http://www.masadelante.com/faqs/ancho-de-banda>. [En línea]. Consulta: Octubre del 2012.

[25] **OoCities.org.** *"El modelo OSI"*. Disponible en: <http://www.oocities.org/dralkzta/osi.htm>. [En línea]. Consulta: Agosto del 2012.

[26] **RYOHNOSUKE.** *"Configurar Mikrotik RB750, RB750G, RB450G, RB433, RB433AH, PC x86, etc"*. Disponible en: <http://www.ryohnosuke.com/foros/showthread.php?t=363>. [En línea]. [Última actualización 4 de Abril del 2011, 12:10 AM]. Consulta: Octubre del 2012.

[27] **SHAPER Works.** "Blue Coat PacketShaper 10000". Disponible en: <http://www.shaperworks.com/PacketShaper-10000.asp>. [En línea]. Consulta: Marzo del 2013.

[28] **HINOJOSA, Rod.** *"Calidad de Servicio, Quality of Service"*. Año 2005. Disponible en: < http://www.slideshare.net/RodHinojosa/calidad-de-servicio-qoshttp://profesores.elo.utfsm.cl/~agv/publications/2006/senacitel/DenzerLopezGonzalezSubmitted.pdf>. [En línea]. Consulta: Enero del 2013.

k. ANEXOS

ANEXO 1. MIKROTIK Routerboard RB750-2HnD 5xPORT [16]

Tabla 40. Características MIKROTIK RouterBoard RB750

Product code	RB751G-2HnD
Current Monitor	No
TX power	30dBm
CPU	Atheros AR7241
Antenna gain	2x2 MIMO PIF antennas, max gain 2.5dBi; external MMCX option
CPU speed	400MHz
Max Power consumption	13W
RAM	64MB
LAN ports	5
Gigabit	Yes
MiniPCI	0
Wireless standards	802.11b/g/n
USB	1
Power Jack	8-30V DC
PoE	8-30V DC on Ether1
Voltage Monitor	No
PCB temperature monitor	No
CPU temperature monitor	No
Dimensions	113x138x29mm
Operating System	RouterOS
Temperature range	-20C...+50C
RouterOS License	L4

ROUTERBOARD. *"RB750"*. Disponible en: <<http://routerboard.com/RB750 >>. [En línea].

Tabla 41. Performance test results

RB750		100M port test (400Mhz)		RouterOS v6.0rc6			
Mode	Configuration	64 byte		512 byte		1518 byte	
		kpps	Mbps	kpps	Mbps	kpps	Mbps
Bridging	none (fast path)	194.0	127.3	*117.0*	*496.1*	*40.3*	*495.2*
Bridging	25 Bridge filter rules	53.7	35.2	52.3	221.9	*40.3*	*495.2*
Routing	none (fast path)	183.7	120.5	*117.0*	*496.1*	*40.3*	*495.2*
Routing	25 Simple Queues	92.8	60.8	88.5	375.1	*40.3*	*495.2*
Routing	25 IP filter rules	37.5	24.6	38.4	162.6	37.6	462.4

ROUTERBOARD. *"RB750"*. Disponible en: <<http://routerboard.com/RB750 >>**.** [En línea].

ANEXO 2. PACKETSHAPER [7]

Packeteer PacketShaper, posee varios modelos de sistemas, la elección del modelo tiene ver con la capacidad del enlace de Red Área Amplia (WAN). Cabe mencionar que la popularidad del equipo en empresas ecuatorianas como: Transelectric S.A en Guayaquil, ETAPA en Cuenca, comparaciones realizadas al equipo con pares segmentadores, el PacketShaper de Blue Coat se lleva la mejor parte.

Analizando criterios de calidad de servicio y esencialmente los cuatro puntos de comparación más importantes como son monitoreo, reporte, clasificación y control se observa cualidades superiores para brindar calidad de servicio en los sistemas administradores de ancho de banda dedicados con respecto a los elementos de red Cisco tomados como referencia para dicha comparación.

PacketShaper:

Su ubicación básica en la red es entre el ruteador de la red de área amplia y el switch o hub de la Red de Área Local (LAN). Los modelos 1500 y 2500 que administran hasta 10 Mbps son utilizados a nivel de una organización, los modelos 4500, 6500, 8500, 9500 y 10000 que administran hasta 1 Gbps son utilizados a nivel de Proveedores de Servicio de Internet (ISP).

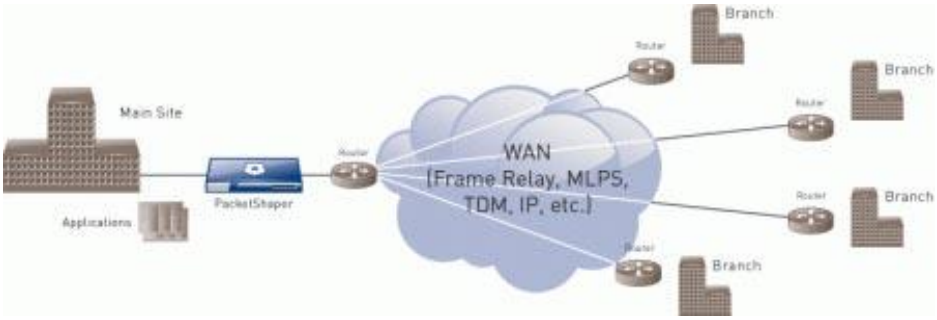


Figura 186. Ubicación básica del PacketShaper

BLUE COAT, Packet Guide. *"PacketShaper 10000 Product Specifications"*. Disponible en: <https://bto.bluecoat.com/packetguide/9.1/products/specifications-10000.htm>. [En línea].

PacketShaper es montable en un rack de 19 pulgadas, posee un puerto ethernet del enlace entrante (Inbound) y un puerto ethernet del enlace saliente (Outbound), en algunos modelos se puede instalar módulos de expansión de puertos que permiten al PacketShaper adaptarse a topologías que incorporan múltiples redes de área local, posee un puerto serial para configuración por consola.

Figura 187. **PacketShaper 10000**

BLUE COAT, Packet Guide. *"PacketShaper 10000 Product Specifications"*. Disponible en: <https://bto.bluecoat.com/packetguide/9.1/products/specifications-10000.htm>. [En línea].

PacketShaper permite una clasificación basada en dirección de destino, localización del servidor, tipo de Extensiones de Correo de Internet Multipropósito (MIME) como por ejemplo extensiones XML, MPEG, etc.; Localizador de Recurso Uniforme (URL), y otros criterios que ayudan a distinguir entre navegación casual, aplicaciones de negocios, actividades en línea de consumidores entre otras aplicaciones.

Monitoreo y Clasificación:

El monitoreo y clasificación son hechas por PacketSeeker, tiene la habilidad para diferenciar cientos de tipos diferentes de tráfico, PacketShaper puede diferenciar tráfico basado básicamente en:

• Aplicación o en capa 7, aplicaciones par a par (P2P) como KaZaA.
• Protocolo, número de puerto.
• Localizador de Recurso Uniforme (URL).
• Nombre de computador, lista de computadores.

• Servicios diferenciados, Tipo de servicio (ToS), Clase de Servicio (CoS).

• Conmutación de Etiquetas MultiProtocolo (MPLS)

• Tipo de servicio (ToS), Clase de Servicio (CoS).Dirección de Control de Acceso al Medio (MAC).

•Dirección IP fuente/destino, subred.

• Rango de velocidad de computador.

• Tipo de Extensiones de Correo de Internet Multipropósito (MIME).

• Bases de datos.

• Redes de Área Local Virtuales (VLAN) basadas en el estándar 802.1q y otras.

PacketSeeker aparece dentro de paquetes y encabezados observando marcas características o aplicaciones específicas, puede distinguir aplicaciones múltiples usando el mismo puerto TCP, descubre tráfico para bases de datos específicos y reconoce otro tráfico que se muestra ilusorio para ruteadores y soluciones similares, cada categoría de tráfico es llamada una clase de tráfico.

Figura 188. Detección por categorías en PacketShaper

BLUE COAT, Packet Guide. *"PacketShaper 10000 Product Specifications"*. Disponible en: <https://bto.bluecoat.com/packetguide/9.1/products/specifications-10000.htm>. [En línea].

Packeteer PacketShaper 10000 [27]

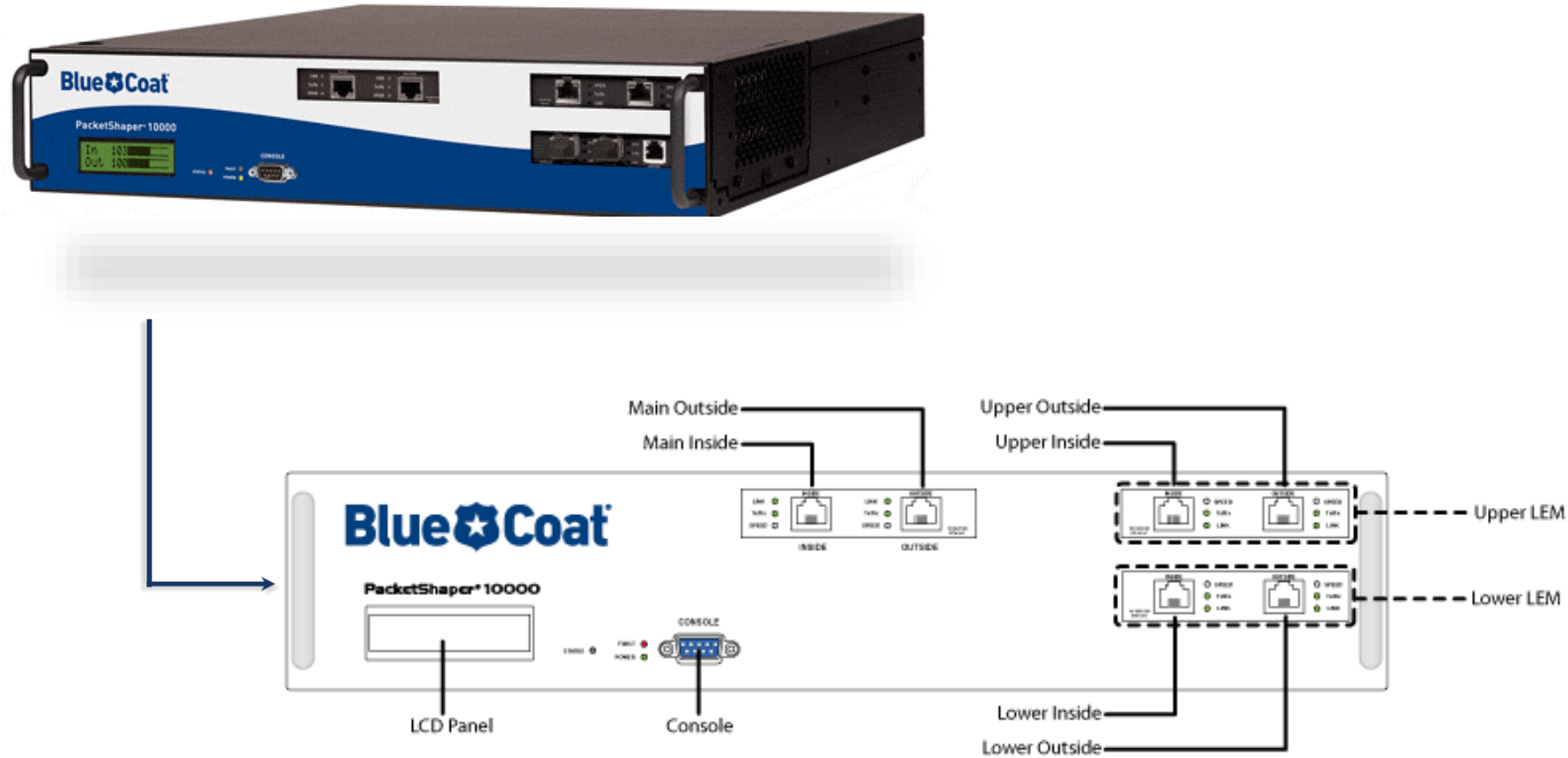


Figura 189. Packeteer PacketShaper 10000

SHAPER Works. "Blue Coat PacketShaper 10000". Disponible en: <http://www.shaperworks.com/PacketShaper-10000.asp>. [En línea].

Tech Sheet PacketShaper y la comparación con otros modelos:

A partir de 2 Mbps a 1 Gbps de rendimiento, hay un PacketShaper para satisfacer sus requisitos de implementación específicos en cualquier ubicación en el centro de datos hasta el borde de la red.

Tabla 42. Especificaciones y comparación con otros modelos

Models:	900	1700	3500	7500	10000	10000 ISP***
Maximum Capacity:						
IP Flows (TCP/Other IP)*	5,000/2,500	30,000/15,000	40,000/20,000	200,000/100,000	300,000/150,000	900,000/360,000
Classes	256	512	1,024	1,024	2,048	5,000
Dynamic Partitions	**	1,024	1,024	10,000	20,000	20,000
Static Partitions	128	256	512	512	1,024	5,000
Shaping Policies	256	512	1,024	1,024	2,048	5,000
Max # of Matching Rules	640	2,562	2,562	5,120	5,000	12,500
IP Hosts*	5,000	15,000	20,000	150,000	200,000	400,000
Active Tunnels	10	15	30	100	1,000	N/A
Software Options & Upgrades:						
Monitoring Only	Yes	Yes	Yes	Yes	Yes	Yes
Link Speeds with Shaping Options	512 Kbps 2 Mbps - -	2 Mbps 6 Mbps 10 Mbps -	2 Mbps 6 Mbps 10 Mbps 45 Mbps	10 Mbps 45 Mbps 100 Mbps 200 Mbps	100 Mbps 200 Mbps 310 Mbps 1 Gbps	100 Mbps 200 Mbps 310 Mbps 1 Gbps
Compression**	2 Mbps	10 Mbps	20 Mbps	45 Mbps	155 Mbps	N/A
Interfaces:						
Network Interface (in and out)	Copper: 10/100 Mbps	Copper: 10/100/1000 Mbps	Copper: 10/100/1000 Mbps	Copper: 10/100/1000 Mbps	Copper: 10/100/1000 Mbps Fiber: 1000 Mbps	Copper: 10/100/1000 Mbps Fiber: 1000 Mbps
LAN Expansion Modules (max 2)	Backup fail-to-wire pair built in	N/A	Copper: 10/100/1000 Mbps	Copper: 10/100/1000 Mbps Fiber SFP	Copper: 10/100/1000 Mbps Fiber SFP	Copper: 10/100/1000 Mbps Fiber SFP

			Fiber SFP			
Interface Pairs	2	1	1+LEM option	1+LEM option	1+LEM option	1+LEM option
Out-of-Band Management Port	Through backup ports	Yes	Yes	Yes	with LEM	with LEM
Console Port	All have RS-232 (AT-compatible) with male DB-9 connectors					
Dimensions: (All are 19 in. rack mountable)						
Height	1U (1.75 in)(4.45 cm)	1U (1.75 in) (4.45 cm)	2U (3.5 in) (8.89 cm)	2U (3.5 in) (8.89 cm)	2U (3.5 in) (8.89 cm)	2U (3.5 in) (8.89 cm)
Width	8.66 in (22.00 cm)	17 in (43.18 cm)	17.35 in (44.07 cm)	17.35 in (44.07 cm)	17.31 in (43.97 cm)	17.31 in (43.97 cm)
Depth	9.68 in (24.60 cm)	14 in (35.56 cm)	16 in (40.64 cm)	16 in (40.64 cm)	20.25 in (51.43 cm)	20.25 in (51.43 cm)
Weight	4.50 lbs (2.05 kg)	14 lb (6.35 kg)	18.04 lb (8.18 kg)	20.48 lb (9.29 kg)	33 lb (14.97 kg)	n/a
Power:						
Power Supply	100/240 VAC; 50/60 Hz, 2A	100/240 VAC; 50/60 Hz, 2.5 A	100/240 VAC; 50/60 Hz, 2.5 A	100/240 VAC; 50/60 Hz, 2.5 A	100/240 VAC; 50/60 Hz, 6 A	100/240 VAC; 50/60 Hz, 6 A
Dual, Redundant Load Sharing	No	No	No	Yes; Hot-swappable	Yes; Hot-swappable	Yes; Hot-swappable
Additional Features:						
Interoperability	XML, XML and CGI APIs, SNMP MIB, SNMP event traps, HP OpenView, infoVista, CA eHealth, Aprisma Spectrum, Micromuse Netcool					
Device Management	Console access, Web browser interface, Telnet CLI, SNMP Blue Coat MIB and MIB-II support					
Agency Approval:						
Safety	IEC 60950-1; EN 60950-1+ A11, CAN/CSA-C22 2 No, 60950-1:03; UL 60950-1:03; EN 60825-1,-2 Class 1 Laser					
EMC/EMI	AS/NZS 3548 Class A; AS/NZS 4252.1; ICES-003 Class A; EMC Direct B9/336/EEC; EN 300 386 v1.3.1: 2001 Telecom EMC standard; EMC Directive 73/23/EEC; EMC Directive 93/6B/EEC; EN 55022: 1998 Class A; EN 61000-3-2: 1995_A1(98) + A2(98), & prA1 4(00); EN 61000-3-3:1:1995; EN 55024:1998; VCCI:2002 Class A; KN55022 Class A; KN6100-4-2,3,4,5,6,8,11; GOST-R 60950-2002; GOST-R 5131B.22,.24-99; FCC 47 CFR part 15, subpart B Class A; CNS 13438 Class A					

SHAPER Works. "Blue Coat PacketShaper 10000". Disponible en: <http://www.shaperworks.com/PacketShaper-10000.asp>. [En Línea]

Nota: No todas las especificaciones de capacidad se puede maximizar al mismo tiempo

*** PacketShaper puede soportar más servidores host y flujos**, estas cifras representan máximos ideales para producir resultados óptimos, los números se redondean hacia arriba o hacia abajo al millar más cercano. Estos máximos representan flujos simultáneos. El rendimiento puede variar en función del número de nuevos flujos, el tipo de tráfico, mezcla de tráfico y otras condiciones propias de cada despliegue.

**** Se refiere a los tipos de tráfico post-comprimido** - máximo rendimiento especificaciones comprimidos para PacketShaper son más bajos cuando se habilita la compresión debido a la potencia de procesamiento adicional que se requiere para comprimir el tráfico.

***** PacketShaper 10000 tiene una opción de configuración para cargas ISP**. Anteriormente, las ediciones ISP le había ofrecido como un producto independiente con el único SKU. Ahora, la carga ISP, que añade capacidad de clase, está disponible como una opción de configuración. Nota: La carga ISP aumentar la capacidad de las clases y de los flujos, pero no proporciona ciertas funciones como la compresión y las estadísticas de tiempo de respuesta, entre otros.

ANEXO 3. CYBEROAM [21]

Ofrece controles basados en identidad de Capa 8 que evitan la congestión y el mal uso del ancho de banda además de optimizar el ancho de banda y rentabilizar mejor de la inversión. La solución prioriza las aplicaciones críticas para el negocio y los usuarios con controles pormenorizados de Capa 7 y Capa 8, permitiendo implementaciones de nube y software como servicio (SaaS) al tiempo que reduce el gasto de capital que conlleva la compra de ancho de banda.

Tabla 43. Características CYBEROAM

Característica	Descripción de la característica	Ventajas
Asignación de ancho de banda de Capa 7 y Capa 8	- Prioriza las aplicaciones críticas para el negocio y los usuarios para la asignación de ancho de banda - Priorización basada en el origen, destino, usuario, servicio o grupo de servicio	- Calidad de servicio asegurada para aplicaciones críticas para el negocio como VoIP o CRM. - Admite requisitos de ancho de banda para aplicaciones SaaS y de nube - Previene la congestión y el mal uso del ancho de banda
Asignación basada en categorías web	- Asignación de ancho de banda basada en categorías de los sitios web: correo web, medios sociales, juegos, ocio, etc. - Límites de carga y descarga - Normativas basadas en identidad de Capa 8 con asignación basada en categorías	- Mejora de la productividad con filtrado web
Asignación basada en	- Ancho de banda programado según la hora del día	- Equilibra valles y crestas en el consumo de ancho de banda.

tiempo	- Ancho de banda concertado para aplicaciones críticas para el negocio durante la programación de horarios	- Calidad de servicio asegurada para aplicaciones críticas para el negocio
Ancho de banda concertado y cuantificable	- Ancho de banda reservado a usuarios críticos en todo momento. - Normativas para asignar automáticamente ancho de banda desocupado a otras aplicaciones	- Uso óptimo del ancho de banda desocupado. - Limita el gasto de capital al evitar la compra de exceso de ancho de banda - La inversión sale rentable
Registros e informes	- Informes de ancho de banda de vínculos WAN múltiples. - Opciones de informes sobre dispositivos e informes centralizados con CCC y Cyberoam iView	- Permite un uso óptimo del ancho de banda y visibilidad del consumo. - Identifica ataques de red por medio de patrones de consumo excesivo de ancho de banda. - Contribuye a cumplir normativas

CYBEROAM. *"Gestión de ancho de banda"*. Disponible en: <http://www.cyberoam.com/es/bandwidthmanagement.html>. [En línea].

Figura 190. Equipos CYEBEROAM

CYBEROAM. *"Gestión de ancho de banda"*. Disponible en: <http://www.cyberoam.com/es/bandwidthmanagement.html>. [En línea].

Aspectos más destacados:

Visibilidad en tiempo real del uso del ancho de banda según usuarios-aplicaciones-protocolos: el módulo Descubrimiento de tráfico de Cyberoam ofrece visibilidad en tiempo real de redes, aplicaciones y usuarios a través de Capas 2 con la Capa 8 humana, identificando usuarios y aplicaciones que utilizan un exceso de ancho de banda. Proporciona alertas en tiempo real sobre uso no productivo e incidencias de amenazas, lo cual permite una rápida respuesta por parte de las organizaciones ante equipos en peligro.

Controla aplicaciones y utilización de ancho de banda en sitios web: Cyberoam permite límites de ancho de banda individual o basada en categorías para aplicaciones y sitios web, lo cual mejora la seguridad y la productividad. P. ej., ancho de banda concertado para VoIP; cuota baja para sitios web con vídeos, música e imágenes que no estén relacionados con el negocio; 64 kbps para la mensajería instantánea con el fin de limitar la transferencia de archivos; ancho de banda nulo para P2P. Cyberoam permite a las

organizaciones limitar el acceso a aplicaciones específicas a determinadas horas del día con límite de duración. Ej.: YouTube y Gmail entre las 5 y las 6 de la tarde.

Controla la utilización de ancho de banda basado en identidad de Capa 8: Cyberoam permite a las organizaciones asignar cuotas de ancho de banda e imponer topes de velocidad de carga y descarga en función de la identidad del usuario. Puede asignarse el ancho de banda concertado y cuantificable. Ej.: ancho de banda reservado al director general, acceso a YouTube para el equipo de marketing después del horario laboral, acceso a Gmail solamente cuando hay disponible ancho de banda de sobra.

TECH SHEET CYBEROAM [20]

Tabla 44. Principales Características de CYBEROAM

Specifications	15i	15wi	25ia	25wi	35ia	35wi	50ia	100ia
Interfaces								
10/100 Ethernet Ports	3	3	-	-	-	-	-	-
Copper GbE Ports	-	-	4	4	4	4	6	6
Configurable Internal/DMZ/WAN	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Console Ports (RJ45/DB9)	1	1	1	1	1	1	1	1
SFP (Mini GBIC) Ports	-	-	-	-	-	-	-	-
USB Ports	1	1	1	1	1	1	2	2
Hardware Bypass Segments	-	-	-	-	-	-	1#	1#
Firewall Throughput (UDP) (Mbps)	150	150	450	450	750	750	1,000	1,250
Firewall Throughput (TCP) (Mbps)	90	90	225	225	500	500	750	1,000
New sessions/second	2,000	2,000	3,500	3,500	5,500	5,500	8,000	10,000
Concurrent sessions	30,000	30,000	130,000	130,000	175,000	175,000	220,000	400,000
3DES/AES Throughput (Mbps)	15/25	15/25	30/75	30/75	50/80	50/80	60/90	80/100
WAF Protected Throughput (Mbps)	-	-	-	-	-	-	35	60
Antivirus Throughput (Mbps)	20	20	65	65	125	125	150	200
IPS Throughput (Mbps)	40	40	70	70	150	150	200	300
UTM Throughput (Mbps)	15	15	50	50	90	90	130	160
Authenticated Users/Nodes	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Built-in Wireless LAN (Only for Wi series)								
Wireless Standards	IEEE 802.11 n/b/g (WEP, WPA, WPA2, 802.11i , TKIP, AES, PSK, 802.1x EAP)							
Antenna	Detachable 2x3 MIMO							
Access Points	Up to 8 bssid							
Transmit Power (EIRP)	11n HT40 : +17dBm, 11b CCK: +19dBm, 11g OFDM:+17dBm							
Receiver Sensitivity	-65dBm at 300Mbps, -70dBm at 54Mbps, -86dBm at 11Mbps							
Frequency Range	USA (FCC): 2.412GHz ~ 2.462GHz, Europe (ETSI): 2.412GHz ~ 2.472 GHz, Japan (TELEC): 2.412GHz ~ 2.483GHz							
Number of Selectable Channels	USA (FCC) - 11 channels, EU (ETSI) / Japan (TELEC) - 13 channels							
Data Rate	802.11n: up to 300Mbps, 802.11b: 1, 2, 5,5, 11Mbps, 802.11g: 6, 9, 12, 18, 24, 36, 48, 54Mbps							
Dimensions								
H x W x D (inches)	1.7 x 6 x 9.1	1.7 x 6 x 9.1	1.7 x 6 x 9.1	1.7 x 6 x 9.1	1.7 x 6 x 9.1	1.7 x 6 x 9.1	1.7 x 16.8 x 10.3	1.7 x 16.8 x 10.3
H x W x D (cms)	4.4 x 15.3 x 23.2	4.4 x 15.3 x 23.2	4.4 x 15.3 x 23.2	4.4 x 15.3 x 23.2	4.4 x 15.3 x 23.2	4.4 x 15.3 x 23.2	4.3 x 42.7 x 26.2	4.3 x 42.7 x 26.2
Appliance Weight	1.5 kg, 3.307	1.5 kg, 3.307	2.3 kg, 5.07	2.3 kg, 5.07	2.3 kg, 5.07	2.3 kg, 5.07	5.3 kg, 11.68 lbs	5.3 kg, 11.68 lbs
Power								
Input Voltage	100-240VAC	100-240VAC	100-240VAC	100-240VAC	100-240VAC	100-240VAC	100-240VAC	100-240VAC
Consumption	13.2W	13.2W	33.5W	33.5W	47.8W	47.8W	90W	90W
Total Heat Dissipation	45	45	114	114	163	163	200	200
(BTU) Redundant Power Supply	-	-	-	-	-	-	-	-

Specifications	200i	300i	500ia/1F/10F	500ia-RP	750ia/1F/10F	1000ia/10F	1500ia/10F
Interfaces							
Copper GbE Ports	6	6	10 / 6 / 6	10	14 / 6 / 6	12 / 4	22 / 14
1GbE SFPMini Ports	-	-	- / 4 / -	-	- / 4 / -	4 / 4	4 / 4
10GbE SFPMini Ports	-	-	- / - / 2	-	- / - / 2	- / 2	- / 2
Configurable Internal/DMZ/WAN Ports	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Console Ports (Rj45)	1	1	1	1	1	1	1
USB Ports	2	2	2	2	2	2	2
Hardware Bypass Segments	1#	1#	2#	2#	2#	2#	2#
System Performance*							
Firewall Throughput (UDP) (Mbps)	2,200	2,600	5,000	5,000	9,000	10,000	12,000
Firewall Throughput (TCP) (Mbps)	1,500	1,800	3,000	3,000	6,500	8,000	10,000
New sessions/second	12,000	15,000	25,000	25,000	80,000	85,000	100,000
Concurrent sessions	450,000	500,000	700,000	700,000	1,000,000	1,500,000	2,000,000
3DES/AES Throughput (Mbps)	150/180	180/200	325/400	325/400	500/750	900/1,200	1,200/1,500
WAF Protected Throughput (Mbps)	100	150	300	300	350	425	500
Antivirus Throughput (Mbps)	280	450	750	750	2,000	2,250	2,750
IPS Throughput (Mbps)	750	850	1,000	1,000	1,600	2,500	3,500
UTM Throughput (Mbps)	250	350	550	550	1,350	1,450	1,800
Authenticated Users/Nodes	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited	Unlimited
Dimensions							
H x W x D (inches)	1.7 x 17.3 x 14.6		1.72 x 17.25 x 11.50	1.72 x 17.44 x 15.98		1.77 x 17.25 x 18.30	3.54 x 17.5 x 23.23
H x W x D (cms)	4.3 x 43.9 x 37.1		4.4 x 43.8 x 29.21	4.4 x 44.3 x 40.6		4.5 x 43.8 x 46.5	9 x 44.5 x 59
Appliance Weight	6.5 kg, 14.33 lbs		5.54 kg, 12.21 lbs	6.04 kg, 13.31lbs		13.5 kg, 29.76 lbs	18.5 kg, 40.78 lbs
Power							
Input Voltage	100-240VAC		100-240VAC	100-240VAC	100-240VAC	90-260VAC	90-260VAC
Consumption	62.7W	72.1W	128W	185W	185W	129W	258W
Total Heat Dissipation (BTU)	324		375	475	475	626	881
Redundant Power Supply	-		-/Yes/Yes	Yes	Yes	Yes	Yes

CYBEROAM. "Unified Threat Management". Tech Sheet. Disponible en: <http://www.cyberoam.com/downloads/Techsheet/CyberoamTechSheet.pdf >. [En línea].

Environmental Conditions: Operating Temperature 0 to 40 °C, Storage Temperature - 25 to 75 °C, Relative Humidity (Non condensing) 10 to 90%.

*If Enabled, will bypass traffic only in case of Power failure.

*Antivirus, IPS and UTM performance is measured based on HTTP traffic as per RFC 3511 guidelines.

ANEXO 4. ASCENFLOW [23]

El AscenFlow de Xtera Networks es un administrador inteligente de tráfico WAN que permite asegurar protección a servicios críticos a través de políticas de control de QoS aplicando tecnologías de inspección profunda de paquetes (Deep Packet Inspection: DPI). El sistema provee un tráfico optimizado, como así también una poderosa herramienta de análisis por usuario para los administradores de red.

Figura 191. Equipo ASCENFLOW
XTRA. "*Optimizando las Redes para hacer más eficientes las activad de las Organizaciones.* Año 2008. Disponible en: <http://www.idris.com.ar/pdf/AscenFlow.pdf>. [En línea].

- **El ancho de Banda Garantizado (Bandwidth Guarantee):** Permite que aplicaciones críticas sean priorizadas y que cuenten con un ancho de banda perfectamente asignado. Esto es especialmente útil para servicios tales ERP, VPN, VoIP y Video Conferencia. También se pueden proteger aquellas aplicaciones sensibles a los delays. Por otro lado, se puede limitar el ancho de banda para aquellas aplicaciones no relativas al negocio, tales como P2P, video en línea y juegos, resolviendo de esta manera el mal uso del ancho de banda.
- **Asignación de Ancho de Banda Homogéneo (Even Bandwidth Allocation):** Esta funcionalidad permite asignar políticas de ancho de banda a todas las IP de una red. Esta característica es especialmente útil para ISP´s y WAN´s muy grandes.
- **Auto Descubrimiento (Auto Discovery):** Permite que los administradores realizar configuraciones instantáneas y retener el control de la red cuando suceden anomalías. De esta forma el sistema permite detectar aquellas aplicaciones que están ocupando un ancho de banda inusualmente grande, de tal forma que el administrador puede generar una nueva política inmediatamente.

- **Límite de Conexión (Connection Limit):** Permite limitar el número de conexiones para cada IP. Esta restricción previene que el número excesivo de conexiones pueda afectar a aplicaciones críticas
- **Autenticación (Authentication):** Permite manejar el ancho de banda según cuentas de usuario con sistemas tales como NTLM, LDAP,
- **RADIUS, POP3 y base de datos local**: Esta característica no solo mejora la seguridad sino que permite el control de cuentas y uso de ancho de banda para los cuales se crean nuevas políticas.
- **Cuota (Quota):** El administrador puede manejar el ancho de banda de acuerdo a la transferencia de información. Esto agrega una forma de administrar y asignar ancho de banda de acuerdo a volumen y tiempo y bloquea el acceso cuando esta cuota se excede.

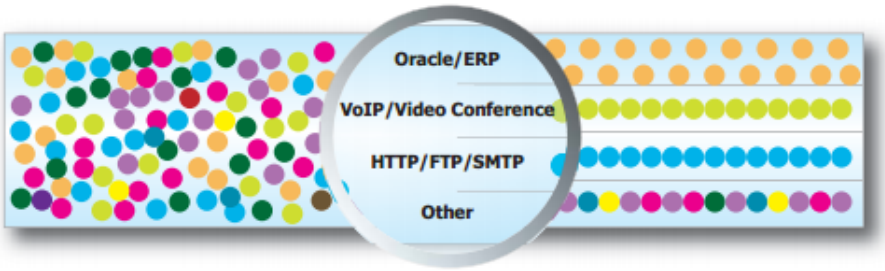


Figura 192. Asignación de Ancho de Banda Homogéneo
XTRA. "*Optimizando las Redes para hacer más eficientes las activad de las Organizaciones.* Año 2008. Disponible en: <http://www.idris.com.ar/pdf/AscenFlow.pdf>. [En línea].

TECH SHEET ASCENFLOW [23]

Tabla 45. Tech Sheet Device AscenFlow

MODELO	M50	M200	M501	M1001	M2500	M5000 C/F	M10000 C/F
Ancho de Banda	10 Mbps	40 Mbps	100 Mbps	200 Mbps	1000 Mbps	1000 Mbps	2000 Mpbs
Número Máximo de Conexiones	50,000	200,000	500,000	1,000,000	1,000,000	2,000,000	3,000,000
Clases	128	512	1024	1024	2048	2048	2048
Interfaz de Red							
10/100 Base-TX	3	3	N	N	1	1	1
10/100/1000 Base - TX	N	N	5	5	6	(C) 4 / (F) 0	(C) 4 / (F) 0
1000 Base SX	N	N	N	N	2	(C) 0 / (F) 4	(C) 0 / (F) 4
Protección							
Bay Pass por Falla (Hardware / Software)	Y	Y	Y	Y	Y	Y	Y
HA (Alta Disponibilidad)	N	N	Y	Y	Y	Y	Y
Instalación							
Transparente	Y	Y	Y	Y	Y	Y	Y
Análisis de Tráfico							
Por Host / Servicio / URL / Clase	Y	Y	Y	Y	Y	Y	Y
Análisis de Latencia	Y	Y	Y	Y	Y	Y	Y
Análisis de Conexión	Y	Y	Y	Y	Y	Y	Y
Asignación de QoS							
Niveles Múltiples de Prioridad (7 Niveles)	Y	Y	Y	Y	Y	Y	Y
Max/Min Ancho de Banda Garantizado	Y	Y	Y	Y	Y	Y	Y
Control de Velocidad de TCP	Y	Y	Y	Y	Y	Y	Y
Soporte de Protocolos de Capa 7	Y	Y	Y	Y	Y	Y	Y
Políticas de Identidad	Y	Y	Y	Y	Y	Y	Y
Por URL	Y	Y	Y	Y	Y	Y	Y
Asignación Uniforme de Ancho de Banda	Y	Y	Y	Y	Y	Y	Y
Auto Descubrimiento	Y	Y	Y	Y	Y	Y	Y
Ignore List	Y	Y	Y	Y	Y	Y	Y
Autenticación							
LDAP	Y	Y	Y	Y	Y	Y	Y
NTLM	Y	Y	Y	Y	Y	Y	Y
Radius	Y	Y	Y	Y	Y	Y	Y
POP3	Y	Y	Y	Y	Y	Y	Y
Base de Datos Local	Y	Y	Y	Y	Y	Y	Y
Página de Autentificación Configurable.	Y	Y	Y	Y	Y	Y	Y
Cuota							
Prepaga/Periódica	Y	Y	Y	Y	Y	Y	Y

Seguridad							
Límite de Conexión	Y	Y	Y	Y	Y	Y	Y
Control de Acceso en Capa 7	Y	Y	Y	Y	Y	Y	Y
Estadísticas/Reportes							
En Tiempo Real	Y	Y	Y	Y	Y	Y	Y
Logs de Tráfico/Sistema	Y	Y	Y	Y	Y	Y	Y
Soporte de Reporte de Flujo	Y	Y	Y	Y	Y	Y	Y
Alertas Vía E-Mail, SNMP	Y	Y	Y	Y	Y	Y	Y
Gestión							
Monitoreo de Estado del Sistema	Y	Y	Y	Y	Y	Y	Y
Backup/Restore de Configuración	Y	Y	Y	Y	Y	Y	Y
Upgrade Firmware	Y	Y	Y	Y	Y	Y	Y
Upgrade de Motor de Análisis de Protocolo	Y	Y	Y	Y	Y	Y	Y
SNMP	Y	Y	Y	Y	Y	Y	Y
Web Admin / Https	Y	Y	Y	Y	Y	Y	Y
Consola / CLI	Y	Y	Y	Y	Y	Y	Y
Dimensiones (LxDxH) mm	440x 270 x 44	440x 270 x 44	505x 330x 88	505x 330x 88	485x 430x 88	437x 653x 178	437x 653x 178
Peso	4.3 kg / 1U	4.3 kg / 1U	8KG / 2U	8KG / 2U	18KG / 2U	33.6KG / 4U	33.6KG / 4U

XTRA. "*Optimizando las Redes para hacer más eficientes las activad de las Organizaciones.* Año 2008. Disponible en: <http://www.idris.com.ar/pdf/AscenFlow.pdf>. [En línea].

* Especificación sujeta a cambios sin notificación previa.
* Las marcas y logos pertenecen a Xtera Communications.
* Para mayor información sugerimos visitar www.xtera-ip.com