ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"ANÁLISIS DE DESEMPEÑO Y OPTIMIZACIÓN DE MECANISMOS DE QoS EN UN ENTORNO WAN"

INFORME DE PROYECTO INTEGRADOR

Previo a la obtención del Título de:

LICENCIADO EN REDES Y SISTEMAS OPERATIVOS

JOHANNA JAZMIN ALVAREZ ALVAREZ

JOHANA INES NEIRA CORNEJO

GUAYAQUIL - ECUADOR

AÑO: 2015

AGRADECIMIENTOS

Agradecemos en primer lugar a Dios por habernos brindado la sabiduría a lo largo de todo este tiempo y culminar con éxito esta etapa universitaria. De manera muy especial a nuestros profesores de LICRED que supieron con mucha paciencia y dedicación inculcarnos sus conocimientos y forjarnos como buenas profesionales además de tener la colaboración de cada uno de ellos en cualquier momento que lo hemos necesitado. Que Dios y la Virgen María les paguen con muchas bendiciones.

DEDICATORIA

Sin lugar a dudas este trabajo se lo dedico a Dios por haber sido mi guía y mi fortaleza. A todos los miembros de mi familia que siempre estuvieron allí para darme una palabra de aliento cuando lo necesitaba pero de manera especial quiero hacer hincapié y nombrar a mi padre que a lo largo de todos estos años es quien ha estado siempre a mi lado y me ha ayudado a levantarme cuando he flaqueado y he caído, a él le dedico este y todos mis logros.

Johanna Jazmín Alvarez Alvarez

Esta tesis la dedico a mi madre que estuvo a mi lado brindándome su mano amiga dándome a cada instante palabras de aliento para llegar a culminar mi profesión, a mi hermana que fue mi fuente de luz; ambas pilares fundamentales para mi profesión y a mi amiga – compañera de Tesis por su esfuerzo y paciencia durante este periodo.

Johana Inés Neira Cornejo

TRIBUNAL DE EVALUACIÓN

_____	_____
Ing. José Roberto Patiño Sánchez	**Ing. Albert Giovanny Espinal Santana**
PROFESOR EVALUADOR	PROFESOR EVALUADOR

DECLARACIÓN EXPRESA

“La responsabilidad y la autoría del contenido de este Trabajo de Titulación, nos corresponde exclusivamente; y damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual”

_____

Johanna Jazmín Alvarez Alvarez

_____

Johana Inés Neira Cornejo

RESUMEN

El presente documento, nos muestra información detallada sobre cómo podemos controlar el tráfico en las redes WAN con diferentes mecanismos de calidad de servicio; los cuales nos ayudan a repartir o planificar como hacer un “reparto” de recursos (ancho de banda, Delay, jitter y pérdida de paquetes) de la red entre los diferentes servicios que nos provee.

El análisis expuesto de la red del Distrito Hotelero presentaba problemas como mala administración de ancho de banda, no funcionaba el balanceo de carga, mala configuración de la tabla de direccionamiento y mal uso de la red por parte del área administrativa de los hoteles.

La solución que presentamos en este documento ante los problemas expuestos de dicha red fue adquirir un nuevo equipo para que actúe como Router en el cual se realizaría el balanceo de carga y el firewall. Además de realizar la correcta configuración del CORE en el cual se administraría las redes tanto del área de los huéspedes como del área de administración.

ÍNDICE GENERAL

CAPÍTULO 1

1. INTRODUCCIÓN

1.1. Descripción

Debido al avance progresivo de las redes, han hecho que estas soporten diferentes tipos de servicios y aplicaciones con requerimientos de performance muy diferentes tales como voz, video y datos sobre una infraestructura común. Cada uno de estos tipos de tráfico tiene varios requerimientos de ancho de banda, retardo, perdida de paquetes, etc.; las cuales en conjunto representan un gran reto para el personal administrador.

Para poder dar respuesta a los diferentes requerimientos de las aplicaciones y servicios sobre una misma infraestructura de red se requiere implementar calidad de servicio QoS, y así asegurar la entrega de información necesaria, dando preferencia a las aplicaciones críticas sobre las demás aplicaciones de menor importancia.

La QoS permite hacer uso eficiente de los recursos de la red ante una situación de congestión, al seleccionar un tráfico especifico de la red y así priorizarlos según su importancia dentro de la red.

En conclusión esta tesis presenta un conjunto de estudios sobre técnicas de optimización del tráfico de servicios de tiempo real, aplicables en el caso de que un número de flujos compartan la misma ruta.

En este escenario la eficiencia se puede mejorar mediante la compresión de cabeceras cuyos campos se repiten o se incrementan de uno en uno para todos los paquetes del flujo. Posteriormente se pueden multiplexar varios paquetes en uno más grande, que se envía de extremo a extremo utilizando túneles.

1.2. Antecedentes

En la actualidad se busca que en las redes de computadoras, así como en los servicios ofrecidos a los usuarios sean eficientes y eficaces. Sin embargo una red homogénea y unificada requiere un cierto nivel de calidad. Para solucionar este problema, se han buscado implementar métodos para satisfacer la demanda de calidad de servicio (QoS).

El concepto de QoS (Quality of Service) puede variar dependiendo del autor, según la ISO/IEC es un conjunto de cualidades relacionadas con la provisión de un servicio hacia un usuario, hoy en día los usuarios de servicios de internet pueden ser tanto humanos como programas de aplicación, buscadores, bases de datos, multimedia, telefonía, entre otros.

Ofrecer QoS en una red convergente es un trabajo donde se ven inmersos una serie de procedimientos que se deben realizar de manera conjunta y dependen de la topología, tecnologías de transporte y dispositivos de interconectividad que se posean tanto el acceso como en el núcleo de la red.

Se debe ofrecer QoS en el bucle de acceso del usuario a la red convergente, ya que generalmente es en este sector donde empieza la congestión y degradación de desempeño de las aplicaciones, pero se debe tener en cuenta el tipo de dispositivo que conecta al usuario a la red, ya que generalmente son dispositivos sencillos y con limitaciones de hardware que permiten configuraciones limitadas en lo referente a QoS.

Paralelo a lo anterior se debe analizar qué tipo de QoS se le va a ofrecer a ese usuario en la red de núcleo, con el fin de garantizar que los parámetros de la recomendación estén dentro de valores admisibles y se garantice buen desempeño y satisfacción al usuario.

1.3. Objetivos

General

Controlar el tráfico en redes WAN fundamentado en procedimientos y técnicas de calidad de servicio a lo largo de una infraestructura de telecomunicaciones.

Específicos

- Analizar el funcionamiento adecuado de los servicios de voz, video y datos; de acuerdo al manejo de parámetros críticos que causan problemas de rendimiento entre ellos:
    - Ancho de Banda
    - Perdida de Paquetes
    - Delay
    - Jitter
- Administrar la congestión de una red WAN aplicando técnicas de encolamiento y prevención de congestión.
- Conocer cada uno de los métodos de QoS que se pueden aplicar sobre los diferentes tipos de tráfico en cada uno de los puntos de la infraestructura de telecomunicaciones:
    - ✓ FIFO
    - ✓ PQ (Priority Queuing)
    - ✓ CQ (Custom Queuing)
    - ✓ WFQ (Weighted Fair Queuing)
    - ✓ CBWFQ (Class-Based Weighted Fair Queuing)
    - ✓ LLQ (Low Latency Queue)
- Diseño comparativo de los diferentes mecanismos de QoS.

1.4. Justificación

Esta propuesta de estudio y análisis está dirigido al sector empresarial que tiene como fin promover el buen servicio de la transmisión de datos, controlando el tráfico y prevaleciendo la entrega de la información a lo largo de la red sin problemas e inconveniente alguno; la misma será realizada para plasmar las ventajas y desventajas que pueden proporcionar los diferentes mecanismos de QoS en un entorno WAN.

Se propondrá en esta propuesta un análisis de una red con el propósito de ilustrar de una manera gráfica y a un nivel de representación más abstracta y entendible el funcionamiento de dichos métodos, para así mismo comprender mejor su arquitectura.

1.5. Metodología

- ✓ Realizar una investigación de los servicios de voz, video y datos para encontrar la causa de los problemas de rendimiento entre ellos.
- ✓ Realizar una investigación de QoS; concepto, parámetros, arquitectura, beneficios, modelos de servicio.
- ✓ Realizar una investigación de cada uno de los métodos de QoS; establecer ventajas, desventajas y características.
- ✓ Realizar el análisis del diseño de una red a la cual se le pueda aplicar QoS para solventar sus problemas.

CAPÍTULO 2

2. MARCO TEÓRICO Y ANTECEDENTES BIBLIOGRAFICOS

2.1. Calidad de Servicio– QoS

Tomando como referencia estándares internacionales acerca del término calidad de servicio, se lo puede definir como un conjunto de procesos colectivos dentro de una infraestructura para satisfacer sus requerimientos en tiempo real.

De acuerdo a la IETF (Internet Engineering Task Force) se considera que la calidad de servicio QoS es la habilidad de segmentar tráfico o diferenciar entre los distintos tipos de tráfico que cruzan la red de datos para que cada flujo sea tratado distintamente.

Desde el punto de vista de la red de comunicación, la calidad de servicio QoS permite una administración y control de características de algunos tipos de tráfico (audio, video, imagen fija y datos digitales).

En definitiva, la calidad de servicio se refiere a la habilidad de la red, de ofrecer prioridad a unos determinados tipos de tráfico, sobre diferentes tecnologías, incluyendo: Frame Relay, Asynchronous Transfer Mode (ATM), LANs y líneas dedicadas.

El objetivo de la calidad de servicio en una red es cuantificar el tratamiento que un paquete debe esperar a medida que circula por la red.

2.2. Métodos básicos para QoS

Existen dos métodos básicos para brindar QoS:

Con Reserva.- En este método se reservan recursos explícitamente. En este caso la red clasifica el flujo de paquetes entrantes y manipula esta identificación para proveer un servicio diferenciado [1].

Sin Reserva.- En este método no existen recursos reservados explícitamente. El tráfico se clasifica en un tipo de clase y la red provee servicio a las distintas clases basándose en su prioridad. Es necesario que la red diferencie el tráfico, controlando la cantidad de tráfico de una determinada clase permitida, para mantener la calidad de servicio que se le brinda a otros paquetes de la misma clase [1].

2.3. Clase de Servicio – CoS

La Clase de Servicio es el esquema de prioridad 802.1 p, esta proporciona un método de asignación de etiquetas a los paquetes con información sobre la prioridad [1].

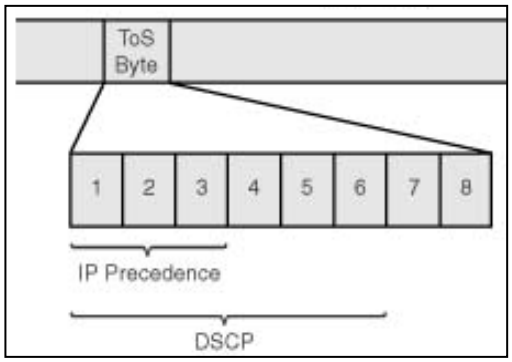
VALORES DE CoS	VALORES DE LAS COLAS DE REENVIO
0	Q2
1	Q1 (Prioridad más baja)
2	Q1 (Prioridad más baja)
3	Q2
4	Q3
5	Q3
6	Q4 (Prioridad más alta)
7	Q4 (Prioridad más alta)

Tabla 1: Valores Predeterminados de Asignación de CoS a Cola

El valor de la clase de servicio está dado entre 0 y 7, este valor es agregado al encabezado de la capa 2 de los paquetes, donde el 0 es la prioridad más baja y el 7 la prioridad más alta.

2.4. Tipo de Servicio – TOS

El Tipo de Servicio proporciona una indicación de los parámetros abstractos de la calidad de servicio deseada. Estos parámetros se usarán para guiar la selección de los parámetros de servicio reales al transmitir un datagrama a través de una red en particular [1].



2.1: Tipo de Servicio – TOS

Imagen tomada de: www.ciscopress.com

Los tres primeros campos representan una prioridad que se denomina precedencia el cual permite marcar los datagramas según su importancia.

111	Control de Red
110	Control entre Redes
101	Critico
100	Muy Urgente
011	Urgente
010	Inmediato
001	Prioridad
000	Rutina

Tabla 2: Valores de Precedencia TOS

El resto se utiliza para solicitar algunas características del servicio (mínimo retardo, máximo Throughput, máxima fiabilidad y mínimo coste) excepto el último que siempre es cero.

2.5. Parámetros de Calidad de Servicio

Los parámetros de QoS pueden cambiar de acuerdo al tipo de servicio en tiempo real, pero se enunciará a continuación los parámetros genéricos requeridos sobre una red de servicios convergentes.

Ancho de Banda.- Se refiere a la capacidad del canal usada o disponible, los proveedores de servicio generalmente aseguran el máximo ancho de banda al cliente y esto debe estar claramente especificado dentro del acuerdo de nivel de servicio SLA (Service Level Agreement).

Perdida de Paquetes.- Las comunicaciones en tiempo real están basadas en el protocolo UDP. Este protocolo no está orientado a conexión y si se produce una pérdida de paquetes no se reenvían. Además la perdida de paquetes también se produce por descartes de paquetes que no llegan a tiempo al receptor.

Delay.- Es el tiempo tomado por un paquete en viajar desde un punto de acceso de servicio hacia un destino determinado. Generalmente este parámetro incluye el tiempo de transporte en la red y el retardo de encolamiento del mismo.

Jitter.- Es la variación en tiempo real entre los paquetes que llegan, causados por la congestión de la red o cambios de ruta [2].

2.6. Modelos de Servicios

Describen un conjunto de capacidades de la calidad de servicio de extremo a extremo. Para comprobar cómo estos realizan un control de congestión y a qué nivel de rigor son capaces de proporcionar QoS.

2.6.1. Modelo del Mejor Esfuerzo (BEST-EFFORT)

El modelo del mejor esfuerzo es un modelo de servicio único en el que una aplicación envía datos en cualquier momento, en diferentes cantidades, y sin pedir permiso, ni notificar previamente a la red. Para el servicio de mejor esfuerzo, la red envía los datos sin ninguna garantía de fiabilidad, los límites de retardo, o el rendimiento, sin garantizar que la información llegue a su destino.

El modelo Best effort es adecuado para una amplia gama de aplicaciones de red tales como transferencias de archivos generales o de correo electrónico. Por lo que no es muy óptimo para aplicaciones que son sensibles a los retardos de la red, provocando así fallos en la transferencia de información. Un ejemplo muy representativo es FIFO [3].

2.6.2. Modelo de Servicio Integrado (INTSERV Integrated Services)

Este modelo de servicio incluye tanto el servicio de mejor esfuerzo o Best-effort y en tiempo real. Este modelo reserva los recursos a lo largo del trayecto de transmisión de la información vía RSVP, en otras palabras establece un circuito virtual. Además usa un servicio determinista y predictivo que se encuentra enfocado a los requerimientos individuales para cada aplicación. En este modelo se manejan dos tipos de clases de tráfico que son: el servicio de carga garantizado y el servicio de carga controlada.

Servicio de Carga Garantizada: Este servicio provee una garantía de gran ancho de banda y límites estrictos en los retardos y por eso es usado para aplicaciones sin distorsión por ejemplo la videoconferencia, por lo que ofrece una perfecta confiabilidad sobre el límite superior del retardo.

Servicio de Carga Controlada: Este servicio ofrece un tiempo de respuesta aunque sin garantías estrictas, por lo que los recursos deben ser reservados para el peor de los casos, al existir ráfagas conlleva una baja utilización de la red y un costo elevado de los recursos.

Este servicio es conocido como servicio predictivo y es bastante confiable, ya que trabaja adecuadamente cuando la red esta levemente cargada, pero, si la red está saturada, se puede presentar algunos paquetes descartados o retardos.

Los beneficios del modelo del servicio integrado es el control de admisión de recursos de extremo a extremo, políticas de control por admisión, por petición y señalización. Como desventaja se puede decir que cada flujo de información necesita señalización continua, usando así recursos extras y haciendo que no sea un modelo altamente escalable [3].

RSVP

Resource Reservation Protocol, es un protocolo de señalización orientado principalmente a redes Ip y que proporciona control para la reserva. Opera sobre IPv4 e IPv6. Debido a que IP no permite realizar reserva de recursos, los mensajes RSVP se envían en paralelo con los paquetes IP. RSVP no es un protocolo de transporte ni de encaminamiento, más bien funciona sobre cualquiera de ellos ya sea unicast o multicast, podría decirse que es un protocolo de control de internet [1].

2.6.3. Modelo de Servicio Diferenciado (DiffServ)

Este modelo es el más actual de los tres y ha sido desarrollado para suplir las deficiencias de los anteriores modelos. Este modelo se encuentra detallado en los

RFC 2474 y 2475. Su objetivo es el de posibilitar una discriminación de servicios escalable en Internet y redes IP.

Este modelo es basado en el concepto de que el tráfico entrante en la red es clasificado y posiblemente marcado, de forma que sea un tratamiento diferenciado de paquetes, y es muy usado para infraestructuras grandes de red como es el Internet.

Este método surge con la alternativa para los servicios integrados para satisfacer los requerimientos como son alta prestaciones, escalabilidad; y así permitir el crecimiento sostenible del tamaño de las redes y su ancho de banda, entre otros parámetros que se mencionaron anteriormente. Entonces este modelo está orientado hacia un servicio de borde a borde a través de un dominio único, con un apropiado SLA17 que se asume está en su lugar en los bordes del dominio [3].

2.7. Marcado y Clasificación de Paquetes

La **clasificación** es el proceso de identificar flujos de paquetes y agruparlos en clases para aplicarles parámetros QoS. Un flujo Ip se identifica por:

- ➔ Ip destino, Ip fuente.
- ➔ Puerto origen, Puerto destino.
- ➔ Protocolo TCP/UDP.

El **marcado** de paquetes corresponde a la alteración de los campos asignados para QoS para que sean procesados posteriormente en función de la marca:

- ➔ Campo TOS en IPv4.
- ➔ Campo Traffic Class IPv6 [4].

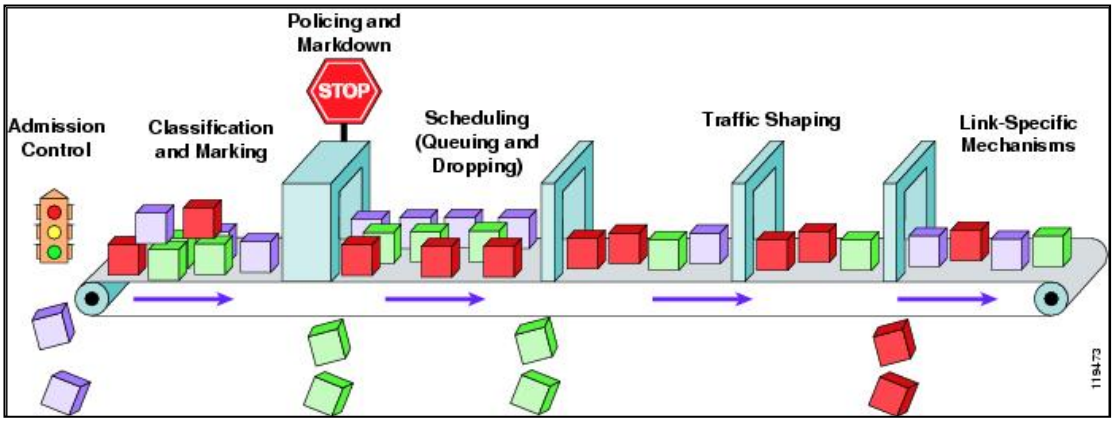


Figura 2.2: Clasificación y Marcado de Paquetes

Imagen tomada de:
http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/WAN_and_MAN/QoS_SRND/QoS-SRND-Book/QoSIntro.html

QoS mediante clasificación consta de tres etapas:

1. Los paquetes se marcan o clasifican en clases.
2. Al envío de paquetes se le aplica una disciplina de planificación en función de su clasificación.
3. La velocidad de envío de paquetes se regula, globalmente o para cada clase.

A continuación se describen algunos métodos importantes para la marcación y la clasificación de paquetes dentro de la calidad de servicio.

2.7.1. Precedencia IP

Es uno de los métodos de Servicios Diferenciados para la ubicación de recursos en la red. Los tres bits en la cabecera IP designados como el campo de tipo de servicio

(ToS) puede ser manipulado para informar a los dispositivos de red que una prioridad debería ser dada al paquete IP a medida que este viaja a través de la red.

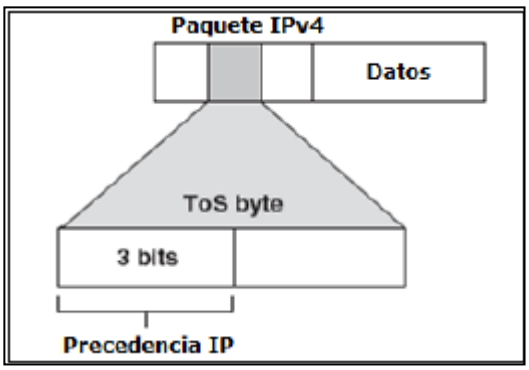


Figura 2.3: Precedencia IP del campo ToS en la cabecera IPv4

Imagen tomada de: http://docwiki.cisco.com/wiki/Quality_of_Service_Networking

Los tres bits más significativos del campo ToS en la cabecera IP constituyen los bits usados para la precedencia IP. Estos bits son usados para proporcionar una prioridad de 0 a 7 (los ajustes de 6 o 7 son reservados y no son configurados por un administrador de red) para el paquete IP.

Se puede dividir tráfico en no más de seis clases de servicio usando la precedencia IP (los otros dos son reservados para uso interno de la red). Entonces, las tecnologías de encolamiento a lo largo de la red pueden usar esta señalización para proporcionar la apropiada manipulación acelerada.

Debido a q solo tres bits del byte ToS son usados para la precedencia IP, se necesita diferenciar estos bits del resto dentro del byte ToS. El tráfico que es identificado puede ser marcado por la colocación de los bits de precedencia IP. En consecuencia, el tráfico necesita ser clasificado solamente una vez. RFC 2475 extiende el número de bits usados en el byte ToS de 3 a 6. Los seis bits más significativos serán usados para la colocación de la precedencia (conocida como puntos de código DS), con los 2 bits menos significativos (los dos bits más a la

derecha) reservados para un uso futuro. Esta especificación es comúnmente referida al DiffServ [4].

2.7.2. Clasificación de Paquetes usando Precedencia IP

Como se mencionó anteriormente, se usan tres bits de precedencia IP en el campo ToS de la cabecera IP para especificar la clase de servicio asignada para cada paquete, adicional a esto, se debe usar políticas de red con el objetivo de definir términos de manipulación de congestión y asignación de ancho de banda para cada clase.

DECIMAL	BINARIO	NOMBRE
0	000	Rutina
1	001	Prioridad
2	010	Inmediato
3	011	Urgente
4	100	Muy urgente
5	101	Critico
6	110	Control de Internet
7	111	Control de Red

Tabla 3: Valores de IP Precedence

En la siguiente tabla se muestra los valores para Precedencia IP con sus respectivos nombres, desde el menos significativo al más importante.

La característica de la precedencia IP permite una considerable flexibilidad para la asignación de precedencias. Esto es, se puede definir un mecanismo propio de clasificación. La asignación del bit de precedencia IP 6 y 7 son reservados para el control de información de red tal como las actualizaciones de enrutamiento [4].

2.7.3. Beneficios de Marcación de Paquetes

Cuando se usa la marcación de paquetes basados en valores de IP Precedence y DSCP IP para los paquetes que entran a la red, los dispositivos internos de la red pueden determinar como el tráfico debería ser tratado usando diferentes técnicas para la administración de la congestión que se detallan en los siguientes apartados. Se usa la marcación de paquetes basados en un Grupo QoS, los enrutadores usan este grupo para determinar cómo priorizar los paquetes para la transmisión en la red [4].

2.7.4. Tasa de Acceso Comprometida

Es un mecanismo de garantía, uno de los más usados ampliamente para el marcado de paquetes en la red, que se basa en las siguientes funcionalidades.

Clasificación de Paquetes: Consiste en distribuir el tráfico en clases de servicio según diferentes políticas como las direcciones IP, el tipo de acceso, etc., considerando el bit de precedencia IP del campo ToS de la cabecera Ip. A cada clase de servicio le corresponde determinada QoS, con su política de gestión de tráfico que incluye gestión de congestión, asignación de ancho de banda y limites de retardo.

Limitación de la Tasa de Transmisión: Consiste en limitar la máxima velocidad de transmisión de tráfico en la interfaz de acceso de la red. Cuando el tráfico excede la tasa límite, se aplican políticas de acción de tráfico. Si el tráfico esta dentro del límite se le permite pasar, caso contrario es transmitido con la prioridad más baja o descartado.

Esta función se realiza en 3 fases:

- *Equiparación de Tráfico:* Identifica el tipo de tráfico para limitar la tasa de transferencia y configurar la precedencia.

- *Medición de Tráfico:* Determina si el tráfico excede o no la tasa de transferencia limite.
- *Política de Acción:* Es la acción a ejecutarse con el tráfico previamente medido, si esta dentro de la tasa límite se ejecuta la acción de conformidad correspondiente, de lo contrario se ejecuta la acción de exceso correspondiente [4].

2.7.5. Encaminamiento basado en Políticas

El enrutamiento basado en políticas (Policy Based Routing o PBR) es un mecanismo para implementar decisiones de enrutamiento de paquetes de datos basados en políticas definidas por el administrador de red.

Cuando un router recibe un paquete, analiza la IP destino y la compara con su tabla de enrutamiento. El PBR permite establecer funciones de enrutamiento basándose en otros criterios, como la dirección origen del paquete, el tipo de tráfico o cualquier otra información contenida en el paquete.

Para permitir el uso de éstas políticas se hace uso de los route maps. Los Route Maps establecen un conjunto de sentencias aplicables según las coincidencias establecidas, una especie de “si -> entonces” lógicos que se configuran en el router (similar a los access lists) [5].

2.7.6. Marcación de Paquetes basado en Clases

La característica de la marcación de paquetes basado en clases provee medios para una eficiente marcación de paquetes mediante los cuales, los usuarios pueden diferenciar paquetes basados en las marcaciones designadas. Permite a los usuarios realizar las siguientes tareas:

- Marcar paquetes por configuración de los bits de la precedencia IP o DSCP en el byte IP ToS.

- Marcar paquetes por configuración del valor clase de servicio CoS (Class of Service) de capa 2.
- Asociar un valor de grupo QoS local con un paquete.

2.8. Traffic Shaping

Un sistema de conformación de tráfico es aquel que permite adecuar el tráfico de datos entrante que proviene de algún nodo de la red dándole un tratamiento especial llamado conformación de tráfico aceptado y que permita de esta manera que las tramas sean reenviadas a través de la red de datos bajo las reglas de tráfico sin haber pasado por algún método de conformación de tráfico, este puede ser detectado como tráfico no conformado en el borde de acceso a la red metropolitana a descarte [6].

GTS (Generic Traffic Shaping o Conformado del Tráfico Genérico)

GTS es un mecanismo de control del flujo del tráfico en un interfaz determinado, donde la circulación de salida es reducida para evitar la congestión y obligando a determinado tráfico a una tasa de bit particular mientras se encolan las ráfagas del citado tráfico. Así, el tráfico adherido a una topología puede ser tratado para configurarlo según los requisitos del tráfico saliente, eliminando los cuellos de botella en topologías con tasa de datos desiguales [6].

Conformado en Frame Relay - FRTS (Frame Relay Traffic Shaping): Gestión del tráfico Frame Relay

FRTS proporciona parámetros útiles para la gestión de la congestión. Incluye CIR, FECN, BECN y el bit DE. Las características de FRTS sobre Frame Relay hacen que este soporte capacidades adicionales que mejoren la escalabilidad y actuación de estas redes, aumentando el número de circuitos virtuales y mejorando el tiempo de respuesta.

Permite configurar los valores de la tasa de tráfico, el CIR u otro valor, así como la prioridad y el encolamiento, dando un mayor control sobre el flujo de tráfico en cada circuito virtual individual.

FRTS puede eliminar los cuellos de botella en las redes Frame Relay con conexiones de gran velocidad en los puntos centrales y conexiones de baja velocidad en los extremos. El administrador podría configurar la tasa de tráfico entre los distintos puntos de la red [6].

Conformado en Redes IP

En redes IP con QoS, es necesario especificar el perfil de tráfico de una conexión para decidir cómo asignar los distintos recursos de la red. El conformado o condicionado del tráfico asegura que el tráfico entrante en un extremo o en un nodo central se adhiere al citado perfil. Típicamente este mecanismo se usa para reducir las grandes ráfagas de tráfico entrantes. Esto implica la toma de decisión entre los beneficios que pueden dar el conformado (por ejemplo las pérdidas de cadenas de la red) y el retardo que forma [6].

Conformado del Trafico en ATM

Traffic shaping es un mecanismo que altera las características de tráfico del flujo de celdas de una conexión para alcanzar una mejor eficiencia en la red mientras se mantienen los objetivos QoS o con la finalidad de asegurar que el flujo de celdas sea conforme con los parámetros de tráfico de acuerdo con la configuración del algoritmo leaky bucket del contrato de tráfico. El traffic shaping puede ser empleado en ATM, por ejemplo, para reducir la velocidad pico, limitar la longitud de la ráfaga por medio del espaciamiento adecuado de las celdas en el tiempo. El uso y ubicación de esta función es específica de la red [6].

2.9. CAR (Committed Access Rate)

Hoy en día en las redes es más común encontrarse con tráfico innecesario, tráfico que no responde a los objetivos de por qué existe la red. Muchas veces este tráfico afecta de modo directo la disponibilidad de recursos de dicha red.

CAR (Committed Access Rate) es un método que permite administrar el tráfico no deseado de modo de asegurarnos que no afecte el tráfico propio de la operación de la red. Hay que tener en cuenta algunas consideraciones previas:

- ✓ CAR solamente afecta el tráfico IP. No opera sobre el tráfico no-IP.
- ✓ Para utilizar CAR es necesario habilitar CEF (Cisco Express Forwarding) en el router.
- ✓ Esencialmente, CAR controla el ancho de banda que puede ocupar cierta tipo de tráfico, que es definido a través de una ACL.
- ✓ CAR puede referirse tanto al tráfico que ingresa, como al que sale a través de la interfaz en la que se aplica CAR [7].

2.10. Políticas de Encolamiento

Los mecanismos de encolamiento, son técnicas usadas para controlar la congestión temporal en una interfaz de salida de un dispositivo de red, creando colas, reteniendo paquetes en ellos y planificando el reenvío de los paquetes.

- ➢ **FIFO**

Es el tipo más simple de encolamiento, se basa en el siguiente concepto: el primer paquete en entrar a la interfaz, es el primero en salir. Usa la técnica de almacenamiento y reenvío; se encarga de almacenar paquetes cuando hay congestión en la red y los envía cuando tiene la posibilidad.

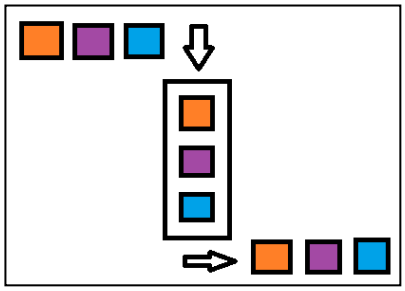


Figura 2.4: Encolamiento FIFO

El encolamiento FIFO mantiene el orden de llegada de los paquetes, es decir, no ofrece ninguna prioridad de unos paquetes sobre otros.

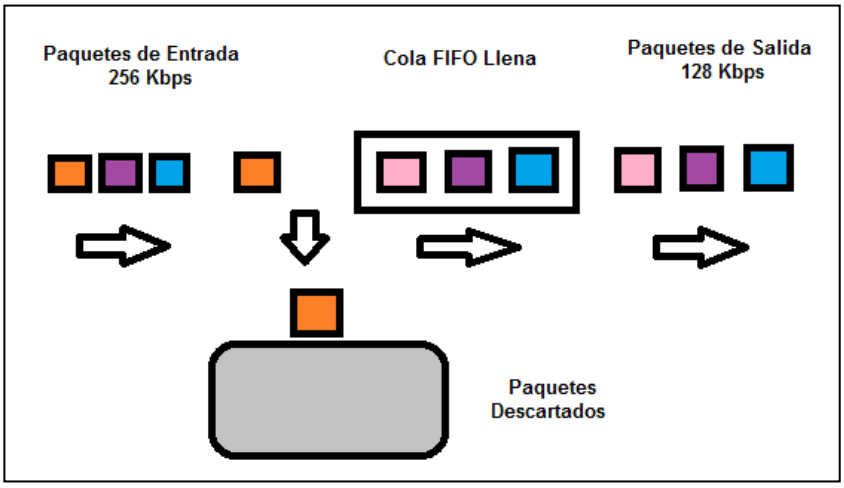


Figura 2.5: Fin de la Caída Encolamiento FIFO

Es adecuado para interfaces de alta velocidad, sin embargo, no para bajas, ya que FIFO es capaz de manejar cantidades limitadas de ráfagas de datos. Si llegan más paquetes cuando la cola está llena, éstos son descartados. No tiene mecanismos de diferenciación de paquetes.

Es el mecanismo más rápido y que se suele utilizar por defecto pero no es recomendado ya que hoy en día se necesitan de algoritmos más sofisticados que

permitan diferenciar los distintos tipos de paquetes. FIFO es soportado en todas las plataformas y en todas las rutas de conmutación [8].

- **PQ - Priority Queuing**

Asegura que el tráfico importante reciba un servicio rápido en cada punto de la red, donde este mecanismo este presente.

Consiste en un conjunto de colas, clasificadas desde alta a baja prioridad. En el mecanismo PQ, cada uno de los paquetes debe de ser colocado en una de las cuatro posibles colas (alta, media, normal, baja prioridad), servidas en riguroso orden de prioridad, lo cual puede crear inanición.

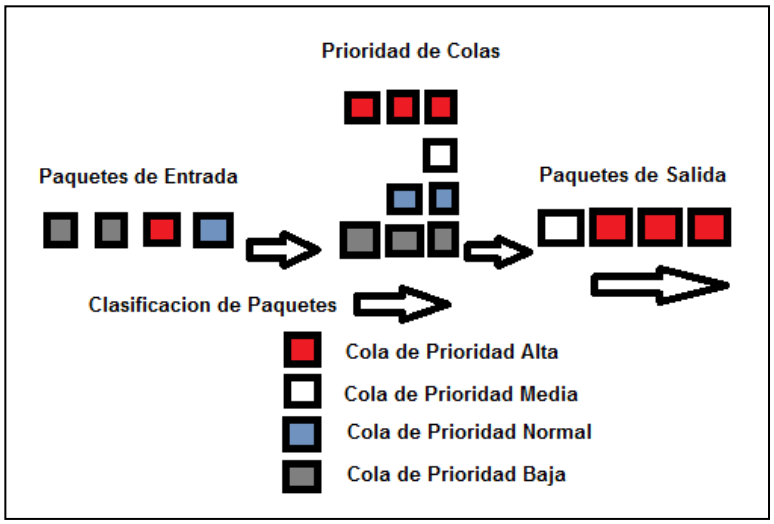


Figura 2.6: Encolamiento PQ

Las colas de mayor prioridad son siempre atendidas primero, luego la siguiente de menor prioridad y así sucesivamente. Si una cola de menor prioridad está siendo atendida, y un paquete ingresa a una cola de mayor prioridad, ésta es atendida inmediatamente. Este mecanismo se ajusta a condiciones donde existe un tráfico importante, pero puede causar la total falta de atención de colas de menor prioridad.

Las prioridades se definen por filtros en los routers. La prioridad de los paquetes puede diferenciarse por diversos medios, como: el protocolo de red, el interfaz del Router por el que llegue el paquete, el tamaño del paquete y la dirección de origen o destino.

Los paquetes que no se puedan clasificar serán asignados a la cola de prioridad normal.

El inconveniente que existe con este método es que PQ es un método estático y no se adapta a los requerimientos de la red, además puede crear inanición, es decir dejar fuera de servicio al tráfico menos prioritario [8].

- **CQ - Custom Queuing**

Para evadir la rigidez de PQ, se opta por utilizar CQ. Permite al administrador priorizar el tráfico sin los efectos laterales de inanición de las colas de baja prioridad, especificando el número de paquetes o bytes que deben ser atendidos para cada cola. CQ fue diseñado para permitir que varias aplicaciones compartieran la red, y que además tuvieran asignado un ancho de banda mínimo garantizado, y unas garantías aceptables en cuanto a los retrasos.

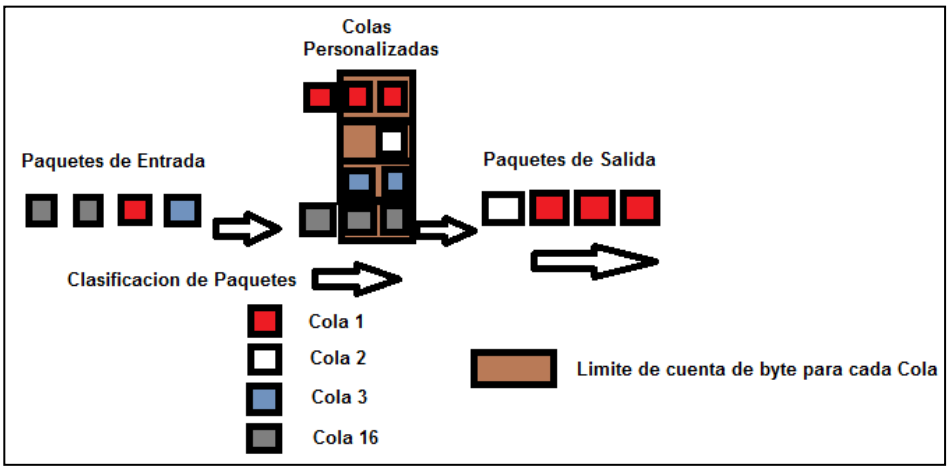


Figura 2.7: Encolamiento CQ

Se pueden crear hasta 16 colas para categorizar el tráfico, donde cada cola es atendida al estilo Round Robin (método para seleccionar todos los elementos en un grupo de manera equitativa y en un orden racional).

CQ ofrece un mecanismo más refinado de encolamiento, pero no asegura una prioridad absoluta como PQ. Se utiliza CQ para proveer a tráficos particulares de un ancho de banda garantizado en un punto de posible congestión, asegurando para este tráfico una porción fija del ancho de banda y permitiendo al resto del tráfico utilizar los recursos disponibles [8].

- **WFQ - Weighted fair queuing**

Este método de encolamiento clasifica paquetes en flujos. Un flujo es un conjunto de paquetes que tienen la misma dirección IP origen y destino y los mismos números de puerto tanto origen como destino. Dado que WFQ es basado en flujos, cada flujo utiliza diferentes colas FIFOS separadas, el número de colas alcanza las 4096 colas por interface.

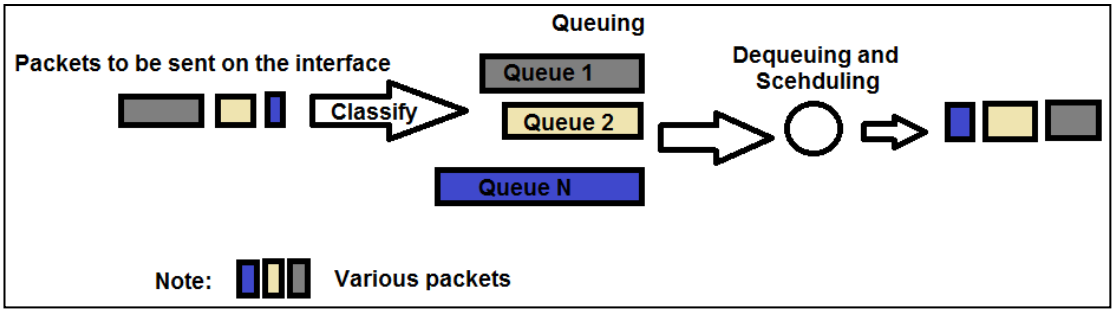


Figura 2.8: Funcionamiento del Encolamiento Equitativo Ponderado

Es un método automatizado que provee una justa asignación de ancho de banda para todo el tráfico de la red. Como se mencionó, WFQ ordena el tráfico en flujos utilizando una combinación de parámetros. Por ejemplo, para una conversación TCP/IP, se utiliza el protocolo IP (dirección origen y destino), etc. Una vez

distinguidos estos flujos el Router determina cuáles son de uso intensivo o sensible al retardo, priorizándolos y asegurando que los flujos de alto volumen sean empujados al final de la cola, y los volúmenes bajos, sensibles al retardo, sean empujados al principio de la cola.

Esta técnica es apropiada en situaciones donde se desea proveer un tiempo respuesta consistente ante usuarios que generan altas y bajas cargas en la red, ya que se adapta a las condiciones cambiantes del tráfico en ésta.

WFQ tiene algunas limitantes de escalamiento, ya que la implementación del algoritmo se ve afectada a medida que el tráfico por enlace aumenta, colapsa debido a la cantidad numerosa de flujos que analizar [8].

- **CBWFQ - Class-Based WFQ**

CBWFQ fue desarrollada para evitar limitaciones de escalamiento, tomando el algoritmo de WFQ y expandiéndolo, permitiendo la definición de clases definidas por el usuario, que permiten un mayor control sobre las colas de tráfico y asignación de ancho de banda. Algunas veces es necesario garantizar una determinada tasa de transmisión para cierto tipo de tráfico, lo cual no es posible mediante WFQ pero sí con CBWFQ.

Las clases que son posibles implementar con CBWFQ pueden ser determinadas según protocolo ACL, valor DSCP o interfaz de ingreso. Cada clase posee una cola separada y todos los paquetes que cumplen con el criterio definido para una clase en particular son asignados a dicha cola. Una vez que se establecen los criterios para las clases, es posible determinar cómo los paquetes pertenecientes a dicha clase serán manejados. Si una clase no utiliza su porción de ancho de banda, otras pueden hacerlo. Se pueden configurar específicamente el ancho de banda y el límite de paquetes máximos (o profundidad de cola) para cada clase. El peso asignado a la cola de la clase es determinado mediante el ancho de banda asignado a dicha clase [8].

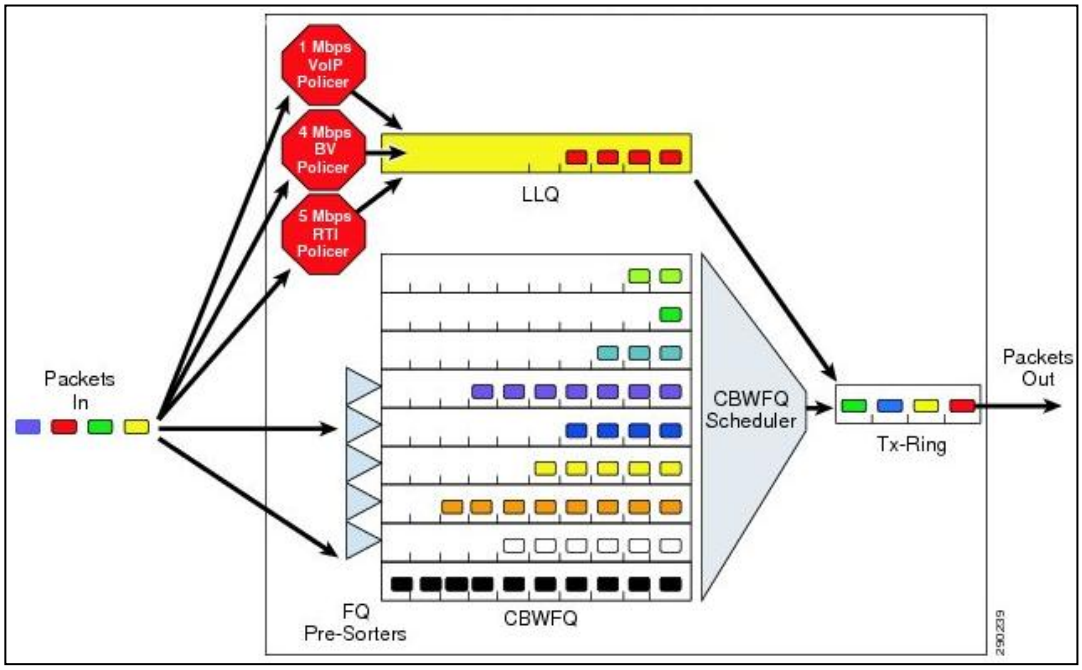


Figura 2.9: Funcionamiento de CBWFQ

Imagen tomada de: https://networkingcontrol.wordpress.com/page/6/

Este método de encolamiento por defecto clasifica paquetes en flujos. Un flujo es un conjunto de paquetes que tienen la misma dirección IP origen y destino y los mismos números de puerto tanto origen como destino.

- **LLQ - Low Latency Queue**

Es una mezcla entre Priority Queueing y Class-Based Weighted-Fair Queueing. Es actualmente el método de encolamiento recomendado para Voz sobre IP (VoIP) y Telefonía IP, que también trabajará apropiadamente con tráfico de videoconferencias.

LLQ consta de colas de prioridad personalizadas, basadas en clases de tráfico, en conjunto con una cola de prioridad, la cual tiene preferencia absoluta sobre las otras colas. Si existe tráfico en la cola de prioridad, ésta es atendida antes que las otras colas de prioridad personalizadas. Si la cola de prioridad no está encolando paquetes, se procede a atender las otras colas según su prioridad.

Debido a este comportamiento es necesario configurar un ancho de banda límite reservado para la cola de prioridad, evitando la inanición del resto de las colas. La cola de prioridad que posee LLQ provee de un máximo retardo garantizado para los paquetes entrantes en esta cola, el cual es calculado como el tamaño del MTU dividido por la velocidad de enlace [8].

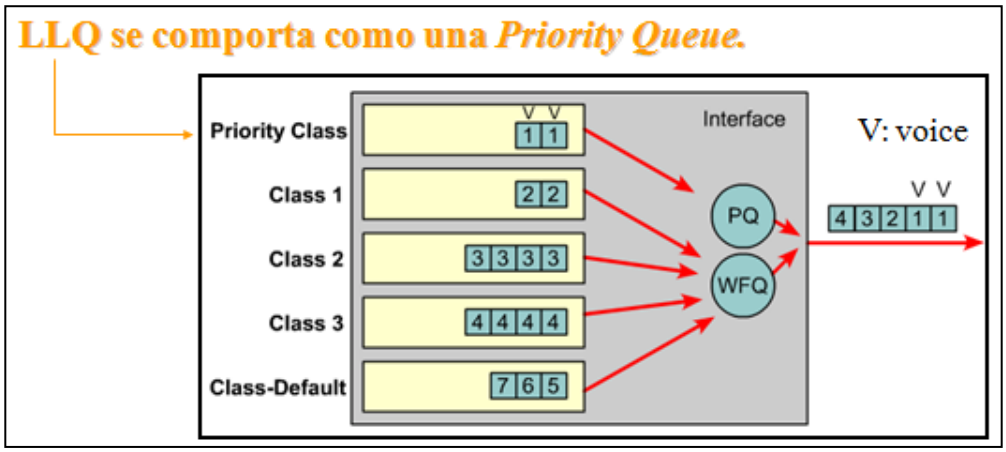


Figura 2.10: Encolamiento LLQ

Imagen tomada de: informatica.uv.es/doctorado/SST/docto-2-qos.ppt

Usado para el tráfico realtime como voz, videoconferencia muy sensibles al delay. Con LLQ, los datos sensibles al retardo, como la voz, son colocados en la cola de mayor prioridad y son los primeros en ser enviados.

CAPÍTULO 3

3. ASPECTOS DE DISEÑO PARA IMPLEMENTACIÓN DE CALIDAD DE SERVICIO

3.1. Características de los Servicios Convergentes

Hoy en día, la convergencia de las comunicaciones de una empresa; voz, datos y videos en una única red IP es una tendencia imparable. Esto es debido a que las soluciones que integran voz y datos aportan importantes beneficios para las empresas y sus usuarios:

- ➔ Ahorro en llamadas
- ➔ Simplificación de la Infraestructura de Comunicaciones
- ➔ Optimización de la Gestión
- ➔ Unificación del Sistema de Telefonía entre Sedes
- ➔ Movilidad del Usuario

Sin embargo una red convergente multiservicio debe de estar correctamente diseñada y gestionada, puesto que se convierte en un elemento mucho más crítico al soportar todas las comunicaciones de empresa.

En ese sentido se deben de tener muy en cuenta aspectos como la fiabilidad, seguridad y control de la calidad de servicio (QoS) para garantizar un funcionamiento óptimo de nuestras comunicaciones.

Mostramos algunas razones para implementar calidad de servicio sobre una topología de red de comunicación:

- ☐ Dar prioridad a aplicaciones de misión crítica dentro de la red.
- ☐ Maximizar el uso de la inversión en infraestructura de la red actual.
- ☐ Mejor rendimiento para aplicaciones sensibles al retardo como la voz y el video.

- ☐ Responder a cambios en los flujos de tráfico en la red.

A menudo, en la práctica se determina que el método más simple para lograr un mejor desempeño en una red es lanzar más ancho de banda sobre el problema. En este tiempo de redes Gigabit Ethernet y ópticas, mayores capacidades están disponibles. De todos modos, más ancho de banda no siempre garantiza un cierto nivel de rendimiento.

Es muy posible que muchos de los protocolos que producen la congestión en primer lugar, simplemente consuman el ancho de banda adicional; lo cual lleva a los mismos problemas de congestión experimentados antes de la actualización de ancho de banda.

Un enfoque más prudente es analizar el tráfico que fluye por el cuello de botella, determinando de esta manera la importancia de cada protocolo y aplicación, y determinar una estrategia para priorizar el acceso al ancho de banda.

QoS permite a los administradores de red tener el control sobre el ancho de banda, la latencia y el jitter, y así, minimizar la pérdida de paquetes dentro de la red mediante la priorización de varios protocolos. El ancho de banda es la medida de la capacidad en una red o una conexión específica, la latencia es el retardo de un paquete viajando por la red y el jitter es el cambio de latencia sobre un período de tiempo determinado. Implementar ciertos procedimientos o técnicas de calidad de servicio puede controlar estos tres parámetros críticos dentro de las aplicaciones especiales.

Debemos de considerar aspectos muy importantes dentro de cada red de comunicación, siendo el comportamiento de esta muy diferente en el sentido de negocio de cada compañía:

- ✓ Auditoría de red.- Con el propósito de identificar cada tipo de tráfico sobre la red.
- ✓ Auditoría del negocio.- Dentro de la que se tiene que determinar cómo cada tipo de tráfico es importante para el negocio de la compañía.

- ✓ Niveles de servicio requeridos.- Para determinar el tiempo de respuesta requerido dentro de cada tipo de tráfico [9].

3.2. QoS útil para Problemas en Redes Convergentes

Actualmente, las redes IP deben proporcionar servicios de transmisión de voz y video, lo que provoca la necesidad de un servicio: seguro, predecible, medible y entrega garantizada. Para obtener estas características es necesario diseñar e implementar QoS, mediante la gestión de retardo, jitter, provisión de ancho de banda y control de pérdida de paquetes.

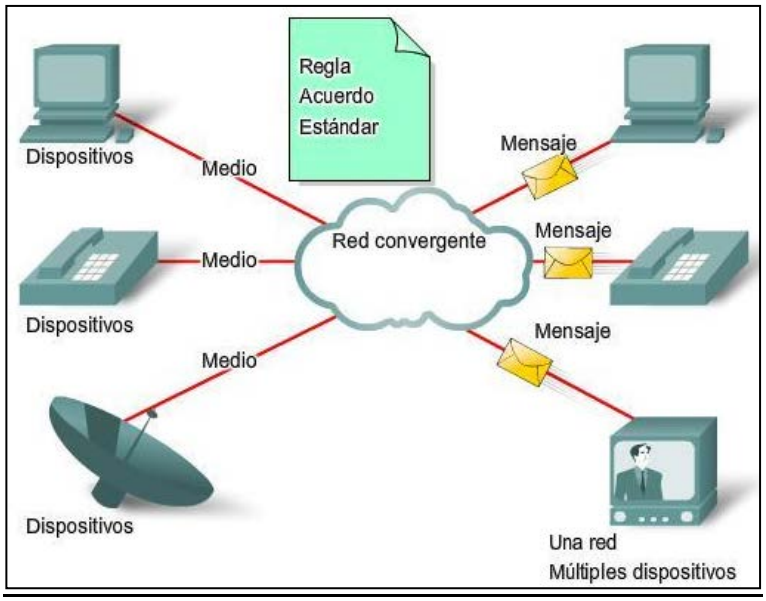


Figura 3.1: Red Convergente

Información tomada de: http://www.taringa.net/post/apuntes-y-monografias/17561913/Redes-Convergentes-y-Modelos-de-Redes.html

Podemos citar los siguientes problemas relacionados con QoS en redes convergentes:

- Telefonía: Llamadas entrecortadas.

- Videoconferencia: El video va a saltos y no esta sincronizado con la voz.
- Call Center: Falta de sincronización entre aplicaciones y las soluciones de voz.

Como conclusión, en una red convergente el tráfico de voz compite con el tráfico de aplicaciones que mueven paquetes pesados:

➔ Tráfico de voz:
Paquetes pequeños
Flujo Constante
Consumo de ancho de banda limitado
No soporta retardo, jitter y pérdida de paquetes

➔ Tráfico de aplicaciones:
Paquetes de tamaño variable pero generalmente grandes
Transmisión a ráfagas
Consumo de ancho de banda no fácilmente limitable
Soporta bien los problemas de retardo, jitter y pérdida de paquetes

El tráfico de voz se ve comprometido por el tráfico de datos en caso de existir congestión [9].

Factores de QoS en Redes Convergentes

- Capacidad de ancho de banda.
- Retardo “Extremo a Extremo”: Es el tiempo que tarda un paquete en ir desde el origen al destino.
- Variabilidad del Retardo o Jitter: Diferencia de retardos extremo a extremo de dos paquetes.
- Perdida de paquetes.

3.2.1. Ancho de Banda

Este problema corresponde a que varios flujos entran en competencia por una cantidad limitada de ancho de banda. Archivos grandes de tráficos, usos multimedia e incremento del uso de voz y video causan problemas de capacidad de ancho de banda sobre las redes de datos.

La determinación del ancho de banda disponible en entornos corporativos es complejo en la mayor parte de los casos.

En el ámbito LAN este factor no es tan determinante:

- ✓ Magnitudes de ancho de banda.
- ✓ Coste del cambio de ancho de banda.

Sin embargo en los enlaces WAN es un factor crítico:

- ✓ Es un elemento mucho más limitante dada su escasez.
- ✓ Su incremento tiene un mayor coste directo.

La mejor manera para aumentar el ancho de banda es incrementar la capacidad del enlace con el fin de adaptar todas las aplicaciones y usuarios, con algún ancho de banda extra libre. Aunque esta solución parece simple, incrementar el ancho de banda es costoso y toma tiempo su implementación. Por lo general, existen limitaciones tecnológicas en las actualizaciones de un muy alto ancho de banda, como por ejemplo la capacidad de los equipos terminales, las tecnologías de acceso, entre otros.

Otra opción para contrarrestar este problema es clasificar el tráfico dentro de clases de QoS y priorizar tráfico de acuerdo a la importancia del mismo. El tráfico de voz y el crítico para el negocio deberían tener suficiente ancho de banda para soportar sus requerimientos dentro de la aplicación, la voz debería tener priorizada su transmisión y el tráfico menos importante debería obtener cualquier cantidad de ancho de banda del sobrante [9].

3.2.2. Retardo Extremo a Extremo

Los paquetes de datos tienen que atravesar algunos dispositivos de red y enlaces de diferentes características, entre su origen y destino, lo que provoca un incremento de la totalidad del retardo del paquete. El retardo es el tiempo tomado por un paquete en alcanzar el punto final de recepción después de ser transmitido desde un punto de envío.

- Retardo de Red Fijo: Es un valor constante para todo el tráfico de la red.
    - Tiempo de Serialización: Es el proceso de Transmisión depende de la velocidad de la interfaz y del tamaño de la trama.
    - Tiempo de Propagación: Es el tiempo de desplazamiento a través del medio de transmisión; habitualmente es despreciable, pero en algunos casos es muy relevante, por ejemplo en las transmisiones vía satélite.
- Retardo de Red Variable: El retardo de cola es la cantidad de tiempo que esta un paquete en un buffer de salida (o cola de salida). Es variable en función del tráfico o nivel de congestión.

Los factores que se pueden controlar para reducir el retardo: longitud media de las colas, longitud media de los paquetes en la cola, ancho de banda del enlace.

Aproximaciones para reducir el retardo variable:

- Incrementar la capacidad del enlace.
- Priorizar los paquetes sensibles al retardo:
    - Es el enfoque con mejor relación coste/efectividad.
    - Tipos de priorización: PQ, CQ, prioridades estrictas, CBWFQ, LLQ.
- Compresión de la carga útil:
    - Reducir el tamaño del paquete, aumenta “virtualmente” el ancho de banda.
    - Es un proceso que consume muchos recursos de hardware. En la mayor parte de los casos, no compensa.

- Compresión de la cabecera:
  - Es un proceso más sencillo que la compresión de la carga útil.
  - Se utiliza como complemento de otros mecanismos en la transmisión de paquetes de voz (RTP) en enlaces punto a punto [9].

3.2.3. Algoritmos de Perdidas de Paquetes

La perdida de paquetes se produce habitualmente en los routers cuando se acaba el espacio en el buffer de la interfaz de salida, cuando llegan paquetes con el buffer lleno, estos se descartan (tail drop).

Los routers también pueden descartar:

- Descarte en la cola de entrada; esta situación se produce cuando la CPU está saturada y no puede procesar los paquetes de entrada
- Errores de transmisión en la trama, detectados en el CRC.

Se pueden utilizar los siguientes procedimientos para prevenir el descarte de paquetes:

- Incrementar la capacidad del enlace.
- Garantizar el ancho de banda suficiente e incrementar el espacio de los buffers para colocar en ellos el tráfico en exceso.
- Descartar los paquetes de baja prioridad antes de que se llene el buffer completamente (WRED) [9].

TAIL DROP

Cuando se produce la congestión de la red debido a que el tamaño de las colas no soporta el número de paquetes, hay que eliminar cierto número de paquetes. Este método elige como paquetes para eliminar a aquellos que se encuentran al final de la cola, es decir, los últimos en llegar.

Las ventajas de este mecanismo de gestión son las siguientes:

- ❖ Tiene una implementación muy fácil de realizar y de entender.
- ❖ Puede reducirse el número de paquetes elegidos para su eliminación.

En cambio, presenta una serie de limitaciones que hacen que no sea el más recomendable:

- ❖ Posee un comportamiento de puerta cerrada, es decir, si llega un paquete nuevo y la cola está saturada, este paquete no tiene oportunidad a ser transmitido.
- ❖ Es problemático para el tráfico basado en TCP.
- ❖ Incrementa el retraso extremo a extremo.

RED (Random Early Detection)

Provee a los operadores de la red, la posibilidad de aplicar normas para el manejo del tráfico y maximizar el throughput bajo condiciones de congestión.

Trabaja junto a protocolos a nivel de transporte como TCP, evitando la congestión aplicando una serie de algoritmos:

- o Distingue entre ráfagas de tráfico temporal que pueden ser absorbidas por la red, y cargas excesivas de tráfico que pueden saturar la red.
- o Trabaja en cooperación con el extremo generador de tráfico, para evitar la oscilación producida por el protocolo TCP, que puede causar ondas de congestión en la red.
- o RED trabaja con TCP, para anticiparse y manejar la congestión en momentos de tráfico excesivo, para maximizar el througput mediante el descarte de paquetes [4].

WRED (Weigted Random Early Detection)

Combina las capacidades de RED y de IP Precedence, para proveer diferentes clases de servicio en función de las características de la información.

WRED también proporciona manejadores para tráfico prioritario en momentos de congestión, además posee todas las capacidades anteriormente citadas para RED.

WRED puede colaborar con RSVP, proporcionando un controlador de carga, o indicando si es factible una reserva de espacio en alguna cola [4].

3.3. QoS en la Infraestructura de Telecomunicaciones

Actualmente se ha visto que las redes de datos tienen una importante influencia sobre la vida diaria de las personas, ya que han llegado a permitir interactuar de una manera novedosa en las comunicaciones del entorno. Se utilizan estas redes de diferentes formas, entre ellas las aplicaciones Web, la telefonía IP, la videoconferencia, los juegos interactivos, el comercio electrónico, la educación, entre otros.

Para que tenga efecto esta interacción entre personas y la utilización de diferentes aplicaciones para su comunicación, la red de datos se encuentra dotada de toda una infraestructura de telecomunicaciones, y en función al modelo TCP/IP utiliza el equipamiento que permiten una adecuada transmisión de la información. Los principales dispositivos a considerarse dentro de la red de datos son los enrutadores y los conmutadores.

Enrutadores.- (Ingles Router) es un dispositivo de hardware para interconexión de red de ordenadores que opera en la capa tres (nivel de red). Un Router es un dispositivo para la interconexión de redes informáticas que permite asegurar el enrutamiento de paquetes entre redes o determinar la ruta que debe tomar el paquete de datos.

Los enrutadores pueden proporcionar conectividad dentro de las empresas, entre las empresas e Internet, y en el interior de proveedores de servicios de Internet (ISP).

Figura 3.2: Router Inalámbrico CISCO

Imagen tomada de:
http://www.pcactual.com/articulo/laboratorio/analisis/comunicaciones/routers/inalambricos/10581/router_inalambrico_cisco_linksys_e4200.html

Un enrutador inalámbrico comparte el mismo principio que un enrutador tradicional. La diferencia es que éste permite la conexión de dispositivos inalámbricos a las redes a las que el enrutador está conectado mediante conexiones por cable. La diferencia existente entre este tipo de enrutadores viene dada por la potencia que alcanzan, las frecuencias y los protocolos en los que trabajan.

Conmutadores.- O switch es un dispositivo digital de lógica de interconexión de redes de computadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Su función es interconectar dos o más segmentos de red, de manera similar a los puentes (bridges), pasando datos de un segmento a otro de acuerdo con la dirección MAC de destino de las tramas en la red.

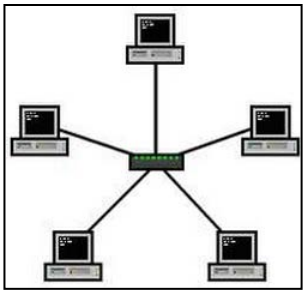


Figura 3.3: Conmutador en el centro de una red estrella

Imagen tomada de: https://es.wikipedia.org/wiki/Conmutador_(dispositivo_de_red)

Los conmutadores se utilizan cuando se desea conectar múltiples redes, fusionándolas en una sola. Al igual que los puentes, dado que funcionan como un filtro en la red, mejoran el rendimiento y la seguridad de las LANs.

CAPÍTULO 4

4. ANÁLISIS E IMPLEMENTACIÓN DE UNA RED DE PRUEBA – DISTRITO HOTELERO

4.1. Antecedentes

Nuestra red de prueba corresponde a un Distrito Hotelero, estructurado físicamente por cuatro hoteles:

- HPSM
- HPDL
- HPDG
- HPJC

Tienen disponibilidad de 81 Mbps entre ellos, contando con 3 proveedores: el primero con 30 Mbps, el segundo con 35 Mbps y el tercero con 16 Mbps, teniendo salida al internet solo por un proveedor.

Los hoteles cuentan con alrededor de 600 huéspedes donde a cada uno al momento de su registro se le asignaba 4Mbps por dispositivo, el problema radica en que el cliente da mal uso del ancho de banda conectando múltiples dispositivos, debido a la mala configuración la tabla de registros se saturaba impidiendo la eliminación de los registros de clientes teniendo alrededor de 4000 registros de dispositivos. Afectando la parte administrativa de los hoteles.

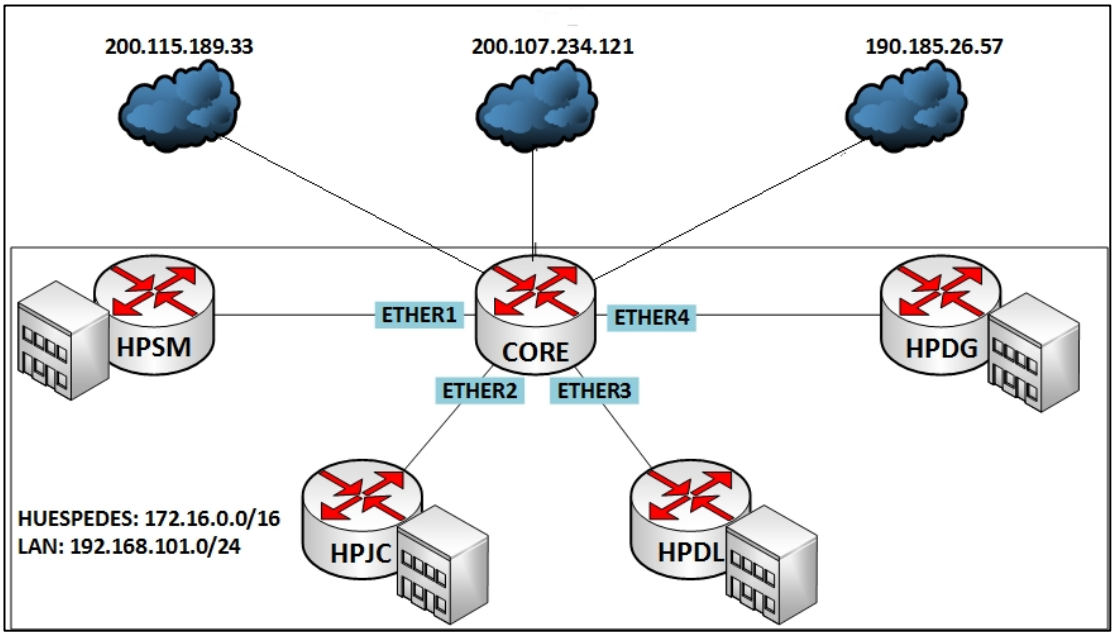


Figura 4.1: Red Actual – Distrito Hotelero

Además existía una mala configuración del CORE (equipo CCR1009-8G-1S+) ubicado en el Hotel HPSM el cual funcionaba como centro de mando dando como resultado una mala administración del ancho de banda limitando el balanceo de carga.

Área Administrativa

Cada hotel contaba con un área administrativa estructurada por 200 máquinas en total de las cuales solo 40 tenían salida al internet y las 160 restantes eran utilizadas para registros internos.

El problema se basa en que los empleados abusan del entorno de trabajo, conectando dispositivos adicionales para el acceso a internet con fines innecesarios provocando desgaste del ancho de banda.

4.2. Planteamiento de la Solución

Se realizó un arduo análisis para conocer cuántos megas se asignaran a cada red, proporcionando 61 Mbps a los huéspedes y 20 Mbps a la área administrativa.

Centrándonos en el área de los huéspedes, dispondremos de un servidor RADIUS para la autenticación, asignándole un único usuario y contraseña a cada huésped. Validaremos su registro por tres días, finalizando su límite de tiempo se eliminara de manera automática el registro de la tabla de direccionamiento por lo que evitaremos saturación en la red.

A cada huésped se le asignara 2Mbps de navegación para todos sus dispositivos.

Por el lado del área administrativa, aplicaremos QoS y CoS para clasificar cada tráfico utilizado en la red (correo, DNS, Http, icmp, p2p, conexiones desconocidas y telefonía) de esta manera daremos prioridad al tráfico más importante, tomando como resultado un análisis realizado por el área de Sistemas del Distrito Hotelero.

Durante el estudio realizado solo vamos a implementar un Router serie RB2011, seleccionamos este equipo ya que mediante un sondeo nos percatamos que son de bajo costo pero tiene muchas características y además el Departamento de Sistemas del Distrito Hotelero contaba con las facilidades para adquirir este equipo Mikrotik.

Toda la parte de implementación de esta solución se encuentra en la parte de Anexo A.

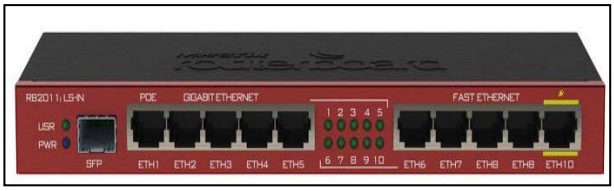


Figura 4.2. Router RB2011

El Mikrotik RB2011 es una serie de productos multi-puerto de precio costeable. Diseñada para uso en interiores, disponible con diferentes gabinetes metálicos y una multitud de opciones.

El RB2011-IN es el modelo básico, con cinco puertos Gigabit Ethernet y cinco puertos Fast Ethernet, puerto de alimentación y soporte PoE. Internamente es impulsado por el nuevo procesador de red Atheros de próxima generación a 600MHz 74K MIPS con 64MB de RAM y licencia RouterOS nivel 4.

Características

- ✓ CPU Atheros AR9344 600MHz
- ✓ Memoria interna 64MB DDR SDRAM
- ✓ Data storage NAND memory chip
- ✓ Cinco puertos Fast Ethernet 10/100 Mbitcon Auto-MDI/X
- ✓ Cinco puertos Gigabit Ethernet 10/100/1000 Mbit con Auto-MDI/X
- ✓ Extras botón de Reset, jumper de Reset
- ✓ LEDs Alimentación, Utilización, actividad Ethernet
- ✓ Opciones de Alimentación Jack 8-28V DC; PoE: 8-28V DC en Ether1 (No 802.3af).
- ✓ Dimensiones 214 mm x 86 mm, Peso: 146g
- ✓ Consumo de Potencia 6W max
- ✓ Sistema Operativo MikroTik RouterOS, licencia L4
- ✓ Paquete incluye RB2011L, gabinete para interiores y fuente de alimentación

Las diferentes cotizaciones realizadas del nuevo equipo se encuentran en Anexo B.

4.2.1. Servidor Radius

La comunicación entre un servidor de acceso de red (NAS) y el servidor RADIUS se basa en el protocolo de datagrama de usuario (UPD). Generalmente, el protocolo RADIUS se considera un Servicio sin conexión. Los problemas relacionados con la disponibilidad de los servidores, la retransmisión y los tiempos de espera son tratados por los dispositivos activados por RADIUS en lugar del protocolo de transmisión.

El RADIUS es un protocolo cliente/servidor. El cliente RADIUS es típicamente un NAS y el servidor de RADIUS es generalmente un proceso de daemon que se ejecuta en UNIX o una máquina del Windows NT. El cliente pasa la información del usuario a los servidores RADIUS designados; los servidores de RADIUS reciben las peticiones de conexión del usuario, autentican al usuario, y después devuelven la información de la configuración necesaria para que el cliente entregue el servicio al usuario. Un servidor RADIUS puede funcionar como cliente proxy para otros servidores RADIUS u otro tipo de servidores de autenticación.

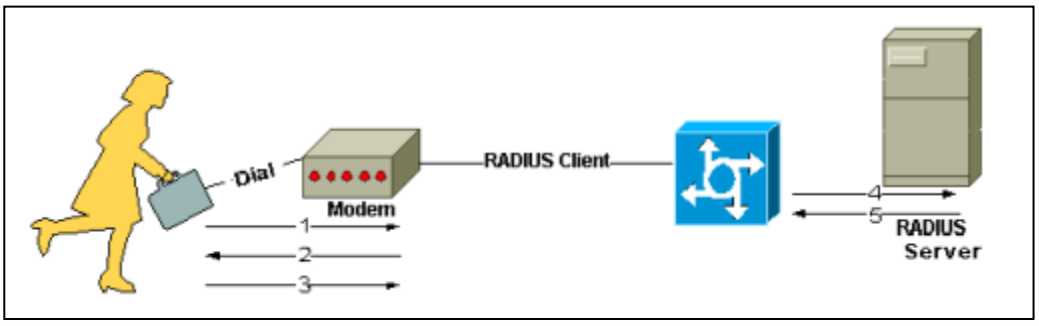


Figura 4.3. Interacción entre un Usuario de Marcación de Entrada y el Servidor y Cliente RADIUS

Imagen tomada de:
http://www.cisco.com/cisco/web/support/LA/102/1024/1024966_32.pdf

1. El usuario inicia la autenticación PPP al NAS.

2. NAS le pedirá que ingrese el nombre de usuario y la contraseña (en caso de Protocolo de autenticación de contraseña [PAP]) o la integración (en caso de Protocolo de confirmación de aceptación de la contraseña [CHAP]).
3. Contestaciones del Usuario.
4. El cliente RADIUS envía el nombre de usuario y la contraseña encriptada al servidor de RADIUS.
5. El servidor RADIUS responde con Aceptar, Rechazar o Impugnar.
6. El cliente RADIUS actúa dependiendo de los servicios y de los parámetros de servicios agrupados con Aceptar o Rechazar.

Autenticación y Autorización

El servidor RADIUS puede soportar varios métodos para autenticar un usuario. Cuando se proporciona el nombre de usuario y la contraseña original dados por el usuario, puede soportar el login PPP, PAP o de la GRIETA, de UNIX, y otros mecanismos de autenticación.

Comúnmente, el ingreso de un usuario al sistema consiste en un pedido (Solicitud de acceso) desde el NAS hacia el servidor RADIUS y de una correspondiente respuesta (Aceptación de acceso o Rechazo de acceso) desde el servidor. El paquete access-request contiene el nombre de usuario, la contraseña encriptada, la dirección IP NAS, y el puerto.

Cuando el servidor de RADIUS recibe el pedido de acceso del NAS, busca una base de datos para el nombre de usuario enumerado. Si el nombre de usuario no existe en la base de datos, se carga un perfil predeterminado o el servidor RADIUS inmediatamente envía un mensaje AccessReject (acceso denegado). Este mensaje de acceso rechazado puede estar acompañado de un mensaje de texto que indique el motivo del rechazo.

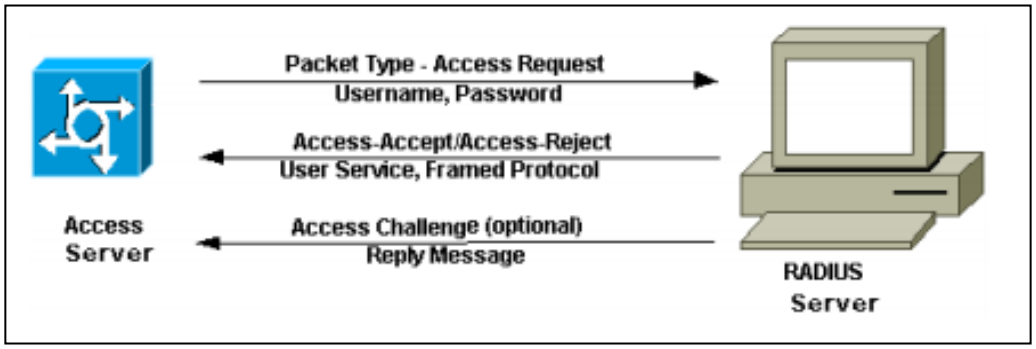


Figura 4.4. Autenticación y Autorización Servidor RADIUS

Información tomada de:
http://www.cisco.com/cisco/web/support/LA/102/1024/1024966_32.pdf

En RADIUS, la autenticación y la autorización están unidas. Si se encuentra el nombre de usuario y la contraseña es correcta, el servidor RADIUS devuelve una respuesta de Acceso-Aceptar e incluye una lista de pares de atributo-valor que describe los parámetros que deben usarse en esta sesión [10].

4.2.2. Mikrotik

Es una compañía fundada en Latvia en 1995 desarrollan Routers y sistemas inalámbricos para ISP (Proveedor de Servicios de Internet) además son proveedores de Hardware y Software. En 1997 crean RouterOS, un software o sistema operativo para routers basado en el Kernel de Linux al cual se puede acceder de varias maneras:

- ✓ Vía Web (WebFIG)
- ✓ Vía Winbox
- ✓ Vía Línea de Comandos (CLI) a través de Telnet y SSH [11].

Winbox

Es un programa ejecutable para Windows y Linux que permite conectarte con el servidor de una manera sencilla accediendo a las configuraciones del mismo mediante una interfaz amigable y administrar tu conexión con equipos Mikrotik. Incluye una sofisticada tecnología para realizar estas conexiones basadas en el sistema operativo RouterOS. Este software permite a sus usuarios realizar conexiones vía FTP, telnet y SSH [12].

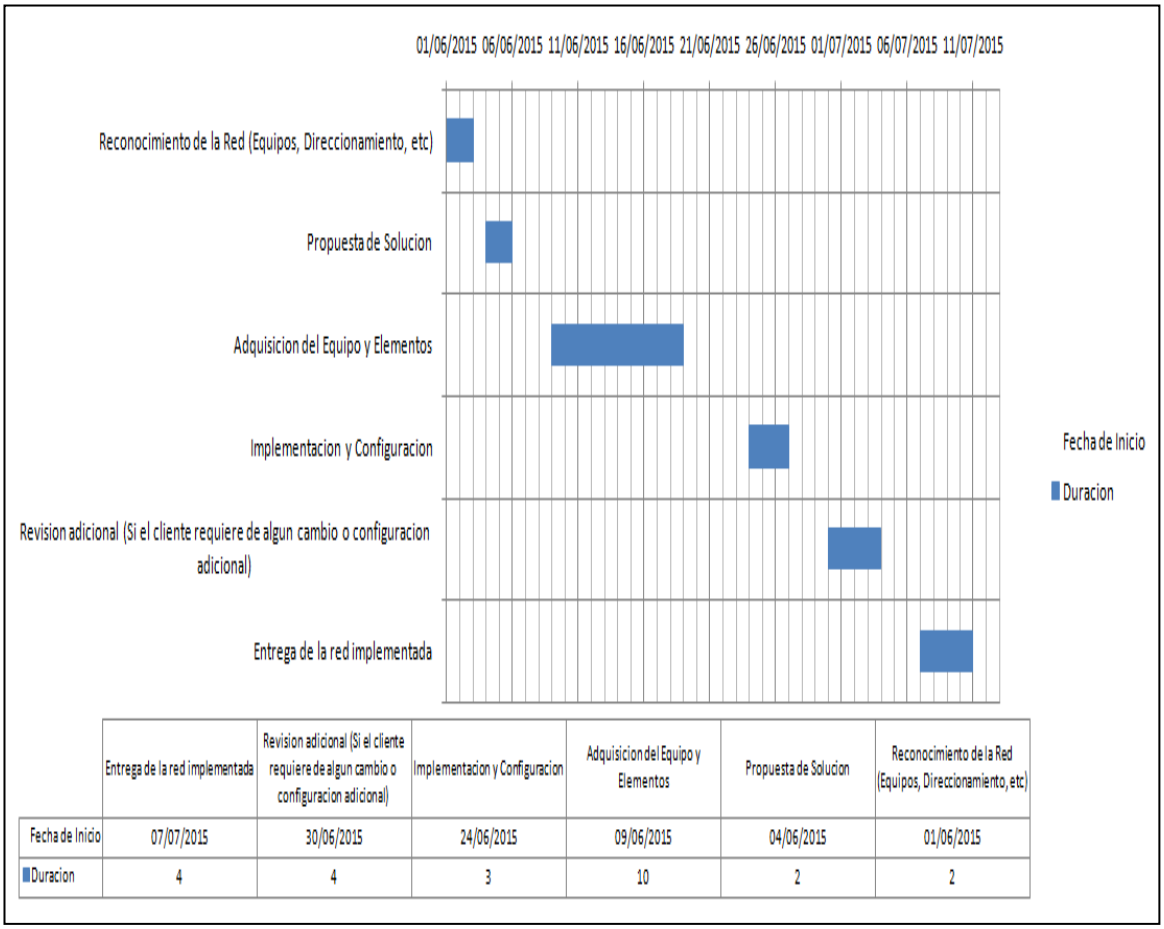
Podemos descargar WinBox desde la página de Mikrotik http://www.mikrotik.com/.

4.3. Planificación

Actividad	Fecha de Inicio	Duracion	Fecha de Terminacion
Reconocimiento de la Red (Equipos, Direccionamiento, etc)	01/06/2015	2	03/06/2015
Propuesta de Solucion	04/06/2015	2	08/06/2015
Adquisicion del Equipo y Elementos	09/06/2015	10	23/06/2105
Implementacion y Configuracion	24/06/2015	3	29/06/2015
Revision adicional (Si el cliente requiere de algun cambio o configuracion adicional)	30/06/2015	4	06/07/2015
Entrega de la red implementada	07/07/2015	4	13/07/2015

Tabla 4: Planificación

La planificación se realizo teniendo en cuenta que los fines de semana no son laborables.



	Entrega de la red implementada	Revision adicional (Si el cliente requiere de algun cambio o configuracion adicional)	Implementacion y Configuracion	Adquisicion del Equipo y Elementos	Propuesta de Solucion	Reconocimiento de la Red (Equipos, Direccionamiento, etc)
Fecha de Inicio	07/07/2015	30/06/2015	24/06/2015	09/06/2015	04/06/2015	01/06/2015
Duracion	4	4	3	10	2	2

Figura 4.5. Planificación

El desarrollo del proyecto con la respectiva implementación se realizo en 25 días laborables.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. Con la implementación realizada que lleva aproximadamente 2 meses se han obtenido los resultados esperados ya que solventamos algunos parámetros críticos con respecto al ancho de banda superando la mala configuración del equipo que realizaba el balanceo de carga.

2. El nuevo equipo adquirido RB2011 hasta el momento ha venido superando las pruebas de rigor ya que no ha presentado inconveniente alguno.

3. Existe conformidad por parte de los huéspedes ya que tenemos ahora una red estable, sin caídas de internet y disponibilidad de direcciones para el registro de un nuevo dispositivo.

4. Por parte del área administrativa se tuvo un mejor uso de los recursos de la red ya que disponen de internet solo las 40 maquinas netamente necesarias evitando uso innecesario del ancho de banda.

5. Con la implementación de la Calidad de Servicio mejoramos notablemente la distribución del tráfico de la red dando prioridad a los servicios necesarios.

Recomendaciones

1. Cuando tenemos algún problema en la red que requiera de la implementación de alguno de los mecanismos de QoS debemos de hacer un

estudio exhaustivo para conocer cuál es el que se ajusta mejor a las necesidades del problema.

2. Se recomienda si trabajamos en la red con los servicios de voz IP y video, que son el tipo de transmisión que tiene que mantenerse constante y en orden, segmentemos nuestra red para que tengan un canal libre por el cual transmitirse. De esta manera evitamos que nuestro video se vea pixelado o nuestra voz IP se escuche entrecortada.

3. Si en nuestra red tenemos envío y recepción de tráfico importante trabajemos directamente con la calidad de servicio para priorizar el tráfico, de tal manera que nuestro canal siempre esté disponible para el tráfico más importante.

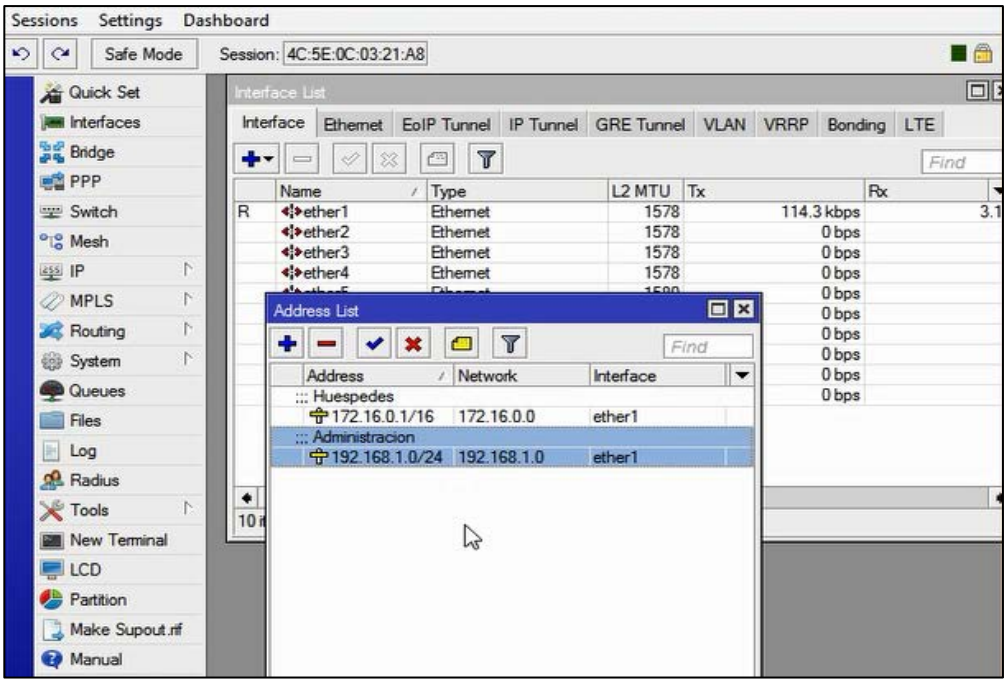
ANEXOS

Anexo A - Implementación

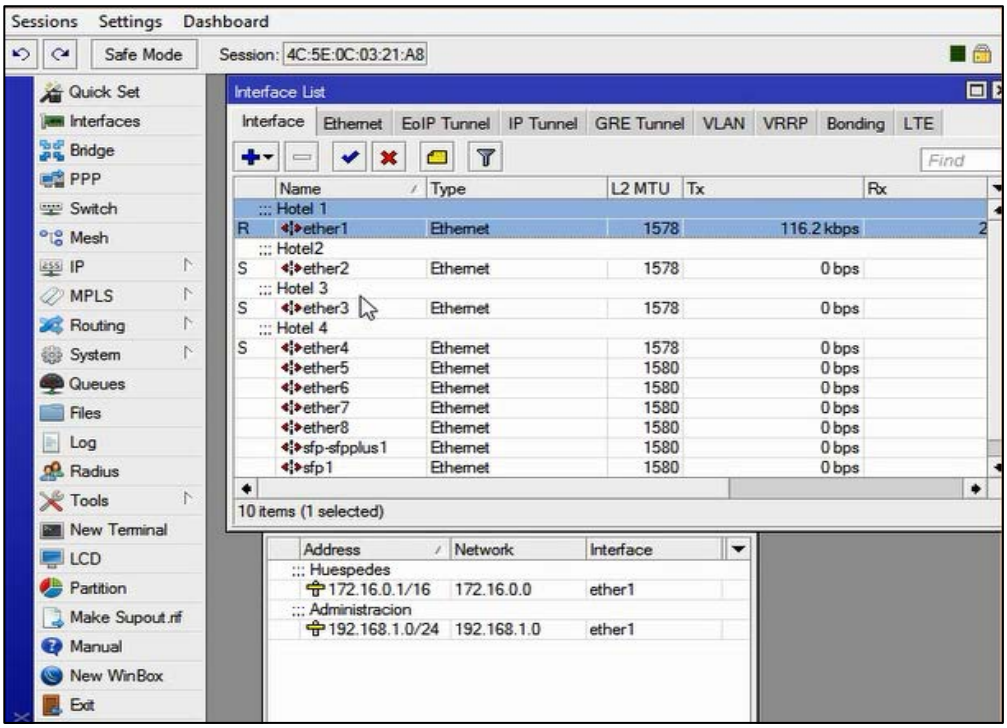
Como ya lo mencionamos anteriormente empezaremos por la configuración del equipo “CORE CCR1009-8G-1S+”, por defecto los equipos Mikrotik son administrados por WinBox.

Pasos a Seguir

1. Asignamos a una misma interfaz las direcciones de red tanto para Huéspedes 172.16.0.1/16 como para Administración 192.168.1.0/24 en la Ethernet1. Para esto nos dirigimos a IP y seleccionamos la opción “Addresses”.



La interfaz Ethernet1 está conectada directamente al Hotel HPSM que es quien manda las direcciones a todos los AP de los demás hoteles. Cabe recalcar que el equipo Core con que estamos trabajando puede funcionar como Router y Switch, en este caso la interfaz Ethernet1 está funcionando como Router y el resto de las interfaces como Switch.

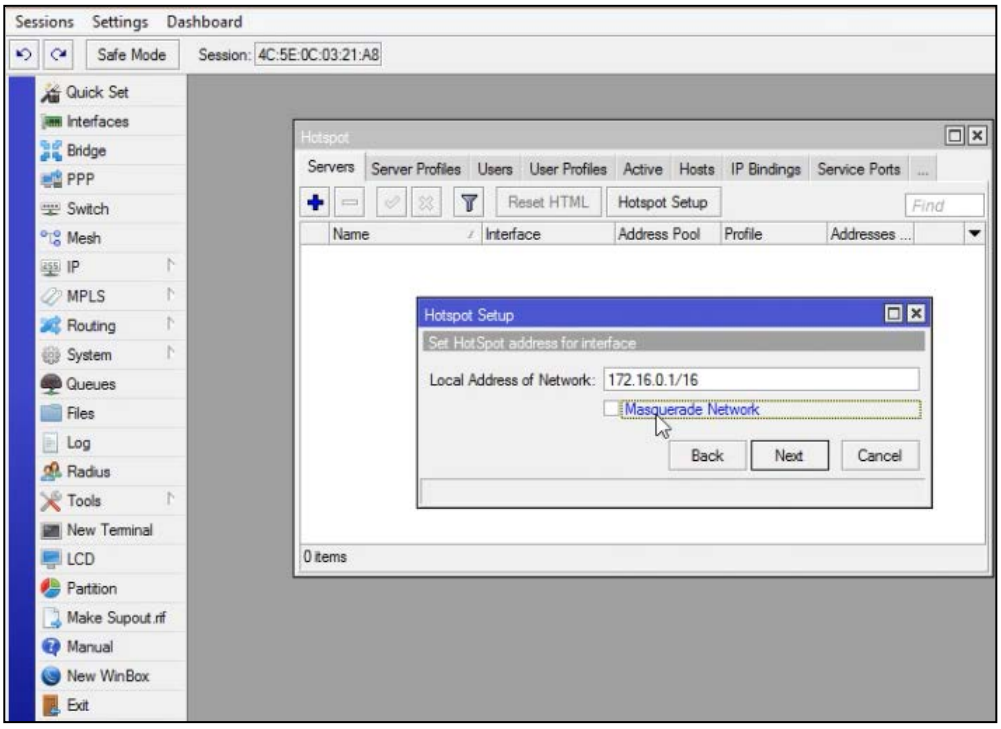


2. Para la asignación de direcciones en la red “Huéspedes” utilizamos el servicio de DHCP para asignarlas automáticamente mientras que en la red “Administración” hicimos un amarre de IP/MAC por ARP debido a que solo cuentan con 200 máquinas.

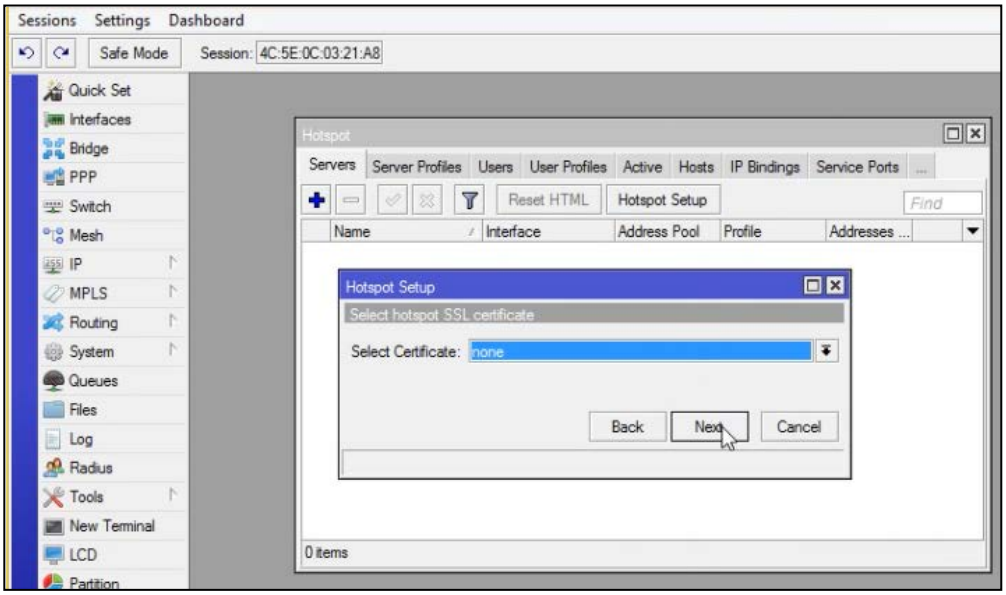
   Para realizar la configuración DHCP primero creamos un Hotspot, este sistema funciona con interfaces en modo Router; es decir la Ethernet1. Nos dirigimos a IP y seleccionamos “Hotspot”, de aquí escogemos la opción “Hotspot Setup” en donde se abre un wizard que nos permite crearlo.

Elegimos la interfaz, en este caso es la Ethernet1 de los Huéspedes, luego ingresamos la Ip asignada.

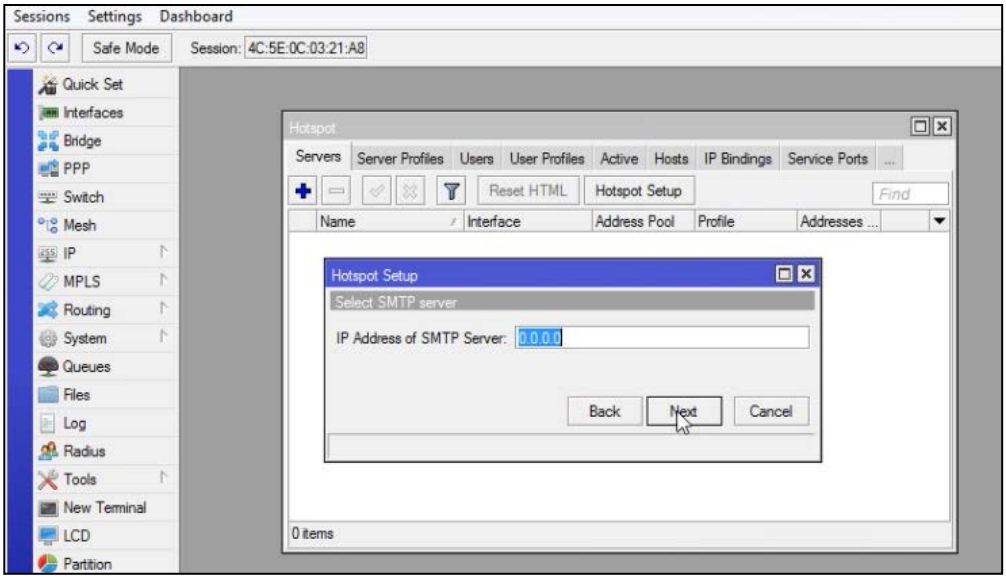
La opción “Masquerade Network” se refiere a NAT, quien transforma las redes privadas a públicas; en nuestra implementación no seleccionaremos esa opción ya que quien realizara el nateo será nuestro nuevo equipo Router RB2011.



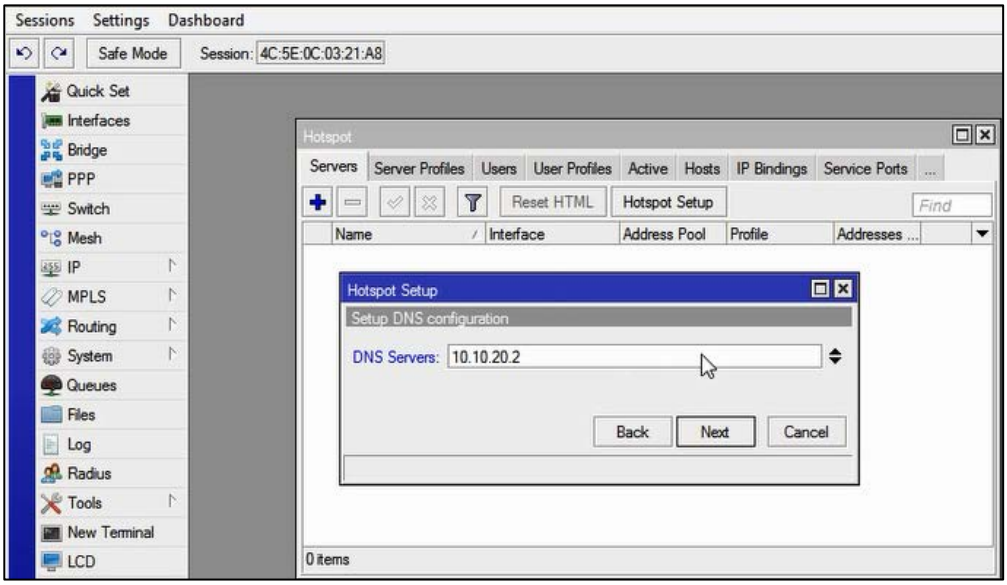
Automáticamente el wizard me reconoce el rango de direcciones que van a ser entregadas para los huéspedes, la siguiente opción que aparece en nuestra implementación no será necesaria ya que eso solo se da en el caso de que queramos usar certificados digitales al momento de que nuestros usuarios se conecten.



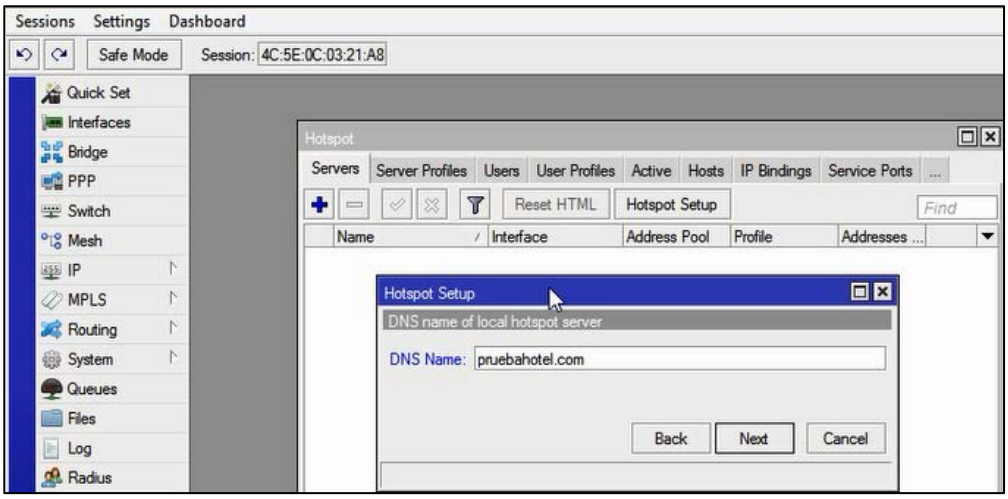
De igual manera lo siguiente se configura si es que se desea entregar alguna Ip de un servidor de correo, en nuestro caso lo dejamos por defecto.



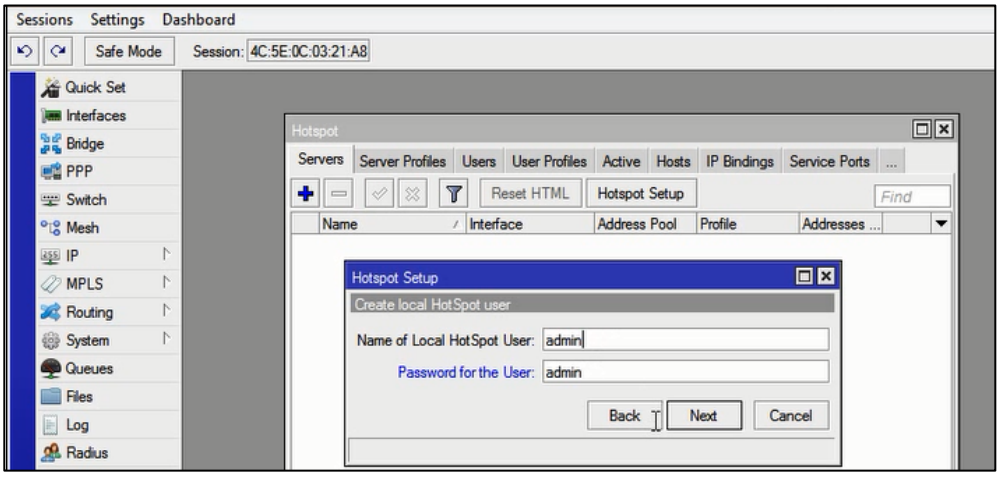
Siguiendo con el wizard configuramos el DNS con su respectiva dirección 10.10.20.2/30.



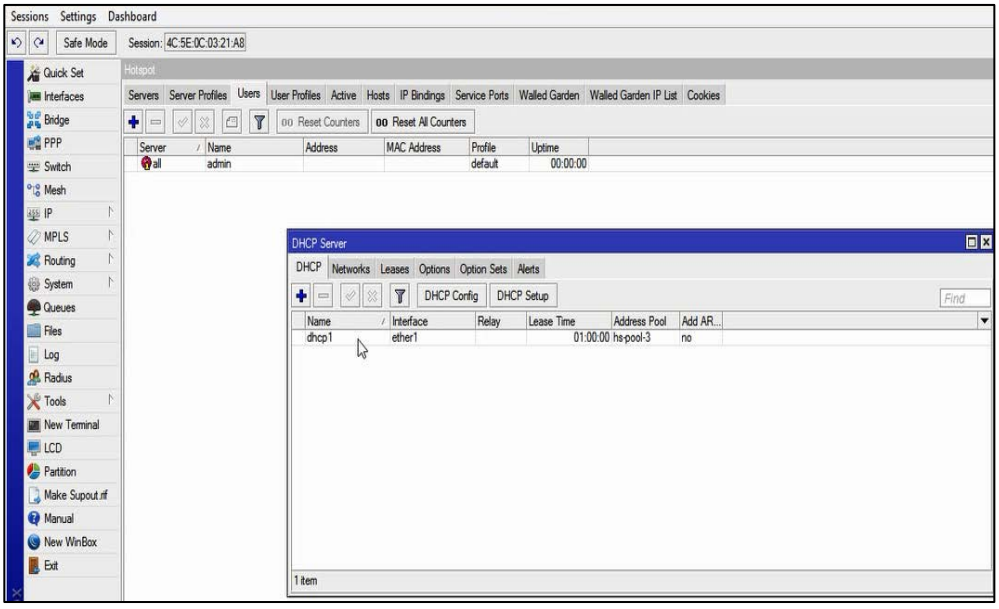
Configuración del DNS Name “pruebahotel.com”.



Creamos el primer usuario por defecto que se va a conectar.



Una vez creado el Hotspot automáticamente se creó el servidor DHCP. Se lo puede visualizar seleccionando IP -> DHCP Server.

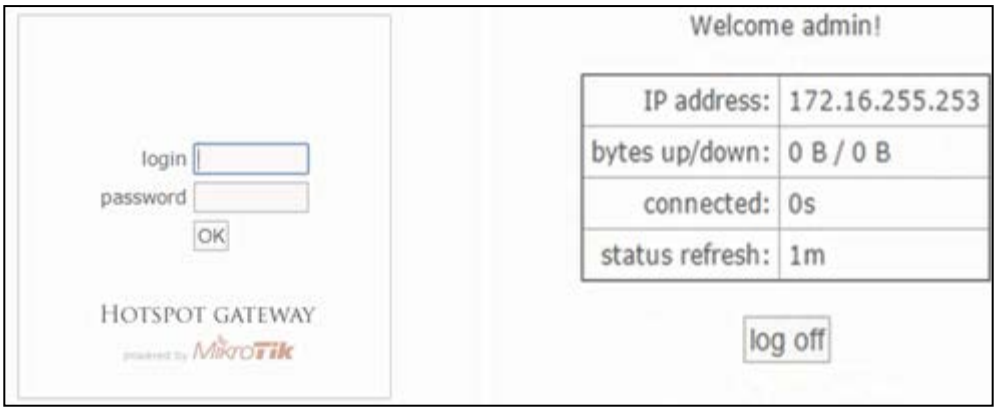


También se creó el primer usuario y contraseña que se deberá ingresar pero la idea de nuestro proyecto es que a cada usuario se le asigne un usuario y contraseña diferente; Hotspot si nos da esta opción pero de manera manual

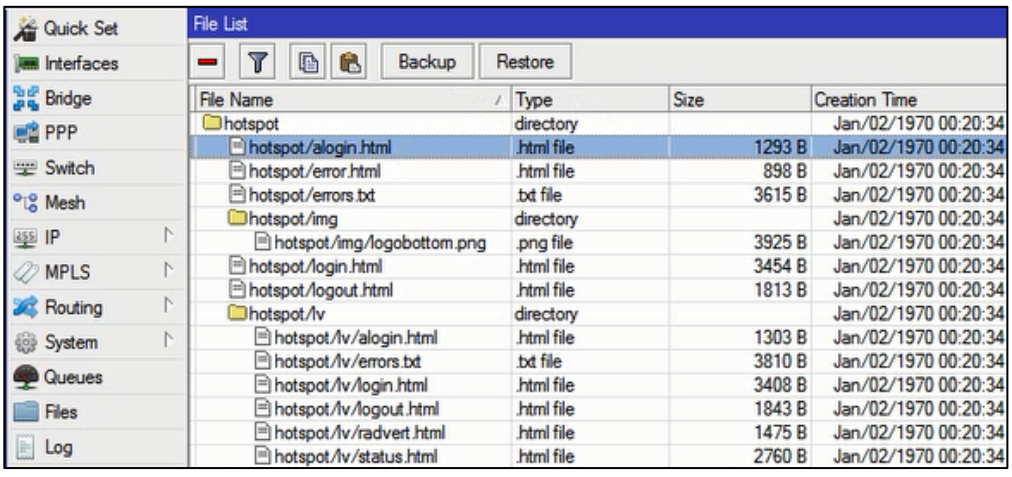
es decir que tenemos que estar ingresando usuario por usuario lo cual resulta un poco tedioso.

Por lo tanto nosotros utilizaremos de manera adicional un Servidor Radius, el cual creara automáticamente los usuarios con sus respectivas contraseñas además de también darme la opción de validar el tiempo de registro.

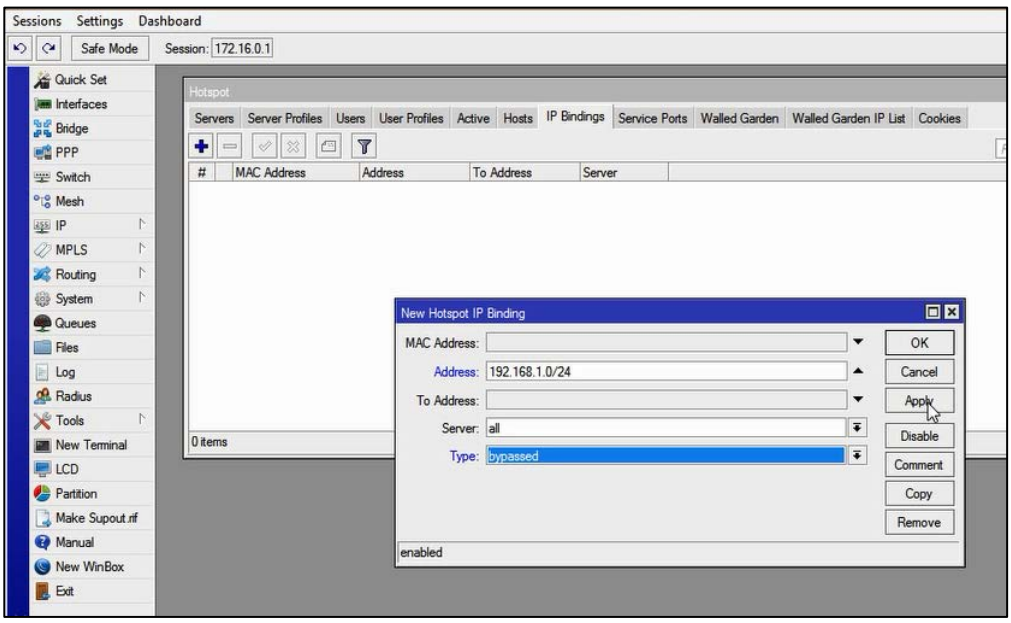
Reiniciamos el equipo y realizamos la prueba de Hotspot ingresando la dirección que dejamos establecida “pruebahotel.com”.



Listas de registros de HotSpot por cada usuario logoneado.



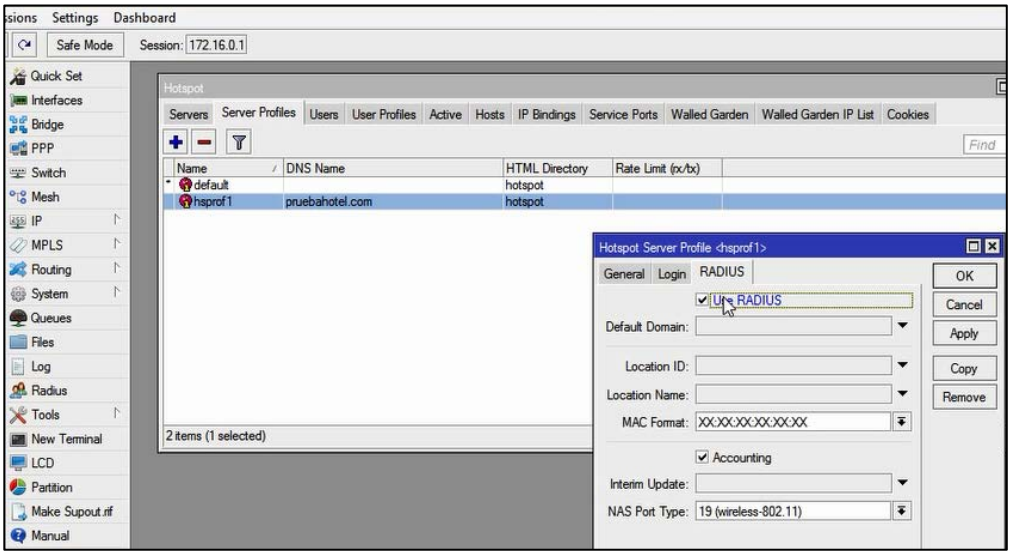
3. Una vez realizados los pasos anteriores, debemos de indicar que el área de administración no debe de pasar por el HotSpot así que nos dirigimos a la opción “IP Bindings” para configurar el rango de IP/MAC seleccionadas indicando que el Type será “bypassed”.



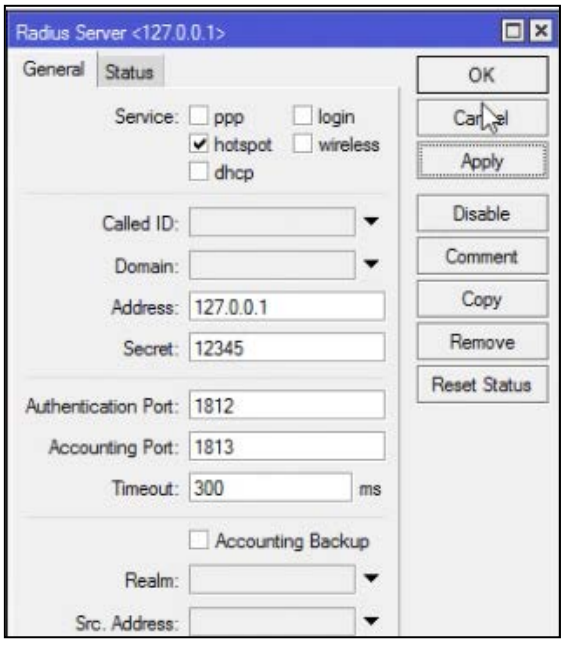
Configuración del Radius

4. Como lo indicamos anteriormente este proceso se lleva a cabo para generar usuarios y contraseñas de manera aleatoria.

   Nos dirigimos a la opción “Server Profiles” y activamos la opción “Use RADIUS” la cual va a indicar al HotSpot que no utilice su usuario (prueba) sino que use los usuarios del RADIUS.



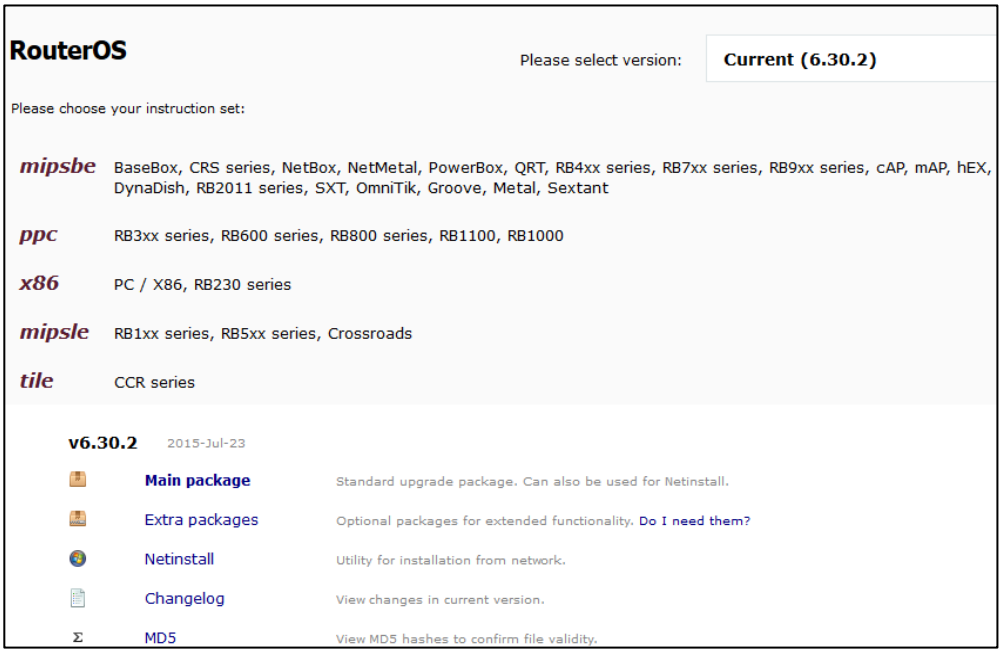
5. Seleccionamos la pestaña “RADIUS” en la cual le vamos a indicar que lea lo que funciona con HotSpot, aquí mismo indicamos la dirección del equipo local host, en este caso es el mismo equipo que estamos utilizando (127.0.0.1) adicional a esto asignamos una contraseña (12345) y le damos aplicar.



User Manager

6. Para la creación automática de usuarios necesitaremos User Manager, es un sistema de gestión que se puede utilizar para usuarios HotSpot, PPP, usuarios DHCP, usuarios inalámbricos, usuarios RouterOS.

   Esta es una aplicación del Servidos RADIUS. Podemos descargar el paquete de la página de Mikrotik (http://www.mikrotik.com/download)



Descargar:

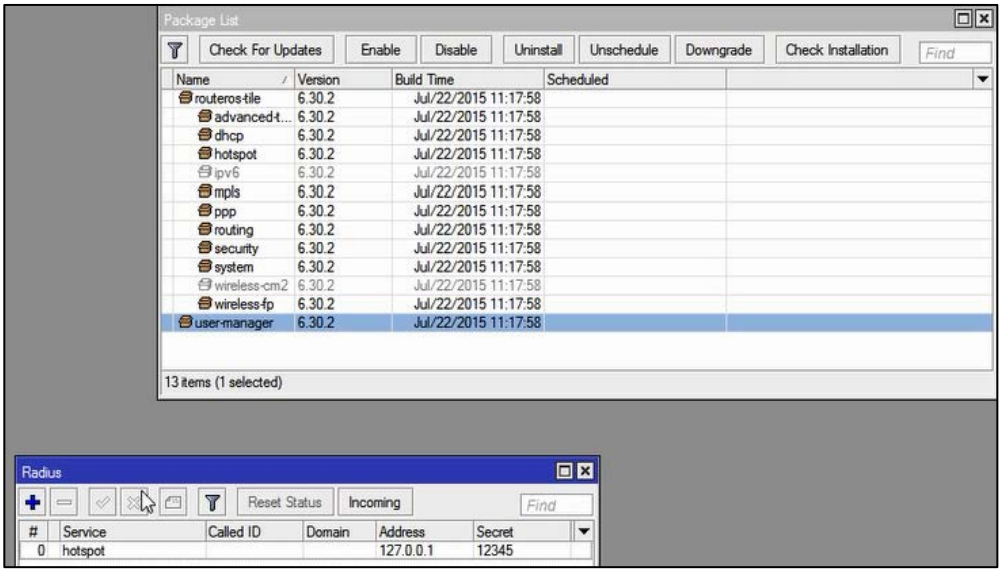
- Main Package para actualizar el equipo es decir el sistema operativo en el caso que se requiera.
- Extra Package para obtener los paquetes necesarios (User Manager)

Ambos paquetes deben ser arrastrados en la ventana “File List”, finalizando con un reboot al sistema.

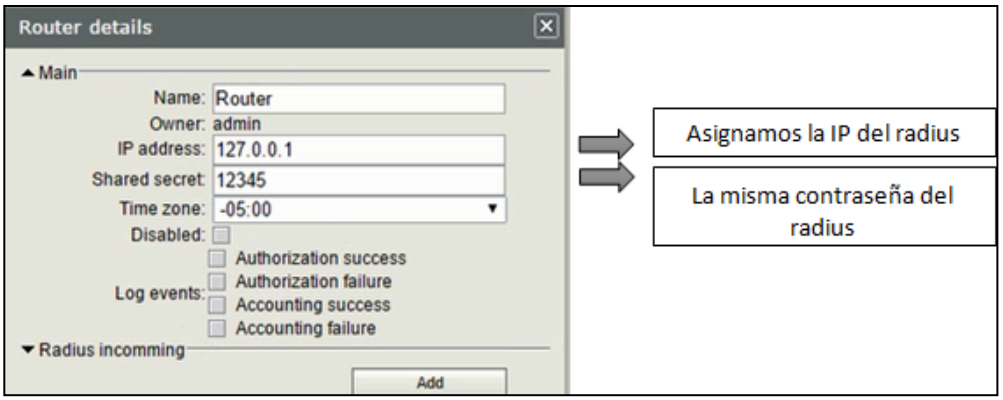
7. Tenemos dos opciones para abrir User Manager; mediante línea de comandos o a través de un navegador con la dirección 172.16.0.1/userman.

Donde el usuario por defecto es “admin” y la contraseña la dejamos en blanco abriendo una nueva ventana.

Una vez habiendo realizado estos pasos debemos hacer que el User Manager y el HotSpot trabajen juntos.



Seleccionamos la opción “Routers” damos click en “Add” e ingresamos la dirección del equipo que actuara como Servidor RADIUS en nuestro caso es el mismo equipo con el cual estamos trabajando.



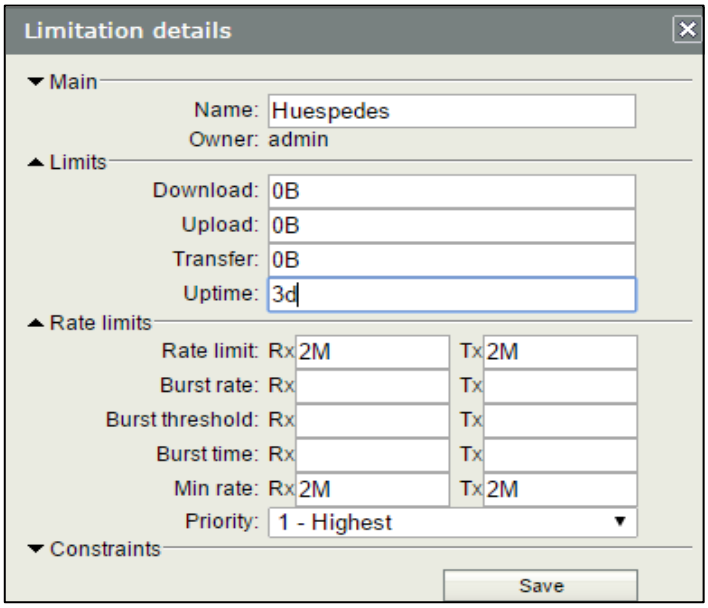
Creación de Tickets

8. En este paso indicaremos las limitantes que tendrá el huésped al momento de su registro, es decir:
   - ✓ Cantidad de megas
   - ✓ Tiempo de validación del tickets

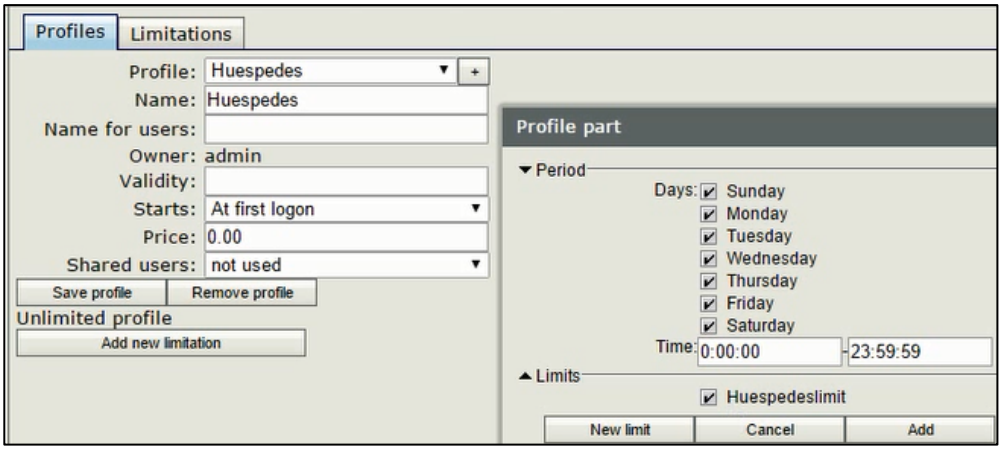
Seleccionamos la opción “Profiles” -> Add

9. Seleccionamos la pestaña “Limitations” -> Add.

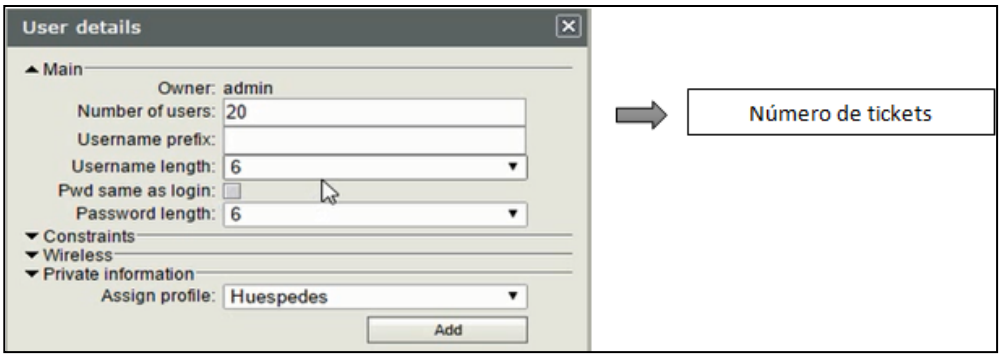
   Aquí especificaremos que se le asignara a cada huésped 2 Mbps en “Rate limit” y “Min Rate”; y el tiempo de registro del huésped lo colocamos en “UpTime”.



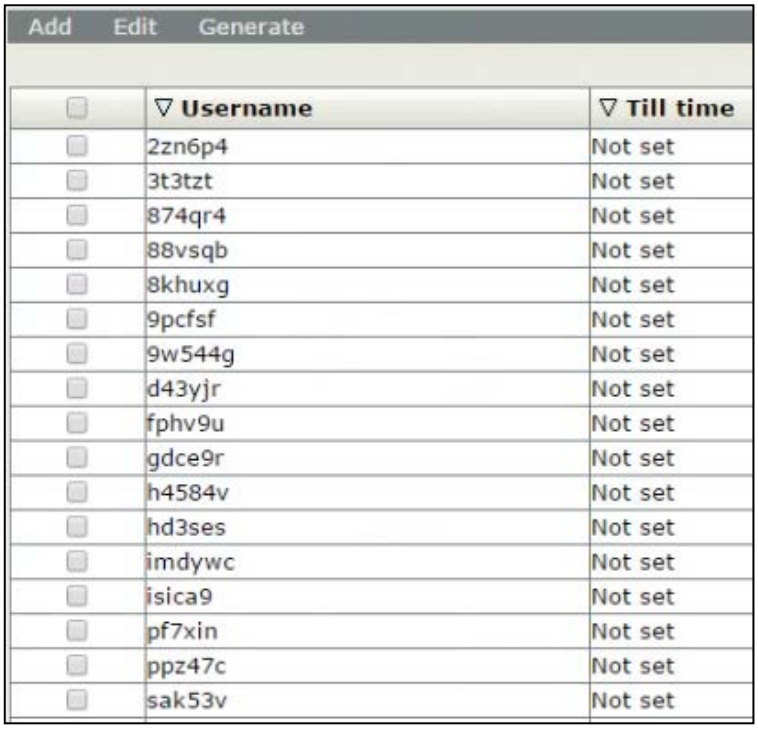
10. Luego procedemos a unir el perfil de los huéspedes con las limitantes que creamos. Vamos a “Add new limitation” y le damos visto a Huespedeslimit.



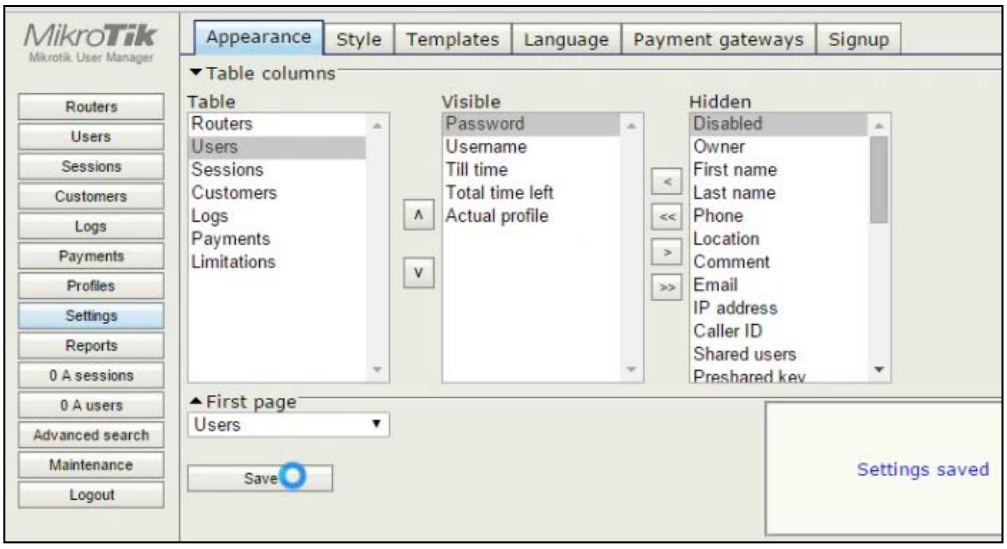
11. Creación de usuarios, nos dirigimos a la pestaña “Users” -> Add aquí se nos permite crear usuario por usuario o por lotes, en este caso seleccionamos Batch que se refiere a la creación por lotes.

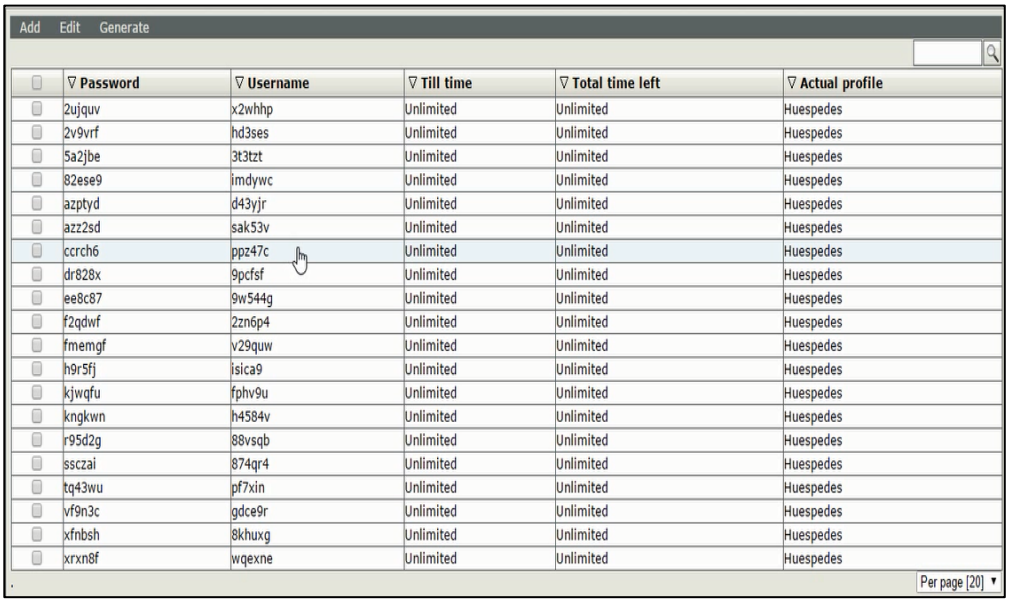


Automáticamente una vez presionada la tecla “Add” se muestran los tickets creados.



Para poder visualizar los usuarios con sus respectivas contraseñas nos dirigimos a Settings, seleccionamos Password seguido de la opción “<” y lo grabamos.

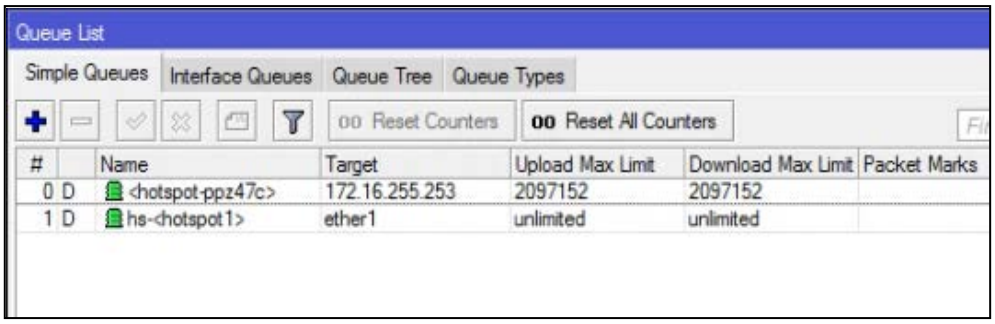




Asignación de Ancho de Banda

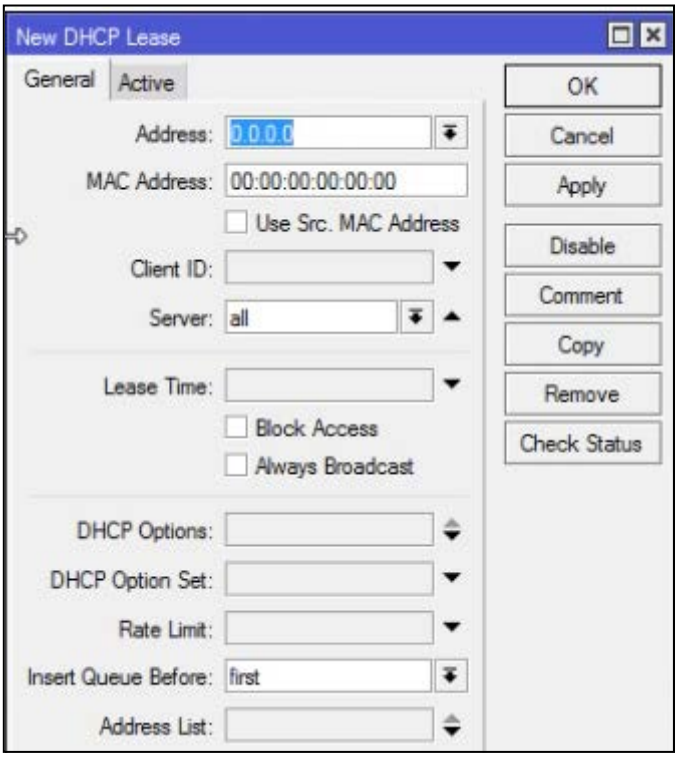
12. En MikroTik se usa dos tipos de asignación de ancho de banda las cuales son:

    - ✓ Simple Queues (diseñado para facilitar la configuración de las tareas de gestión de colas simples y cotidianas)
    - ✓ Queue Tree (para implementar en políticas de priorización global, limitaciones de grupos de usuarios)

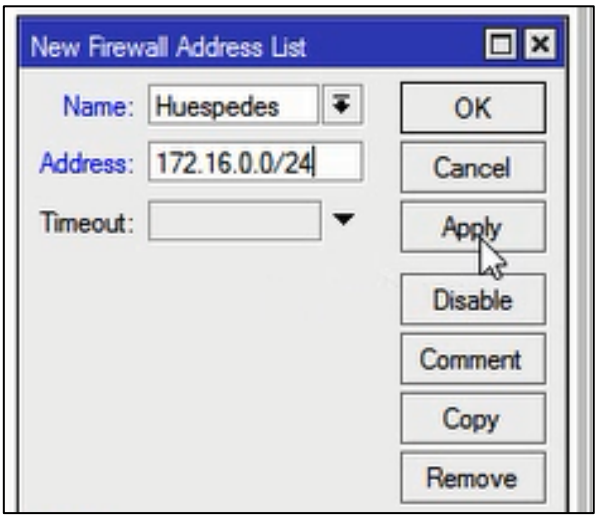


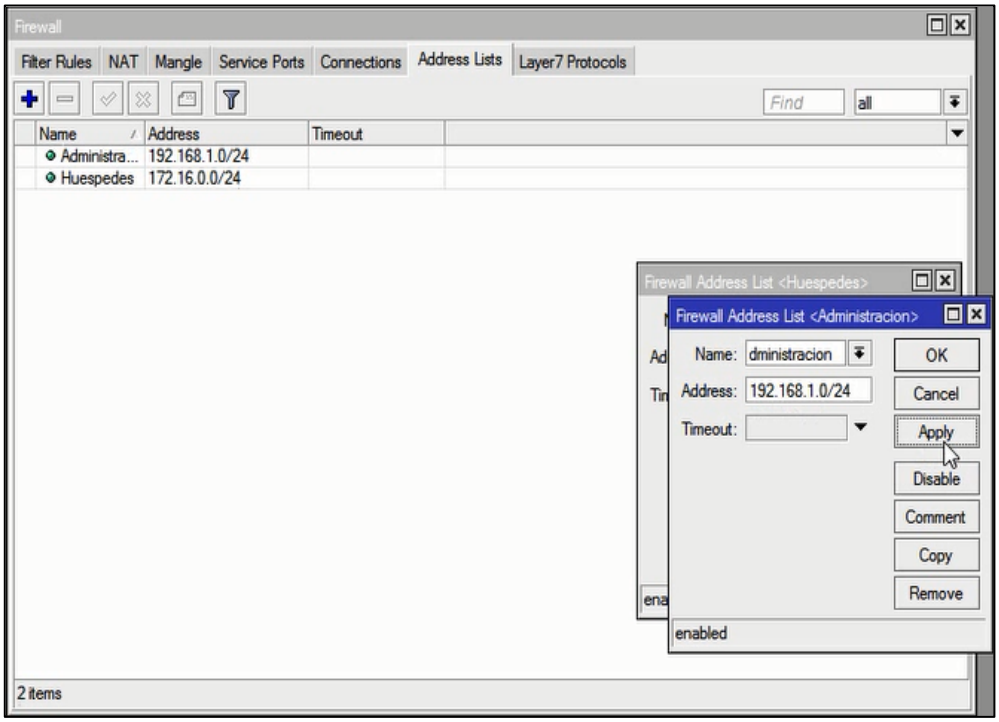
En la imagen visualizamos un usuario conectado que tiene 2 Mbps de navegación, cuando el tiempo de validación del ticket expira ese usuario se elimina automáticamente de la tabla.

13. Para la parte de administración en el denominado amarre de MAC nos dirigimos a IP, seleccionamos DHCP Server; en la opción “Leases” le damos al signo “+”, allí agregamos cada MAC de las diferentes PC del área administrativa con la dirección correspondiente que le toca.



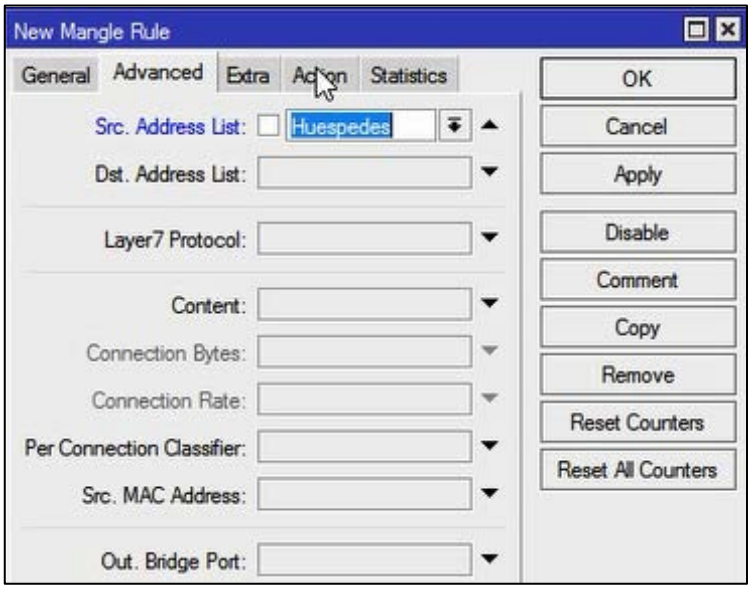
14. Nos dirigimos a la pestaña IP -> Firewall -> Address Lists para indicar que direcciones van aplicar QoS así que vamos a dividir la parte de Administración (20 Mbps) y la de los Huéspedes (61 Mbps) para la cual seleccionamos la opción “+” y agregamos las direcciones.

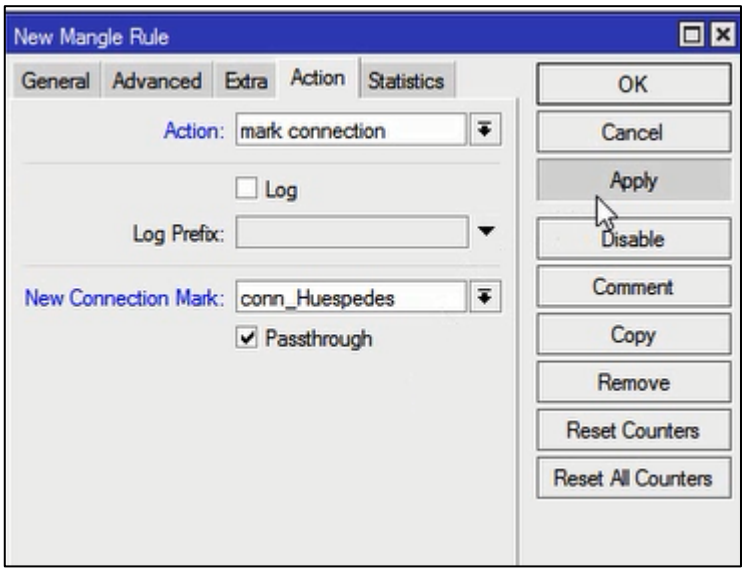


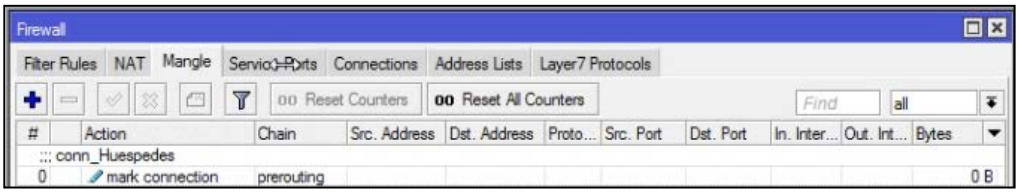


15. No solo basta indicar la dirección de cada red sino que también es recomendable hacerle un seguimiento, es decir por ejemplo que a todas las redes que tengan la dirección 172.16.0.0 se le asigne la etiqueta “Huéspedes” para a todas esas etiquetas meterlas en un solo paquete y asignarle el respectivo ancho de banda.

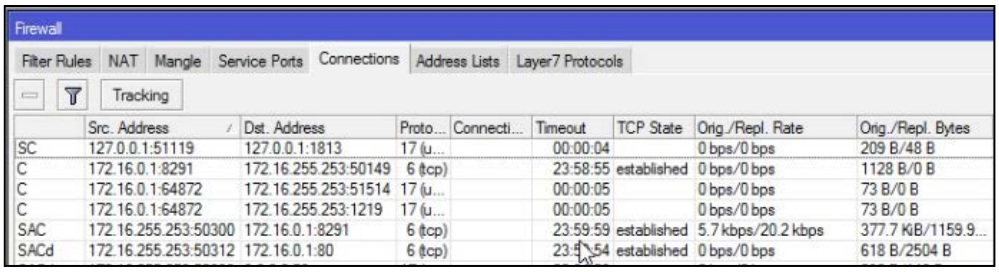
    Para esto nos dirigimos a la pestaña “Mangle” -> Add. Aquí creamos dos cosas; marca de conexión, con eso realizamos el seguimiento y la marca de paquetes es para meter todas esas conexiones en ese paquete.


New Mangle Rule
General
Advanced
Extra
Action
Statistics
Src. Address List:
Huespedes
Dst. Address List:
Layer7 Protocol:
Content:
Connection Bytes:
Connection Rate:
Per Connection Classifier:
Src. MAC Address:
Out. Bridge Port:
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

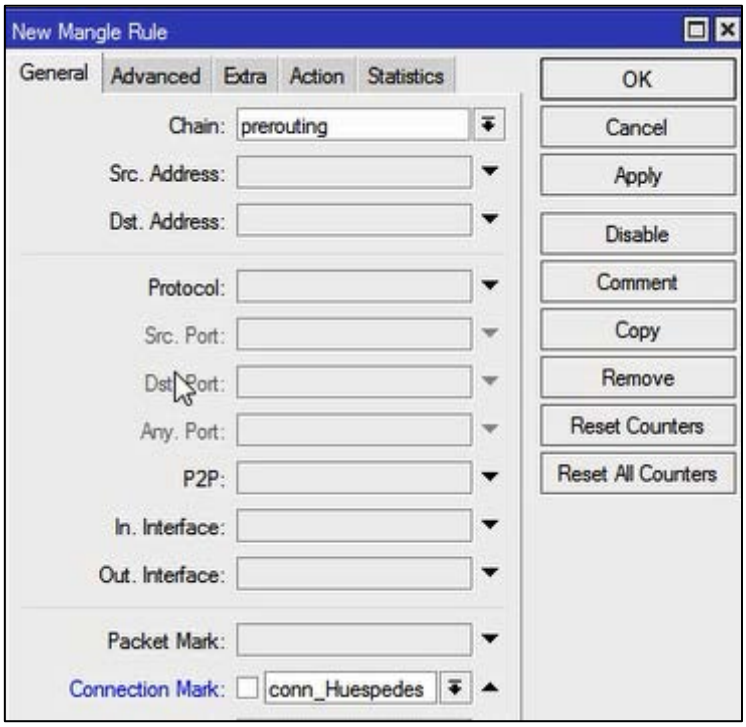

New Mangle Rule
General
Advanced
Extra
Action
Statistics
Action:
mark connection
Log
Log Prefix:
New Connection Mark:
conn_Huespedes
Passthrough
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

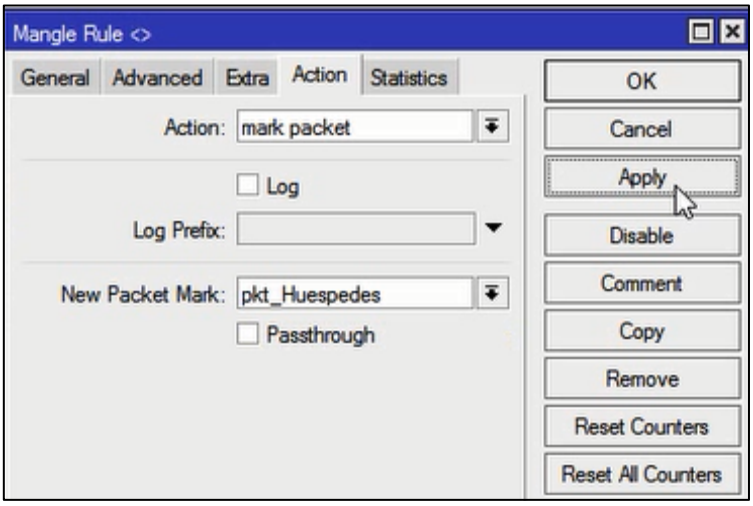

Firewall
Filter Rules
NAT
Mangle
Service Ports
Connections
Address Lists
Layer7 Protocols
Reset Counters
Reset All Counters
Find
all
Action Chain Src. Address Dst. Address Proto... Src. Port Dst. Port In. Inter... Out. Int... Bytes
;;; conn_Huespedes
0 mark connection prerouting 0 B

Una vez que se comienza a generar tráfico de Huéspedes lo podemos visualizar en la pestaña Connections en la cual se monitorea el tráfico en tiempo real.



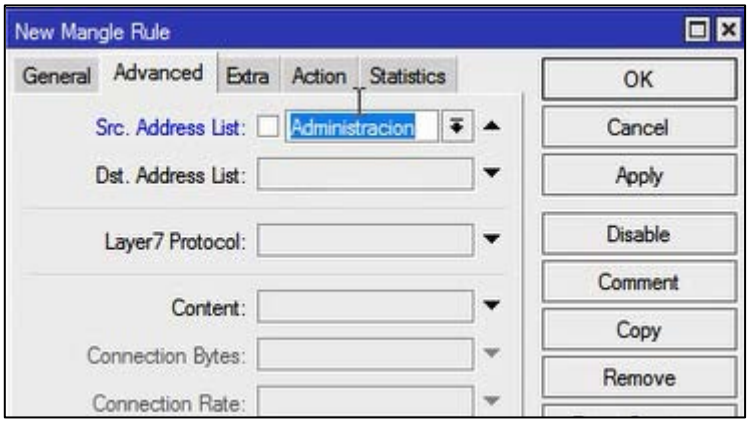
16. Ahora nos dirigimos a agrupar los paquetes según su tipo.

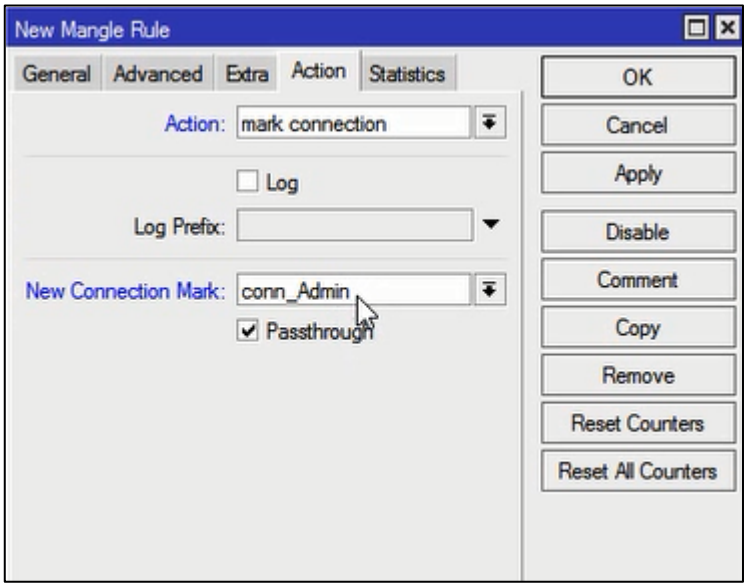


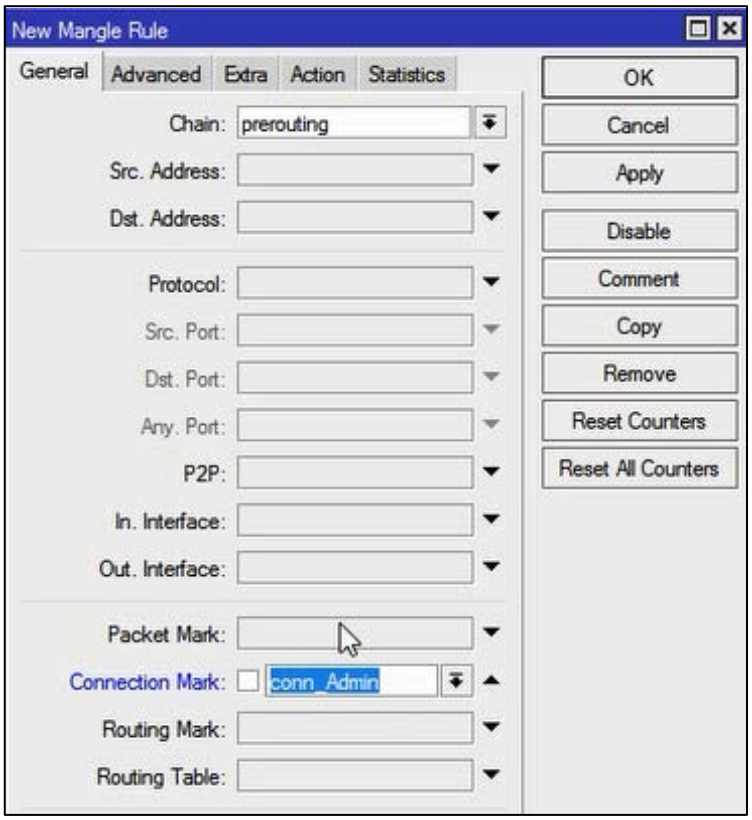


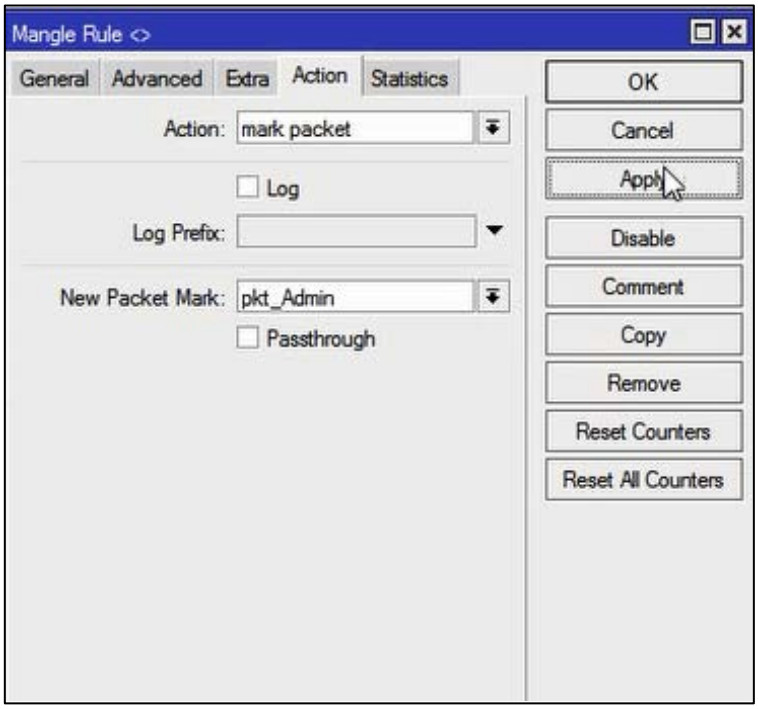
En este punto le quitamos la opción que por defecto viene activada “Passthrough” (Siguiente Paso) ya que lo único que debe de ser procesado son las marcas de conexiones y en este caso los paquetes son procesados en el Queue Tree.

17. El mismo procedimiento se lo lleva a cabo para el área de la Administración.



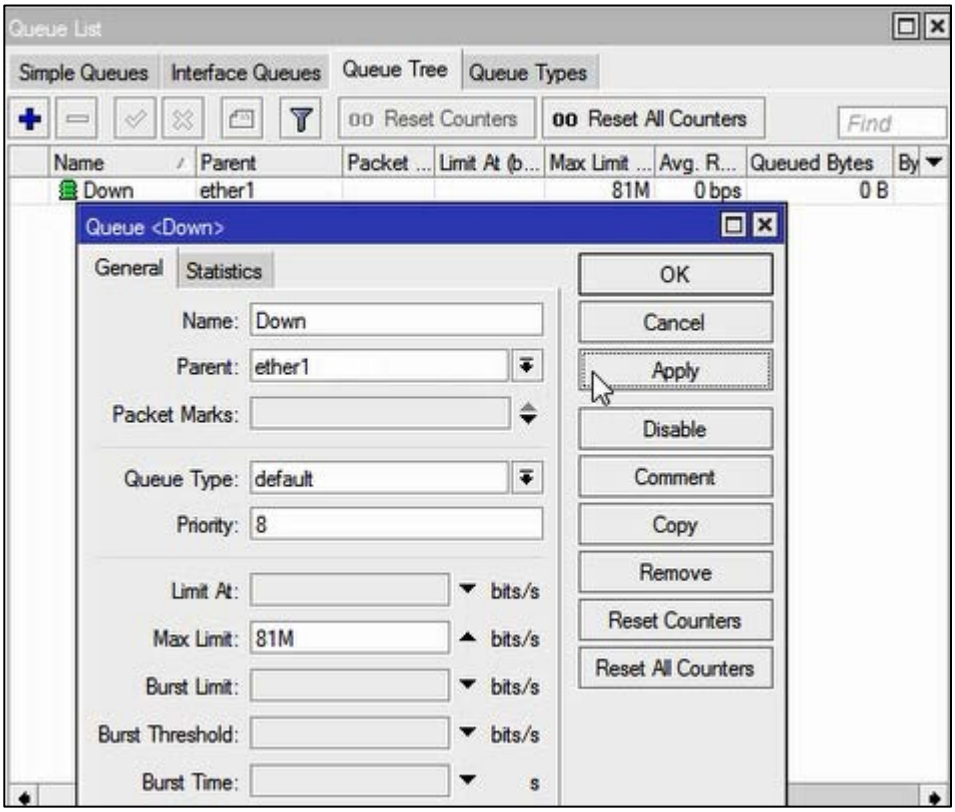

New Mangle Rule
General
Advanced
Extra
Action
Statistics
Action:
mark connection
Log
Log Prefix:
New Connection Mark:
conn_Admin
Passthrough
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters


New Mangle Rule
General
Advanced
Extra
Action
Statistics
Chain:
prerouting
Src. Address:
Dst. Address:
Protocol:
Src. Port:
Dst. Port:
Any. Port:
P2P:
In. Interface:
Out. Interface:
Packet Mark:
Connection Mark:
conn_Admin
Routing Mark:
Routing Table:
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

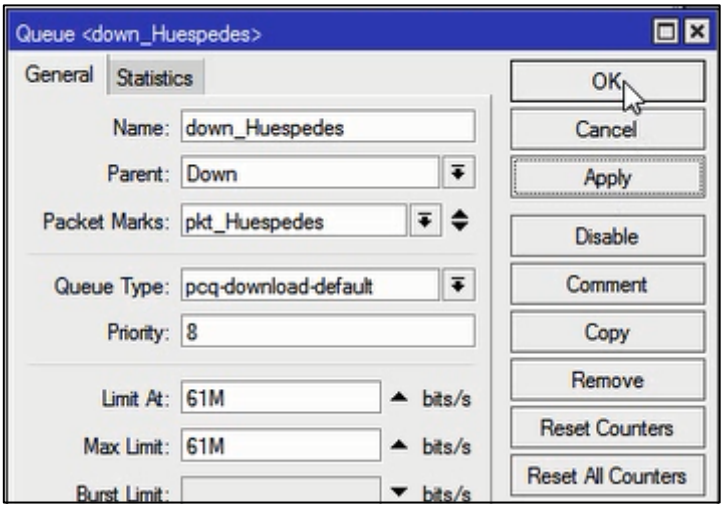


Configuración del Queue Tree – Árbol de Colas

18. Esto lo realizamos en la opción “Queues”, primero vamos a marcar el tráfico de bajada seleccionando “+” aquí indicamos cual es la interfaz que está administrando todo el direccionamiento (Ethernet 1) en este caso estamos creando según Jerarquía “Padre”. Adicional a esto especificamos cuantos son los megas totales en la opción “Max Limit”.

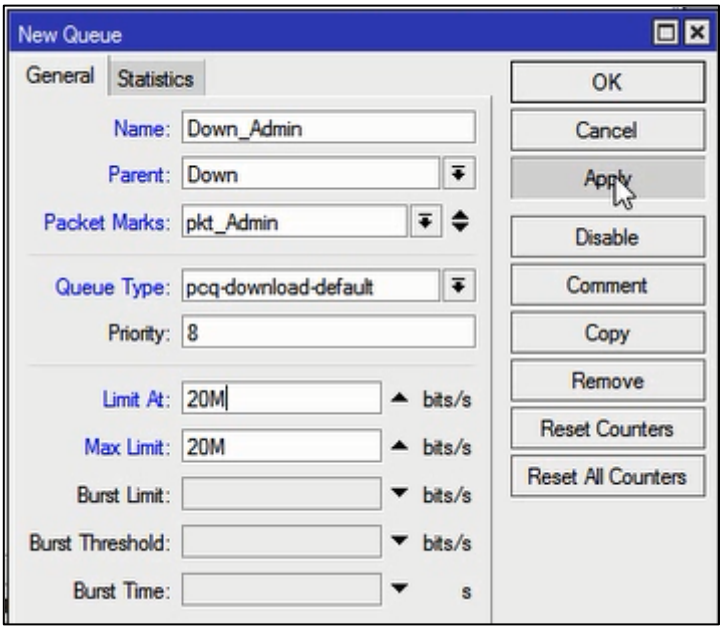


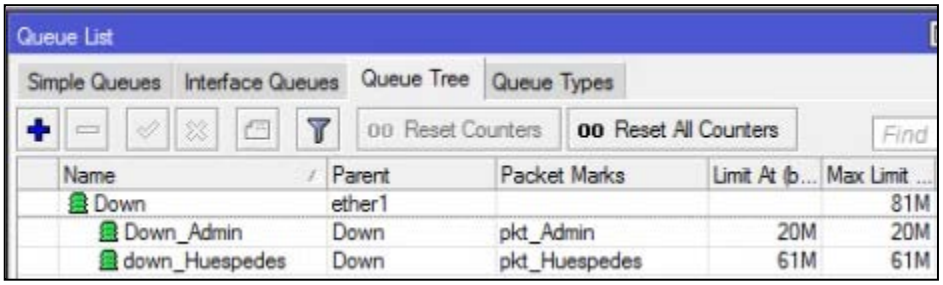
19. Procedemos luego a agregar los “Hijos”.



Aquí especificamos que los Megas totales para el área de los Huéspedes son de 61 Mbps.

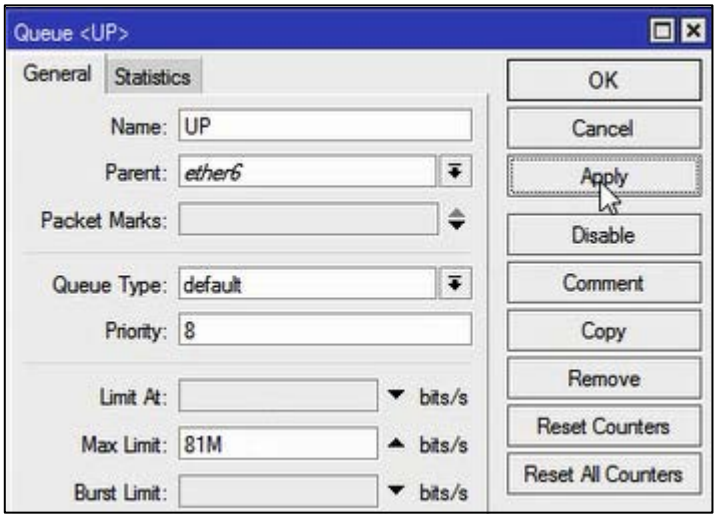
20. El mismo procedimiento se realiza para el área de Administración.



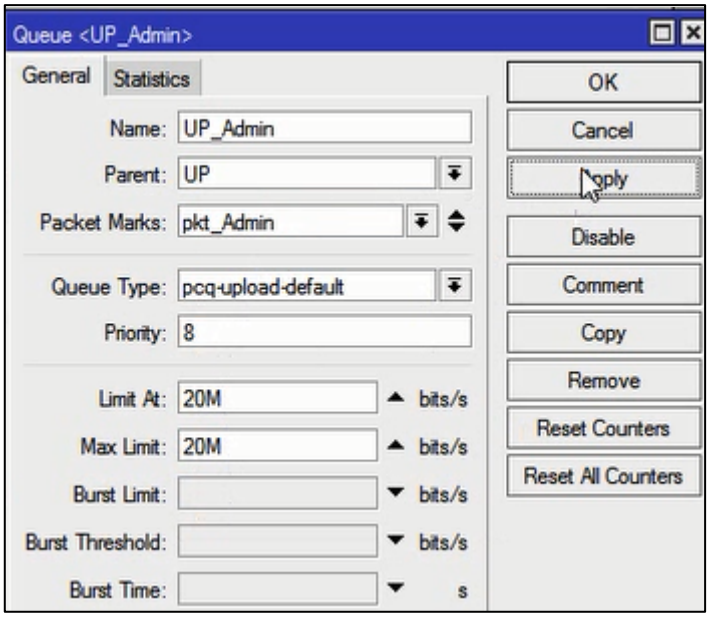


Vemos que ya tenemos especificado el tráfico de bajada.

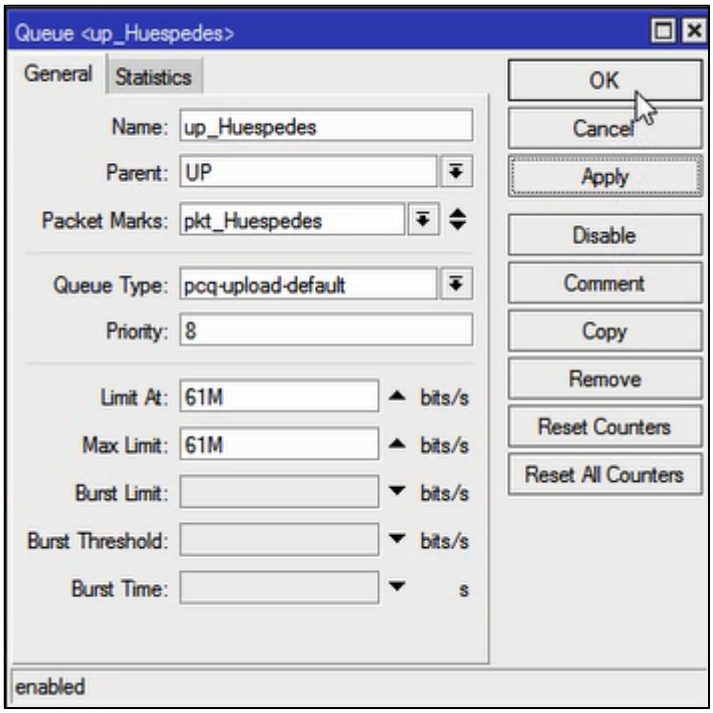
21. Ahora marcamos el tráfico de subida indicando la interfaz por la cual va a salir al Internet (Ethernet 6).

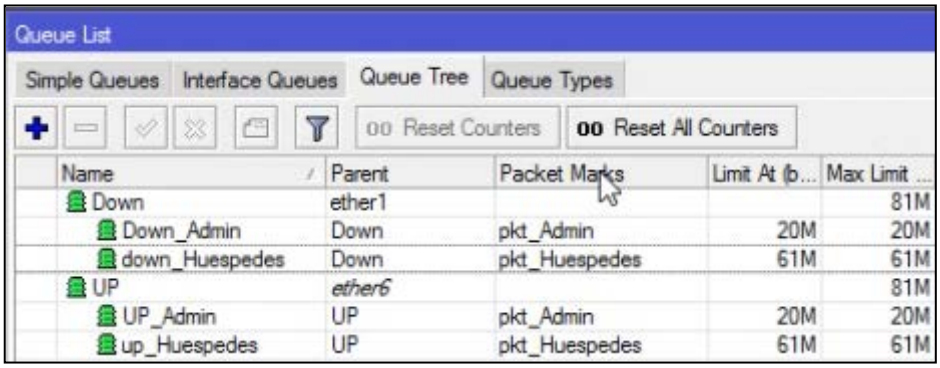


22. Tráfico de salida en el área de la Administración.



23. Tráfico de salida en el área de Huéspedes.

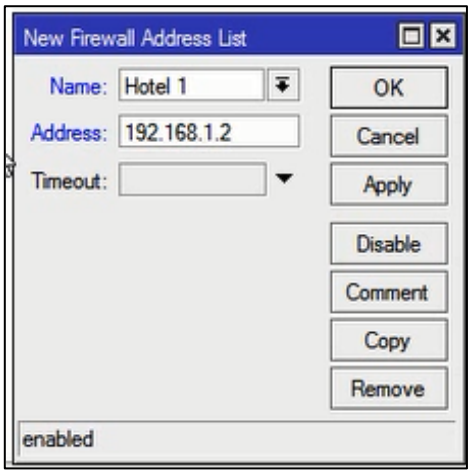


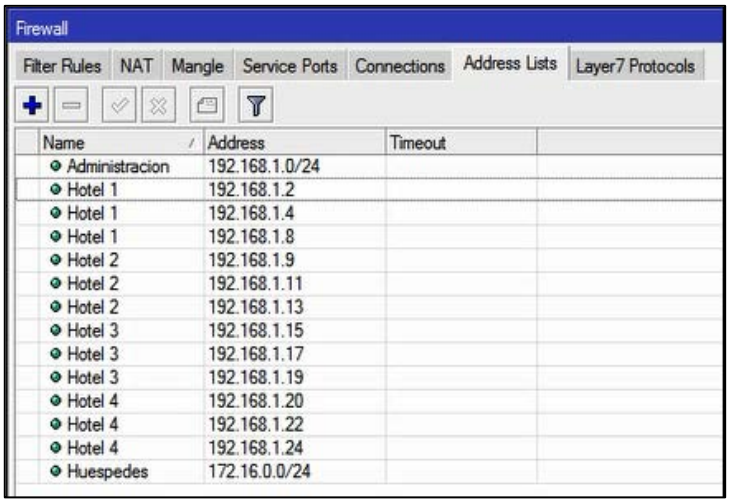


Aquí ya vemos nuestra asignación de ancho de banda tanto para el área Administrativa como para la de los Huéspedes.

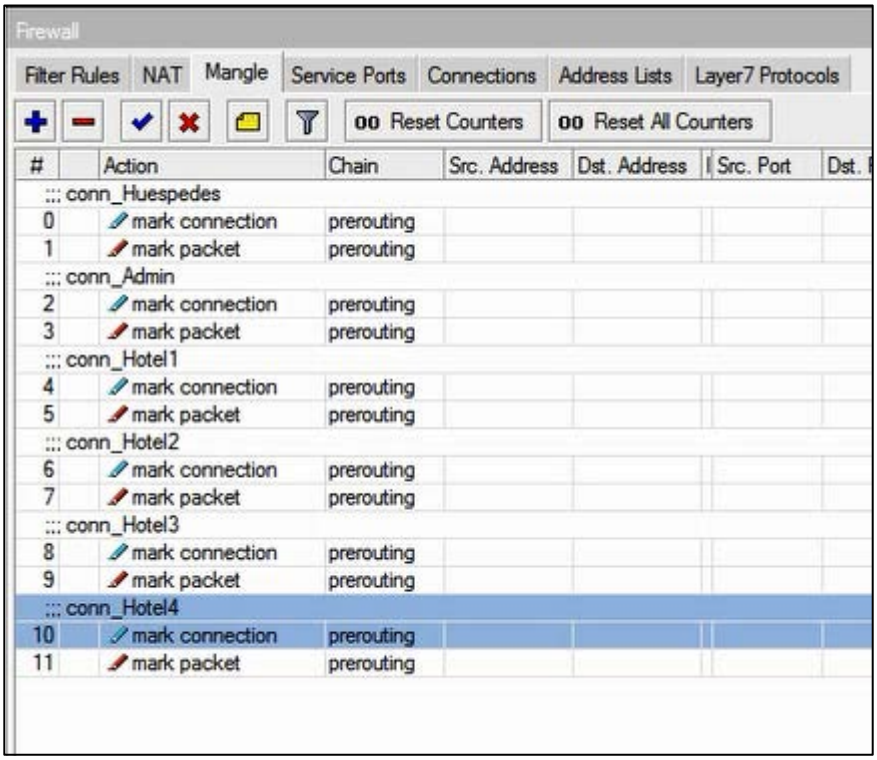
24. Para comenzar a aplicar QoS tenemos que dividir Administración en 4 grupos refiriéndonos a los 4 hoteles.

    Nos dirigimos a la opción Firewall -> Address Lists. Cabe recalcar que la Calidad de Servicio solo se aplicara en el área Administrativa.



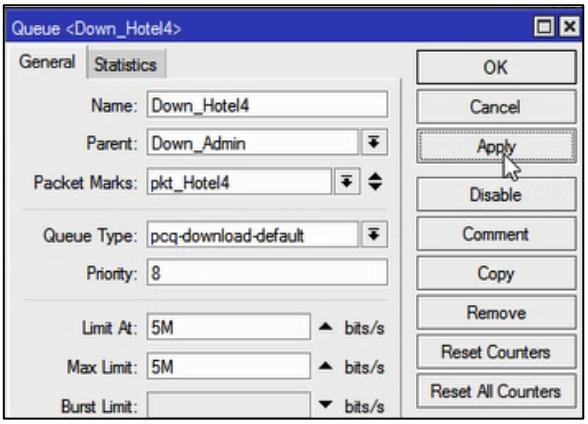


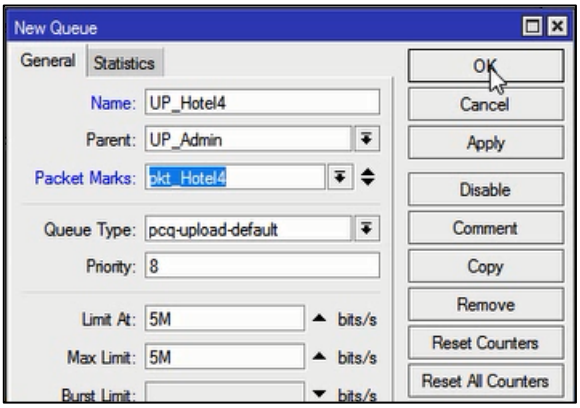
25. Realizamos en cada grupo creado el seguimiento correspondiente, como en los pasos anteriormente expuestos.

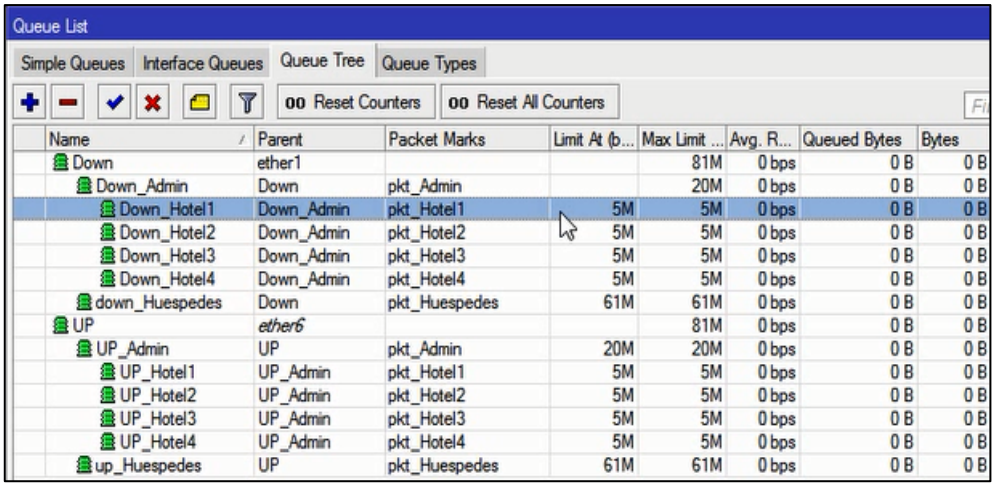


26. Cada grupo (Hotel1, Hotel2, Hotel3 y Hotel4) deberá tomar como Padre a Down_Admin y a UP_Admin.

    Se debe especificar también que por cada hotel en el área Administrativa se le asigna 5 Mbps.

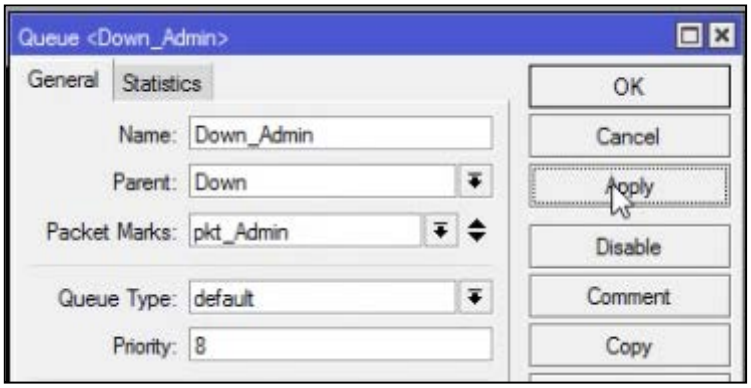


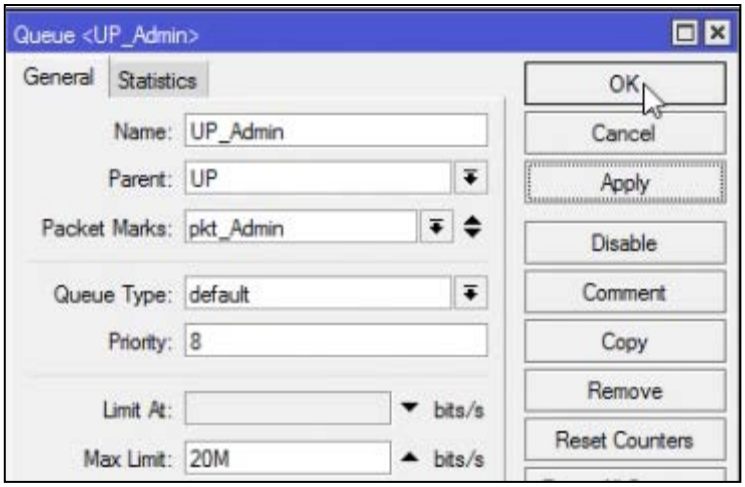


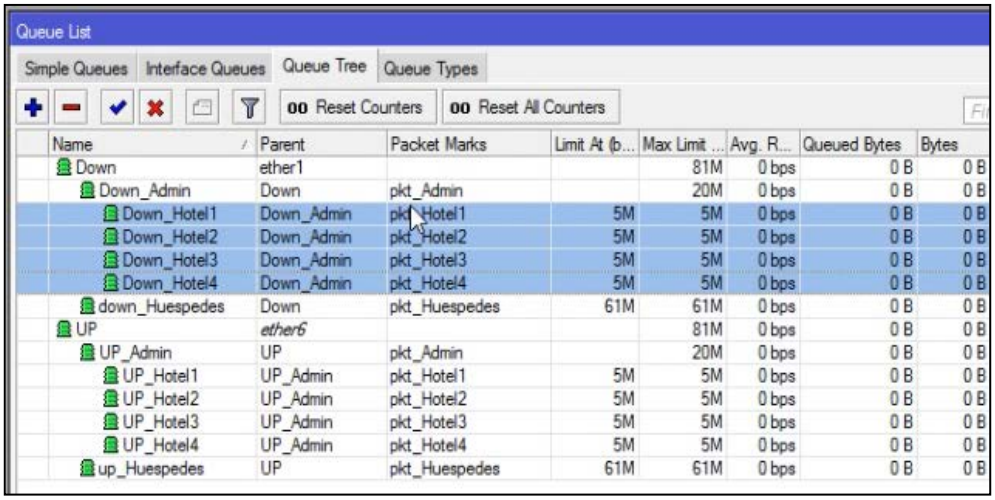


Como ahora Down_Admin y UP_Admin se convirtieron en “Padres” siguiendo la jerarquía les quitamos lo que anteriormente habíamos especificado; el “Limit At” ya que a los “Padres” no se los limita, a ellos se le da todo el ancho de banda posible.

Además también a los “Padres” debemos de dejarle por default la opción “Queue Type”.



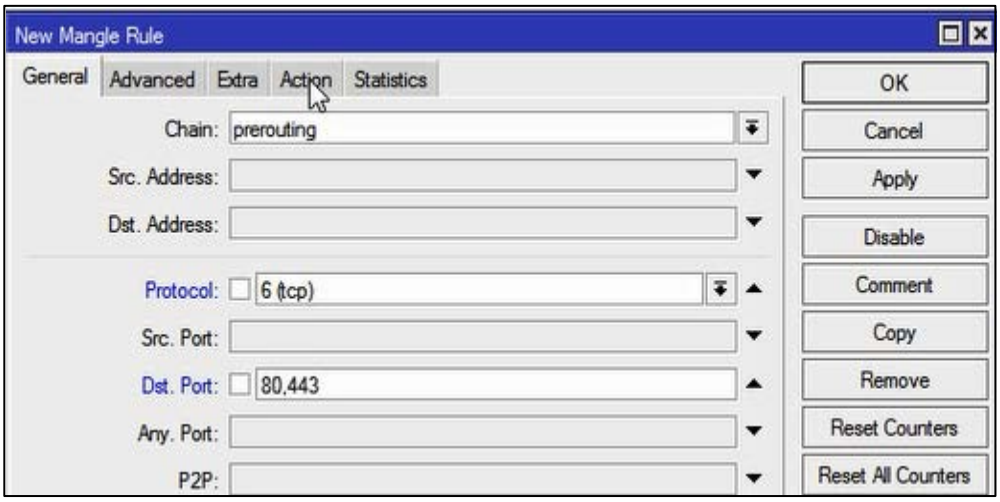


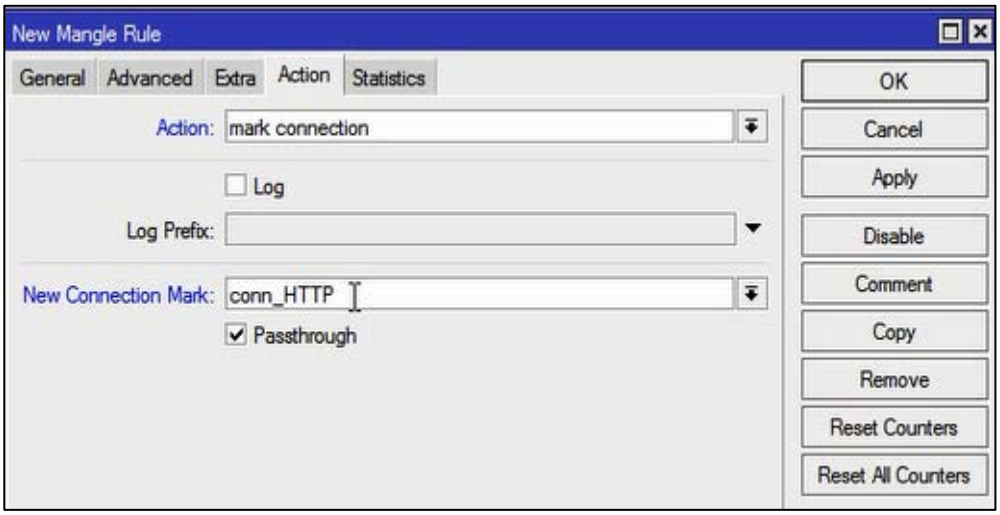


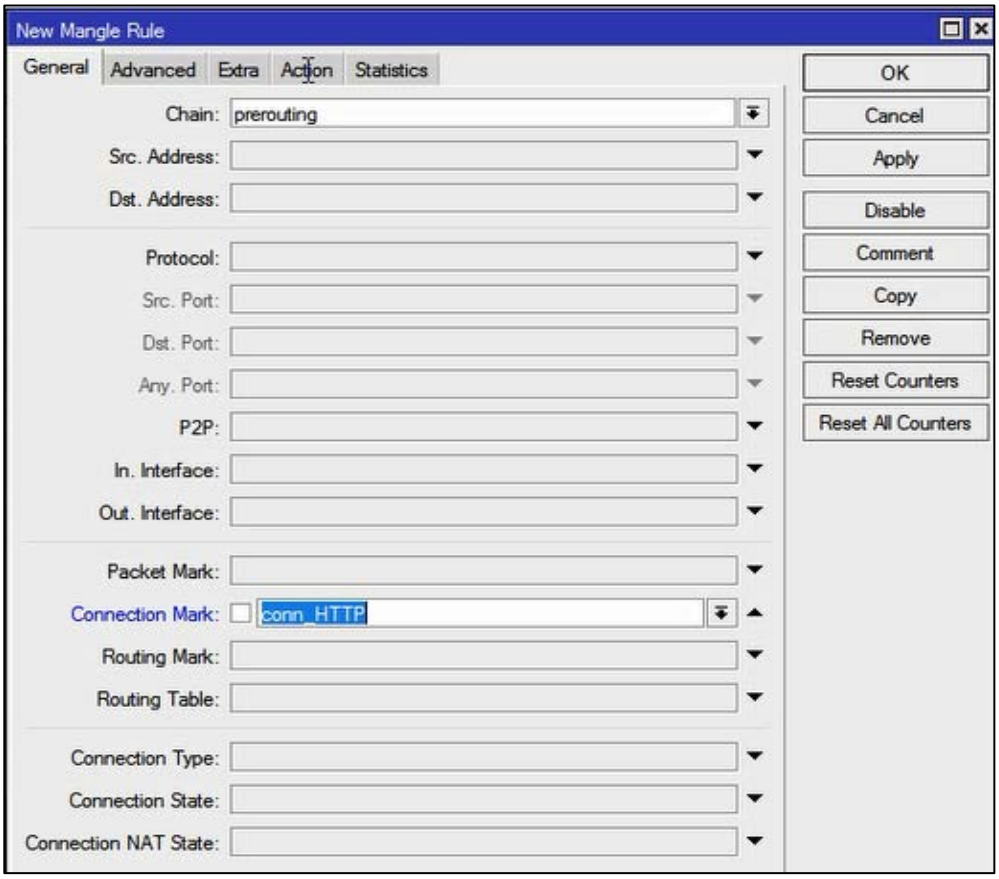
Name	Parent	Packet Marks	Limit At (b...	Max Limit ...	Avg. R...	Queued Bytes	Bytes
Down	ether1			81M	0 bps	0 B	0 B
Down_Admin	Down	pkt_Admin		20M	0 bps	0 B	0 B
Down_Hotel1	Down_Admin	pkt_Hotel1	5M	5M	0 bps	0 B	0 B
Down_Hotel2	Down_Admin	pkt_Hotel2	5M	5M	0 bps	0 B	0 B
Down_Hotel3	Down_Admin	pkt_Hotel3	5M	5M	0 bps	0 B	0 B
Down_Hotel4	Down_Admin	pkt_Hotel4	5M	5M	0 bps	0 B	0 B
down_Huespedes	Down	pkt_Huespedes	61M	61M	0 bps	0 B	0 B
UP	*ether6*			81M	0 bps	0 B	0 B
UP_Admin	UP	pkt_Admin		20M	0 bps	0 B	0 B
UP_Hotel1	UP_Admin	pkt_Hotel1	5M	5M	0 bps	0 B	0 B
UP_Hotel2	UP_Admin	pkt_Hotel2	5M	5M	0 bps	0 B	0 B
UP_Hotel3	UP_Admin	pkt_Hotel3	5M	5M	0 bps	0 B	0 B
UP_Hotel4	UP_Admin	pkt_Hotel4	5M	5M	0 bps	0 B	0 B
up_Huespedes	UP	pkt_Huespedes	61M	61M	0 bps	0 B	0 B

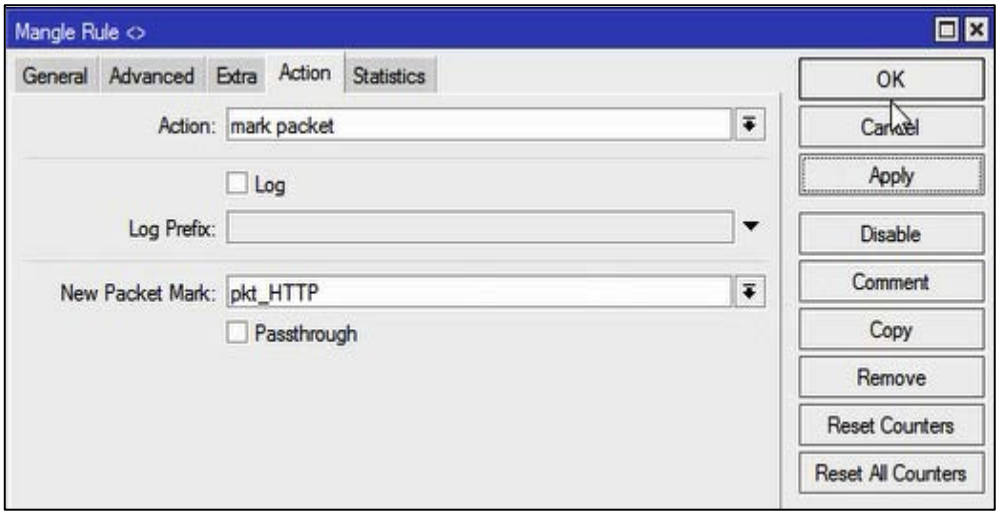
27. Para la Calidad de Servicio tenemos que darle también seguimiento a los tráficos que tienen más demanda como lo es el de navegación, correo y telefonía. Nos dirigimos a la opción “Firewall” -> Mangle -> “+” para especificar los protocolos que vamos a utilizar.

Navegación – HTTP & HTTPS

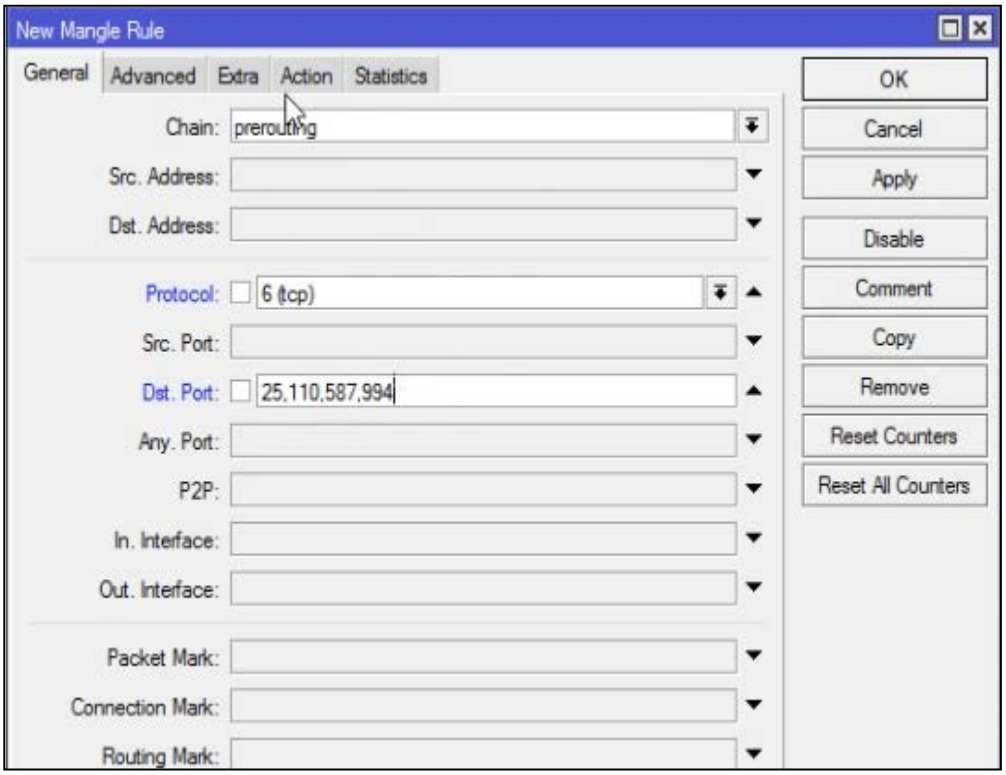




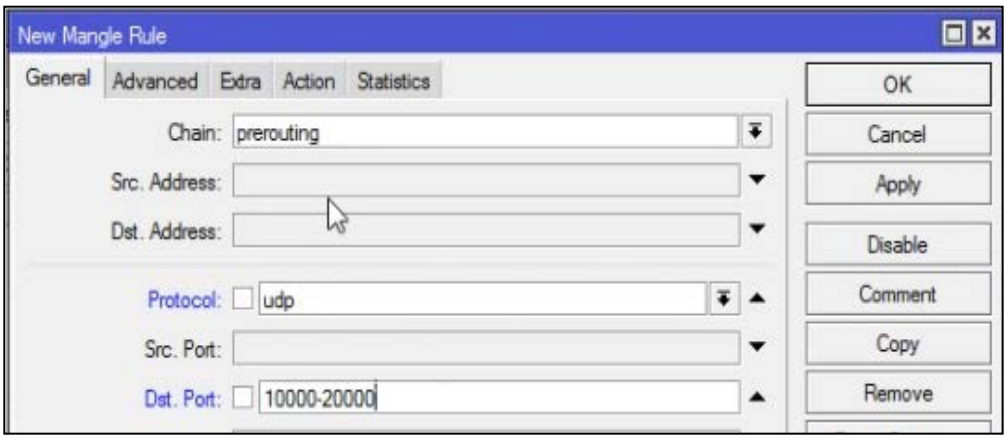

New Mangle Rule
General
Advanced
Extra
Action
Statistics
Chain: prerouting
Src. Address:
Dst. Address:
Protocol:
Src. Port:
Dst. Port:
Any. Port:
P2P:
In. Interface:
Out. Interface:
Packet Mark:
Connection Mark: conn_HTTP
Routing Mark:
Routing Table:
Connection Type:
Connection State:
Connection NAT State:
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters


Mangle Rule <>
General
Advanced
Extra
Action
Statistics
Action: mark packet
Log
Log Prefix:
New Packet Mark: pkt_HTTP
Passthrough
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

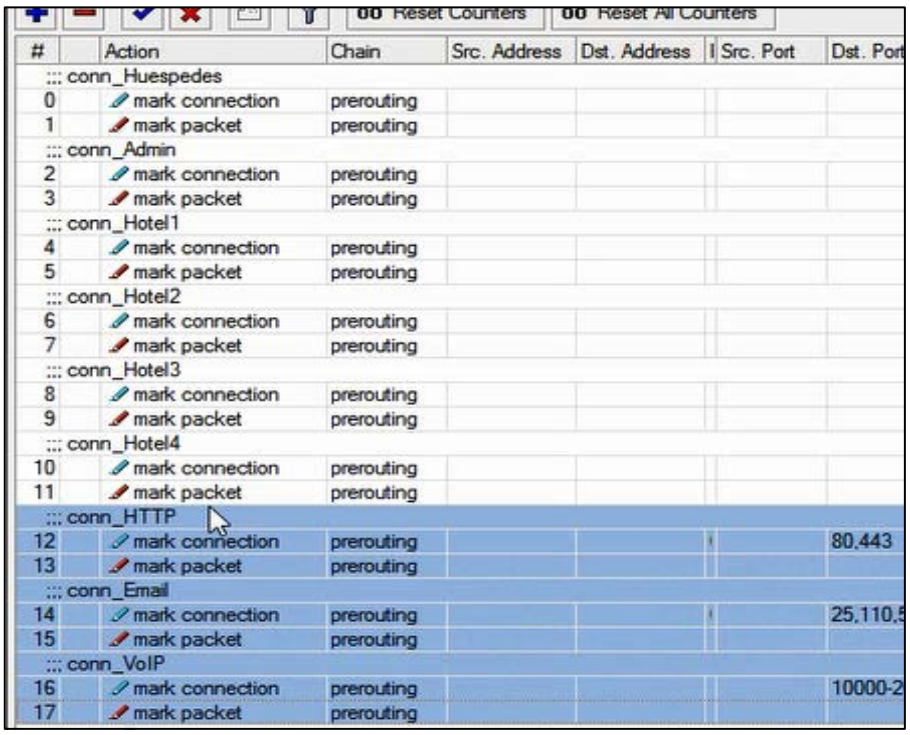
Correo



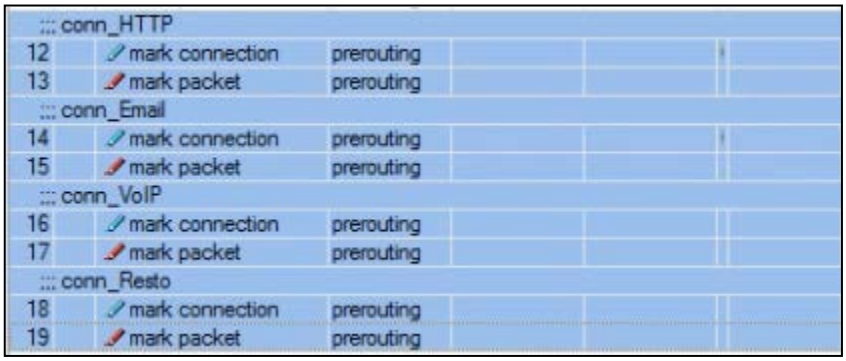
Telefonía



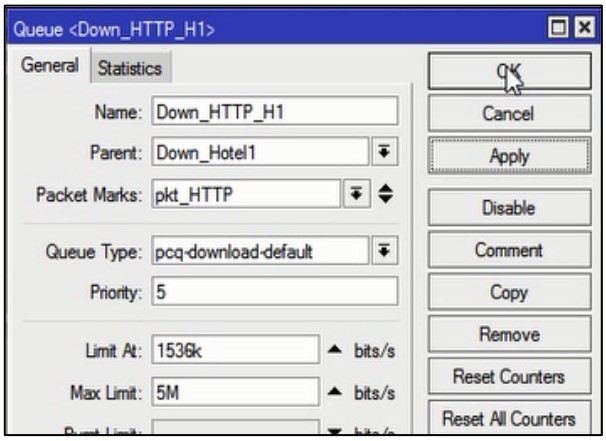
Repetimos el mismo procedimiento que realizamos en Navegación para Correo y Telefonía quedándonos de esta manera:

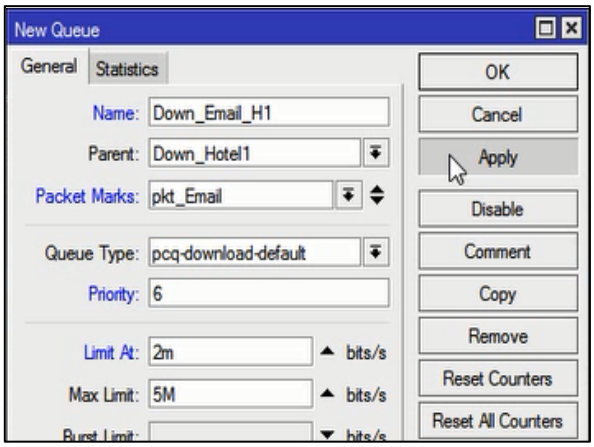


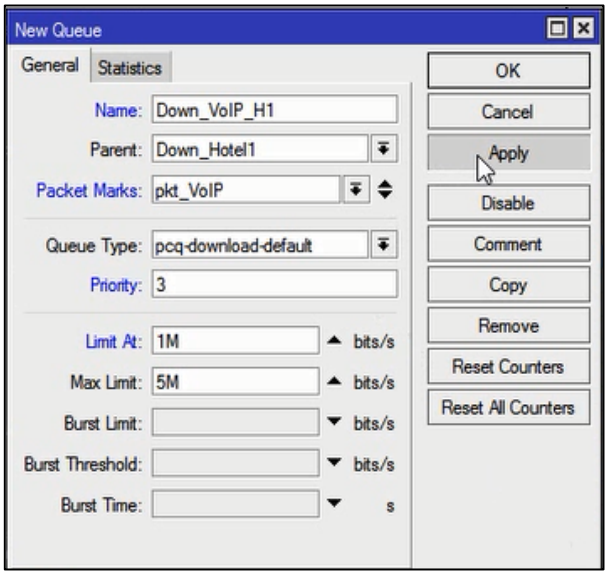
Luego de esto debemos de crear también un Marcado Total es decir para que en este punto se marque cualquier tipo de protocolo para asignarle un pequeño ancho de banda.

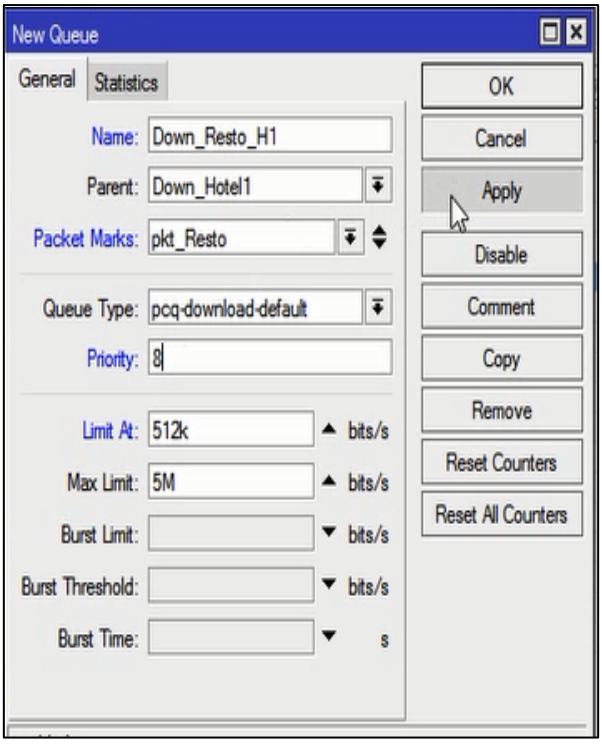


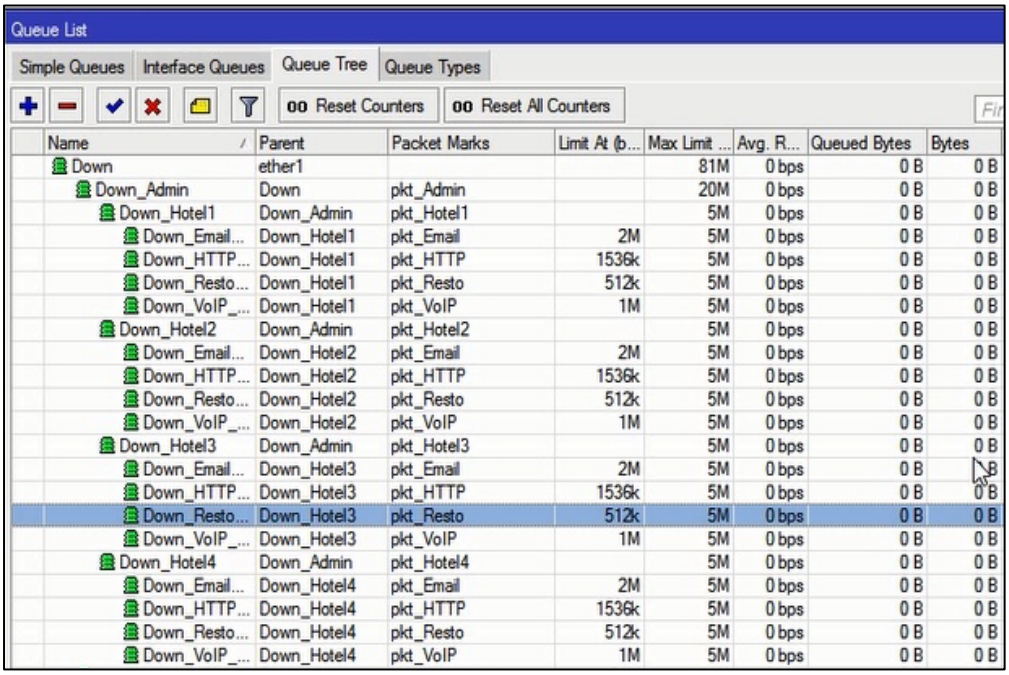
28. Cada paquete de protocolo debe de seguir la Jerarquía configurada anteriormente, proporcionando la totalidad de megas disponibles por cada protocolo y sus limitantes. También aplicaremos la prioridad que sea necesaria según los requerimientos.






New Queue
General
Statistics
Name: Down_VoIP_H1
Parent: Down_Hotel1
Packet Marks: pkt_VoIP
Queue Type: pcq-download-default
Priority: 3
Limit At: 1M bits/s
Max Limit: 5M bits/s
Burst Limit: bits/s
Burst Threshold: bits/s
Burst Time: s
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters


New Queue
General
Statistics
Name: Down_Resto_H1
Parent: Down_Hotel1
Packet Marks: pkt_Resto
Queue Type: pcq-download-default
Priority: 8
Limit At: 512k bits/s
Max Limit: 5M bits/s
Burst Limit: bits/s
Burst Threshold: bits/s
Burst Time: s
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters



Name	Parent	Packet Marks	Limit At (b...	Max Limit ...	Avg. R...	Queued Bytes	Bytes
Down	ether1			81M	0 bps	0 B	0 B
Down_Admin	Down	pkt_Admin		20M	0 bps	0 B	0 B
Down_Hotel1	Down_Admin	pkt_Hotel1		5M	0 bps	0 B	0 B
Down_Email...	Down_Hotel1	pkt_Email	2M	5M	0 bps	0 B	0 B
Down_HTTP...	Down_Hotel1	pkt_HTTP	1536k	5M	0 bps	0 B	0 B
Down_Resto...	Down_Hotel1	pkt_Resto	512k	5M	0 bps	0 B	0 B
Down_VoIP_...	Down_Hotel1	pkt_VoIP	1M	5M	0 bps	0 B	0 B
Down_Hotel2	Down_Admin	pkt_Hotel2		5M	0 bps	0 B	0 B
Down_Email...	Down_Hotel2	pkt_Email	2M	5M	0 bps	0 B	0 B
Down_HTTP...	Down_Hotel2	pkt_HTTP	1536k	5M	0 bps	0 B	0 B
Down_Resto...	Down_Hotel2	pkt_Resto	512k	5M	0 bps	0 B	0 B
Down_VoIP_...	Down_Hotel2	pkt_VoIP	1M	5M	0 bps	0 B	0 B
Down_Hotel3	Down_Admin	pkt_Hotel3		5M	0 bps	0 B	0 B
Down_Email...	Down_Hotel3	pkt_Email	2M	5M	0 bps	0 B	0 B
Down_HTTP...	Down_Hotel3	pkt_HTTP	1536k	5M	0 bps	0 B	0 B
Down_Resto...	Down_Hotel3	pkt_Resto	512k	5M	0 bps	0 B	0 B
Down_VoIP_...	Down_Hotel3	pkt_VoIP	1M	5M	0 bps	0 B	0 B
Down_Hotel4	Down_Admin	pkt_Hotel4		5M	0 bps	0 B	0 B
Down_Email...	Down_Hotel4	pkt_Email	2M	5M	0 bps	0 B	0 B
Down_HTTP...	Down_Hotel4	pkt_HTTP	1536k	5M	0 bps	0 B	0 B
Down_Resto...	Down_Hotel4	pkt_Resto	512k	5M	0 bps	0 B	0 B
Down_VoIP_...	Down_Hotel4	pkt_VoIP	1M	5M	0 bps	0 B	0 B

Tanto para el tráfico de bajada como para el de subida.

down_Huespedes	Down	pkt_Huespedes	61M	61M	0 bps	0 B	0 B
UP	*ether6*			81M	0 bps	0 B	0 B
UP_Admin	UP	pkt_Admin		20M	0 bps	0 B	0 B
UP_Hotel1	UP_Admin	pkt_Hotel1	5M	5M	0 bps	0 B	0 B
UP_Email_H1	UP_Hotel1	pkt_Email	2M	5M	0 bps	0 B	0 B
UP_HTTP_H1	UP_Hotel1	pkt_HTTP	1536k	5M	0 bps	0 B	0 B
UP_Resto_H1	UP_Hotel1	pkt_Resto	512k	5M	0 bps	0 B	0 B
UP_VoIP_H1	UP_Hotel1	pkt_VoIP	1M	5M	0 bps	0 B	0 B
UP_Hotel2	UP_Admin	pkt_Hotel2	5M	5M	0 bps	0 B	0 B
UP_Email_H2	UP_Hotel2	pkt_Email	2M	5M	0 bps	0 B	0 B
UP_HTTP_H2	UP_Hotel2	pkt_HTTP	1536k	5M	0 bps	0 B	0 B
UP_Resto_H2	UP_Hotel2	pkt_Resto	512k	5M	0 bps	0 B	0 B
UP_VoIP_H2	UP_Hotel2	pkt_VoIP	1M	5M	0 bps	0 B	0 B
UP_Hotel3	UP_Admin	pkt_Hotel3	5M	5M	0 bps	0 B	0 B
UP_Email_H3	UP_Hotel3	pkt_Email	2M	5M	0 bps	0 B	0 B
UP_HTTP_H3	UP_Hotel3	pkt_HTTP	1536k	5M	0 bps	0 B	0 B
UP_Resto_H3	UP_Hotel3	pkt_Resto	512k	5M	0 bps	0 B	0 B
UP_VoIP_H3	UP_Hotel3	pkt_VoIP	1M	5M	0 bps	0 B	0 B
UP_Hotel4	UP_Admin	pkt_Hotel4	5M	5M	0 bps	0 B	0 B
UP_Email_H4	UP_Hotel4	pkt_Email	2M	5M	0 bps	0 B	0 B

Con este análisis presentado nos podemos dar cuenta que con la implementación del nuevo equipo y las configuraciones realizadas tenemos un óptimo funcionamiento de nuestra red ya que superamos los problemas anteriormente expuestos.

Anexo B - Cotizaciones del Equipo utilizado en el Diseño

➔ http://routerboard.com/RB2011iLS-IN

Details	
Product code	RB2011iLS-IN
CPU nominal frequency	600 MHz
SFP DDMI	Yes
CPU core count	1
Size of RAM	64 MB
Architecture	MIPS-BE
10/100 Ethernet ports	5
10/100/1000 Ethernet ports	5
MiniPCI slots	0
MiniPCI-e slots	0
Wireless standards	802.11
Number of USB ports	0
Power Jack	1
Supported input voltage	8 V - 30 V
PoE in	Yes
PoE out	Yes
Voltage Monitor	No
CPU temperature monitor	No
PCB temperature monitor	No
Dimensions	214mmx86mm
Operating System	RouterOS
Operating temperature range	-35C to +65C
License level	4
Antenna gain DBI	No
Current Monitor	No
CPU	AR9344-DC3A-R
Max Power consumption	6W
SFP ports	1
SFP+ ports	0
Number of chains	0
Serial port	None
Suggested price	$109.00

El precio que se especifica en la tabla corresponde al de la compañía Latvian, aquí en Ecuador el precio seria $152,60 ya que se suma el 40% por cargos de envío.

➔ https://www.ubnt.com/edgemax/edgerouter-lite/

From: kcevallos@enlacedigital.com.ec
To: johan_8477@hotmail.com
Subject: COTIZACIÓN
Date: Wed, 8 Jul 2015 10:56:45 -0500

ESTIMADA,

Según su requerimiento los más cercano a lo que usted necesita tengo el UBQ-ERLITE-3 que está en 49+iva precio de promo, le puede revisar las especificaciones en el siguiente link: https://www.ubnt.com/edgemax/edgerouter-lite/

Quedo atenta a sus gentiles comentarios,

Saludos cordiales,

enlacedigital

Karen Cevallos
Asesora Comercial
CONSUMER

0985 516 147

Telfs.: 2455 432 - 2452 886 - 2463 842 2463 522 - 2463 523 **Ext. 202**

Francisco de Izázaga N45-07 y Pío Valdivieso, Sect. El Inca, Quito – Ecuador

	ERLite-3
Performance	1 million pps
Gigabit RJ45 Ports	3
SFP Ports	N/A
PoE	N/A

➔ http://www.academyxperts.com/

academy xperts

NETWORK XPERTS S.A. NEXE
RUC: 0992450029001

Cotización # 150428-01
Producto: EQUIPOS

Info

Customer : Johanna Alvarez
Contact : Johanna Alvarez
Address : Av. Francisco de Orellana y Alberto Borges, Edificio Centrum, Piso 13, Ofic. 1
Email: jrosado@sercoel.com
Phone : 042634235 ext 141

Date : 01/jul/2015
Rep. : GES
RUC:

Cant.	Detalle	Precio U.	Precio Total
	Puntos de Acceso Inalámbrico		
1	RB2011iLS-IN	$168,95	$168,95
	Desktop metal case, 5xEthernet, 5xGigabit Ethernet, SFP cage, PoE out on port 10, 600MHz CPU, 64MB RAM, RouterOS L4		
	* Los valores de velocidad y cobertura se basan en ambientes óptimos y pueden variar		
		Sub-Total	$168,95
		IVA 12%	$20,27
		TOTAL	$189,22

Condiciones

- Esta propuesta es válda por 5 días
- Forma de Pago: 70% a la firma de la orden de compra, 30% a la entrega y configuración de equipos

Guisela Espinoza

Guisela Espinoza F.
Gerente Administrativa
gigie@academyxperts.com

sequreISP 3.0 WildPackets MikroTik iboss UBIQUITI

Guayaquil - Ecuador
www.academyxperts.com
cursos@academyxperts.com

Edif. Professional Center, Piso 5, Ofic. 507
Celular: +593 9 9535 2133
PBX: +593 4 600 8590

➔ http://wni.mx/index.php?page=shop.product_details&flypage=flypage_new.tpl&product_id=433&category_id=41&keyword=Router+RB2011&option=com_virtuemart&Itemid=53

Ruteador Multipuertos Giga/Fast Ethernet con salida PoE

Ver imagen grande

Mikrotik RB2011iL-IN

$99.00

¿TIENE DUDAS ACERCA DE ESTE PRODUCTO?

Los nuevos Routers de la serie RB2011, tienen una letra "i" en el identificador de producto. Esto hace referencia a "inyector", que significa que uno de los puertos LAN (Ethernet #10) ahora cuenta con la función de salida PoE (Power over Ethernet). De esta forma es posible alimentar a otros dispositivos compatibles con la tecnología PoE que manejen el mismo voltaje. La carga máxima en el puerto es de 500mA a 24V para 12W.
El Mikrotik RB2011 es una serie de productos multi-puerto de precio costeable. Diseñada para uso en interiores, disponible con diferentes gabinetes metálicos y una multitud de opciones.
El RB2011iL-IN es el modelo básico, con cinco puertos Gigabit Ethernet y cinco puertos Fast Ethernet, puerto de alimentación y soporte PoE.
Internamente es impulsado por el nuevo procesador de red Atheros de próxima generación a 600MHz 74K MIPS con 64MB de RAM y licencia RouterOS nivel 4.

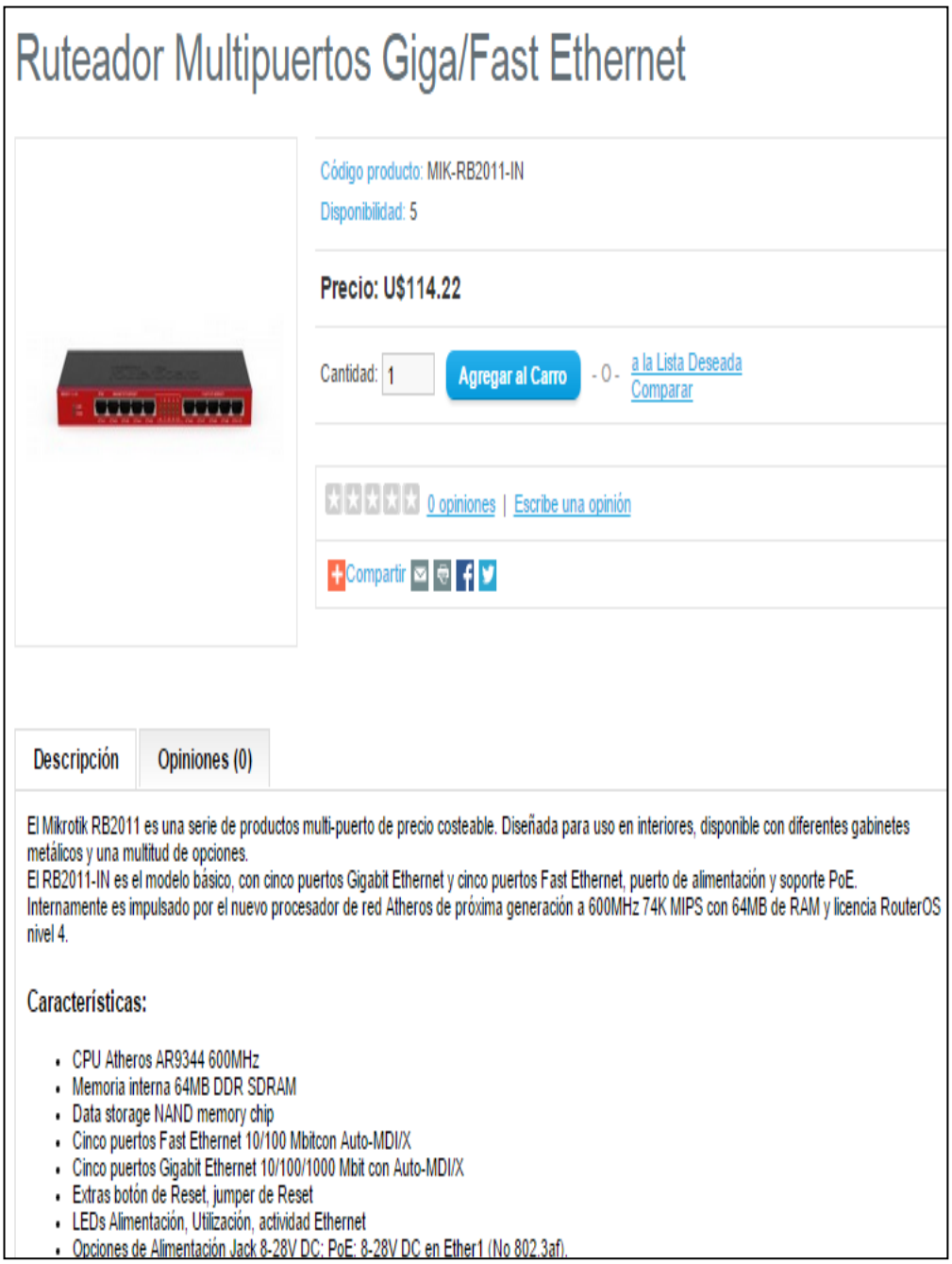
¡Menos adaptadores de alimentación y cables de qué preocuparse!

El Paquete incluye RB2011iL, gabinete para interiores y fuente de alimentación.

Características

Modelo	RB2011iL-IN
CPU	Atheros AR9344 600 MHz
Memoria RAM	64 MB DDR2 SDRAM
Ethernet	5 Puertos Fast Ethernet 10/100 Mbit/s con Auto-MDI/X 5 Puertos Gigabit Ethernet 10/100/1000 Mbit/s con Auto-MDI/X
Extras	Botón de Reset, jumper de Reset
LEDs	Led de encendido Led del puertos Ethernet Led de alimentación
Energía de entrada	PoE 8-30V en Ether1 (no 802.3af) Adaptador eléctrico de 24 Volts

➔ http://mubu.com.mx/index.php?route=product/product&path=89_93&product_id=206



Ruteador Multipuertos Giga/Fast Ethernet

Código producto: MIK-RB2011-IN

Disponibilidad: 5

Precio: U$114.22

Cantidad: 1 Agregar al Carro - O - a la Lista Deseada Comparar

0 opiniones | Escribe una opinión

Compartir

Descripción | Opiniones (0)

El Mikrotik RB2011 es una serie de productos multi-puerto de precio costeable. Diseñada para uso en interiores, disponible con diferentes gabinetes metálicos y una multitud de opciones.
El RB2011-IN es el modelo básico, con cinco puertos Gigabit Ethernet y cinco puertos Fast Ethernet, puerto de alimentación y soporte PoE.
Internamente es impulsado por el nuevo procesador de red Atheros de próxima generación a 600MHz 74K MIPS con 64MB de RAM y licencia RouterOS nivel 4.

Características:

- CPU Atheros AR9344 600MHz
- Memoria interna 64MB DDR SDRAM
- Data storage NAND memory chip
- Cinco puertos Fast Ethernet 10/100 Mbitcon Auto-MDI/X
- Cinco puertos Gigabit Ethernet 10/100/1000 Mbit con Auto-MDI/X
- Extras botón de Reset, jumper de Reset
- LEDs Alimentación, Utilización, actividad Ethernet
- Opciones de Alimentación Jack 8-28V DC; PoE: 8-28V DC en Ether1 (No 802.3af).

GLOSARIO

Frame Relay. Es una red de conmutación de paquetes que envía paquetes de longitud variable sobre Lan's o Wan's. Los paquetes de longitud variable, o tramas, son paquetes de datos que contiene información de direccionamiento adicional y gestión de errores necesaria para su distribución.

802.1 p. Estándar IEEE que proporciona priorización de tráfico y filtrado multicast dinámico. Proporciona un mecanismo para implementar QoS a nivel de MAC.

IPv4. Protocolo de Internet de capa 3 que utiliza 4 octetos (255.255.255.255.).

IPv6. Protocolo de Internet versión 6, es el encargado de dirigir y encaminar los paquetes en la red.

RFC 2474. Definición del campo DS en los encabezados IPv4 e IPv6.

RFC 2475. Una arquitectura para servicio diferenciado.

SLA17. Es un acuerdo de niveles de servicio que se firma entre el proveedor y el cliente.

DSCP. Hace referencia al segundo byte en la cabecera de los paquetes IP que se utiliza para diferenciar la calidad en la comunicación que quieren los datos que se transportan.

CIR. Es la tasa que se compromete el proveedor en entregar al cliente.

SNA. Conjunto de protocolos de comunicaciones para manejo de redes.

Leaky bucket. Algoritmo utilizado para controlar la tasa en la cual los datos son inyectados dentro de una red. Utiliza las siguientes especificaciones:

considerar una cubeta con un hueco en el fondo; si los paquetes arriban son ubicados dentro de la cubeta, si la cubeta está llena estos son descartados; los paquetes en la cubeta son enviados con una tasa constante, equivalente al tamaño del hueco en esta.

CRC. Es un mecanismo de detección de errores en sistemas digitales.

MAC. Es un identificador de 48 bits (6 bloques hexadecimales) que corresponde de forma única a una Ethernet de red.

HotSpot. El Mikrotik HotSpot Gateway proporciona autenticación para los clientes antes de acceder a las redes públicas.

ABREVIATURAS

ARP	Protocolo de Resolución de Direcciones	Address Resolution Protocol
ATM	Modo de Transferencia Asíncrona	Asynchronous Transfer Mode
DHCP	Protocolo de Configuración Dinámica de Host	Dynamic Host Configuration Protocol
FTP	Protocolo de Transferencia de Archivos	File Transfer Protocol
IEC	Comisión Electrotécnica Internacional	International Electrotechnical Commission
IETF	Grupo de Trabajo de Ingeniería de Internet	Internet Engineering Task Force
ISO	Organización Internacional de Normalización	International Organization for Standardization
LAN	Red de Área Local	Local Area Network
MTU	Unidad Máxima de Transferencia	Maximum Transfer Unit
PSTN	Red Telefónica Publica Conmutada	Public Switched Telephone Network
SMTP	Protocolo de Transferencia de Correo	Simple Mail Transfer Protocol

ABREVIATURAS

TCP	Protocolo de Control de Transmisión	Transmission Control Protocol
UDP	Protocolo de Datagrama de Usuario	User Datagram Protocol
VoIP	Voz sobre Protocolo de Internet	Voice Over IP
WAN	Red de Área Amplia	Wide Area Network

BIBLIOGRAFÍA

[1] C. F. Vaca. “Estudio de VoIP en Redes Privadas”, Tesis Pregrado, Dpto. Ing., en Ciencias Aplicadas, Univ. Técnica del Norte, Ecuador, 2011.

[2] M. Saldaña. (2010, Noviembre 16). Calidad de Servicio en Redes IP [Online]. Disponible en: http://www.monografias.com/trabajos82/calidad-servicios-redes-ip/calidad-servicios-redes-ip.shtml.

[3] O. Gerometta. (2010, Agosto 30). Modelos de Implementación de QoS [Online]. Disponible en: http://librosnetworking.blogspot.com/2010/08/modelos-de-implementacion-de-qos.html.

[4] U. Sevilla. (2012, Noviembre 01). Gestión de Trafico – Calidad de Servicio QoS [Online]. Disponible en: http://www.dte.us.es/docencia/etsii/gii-ti/tecnologias-avanzadas-de-la-informacion/curso-2012-13/Tema3%20-%20QoS.pdf.

[5] G. Melo. (2012, Julio 05). Networking IP to IP [Online]. Disponible en: http://blog-ip.blogspot.com/2012/07/pbr.html.

[6] S. Daza. (2011, Febrero 12). Conformación del Trafico [Online]. Disponible en: https://electrotelematica.wordpress.com/2011/02/12/conformacion-del-trafico-traffic-shaping/.

[7] O. Gerometta. (2010, Enero 22). Control del Tráfico no Deseado utilizando CAR [Online]. Disponible en: http://librosnetworking.blogspot.com/2007/01/control-del-trfico-no-deseado.html.

[8] S. Álvarez, “Estudio y Configuración de Calidad de Servicio para Protocolos IP v4 e IP v6 en una red de Fibra Óptica WDM”. Tesis de Maestría, Fac. Ingeniería, Univ. Tarapacá, Chile, 2010.

[9] F. Novoa. (2014, Diciembre 11). QoS en Redes Corporativas [Online]. Disponible en: http://es.slideshare.net/FranciscoNvoaManuel/qos-en-redes-corporativas.

[10] Cisco (2015, Agosto 13). Como trabaja el RADIUS? [Online]. Disponible en: http://www.cisco.com/cisco/web/support/LA/102/1024/1024966_32.pdf.

[11] Mikrotik (2011, Julio 19). Mikrotik RouterOS Preguntas Frecuentes [Online]. Disponible en: http://wiki.mikrotik.com/wiki/Tutorials_in_spanish_language.

[12] R. Anrrango. (2012, Agosto 31). Conociendo la Interfaz de Winbox, el Software RouterOS [Online]. Disponible en: http://configurarmikrotikwireless.com/blog/interfaz-winbox-software-routeros.html.