UNIVERSIDAD DEL AZUAY

FACULTAD DE CIENCIAS DE LA ADMINISTRACIÓN

ESCUELA DE INGENIERÍA DE SISTEMAS

"Calidad de servicio en Redes Inalámbricas (QoS) en la Universidad del Azuay"

Trabajo de Tesis previo a la obtención del Título de:

Ingeniero de Sistemas

Autores:

Edwin Antonio Salazar Ordoñez

Oswaldo Geovanny Silva Jiménez

Director:

Ing. Pablo Esquivel

Cuenca, Ecuador

2012

DEDICATORIA

Esta tesis le dedico a mi Madre, quien con mucho esfuerzo y entrega me educó soportando mis errores y logrando que cumpla su mayor anhelo.

A mis hermanas con quienes hemos compartido felicidad, alegrías y sacrifico; sobre todo a mi hermana Verónica que es mi guía en los pasos como profesional y con quien siempre puedo contar.

A mi Esposa e hijas que han inspirado esperanza en la culminación y también a todos quienes de manera directa o indirecta aportaron día a día con su apoyo.

Dedico también a la memoria de mi Padre quien al saber de estos logros estaría muy orgulloso de sus hijos.

Edwin Salazar Ordóñez.

DEDICATORIA

Esta tesis la dedico primero a Dios, porque gracias a sus bendiciones he podido llegar a cumplir una más de mis metas.

A mis padres, por su gran esfuerzo y sacrificio para que pueda llegar a ser un profesional.

A mi hermana y sobrinos, por su apoyo en todo momento.

A los amigos y familiares, porque siempre están pendientes y dispuestos a colaborar de alguna manera con sus concejos y experiencia.

Oswaldo Geovanny Silva Jiménez

AGRADECIMIENTOS

Agradecemos a la Universidad del Azuay y de manera especial al Ing. Pablo Esquivel y a la Ing. Katherine Ortiz por el apoyo incondicional en la realización de esta tesis, a nuestras familias por alentarnos en todo momento, y a nuestros amigos que siempre han estado pendientes y tratando de ayudarnos de alguna manera.

IINDICE DE CONTENIDO

CAPITULO 4

CAPITULO 5

RESUMEN.

Debido al crecimiento de los dispositivos móviles como las portátiles, tablas, celulares, es de suma importancia que la calidad de servicio brindada a los usuarios sea excelente.

Para tal objetivo se evaluó el sistema operativo RouterOS de la empresa Mikrotik , que en los últimos años se ha ido haciendo conocida, debido a su funcionalidad y el bajo costo de sus licencias. Para las pruebas realizadas se utilizó un hardware Mikrotik RB1100 que incluye una licencia de nivel 6 la cual nos permite manejar todas las características del equipo.

ABSTRACT

Because of the expansion of mobile devices such as laptops, tablets, and cellular phones, it is essential to provide excellent quality customer service.

For this purpose, the Router OS operative system of Mikrotik enterprise was evaluated. This company has become well known in the past few years for its functionality and the low cost of its licenses. For the tests, a Mikrotik RB1100 hardware was employed, which includes a level 6 license that allows us to manage all of the equipment's features.

UNIVERSIDAD DEL
AZUAY
DPTO. IDIOMAS

Translated by,

Diana Lee Rodas

INTRODUCCION

Debido a la evolución que tienen los dispositivos tecnológicos y sus aplicaciones, es necesario emplear políticas de calidad de servicio para poder mantener un desarrollo constante y de esta manera brindar un mejor servicio a los usuarios permitiendo que se optimicen los recursos de la red.

Para el desarrollo de esta tesis se investigó conceptos teóricos sobre redes inalámbricas, su historia y evolución hasta la actualidad. También se estudió el estándar IEEE-802.11e el cual indica la calidad de servicio sobre redes inalámbricas.

Actualmente existen diferentes herramientas de hardware y software que permiten mejorar la calidad de servicio, para el desarrollo de la presente tesis se utilizó el RouterOS Mikrotik, debido a la funcionalidad que nos ofrece y su costo.

CAPITULO 1

1. Redes inalámbricas.

Introducción.

En la década de los 70 se empezaron a interconectar las computadoras a través de un medio físico como los cables Ethernet y coaxiales con velocidades que no superaban los 10 Mbps, actualmente las conexiones físicas alcanza velocidades de hasta 26 Terabits por segundo a través de Fibra Óptica. Estas conexiones permiten intercambiar información y conectar a la red más grande en el mudo conocida como Internet. Durante mucho tiempo necesitamos un medio físico para poder enlazar un grupo de computadoras lo que mantenía atado a un lugar específico restando movilidad, en busca de una solución surgieron las redes inalámbricas que permiten conectar a una red sin la necesidad de cables e incrementar movilidad ya sea en el hogar u oficina, así como han evolucionado las redes de comunicación también lo han hecho las computadoras que hoy en día vienen integrados con dispositivos para conexiones inalámbrica, a más de las computadoras también encontramos otros dispositivos que permiten este tipo de conexión como son: teléfonos celulares, PDA, tablas, impresoras, etc.

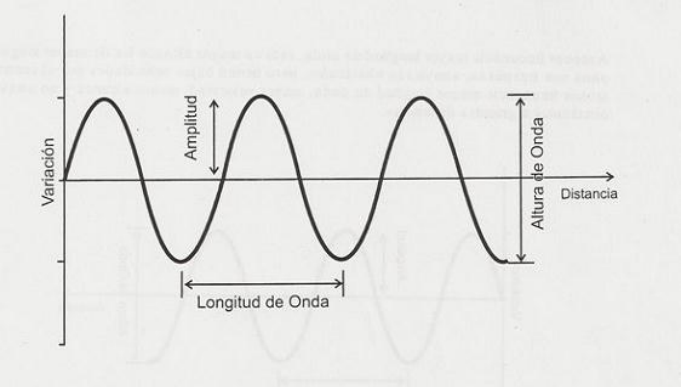
1.1. Conceptos Básicos.

Una red inalámbrica utiliza ondas electromagnéticas o también conocidas como ondas de radio para la transmisión y recepción de la información, funciona de manera similar a los teléfonos celulares y otros equipos como radios, etc.

1.1.1. Ondas Electromagnéticas

Es la forma como se propaga la energía electromagnética a través del espacio, es un tipo de radiación en forma de onda que no necesita un medio físico para propagarse, sino que se propagan libremente por el aire.

1.1.1.1. Componentes de una onda



Fuente: Internet y Redes Inalámbricas, CLANAR Internacional, Pag 1.

Gráfico 1.1: Componentes de una onda.

Amplitud.- Es la distancia Vertical entre la base y el punto más alto de la onda.

Periodo.- Es el tiempo en el que la onda completa un ciclo.

Frecuencia.- Se refiere al número de periodos que se repiten en una unidad de tiempo (segundo) y se mide en hertz.

Longitud de onda.-Es la distancia entre el punto inicial y final de una onda.

1.1.1.2. Espectro Electromagnético.

Se denomina espectro electromagnético a la distribución energética del conjunto de las ondas electromagnéticas. Estas se agrupan bajo distintas denominaciones dependiendo de su rango de frecuencias. Los espectros se pueden observar a través de espectroscopios estos también permiten hacer medidas, como la longitud de onda, frecuencia y la intensidad de la radiación.

1.2. Bandas de Radiofrecuencia para redes inalámbricas.

Generalmente se utilizan las bandas no licenciadas es decir de libre uso, estas son:

- 900 MHz, Su taza de transmisión es de 1Mbps, se utilizan generalmente para transmisiones de voz ya que no son muy útiles para transmisión de datos.
- 2.4 GHz, corresponden a las normas *WiFi* de la IEEE 802.11b, 802.11g, 802.11n, su taza de transmisión oscila entre 11 y 22Mbps (modo b) y 54 y 108Mbps (modo g)
- 5 GHz, corresponde a la norma 802.11a, es compatible con los estándares 802.11b y g, su transmisión máxima es de 108Mbps.
- A más de las normas 802.11a, b y g existe una nueva versión la 802.11n, esta puede trabajar en dos bandas la de 2.4GHz(normas b y g) y en 5GHz (norma a), por lo que es compatible con dispositivos de las tres normas anteriores, pero a diferencia de las anteriores puede llegar alcanzar velocidades de transmisión de hasta 600Mbps.

1.3. Clasificación de las Redes.

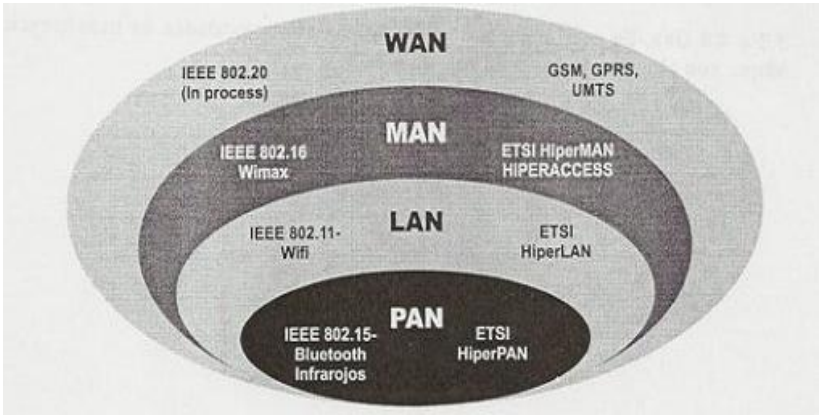
Se las clasifica en cuatro categorías según su tipo de enlace:

- WAN (*WorldArea Network*)
- MAN (*MetropolitanArea Network*)
- LAN (*Local Area Network*)
- PAN (*Personal Area Network*)

En las dos primeras categorías WAN y MAN están las redes que cubren desde desenas hasta miles de Kilómetros, las redes LAN llegan a cubrir áreas locales con desenas de metros y finalmente las redes PAN o personales cubren hasta 30 metros aproximadamente.

Para la categoría LAN en 1997 se estableció la norma 802.11 que tiene un alcance local y usa como medio de transmisión el aire, es conocida también como red *Wi-Fi*.

De aquí en adelante estudiaremos más a fondo las redes *Wi-Fi* que son el motivo de análisis de esta tesis.



Fuente: Internet y Redes Inalámbricas, CLANAR Internacional, Pag 6.

Gráfico 1.2: Clasificación de redes.

1.4. Redes Wi-Fi.

Este tipo de red utiliza ondas electromagnéticas para comunicarse con los equipos de la red, evitando así el uso de cables y permitiendo la movilidad

que ofrecen las tecnologías inalámbricas. En junio de 1997 la IEEE terminó de elaborar el estándar 802.11 para de esta manera consolidar este tipo de red.

1.4.1. Historia del WiFi

En 1986 se utilizaron por primera vez los sistemas inalámbricos, las primeras redes de este tipo eran lentas y toda su infraestructura tenía que ser del mismo fabricante debido a que cada uno tenía su estándar.

En 1997 con la aparición de la norma IEEE 802.11 se logra estandarizar el funcionamiento de las redes *wifi* para de esta manera tener compatibilidad entre equipos de diferentes fabricantes.

La Diferencia entre las normas IEEE 802.3(Ethernet) y 802.11(WiFi) es el medio de transmisión por lo que son compatibles entre sí.

WiFi se caracteriza por utilizar frecuencias de uso libre, pero se debe tomar en cuenta que estas son utilizadas sin control alguno, razón por la cual están expuestas a interferencias.

1.4.2. Ventajas de una Red WiFi.

Movilidad. Es una de las principales ventajas ya que se puede trasladar de un punto de conexión en la red a otro sin necesidad de reiniciar ningún tipo de conexión, de esta manera logramos movilidad de los dispositivos a cualquier parte dentro del área de cobertura, y al igual que una red Ethernet se puede acceder a recursos de la red, compartir archivos, imprimir, navegar en internet, etc.

Portabilidad. permite conectar diferentes redes de acceso, pero siendo necesario detener y reiniciar las conexiones de red activas, esto facilita el desarrollo de algunas actividades que requieren portabilidad.

Flexibilidad. Aparte de mantener conectados mientras se produce movimiento de un lugar a otro, También evita pasar cables de red por lugares peligrosos o en lugares donde se accede esporádicamente.

Reducción de Costos. Diseñar una red inalámbrica no solo ahorra dinero sino también tiempo ya que son sencillas de implementar a comparación de una red cableada.

Escalabilidad. Permite expandir la red de una manera fácil y rápida ya que en el peor de los casos no implica más que la instalación de una tarjeta, a comparación de una red cableada donde se tienen que instalar un nuevo cableado.

1.4.3. Desventajas de una Red WiFi.

Velocidad. Debido al medio por el cual se propagan son susceptibles a interferencias lo que hace que la velocidad de transmisión sea menor que la de una red cableada.

Seguridad. Está en la principal desventaja de las redes WiFi, debido a que se propagan por el aire cualquier persona puede intentar conectarse a la red siempre y cuando este dentro del área de cobertura, aunque se han incorporado un sistema de seguridad en los puntos de acceso de la red como encriptación WEP, WPA, WPA2, pero lamentablemente pueden ser vulnerados de alguna manera.

Interferencias. Debido a que la mayoría de redes de este tipo utilizan el espectro radio eléctrico en frecuencias de libre uso como son la 2.4Ghz y 5Ghz están expuestas a diferentes interferencia en el medio, pudiendo ser un claro ejemplo de problemas las redes continuas.

Alcance. Depende mucho la potencia de los Equipos y la ganancia de las antenas, cuando no son suficientes en algunas zonas donde no tengamos cobertura.

1.4.4. Modelo de Referencia 802.11.

Al pertenecer a la familia 802.x toma la misma arquitectura del modelo OSI con la diferencia que especifica las normas de funcionamiento para las dos capas inferiores (capa física y de enlace) para el estándar 802.11.

La primera versión del estándar fue lanzada en 1997 llamada IEEE 802.11, la misma que funcionaba a una velocidad de entre 1 y 2 Mbps en la frecuencia de 2.4GHz. En 1999 se lanzó otra versión del estándar conocida como IEEE 802.11b, funcionaba a una velocidad de 5 a 11 Mbps en la frecuencia de 2.4GHz, al mismo tiempo salió una versión conocida como IEEE 802.11a y alcanzaba velocidades de hasta 54 Mbps en la frecuencia de 5GHz, esta versión era incompatible con el estándar 802.11b por lo que en ese tiempo casi no se desarrollaron muchos productos con este estándar. La versión más reciente es la conocida como IEEE 802.11n que en teoría podría llegar a velocidades de 600Mbps y es compatible con los estándares anteriores (a,b,g) debido a que puede funcionar en la banda de 2.4Ghz y 5HGz. Desde el inicio del IEEE802.11 se tomó en cuenta la seguridad que igualmente con el pasar del tiempo se ha ido mejorando con la finalidad de brindar al usuario no solo la estabilidad en la conexión si no la transmisión segura de su información.

A continuación una breve descripción del funcionamiento de la capa de enlace y física para el estándar IEEE 802.11

1.4.4.1. Capa Física.

Esta encargada de la modulación, señalización y características de la transmisión de los datos.

Existen dos tecnologías que generalmente se emplean en las radiofrecuencias, espectro ensanchado por secuencia directa y espectro ensanchado por salto de frecuencia.

Tecnología de espectro ensanchado por secuencia directa (DSSS).

Esta técnica genera un patrón en bits redundantes conocida como Señal de chip para cada bit que compone la señal de información y seguido de la modulación de la señal resultante mediante una portadora de RF (Radio Frecuencia). EL receptor realiza el proceso inverso para obtener la información original.

Esta técnica sustituye cada uno de los bits de datos que se quiere transmitir por una secuencia de 11 bits equivalentes, la misma que permite reconstruir la información aunque esta se vea afectada por algún tipo de interferencia.

Después de ser aplicada la señal de chip, se definen dos tipos de modulación para el estándar IEEE 802.11 para esta técnica de espectro ensanchado por secuencia directa: DBPSK (*Differential Binary Phase Shift Keying*), DQPSK (*Diferential Quadrature Phase Shift Keying*), las mismas que proporciona velocidades de 1 y 2 Mbps respectivamente, con el tiempo se han ido mejorando las velocidades y niveles de seguridad, por ejemplo el estándar IEEE 802.11b llega a una velocidad de 11Mbps.

DSSS opera generalmente en las frecuencia que va desde los 2.4Ghz hasta los 2.4835Ghz, es decir se dispone de un ancho de banda total de 83.5 MHz, que a su vez de dividen en 14 canales cada uno de 5MHz, estos canales se utilizan dependiendo de las normas establecidas por cada país. Cada canal necesita de 22MHz para poder transmitir información produciendo un solapamiento entre los canales, por lo que se recomienda en el caso de tener puntos de acceso cercanos utilizar canales separados como el canal 1, 8 y 14.

Tecnología de espectro ensanchado por salto de frecuencia (FHSS).

Esta técnica transmite una parte de la información por una frecuencia determinada durante un tiempo inferior a los 400ms, denominado *dwell time*, después de que pasa este tiempo se cambia la frecuencia de emisión para seguir transmitiendo en la otra frecuencia, es decir cada parte de la información se transmite en una frecuencia diferente en un periodo de tiempo corto.

Una secuencia pseudoaleatoria que se almacena en unas tablas es la que determina el orden de los cambios de frecuencia, estas tablas deben ser conocidas tanto por el emisor y el receptor para poder sincronizar los saltos de frecuencia.

Utiliza el rango de frecuencias de los 2.4GHz, al mismo que los divide en 79 canales cada uno con un ancho de banda de 1MHz, cada país se encarga de regular el número de saltos por segundo.

También se establece la modulación para el estándar IEEE 802.11, denominada FSK (*Frequency Shift Keying*), que funcionan a una velocidad de entre 1 y 2 Mbps. Para el estándar IEEE 802.11b aumento la velocidad a 11Mbps.

1.4.4.2. Capa de Enlace.

Esta capa es la responsable de que la información transmitida por la red esté libre de errores, se encuentra conformada por dos capas (LLC: *Logical Link Control*, MAC: *Medium Access Control*), el funcionamiento de la capa de enlace es similar para los diferentes métodos de acceso de IEEE 802 ya que fueron creados según el modelo OSI, por esta razón analizaremos el funcionamiento de la capa MAC para el estándar IEEE 802.11.

La capa MAC es la encargada de realizar el control de flujo en la transmisión de paquetes dentro de una red, para ello utiliza el algoritmo llamado CSMA/CA (*Carrier Sense Multiple Access / Collision*

Advoidance), el mismo ayuda a evitar colisiones, identifica el final de una transmisión deja pasar un tiempo aleatorio antes de empezar a transmitir su información así evita la posibilidad de una colisión.

1.4.4.3. Sub capa MAC.

La sub capa MAC para el estándar IEEE 802.11 es la misma que para los estándares de IEEE 802.11x. El estándar IEEE 802.11 define nueve servicios MAC, de los cuales seis son para la transmisión de paquetes y los trece restantes para controlar el acceso a la red y asegurar la confidencialidad de los datos. Los servicios son:

- Privacidad.- Previene el acceso no autorizado a la red implementando algoritmos de encriptación (WEP y WPA) para la encriptación de los datos que atraviesan por la red.

- Distribución.- Se asegura de que los datos transmitidos entre una terminal y otra lleguen a su destino.

- Asociación.- Antes de que un terminal pueda comunicarse con otros terminales debe asociarse a un punto de acceso, este será el responsable de la información que manda o recibe dicho terminal. Cada terminal solo puede estar asociado con un solo punto de acceso a la vez.

- Des asociación.- En caso de que el terminal sale del área de cobertura o porque el punto de acceso termina con la conexión, se cancela la asociación.

- Re asociación.- Cuando un terminal ha perdido la asociación debido a que se salió del área de cobertura del punto de acceso y regresa al mismo. También cuando un terminal se mueve del área de cobertura de un punto de acceso a la de otro, en este caso se hace la transferencia de la asociación entre los dos puntos de

acceso ya que la asociación ahora depende del último punto de acceso al que se conectó el terminal.

- Autenticación.- Comprueba la identidad de cada terminal que se quiere conectar a la red antes de permitirle asociarse a la misma.
- Des autenticación.- Da por concluida la conexión cuando un terminal se desconecta de la red.
- Entrega de datos.- Facilita la entrega de datos entre terminales.
- Integración.- facilita la transferencia de información en redes que funcionan con diferentes estándares por ejemplo WiFi(802.11x) y Ethernet(802.3).

CAPITULO 2

2. QoS (Calidad de Servicio).

Cuando hablamos de QoS se hace referencia a la capacidad de una red para seleccionar y priorizar el tráfico, es decir se puede mejorar el rendimiento de la red optimizando los recursos de administración.

QoS también tiene la capacidad de administrar el ancho de banda ya sea por protocolo, por usuario o ambos, así por ejemplo se podría dar mayor prioridad y asignar un ancho de banda para la VoIp, Video, Datos, según la necesidad.

Mediante la utilización de QoS se puede definir los parámetros pata transportar paquetes entre nodos tomando en cuenta el rendimiento, disponibilidad y retardos óptimos.

Debemos aclarar que al dar prioridad a cierto tipo de tráfico no afectemos el trabajo ni desempeño de los demás.

2.1. Clasificación de QoS.

QoS está encargada de clasificar el tráfico que pasa por la red, esto lo hace usando algunos criterios de clasificación como: Equipo destino, marcas de los paquetes, tipo de aplicación, etc.

Todas las aplicaciones dejan una marca en lo paquetes para que se pueda identificar la aplicación fuente. Existen cuatro métodos de clasificación:

- Protocolo.- Se identifican los protocolos por el valor del campo *EtherType* de cada paquete, luego de identificar se priorizan los paquetes en función del protocolo al que pertenecen.

- TCP y UDP *Socket Number*.-Ya que muchas aplicaciones utilizan ciertos *sockets* UDP para comunicar, se examina el número de *socket* del paquete IP para determinar a qué tipo de aplicación pertenece el paquete.

- *Source IP Address*.- El Análisis de una dirección IP de origen permitir identificar que aplicación generó cierto paquete, ya que algunos servidores están dedicados a soportar una sola aplicación como por ejemplo Mail.

- *Physical Port Number*.- Al igual que las direcciones de origen ip, el *Physical Port Number* puede identificar el servidor que está generando los datos, se basa en el mapeado de puertos físicos de un conmutador a un servidor de aplicación, siempre y cuando el servidor esté conectado directamente al conmutador.

2.2. Objetivo de QoS.

Debido al crecimiento y el avance de las redes de datos, es necesario brindar mejoras en el rendimiento, es por esto que el tráfico se clasifica con diferentes criterios como: Voz/Ip, Video Conferencia, Navegación Web, etc.

La implementación de QoS ayuda a cumplir con los requerimientos de rendimiento para cada tipo de tráfico.

Los objetivos esenciales de QoS son:

- Control sobre los recursos: Limitar el ancho de banda dependiendo del tipo de aplicación que lo esté utilizando.

- Permite utilizar de forma eficiente los recursos de la red: establecer prioridades sobre los diferentes tipos de tráfico.

- Menor Latencia: Para el caso de aplicaciones sensibles al retardo como la Voz/Ip que requieren menor tiempo de respuesta para un óptimo funcionamiento.

Para que en una red pueda ofrecer un buen manejo de QoS, es necesario que todos los dispositivos intermedios (*Routers, Switch, Acces Point*.) posean mecanismos de QoS que brinden un desempeño adecuado.

El rendimiento de estos dispositivos se pueden distinguir por el usuario ya que todos los parámetros de QoS como son: el retardo, la pérdida de paquetes se perciben de manera muy fácil.

Para garantizar QoS es necesario la implementación de políticas de Calidad de Servicio, las mismas que no solo dependen del *hardware* sino de diferentes variables como:

- Aplicaciones.- Maneja Señalización necesaria para hacer la negociación de parámetros de red.
- Acceso LAN.- Tipo de Arquitectura de red, protocolos, mecanismos de calendarización, control de tráfico y de admisión.
- Acceso WAN.- Es la arquitectura de transporte de información que ofrece la capacidad de mantener el mínimo retardo y pérdidas de información, por medio de mecanismos de diferenciación y control de tráfico.

2.3. Parámetros de QoS.

A continuación una breve descripción de los parámetros clave que maneja QoS:

- Trafico de Red.- Es toda la información que pasa por la red y se pueden clasificar en dos grupos principales que se basan en:
    - Tipo de aplicación (multimedia, multicast, broadcast, tiempo real, etc.).

    - Sensibilidad al retardo (transacciones on-line, video conferencias, etc.)

- Retardo.- Es el tiempo que le toma en llegar los datos a su destino, generalmente este tiempo es variable lo que influye en el funcionamiento de ciertas aplicaciones como una video conferencia en donde la señal de la voz llega antes que la señal del video, también con la llegada de protocolos como Voz/Ip surge la necesidad de establecer políticas de QoS para que este parámetro sea el mínimo posible.

- Latencia.- El tiempo que le toma a un nodo enviar un mensaje más el tiempo que le toma al otro nodo en receptarlo, incluye el tiempo de todo el recorrido y los dispositivos intermedios por los que pasa.

- *Jitter*.- Es algo semejante a la distorsión de una señal, dado que los paquetes no llegan a su destino en el orden que fueron transmitidos, generalmente es perjudicial para el tráfico multimedia.

- Ancho de Banda.- Teóricamente es la capacidad máxima con la que se pueden transmitir los datos, generalmente se la expresa en Kilobits por segundo (Kbps) o Megabits por segundo (Mbps), esta capacidad máxima se ve deteriorada por factores como retardos en la transmisión o la saturación del canal debido a una mala administración del mismo.

- Perdida de paquetes.- Mide el número de paquetes perdidos durante una transmisión, generalmente se la expresa en %.

- Disponibilidad.- Indica el porcentaje de utilización de diferentes recursos.

- Rendimiento.- Depende directamente del ancho de banda y su variación debido a congestiones en la red.

- Priorización.- Asignar QoS al tráfico de la red para que primero sean atendidas las aplicaciones de mayor importancia. Es necesaria cuando la capacidad de la red no es suficiente para atender todo el tráfico de la misma.

- Encolado.- Es el encargado de organizar el tráfico ante un determinado dispositivo, se encarga de ofrecer un mejor servicio al tráfico de alta prioridad y al mismo tiempo se distribuye el tráfico de baja prioridad.

  Esto no quiere decir que garantice que el tráfico de alta prioridad llegue a tiempo, si no que sean atendidos antes que los paquetes de baja prioridad.

- Planificación.- Es el proceso de decidir que paquetes enviar primero en un sistema de múltiples colas.

- Flujo.- Conjunto de datos que debido a tamaño debió ser descompuesto en varios paquetes, por lo que el flujo de los mismos debe ser secuencial y a una frecuencia constante de transmisión de datos.

- Acuerdo de niveles de servicio.- Es un acuerdo entre el proveedor de servicios y el cliente, en el que se define los parámetros de funcionamiento de la red (rendimiento, tasa de perdidas, retardos, variaciones), aquí se establece el precio del servicio y las consecuencias de no cumplir con los niveles de funcionamiento de la red como proveedor, o de exceder los límites de tráfico por parte del cliente.

2.4. Arquitectura de QoS.

El IETF(*Internet Engineering Task Force*) ha desarrollado algunas técnicas para la aplicación de QoS las más conocidas son:

- "*IntServ (Integrated Services). Este es un modelo para proporcionar calidad de servicio en Internet e intranets. La intención de los diseñadores IntServ fue dejar a un lado una parte del ancho de banda de red para el tráfico, tales como voz en tiempo real y video que requieren bajo retardo, bajo jitter (retardo variable), y el ancho de banda garantizado. El IntServ Grupo de Trabajo desarrolló RSVP (Resource Reservation Protocol), un mecanismo de señalización para especificar los requisitos de QoS en una red. IntServ tiene problemas de escalabilidad y era demasiado difícil de implementar en Internet. Sin embargo, RSVP se utiliza en las redes empresariales, y su mecanismo de control para ajustar el ancho de banda a través de una red se está utilizando en nuevas formas con MPLS.*

- *Diff-Serv (Differentiated Services). Diff-Serv clasifica y marca los paquetes para que reciban una transmisión específica por salto a los dispositivos de red a lo largo de una ruta. Lo importante es que no necesita que todos los nodos tengan implementada esta arquitectura para que su uso mejore el rendimiento del sistema. Diff-Serv trabaja en el nivel de IP para proporcionar calidad de servicio basado en IP configuración ToS. Diff-Serv es quizás la mejor opción para la señalización de los niveles de calidad de servicio disponibles en la actualidad.*

- *MPLS (Multi-Protocol Label Switching). Es un protocol diseñado principalmente para las redes centrales de Internet, está desarrollado para gestionar anchos de banda y calidad de servicio, su comunicación se basa en utilizar etiquetas de identificación logrando de esta manera clasificar paquetes y evitar que cada dispositivo realice un análisis de inspección, esto reduce significativamente la sobrecarga y agilita el flujo de todo el tráfico, MPLS tiene cierta similitud con los circuitos virtuales ATM en las redes Frame Relay."*. Linktionary. [15 de 04 de 2010]. QoS (Quality of Service.) Tomado el 18 de 04 de 2010 de (*http://www.linktionary.com/q/qos.html*)

2.5. Mecanismos y Herramientas de QoS.

Debido a la gran cantidad de tráfico por el incremento de aplicaciones que funcionan en internet se congestionan cada vez más las redes y la demanda de recursos es mayor a la capacidad disponible. Aumentar el ancho de banda podría ser una solución pero desafortunadamente no siempre es posible.

Los costos y la tecnología utilizada son algunas de las limitantes o restricciones que obligan a optimizar los recursos de las redes por medio de la implementación de QoS.

Administrar los parámetros de pérdida o retraso de paquetes en la red es parte de la solución para lograr un buen nivel de QoS en la red. Para la administración de los recursos de la red se necesitan de algunos tipos de Herramientas que son:

- Clasificación.- Identifican que tipo de tráfico está pasando por la red, y dependiendo del mismo se les da una marca con una prioridad, por medio de la cual se establece que tratamiento se le debe dar a cada paquete como por ejemplo: Paquetes de Voz/Ip tienen mayor prioridad que paquetes que conforman un p2p.

- Administración de Congestión.- Se encargan de formar las colas que determinan el orden en que los paquetes van a ser transmitidos dependiendo de las prioridades que posea cada paquete.

- Administración de colas (*Queue Management*).- Impide que una cola se llene, para permitir que el tráfico de alta prioridad ingrese a la cola.

- Política/Control.- Es un mecanismo que es utilizado para limitar el ancho de banda que cada tipo de paquete utiliza en la red.

- Eficiencia del enlace.- Proporcionan un método de mitigación del retraso que se experimenta con los enlaces de menor velocidad.

2.6. Gestión de políticas de QoS.

Es una forma de asignar recursos a la red, de acuerdo a las necesidades definidas. La definición de políticas son las repuestas a preguntas como:

- Qué tipo de tráfico se puede descartar cuando la red está ocupada?
- Que ancho de banda se garantiza para el tráfico de mayor prioridad?

Responder a estas preguntas permite definir reglas y manejarlas en un sistema político. Estas reglas tienen la forma "Si una condición, entonces una acción."

La IETF se encargó del desarrollo de una arquitectura para la gestión de políticas de QoS, incluye los siguientes componentes:

-Servicio de administración de políticas.- Es un interfaz gráfica donde el usuario puede especificar, editar y administrar las políticas.

-Repositorio dedicado de políticas.- Lugar donde se almacena la información sobre las políticas, puede ser un servidor LDAP (*Light weight Directory Access Protocol*, Protocolo Ligero de Acceso a Directorios) o un dispositivo DEN (Directory Enabled Network, Directorio habilitado en la red).

-PDP (*Policy decition point*, Punto de decisión).- Es el responsable de obtener las políticas de la base de datos y tomar las decisiones basadas en las peticiones de los PEP.

-PEP (*Policy enforcement point*, punto de aplicación de la política).- Están en los nodos de la red como, Router, firewall, host. Es el encargado de hacer las políticas basadas en el conjunto de reglas que recibe de PDP.

-COPS (*Common Open Policy Service*).-El objetivo principal es suministrar las políticas pudiendo estas ser inicialmente simples e ir adquiriendo mayor complejidad.

-LPDP (local policy decisition point, punto de decisión de política local).- Esta es una escala reducida del PPD que existe dentro de un nodo de red y se utiliza en los casos en que un servidor de la política no está disponible. Las decisiones básicas de política pueden ser programadas en este componente.

2.6.1. QoS Aplicado a redes inalámbricas.

Debido a que el estándar original IEEE 802.11 no permitía la implementación de QoS, la IEEE a finales del 2005 lanzo el estándar IEEE 802.11e el mismo que permite la gestión de QoS sobre cualquiera de los estándares de IEEE 802.11.

Esta norma es considerada de vital importancia para las redes *WiFi*, debido a que en la actualidad manejamos aplicaciones sensibles al retardo, como la Voz/Ip, Video conferencia, etc.

La Arquitectura 802.11 Mac se compone de dos funciones básicas que son la de: Función de Coordinación Puntual (PCF) y la Función de Coordinación Distribuida (DCF), en el estándar 802.11e se introducen dos nuevos modos de operación Mayor DCF (EDCF) y la Función de Coordinación Hibrida (HCF) los cuales están creados para trabajar con todos los 802.11 Mac.

2.6.1.1. Función de Coordinación Distribuida (DCF)

Es la función básica de acceso al canal de 802.11 MAC la cual proporciona un acceso compartido al medio para los dispositivos. Está basada en el protocolo CSMA/CA, todos los equipos 802.11 soportan esta función y deben incluir obligatoriamente este mecanismo, a diferencia del PCF que es opcional.

2.6.1.2. Función de Coordinación Centralizada (PCF).

Este mecanismo forma parte del estándar 802.11 pero a diferencia con la función DCP su uso es opcional por lo cual los productos 802.11 no están en la obligación de realizar su implementación. Los puntos de acceso manejaran un elemento llamado Punto de Coordinación que se encargara de priorizar el acceso al medio de determinadas estaciones.

El mecanismo de PCF ha presentado muchos problemas, razón por la cual el grupo de trabajo 802.11 ha propuesto mejoras para el soporte de calidad de servicio.

2.6.1.3. Norma IEEE 802.11e.

Este estándar es considerado de muchísima importancia en especial para el soporte de aplicaciones que necesitan garantizar la calidad de servicio como son las aplicaciones en tiempo real y sensibles al retardo como videoconferencia o voz/ip, etc.

Para soportar la calidad de servicio si introdujo una nueva función de coordinación, denominada HCF (*Hybrid Coordination Function*), la misma que incorpora dos nuevos mecanismos de acceso al canal:

EDCA (*Enhanced Distributed Channel Access*), equivalente a DCF.

HCCA (*HCF Controlled Access*), equivalente a PCF.

Una de las principales características de HCF es que define cuatro categorías de acceso y ocho categorías a nivel de MAC de flujo de tráfico (TS). Cuando los paquetes provenientes de las capas superiores llegan a la capa MAC, aquí se etiqueta con un identificador de prioridad de cada paquete, pueden obtener un valor entre 0 y 15. Si el TID tiene

valores entre 0 y 7 se utiliza el método EDCA con respecto a las cuatro categorías de acceso, y si el valor está entre 8 y 15 usara la función HCCA para acceder al medio, el paquete permanece almacenado en la cola de TS correspondiente a su TID.

Otra característica incluida en el estándar es el intervalo de tiempo en el cual la estación que lo posea tiene permiso para enviar sus tramas, es conocido como: TXOP (*Transmision Opportunity*).

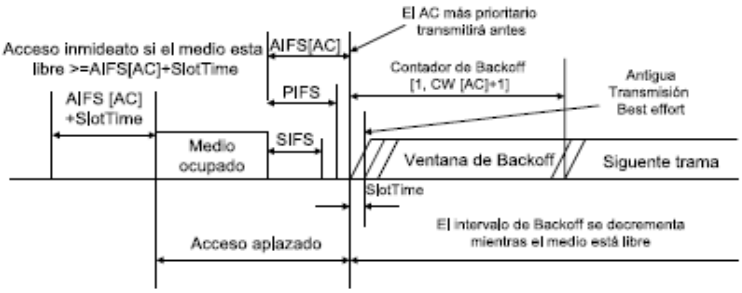
2.6.1.3.1. EDCA (*Enhanced Distributer Channel Access*)

Permite proporcionar mayor o menor prioridad a las tramas dependiendo del tipo de tráfico al que pertenezcan, esto se logra configurando los distintos parámetros de acceso al medio.

EDCA utiliza cuatro categorías de acceso que manejan las distintas prioridades y se permite diferenciar entre cuatro tipos de tráfico, cada categoría tiene su propia cola de transmisión, caracterizada por el ajuste de los parámetros de acceso.

Para hacer esta diferenciación EDCA introduce dos métodos:

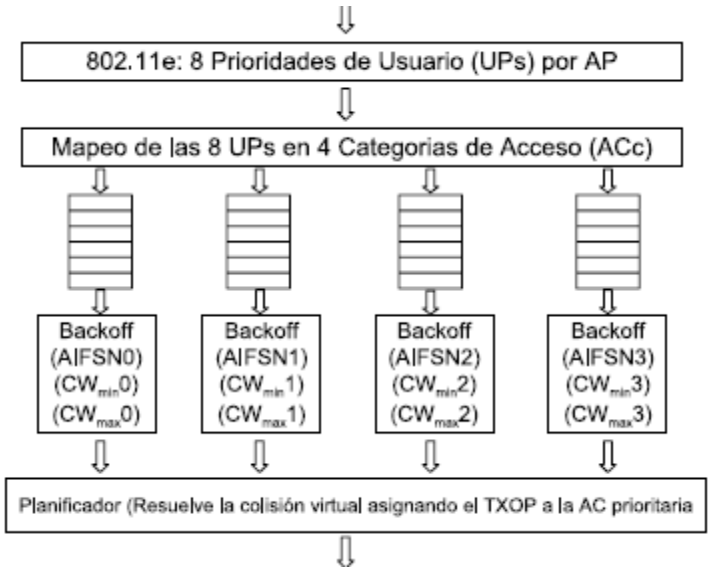
- El primero asigna distintos IFS a cada categoría de acceso, por lo que es necesario introducir el nuevo tiempo de espera denominado AIFS (*Arbitration Inter Frame Space*). El valor de AIFS es AIFS[AC] = AIFSN[AC] x aSlotTime +SIFS, donde AIFSN *(Arbitration Inter Frame Space Number*), es utilizado para la diferenciación entre las distintas AC.



Fuente: IEEE 802.11e Contention-Based Channel Access(EDCF) Performance Evaluation.

Gráfico 2.1: IEEE 802.11e EDCA canal de acceso.

- En el segundo método se utiliza varios tamaños de ventana para cada AC. En este método se pretende asignar menores tiempos de espera a las estaciones más prioritarias cuando estas tengan que efectuar el mecanismo de *back off*. Estos tamaños se obtienen asignando distintos tamaños de límite de ventana CWmin y CWmax. Otro factor utilizado para la distinción en EDCA, es la duración del TXOP, el mismo que limita el tiempo en que una estación tiene los derechos para transmitir sin que el resto de estaciones disputen el canal.



Fuente: IEEE 802.11e Contention-Based Channel Access(EDCF) Performance Evaluation.

Gráfico 2.2: Acceso por categorías para EDCF.

Las cuatro AC que definen el estándar de mayor a menor prioridad son:

I. AC_VO (Voz).
II. AC_VI (Video).
III. AC_BE (Best-effort).
IV. AC_BK (Background).

A continuación un tabla donde se especifican los valores por defecto de los diferentes parámetros en función de los AC.

AC	CW_min	CW_max	AIFSN	TXOP limit		
				For PHYs defined in Clause 15[1] and Clause 18[2]	For PHYs defined in Clause 17[3] and Clause 19[4]	Other PHYs
AC_BK	aCWmin	aCWmax	7	0	0	0
AC_BE	aCWmin	aCWmax	3	0	0	0
AC_VI	(aCWmin+1)/2-1	aCWmin	2	6.016 ms	3.008 ms	0
AC_VO	(aCWmin+1)/4-1	(aCWmin+1)/2-1	2	3.264 ms	1.504 ms	0

Fuente: Ricardo Moreles, P. P.,F. V.,R.C.[2010]Assessment of the IEEE 802.11e EDCA Protocol Limitations when Dealing with Real-Time Communication [online]. Recuperado 11 de 10 de 2010 de, http://www.hindawi.com/journals/wcn/2010/351480/tab1/

Gráfico 2.3: Acceso por categorías para EDCF

También es posible ofrecer Calidad de Servicio parametrizada, utilizando el mecanismo de control de admisión de tráfico, por medio de la trama TSPEC (*Traffic Specification*)., Esta trama describe el tamaño de los paquetes, el caudal o el retardo. Proporciona el mecanismo para el control de la admisión, establecimiento, ajuste y eliminación de flujos de tráfico.

El control de Admisión puede ser utilizado para regular el ancho de banda disponible, también puede garantizar el tiempo q una estación puede tener acceso al canal.

2.6.1.3.2. HCCA *(HCF Controlled Access*).

A diferencia del EDCA en este método se utiliza una forma más avanzada y compleja para acceder al medio, es decir la calidad de servicio puede ser ajustada según las necesidades con gran precisión. Las estaciones pueden verificar la información sobre el estado de otras estaciones, con esta información pueden darse prioridades a unas estaciones sobre otras, de esta manera las estaciones pueden aplicar los parámetros de calidad dependiendo del tipo de tráfico que está pasando por cada estación.

CAPITULO 3

3. Sistema Operativo RouterOS.

Este Sistema Operativo está diseñado para la administración de diferentes tipos de redes, de entre las cuales se puede enunciar redes domésticas y también redes corporativas. Para llevar a cabo las muestras de aplicación de QoS se utilizara esta herramienta que permite mostrar claramente el proceso y tratamiento al tráfico de la red, el sistema operativo cuenta con diferentes productos entre hardware y software independientemente, incluso puede ser instalado en una PC de una manera muy sencilla.

3.1. Reseña.

RouterOS nace en el año 1995 de una tesis universitaria, en la cual tenía como idea principal crear un *router* básico que estaría basado en Linux. En el ano de 1996 inicia su introducción al mundo del WISP (*Wireless Internet Service Provider)*

Estos dos años incentiva mucho a sus desarrolladores para continuar con el proyecto y es así cuando en el año de 1997 inician el desarrollo de su propio software para la plataforma Intel.

El proyecto continua su crecimiento y en el año 2002 desarrollan su propio Hardware al cual lo denominaron con el nombre de *RouterBoard* 230, la empresa continua así su crecimiento con la fabricación de *software* y *hardware* para soluciones de *Networking*.

Sus productos actualmente han logrado una posición muy importante en el mercado y ahora son considerados una opción más en los nuevos proyectos, son

utilizados en diferentes áreas como la construcción de infraestructura de acceso y en la red de distribución.

Uno de los objetivos fundamentales ahora es actualizar las tecnologías de Internet de una manera más poderosa y al alcance de una gran cantidad de usuarios.

3.2. Características Principales.

RouterOS, es un Sistema Operativo que tiene como principal característica el convertir un dispositivo de red (RouterBoard o PC) en:

- *Router* dedicado
- *Firewall*
- Controlador de Ancho de Banda
- Filtro transparente de paquetes
- Equipo 802.11 a/b/g/n – PaP / PMP
- Concentrador de VPN
- *Hotspot gateway*
- y más...

Mikrotik como otras marcas desarrolla su propio *hardware* al cual se lo ha denominado RouterBOARD, este hoy en día abarca un amplio rango de productos dentro de los cuales se pueden encontrar *routers* SOHO hasta los de *Carrier Class.*

Todos los equipos de Mikrotik permiten diferentes modos de acceso entre los cuales se detallan a continuación:

3.3. Modos de Administración.

3.3.1. GUI *Graphical user interface*)

Es una interfaz gráfica de usuario y su herramienta principal se llama WinBox, esta fue diseñada para sistemas operativos de Windows únicamente, aunque puede ser también utilizada en otros sistemas operativos.

Esta aplicación es gratuita y permite configurar cualquier RouterOS en un modo más amigable debido a su interfaz que permite interactuar gráficamente se puede descargada de [www.mikrotik.com/download.](http://www.mikrotik.com/download)

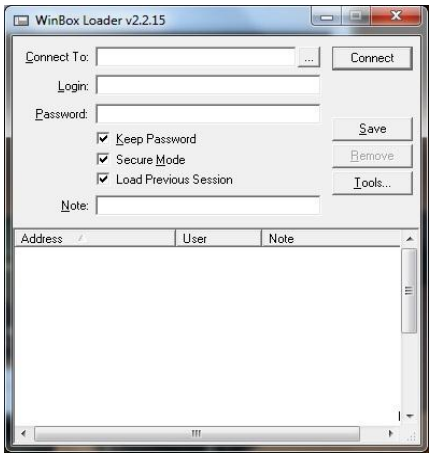


Gráfico 3.1: Ingreso por WinBox.

La ip que utiliza por defecto el sistema RouterOS es la 192.168.88.1 y winbox usa el puerto TCP 8291, el usuario por defecto es admin sin *password*, esta herramienta permite acceso en capa 2 y 3.

3.3.2. CLI *Command line interface*)

Interfaz de línea de comandos es el más común y mantiene compatibilidad con todos los sistemas operativos, sus requisitos son mínimos: Monitor, teclado y un puerto serial, entre algunas aplicaciones están:

- Telnet / Mac Telnet
- SSH

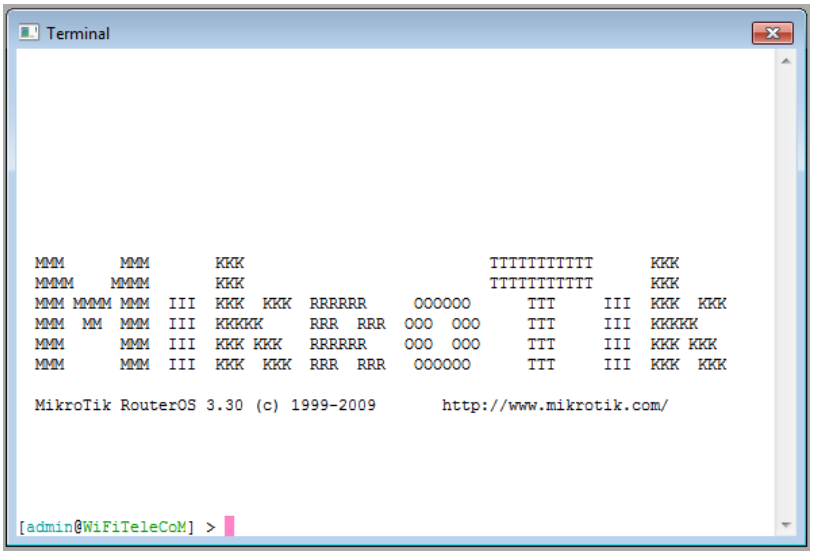


Gráfico 3.2: Ingreso por terminal.

3.3.3. Interfaz Web.

La administración también es posible a través de cualquier navegador y resulta muy sencilla ya que su interfaz es muy parecida a la administración con winbox.

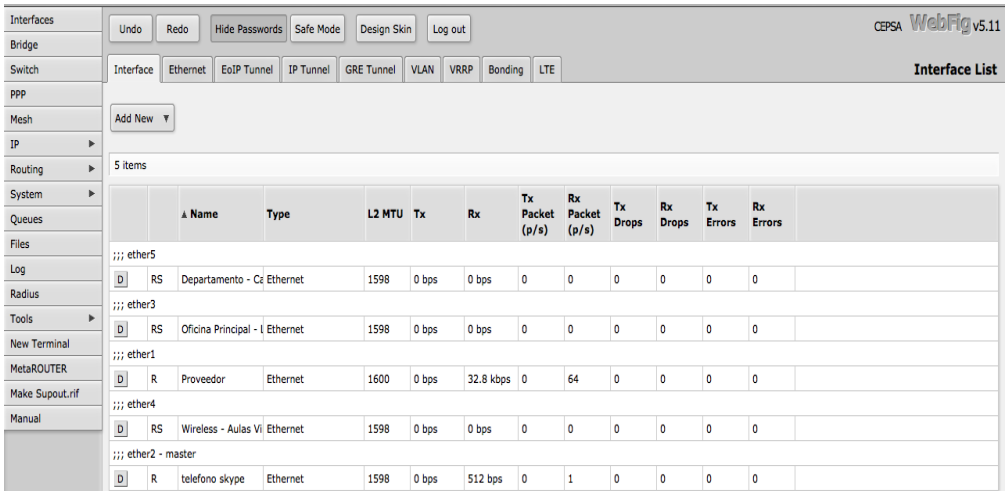


Gráfico 3.3: Ingreso por Web.

3.4. Licenciamiento.

El sistema operativo ofrece una licencia que se otorga al medio que lo almacena que puede ser un disco duro o un medio de almacenamiento extraíble, la licencia es entregada a través de un *SOftID* por cada instalación, generalmente cada uno de los *RouterBoard* traen una licencia ya incluida y una de las ventajas es que ninguna licencia expira además permiten actualización y soporte, Up y *Downgrade*, posee diferentes niveles de licenciamiento diferenciado por sus características en servicios:

Level number	0 (FREE)	1 (DEMO)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Controller)
Price	no key	registration required	volume only	$45	$95	$250
Upgradable To	-	no upgrades	ROS v5.x	ROS v5.x	ROS v6.x	ROS v6.x
Initial Config Support	-	-	-	15 days	30 days	30 days
Wireless AP	24h limit	-	-	yes	yes	yes
Wireless Client and Bridge	24h limit	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h limit	-	yes(*)	yes	yes	yes
EoIP tunnels	24h limit	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	24h limit	1	200	200	500	unlimited
PPTP tunnels	24h limit	1	200	200	500	unlimited
L2TP tunnels	24h limit	1	200	200	500	unlimited
OVPN tunnels	24h limit	1	200	200	unlimited	unlimited
VLAN interfaces	24h limit	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h limit	1	1	200	500	unlimited
RADIUS client	24h limit	-	yes	yes	yes	yes
Queues	24h limit	1	unlimited	unlimited	unlimited	unlimited
Web proxy	24h limit	-	yes	yes	yes	yes
Synchronous interfaces	24h limit	-	-	yes	yes	yes
User manager active sessions	24h limit	1	10	20	50	Unlimited

Fuente: http://wiki.mikrotik.com/wiki/Manual:License

Gráfico 3.4: Licencias de RouterOS

3.5. Servicios.

A continuación la descripción de los servicios del sistema operativo utilizados en el desarrollo de esta investigación.

3.5.1. Firewall.

RouterOS cuenta con el módulo de *Firewall* el cual permite proteger el *router* y todo lo que está detrás de él únicamente con la creación de reglas en el módulo de *Filter Rules.*

Las diferentes reglas que se pueden crear en *Filter Rules*, consiste en reglas definidas por el usuario las cuales trabajan con el principio condicional básico: SI, ENTONCES.

El usuario cuenta con cadenas predefinidas pero además puede crear cadenas adicionales para de esta manera tener una mejor estructura y orden, debemos tomar en cuenta al momento de la creación de las reglas, el orden, ya que este es un factor muy importante.

Las cadenas por defecto que tiene RouterOS son:

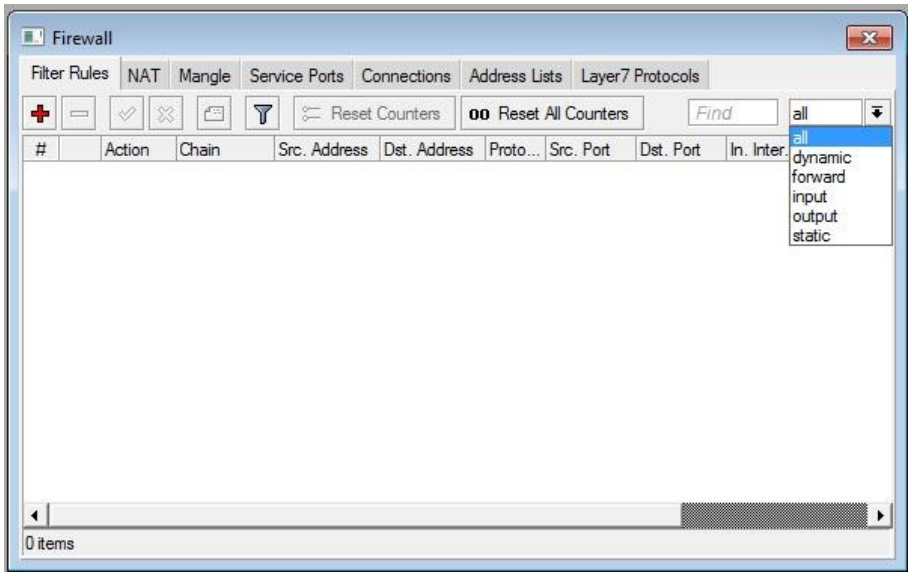


Gráfico 3.5: Cadenas de Firewall.

INPUT.- Esta cadena es la encargada de procesar todos los paquetes que tienen como destino final el *Router.*

OUTPUT.- Encargada de procesar paquetes enviados por el *Router.*

FORWARD.- Procesa paquetes que atraviesan el *Router* con tráfico desde y hacia los clientes.

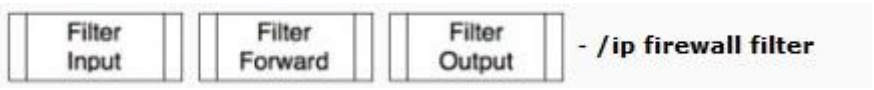


Gráfico 3.6: Flujo ip firewall.

En Firewall existen dos tácticas diferentes que se pueden utilizar generalmente todas las opciones siempre van a demandar experiencia y

conocimiento, la primera seria aceptar únicamente lo conocido y bloquear todo el resto, y otra táctica aunque menos eficaz y con mayor vulnerabilidad es bloquear lo conocido y aceptar el resto.

Todas las reglas que se crean independientemente de la cadena a la que pertenece utilizan una estructura básica la cual se muestra con el siguiente ejemplo:

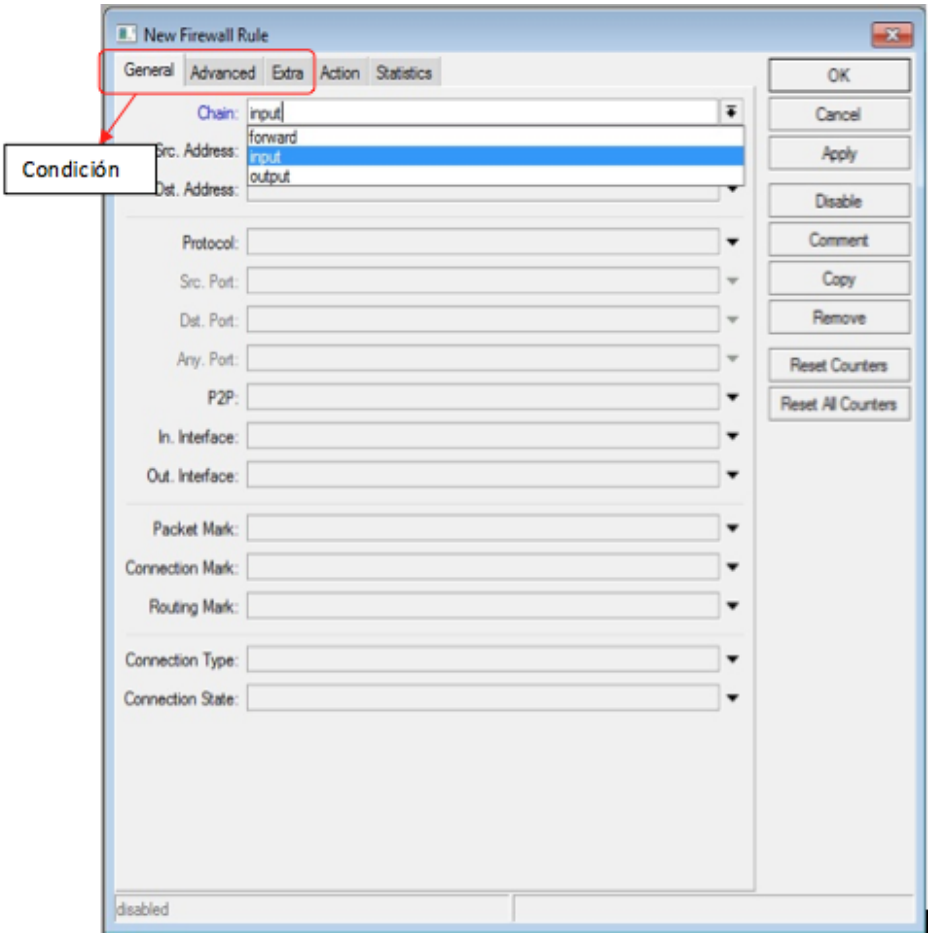


Gráfico 3.7: Creación de nueva regla de firewall

Como se muestra en la parte superior las tres primeras pestañas permiten condicionar la regla con sus diferentes opciones para que cumpliendo esta se tome una acción.

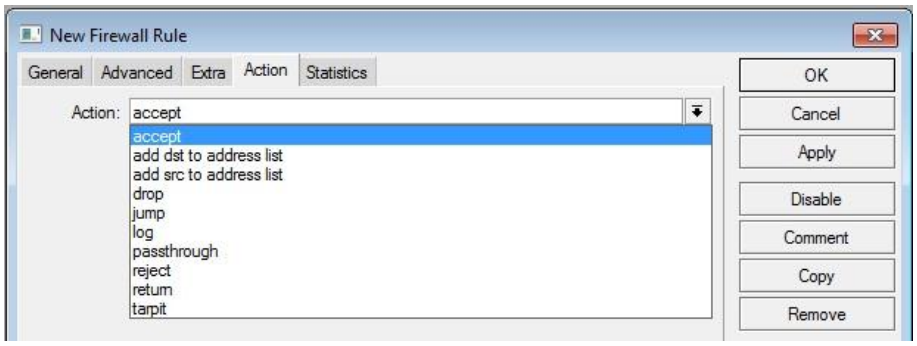


Gráfico 3.8: Accion Nueva regla de firewall.

Una de las partes más importantes dentro del Módulo de *Firewall* está en la pestaña de *Connections*, la opción *Tracking* es parte fundamental ya que está encargada de recopilar y manejar todas las conexiones activas.

Cada una de las entradas que se pueden visualizar representa una un intercambio bidireccional de datos por lo tanto se puede notar claramente que está utilizara muchos recursos de CPU, al deshabilitar el *ConnTrack* el sistema pierde su capacidad de hacer *NAT*, así como también la mayor parte de las condiciones de filtrado y marcado que se pueden hacer.

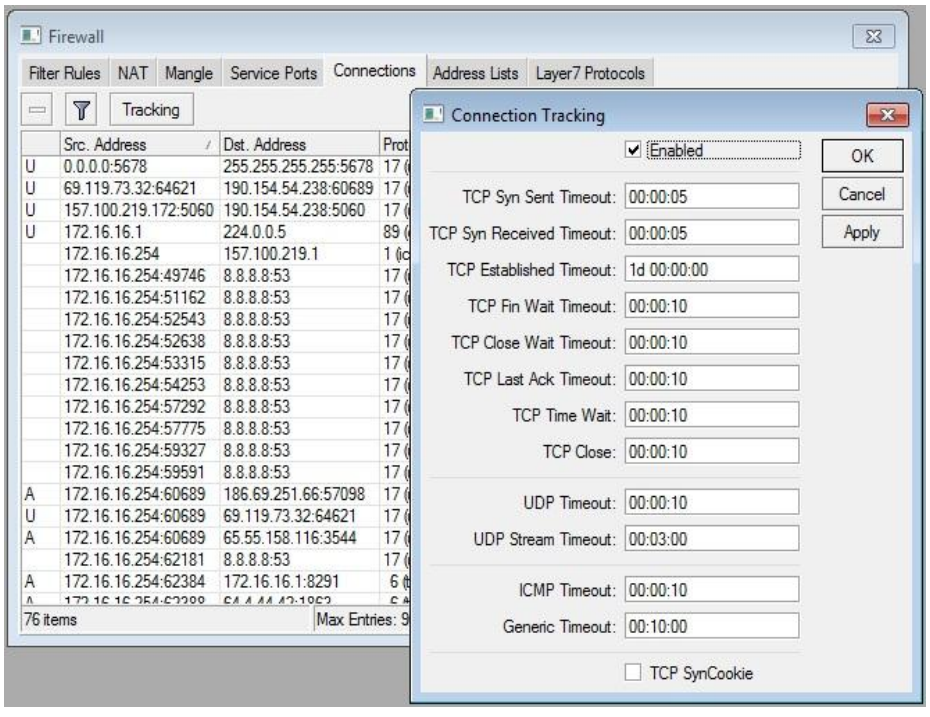


Gráfico 3.9: Connection Traking.

3.5.2. NAT (*Network AddressTranslation*)

Nat es el encargado de la traducción de direcciones de red, es un mecanismo que se utiliza comúnmente entre los *routers* para de esta manera poder intercambiar paquetes. El encabezado del paquete IP está compuesto por una dupla de direcciones (origen y destino) y además también una dupla de puertos.

El RouterOS tiene la capacidad de cambiar el origen o destino de cualquier paquete que lo atraviesa, este proceso se llama src-nat o dst-nat, dependiendo del parámetro que se modifique.

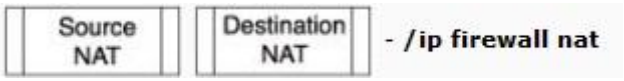


Gráfico 3.10: Flujo ip firewall NAT.

Al igual que el Filter Rules estas reglas de NAT también trabajan con el principio condicional: SI > ENTONCES, debemos tener en cuenta que NAT solo trabaja con el *Connection Tracking* habilitado.

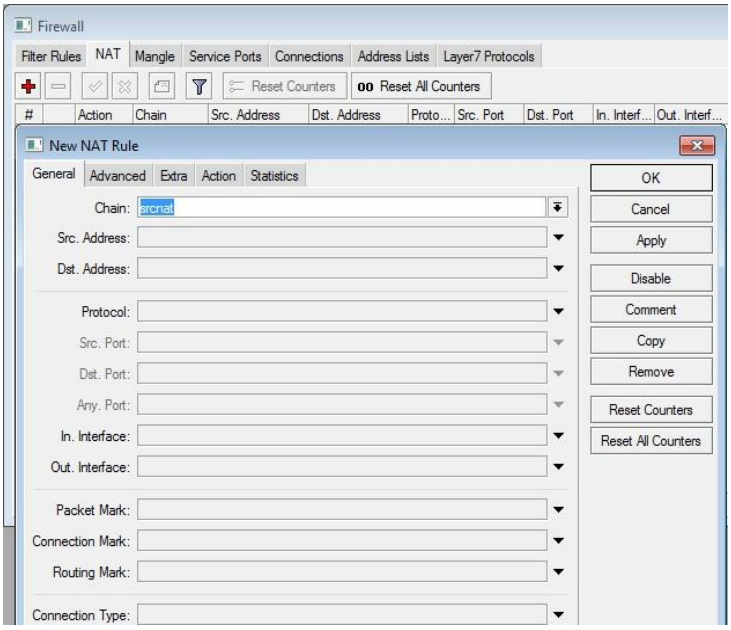


Gráfico 3.11: Creación de reglas NAT.

Las reglas de *NAT* tienen diferentes acciones que se pueden utilizar dependiendo de las necesidades para cada uno de los casos o aplicaciones.

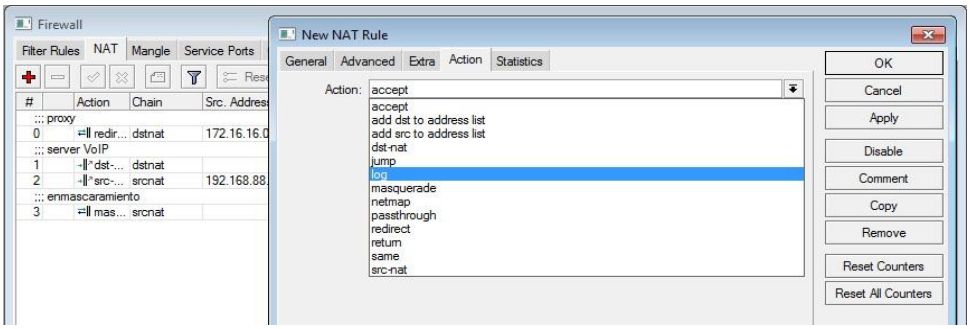


Gráfico 3.12: Acción de la regla de NAT.

3.5.3. Mangle.

Este módulo permite marcar los paquetes de IP de manera especial para poder darles un tratamiento interno. Estas marcas son usadas dentro de otros módulos del *router* como pueden ser el ruteo o para brindar calidad de servicio en una red.

Adicionalmente la funcionalidad Mangle permite modificar ciertos campos en el encabezado del paquete IP como el TTL, TOS (ó DSCP), aquí encontramos 5 cadenas por defecto las cuales mostramos a continuación:

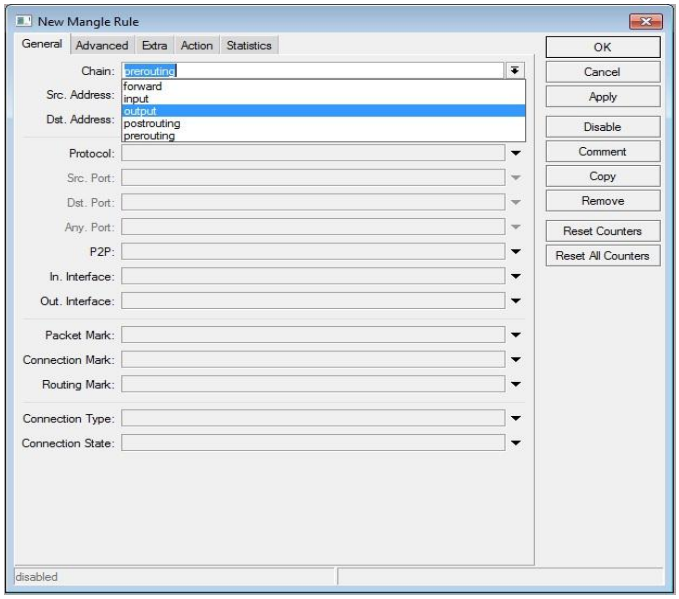


Gráfico 3.13: Creación de Reglas de Mangle.

Para poder hacer una breve descripción de la manera que trabajan las cadenas en el Mangle es necesario revisar adicionalmente la estructura que este tiene:

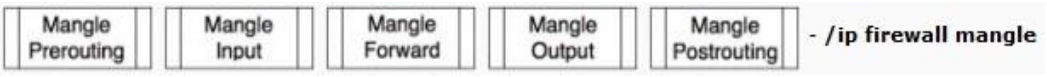


Gráfico 3.14: Flujo Ip firewall mangle simplificado.

El flujo de paquetes tiene el siguiente orden que se muestra a continuación:

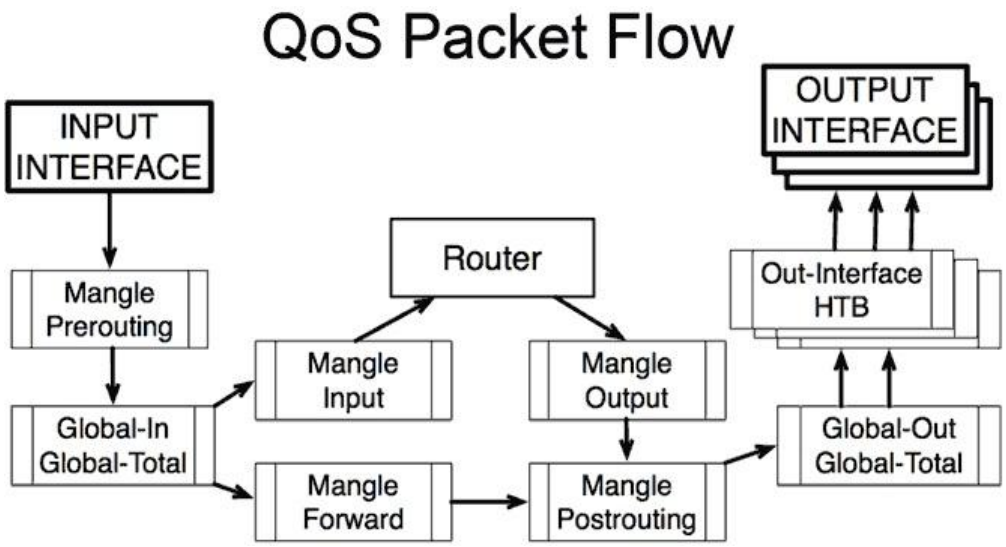


Gráfico 3.15: Flujo Ip Firewall Mangle.

3.5.3.1. Prerouting.

El lugar más común donde están las reglas del mangle, que permitirá aplicar marcas a los datos que fluyen a través del *router* antes de encolar en Global-in, así de esta manera podrá el *router* determinar qué acción realizar.

3.5.3.2. Postrouting.

Encontramos todos los paquetes que salen del router y de esta manera se realizar cambios al encabezado del paquete, como por ejemplo modificar el bit TOS del paquete o cambiar el tamaño del TCP MSS (Tamaño Máximo de Segmento), esto se realiza antes de encolar en *Global-out*.

3.5.3.3. Input.

La cadena de entrada en el Mangle es la misma que la del *FirewallFilter*, estos son los paquetes que están destinados al *router*, un ejemplo puede ser cuando se realiza un ping al *router,* entonces podremos dar un tratamiento a estos paquetes si utilizamos la cadena input. La marca se realiza justo antes del filtro de *Input.*

3.5.3.4. Forward.

De igual manera trabaja como la cadena *Forward* del *Firewall Filter*, pudiendo dar un tratamiento también a los paquetes que únicamente atraviesan el *router* y su marca se hace antes del filtro *Forward.*

3.5.3.5. Output.

Aquí se pueden tratar los paquetes que son generados por el *router* los cuales van a ser enviados a una interfaz, su marca se hace antes del filtro *output* y funciona de igual manera que la cadena de *Firewall Filter*.

Debemos tomar en cuenta que las marcas que se realizan en cualquiera de las cadenas del Mangle serán muy importantes y forman parte fundamental de esta tesis, ya que dependerá del marcado para su oportuno tratamiento a todos los paquetes, generalmente las marcas más utilizadas son: el Marcado de Conexión, Marcado de Paquetes y Marcado de Rutas, todas las marcas generalmente deben ser

complementadas con una segunda funcionalidad de los RouterOS como puede ser con el módulo de *Queue* (Colas) que describiremos a continuación.

3.5.4. Queues.

3.5.4.1. Simple Queues.

Simple *Queues* o Colas simples son utilizadas para el control de ancho de banda, estas permiten tener un control simplificado de la asignación de velocidad a una dirección ip o a una subred de manera sencilla.

La creación de colas simples en gran número afectan directamente el desempeño del *router*, cada vez que aumentan colas simples se ve afectado el proceso del CPU, debido a que este tipo de colas realiza su control en forma estrictamente secuencial donde todos los paquetes deben pasar por cada cola hasta que se cumplan las condiciones, ejemplo: si existen 1000 colas la última tendrá que esperar que haya pasado por las 999 colas anteriores para poder cumplir la condición.

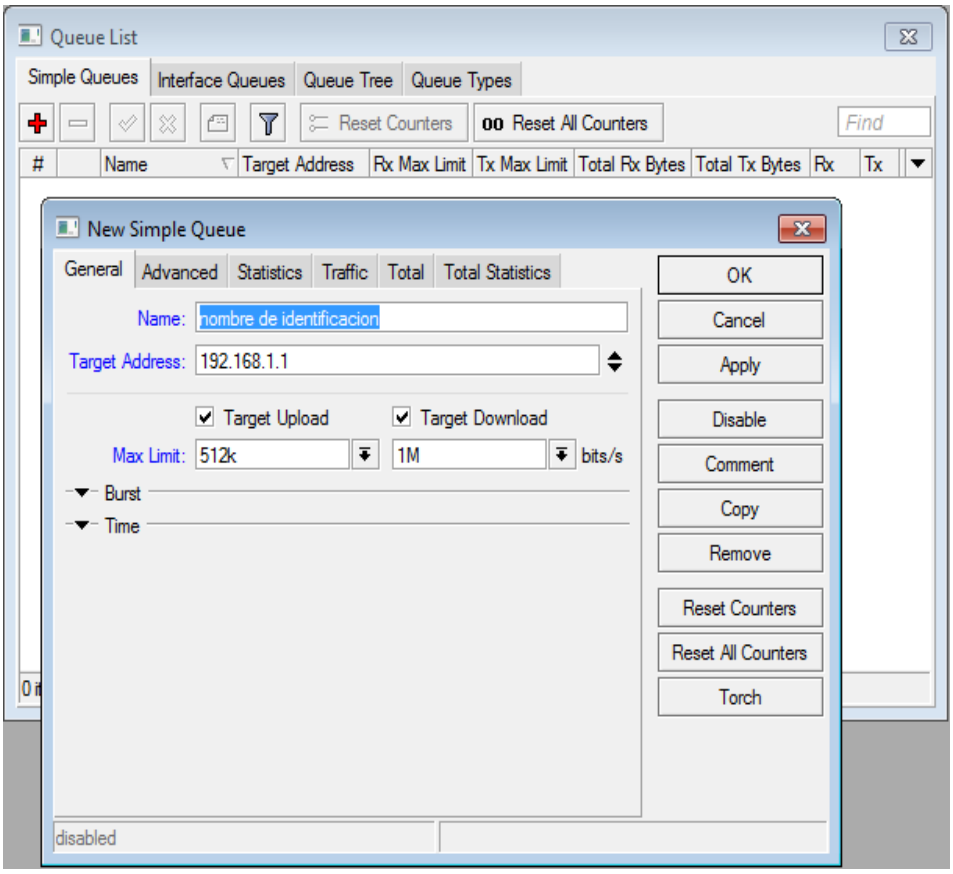


Gráfico 3.16: Creación cola simple.

Como se puede ver en el gráfico el campo *Name* le damos un nombre de identificación, *Target Address*(dirección de destino) puede ser de opción multiple ya que podrá tener la ip o subred a la cual se controlará el ancho de banda, en el *Max Limit* existen dos campos que son: Subida y Descarga en los que se asigna independientemente la velocidad para cada uno de estos.

Además es posible también realizar tratamiento adicional entre los que nombramos: garantizar ancho de banda, priorizar la ip o subred, agrupar, controlar ancho de banda por interface o destino.

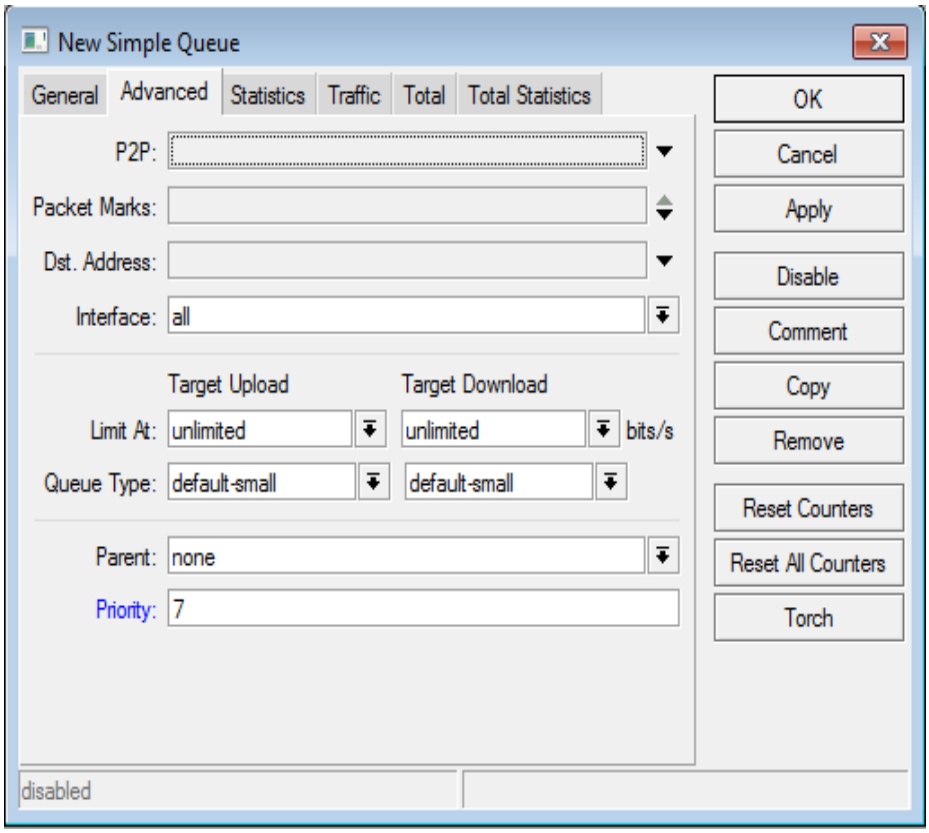


Gráfico 3.17: Propiedades Avanzados de colas simples.

Prioridad.- Este campo está por defecto en 8 siendo esta la prioridad menor hasta llegar a 1 que es la máxima prioridad.

Parent.- Aquí se indica si esta cola pertenece alguna cola padre, esto permite elegir si la cola va o no a pertenecer a un grupo como puede ser el caso de usuarios con 512kbps.

Limit At.- Permite garantizar los anchos de banda de subida y bajada independientemente a cada cola creada, tomando en cuenta que jamás puede ser esta mayor a la velocidad asignada.

Interface, *Dst. Address*.- En este campo se podrá elegir a que interfaz o destino estamos limitando el ancho de banda según la cola.

Las demás pestañas que muestra esta ventana de Simple Queues son informativas del comportamiento de la Cola donde se muestra las estadísticas y tráfico.

3.5.4.2. *QueueTree.*

QueueTree o Arbol de Colas es una implementación de HTB que solo trabaja en una dirección, es la única manera de separar el control de las interfaces y facilitar la configuración del Mangle ya que no es necesario realizar dos marcas diferentes para subida y descarga; todas las colas dentro del árbol son procesadas al mismo tiempo lo cual todo el proceso se lleva con mayor agilidad que en las colas simples.

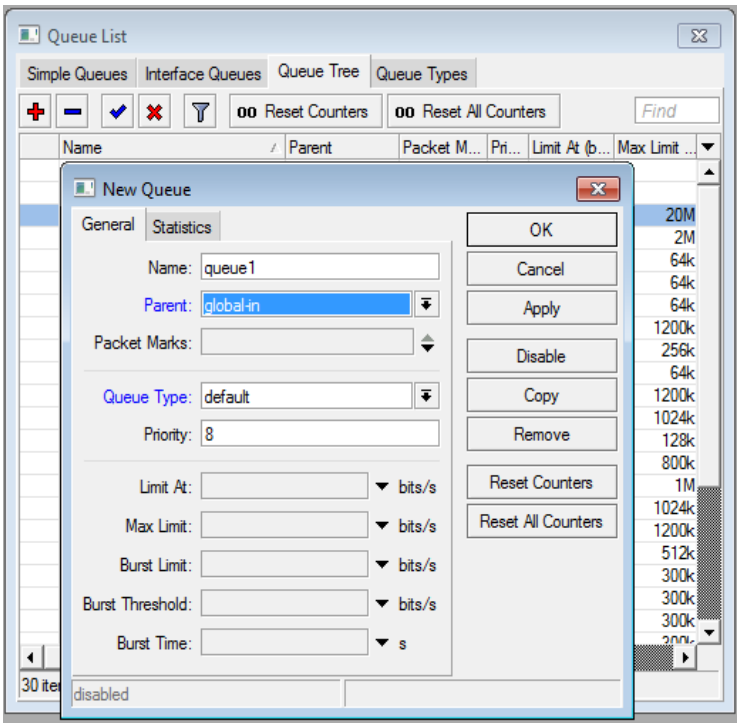


Gráfico 3.18: Arbol de colas.

Detallaremos los calores que se llenan en los campos: *Name* se le asigna una breve descripción de la cola, *Parent*: en el caso de tener una cola padre aquí indicamos cual es la que corresponde, *Packets Marks*: muestra una lista donde elegimos la marcas que se han dado en */Ip/Firewall/Mangle*.

Generalmente se configura un padre para la interfaz WAN y otra para la LAN, a estas van relacionadas todas las demás colas hijas que llevaran las diferentes marcas dependiendo del criterio para el cual son creadas.

3.5.4.3. Queue Types.

En RouterOS se encuentrar cinco diferentes tipos de colas que son: PFIFO, BFIFO, RED, SFQ y PCQ.

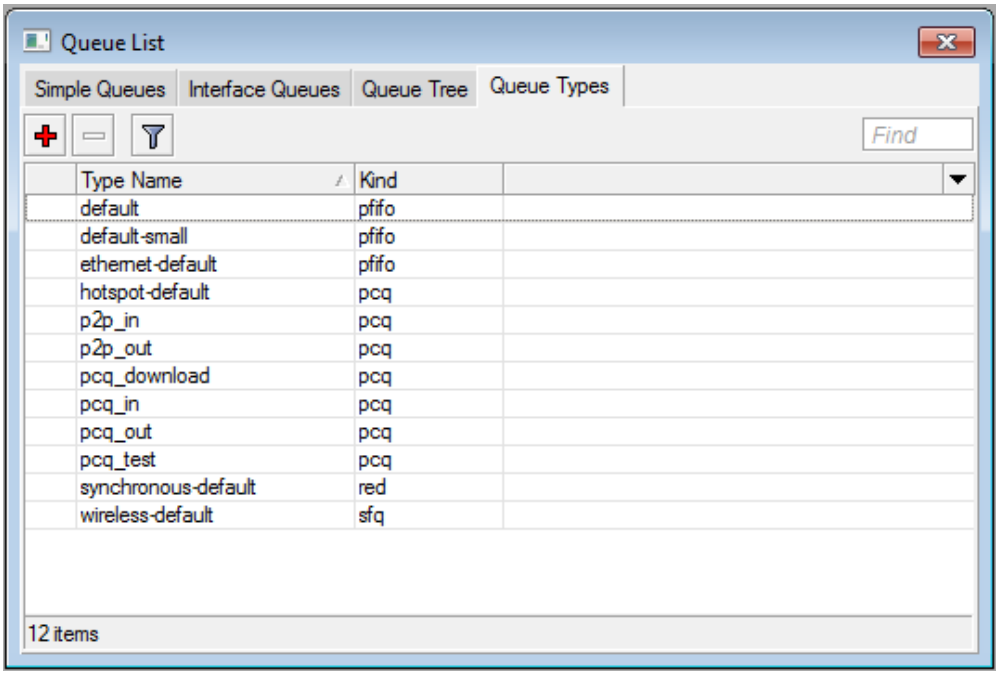


Gráfico 3.19: Tipo de colas.

3.5.4.3.1. PFIFO y BFIFO.

Este tipo de cola está básicamente fundamentado en el algoritmo Primero en entrar, primero en salir con la única diferencia que el uno se mide en paquetes y el otro en bits.

Uno de sus usos puede ser la limitación y control de Ancho de Banda de la manera más sencilla y rápida, una de las desventajas es que si la cola está llena el siguiente paquete será bloqueado o descartado, además los grandes tamaños de las colas aumenta la latencia.

3.5.4.3.2. Red.

Este es un mecanismo que procura evitar la congestión de la red a través del control del tamaño de la cola, cuando el tamaño está llegando a su umbral este inicia a descarta los paquetes de manera aleatoria.

3.5.4.3.3. Sfq.

Su funcionamiento está garantizado por métodos como el algoritmo *round-robin* donde el flujo de tráfico puede ser identificado únicamente por cuatro opciones: dirección origen, dirección destino, puerto origen y puerto destino, estos parámetros son utilizados por el algoritmo de Hash para clasificar los paquetes de uno de los 1024 posibles sub flujos. Luego de esto el algoritmo de *round-robin* iniciara la distribución del ancho de banda disponible para todas los sub flujos.

Todas las colas SFQ pueden contener 128 paquetes y estos 1024 sub corrientes disponibles.

Es una de las mejores opciones para proporcionar QoS ya que permite hasta 16 niveles de colas, aunque su desventaja es la del consumo de CPU.

3.5.4.3.4. Pcq.

Se puede decir que su principio se basa en SFQ, pero con características adicionales en las que se eligen identificadores de flujo como: dirección origen, puerto origen o dirección destino y puerto destino.

Es posible asignar velocidad de limitación a los sub flujos de manera equitativa o configurar bajo su propio criterio.

Un ejemplo seria el considerar que todos los usuarios compartan equitativamente el ancho de banda dentro de una oficina.

3.5.5. Herramientas de Manejo de Red.

RouterOS cuenta con algunas herramientas que sirven y facilitan la administración de una red, entre las de mayor relevancia están las siguientes:

3.5.5.1. Watchdog.

O perro guardián en español; esta herramienta puede cumplir dicha función en dos diferentes modos, en modo hardware con todos los router boards o en un sistema x86 en modo software.

Su funcionamiento se lo puede explicar de manera sencilla, cuenta con un temporizador de vigilancia que será el encargado de reiniciar el sistema si este ha fallado en varias ocasiones sin emitir respuesta de ping.

Antes de reiniciar este crea además un archivo de soporte que puede ser enviado por correo siempre y cuando tengamos previamente definido un e-mail.

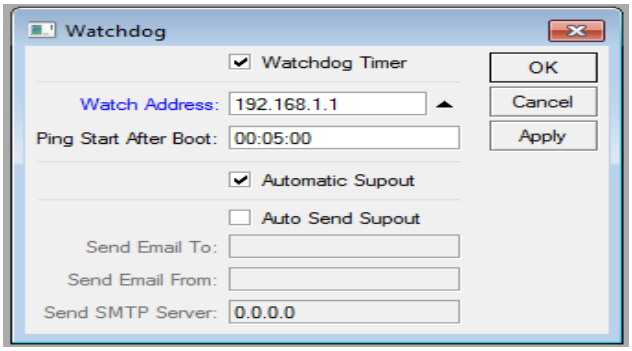


Gráfico 3.20: Herramienta Watchdog.

3.5.5.2. Bandwidth Test Client.

Permite realizar mediciones de ancho de banda entre el cliente y un servidor, para lo cual será necesario como mínimo conocer la dirección ip del servidor de prueba teniendo que colocar además el nombre de usuario y contraseña si fuese necesario.

Se encuentra también la opción de indicar cuál será el tamaño y tipo de paquete udp o tcp, el sentido de la dirección es otra de las opciones que se pueden configurar, pudiendo utilizar enviar, recibir o ambas a la vez.

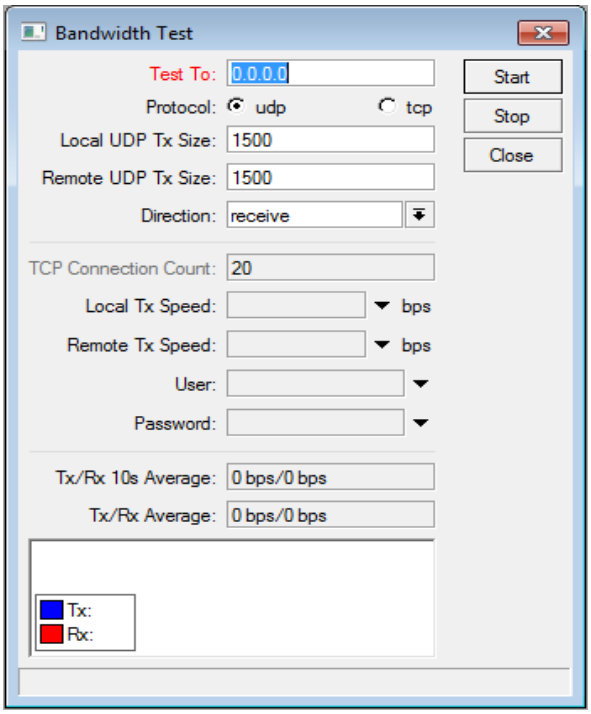


Gráfico 3.21: Herramienta Bandwidth Test.

3.5.5.3. E-Mail System.

E-Mail System es una función que permite enviar mensajes de correo electrónico basado en los sucesos dentro del RouterOS.

Es necesario configurar las opciones de correo y utilizar también la secuencia de comandos o scripting para así de esta forma conseguir notificaciones y alertas del sistema.

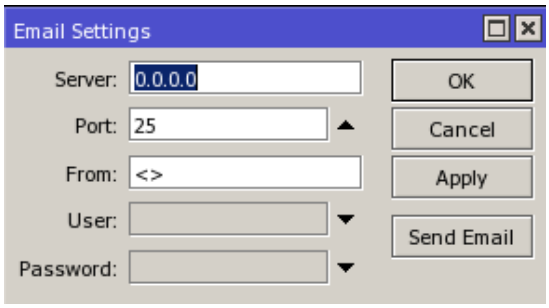


Gráfico 3.22: Configuración de Email

3.5.5.4. *Netwach*

Es una herramienta que permite monitorear los diferentes dispositivos de la red por medio del ping generando eventos en el cambio de estado de los mismos, permite tomar acciones ante los posibles sucesos que se puedan presentar.

La ejecución de comandos de consola o scripts son la manera de alertar ante cualquier eventualidad en el cambio de estado.

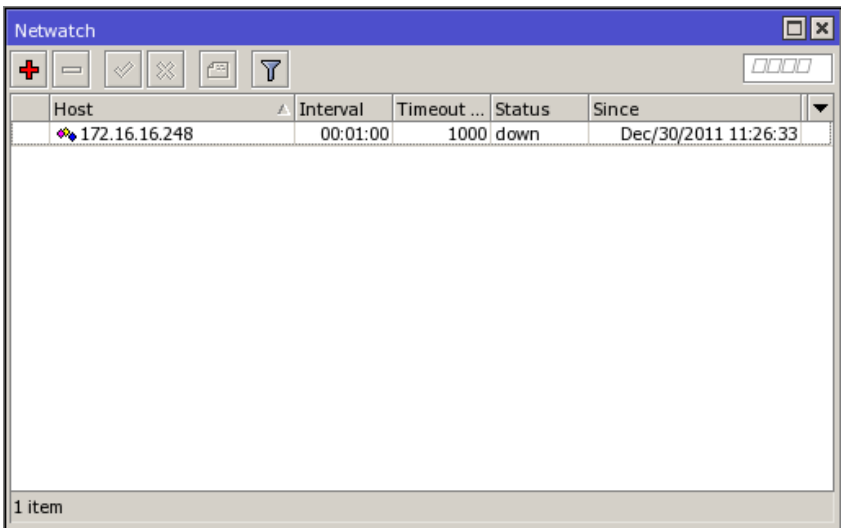


Gráfico 3.23: Herramienta Netwach.

Esta herramienta está dentro del menú Tools y para la creación de una nueva regla iniciamos dando click en el signo más.

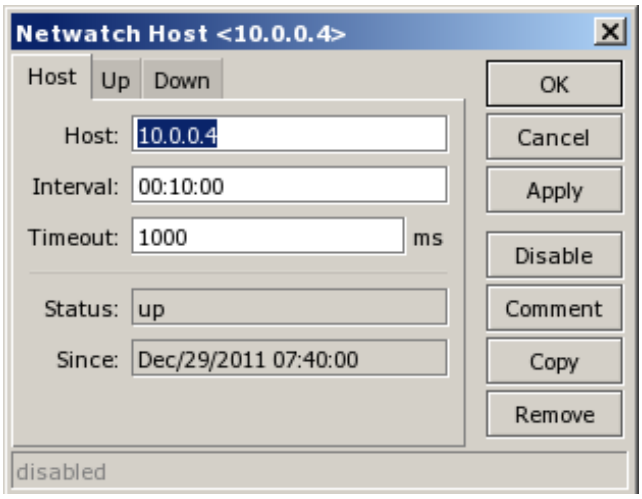


Gráfico 3.24: Creación de una regla en Netwatch.

Host.- Es la dirección ip del dispositivo que se desea monitorear, para el ejemplo se utilizará la dirección ip de un Access Point donde se sabrá si esta fuera de línea o está trabajando normalmente.

Interval.- Es el tiempo que se define para verificar el estado del dispositivo monitoreado.

Timeout.- Tiempo fuera es un valor en milisegundos el cual si es superado se considera como down o fuera.

Status.- Mostrara el estado del dispositivo actual.

Since.- Indica el mes, día, año y hora exacta desde el último cambio de estado.

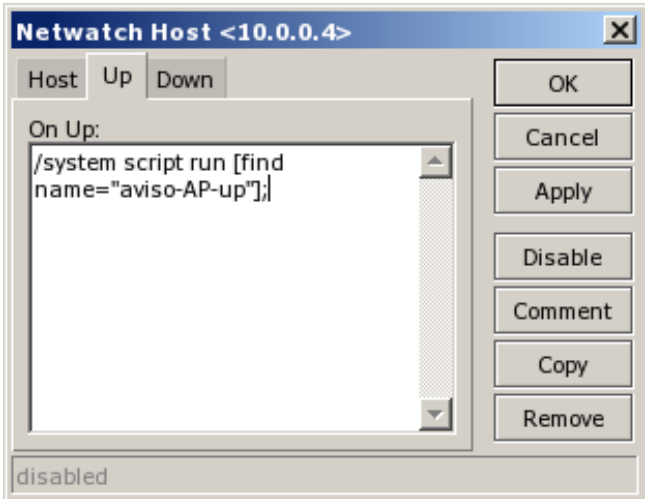


Gráfico 3.25: Acción en el estado Up.

Se puede observar que existen dos pestañas que son *Up* y *Down*, aquí se indicara en cada uno de los estados cual será la acción a realizar.

En este caso para cuando el estado es *Up* está configurado que ejecute un script con el nombre “aviso-AP-up”

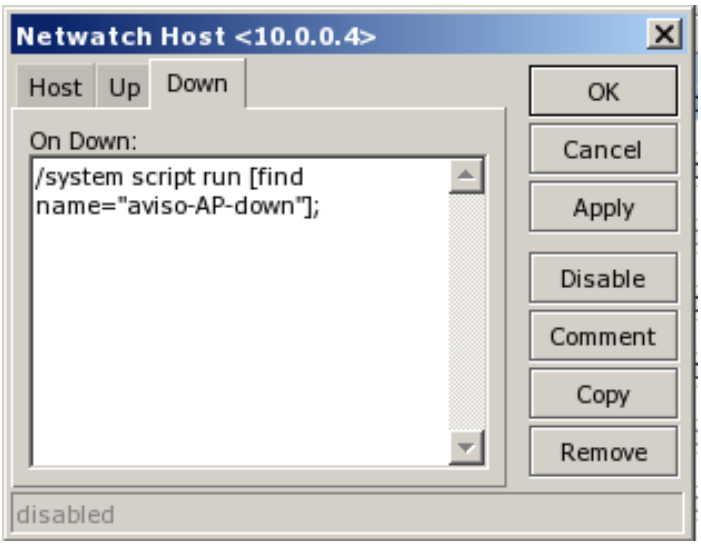


Gráfico 3.26: Acción en el estado Down.

En la pestaña *Down* se ha configurado que al no tener respuesta o exceder del tiempo establecido en *timeout* se ejecute otro script llamado "aviso-AP-down"

3.5.5.5. Script

Son archivos de órdenes, instrucciones o procesamientos por lotes almacenados en un archivo que se crean por el usuario para simplificar alguna tarea repetitiva, la opción de script la encontramos dentro del menú *System*, aquí se mostrara un listado completo de todos los scripts que tengamos creados en el *router*.

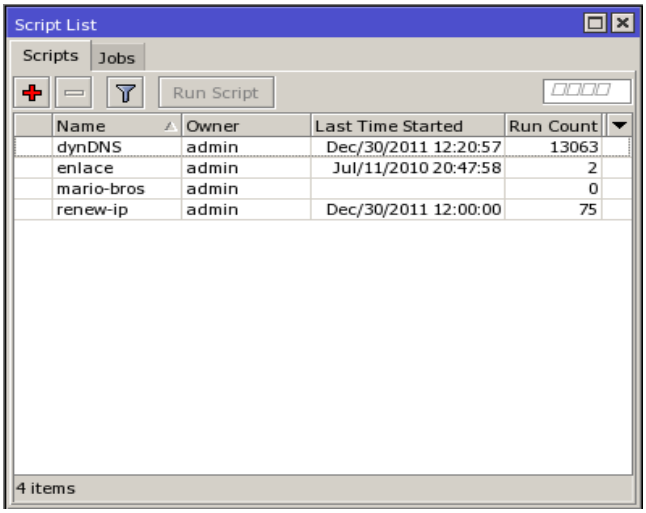


Gráfico 3.27: Sistema de Script.

En esta ventana se muestra información como el nombre del *script*, usuario que lo creo, fecha de la última vez que se ejecutó y un contador del número de veces que se ha ejecutado esta acción.

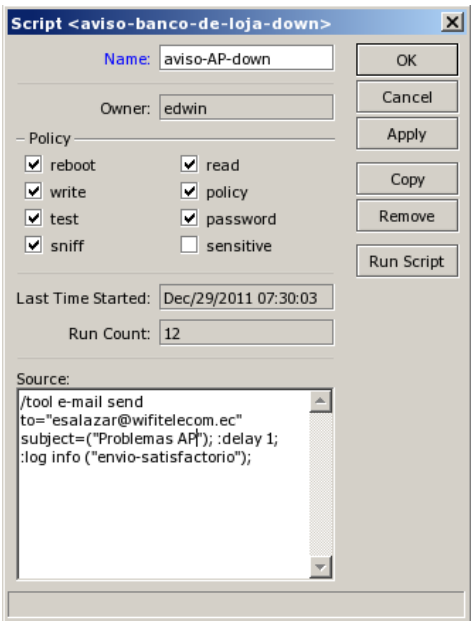


Gráfico 3.28: Creación de un script.

En la creación de todo *script* se pueden ver las siguientes opciones que se deben configurar: un nombre que tendrá el script, el usuario que lo está creando, y definiremos las políticas que serán aplicadas a este.

En este caso el código que está dentro del script creado permitirá enviar un correo electrónico como aviso del estado de un ap que se encuentra monitoreado.

3.5.5.6. Reportes MRTG (*Graphing*).

Es quizá una herramienta muy importante que permitirá saber de manera rápida y eficaz el uso de los recursos del sistema, además también es posible visualizar el consumo de interfaces y colas simples del RouterOS.

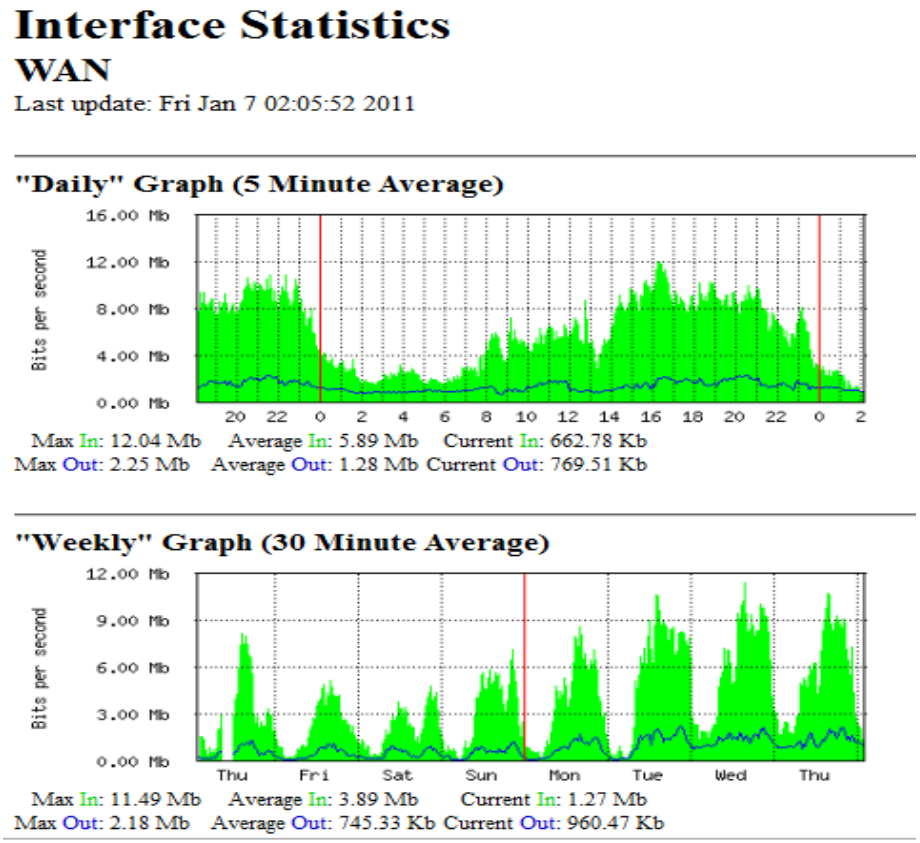


Gráfico 3.29: Herramientas de Gráficos de consumo.

CAPITULO 4

4. Manual de Instalación y Configuración de QoS en RouterOS

QoS forma parte muy importante de la mayoría de grandes redes existentes lo cual ha permitido mejorar eficientemente los servicios, es por eso que se ha venido trabajando continuamente en una mejora.

En la actualidad es necesario implementar QoS ya que cada día se incrementa el tráfico en todas las redes y esto obliga a que todo ambiente sin diferenciación busque una mejora en la agilidad con la que trabaja.

La rapidez ya no solo depende de los estándares físicos que se aplican a los equipos sino también de QoS que complementa los servicios y la calidad de los mismos.

QoS puede ser implementado en una variedad de productos que van desde productos propietarios que incluyen hardware y software como también soluciones gratuitas de código abierto comúnmente utilizadas bajo sistemas operativos GNU.

El escenario seleccionado para realizar la instalación y configuración es la red Wireless de la Universidad del Azuay, la versión del Sistema Operativo utilizado en este caso es RouterOS V.5.7.

Para proceder con la instalación de RouterOS en una pc es necesario tener los siguientes elementos: Cd de instalación de la última versión de RouterOS que se puede descargar de la página en línea, Monitor y Teclado.

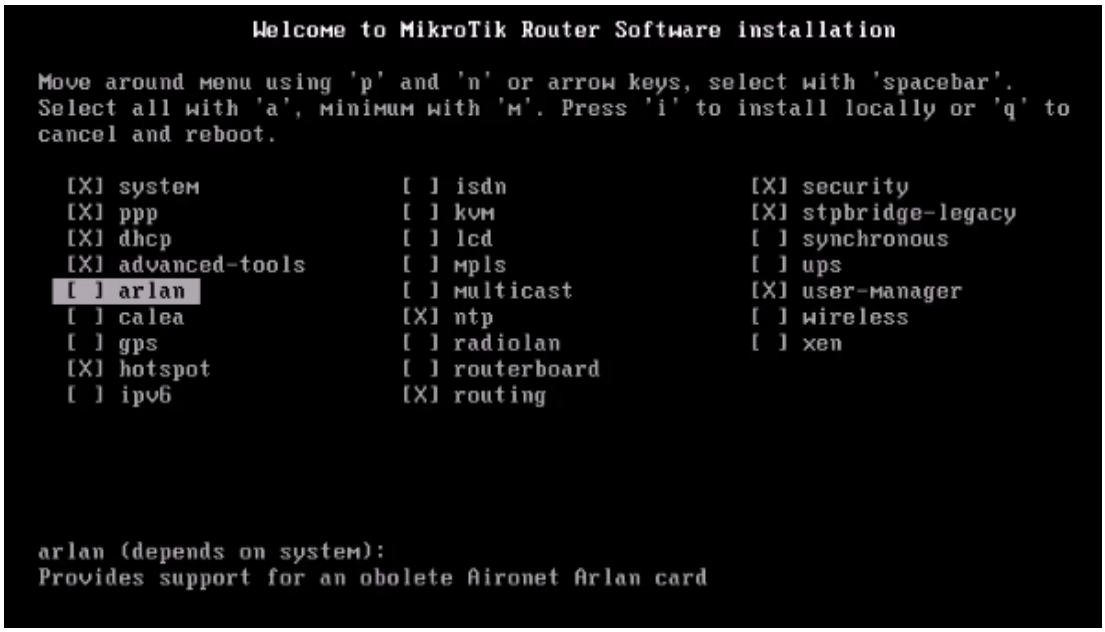


Gráfico 4.1: Selección de paquetes en la instalación de RouterOS.

Al bootear con el disco de instalación se tendrá la pantalla que se muestra en el gráfico 4.1, donde se puede seleccionar los paquetes y a continuación se presiona la "i" para proceder con la instalación.

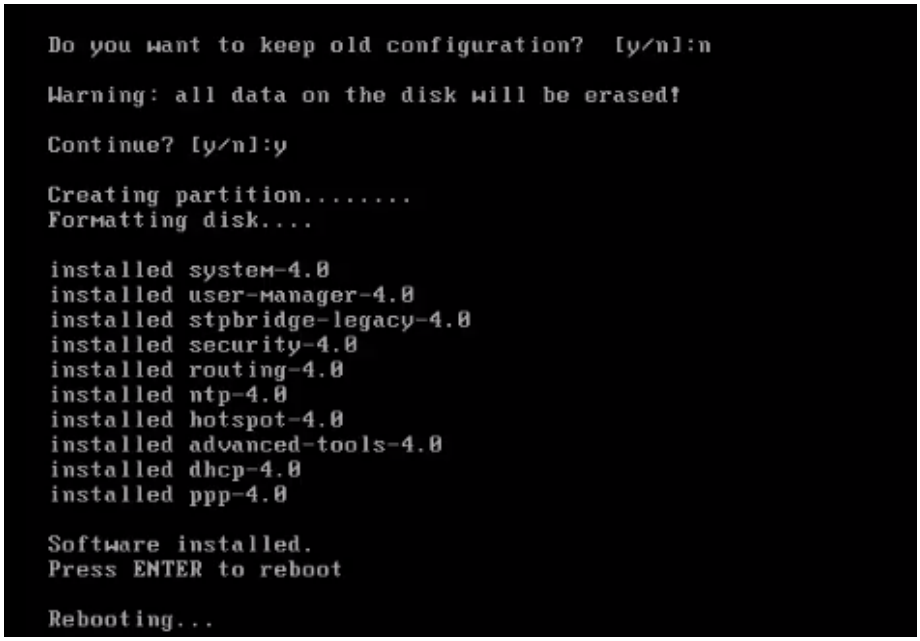


Gráfico 4.2: Proceso de instalación.

A continuación se tiene que responder a la pregunta: "Desea mantener la configuración antigua?" esto será válido en el caso de hacer una reinstalación, en este caso se elige "n"

La instalación solicita una confirmación de parte del usuario indicando que todos los datos en el disco serán borrados, en este caso se responde "y"

Se procede con la instalación y se debe esperar el mensaje solicitando que presione ENTER para reiniciar.

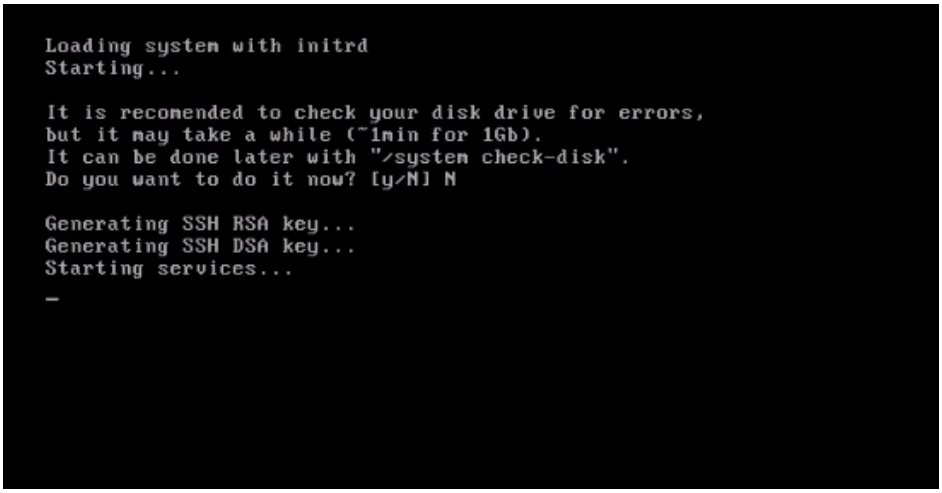


Gráfico 4.3: Chequeo del disco y generación de llaves.

Con el reinicio se solicita la aprobación para chequear el disco y automáticamente se generan las llaves SSH RSA y SSH DSA.

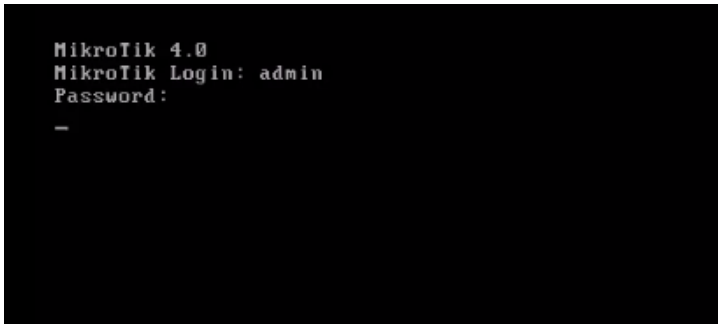


Gráfico 4.4: Pantalla de ingreso.

La pantalla general desde este momento será la de ingreso al RouterOS donde se verifica el usuario y clave; el usuario es admin y no tiene clave.

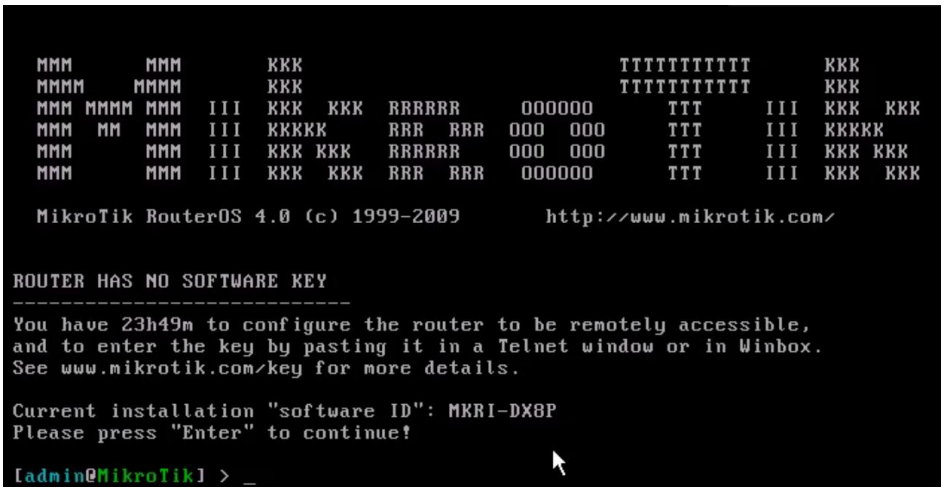


Gráfico 4.5: Interface de Comandos RouterOS.

Una vez validado el ingreso a Mikrotik se observa un mensaje indicando que el router no tiene una licencia y nos muestra el "software ID" que sirve para registrar la licencia que se adquiera.

4.1. Configuración de RouterOS

Antes de iniciar la configuración del *router* debemos realizar un esquema gráfico que facilita el progreso y comprensión de las actividades que se van desarrollando.

El primer paso en este proceso es identificar cuáles serán las interfaces que se utilizaran, direcciones ip que se asignan y subredes que utilizaremos, de esta manera se podrá iniciar correctamente y con una visión clara de los resultados que se buscan.

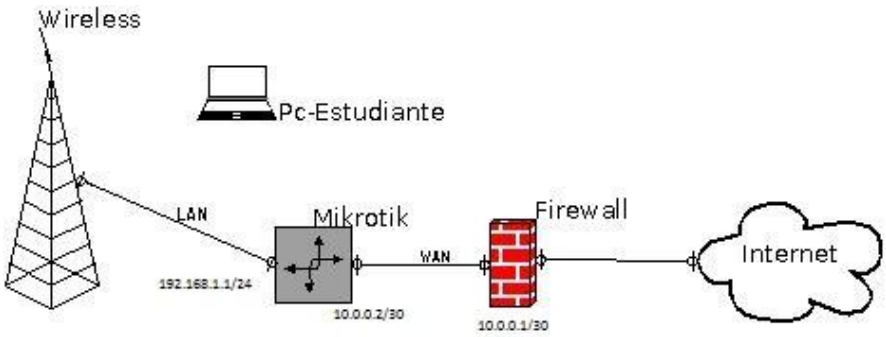


Gráfico 4.6: Esquema de red.

En este caso utilizaremos como base el diagrama presentado, y el direccionamiento lo detallaremos a continuación:

INTERFACE	RED	MASCARA	BROADCAST	DESCRIPCION
WAN	10.0.0.0	255.255.255.252	10.0.0.3	Conexión al Proveedor
LAN	192.168.1.0	255.255.255.0	192.168.1.255	Direcciones asignadas a Estudiantes

En el Capítulo 3 se indica la manera de ingresar por los diferentes métodos para poder administrar e iniciar la configuración de RouterOS, en este caso lo realizaremos por su interfaz gráfica WINBOX.

4.2. Asignación de Nombres a Interfaces y Direccionamiento.

En el menú principal del lado izquierdo dentro del Winbox elegimos la opción Interfaces la cual mostrará la lista de interfaces físicas y lógicas dentro del *Router*:

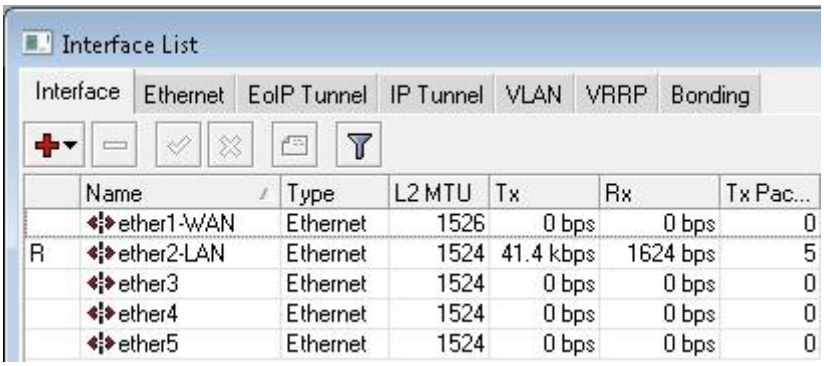


Gráfico 4.7: Interfaces RouterOS.

Aquí se puede cambiar nombres de las interfaces, velocidad a la que estas trabajarán y negociación, también es posible comentar a cada una de las interfaces para lograr tener un mejor orden e identificación de conexiones.

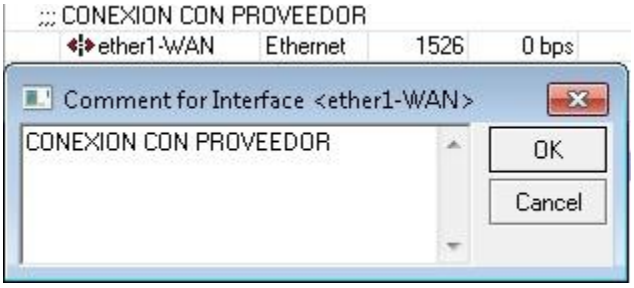


Gráfico 4.8: Agregar comentario a una interface.

La asignación de direcciones ip se la realiza en el menú IP > ADDRESS> +, es aquí donde a las interfaces renombradas y comentadas le designaremos su dirección IP, ya en este caso para la red WAN asignada por el proveedor así como también para la red interna que fue definida anteriormente.

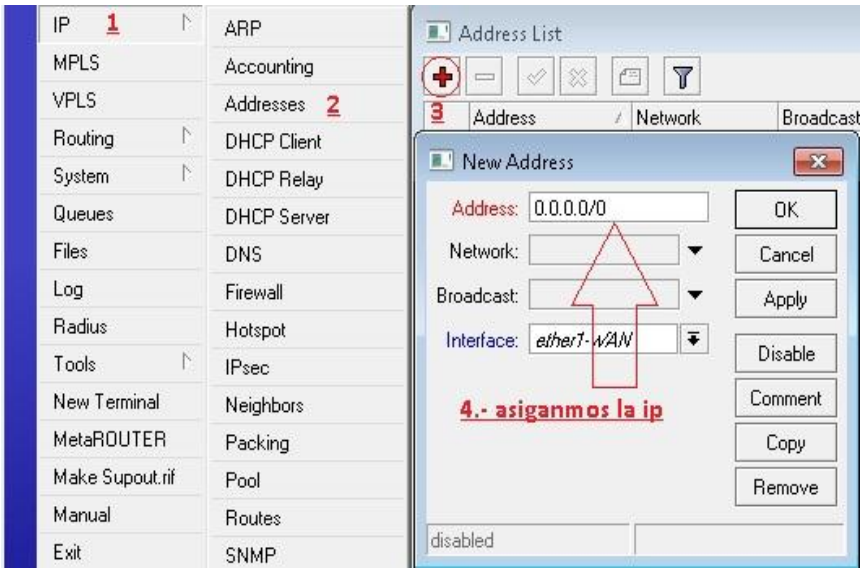


Gráfico 4.9: Asignacion de direccion IP.

En este caso se utiliza para la interfaz WAN la dirección IP: 10.0.0.2/30 y para la LAN se utilizara la IP: 192.168.1.1/24

4.3. Creación de la Ruta por defecto, Enmascaramiento y asignación de DNS.

4.3.1. Ip Routes.

Procedemos a la creación de la ruta que se utilizar por defecto para tener salida al mundo, esto lo haremos en la opción IP > ROUTES > +, en caso de ser necesario podremos agregar rutas personalizadas para otros servicios:

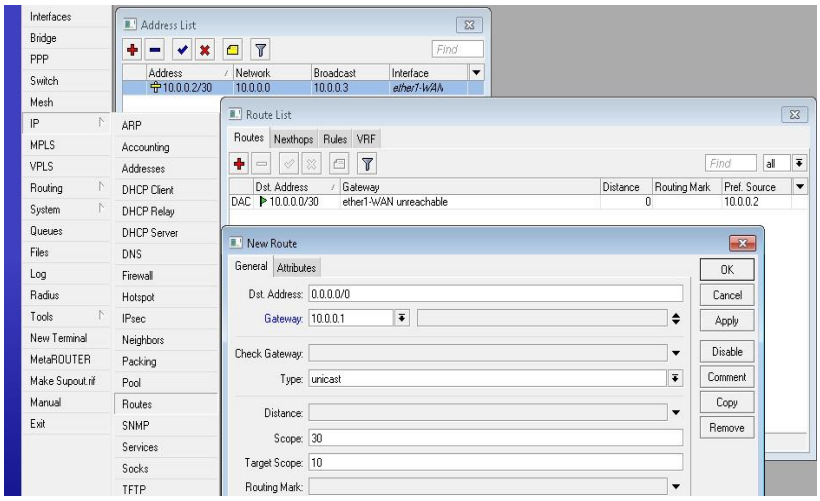


Gráfico 4.10: Asignacion de ruta por defecto.

4.3.2. Ip Dns

Ahora se asignan los DNS que serán los encargados de la resolución de nombres, esto generalmente es proporcionando por el proveedor pero alternativamente se puede utilizar DNS públicos como los de Google u OpenDNS: 8.8.8.8 - 208.67.222.222, la opción esta en el menú de: IP > DNS > SETTINGS.

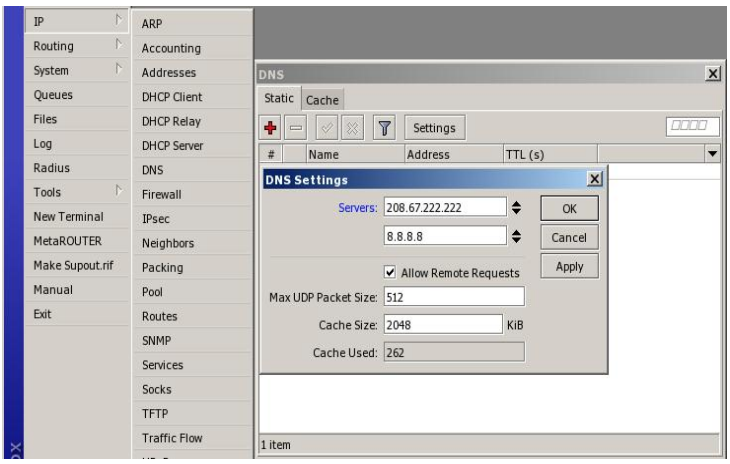


Gráfico 4.11: Asignación de servidores DNS.

4.3.3. Ip Firewall Nat.

Ahora en la opción IP > FIREWALL > NAT, se procede con el enmascaramiento de la red, para esto se utiliza la acción de MASQUERADE que es una forma especial de SRC-NAT en RouterOS la cual permite que todo el grupo de la red tenga salida al mundo con una sola IP Publica, en el chain utilizamos SRC-NAT, en OUT INTERFACE se utilizará la interfaz de salida que para el caso es ether1-WAN, por último en action seleccionamos MASQUERADE.

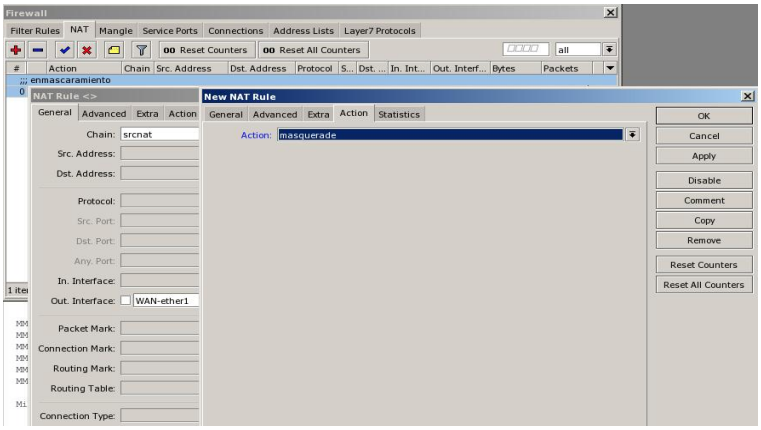


Gráfico 4.12: Enmascaramiento de la red.

4.4. Servidor y Cliente DHCP.

RouterOS tiene la funcionalidad de ser un múltiple servidor DHCP (Protocolo de configuración dinámica de host), lo cual permite la fácil distribución de direcciones IP en la red.

Algo muy importante es que únicamente se debe tener un servidor DHCP por cada interfaz, en el caso de las interfaces que forma parte de un *Bridge* el servidor DHCP va en la interface lógica porque no es posible hacerlo en las físicas que están dentro del mismo.

La configuración de este servicio es muy simple y la manera más adecuada de hacerlo cuando no se tiene mayor conocimiento es utilizando el mago de configuración (*wizard*) que mostraremos:

4.4.1. Servidor DHCP.

Antes de iniciar con la configuración del Servidor DHCP primero definimos una dirección IP La opción del DHCP-Server está ubicado dentro de la opción IP.

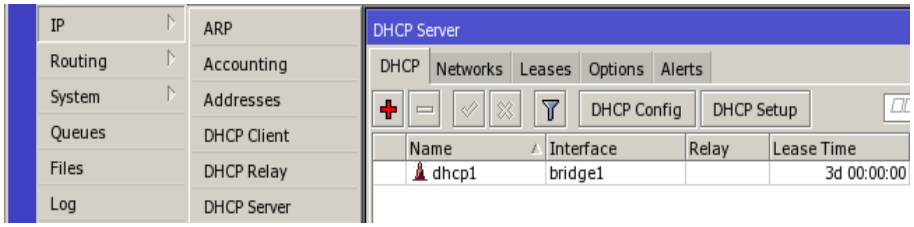


Gráfico 4.13: Servidor DHCP.

Para iniciar el asistente de configuración damos *click* en el botón DHCP *Setup* y se muestra lo siguiente:

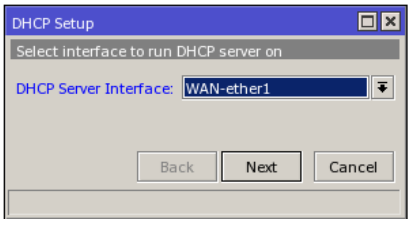


Gráfico 4.14: Selección de interface.

Aquí indicamos la interface en la que necesitamos activar el servicio del DHCP, sin olvidar que es posible tener un servidor DHCP por cada red e interface.

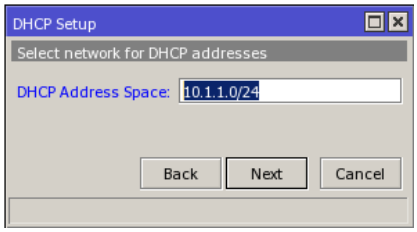


Gráfico 4.15: Asignación de red para el pool DHCP.

Seleccionamos la red que utilizará el servidor para la asignación de direcciones en la red, para el ejemplo utilizamos la red 10.1.1.0/24 y damos *click* en *next*.

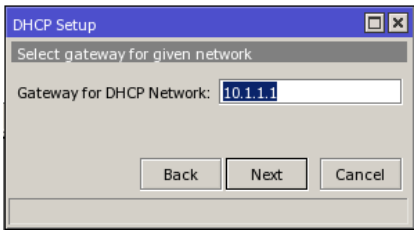


Gráfico 4.16: Asignación puerta de enlace para pool DHCP.

Definimos el *gateway* que utilizará la red que es generalmente la ip del *router* que se encuentra en esta misma interfaz.

En la siguiente opción ingresamos la dirección IP del servidor DHCP Relay (Servidor DHCP Externo) en caso de que exista, caso contrario esta opción se oculta utilizando la flecha que resaltamos en el gráfico.

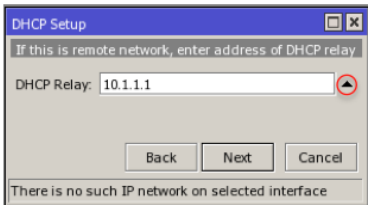


Gráfico 4.17: Asignación DHCP Relay.

Continuamos con el siguiente paso donde seleccionamos el rango de direcciones IP's disponibles para la asignación a los distintos usuarios. Por defecto el RouterOS utiliza toda la subred asignada en la interfaz únicamente dejando libre la dirección utilizada en el RouterOS.

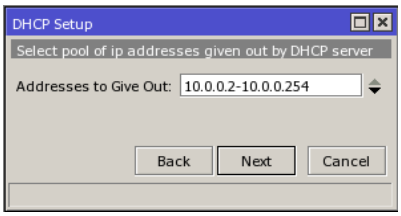


Gráfico 4.18: Ip's Disponibles para host.

Es recomendable reservar un segmento de toda la subred con al menos 20 direcciones IP´s que se podrán disponer de las mismas en caso de ser necesario para asignación estática a diferentes equipos o usuarios como pueden ser impresoras, servidores, etc.

Los servidores de DNS se definen automáticamente en el caso de tener habilitada la función del DHCP-CLIENT y de no ser así podremos definir manualmente el servidores de DNS que se encarga de resolver los nombres de Dominio.

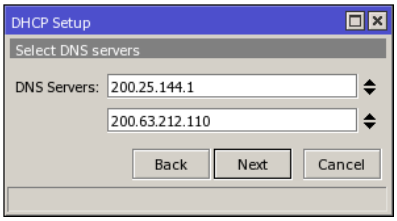


Gráfico 4.19: Servidores DNS para host.

El último paso en la configuración es definir el tiempo que permanecerá relacionado la mac con la dirección ip asignada, cuando este tiempo expira será necesario renegociar automáticamente una nueva solicitud para la asignación de otra dirección Ip.

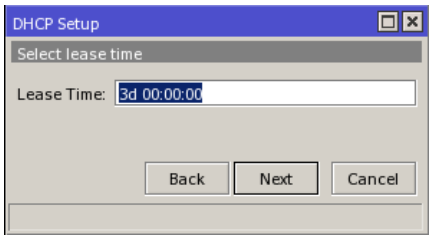


Gráfico 4.20: Tiempo de Vida para host.

Al configuran redes que tienen muchos usuarios transitorios es recomendable definir un tiempo de conexión de entre 2 y 3 horas para evitar dejar fuera de asignación a otros usuarios.

Estos son todos los pasos necesarios que permiten tener en funcionamiento un servidor DCHP.

4.4.2. Cliente DHCP.

RouterOS además de ser un servidor de DHCP también puede ser un cliente y la configuración es aún más simple, cabe indicar que no se produce ningun conflicto al utilizar estas dos funciones en un mismo RouterOS pero hay que tener cuidado de no levantar el servicio en la misma interfaz.

La opción para configurar el cliente dhcp es la siguiente:

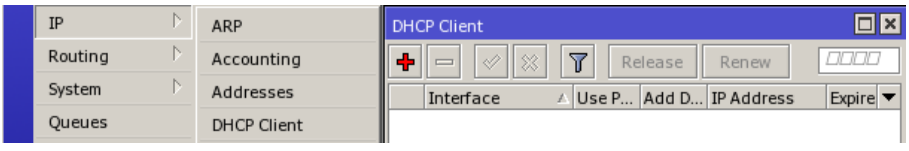


Gráfico 4.21: Cliente DHCP.

Habiendo ingresado en esta opción es necesario dar *click* en el signo más para adicionar una interfaz que será un cliente del DHCP.

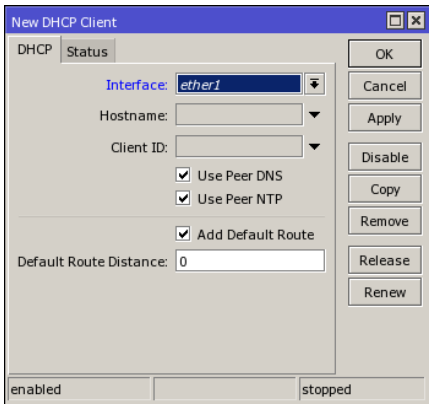


Gráfico 4.22: Asignación de interface cliente DHCP.

La interfaz configurada como cliente DHCP no recibe únicamente la dirección IP sino también la máscara de subred, configuración de los DNS, datos del servidor NTP y la ruta por defecto.

Estos valores están definidos para ser aceptados por defecto pero en caso de no ser necesario o querer cambiar la distancia de la ruta es aquí donde debemos hacerlo.

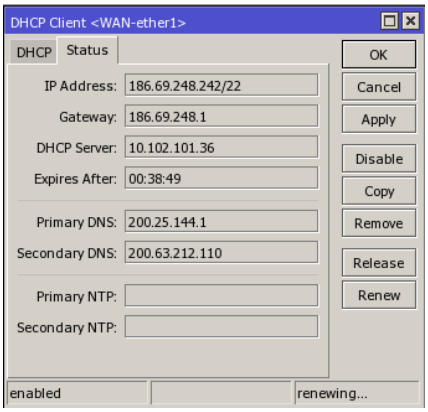


Gráfico 4.23: Estado cliente DHCP.

En la pestaña de status se observar información como la ip, tiempo restante para que expire dicha asignación, gateway, dns, ntp y cuál es el servidor DHCP.

4.5. Firewall en RouterOS

Mediante la utilización firewall podremos bloquear y restringir diferentes accesos no autorizados al *Router*.

4.5.1. Reglas y recomendaciones para proteger un *router*.

La creación de algunas reglas permitirán tener una protección básica de un *router*, aquí se puede incrementar y mejorar la seguridad según las necesidades.

4.5.2. Mac Server

Es utilizado para proporcionar acceso a un router a través de la dirección Mac mediante telnet o winbox, Mac telnet únicamente es posible realizar entre RouterOS, se utiliza también para configurar un router que no tenga dirección IP.

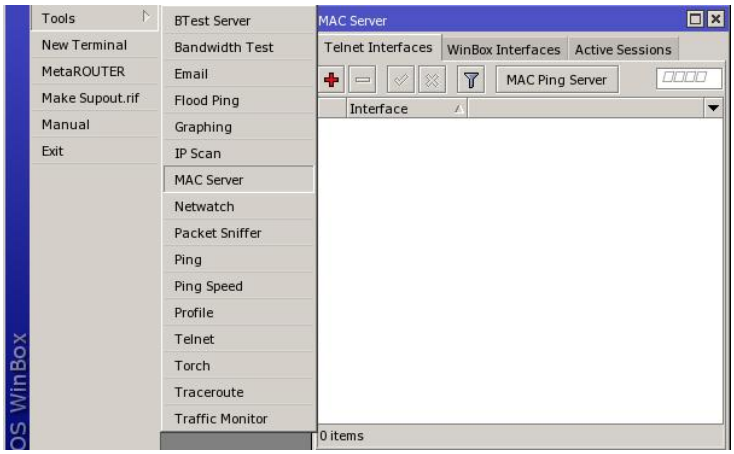


Gráfico 4.24: configuración Mac Server.

En la opción TOOLS > MAC SERVER, se debe configurar las interfaces en las cuales se permite accesos al equipo de diferentes formas como son: Telnet y Winbox, por defecto se tiene acceso de todas las interfaces, se recomienda cambiar esto y permitir solo a la interfaz de administración.

4.5.3. Ip Service List.

Muestra la lista de protocolos y puertos que RouterOS utiliza para distintos servicios, aquí es donde se verifica, deshabilita o se hace cambio de los puertos por defecto si es necesario.

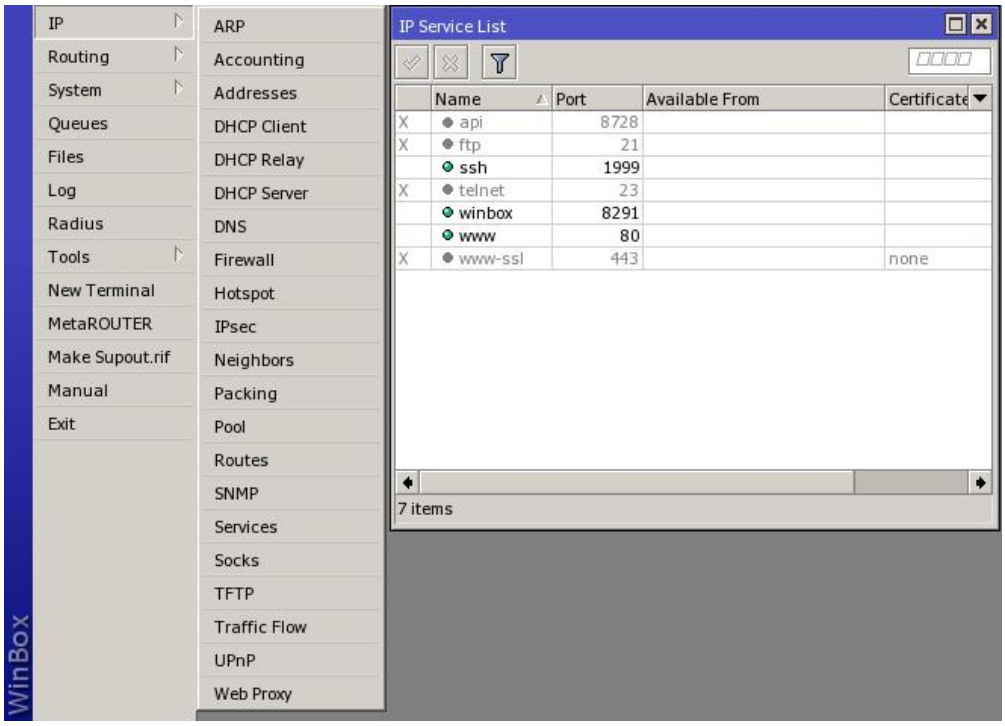


Gráfico 4.25: Puertos del RouterOS.

4.5.4. User.

Es donde se configuran los usuarios y permisos para acceso al RouterOS, la opción está en el menú System, se puede también crear nuevos grupos con diferentes políticas para cada uno de estos.

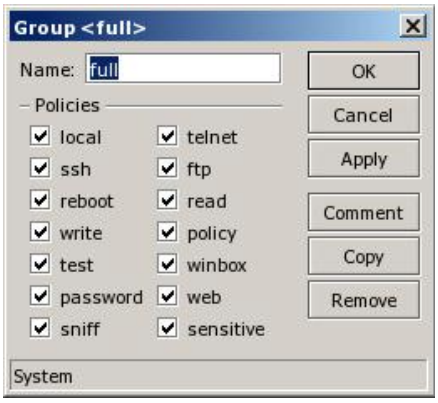


Gráfico 4.26: Permisos para usuarios.

El usuario por defecto es admin, el cual por seguridad lo renombraremos y será asignado un *password.*

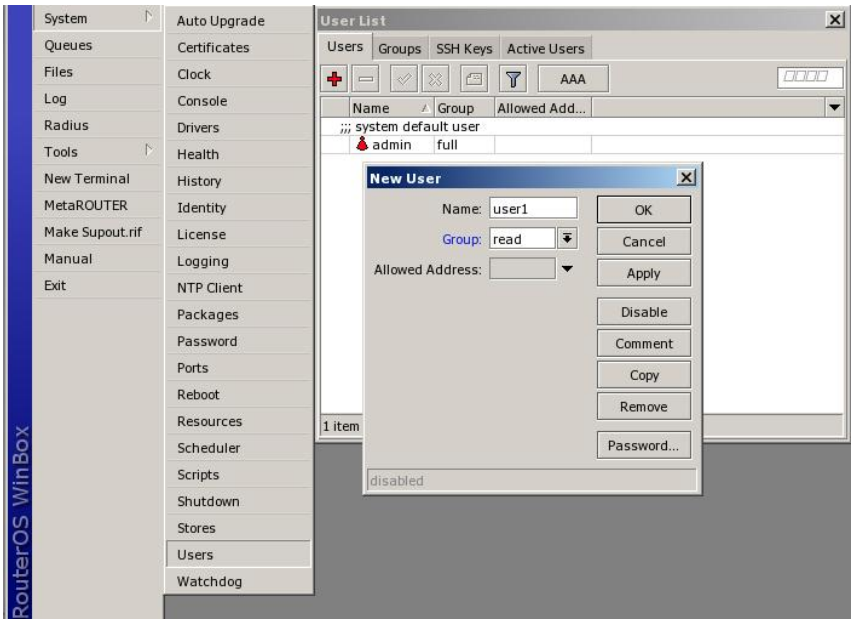


Gráfico 4.27: Usuarios RouterOS.

4.5.5. Reglas para IP Firewall Filter.

La opción de *Filter* permite personalizar de mejor manera todas las restricciones necesarias de seguridad para la protección no solamente del RouterOS sino también de toda la Red en general.

Para poder crear reglas en este punto es necesario un conocimiento más avanzado de Redes, ya que se utilizaran puertos y protocolos en la mayoría de los casos para poder lograr el filtrado de los paquetes.

Este *Firewall* o cortafuegos son utilizados para prevenir o al menos minimizar los riesgos de seguridad en las redes, el uso adecuado ayuda a mejorar la seguridad y la eficiencia de toda la red.

A continuación se muestran algunas reglas que permiten alejar a los intrusos del Router, restringir ataques muy conocidos como el de Fuerza Bruta, Negación de Servicio y también el escaneo de puertos.

A continuación se indica la creación de un conjunto de reglas que permite bloquear un ataque de fuerza bruta.

4.5.5.1. Bloquear ataques de Fuerza Bruta

Los ataques de fuerza bruta son un método utilizado generalmente por hackers o personas mal intencionadas para obtener una clave de acceso probando todas las combinaciones posibles de caracteres.

A continuación se crean las reglas necesarias para evitar este tipo de ataque:

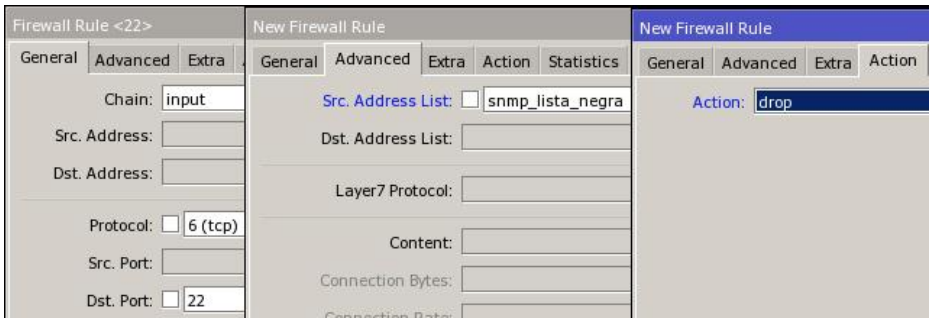


Gráfico 4.28: Regla 1 bloqueo fuerza bruta.

La regla número uno realiza el bloqueo de todo lo que tenga como destino el RouterOS, chain: INPUT, protocolo: 6 (tcp), Dst. Port: 22, que su origen sea Src. Address List: ssh_lista_negra y en Action:drop.

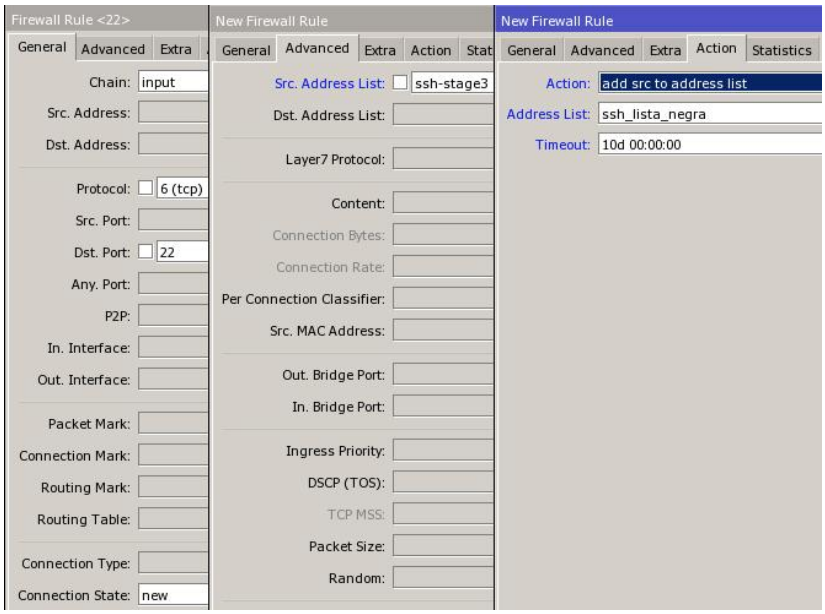


Gráfico 4.29: Regla 2 bloqueo fuerza bruta.

Regla número dos, el chain seguirá siendo INPUT, protocolo: 6 (tcp), Dst. Port: 22, Connection State:new, en la pestaña Advanced Src. Address List: ssh-stage3y en Action:add src to address list, Address List:ssh_lista_negra y en Timeout: 10d 00:00:00.

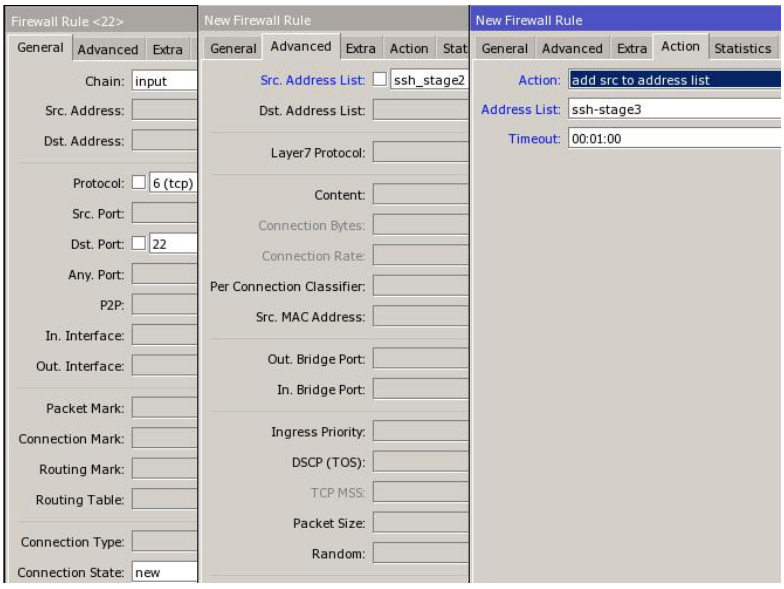


Gráfico 4.30: Regla 3 bloqueo fuerza bruta.

Regla tres, chain: INPUT, protocolo: 6 (tcp), Dst. Port: 22, Connection State: new, en la pestaña Advanced Src. Address List: ssh-stage2 y en Action: add src to address list, Address List: ssh-stage3 y en Timeout: 00:01:00.

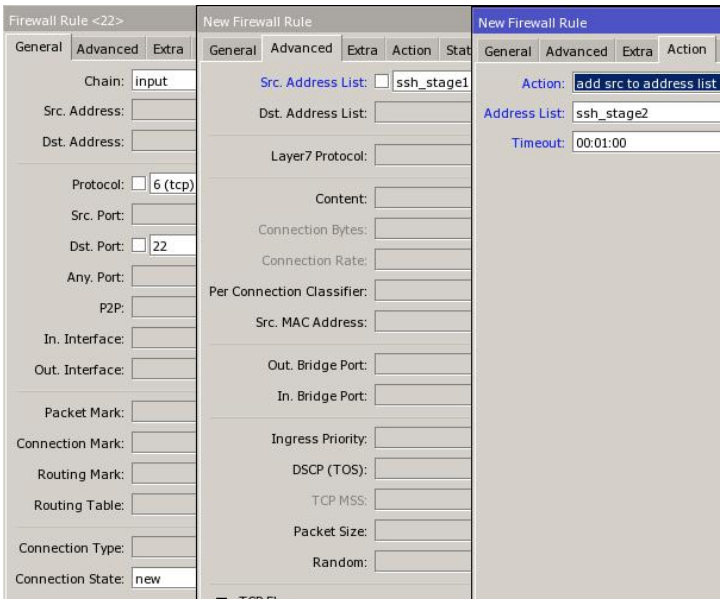


Gráfico 4.31: Regla 4 bloqueo fuerza bruta.

Regla cuatro, chain: INPUT, protocolo: 6 (tcp), Dst. Port: 22, Connection State: new, en la pestaña Advanced Src. Address List: ssh-stage1 y en Action: add src to address list, Address List: ssh-stage2 y en Timeout: 00:01:00.

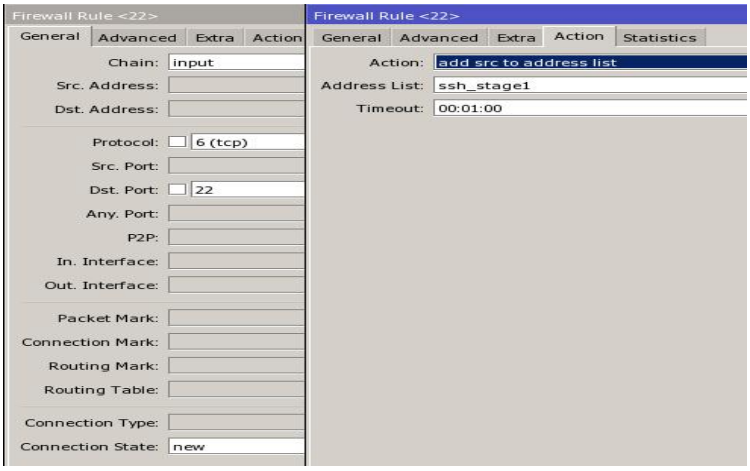


Gráfico 4.32: Regla 5 bloqueo fuerza bruta.

La última regla el chain: INPUT, protocol 6 (tcp), Src Port 22, Connection State “new” y ahora indicaremos a que cree un nuevo Address List con un nuevo nombre que será “ssh_stage1” y en Timeout 00:01:00.

4.5.5.2. Protección del Escaneo de puertos.

Es una forma de buscar vulnerabilidades de seguridad mediante el uso de programas capaces de analizar el estado de los puertos de un dispositivo de red, el objetivo es detectar si un puerto está abierto, cerrado o protegido por un firewall, existe una manera de evitar que terceras personas hagan un escaneo de puertos del RouterOS el cual se mantendrá expuesto a la red pública y privada.

Gráfico 4.33: Regla 1 bloqueo Escaneo de Puertos.

Son dos reglas muy sencillas que necesitamos crear, donde la primera se encargará de bloquear todo lo que mantiene como destino el router en el protocolo 6 (tcp) y que venga del address List: lista_negra

Y la segunda será la encargada de ir agregando a el Address List: lista_negra las direcciones Ips que intentan hacer un escaneo de puertos al RouterOS, esta es la más importante.

Gráfico 4.34: Regla 2 bloqueo Escaneo de Puertos.

4.5.5.3. Denegación de Servicio.

Es un ataque a una red que causa que los servicio o recurso sean inaccesibles, generalmente el ataque satura el ancho de banda o sobrecarga los recursos computacionales del sistema de la víctima, la solución que se utiliza no es óptima pero ayuda de gran forma a minimizar el impacto del ataque.

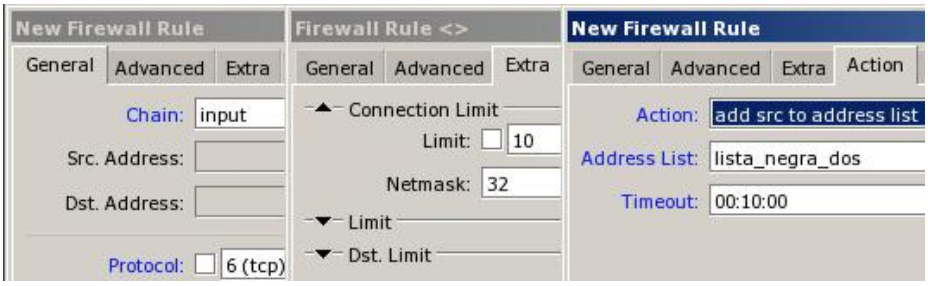


Gráfico 4.35: Regla 1 bloqueo denegación de servicio.

Esta regla dice que todo lo que tenga como destino el RouterOS en el protocolo 6 (tcp) y que provenga de la misma dirección ip no deberá sobrepasar de 10 conexiones, al hacerlo se agrega a un Address List: lista_negra_dos, por un período de 10 minutos.

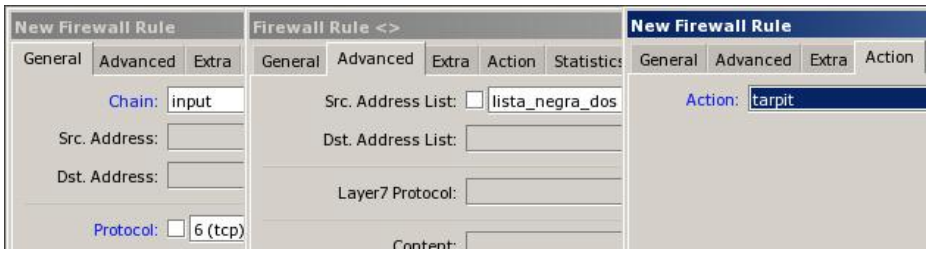


Gráfico 4.36 Regla 2 bloqueo denegación de servicio.

Esta regla al utilizar como *action* TARPIT no bloquea los ataques como lo hace el Drop, sino captura y mantiene conexiones con el *router* de la manera más firme posible para tratar de aniquilar al intruso.

4.5.5.4. Permitir acceso solo para Administradores.

Es recomendable también mantener ACL (Listas de Control de Acceso), que permitan realizar un control de acceso únicamente a determinadas redes o direcciones ip específicas de los administradores de la Red.

Para la creación de un ACL se procede de la siguiente manera:

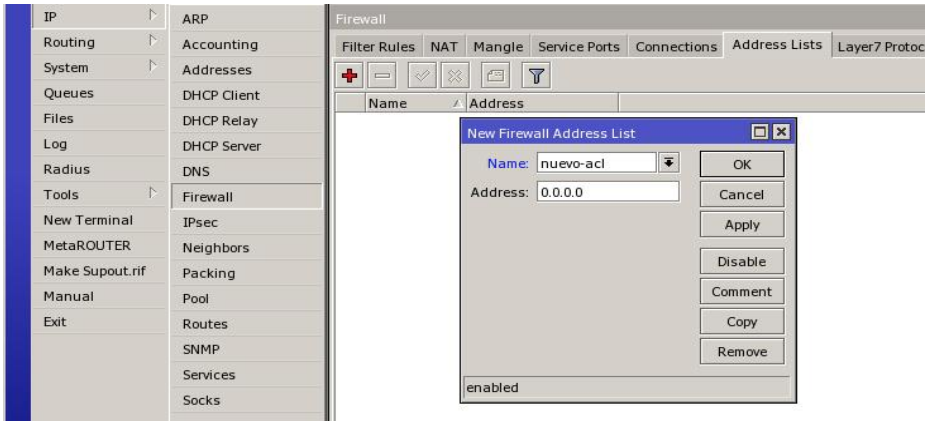


Gráfico 4.37: Regla 1 Permitir Acceso solo Administradores.

En la opción IP > Firewall > Address Lists > Add (+); mediante estos pasos se agrega un nuevo ACL, en la opción NAME se utiliza un nombre que identifique el servicio o función de esta nueva lista, en *Address* se detalla si es una sola ip o cuando es toda una red se indica su máscara, ejemplo de acceso a Winbox solo a usuarios autorizados en el ACL:

- agregar una subred

  Name: administración (nombre de la nueva lista)

  Address: 192.168.0.0/24

- agregar una red

  Name: administración (nombre de la nueva lista)

  Address: 192.168.0.1

Esto es únicamente la creación del ACL, ahora para poder limitar el acceso o autorizar a esta lista es necesario la creación adicional de un Filtrado en IP > Firewall > Filter Rules, esto lo haremos de la siguiente manera:

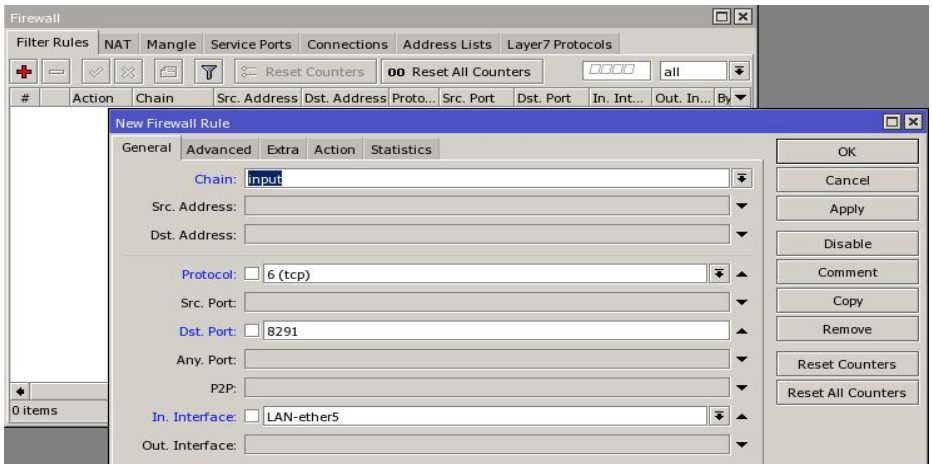


Gráfico 4.38: Regla 2 Permitir Acceso solo Administradores.

El chain a utilizar en este caso es el INPUT por ser que vamos a proteger el acceso a Winbox en el Router, este estará solo permitido para los administradores; el protocolo es: 6 (TCP), puerto de destino: 8291, interface de entrada: LAN-ether5.

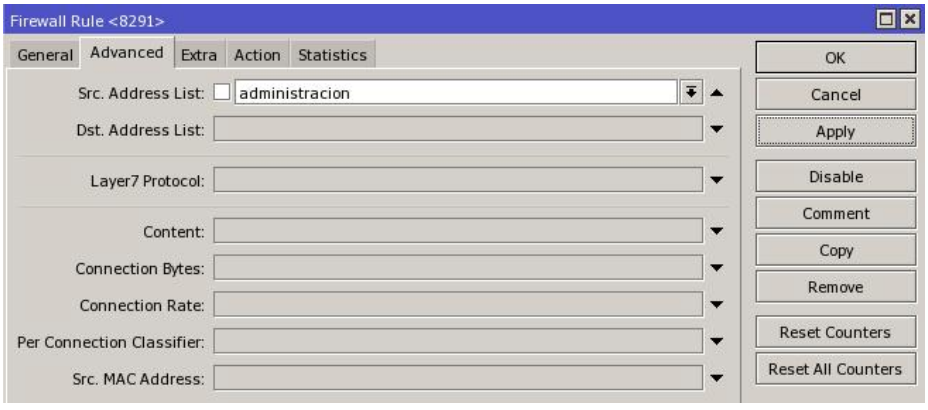


Gráfico 4.39: Regla 3 Permitir Acceso solo Administradores.

Ahora en la pestaña de Advanced, se utiliza la opción de Src. Address List: donde indica el ACL creado anteriormente, en este caso es:

administración, cabe indicar que en el gráfico se puede ver un casillero entre Src. Address List y administración, cuando a este se le da clic se marca un signo de admiración que indica una excepción (todas menos la indicada).

Gráfico 4.40: Regla 4 Permitir Acceso solo Administradores.

En la pestaña ACTION se indica que se hará un accept, la regla explicada totalmente quedaría de la siguiente manera:

Todo lo que entra (CHAIN: Input) por la Interface: LAN-Ether5, con destino el puerto 8291 de TCP, proveniente del Address List: administración, será aceptado.

Para poder cerrar el firewall del router hace falta la creación de una regla que será la encargada de bloquear todo el tráfico restante que tenga como destino el RouterOS, entonces con la creación de estas reglas se ha permitido el acceso del tráfico conocido y que se bloquee el resto que no sabemos qué riesgos pueden generar en el RouterOS.

La regla para cerrar el *firewall* es muy sencilla pero se debe estar seguro de haber permitido el acceso a todos los puertos de las aplicaciones y servicios utilizados.

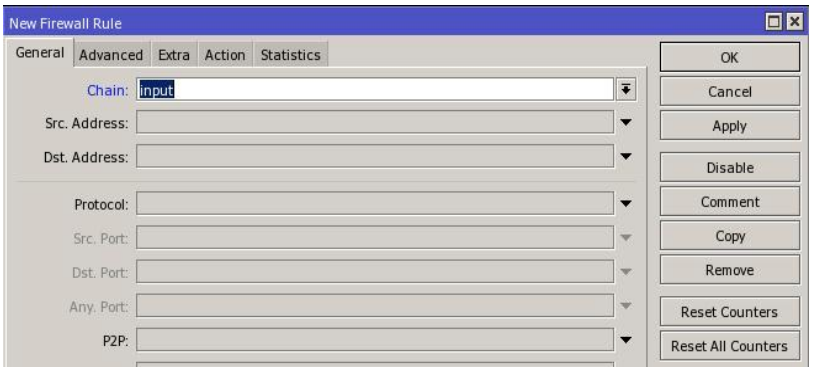


Gráfico 4.41: Regla 5 Permitir Acceso solo Administradores.

En el chain: INPUT, todo lo que entre al *router* se realizara la acción de DROP, esto no permitirá ningún acceso adicional al RouterOS que no haya sido aceptado previamente a la creación de esta regla, es por esto que el orden de las reglas es muy importante.

Gráfico 4.42: Regla 6 Permitir Acceso solo Administradores.

4.6. Servidor de Hotspot.

Hotspot es un método de acceso basado en autenticación para poder utilizar los diferentes recursos de la red este método es comúnmente utilizado en redes *wireless* pero cabe indicar que es posible también que se utilice en cualquier otro medio TCP/IP como es también Ethernet.

El objetivo principal de *Hotspot* es permitir el acceso a los recursos de la red únicamente a los usuarios que están autorizados, en la mayoría de casos

hablamos del recurso de Internet específicamente ya que es el más común utilizado en la actualidad para redes públicas en donde se permite el acceso a dispositivos portátiles.

La configuración de Hotspot en RouterOS se la realiza utilizando el boton de *Hotspot Setup* que será el encargado de guiarnos a través de los diferentes pasos necesarios para levantar el servicio en una interfaz.

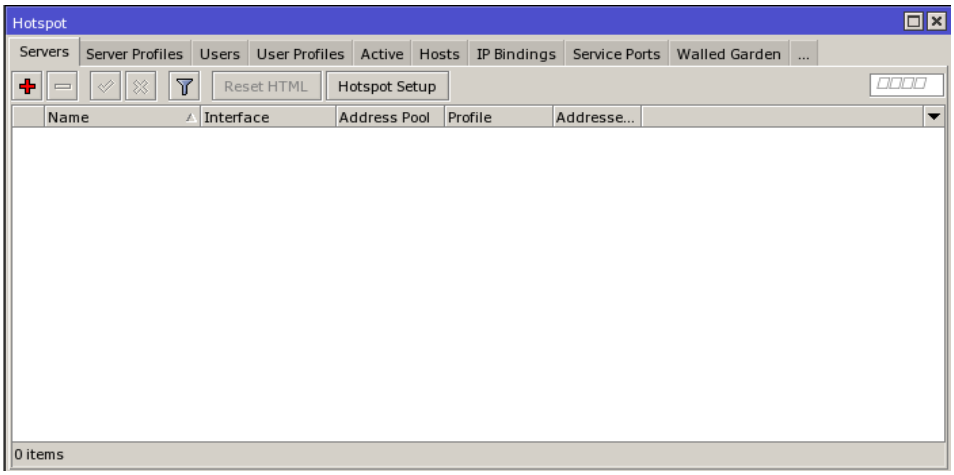


Gráfico 4.43: Servico de Hotspot.

Lo primero que se debe hacer es asignar una IP a la interfaz así como una subred en este caso se utiliza 192.168.0.1/24, la opción de Hotspot esta en el menú IP > HOTSPOT.

Al dar click en el boton Hotspot Setup muestra la primera ventana de configuración.

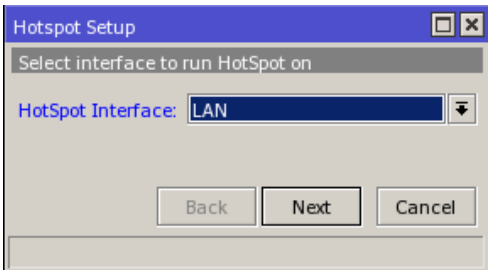


Gráfico 4.44: Configuración de Interface.

Aquí es donde se indicará la interfaz que usara el servicio de hotspot.

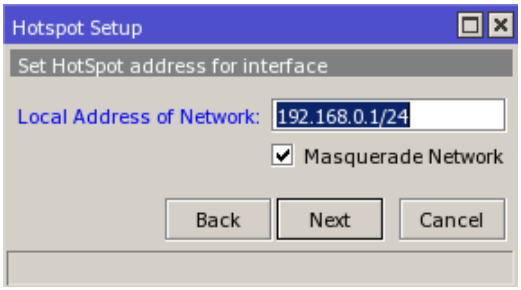


Gráfico 4.45: Asignación de dirección IP y Subred.

En el segundo paso se debe elegir la dirección local de la red para el hotspot que es la misma asignada inicialmente a la interface, también se debe indicar si es necesario enmascarar la red para que automáticamente se añada la regla de Nat.

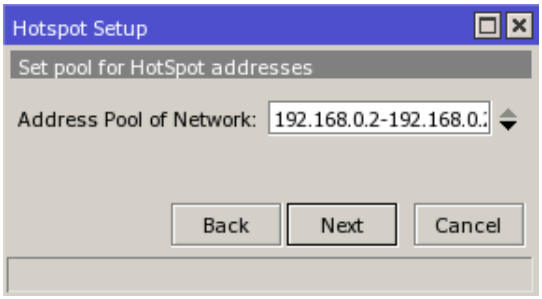


Gráfico 4.46: Rango de direcciones para host.

Ahora se observa el rango que se utiliza para la asignación de direcciones a los usuarios que se registren mediante el servicio de hotspot.

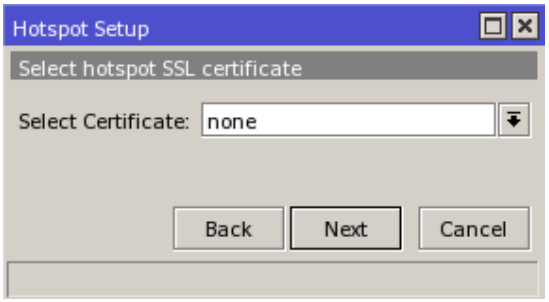


Gráfico 4.47: Selección de certificado.

En esta opción es necesario ingresar un certificado SSL si se cuenta con uno, para el ejemplo no contamos por lo cual se deja por defecto en: none.

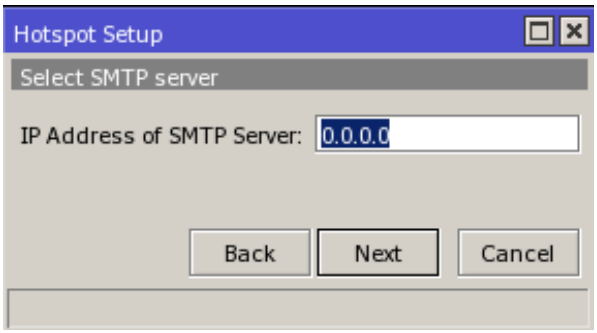


Gráfico 4.48: Dirección IP del Servidor SMTP.

La dirección IP que se solicita a continuación es la de un servidor SMTP, sirve en el caso de querer redireccionar todo el tráfico del puerto 25, en este caso al dejar con 0.0.0.0 que es el valor por defecto indica que no existe ningún servidor.

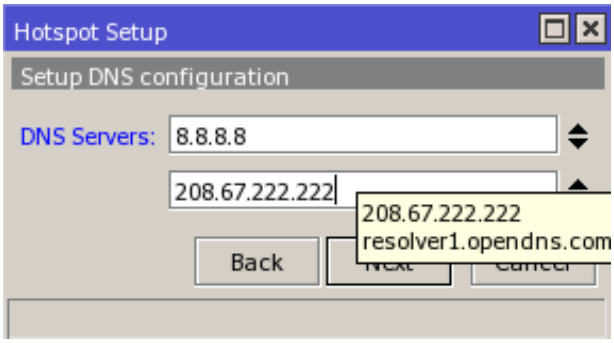


Gráfico 4.49: Servidores DNS.

El siguiente paso es configurar los servidores DNS, en este caso se utilizan DNS públicos.

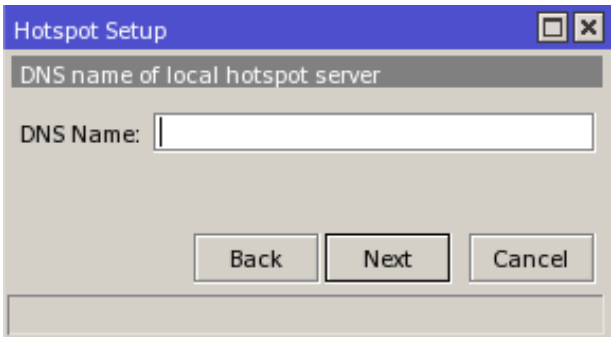


Gráfico 4.50: Nombre del DNS local.

DNS Name es un nombre que no necesita ser válido públicamente porque es para la entrega de la página de inicio, es únicamente un nombre local.

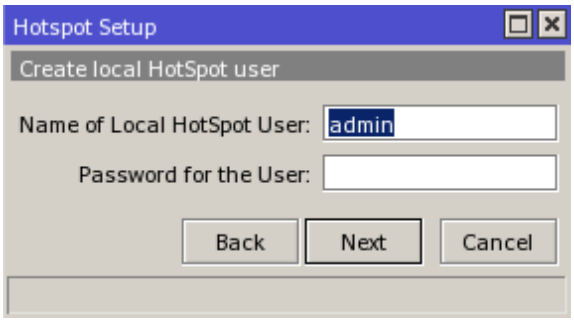


Gráfico 4.51: Usuario y Clave de acceso.

El último paso es la configuración de un nombre de usuario y clave para la autenticación de hotspot.

Al terminar estos pasos la configuración concluye y ahora al tratar de ingresar se muestra la pantalla de validación que es la siguiente:

Gráfico 4.52: Página de inicio de Hotspot

4.7. Control de Ancho de Banda por usuario.

La autenticación por *Hotspot* ha permitido limitar el ancho de banda a cada usuario conectado, con esto se ha tratado de garantizar un mínimo en horas de congestión y un máximo en horas que no existe mucho tráfico, la desventaja de este método es que no se aprovecha todo el ancho de banda disponible debido a que se limita en casos innecesario aun existiendo capacidad disponible.

Hotspot permite la creación de diferentes perfiles de usuario esto con la finalidad de personalizar los grupos, para ejemplo crearemos un perfil donde detallaremos las opciones más básicas e importantes:

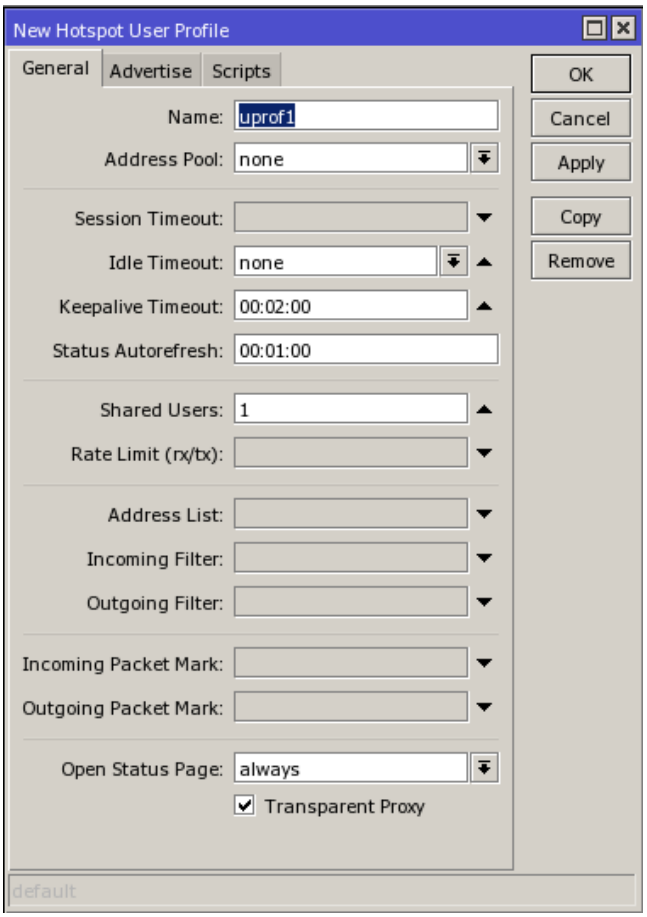


Gráfico 4.53: Creación de perfil de Hotspot.

Otra manera de hacer un control más eficiente del ancho de banda disponible que se ha probado y con mejores resultados es el de repartir el ancho de banda de manera dinámica a todos los usuarios, así se ha conseguido poder hacer uso de toda la capacidad disponible. En ciertos casos que han existido demasiadas conexiones concurrentes la mejor ventaja de utilizar asignación de ancho de banda dinámico es que automáticamente se dividirá en partes iguales toda la capacidad y se puede evitar de esta manera el abuso por los usuarios en la red.

La configuración de anchos de banda dinámico es posible realizar mediante la utilización de herramientas que también son propias de RouterOS, para este caso puntual se ha utilizado *Queues*, en donde encontramos.

4.8. Asignación dinámica de Ancho de Banda.

Una de las maneras de aprovechar el ancho de banda al máximo es repartiéndole de manera dinámica, es decir que el ancho de banda se va ir dividiendo en partes iguales para todos los usuarios conectados, es te método funcionaria como un nivel de compartición de 1:N donde N seria el número de usuarios conectados, de esta manera todos los usuarios tendrían asegurado un mínimo de ancho de banda garantizado dependiendo de los usuarios conectado y podrían tener picos máximos dependiendo del uso del resto de usuarios.

4.9. Administración de Ancho de Banda por Protocolo Layer 7.

Layer 7 es una característica muy importante al momento de brindar calidad de servicio en cualquier tipo de red, es un método de búsqueda que en base a patrones ICMP, TCP o UDP puede lograr determinar de dónde provienen los paquetes.

Estas búsquedas funcionan con una comparación de los primeros 10 paquetes o los primeros 2kb de conexión, en caso de no encontrar coincidencias en los patrones no hace falta continuar la búsqueda con el flujo restante de dicha conexión, de esta manera se libera la memoria asignada y se considera a este protocolo como desconocido, así se podrá liberar memoria y evitar que una gran cantidad de conexiones simultaneas aumente significativamente el uso de esta.

Layer 7 siempre realiza la verificación de los dos sentidos del tráfico (entrante y saliente) y de esta manera al poder determinar si coincide con los patrones se podrá dar un tratamiento especial o puntual al mismo.

Los protocolos soportados por los filtros de *Layer*7 se los encuentra en la página fuente: http://l7-filter.sourceforge.net/protocols

4.9.1. Diagrama para marcado de paquetes.

Gráfico 3.15: Flujo Ip Firewall Mangle.

En el diagrama observamos el orden del flujo que se da al tráfico en todo RouterOS, donde se indica que el marcado de paquetes se lo puede hacer en la opción del Mangle en IP > Firewall, aquí existen 5 lugares específicos que son:

- *Prerouting*
- *Input*
- *Forward*
- *Output*
- *Postrouting (Output + Forward*)

La limitación de velocidad o prioridad se la realiza en los *QUEUES* en 4 lugares que son los siguientes:

- *Global-In*
- *Global-Out*
- *Global-Total (Global-In + Global-Out)*
- *Out-Interface*

Ahora con el siguiente diagrama podremos tener una mejor idea del flujo generalmente en toda red y lo que se debe hacer para mejorar.

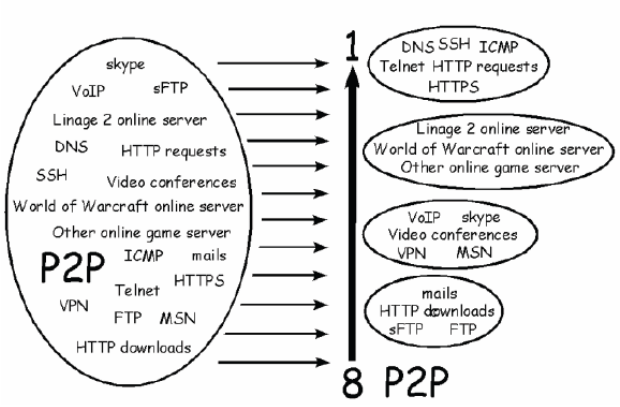


Gráfico 4.54: Asignación de prioridades Layer 7.

El tráfico debe cumplir con una clasificación de las aplicaciones donde lo fundamental es saber qué tipo de tráfico es tolerante a perdida de paquetes y cual no lo es, así como también las aplicaciones que se llevan a cabo en tiempo real.

Las principales aplicaciones en este caso que se realizan en tiempo real son: *Streaming*, Video conferencia, Voz/IP, etc.

Entre los datos intolerante a pérdidas mencionamos los siguientes: protocolo TCP como e-mail y FTP, etc.

En el Mangle asignamos marcas a los paquetes para de esta manera poder darles un tratamiento adecuado más adelante en el encolamiento.

4.9.2. QoS con *Layer* 7

El marcado de paquetes es el fundamento general de todo QoS, pero a diferencia del marcado convencional se utilizará la herramienta de *Layer* 7 que tiene RouterOS permitiendo mejorar en otro nivel el trato que se dará a los paquetes.

En la página fuente del proyecto *Layer7* se encuentra con detalle el funcionamiento de las reglas básicas existentes, la velocidad con la que opera, grupos a los que pertenece y protocolo que corresponde.

La configuración en RouterOS inicia con la creación de las reglas en: IP > FIREWALL > LAYER7.

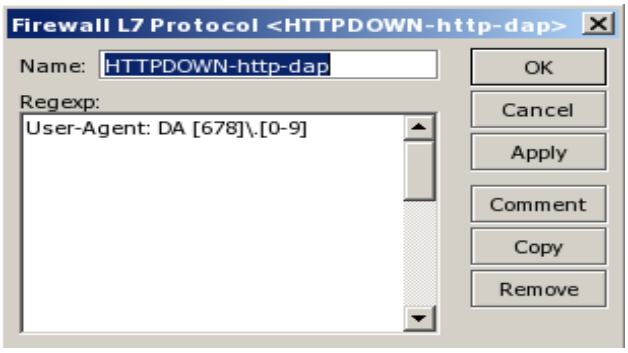


Gráfico 4.55: Creación de Regla Layer 7.

En esta parte el nombre de la regla permite identificar a cada una de las que se hayan creado, lo más importante está dentro del campo Reg exp que es donde esta exactamente el mismo texto que se muestra dentro de la página del proyecto como patrón previamente analizado y probado.

Una vez ingresado los patrones necesarios para poder ser utilizados se continúa con el tratamiento al mismo que se lo realiza en la parte de Mangle.

Se procede con la creación de una nueva regla en el mangle para poder dar otro tratamiento diferente a este paquete, en la pestaña General elegimos el Chain: prerouting

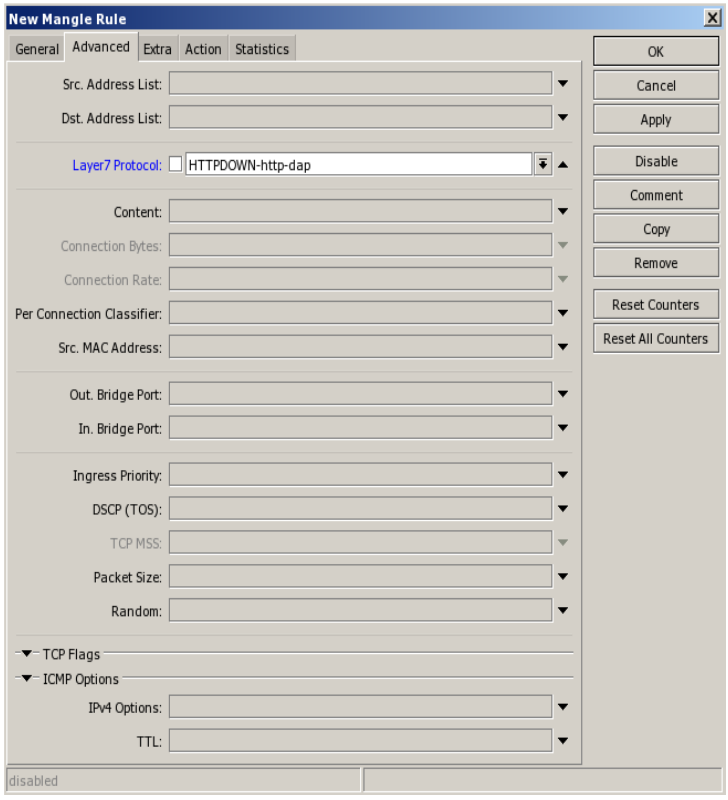


Gráfico 4.56: Marcado de paquete con Layer 7.

En *Advanced* elegimos la opción *Layer 7 Protocol* donde será seleccionado el nombre que fue creado anteriormente.

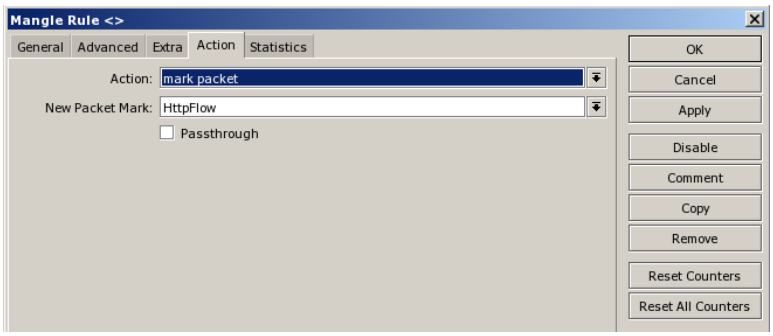


Gráfico 4.57: Marca asignada al paquete.

La acción que se debe seleccionar es *mark packet*, en el casillero *New Packet Mark* se ingresa el nombre que se designa para el paquete marcado, en este caso: HttpFlow

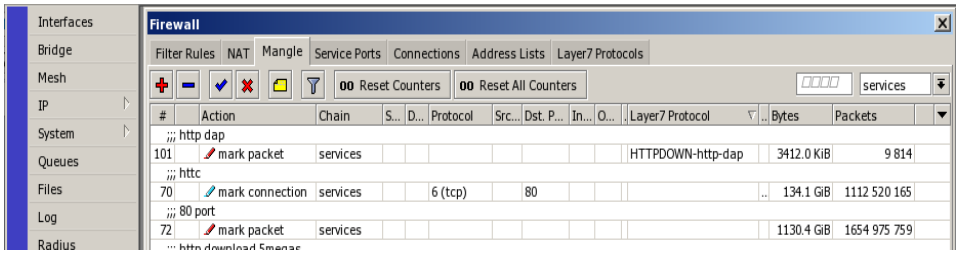


Gráfico 4.58: Paquetes marcados en el mangle.

Todo el tráfico que pasa por el *router* llevara la marca definida previamente. Ahora se procede con la asignación de la prioridad y ancho de banda especifico a este tipo de tráfico.

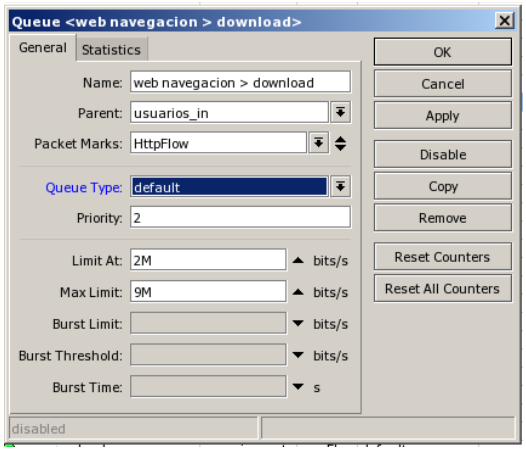


Gráfico 4.59: creación de cola para paquete marcado.

Los parámetros que configuramos son:

- *Name*: Este campo permite identificar con un nombre a la cola dentro del arbol, en este caso “web navegación > download”

- *Parent*: Indica si esta cola tiene un padre al cual se debe regir, usuarios_in es una cola padre.

- *Packet Marks*: Es el nombre del paquete según lo hayamos marcado en el Mangle (HttpFlow)
- *Queue Type*: El tipo de cola que se utilizara en este caso será el valor por defecto (default)
- *Priority*: La prioridad que tendra la cola siendo 1 la máxima prioridad y 8 la más baja.
- *Limit At*: Es el ancho de banda que se garantiza en momentos de saturación (2M).
- *Max Limit*: Será el límite de ancho de banda que podrá disponer (9M).

Mediante la utilización de esta herramienta que resulta ser muy eficiente podremos lograr una mejora significativa en los servicios, será necesario identificar el flujo existente y colocar marcas para de esta manera asignar prioridad y ancho de banda.

4.10. Generar alertas automáticas mediante envío de mails.

El servidor se configura con su dirección IP del servidor de correo, indicando el puerto que este configurado y los datos de la cuenta del correo como son usuario y contraseña.

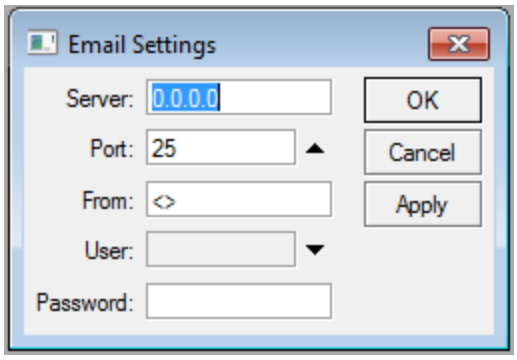


Gráfico 4.60: Herramienta Email.

Una forma de probar que esté funcionando él envió de correo es mediante línea de comandos, ejecutamos lo siguiente:

/tool e-mail send subject=Subject to=prueba@dominio.com body=texto

Para poder verificar que se está realizando él envió satisfactoriamente es necesario configurar el registro en el log del RouterOS como se indica a continuación:

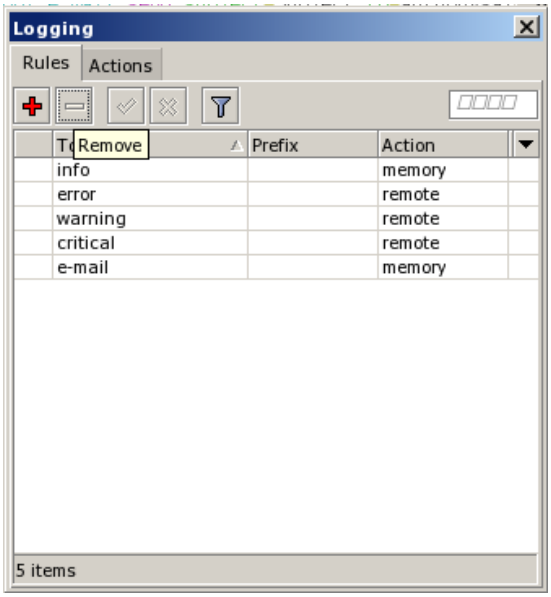


Gráfico 4.61: Logs de RouterOS.

La opción está en System > Logging y para agregar es necesario dar click en el signo más donde se muestra lo siguiente:

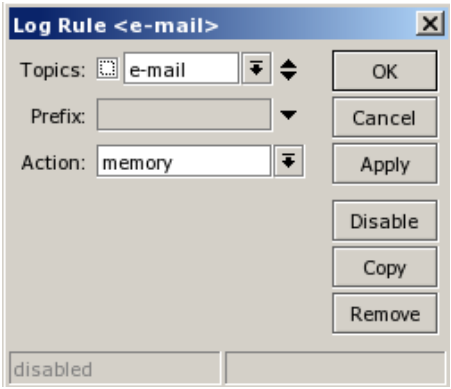


Gráfico 4.62: Creación de log para email.

El tema a elegir en este caso es: e-mail y la acción será: memory, con este se registran todos los sucesos de email en la memoria del RouterOS.

4.11. Habilitar gráficas MRTG (Graphing).

Se puede habilitar las gráficas para tener reportes del estado de los recursos del equipo así como del tráfico de las interfaces.

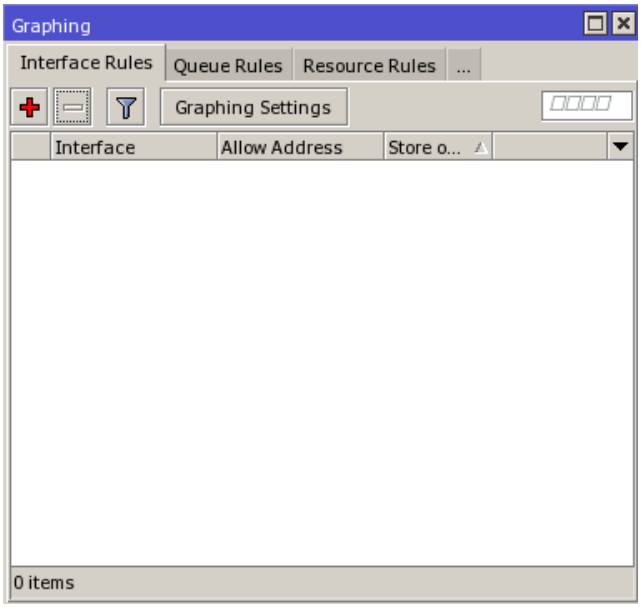


Gráfico 4.63: Configuración de Gráficos

En el botón Graphing Settings se definen el tiempo para el almacenamiento de los eventos, generalmente es utilizado el menor tiempo 5 minutos.

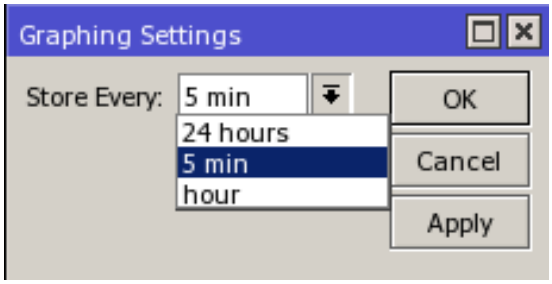


Gráfico 4.64: Tiempo de eventos.

En el reporte de gráficas se puede agregar cada uno de los recursos o todos si es necesario, esto se lo realiza creando una regla en la pestaña *Resource Rules*

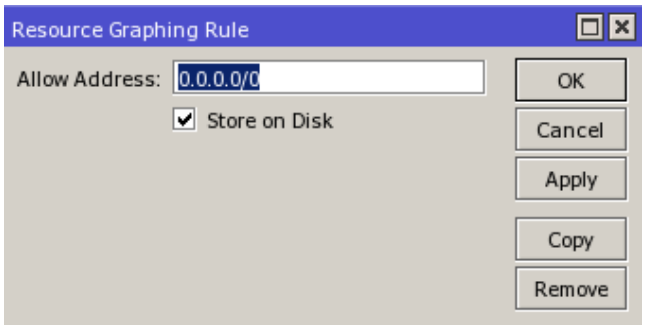


Gráfico 4.65: Regla de gráficos para recursos.

Debe estar seleccionado con un check Store on Disk para así permitir que el almacenamiento sea en disco y mantener como historial.

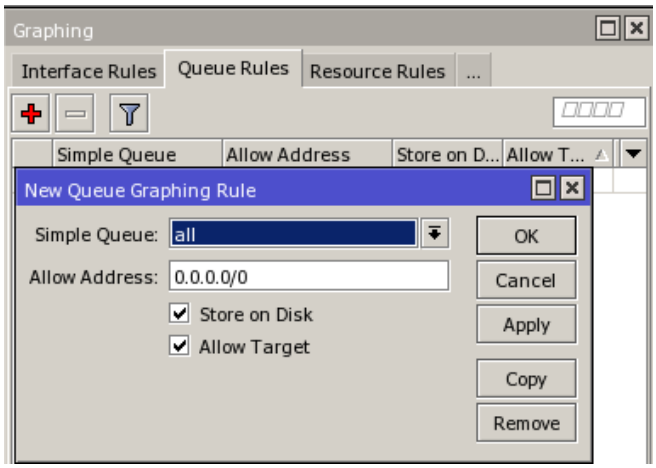


Gráfico 4.66: Regla de gráficas para Queues Simples

En la pestaña Queue Rules se crea una nueva regla que será la encargada de graficar todos los Queue que se encuentran en la opción Queue Simple.

En esta última opción se agregan las interfaces que necesitamos gráficas, para el ejemplo están seleccionadas todas.

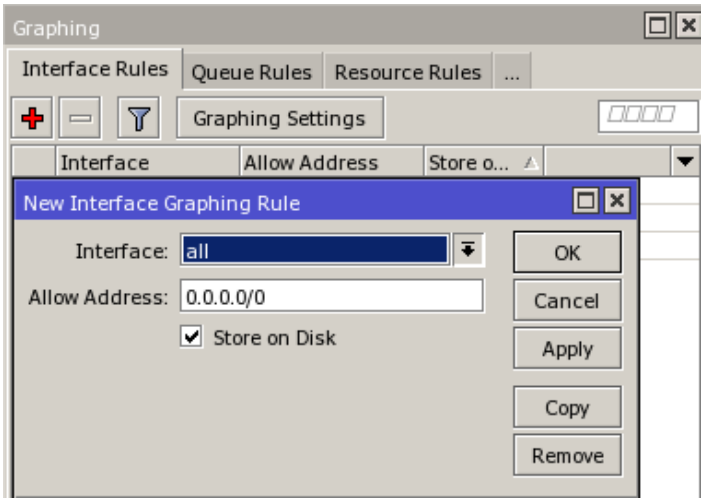


Gráfico 4.67: Regla de gráficas por interface.

CAPITULO 5

5. Pruebas de Implementación.

Introducción.

El escenario de pruebas utilizado fue la red inalámbrica de la Universidad del Azuay, se combinaron las configuraciones descritas en el capítulo anterior hasta lograr un funcionamiento adecuado de la misma, también se detectaron algunos problemas en la red que impiden llegar a un óptimo funcionamiento.

Los diferentes equipos probados permiten determinar capacidades y de esta manera elegir los más adecuados para un mejor desempeño, la configuración se realizó con diferentes equipos de Mikrotik y también una PC con RouterOS.

5.1. Equipos Utilizados.

A continuación haremos una breve descripción de los diferentes equipos utilizados.

- Routerboard Mikrotik RB450G.

Gráfico 5.1: Routerboard Mikrotik RB450G

Inicialmente el *Router Board* que utilizamos fue un Mikrotik RB450G que tiene las siguientes características:

- CPU 680MHz
- RAM 256MB
- Puertos GigabitEternet 5
- Licencia Nivel 5

- PC

Gráfico 5.2: PC x86.

La computadora utilizada para las pruebas que se realizaron tuvo las siguientes características:

- Pentium 4
- 512 en RAM
- 40GB de disco
- Dos tarjetas Ethernet
- Licencia Nivel 4

- RouterBoard RB1100

Gráfico 5.3: RouterBoard RB1100

El RB1100 forma parte de la línea *Router* de *Core* de la marca Mikrotik, entre las principales características de este equipo se describen las siguientes:

- CPU 800MHz
- RAM 512
- Arquitectura PPC
- 13 puertos GigabitEthernet
- 2 puertos con capacidad de ethernet bypass
- Licencia Nivel 6

5.2. Pruebas realizadas con los equipos.

Con los diferentes equipos se tuvo la oportunidad de manejar varias alternativas de configuraciones, de esta forma se trató de determinar en base a experiencias el mejor desempeño y funcionamiento de la red.

El escenario en el cual se realizan todos los cambios es totalmente real. A continuación una breve descripción de pruebas realizadas en los equipos con sistema operativo RouterOS.

5.2.1. Prueba 1

Inicialmente comenzamos utilizando el Mikrotik RB450G, cargada con las siguientes configuraciones:

- Servidor DHCP
- Firewall (Básico)
- NAT

Debido a la carga de usuarios el procesador del equipo a ciertas horas del día llego al 100% de procesador, lo que ocasionaba caídas de la red.

5.2.2. Prueba 2

En busca de mejorar o superar el inconveniente se decide reemplazar por otro equipo con mayor capacidad en hardware, para esto se utiliza la PC mencionada anteriormente en donde se instaló el Sistema Operativo RouterOS.

Las configuraciones utilizadas para esta prueba fueron las siguientes:

- Servidor DHCP
- Firewall
- NAT
- HOTSPOT

- Limitación de ancho de banda por usuario

Con este equipo ya no detectamos problemas de caídas en la red, pero debido a que utilizamos una licencia de nivel 4 para el sistema operativo, el servidor de *Hotspot* no admitía más de 200 usuarios conectados simultáneamente a la red. La solución a este problema era dar de baja el servidor de *hotspot* y a la limitación de ancho de banda por usuario debido a que depende del servicio deshabilitado para funcionar.

5.2.3. Prueba 3

Se busca otra alternativa más para solucionar los problemas de la prueba anterior y se prueba un Router Mikrotik RB1100, el *router* más robusto disponible en el medio en cuanto a hardware y debido a su licencia de nivel 6 permite utilizar toda la funcionalidad del sistema operativo.

Ser cargó las mismas configuraciones de la prueba anterior y se adiciona otras.

- Servidor DHCP
- Firewall
- NAT
- HOTSPOT
- Control de ancho de banda Dinámico
- QoS capa 7

Inicialmente no se presentó ningún problema, pero con el tiempo se detecta caídas de la red a horas pico del día, al revisar el equipo claramente se logró detectar que el cpu llega a su límite, la causa del problema es debido a la utilización de un de firewall que a más de la configuración básica que proteger el equipo, también existen reglas adicionamos para proteger toda la

red, esto lleva al equipo a su límite produciendo una saturación del uso de su procesador.

5.2.4. Prueba 4

Finalmente probamos distribuyendo la carga en dos equipos, la configuración se realizó de la siguiente manera:

Para el Mikrotik RB 1100:

- Servidor DHCP
- Firewall(básico)
- NAT
- HOTSPOT
- Control de ancho de banda dinámico

Para la PC:

- Firewall de toda la red
- QoS capa 7

Al distribuir la carga en los dos equipos se logró solucionar los problemas presentados en las pruebas anteriores.

5.3. Monitoreo de Equipo.

El sistema operativo RouterOS, tiene algunas herramientas que permiten monitorear el comportamiento de la red y el equipo.

5.3.1. Monitoreo web.

Permite acceder a través de un entorno web, donde se puede ver gráficas históricas del estado del cpu, tráfico de cada interface, colas simples, uso del disco duro y memoria.

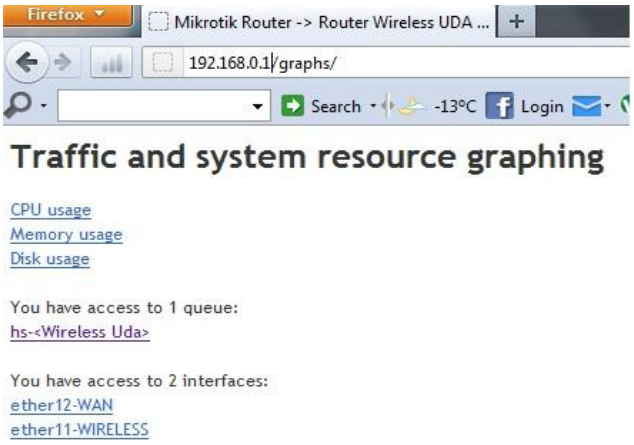


Gráfico 5.4: Interface web de monitoreo.

Al dar click en cualquiera de esos enlaces nos mostrara un gráfico como el siguiente:

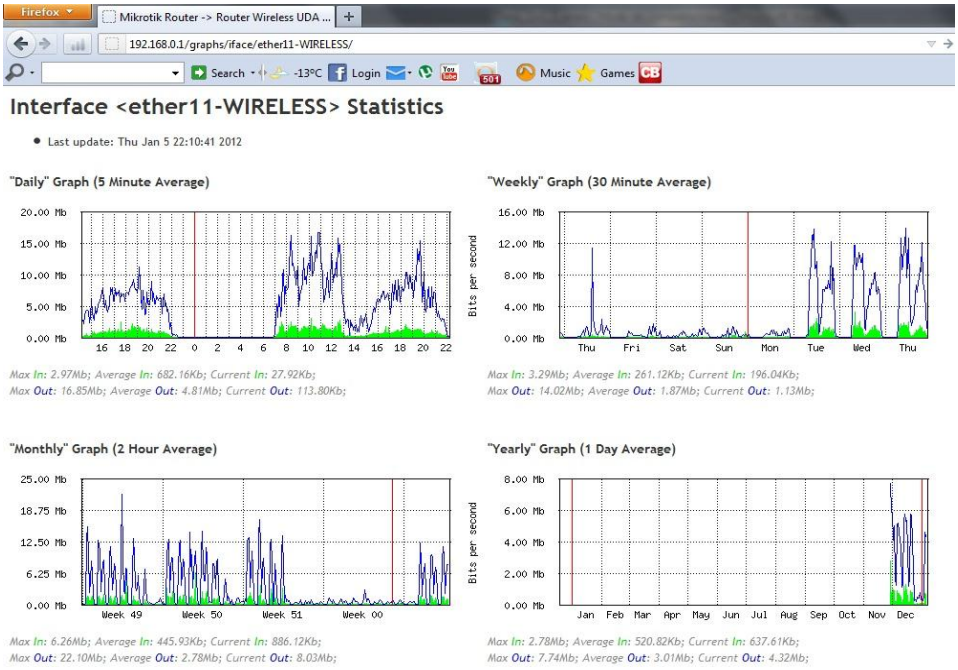


Gráfico 5.5: Trafico Interface Wireless.

Esta herramienta muestra 4 gráficos, de consumo diario, semanal, mensual y anual, los gráficos se actualizan cada 5 minutos.

5.3.2. Monitor de tráfico en tiempo real.

Esta herramienta permite monitorear el tráfico que pasa a través de una interface, esta información se puede clasificar por protocolo, la dirección fuente y destino, puerto. Torch muestra los protocolos elegidos y la velocidad de recepción y transmisión de los datos.

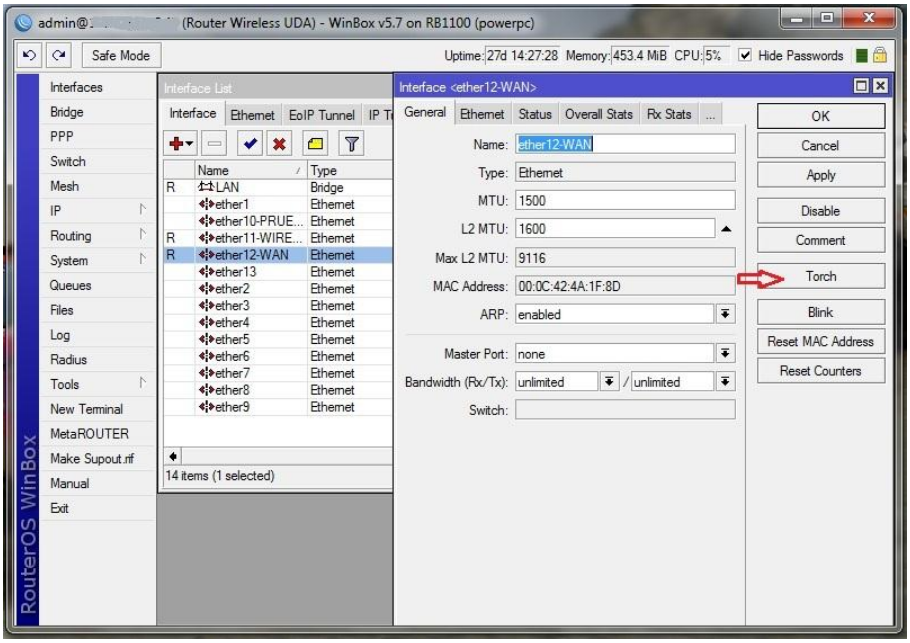


Gráfico 5.6: Monitoreo de interfaz WAN.

Para ejecutar la herramienta demos click en el botón Torch y nos aparecerá la siguiente ventana:

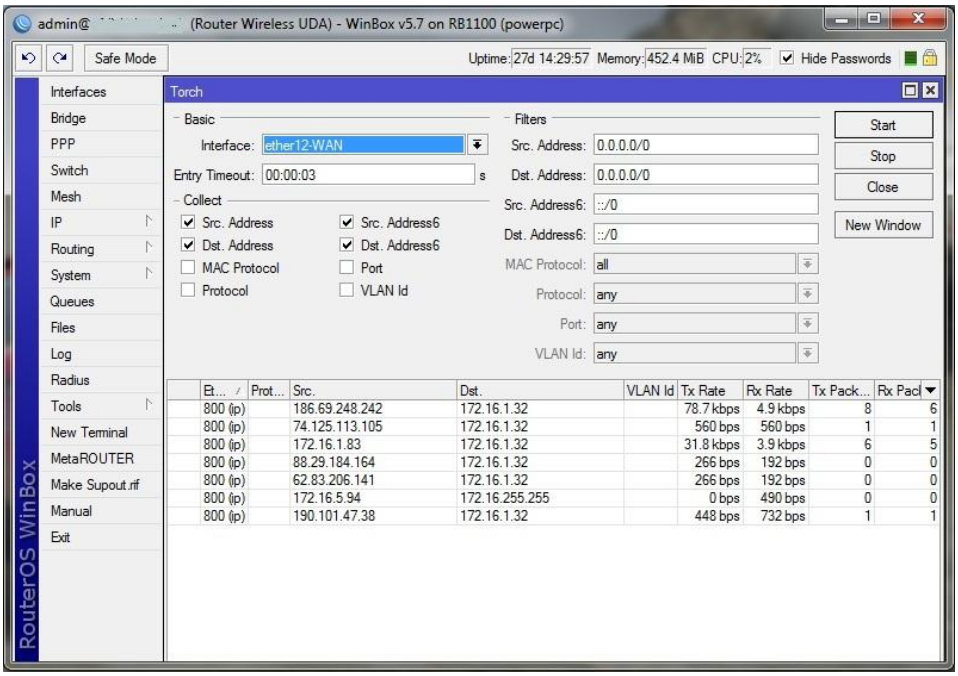


Grafico 5.7: Torch en Ejecución.

Aquí se puede ver el detalle del tráfico que pasa por esta interfaz.

5.3.3. Barra de estado de Winbox.

En la parte superior de la ventana de Winbox se encuentra una barra con algunos detalles y funciones importantes del equipo.

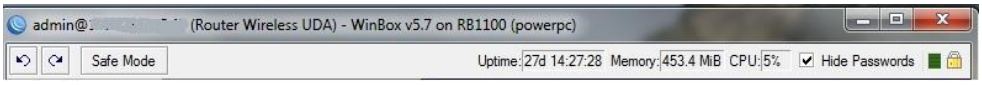


Gráfico 5.8: Barra de estado.

Se recomienda activar el botón Safe Mode antes de realizar cambios de configuración en el equipo, ya que si dicho cambio produce que el equipo falle automáticamente se restablece la configuración al estado en el que

estaba cuando se activó el botón, si los cambios funcionaron simplemente desactivamos el botón y la configuración se grabara permanentemente.

Uptime: muestra en tiempo que el equipo a estado activo.

Memory: muestra el estado de la memoria en tiempo real.

CPU: Y el recuadro verde de la izquierda muestra el estado del CPU en tiempo real.

La pestaña Hide Passwords sirve para ocultar o mostrar los caracteres de las contraseñas.

CONCLUSIONES.

Una vez terminado nuestro trabajo de tesis podemos concluir que:

El routerboard 1100 con aproximadamente 300 conexiones activas simultaneas no soporta el trafico si se le incluye un firewall.

El routerboard 1100 se lo debe configurar únicamente como Hotspot y QoS para soportar el tráfico de 300 conexiones.

Con Access Point mikrotik (versión 5.7) se notó que si se activaban todos los estándares (a/b/g/n) de comunicación no funcionaban correctamente, desconectándose los usuarios repentinamente. Se tuvo que deshabilitar el estándar n para que funcione.

La capacidad de usuarios por tarjeta mini pci de un Access Point Mikrotik es de aproximadamente 40 usuarios para que el rendimiento sea el adecuado.

La capacidad de incrementar protocolos para Layer 7 de forma manual hace que el equipo sea muy flexible para poder realizar QoS en este Layer lo que no sucede con los fabricantes que venden soluciones cerradas a las cuales no se les puede aumentar protocolos.

Se puede determinar una prioridad o bloquear, un mínimo y un máximo de ancho de banda por protocolo de Layer 7.

El Sistema Operativo RouterOs permite también el control de ancho de banda por ip.

El Sistema Operativo RouterOs tiene una herramienta de análisis de tráfico de red en tiempo real llamada Torch

RECOMENDACIONES.

Para poder garantizar el óptimo funcionamiento de la red WiFi, se recomienda realizar un estudio para la modernización de la infraestructura actual, tomando en cuenta el gran crecimiento que en los últimos años han tenido los dispositivos móviles.

Revisar las frecuencias en las que trabajan cada punto de acceso, para evitar el solapamiento entre puntos de acceso cercanos.

Tomar en cuenta el área que se quiere cubrir con un punto de acceso, para dimensionar la potencia del equipo y el número de posibles usuarios.

Implementar un servidor RADIUS para que en la autenticación por hotspot y el resto de servicios con los que cuenta la Universidad.

Para configurar todos los servicios del RouterOS de Mikrotik se lo debe realizar en un servidor y no en el RouterBoard 1100.

GLOSARIO.

RF(Radio Frecuencia).

DBPSK (DifferentialBinaryPhaseShiftKeying)

DQPSK (DiferentialQuadraturePhaseShiftKeying)

DSSS (Tecnología de espectro ensanchado por secuencia directa).

FHSS (Tecnología de espectro ensanchado por salto en frecuencia).

FSK (FrequencyShiftKeying)

LLC (Logical Link Control)

MAC (Medium Access Control)

CSMA/CA (Carrier Sense Multiple Access / Collision Advoidance)

QoS(Calidad de Servicio)

IETF(Internet Engineering Task Force)

IntServ (Integrated Services).

RSVP (Resource Reservation Protocol)

DiffServ (Differentiated Services).

MPLS (Multi-Protocol Label Switching).

LSP(LabelSwitchedcaminos)

LDAP(LightweightDirectory Access Protocol, Protocolo Ligero de Acceso a Directorios)

DEN(DirectoryEnabledNetwork,Directorio habilitado en la red).

PDP(policydecisionpoint,Punto de decisión)

PEP(policyenforcementpoint, punto de aplicación de la política)

COPS(Common Open Policy Service)

LPDP(local policydecisionpoint, punto de decisión de política local)

PCF (Función de Coordinación Puntual)

DCF (Función de Coordinación Distribuida)

DCP (Digital Cinema Packag)

HCF (HybridCoordinationFunction)

EDCA(EnhancedDistributedChannel Access),

HCCA(HCF Controlled Access)

TS (flujo de tráfico)

TXOP (TransmisionOpportunity).

AIFS(Arbitration Inter FrameSpace).

AIFSN (ArbitrationInterFrameSpaceNumber)

AC (Admission Control)

TSPEC (TrafficSpecification)

SRC (Source)

DST (Destiny)

NTP (Network Time Protocol)

DNS (Domain Name System)

NAT (Network Address Translation)

SRC-NAT (Source NAT)

PCQ (per connection Queue)

SFQ (Stochastic Fairness Queueing)

FIFO (First Input First Output)

HTB (Hierarchical Token Bucket)

TTL (Time To Live)

TOS (Terms of service)

BIBLIOGRAFIA.

Frank Ohortman , K.R. [2003] Wi-Fi Handbook: Building 802.11b Wireless Networks. New York: McGraw-Hill.

Internet y Redes Inalámbricas. Arequipa – Peru: CLANAR Internacional

.

Matthew S. Gast. [2002] 802.11 Wireless Networks: the definitive guide. 1ra ed. United States of America: O'Reilly.

Dennis Burgess. [2009] Learn RouterOS. 1ra ed. United States of America. ISBN:978-0-577-09271-0.

Cisco DokWiki. [20 de 06 de 2010]. Quality of Service Networking. Recuperado el 13 de 07 de 2010 de , http://docwiki.cisco.com/wiki/Quality_of_Service_Networking

Radioayudas a la Navegación Aérea. [15 de 02 de 2010]. Conceptos sobre las Ondas Electromagnéticas. Recuperado el 26 de 02 de 2010 de, http://nacc.upc.es/navegacion-aerea/x360.html

Centro de Investigación para la Sociedad de la Información. [02 de 07 de 2010]. Representación semántica de funciones para evaluación de la calidad de servicios telemáticos. Recuperado el 10 de 07 de 2010, de http://www.imaginar.org/ecollecter/fullpapers/p91-RepresentacionSemanticaDeFunciones.pdf

Linktionary. [15 de 06 de 2010]. QoS (Quality of Service). Recuperado el 13 de 07 de 2010, de http://www.linktionary.com/q/qos.html

MikroTik Wiki. [20 de 12 de 2010] Mikrotik RouterOS Documentation. Recuperado el 05 de 01 de 2011, de http://wiki.mikrotik.com/wiki/Manual:TOC

ANEXOS

DOCTOR ROMEL MACHADO CLAVIJO,
SECRETARIO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACION DE LA UNIVERSIDAD DEL AZUAY,
C E R T I F I C A:

Que, el H. Consejo de Facultad en sesión realizada el 7 de enero de 2010, conoció la denuncia de tesis presentada por los señores **OSWALDO GEOVANNY SILVA JIMENEZ y EDWIN ANTONIO SALAZAR ORDOÑEZ** con el tema que deberá decir: "**Calidad de servicio en Redes Inalámbricas (QoS) en la Universidad del Azuay**", previa la obtención del grado de Ingeniero de Sistemas. El Consejo, en atención al informe favorable de la Junta Académica aprueba la denuncia presentada y designa como Director del trabajo al ingeniero Pablo Esquivel León y como miembros del Tribunal Examinador los ingenieros Fernando Balarezo Rodríguez y Fabian Carvajal Vargas. De conformidad a las disposiciones reglamentarias las denunciantes deberán presentar su trabajo en un plazo de **DIECIOCHO MESES** contados a partir de la fecha de aprobación, es decir **hasta el 7 de Julio de 2011.**

Cuenca, enero 8 de 2010

UNIVERSIDAD DEL AZUAY
FACULTAD DE ADMINISTRACION
SECRETARIA

UNIVERSIDAD DEL AZUAY

Cuenca, 21 de diciembre del 2009

Economista
Luis Mario Cabrera González,
DECANO DE LA FACULTAD DE CIENCIAS DE LA ADMINISTRACION,
Ciudad.

Señor Decano:

Nosotros: Oswaldo Geovanny Silva Jiménez, egresado de la Escuela de Ingeniería de Sistemas y, Edwin Antonio Salazar Ordóñez, estudiante de noveno ciclo de Ingeniería de Sistemas nos dirigimos a usted y por su digno intermedio al H. Consejo de Facultad, para solicitar de la manera mas comedida la aprobación del diseño de tesis "Calidad de Servicio en Redes Inalámbricas (QoS), previa la obtención del título de Ingeniero de Sistemas, así como la asignación del director.

Nos permitimos sugerir el nombre del Ingeniero Pablo Esquivel como director de Tesis por cuanto ha sido quien nos ha asesorado en la elaboración del diseño y por contar con su valiosa aceptación.

Por la atención a la presente, anticipamos nuestro agradecimiento.

Atentamente,

Oswaldo Silva Jiménez.
Cod. 29814

Edwin Salazar Ordóñez
Cod. 33107

Edición autorizada de 15.000 ejemplares
Del 0423501 al 0438500 Nº 0429694

UNIVERSIDAD DEL AZUAY

Cuenca, 11 de Diciembre de 2009

Señor Economista
Luis Mario Cabrera
Decano de la Facultad de Ciencias de la Administración
Ciudad.

De mi consideración.

Por medio de la presente me permito informar que el diseño de tesis adjunto, ha sido aprobado por la Junta Académica de la Escuela de Ingeniería de Sistemas en sesión del día martes 13 de Octubre de 2009, razón por la cual solicito, por su digno intermedio, el conocimiento y aprobación por parte del Consejo de Facultad

El diseño indicado se denomina: "Calidad de Servicio en Redes Inalámbricas (QoS)", planteado por los estudiantes Oswaldo Geovanny Silva Jiménez y Edwin Antonio Salazar Ordóñez.

Además pido por favor se sirva considerar como director de tesis a mi persona y como tribunal al Ing. Fernando Balarezo con el Ing. Fabián Carvajal.

Por la favorable acogida que se sirva dar al presente, anticipo mis agradecimientos

Atentamente,

Ing. Pablo Esquivel
Director de la Escuela de Ingeniería de Sistemas

Edición autorizada de 15.000 ejemplares
Del 0423501 al 0438500
Nº 0429695

UNIVERSIDAD DEL AZUAY

Cuenca, 11 de Diciembre de 2009

Señor Economista
Luis Mario Cabrera
Decano de la Facultad de Administración
De la Universidad del Azuay
Cuenca.-

De mis consideraciones:

Quien subscribe comunica a Usted que se ha procedido a revisar el Diseño de Tesis presentado por los estudiantes Oswaldo Geovanny Silva Jiménez y Edwin Antonio Salazar Ordóñez , con el tema **"Calidad de Servicio en Redes Inalámbricas (QoS)"**, como requisito previo a la obtención del título de Ingeniero de Sistemas, sobre el cual presento el siguiente informe:

1.- El contenido propone un trabajo de investigación objetivo y coherente sobre lo que es calidad de servicio en Redes Inalámbricas.

2.- El diseño cumple con los requisitos metodológicos básicos exigidos por la Facultad, en cuanto a la descripción del objeto de estudio, resumen del proyecto, situación actual, situación proyectada, justificación – impactos, procedimientos metodológicos, recursos, cronograma y bibliografía necesaria para el desarrollo de la tesis.

Por las consideraciones anotadas, se emite un informe favorable y salvo su mejor criterio, se recomienda la aprobación.

Atentamente,

Ing. Pablo Esquivel L.
DIRECTOR DE TESIS

Edición autorizada de 15.000 ejemplares
Del 0428501 al 0438500
Nº 0429696

UNIVERSIDAD DEL AZUAY

TÍTULO DEL PROYECTO

"Calidad de Servicio en Redes Inalámbricas (QoS)"

2. MARCO TEÓRICO

Hoy en día es común encontrarnos con redes inalámbricas que nos permiten estar conectados al mundo a través del internet, por lo que es importante aplicar calidad de servicio aunque en este tipo de redes se vuelve un poco más dificultoso debido a que existe factores externos que pueden afectar el funcionamiento de la red.

En la actualidad, QoS es parte importante de todo tipo de redes, Por lo que la configuración de la misma ha pasado a ser parte fundamental y requerida en todos los casos para lograr un funcionamiento óptimo y adecuado.

El QoS nos ayuda establecer un nivel de calidad de servicio a los usuarios a través de una serie de reglas que son creadas para distinguir los diferentes tipos de paquetes que se genera en una red, lo que nos permitirá priorizar a cada uno de ellos, dependiendo de las necesidades.

Ventajas

La mayoría de redes en la actualidad tienden a ser inalámbricas por las facilidades de implementación y esto se ve complementado con QoS, presentando entre algunas ventajas las siguientes:

- Menor tiempo de implementación y costos reducidos
- Ofrece mayor rango de movilidad al usuario debido a que no se necesitan cables
- Reducción de tiempo y costos en mantenimiento
- Facilita el crecimiento de usuarios dentro de la red
- Se puede priorizar servicios como Volp, Video, etc.
- Mejor administración del ancho de banda por usuario
- Control de ancho de banda en base a servicios

- Restricción y/o limitación de servicios innecesarios como P2P, MSN, etc.

Desventajas

No obstante un sistema de este tipo también puede presentar una serie de dificultades como por ejemplo:

- Debido al medio de transmisión se expone a posibles fallos por factores externos
- Mayor vulnerabilidad a posibles ataques (Hacking)
- Rápida evolución de tecnología y discontinuidad de equipos

3. IDENTIFICACION DEL PROBLEMA

Como hemos mencionado hoy en día la implementación de redes inalámbricas es muy común en nuestro medio, generalmente ninguna de estas redes logra un óptimo desempeño, debido a que normalmente no se aplica QoS para priorizar y restringir servicios y controlar el ancho de banda.

Aplicar QoS a una red inalámbrica puede ser de gran utilidad si queremos lograr un buen desempeño de la misma, así los usuarios tendrán un servicio eficiente de una calidad aceptable.

Uno de los principales problemas en una red inalámbrica es que no se puede garantizar un servicio 100% confiable ya que no depende únicamente del QoS, ya que existen factores externos como interferencias que afectar el rendimiento.

Para aplicar QoS se necesita un conocimiento intermedio avanzado de networking, además necesitamos dedicar tiempo para el análisis de los problemas que presenta la red en cuanto al tipo de trafico que se está generando, así de esta manera establecer las reglas de calidad que nos ayudaran a mejorar el rendimiento.

UNIVERSIDAD DEL AZUAY

4. JUSTIFICACION DEL PROBLEMA

Es en función de resolver los problemas mencionados en el apartado de este documento llamado "Identificación del Problema", hemos visto necesario utilizar una solución basada en QoS utilizando como plataforma un Sistema Operativo diseñado exclusivamente para la administración de redes el cual nos permitirá sacar el máximo provecho a una red.

El Sistema Operativo que utilizaremos es una versión basada en Linux llamada Mikrotik RouterOS, esta nos permite conectarnos remotamente al equipo de diferentes maneras como: interfaz gráfica, web, ssh, telnet. Una de las más usadas es la aplicación llamada Winbox ya que está diseñada para Windows, esta utiliza una interfaz gráfica, es intuitivo y fácil de operar, hay que tener en cuenta que no todas las funciones están implementadas solo son accesibles por consola.

5. OBJETIVOS

Objetivo general

- Elaborar QoS para una Red Inalámbrica utilizando un servidor Mikrotik

Objetivos específicos

- Elaborar QoS para la Red Inalámbrica de la Universidad del Azuay.
- Administrar el ancho de banda por protocolo capa 7
- Generar reportes mediante MRTG
- Generar alertas automáticas mediante envió de emails en caso de fallos en puntos de acceso
- Configuración del firewall de Mikrotik
- Elaborar un manual de instalación y uso de los puntos anteriores

6. ALCANCE Y METODO DE TRABAJO.

Creemos conveniente que para Elaborar la QoS de este servidor, se debe realizar

las siguientes etapas de investigación y desarrollo, las cuales detallamos a continuación:

Recopilación y análisis de material bibliográfico, publicaciones, artículos, etc, relacionados con Redes Inalámbricas y Aplicación de QoS, lo cual nos permitirá conocer los preceptos teóricos necesarios para entender el funcionamiento de la calidad de servicio y como aplicarlo.

Profundizar el estudio de QoS aplicando capa 7, para priorizar y restringir el tráfico por tipo de protocolo utilizado y de esta manera lograr un buen rendimiento de la red.

Estudiaremos el funcionamiento del firewall que se puede aplicar en el sistema operativo Mikrotik, lo cual nos permitirá conocer sobre las seguridades que se pueden configurar e implementar en el servidor para evitar algún tipo de vulnerabilidad.

Analizaremos herramientas de Monitorio que incluyen el Sistema Operativo, lo que nos ayudara a llevar un control de los puntos de acceso y un historial de su uso, el sistema podrá generar gráficas MRTG del consumo por punto de acceso, usuario y consumo general de toda la red, también podrá disparar alarmas vía email cuando se pierda conexión a algún punto de acceso.

La implementación de la QoS en Redes Inalámbricas, contara con tres módulos esenciales para el desarrollo que se describen a continuación:

Primer Módulo.- Construcción de la documentación en base a las referencias que se han obtenido previas al desarrollo de la tesis, conceptos generales: Redes Inalámbricas, QoS y Firewall.

Segundo Módulo.- Documentación del Sistema Operativo Mikrotik RouterOS, y conceptos de las herramientas utilizadas.

Tercer Módulo.- Instalación de Mikrotik RouterOS y aplicación de Firewall, QoS y configuración de herramientas de MRTG y Disparadores de Alertas.

UNIVERSIDAD DEL AZUAY

7. ESQUEMA TENTATIVO

1 Redes inalámbricas
- 1.1 Introducción y conceptos
- 1.2 QoS en redes inalámbricas

2 Sistema Operativo Mikrotik RouterOS
- 2.1 Características Principales
- 2.2 Firewall
- 2.3 QoS
- 2.4 Colas
- 2.5 Herramientas de manejo de red
- 2.6 Administración de Mikrotik

3 Configuración servidor Mikrotik
- 3.1 Firewall
- 3.2 Filtrado de paquetes
- 3.3 Control de ancho de banda
- 3.4 Monitor de trafico
- 3.5 Alertas mediante email

4 Pruebas
- 4.1 Instalación y configuración de un monitor de red para ver el estado actual de la red
- 4.2 Instalación y configuración de un monitor de red para ver los cambios con la configuración nueva de la red

5 Documentación final
- 5.1 Elaboración del manual de instalación y configuración de Mikrotik de los pasos anteriores
- 5.2 Elaboración del Manual de Usuario.

6 Conclusiones

7 Recomendaciones

8 Bibliografía

8. PROCEDIMIENTOS METODOLÓGICOS

UNIVERSIDAD DEL AZUAY

Con el fin de recopilar toda la información necesaria para la administración de una red inalámbrica con QoS, hemos visto la necesidad de hacer uso de las siguientes técnicas de investigación:

Libros y Material Bibliográfico:

Serán indispensables, a fin de obtener los conocimientos necesarios sobre el tema del proyecto a desarrollar.

- **Navegación en Internet**

Este método de investigación será fundamental para el desarrollo de nuestro proyecto, debido a la existencia de escaso material bibliográfico impreso sobre el tema, complicando la tarea de recopilación de dicho material dentro de nuestro medio.

Además de que, este método se caracteriza por proveer diversos tipos de material de actualidad, como por ejemplo: investigaciones, publicaciones, wikis, etc., y de otras fuentes de información también de relevancia como son: foros, debates, experiencias, etc.

9. RECURSOS TÉCNICOS Y FINANCIEROS

Recursos Humanos

Con el propósito de alcanzar los objetivos planteados en este proyecto, serán necesarios los siguientes recursos humanos y materiales:

- Director de tesis.
  Ing. Pablo Esquivel L.

- Desarrolladores del proyecto:
  Edwin Antonio Salazar Ordóñez.
  Oswaldo Geovanny Silva Jiménez

Recursos Materiales

Para la elaboración del proyecto se requerirán los siguientes recursos materiales:

Hardware

1. Computadores personales.
2. Servidor PC X86 platform
3. Conexión a internet.
4. Impresora.

Edición autorizada de 15.000 ejemplares
Del 0423501 al 0438500 Nº 0432355

UNIVERSIDAD DEL AZUAY

Software

Mikrotik RouterOS 3.30

Recursos Financieros

Los siguientes recursos son necesarios para el desarrollo del proyecto:

1. Servidor PC x86.....$635,00
2. Licencia Mikrotik level 6.....$250,00
3. Router board rb450.....$215,00
4. Servicio de Internet.....$200,00

Total: Mil trescientos dólares de estados unidos de América.

Edición autorizada de 15.000 ejemplares
Del 0423501 al 0438500
Nº 0426822

UNIVERSIDAD DEL AZUAY

10. CRONOGRAMA

Fases \ Tiempo	Mes 1				Mes 2				Mes 3				Mes 4				Mes 5				Mes 6			
	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Investigación y recopilación de información.	x	x																						
Análisis Mikrotik RouterOS.			x	x	x	x	x	x																
Configuración y pruebas									x	x	x	x	x	x	x	x								
Documentación									-								x	x	x	x	x	x		

13. BIBLIOGRAFÍA

Referencias:

[1]. John Evans, Clarence Filsfils. "Deploying IP and Mpls QoS for Multiservice Networks", The Morgan Kaufmann Series in Networking, 2007.

[2]. Mario Marchese. "QoS Over Heterogeneous Networks", John Wiley & Sons Ltd, 2007.

[3]. José M. Huidobro Moya, David Roldán Martínez "Comunicaciones en Redes WLAN", Editorial LIMUSA, SA. 2006 México DF.

[4]. Andrew A. Vladimirov, Konstantin V. Gavrilenko, Andrei A. Mikhailovsky. "Hacking Wireless Seguridad en Redes Inalámbricas", Grupo Anaya, SA. 2005 Madrid.

[5]. Stephen J. Bigelow. "Localización de averías, reparación, mantenimiento y optimización de Redes", McGraw-Hill/Interamericana de España, S.A.U. 2003 España.

Sitios Web:

- Mikrotik Routers and Wireless, http://www.mikrotik.com
- Mikrotik RouterOS V3.0 Reference Manual, http://www.mikrotik.com/testdocs/ros/3.0
- Main Page – Mikrotik Wiki, http://wiki.mikrotik.com/wiki/Main_Page
- Mikrotik RouterOS – Index page (Foro)http://forum.mikrotik.com/
- Mikrotik – Wikipedia, http://es.wikipedia.org/wiki/Mikrotik