UNIVERSIDAD POLITÉCNICA SALESIANA

SEDE CUENCA

CARRERA DE INGENIERÍA DE SISTEMAS

Tesis previa a la obtención del Título de:

Ingeniero de Sistemas

TÍTULO DEL TEMA:

"Estudio e implementación de la nueva arquitectura física y lógica de la red de datos, servicios utilizando RouterOS y tecnologías Open Source de bajo costo, integradas a un sistema de administración Web para control de abonados y gestión de planes de Internet para el proveedor de Servicios de Internet Inalámbricos Sigsignet."

AUTORES:

Denys Marcelo Siguenza Suscal.

Jorge Patricio Jiménez Pesantez.

DIRECTOR:

Ing. Wilson Quintuña.

Cuenca, Julio 2014

DECLARACIÓN DE RESPONSABILIDAD

El trabajo de grado que presentamos, es original y basado en el proceso de investigación y/o adaptación tecnológica establecido en la Carrera de Ingeniería de Sistemas de la Universidad Politécnica Salesiana. En tal virtud los fundamentos técnicos – científicos y los resultados son exclusiva responsabilidad de los autores

A través de la presente declaración cedemos los derechos de propiedad intelectual correspondiente a este trabajo, a la Universidad Politécnica Salesiana, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la Normativa Institucional Vigente.

Cuenca, 18 de Julio del 2014

Denys Marcelo Siguenza Suscal.

AUTOR

Jorge Patricio Jiménez Pesantez.

AUTOR

Wilson Quintuña, Director de la Tesis,

CERTIFICA

El presente trabajo de tesis previo a la obtención del título de Ingeniero de Sistemas fue desarrollado bajo todos los reglamentos estipulados por la Universidad Politécnica Salesiana y ha cumplido con los requerimientos para su aprobación.

Ing. Wilson Quintuña

DIRECTOR DE TESIS

DEDICATORIA.

El fruto de este trabajo está enteramente dedicado en primera instancia para mis padres y hermanos, apoyo incondicional para lograr esta meta; además a mi amigos, profesores y en especial a la memoria de mi abuelito Julio Siguenza quien con sus sabias enseñanzas fueron mi mayor motivación para lograr todos mis objetivos y metas planteadas.

Denys Marcelo Siguenza Suscal.

DEDICATORIA.

Quiero hacer extenso mi más sincero agradecimiento al Ing. Wilson Quintuña quien muy desinteresadamente nos guió y acompañó en el desarrollo de esta tesis, al igual que al Ing. Marco Carpio ya que gracias a su constante apoyo nos motivó para la realización de este proyecto. También a mi madre Gloria Pesántez quién incondicionalmente estuvo apoyándome a lo largo de mi camino de preparación, a mi esposa y a mis tíos que siempre estuvieron para darme una mano y levantarme de mis innumerables caídas y sobre todo a Dios porque sin su bendición nada sería posible.

Jorge Jiménez.

AGRADECIMIENTOS.

De manera muy especial, nuestro más sincero agradecimiento al Ing. Marco Carpio e Ing. Wilson Quintuña por sus grandes contribuciones guías y enseñanzas para nuestra superación personal, y para que este trabajo y otras metas se vuelvan realidad, a todos nuestros profesores que en el camino nos han inculcado buenas enseñanzas, a nuestro Dios todo poderoso porque sin él no fuéramos capaces de haber obtenido dicho logro y la satisfacción de una meta cumplida.

JORGE & DENYS

ÍNDICE

CONTENIDOS **PÁG**

ÍNDICE DE FIGURAS

CONTENIDO **PÁG**

ÍNDICE DE TABLAS

CONTENIDOS **PÁG**

INTRODUCCIÓN

La imperiosa necesidad hoy en día de estar "Conectados", la llegada de la Web 2.0 y la multitud de servicios que hoy en día se están potenciando por la "Gran red", ha cambiado mucho el estilo de vida e incluso la forma en cómo se relacionan con las personas ya que muchas actividades de negocio, estudio, conocimiento, trabajo e incluso ocio y entretenimiento se han mudado para buscar lugar en la nube; ante tal situación los medios antiguamente disponibles que brindaban acceso a Internet como las tradicionales dial-UP se están quedado un tanto cortas por los elevados anchos de banda que no solo las empresa requieren sino ahora los hogares así lo demandan, y porque no decirlo la Web 2.0 para brindar sus servicios de manera óptima lo requiere así, por ende muchos proveedores de acceso a Internet han optado por medios alternos que permitan llevar a la red al siguiente nivel y poder así incrementar su capacidad de acceso a muchas más personas; por ende hoy en día escuchar hablar de medios tales como la fibra óptica, fibra aérea, cable coaxial, power line y otros términos relacionados son y serán los encargados de dar conectividad no solo a empresas sino a hogares.

Con la evolución de tecnología, en la actualidad muchas empresas dedicadas a brindar "Conectividad" han visto un amplio mercado en cuanto a las comunicaciones inalámbricas se refiere y a posibilitar el acceso mediante dicho medio en donde prácticamente una red cableada no tiene posibilidad de llegar refiriéndose con ello a zonas rurales en específico, debido a esto en estos últimos años han nacido muchos ISP ahora llamados WISP (Wireless Internet Service Provider) "Proveedor de servicios de Internet Inalámbricos", al incrementarse la demanda en lugares como: Comunidades, Parroquias, Cantones y zonas rurales en sí que consideradas desde el punto de vista de negocio, como áreas en potencial crecimiento y sumando a ello las ventajas de la tecnología Wireless en las que destaca su flexibilidad para ser implementada, escasa saturación del espectro de frecuencias en dichas zonas y costos asequibles de instalación, han hecho que este medio se expanda abrumadoramente a tal punto que hoy en día está siendo ampliamente usada incluso en zonas antes no pensadas como son las Ciudades en si o zonas urbanas en donde ha adquirido un apelativo denominado "Fibra Aérea" debido a su capacidad del medio

para transmitir elevados anchos de banda incluso a nivel de una red cableada; pero no todo se pinta de color rosa desde el punto de vista lógico, y que pueden dar un gran dolor de cabeza a un administrador de red; se debe a que generalmente muchas de estas empresas en sus inicios al no disponer de altos capitales y un extenso conocimiento en el área optan generalmente por tecnologías de bajo coste e incluso gratuitas, y más que eso la escasa planificación que se realiza y los pocos conocimientos sobre la funcionalidad y la forma emperica que se usa para la gestión y administración del mismo son causales iniciales para que más tarde este tipo de negocios tiendan a divisar un rotundo fracaso.

Quizá el santo grial de este tipo de empresas al iniciar con pocos recursos es conjugar soluciones fiables hablando desde un punto de vista técnico con un proceso de planificación y expansión detallado. A lo largo de estos años muchas empresas se ha posesionado como líderes en proveer soluciones al área del Networking, redes de datos y en si a los WISP como es el caso del Cisco por mencionar una de ellas, soluciones altamente fiables pero que como recursos iniciales a ser implementados tienden a ser muy costos, en cambio optar por tecnología Open Source se puede considerar como una opción que conlleva un riesgo implícitamente de poder acertar o fallar y que tarde o temprano puede representar un costo inclusive mucho más alto, es así que surge la presente de realizar un proceso de estudio de la red actual de proveedor Sigsignet cuyos servicios presentes se han implementado bajo tecnología Open Source y que en los últimos años la misma experimentando un crecimiento exponencial muy grande a tal punto que se requiere la implementación de Hardware dedicado y una restructuración de la red tanto a nivel físico como lógico para poder aumentar la capacidad no solo de forma local como es el cantón Sigsig sino a lugares aledaños y mejorar la condición de la misma posibilitándola así se puedan implementar nuevos servicios, una mejor calidad de servicio, seguridad etc., con el objetivo de que dicha empresa pueda seguir brindando un servicio eficaz y eficiente como lo ha venido haciendo desde hace algunos años atrás, en dicho proceso se considera también la integración de dichas soluciones dedicadas basadas en RouterOS (Un potente sistema operativo de red desarrollado por MikroTik que está teniendo gran auge por su alta flexibilidad, disponibilidad de servicios y una relación beneficio/costo muy alto) con un sistema externo implementado en Java, que pueda comunicarse con dichos dispositivos en tiempo real sin un intermediario de por

medio y llevar un control de abonados y gestión de planes de Internet de forma eficiente en esta etapa inicial.

CAPÍTULO I: INFORMACIÓN Estratégica de la Empresa

Objetivos:

- Conocer la estructura lógica y física de la empresa Sigsignet así como su orientación, misión visión y Objetivos.

Objetivos Específicos:

- Encontrar las problemáticas, deficiencias y fortalezas de la empresa.
- Estudiar y analizar la estructura organizacional de la empresa Sigsignet.
- Conocer la estructura y organización de la empresa Sigsignet.

1.1 Historia

Sigsignet es un proveedor de servicios de Internet Inalámbricos nacido allá por el año de 1998, se caracteriza por brindar un servicio ágil y eficiente dentro del cantón Sígsig, operando sobre el mismo de manera legal. El enfoque de Sigsignet es brindar un servicio personalizado y con tecnología de punta, que le permita al subscriptor conectarse a Internet rápidamente, sin demoras y de manera ininterrumpida, además dando un soporte inmediato sin demoras ni inconvenientes. Siendo el mercado objetivo los hogares, estudiantes, pequeñas y medianas empresas y todos aquellos que deseen pertenecer a una red de servicio personalizada y con altos estándares de servicio al cliente.

1.2 Misión

Facilitar el acceso a la información, impulsando el uso de las tecnologías de la comunicación, proveer servicios integrales de telecomunicaciones con recursos humanos calificados, contribuir con el crecimiento de clientes y colaboradores.

1.3 Visión

Ser el mejor proveedor de servicios de internet de los cantones orientales en cuanto a asistencia técnica hacia los clientes como en calidad de servicio (QoS) con alto grado de compromiso social.

1.4 Objetivo de la Empresa

- Sigsignet es una empresa joven que provee servicios de internet de manera inalámbrica al cantón Sígsig así como a sectores y parroquias aledañas que estén dentro del rango de cobertura, con una excelente competitividad dentro del mercado tecnológico, para así lograr expandirse a diferentes cantones donde se vea la necesidad de brindar un mejor servicio.

1.5 Estructura de la empresa.

Sigsignet es una empresa que trabaja con un personal capacitado constantemente, por brindar un servicio eficiente y de calidad, su organigrama se centra de la siguiente forma, todas entidades subalternas como la Gerencia General, Presidente y Representante Legal se rigen a la Junta General de Accionistas.

Dentro de la institución existen los siguientes departamentos:

- Departamento Networking: Encargado de brindar conectividad, soporte a la red de datos, administración del direccionamiento IP, calidad de servicio, segmentación de ancho de Banda, Firewall y tareas afines.

- Departamento Soporte & Asistencia al Cliente: Encargado de brindar asistencia y soporte básico o primer nivel al cliente, ante eventuales inconvenientes que puedan surgir con el servicio o relacionados.

- Departamento Ventas & Marketing: Encargado de la venta de productos y servicios de la empresa así como el manejo de publicidad y la imagen de la empresa.

- Departamento Financiero.- Encarga de manejar toda la parte contable y finanzas de la empresa, así como la asignación de presupuestos para la implementación

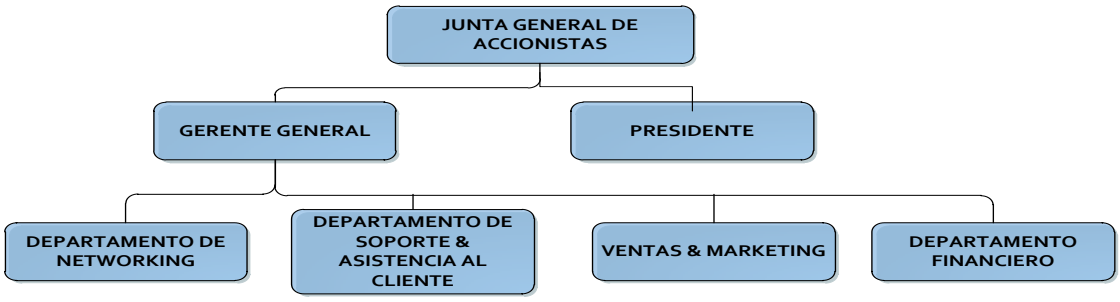


Figura 1.1. Organigrama de la Empresa Sigsignet.

Fuente: Sigsignet, Proveedores de Servicio de Internet 2013.

1.6 Productos y Servicios

Sigsignet cuenta hoy en día con un amplio catálogo de productos y servicios, todos los planes de Internet por el momento están disponibles solo para cantones aledaños al Sígsig, sin embargo en cuanto a sus servicios se ofertan a nivel nacional, el soporte y la asesoría en Radio Enlaces actualmente es uno de sus fuertes ya que cuentan con personal calificado y certificado en dicho ámbito, así como la consultaría a proveedores de Servicios de Internet Inalámbricos.

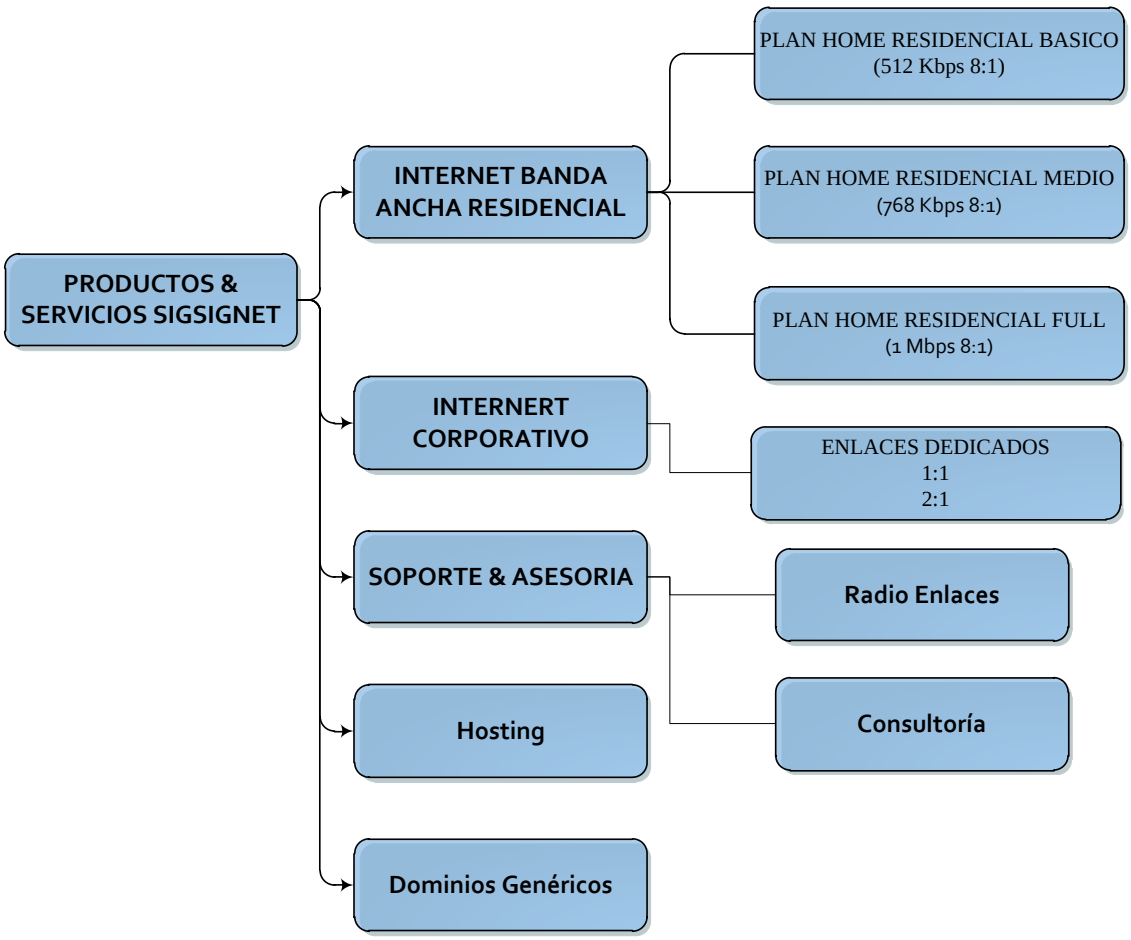


Figura 1.2. Productos y Servicios de la Empresa Sigsignet.

Fuente: Sigsignet, Proveedores de Servicio de Internet, 2013.

Conclusiones del Capítulo I

Culminado el Primer Capítulo, claramente se ha identificado la estructura de la empresa, además la variedad de productos y servicios comercializados por Sigsignet, ello es un pilar fundamental en cualquier proceso de reingeniería ya que generalmente cuando se intenta reestructurar sus servicios en el caso de empresas de este tipo cuyo producto es un bien intangible, se puede dar el caso de que los mismos de cierta forma se vean afectados, por tal razón su importancia en conocer de cierta forma su organización.

CAPÍTULO II: FUNDAMENTOS TEORICOS.

Objetivos:

- Entender los fundamentos teóricos básicos acerca de Networking y RouterOS necesarios para la realización del estudio y posterior implementación.

Objetivos Específicos:

- Comprender los modelos de referencia TCP/IP y OSI junto con los principales protocolos de red existentes.
- Diferenciar el Hardware y Equipamiento necesario en una infraestructura de un WISP.
- Conocer RouterOS, características generales, modelos de licenciamiento y servicios disponibles.

2.1. NORMAS, PROTOCOLOS

Dentro del uso de sistemas informáticos y las redes de Datos o Networking es y ha sido necesario siempre el uso de normas y protocolos con el fin de buscar siempre la interoperabilidad, evitando el caos por el constante surgimiento de nuevas tecnologías en la cual cada una imponía su normas y protocolos es aquí que el uso correcto de las mismas y su conocimiento se ha vuelto tan esencial no solo para entender su funcionamiento sino como está estructurada muchos aspectos de la Internet y las redes de datos en sí.

Una norma o estándar puede contener una especificación que reglamenta procesos y productos que garantizan la interoperabilidad o reglamentan mediante una directriz un determinado grupo de actividades[1], en tanto un protocolo se puede entender como un conjunto de normas o estándares que permiten el intercambio de información a través de un medio[2] como en el caso de las Redes de datos; sin estos dos prácticamente una comunicación adecuada y el intercambio de información seria defectuoso por no decir nulo entre diferentes sistemas.

Por ende aplicar el uso de normas, protocolos y más que nada entenderlos tiene gran relevancia en el desarrollo y la implementación de sistemas.

2.1.1 PILA DE PROTOCOLOS

Se entienden como un conjunto de reglas definidas y organizadas en mutuo acuerdo entre los diversos participantes de una comunicación definidos en una jerarquía que trabajan juntos para llevar a cabo la transmisión de datos ente dos nodos de red o de los participantes.[3] Cabe mencionar la analogía que tiene un alto parecido a la carrera de relevos, pero en vez de pasar un testigo, lo que se realiza es transmitir paquetes de

[1] equipoteccelaya, Norma, Estándar, Modelo, 07 de Febrero del 2009, http://equipoteccelaya.blogspot.es/1234029360/norma-est-ndar-modelo/
[2] WordReference, protocolo-Definición, 3 de Septiembre del 2013, http://www.wordreference.com/definicion/protocolo
[3] Victor Dominguez Caraballo, PILA DE PROTOCOLOS TCP/IP, p 3-12

datos entre un protocolo a otro, de forma adecuada y solventando cualquier error entre cada una de las capas, evitando así duplicidad o perdida de información.

2.1.1.1 MODELO DE REFERENCIA OSI

Se lo considera como un modelo de referencia netamente con fines educativos no así como TCP/IP que se encarga de describir como está establecida la Internet y sus fundamentos en sí, el estudio de dicho modelo arranco por el año de 1984 a cargo de la Organización Internacional de Estandarización (ISO), en dicho modelo se plantea un concepto en base a capas especificando determinados protocolos que se distribuyen en cada una de las capas. Las capas son completamente independientes y en si el uso del modelo es empleado para en la detección de errores y transferencia de datos.

Para una mejor compresión se describe a continuación la estructura de las 7 capas en las cuales se encuentra divido el modelo OSI describiendo teóricamente como funciona cada una de ellas dentro del proceso de transmisión de datos dentro de una red:

Capa	Descripción
Aplicación	Proporciona los servicios utilizados por las aplicaciones para que en si todos los usuarios se comuniquen a través de la red, tales como transporte de correo electrónico, acceso archivos remotos, Directorios, Tareas remotas etc., por ende es aquí inclusive donde se especifican los tan hoy conocidos API que no son nada más que un conjunto de reglas que permiten que las aplicaciones creadas por los usuarios puedan acceder a los servicios de un sistema de Software.[4]
Presentación	Esta capa es la responsable de presentar los datos a la capa de aplicación, en determinados casos la capa de presentación es capaz de traducir datos de un formato a otro y así se utilicen los formatos

[4] ALARCON HERRERA, ERIKA; CROVETTO HUERTA, CHRISTIAN, Redes de Computadoras y Conectividad, Editorial Megabyte, 20 de Diciembre del 2004, p. 193.

	adecuados (semántica y la sintaxis) para su transmisión. Otras funciones que se delegan a dicha capa son: **Compresión/Descompresión.-** Restar o agregar la cantidad de bits a ser transmitidos. **Encriptación/Desencriptación.-**Especificar un nuevo formato a un mensaje con la finalidad de mantener la privacidad del mismo. **Traducción.-**En el origen la información es cambiada para que la misma sea interpretada por el ordenador, y de igual forma al llegar al destino dicho mensaje sea presentado como el original.
Sesión	En esta capa se encarga de establecer el enlace de comunicación entre un origen y un destino, utilizando mecanismos que permitan controlar que el dialogo y las actividades sean a nivel de aplicación, dicha comunicación puede producirse en tres modos de dialogo. **Simple (Simplex).-** Este modo de dialogo especifica que un nodo origen transmite de manera y el otro lo recibe de igual forma. **Semiduplex (Half-Duplex).-** Aquí se especifica que un solo nodo puede transmitir en un momento dado, y los demás se turnan para transmitir. **Duplex Total(Full Duplex).-** Aquí todos los nodos o emisores y receptores pude transmitir y recibir simultáneamente , generalmente este tipo de comunicación suele requerir de un control de flujo que determine que ninguno de los demás dispositivos participantes envié datos a mayor velocidad que el otro dispositivo pueda recibir Cada sesión mantiene 3 fases que son: **Establecer la conexión:** Negocian reglas de comunicación. **Transferencia de Datos.** Inician un dialogo para intercambiar datos.

	Liberación de la conexión. Cuando los nodos no necesitan seguir comunicados.
Transporte	Se encarga de efectuar el transporte de la data ubicados dentro del paquete, además que llegue tal y como fue entregado por el receptor. Dentro de esta capa las unidades de información se denominan Segmento o Datagrama dependiendo si corresponde a TCP o UDP, respectivamente protocolos orientados a conexión y el otro sin conexión, además en esta capa se especifican las siguientes funciones: **Control de Errores:** Permite que el mensaje llegue desde el origen al destino sin perdidas, daños o duplicaciones, efectuándolo end to end. **Control de Flujo:** Evita el desbordamiento de paquetes. **Segmentación:** Aquí el mensaje es dividido en varios segmentos cada uno con su respectivo identificativo o numeración, permitiéndole más tarde que el mensaje al llegar al destino sea unificado correctamente, teniendo presente que dicho capa maneja un control de errores en el caso de paquetes se extravíen durante el camino, se ejecute una petición de reenvió al origen. **Identificación de Aplicaciones:** Es necesario para poder transferir todos los flujos de datos a las aplicaciones adecuadas, la capa de transporte necesariamente debe asignar un identificador a la aplicación como un puerto.
Red	La capa de red cuya actividad principal es llevar los paquetes desde el origen a su respectivo destino proporcionándoles un trato independiente entre cada uno de ellos, a través del empleo de dispositivos de conexión y siguiendo una dirección adecuada por medio de Internet, dentro de esta capa las unidades de información como se lo menciono anteriormente se denominan paquetes y especifican los siguientes subniveles:

	Enrutamiento: Permite que los paquetes en camino lleguen al destino final por medio de la utilización de dispositivos de enrutamiento. **Direccionamiento:** Aquí se agrega un campo nuevo al paquete en a dicho campo se le incluye la dirección lógica de origen y destino.
Enlace de Datos	Encargada de desplazar las tramas de manera ordenada por el enlace físico de comunicación hasta el nodo receptor, convirtiendo a la capa física en un medio fiable libre de cualquier error, en la misma las funciones especificadas de la capa de enlace de datos son: - **Tramado:** Definir tramas, utilizando los bits recibidos y dividiéndolos. - **Control de Acceso al Medio:** Indica cuál de los dispositivos participantes en la comunicación tiene el control de la transmisión. - **Control de Flujo:** Evita el desbordamiento de paquetes del lado del receptor, de forma que entre el emisor y receptor dichos paquetes viajen a una misma velocidad. - **Control de Errores:** Se utiliza en caso de tramas defectuosas o extravió de algunas de ellas, volviéndolas necesariamente a ser retransmitidas, también es utilizada para el control de duplicidad de tramas por medio de técnicas de detección y corrección.
Físico	Es la capa que actúa a nivel más bajo de la comunicación y comprende aspectos físicos de la red (es decir, cables, hubs, y demás dispositivos que comprenden el entorno físico de la red), por medio de esta se establece los métodos necesarios para la transmisión de datos a través de un medio físico, especificando dos casos en una transmisión: - **Codificación.-** Convertir impulsos eléctricos en paquetes.

	- **Decodificación.-** Convertir información binaria o paquetes en impulsos eléctricos.

Tabla 2.1. Modelo OSI y sus Capas.

Fuente: TEXTOS CIENTIFICOS, TCP/IP y el modelo OSI, 02 de Octubre de 2006.

Con dicho modelo de referencia se dispone de un marco de trabajo conceptual del que puede servirse cualquiera para comprender el funcionamiento de dispositivos de red complejos, como Conmutadores, Puentes e inclusive Routers.

Figura 2.1. Modelo de Referencia OSI

Fuente: UCOL, Modelo OSI, 07 de Junio de 2001
http://docente.ucol.mx/al008353/public_html/tarea2.htm

2.1.1.2 MODELO DE REFERENCIA TCP/IP

El modelo de referencia TCP/IP no se corresponde con el modelo OSI, el objetivo de TCP/IP es más que nada abarcar un determinado conjunto de protocolos de red en los que se basa la Internet, determinando un estándar que permita la comunicación origen-destino entre diferentes nodos u ordenadores, manteniendo más que nada la compatibilidad con cualquier variedad de Sistemas operativos y hardware en sí.

Todos los estándares de TCP/IP se publican a través de una serie de documentos denominados (RFC o Requests from comment) o solicitud de comentarios, teniendo por objetivo primordial proporcionar información o describir el estado de desarrollo.

TCP/IP especifica 4 niveles que son:

Capas	Descripción
Interfaz de Red.	Corresponde a los niveles físicos y enlace de Datos en el modelo OSI, es la encargada de comunicarse directamente con la Red, proporcionado la Interfaz entre la arquitectura de Red.
Internet.	Permite realizar el enrutamiento de paquetes entre diferentes caminos pertenecientes a la Internet.
Transporte.	La actividad principal de esta capa es intercambiar el mensaje de manera fiable, verificando la recepción de mensajes el orden de envió establecido por el emisor.
Aplicación.	Permite el uso de aplicaciones para que las mismas puedan ser empleadas por el usuario final.

Tabla 2.2. Modelo de Referencia TCP/IP y sus Capas.

Fuente: UCOL, Capas del Modelo TCP/IP, 07 de Junio de 2001, http://docente.ucol.mx/al008353/public_html/tarea2.htm,

Figura 2.2. Estructura del Modelo TCP/IP

Fuente: UCOL, Modelo TCP/IP, 07 de Junio de 2001 http://docente.ucol.mx/al008353/public_html/tarea2.htm,

2.1.2 HARDWARE DE RED Y EQUIPAMENTO PARA WISP

La variedad de alternativas existentes en Hardware de Red y Equipamiento para WISP hoy en día es tan diversificada, el cómo saber combinar dichas soluciones es quizá la parte más complicada que ello implica ya que generalmente las mejores y más costosas soluciones no son siempre las adecuadas en determinadas empresas depende mucho el análisis de ciertos parámetros de gran importancia como son: procesamiento, memoria Ram etc., teniendo siempre presente la relación beneficio/costo para poder determinar que una solución sea lo más eficaz posible, y que se pueda acoplar a las necesidades actuales de la empresa, sin que ello implique necesariamente un alto valor de inversión.

Muchos son los dispositivos de red necesarios para mantener una red de datos completamente operativa y proveer la comunicación entre los dispositivos de usuario final y el NOC con un alto porcentaje de disponibilidad tales como firewall, routers, switch etc., permitiendo a la misma ofertar una conexión pura, segura e ininterrumpida hacia internet, por ende la importancia de acertar con las soluciones disponibles en el mercado sin que ello implique como se lo mencionó anteriormente realizar una cuantiosa inversión es quizá un punto a tener muy presente.

2.1.2.1 ROUTER

Se entiende por Router a aquel dispositivo capaz de encaminar paquetes proporcionando conectividad a nivel de la capa de red según el modelo OSI es decir en capa 4,entre sus funciones principales se comprende conmutar y encaminar paquetes entre múltiples redes, para ello realiza esto intercambiando información específica de protocolos entre diferentes redes, cada Router es capaz de leer la información de direccionamiento contenida dentro de cada paquete teniendo incluso acceso a información adicional de redes complejas ya que las mismas trabajan incluso a un nivel superior del modelo OSI.

Un Router generalmente mantiene tablas de encaminamiento, las mismas que están constituidas por direcciones de red, con dichas tablas el Router es capaz de seleccionar la mejor ruta y la óptima en función de los caminos disponibles y del coste, por ende vale recalcar que los Routers no conversan con equipos remotos, y son más lentos que los bridges, puesto que deben realizar funciones y tratamientos complejos sobre cada paquete.

Algunas de las principales funciones de los Routers son:

- Actuar como barreras de seguridad entre los diferentes segmentos de red.
- Segmentar grandes redes en otras más pequeñas.
- Prohibir las tormentas de difusión, puesto que no se envía dichos mensajes de difusión

Un Router es el encargado de decidir qué camino utilizará un determinado paquete de datos de acuerdo al número de saltos que se generan entre los segmentos de red utilizando para ello tablas de encaminamiento que emplean protocolos de enrutamiento dinámicos como OSPF (Primer Camino Abierto más corto), RIP (Protocolo de Información de encaminamiento) etc., o simplemente estáticos que requieren de un administrador para generar y configurar manualmente la tabla de encaminamiento y especificar cada ruta, no así los dinámicos pueden localizar de

forma automática rutas y por ende casi no es necesaria la presencia de un administrador para gestión de dichas rutas.

2.1.2.2 SWITCH Y PUNTOS DE ACCESO

Son considerados como dispositivos lógicos de interconexión de redes de datos y que a su vez según el modelo de referencia OSI operan a nivel de la capa de enlace de datos, incluso una variedad de estos en la actualidad ya operan a nivel de Capa 3 conocidos como "Switch Multicapa"; entre sus principales tareas se encuentra interconectar dos o más segmentos de red, transmitiendo datos entre un segmento y otro de acuerdo con la dirección MAC de destino especificado en las tramas de red, vale recalcar que un switch toma las decisiones de envió basándose en una dirección MAC contenidas en una trama de datos trasmitidas, además también pueden funcionar como un filtro en una red, mejorando el rendimiento y a su vez agregando seguridad a la misma, tanto los switch como los puntos de acceso o mejor conocidos como AP mantienen similitudes ya que su función principal es servir como concentradores sin embargo los dos mantienen protocolos diferentes que varían en cierta forma de acuerdo al modelo OSI en las capas: física y de enlace de datos, los switch utilizan como medios físicos las conexiones cableadas, en tanto los Puntos de Acceso las ondas electromagnéticas.[5]

Hoy en día este tipo de dispositivos son diseñados de manera inteligente tanto así que son capaces de solventar problemas y prevenirlos en su respectiva capa de trabajo, son capaces ya de evitar bucles de red mediante la activación de determinados protocolos en dichos dispositivos permitiendo así disponer de caminos adicionales para llegar hacia un mismo destino o las inundaciones de tráfico que tienden a multiplicar de forma exponencial tramas, sin olvidar las tan problemáticas tormentas de Broadcast que genera muchos dolores de cabeza a los de administradores de red.

[5] Ms.Gonzalez, El switch: cómo funciona y sus principales característicasr, 08 de Noviembre de 2013, http://redestelematicas.com/el-switch-como-funciona-y-sus-principales-caracteristicas/

El uso de los puntos de acceso en los proveedores de servicios de Internet inalámbrico cada vez demanda mejoras y altas capacidades de ancho de banda; hace no muchos años atrás proveer el servicio de Internet por este medio era extremadamente caro no solo por los elevados costos de equipos e infraestructura sino por la limitación de cada punto de acceso para manejar un determinado tráfico por enlace y un personal técnico con elevados conocimientos en la materia que permitieran elaborar un enlace satisfactorio; esto en la actualidad ha cambiado los costos en infraestructura cada vez disminuyen más y la facilidad que los fabricantes brindan para armar enlaces en cuestión de minutos con apenas los conocimientos mínimos necesarios proveyendo incluso de herramientas adicionales que permitan verificar la calidad y estado de un enlace de datos inalámbrico ha hecho posible que hoy este tipo de acceso inalámbrico este ya disponible en hogares, las limitaciones aún están presentes en dicho medio y quizá algún día se lo logre superar la más prominente es la capacidad para manejar por puntos de acceso un número reducido de clientes esto debido a la capacidad que cada punto de acceso determina sea por su Hardware o sus características físicas especificando un throughput (volumen de tráfico real de data que fluye sobre el dispositivo) aún bajo en comparación con dispositivo que utilizan medios cableados.

2.1.2.3 ANTENAS.

El mundo de las Antenas de Transmisión aplicadas en entornos como los WISP, enlaces de datos y en si conceptos de Radio Frecuencia, es una temática sumamente compleja y de amplio estudio, por ende el desarrollo de este tema de tesis no pretende abarcar todos los tópicos que dicha materia engloba porque ello sería un tema de estudio aparte, ya que el objetivo de este tema de tesis no es conocer a detalle su funcionamiento, clasificación detallada, variedades, modos de operación, formas de propagación, y configuraciones especificas pero si entender su aplicativo en un WISP, funcionamiento básico, definiciones y sobre todo su aplicación y usos adecuados en el proceso de reestructuración que lleva a cabo la empresa Sigsignet.

Las Antenas WiFi están diseñadas para recibir o emitir ondas electromagnéticas a través de un espacio libre, su función principal es radiar la potencia que se le suministrar y convertir señales de voltajes en ondas electromagnéticas y su función inversa del lado receptor, incluso con las características de direccionalidad adecuadas para la aplicación.[6]

En la actualidad existe una gran variedad de tipos de antenas para el uso dentro de proveedores de servicios de Internet Inalámbricos (WISP) y su uso se está extendiendo cada vez más y más, no solo por la facilitad de implementación sino por los beneficios que dicho medio presenta, a tal punto que hoy se ha vuelto tan robustos que permiten armar enlaces con un alto grado de calidad tanto que mantienen una similitud con medios cableados limitados únicamente por su capacidad para manejar elevados anchos de banda como lo haría un medio cableado pero en si sus actuales tasas de transferencia no dan nada que desear, en tanto sus frecuencias de trabajo cada vez se van optimizando y ampliando, ahora ya no solo podemos disponer de frecuencias en los 900 Mhz, 2 Ghz sino también en los 5Ghz y 24 Ghz, con técnicas de optimización sobre la onda portadora haciéndola más robusta e inmune a condiciones climáticas poco favorables.

Es necesario antes de conocer las diversas variedades de antenas comprender algunos parámetros importantes en telecomunicaciones imprescindibles para determinar el uso de una antena adecuada:

Propagación o Radiación.- Es un parámetro representado utilizando una gráfica acerca de las características de radiación que tiene una antena, tales como Dirección de apuntamiento, Lóbulo Principal y secundario, Ancho de Haz, radiación del lóbulo principal a secundario y relación Front-Back, en si intentando representar la densidad de potencia radiada, y más que nada debemos saber que por medio de dicho

[6] "Salvan: Cradle of Wireless, How Marconi Conducted Early Wireless Experiments in the Swiss Alps", Fred Gardiol & Yves Fournier, Microwave Journal, February 2006, pp. 124-136

diagrama se puede definir la directividad de una antena(isotrópica, directiva, bidireccional, omnidireccional).[7]

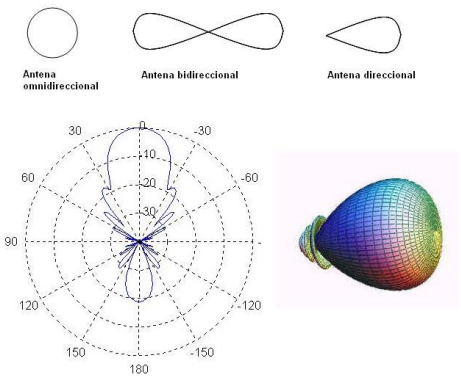


Figura 2.3. Diagrama de Radiación de una Antena.

Fuente. UPV, Diagramas de Radiación, 13 de Enero de 2004, http://www.upv.es/antenas/Tema_1/diagramas_de_radiacion.htm

Ganancia.-Uno de los parámetros de mayor importancia a la hora de elegir una antena adecuada para un determinado medio o zona geográfica se denomina la ganancia, que comprende la potencia de amplificación de la señal, y representa la relación entre la intensidad de campo que produce una antena en un punto determinado, en si cuando mayor es la ganancia se puede asumir que mejor es la antena.

Polarización.-Este parámetro indica la orientación de los campos electromagnéticos que emite o recibe una antena y puede ser lineal, circular o elíptica, tomando en la polarización lineal orientaciones tanto horizontales como verticales entre los +45º y los -45º clasificándolos de la siguiente manera:

[7]Iván Bernal, Revisión de Conceptos Básicos de Antenas y Propagación, 21 de Abril de 2006 http://clusterfie.epn.edu.ec/ibernal/html/CURSOS/AbrilAgosto06/Inalambricas/CLASES/AntenasParteI.pdf

Vertical: El campo electromagnético generado por la antena es vertical con respecto al horizonte es decir de arriba hacia abajo.

Horizontal: Aquí el campo electromagnético generado por la antena es paralelo al horizonte terrestre.

Circular: El campo electromagnético gira de vertical a horizontal y viceversa, generando movimientos en sentido horario o viceversa en forma de circulo y en todas las direcciones.

Elíptica: El campo electromagnético se mueve igual que en el caso anterior, pero con desigual fuerza en cada dirección.

Relación Front-Back.- Generalmente muchas personas y técnicos iniciados durante la puesta en marcha de una antena omiten este parámetro o casi nunca es tomado en consideración y quizá dicho parámetro es determinante en ciertas condiciones para la correcta operatividad de una antena, ya que determina la relación existente entre la máxima potencia radiada en una dirección geométrica y la potencia radiada en la dirección opuesta a esta, en muchos casos al armar un array de antenas en direcciones opuestas es necesario tomar en cuenta este factor ya que caso contrario las señales emitidas por cada antena podría ser objeto de interferencia impidiendo un correcto y normal funcionamiento de las mismas. Por ende este parámetro llega a ser especialmente útil cuando la interferencia hacia atrás es crítica en la elección de la antena que se pretende utilizar, algo importante que se debe recalcar es que si se dispone del patrón de radiación de la antena no es necesaria ya la relación F/B.

Línea de Vista.- Es el camino o ruta limpio sin obstrucciones entre una antena trasmisora y otra receptora, permitiendo así una correcta propagación de la señales emitidas, es importante conocer que cuando se instala un sistema inalámbrico que hace uso de un espectro electromagnético se debe tratar de transmitir ante la menor cantidad de materiales posibles u obstrucciones para obtener del lado receptor la mejor señal posible, este parámetro se lo considera más que técnico de una antena, un procedimiento necesario para el empleo de tales dispositivos y poder brindar una

comunicación satisfactoria entre dos puntos, muchas tecnologías actuales como Wimax y algunas en desarrollo no requerirán una línea de vista disponible para entablar una comunicación sino más bien solo de un equipo receptor de dichas señales es decir el equipo de lado del Abonado o usuario final.

Anchura de Luz.- Se entiende como la separación angular entre dos puntos de media potencia de acuerdo al grafico anterior expuesto "Diagrama de Radiación de una Antena", y especifica la siguiente relación que indica que cuanto mayor es la ganancia, menos es la apertura angular.

Zona de Fresnel: Se considera como el efecto de la difracción de onda, entendido como el espacio que existe entre el emisor de una onda y su receptor de modo que dicho desfase en las ondas en su volumen no supere los 180º, es importante determinar que en el grafico detallado a continuación, el factor K ya que este especifica la curvatura de la tierra considerando que para un K=4/3 la primera zona de Fresnel debe estar despejada al 100% mientras que para un estudio con K=2/3 debe tener despejado el 60% de la primera zona de Fresnel, sin olvidar que para establecer las zonas de Fresnel primero se debe determinar un línea de vista de RF.[8]

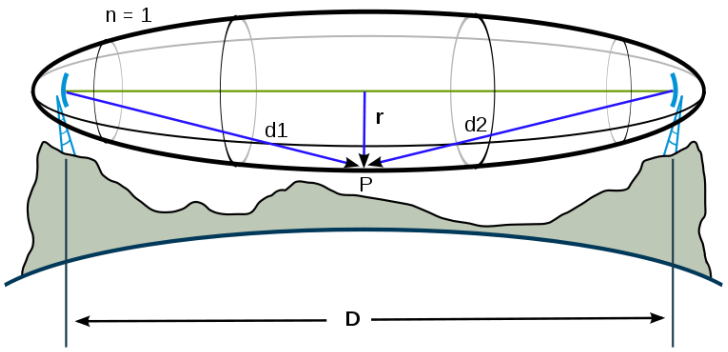


Figura 2.4. Diagrama de Zona de Fresnel.

Fuente. INFOSATELITE, Diagrama de Zona de Fresnel, http://www.infosatelite.net/wifi.php.

[8] José Paul Alvarado Robles, Zonas de Fresnel, QUETZALTENANGO, 22 DE OCTUBRE DE 2008, http://es.scribd.com/doc/55774691/zonas-de-fresnel

Dónde:

- r_n = radio de la enésima zona de Fresnel en metros (n=1,2,3...).
- d_1 = distancia desde el transmisor al objeto en metros.
- d_2 = distancia desde el objeto al receptor en metros.
- λ = longitud de onda de la señal transmitida en metros.

Y su fórmula de cálculo de las zonas esta dado de la siguiente forma:

$$r_n = \sqrt{\frac{n\lambda d_1 d_2}{d_1 + d_2}}$$ [9] (1)

Difracción.- Es un fenómeno característico dentro de las telecomunicaciones y en si las ondas electromagnéticas que se produce cuando estas se atenúan al encontrarse con obstáculos en el aire, por tal motivo la onda radiada por el transmisor se convierten en superposición de onda secundarias.

Frecuencia.- Se determina como la magnitud que mide el número de repeticiones por unidad de tiempo de una determinada onda, su unidad se representa en los Hz (Herzios), tiene una relación inversa con el concepto de longitud de onda, es decir que a mayor frecuencia menor longitud de onda y viceversa; dicho parámetro es necesario comprenderlo no solo por su uso dentro de las Telecomunicaciones y otras áreas, sino que por dicho medio se emplean las distintas regulaciones impuestas por el estado para su uso y explotación, ya que es el medio físico que emplean los distintos equipamientos para realizar la transmisión física de datos. Muchas frecuencias en nuestro país y en todo el mundo se encuentran reguladas por el estado, siendo estos los entes que aprueban o niegan el uso de las mismas, salvo estas sean de libre uso.

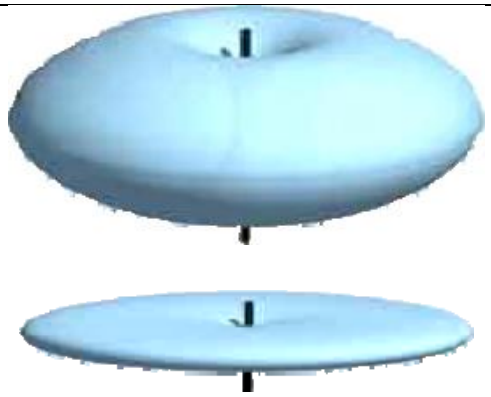
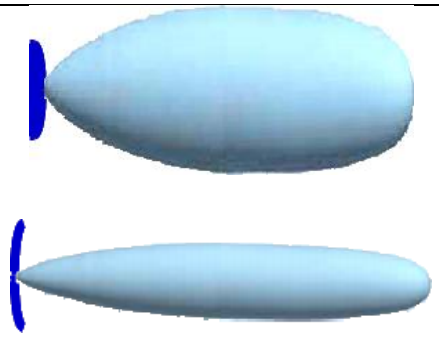
[9] José Paul Alvarado Robles, Zonas de Fresnel, QUETZALTENANGO, 22 DE OCTUBRE DE 2008, http://es.scribd.com/doc/55774691/zonas-de-fresnel

Tipos de Antenas.-

Las antenas se clasifican de la siguiente forma:

Antenas Omnidireccionales.- Son y han sido utilizadas desde los primeros días de las comunicaciones inalámbricas para irradiar y recibir de igual manera en todas las direcciones, actualmente en entornos RF simples su eficacia se encuentra cuestionada, por ende los usuarios que accedan al sistema lo hacen con un pequeño porcentaje de la energía radiada esto debido al radiación incontrolada de la energía que dicha antena mantiene.

Antenas Direccionales.-Esta variedad de antenas pretende controlar la dispersión de la energía por radiación de un sector de al menos 120º en un array de antenas sectorizadas de hasta 3 para alcanzar los 360º, brindando así mayor alcance y utilizando la misma cantidad de potencia de transmisión usada en una antena omnidireccional, permitiendo a la señal viajar más lejos y aumentar la eficiencia del espectro.

Geometría	Diagrama de Radiación	Tipo
		**Omnidireccionales**
		

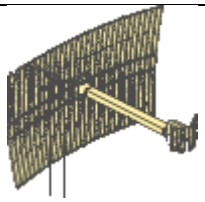
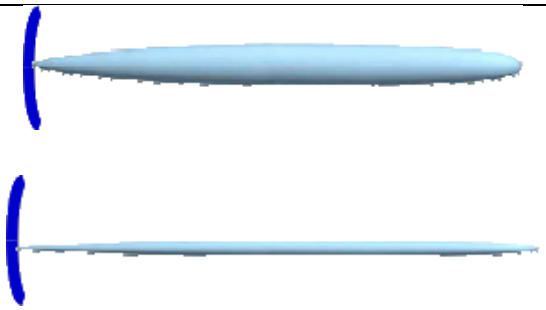
		**Unidireccionales**[10]
		

Tabla 2.3. Clasificación de las Antenas por Geometría y Radiación.

Fuente: n/d, 30 de Mayo de 2010, Patrones de Radiación, http://rdspako.blogspot.com/2010_05_01_archive.html

2.1.2.4 GATEWAY

Conocido como pasarela también, los Gateway permiten activar la comunicación entre diferentes arquitecturas y entornos de red e incluso encargados de dar conectividad externa, además de empaquetar y convertir los datos de un entorno a otro de forma que cada uno pueda entender los datos del otro y así pueda coincidir con los requerimientos de un sistema de destino, además una utilización habitual de los gateway es actuar como transductores entre equipos personales o entornos de grandes sistemas.

Dentro de un entorno LAN normalmente se diseña un equipo para realizar el papel del Gateway. Los programas de aplicaciones especiales en los equipos personales acceden a los grandes sistemas comunicando con el entorno de dicho sistema a través del equipo Gateway.

[10] Conceptos Generales de Antenas, 2011, http://www.edutecne.utn.edu.ar/wlan_frt/antenas.pdf

2.1.2.5 FIREWALL

Es un sistema de seguridad, que utiliza tanto una combinación de hardware como de Software, cuya funcionalidad es proteger la red de una organización frente a una amenaza externa procedentes de otra red, incluyéndose en esta Internet, evitando así que los equipos de red de una organización internos se comuniquen con equipos externos y viceversa, se podría decir que su función aparte de auditar la actividad sobre la red, registrando volumen de tráfico, detección de ataques, actividades maliciosas sobre la red y mitigación sobre tales efectos, además permitir solo comunicaciones autorizadas por el mismo o de acuerdo a políticas previamente establecidas; el funcionamiento de un firewall es sencillo todo mensaje que pasa a través de este debe cumplir con los criterios especificados caso contrario son descartados, por ende recalcar que un firewall correctamente configurado da un valor agregado de seguridad a una red pero en todo caso nunca es suficiente ya que la seguridad informática abarca ámbitos y niveles de trabajo y protección entre varios dispositivos incluso aplicativos.

Al hablar de firewall es también común escuchar el término DMZ o zona desmilitarizada, creada a partir de un Firewall en donde se ubican los servidores o dispositivos cuya información o servicios necesitan ser resguardados con un alto grado de importancia.

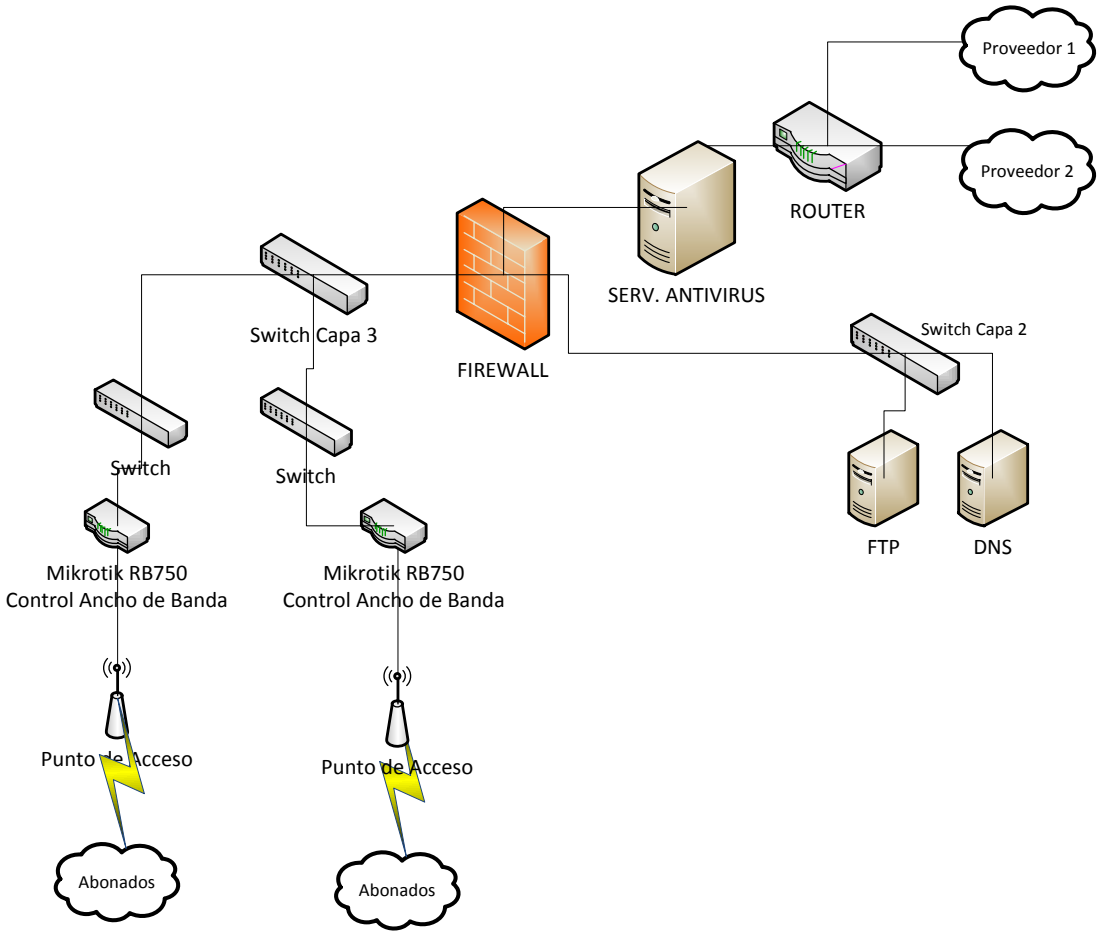


Figura 2.5. Topología de Ubicación de un Firewall.

Fuente: Los Autores, Modelo de Topología de un Firewall, 2013

2.1.2.6 PROXY CACHE

Se entiende como aquel sistema o mecanismo destinado al almacenamiento temporal de objetos que constituyen una Web 2.0, como videos, paginas HTML, imágenes. Su funcionamiento se basa en interceptar peticiones y conexiones de red que un cliente realiza a un determinado servicio y en tal servidor si el objeto solicitado en la petición se encuentra almacenado de forma local este es entregado sin ejecutar la petición externa y prácticamente a velocidad de la Limitada Internamente, son múltiples las tareas que un proxy puede cumplir entre ellas y las más relevantes son mantener el anonimato, optimización y rendimiento e incluso a nivel de seguridad.

Muchos proveedores de Internet en la actualidad hacen uso de este tipo de Sistemas, no solo por el hecho de que permite un amplio ahorro en cuanto a ancho de banda se refiere sino a permitir una mejor experiencia de acceso a Internet y privacidad, ya que muchos casos generalmente en descargas o reproducción de videos dicho contenido es entregado localmente mas no desde la Internet.

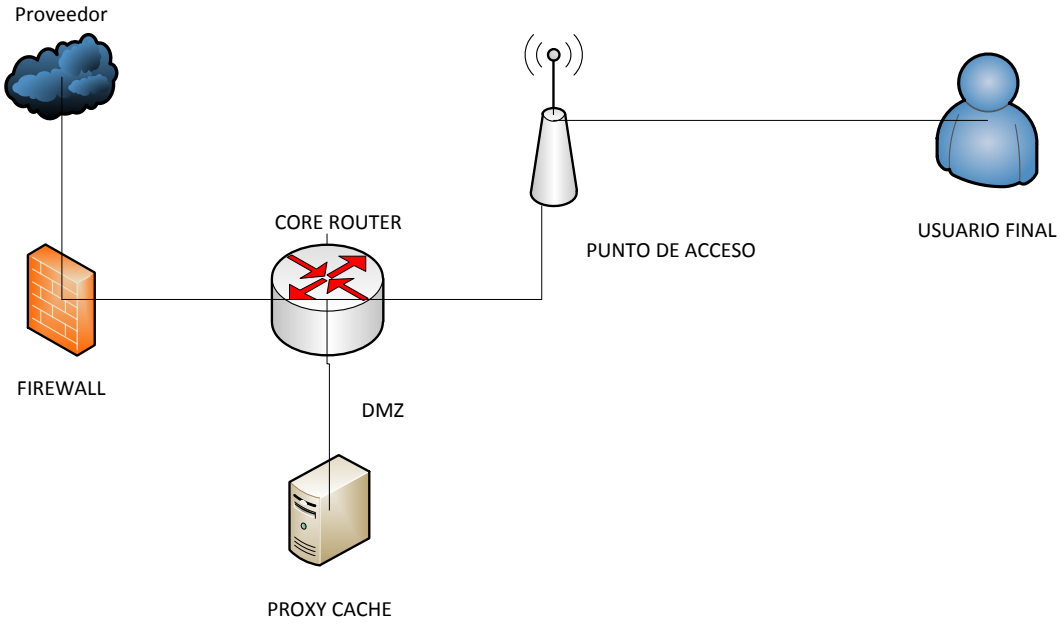


Figura 2.6. Topología Básica de un Proxy Cache

Fuente: Los Autores, Modelo Ubicación Básico de un ProxyCache, 2013

2.1.2.7 ADMINISTRADOR DE ANCHO DE BANDA & QOS

El tema de administración de Ancho de Banda & QoS es quizá considerado hoy en día como una temática sumamente compleja que abarca muchos temas independientes y que incluso se considera objeto de estudio con sus respectivas titulaciones, es decir un mundo completamente nuevo dentro de las redes de datos. Por ende en entornos como los WISP es de suma importancia su implementación, no solo porque permite racionar el ancho de banda a los abonados sino mediante la calidad de servicio o QoS brindar un acceso con una latencia reducida.

La función principal de un administrador de ancho de banda, es limitar el uso de la misma mediante el empleo de diversos algoritmos que permitan racionar el total del ancho de banda, de tal forma que pueda satisfacer el consumo con límite deseado establecido en las políticas de red iniciales.

2.1.2.8 HUB

Conocido como un concentrador y de acuerdo al modelo OSI su trabajo está centrado en la capa 1, por lo tanto se entiende como aquel dispositivo que permite la concentración de varios dispositivos de red establecidos en un solo dominio de colisión o segmento, teniendo como función principal regenerar en señales de datos en caso de pérdida de parte de las mismas o amplificar las mismas, para todos los dispositivos de red asociados menos para el que originó la transmisión.

En otra de sus funciones asignadas es la de actuar como repetidor multipuerto y así extender los dominios de colisión.

2.1.2.9 CPE

Conocido también como (Customer Premises Equipment) o equipo Local del cliente hoy en día ampliamente usados por los proveedores de servicio de Internet Inalámbrico WISP de lado de sus subscriptores, son unidades terminales asociadas a equipos de telecomunicaciones cuya función principal es ser usado de puente de conexión entre la red de datos inalámbrica y el usuario final, pudiendo así proveer tanto video, voz, datos y diversos servicios a nivel de red.

2.1.2.10 ESTRUCTURAS BÁSICAS DE TELECOMUNICACIONES.

Las estructuras dentro del ámbito de telecomunicaciones comprenden aquellos medios físicos metálicos o afines con el nombre de “torres de transmisión” que

alojan todo el equipamiento de red destinado para la transmisión de señales en una determinada zona, elaborados con partes metálicas y con una altura considerable, y mantiene diversas formas como son:

Torres Atirantadas.- Son estructuras metálicas que pueden o no utilizar una base cimentada en su centro por lo tanto necesitan soportes adicionales para estabilizar su peso, por ende utilizan cables tensores metálicos con una alta resistencia que permitan mantener su centro de gravedad estable y fijo.

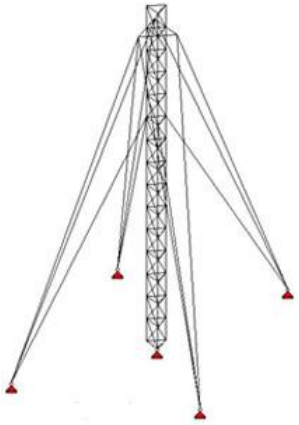


Figura 2.7. Torre Metálica Atirantada.

Fuente: Wahba Y.; Madugula M. And Monforton G. "Evaluation of non-linear analysis of guyed antenna towers". Computers and Structures. 1998, vol. 68, p. 207-212.

Torres Auto Soportadas.-

Son montadas sobre terrenos, en áreas urbanas o cerros, mantiene su centro de gravedad completamente estable ya que cuentan con una cimentación adecuada y de gran envergadura para poder resistir las fuerzas externas, cuando las mismas superan alturas establecidas es necesario el uso de tensores para mantener la estabilidad de las mismas.

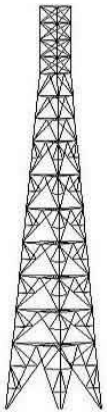


Figura 2.8. Torre Metálica Autosoportada.

Fuente: Wahba, Y.; Madugula, M. And Monforton, G. "Evaluation of non-linear analysis of guyed antenna towers". Computers and Structures. 1998, vol. 68, p. 207-212.

Torres Mono Polo.-

Figura 2.9. Torre Metálica Mono Polo.

Fuente: Wahba, Y.; Madugula, M. And Monforton, G. "Evaluation of non-linear analysis of guyed antenna towers". Computers and Structures. 1998, vol. 68, p. 207-212.

Estructuras elaborados sobre mástiles metálicos circulares, de gran uso por el poco espacio que ocupan y su estética más atractiva, es necesario montarla sobre una base cimentada, una de sus grandes desventajas es quizá que no pueden ser empleadas para cubrir grandes alturas por su poca resistencia a la intemperie.

Muchas de los veces los centros de red o NOC no pueden ser alojadas directamente en un local físico ya que dichas torres y nodos son montados generalmente en cerros

o lugares distantes, por ende se opta por llevar los mismos al lugar, y se alojan utilizando una caja metálica especialmente construida para soportar la intemperie.

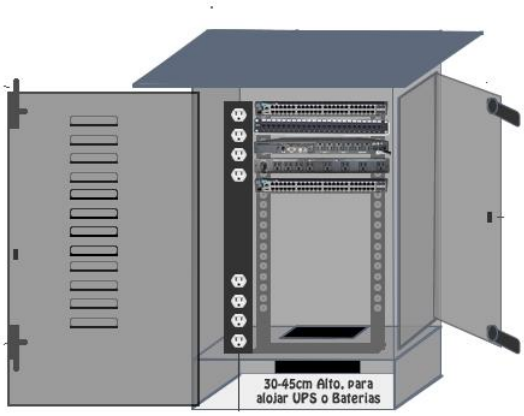


Figura 2.10. Caja Metálica para Dispositivos de Red.

Fuente: Los Autores, Modelo de Caja Metálica para NOC, 2013

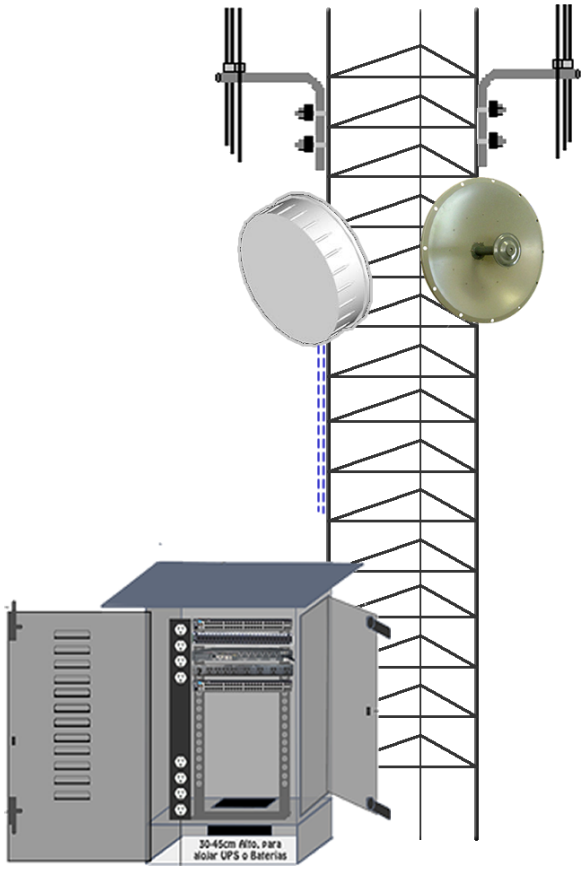


Figura 2.11. Torre Metálica Atirantada y NOC de red.

Fuente: Los Autores, Modelo Caja Metálica Y Torre Atirantada, 2013

2.2. ROUTEROS MIKROTIK

Es un sistema operativo basado en Linux destinado a tareas de red orientado a arquitecturas tanto CISC, RISC, MIPS, ARM, Tilera, conocido como el "todo en uno" ya que todos sus servicios se encuentran disponibles en cualquiera de los niveles de licenciamiento es solo necesario activarlos para tener disponibilidad de los mismos, RouterOS puede ser un firewall, Router, QoS, switch etc. Incluye protocolos propietarios especiales a nivel inalámbrico, Calidad de Servicio etc. que dan un valor agregado el S.O., en sus inicios muchos de los servicios implementados por parte de RouterOS eran en su totalidad código bajo licencia GNU/Linux, hoy gran parte de su código es propietario, una de las ventajas de gran relevancia es que quizá la posibilidad de convertir cualquier PC en un Router con todas las características que RouterOS dispone, no siendo necesario como en alternativas existentes comprar el Hardware para luego usarlo como por ejemplo Cisco o Juniper, el licenciamiento del Sistema Operativo es muy flexible y se basa en niveles, con precios asequibles en donde no solo es necesario comprar el Hardware para disponer de los beneficios del Sistema Operativo sino el mismo puede ser descargado y luego licenciado con la compra de la misma.

El sistema operativo como tal dispone de herramientas alternativas de administración grafica facilitando las tareas al administrador y brindando estadísticas puntuales, dichas herramientas están orientadas a la Web así como una aplicación ejecutable para Windows, y funcional para Linux bajo emulación con Software Wine denominada Winbox, y en si uno de los agregados de más relevancia es su API posibilitando diseñar sistemas externos e intégralos a cualquiera de los dispositivos de red RouterOS.

Además si se desea una solución dedicada, RouterOS hace uso de su propio Hardware que es RouterBoard posibilitando que al mismo alcanzar niveles de rendimiento elevados.[11]

2.2.1 CARACTERISTICAS GENERALES

Muchas son las características que RouterOS pone a disposición por la tanto se mencionará las principales tales como:

- Enrutamiento avanzado OSPF, BGP ó VPLS/MPLS
- Calidad de servicio o QoS.
- Soporte técnico inmediato en caso de detectarse errores en su programación se puede generar un archivo de soporte para luego ser corregida mediante una actualización.
- Múltiples servicios de red integrados en uno solo.
- Niveles de licenciamiento flexible a costos asequibles.
- Funcional tanto en arquitecturas CISC, RISC, MIPS, TILERA, ARM
- Puede obtener gran rendimiento al estar funcionando sobre un RouterBoard que es el hardware dedicado para RouterOS.
- Posibilidad de virtualización por medio de KVM.
- Diversa variedad de encriptación incluso de grado militar soportadas.

2.2.1.1 MODELOS DE LICENCIAMIENTO Y COSTOS.

Como se ha mencionado en temas anteriores el modelo de licenciamiento aplicado por Mikrotik para RouterOS mantiene hasta el momento una política flexible en cuanto a costos se refiere, ya que se puede adquirir la licencia más económica pero sin embargo se dispone de todos los servicios y funcionalidades disponibles en RouterOS, pudiendo incluso realizar actualizaciones hasta las versiones permitidas de acuerdo a su nivel de Licencia, por ende se define la siguiente tabla de licenciamiento:

[11] DISCHER, STEHHEN R.W, "RouterOS by example", Learn Mikrotik, 2011, p 10

Licencia Nivel	0 (Modo Demo)	1 (Gratis)	3 (CPE WISP)	4 (WISP)	5 (WISP)	6 (Controlador)
Precio	Sin licencia	requiere registración	solo en volumen	$45	$95	$250
Actualizable a	-	No actualizable	ROS v6.x	ROS v6.x	ROS v7.x	ROS v7.x
Soporte en Configuración Inicial	-	-	-	15 días	30 días	30 días
Wireless AP	24h prueba	-	-	si	si	si
Cliente Wireless y Bridge	24h prueba	-	Si	si	si	si
Protocolos RIP, OSPF, BGP	24h prueba	-	si (*)	si	si	si
Túneles EoIP	24h prueba	1	ilimitadas	ilimitadas	ilimitadas	ilimitadas
Túneles PPPoE	24h prueba	1	200	200	500	ilimitadas
Túneles PPTP	24h prueba	1	200	200	500	ilimitadas
Túneles L2TP	24h prueba	1	200	200	500	ilimitadas
Túneles OVPN	24h prueba	1	200	200	ilimitadas	ilimitadas

VLAN interfaces	24h prueba	1	ilimitadas	ilimitadas	ilimitadas	ilimitadas
Usuarios Activos HotSpot	24h prueba	1	1	200	500	ilimitadas
Cliente RADIUS	24h prueba	-	Si	si	si	si
Colas / Cuotas	24h prueba	1	ilimitadas	ilimitadas	ilimitadas	ilimitadas
Web proxy	24h prueba	-	Si	si	si	si
User manager sesiones activas	24h prueba	1	10	20	50	ilimitadas
Número de invitados KVM	No disponible	1	ilimitadas	ilimitadas	ilimitadas	ilimitadas

Tabla 2.4. Modelos Licenciamiento para RouterOS

Fuente: Mikrotik, Niveles de Licencimiento, Abril del 2013, http://wiki.mikrotik.com/wiki/Manual:License_levels

Generalmente las licencias 4,5 y 6 son las más comercializadas el nivel 3 es una versión no disponible que no tenía capacidad Wireless y que ahora ha sido reemplaza por la nivel 4 según Mikrotik puede ser adquirida siempre y cuando se necesite más de 100 inmediatamente, las versiones mencionadas serán actualizables al release mayor o siguiente, inclusive versiones en desarrollo Beta como por ejemplo ir de las versión 4.9 a la versión 5 o 5beta, en el caso de actualizaciones es posible realizarlas las veces que se quieran, muchas actualizaciones son de vital importancia ya que corrigen errores de versiones anteriores.

Generalmente el proceso de licenciamiento se basa en un método de reconocimiento de hardware, en específico sobre el disco duro o MBR (Master Boot Record) si lógicamente el medio a instalar es una PC, generando un numero de Soft_ID único mismo contra el cual la licencia deberá ser generada y validada, el formato del disco se permite siempre y cuando se utilicen herramientas brindadas por Mikrotik, para generar los respectivos Backups, caso contrario la misma corre el riesgo de perderse; la licencia es intransferible, en el caso de remover accidentalmente una licencia es posible acceder al soporte de Mikrotik y solicitar ayuda para recuperar la misma, pagando un costo adicional mínimo.

Las compras de las licencias se las realizan directamente desde la web www.mikrotik.com antes que nada creando una cuenta y luego ejecutando la compra.[12]

2.2.1.2 COMPARATIVAS CON SOLUCIONES PRESENTES EN EL MERCADO

Muchas son las soluciones actuales en el mundo de Networking proveídas por distintos fabricantes tales como Cisco, Juniper, Motorola etc, líderes mundiales en este sector no solo por sus años de presencia en el mercado sino por sus soluciones y dispositivos en sí, claro está que muchas de las grandes empresas generalmente al adquirir nuevos recursos IT uno de los parámetros esenciales al implementar este tipo de tecnología es el costo/beneficio que puede aportar la misma a la empresa, y en ello tiene un punto a su favor RouterOS al ser una solución con un costo asequible y mínimo representa una inversión casi asegurada.

El segundo punto a comparar es el rendimiento que aporta el Sistema Operativo en conjunto con su Hardware en el caso de empresas como Cisco cuyas soluciones no es de extrañar, son tan efectivas que pueden procesar grandes cantidades de tráfico a velocidades increíbles al igual que su semejante Juniper con su tan afamado JunOS, pero elevando los costos a la par, esto se debe a que dichas empresas sacan más crédito ya que su sistema operativo al igual que su hardware están mejor optimizados

[12] Mikrotik, Niveles de Licencimiento, Abril del 2013, http://wiki.mikrotik.com/wiki/Manual:License_levels

para trabajo en conjunto, Mikrotik por tal razón ha decidido no quedarse atrás y aportar su solución propietaria denominada RouterBoard, brindado hardware dedicado para pequeñas y medianas empresas, equipos dedicados capaces de mover y procesar cientos de Mbps/s, tal es el caso de uno de ellos dedicado al segmento denominado Cloud Core Router.

Muchas de las soluciones actuales proveídas a nivel de Networking se encuentran disponibles como productos o appliances cuya funcionalidad es dedicada e independiente, pudiendo o bien tener una solución exclusiva para ruteo o con un servicio de red exclusivo, es decir si se necesita una solución para ruteo se paga por ella y se dispone de la misma así de igual forma el caso de un firewall o Switch etc., por ende los costos en inversión IT empiezan a incrementar y muchas de las pequeñas empresas tiene que lidiar con las mismas, en cambio Mikrotik pone a disposición todos sus servicios en uno solo, es decir simplemente basta activarlos y poder disponer de todos, es decir puede ser un Router, un Switch, aunque muchas de las veces no sea lo adecuado pero queda a decisión del usuario el criterio para elegir que puede hacer dicho equipo y que servicios pueden funcionar o activar sobre RouterOS.

2.2.1.3 VENTAJAS Y DESVENTAJAS.

Muchas son las ventajas que acompañan a RouterOS tales como:

- Múltiples servicios de red en uno solo.
- Soporte Inmediato por parte del fabricante y actualizaciones constantes.
- Licenciamiento Flexible.
- Integrable con cualquier sistema externo.
- Facilidad de administración.
- Router con altas prestaciones.
- Administrador de Ancho de Banda con algoritmos propietarios.
- Económico y Fiable.
- Ideal para entornos como WISP y otros.
- Robusto.

- Altamente Configurable.
- Poderosa Shell comandos auto complementable y ayuda en tiempo real.
- Protocolos propietarios eficientes para enlaces de radio.

Sus grandes desventajas quizá se consideran las siguientes:

- Nivel de madurez del sistema operativo es medio aun muchos aspectos necesitan ser mejorados y pulidos, pero se compensan con su constante actualización.

2.2.1.4 ROUTERBOARD COMO HARDWARE DE RED DEDICADO.

RouterBoard es la división de Mikrotik dedicada a la fabricación de Hardware para RouterOS utilizando placas base pensadas para construir Routers de carácter dedicados, muchas de estas antes de ser puesta en producción son probadas al límite por su partner Xena Networks y así obtener estadísticas y características de rendimiento pegadas a la realidad.

En la actualidad son ya comercializadas versiones dedicadas a la administración de red con hardware de altas prestaciones y rendimiento que tranquilamente pueden competir a la par con soluciones de gran nivel como Cisco y Juniper. Así como también hardware a precios asequibles con las mismas funcionalidades.

2.2.2 PRINCIPALES CONFIGURACIONES.

Es necesario antes de realizar cualquier configuración sobre servicios de Red, o configuraciones puntuales, establecer las configuraciones elementales indispensables para poder mantener no solo un nivel de seguridad adecuado sino además para permitir un buen funcionamiento por lo tanto en este punto se describe a continuación dichas configuraciones elementales.

2.2.2.1 CONOCIENDO ROUTEROS, ¿QUÉ ES? Y COMO OBTENERLO

RouterOS un sistema operativo basado en Linux destinado a trabajar en redes de datos, puedes ser instalable en un PC sin problema alguno generalmente en los

RouterBoard dicho sistema viene preinstalado pero de todas formas se mencionará los procedimientos de reinstalación en caso de daño alguno; RouterOS se lo puede obtener directamente desde http://www.mikrotik.com/download, el mismo se presenta en diferentes arquitecturas instalables que van desde x86 a RISC ya mencionadas anteriormente, incluso pudiendo descargar sus respectivos paquetes para cada uno de sus servicios e instalarlos de forma manual tales como DHCP Server, IPv6, Routing etc, es necesario antes de realizar la descarga confirmar la versión y arquitectura sobre la cual se pretende hacer una instalación limpia, en caso de que se cometiera error de arquitectura y se quisiera instalar en otra simplemente tendríamos un error de instalación que nos impediría continuar con la instalación normal.[13]

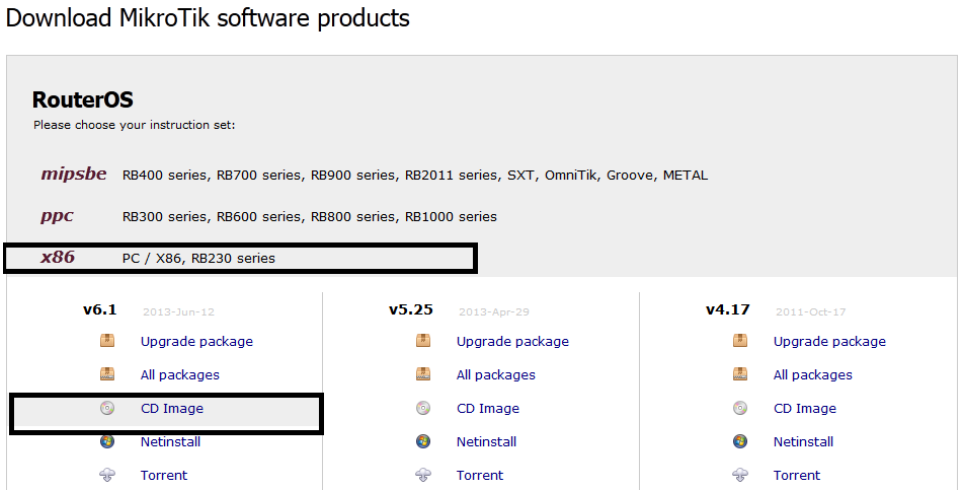


Figura 2.12. Página de descarga instaladores RouterOS

Fuente: Mikrotik, Download Mikrotik software products, 2013, http://www.mikrotik.com/download

2.2.2.2 PROCESO DE INSTALACIÓN Y CARGA DE LICENCIA

El procedimiento de instalación en arquitecturas x86 se describe de la siguiente forma:

[13] DISCHER, STEHHEN R.W, "RouterOS by example", Learn Mikrotik, 2011, p 10

- Descargar el RouterOS desde http://www.mikrotik.com/dowload, el momento disponible la versión 6.1 en formato .iso.
- Una vez descargado es necesario grabarlo en un CD para su instalación.
- Con el CD proceder a bootear, el ordenador por el medio óptico, donde la primera pantalla a divisar es la selección de paquetes, donde será definir cuál serán los que vamos a instalar o si a su vez instalaremos todos, depende nuestra necesidad y uso que se pretenda dar.
- Seleccionar los paquetes a instalar y continuar con la instalación presionar la tecla i, luego de seleccionados.

Figura 2.13. Instalación de RouterOS y selección de paquetes.

Fuente: Los Autores, Pantalla Inicial de instalación V.5.X, 2013

- Iniciado el proceso se mostrará un mensaje indicando que si se desea mantener la configuración anterior, esto es recomendable cuando se está realizando una reinstalación caso contrario como es una nueva instalación se procede a presionar la letra n o (no).
- En el siguiente paso se visualizará un mensaje de aviso indicando que todos los datos almacenados en el disco serán borrados así mismo presionar la letra y (yes).
- Al terminar la instalación saldrá la ventana de información indicando que el Software ha sido instalado.

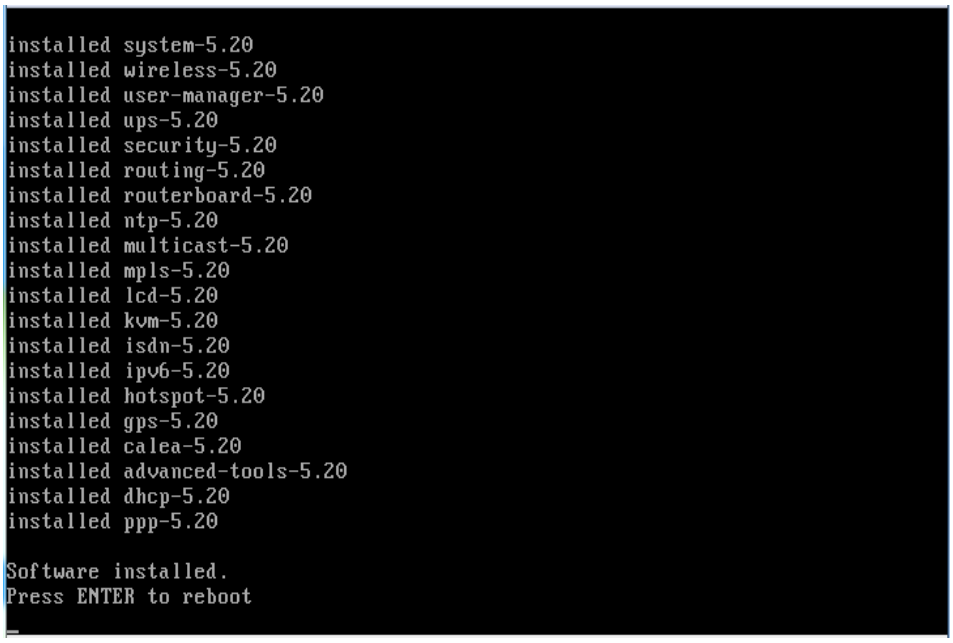


Figura 2.13. Confirmación de instalación de paquetes RouterOS.

Fuente: Los Autores, Confirmación de Instalación paquetes V 5.X, 2013

La lista de paquetes disponibles en la actualidad son las siguientes:

Paquetes	Características
advanced-tools (*mipsle, mipsbe, ppc, x86, Tilera*)	Herramientas Avanzadas: ping, netwatch, ip-scan, sms tool, wake-on-LAN
calea (*mipsle, mipsbe, ppc, x86, Tilera*)	Herramienta de recolección de datos para uso específico y posterior análisis forense de la "Communications Assistance for Law Enforcement Act" de Estados Unidos.
dhcp (*mipsle, mipsbe, ppc, x86, Tilera*)	Servidor DHCP y Cliente
gps (*mipsle, mipsbe, ppc, x86, Tilera*)	Soporte para Sistema de Posicionamiento Global
hotspot (*mipsle, mipsbe, ppc, x86, Tilera*)	Paquete para soporte Hotspot

ipv6 (*mipsle, mipsbe, ppc, x86, Tilera*)	Paquete para soporte para direccionamiento IPv6
mpls (*mipsle, mipsbe, ppc, x86, Tilera*)	Paquete para soporte MPLS
multicast (*mipsle, mipsbe, ppc, x86, Tilera*)	Protocolo Independiente Multicast - Sparse Mode;Internet Group Managing Protocol - Proxy
ntp (*mipsle, mipsbe, ppc, x86, Tilera*)	Network Protocol, protocol para sincronizar los relojes de los sistemas informáticos.
ppp (*mipsle, mipsbe, ppc, x86, Tilera*)	Protocolo para administrar conexiones punto a punto Cliente MlPPP, PPP, PPTP, L2TP, PPPoE, ISDN PPP cliente y servidor.
routerboard (*mipsle, mipsbe, ppc, x86, Tilera*)	Acceso y administracion RouterBOOT, RouterBOARD e información específica.
routing (*mipsle, mipsbe, ppc, x86, Tilera*)	Paquete de soporte para protocolos de enrutamiento dinámico tales como RIP, BGP, OSPF y utilitarios de enrutamiento tales como likeBFD, o filtros para rutas.
security (*mipsle, mipsbe, ppc, x86, Tilera*)	IPSEC, SSH, Secure WinBox
system (*mipsle, mipsbe, ppc, x86, Tilera*)	Caracterisiticas Básicas del router tales como enrutamiento estático, direccionamiento IP, sNTP, telenet API, , *queues, firewall, web proxy, DNS cache, TFTP, IP pool, SNMP, packet sniffer, e-mail send tool, graphing, bandwidth-test, torch, EoIP, IPIP,bridging, VLAN, VRRP etc.*

	También para MetaRouter y Virtualizacion.
ups (*mipsle, mipsbe, ppc, x86, Tilera*)	Paquete destinado a monitorizar el estado de un APC ups
user-manager (*mipsle, mipsbe, ppc, x86, Tilera*)	Paquete Radius de administracion de Usuarios Mikrotik
wireless (*mipsle, mipsbe, ppc, x86, Tilera*)	Soporte para interfaces wireless
arlan (*x86*)	Soporte para chipset Aironet Arlan
isdn (*x86*)	Soporte para ISDN (Red Digital de servicios Integrados)
lcd (*x86*)	Soporte para panel LCD
radiolan (*x86*)	Soporte para tarjetas radiolan
synchronous (*x86*)	Soporte para FarSync
xen (*discontinued x86*)	Soporte para virtualización XEN.
kvm (*x86*)	Soporte para virtualización KVM.
routeros-mipsle (*mipsle*)	Paquetes combinados para arquitectura mipsle (RB100, RB500) (incluye paquetes *system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, imv6, routing*)
routeros-mipsbe (*mipsbe*)	Paquetes combinados para arquitectura mipsle (RB400) (inluye paquetes *system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, imv6, routing*)
routeros-powerpc (*ppc*)	Paquetes combinados para arquitectura powerpc (RB300, RB600, RB1000) (incluye paquetes

	system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, imv6, routing)
routeros-x86 (*x86*)	Paquetes combinados para arquitectura x86 (Intel/AMD PC, RB230) (incluye paquetes *system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, imv6, routing*)
routeros-Tilera (*Tilera*)	Paquetes combinados para arquitectura Tilera (incluye paquetes *system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, imv6, routing*)
mpls-test (*mipsle, mipsbe, ppc, x86, Tilera*)	Soporte para apoyo de MPLS Multi Protocol Labels Switching.
routing-test (*mipsle, mipsbe, ppc, x86, Tilera*)	Soporte de apoyo para protocolos (RIP, OSPF, BGP) [14]

Tabla 2.5. Lista de paquetes disponibles para RouterOS.

Fuente: MIKROTIK, "Paquetes disponibles RouterOS", 2013, http://wiki.mikrotik.com/wiki/System/Packages_spanish

2.2.2.3 MÉTODOS DE ACCESO, CONFIGURACIONES BÁSICAS Y CARGA DE LICENCIA.

Luego de terminado el proceso de instalación es necesario proceder con la carga de la licencia y configuraciones iniciales, para dicho caso se utilizara la herramienta de administración grafica denominada Winbox. (Es un archivo ejecutable se conecta a RouterOS utilizando una IP o realizando un barrido en capa 2 por medio de su MAC es decir establece una conexión en capa 2, mismo que utilizando el usuario y

[14] Mikrotik, Sistema y Paquetes, 20 Junio del 2011, http://wiki.mikrotik.com/wiki/Manual:System/Packages

password de RouterOS por defecto, se ingresara a realizar las configuraciones iniciales en RouterOS

http://download2.mikrotik.com/winbox.exe

Al ejecutarlo se dispondrá de una venta como esta:

Figura 2.14. Winbox, Herramienta Grafica para administrar RouterOS

Fuente: Fuente: Los Autores, Ventana Loggin Winbox, 2013

- En su configuración por defecto RouterOS establece una IP por defecto que es: 192.168.88.1/24 y el usuario admin sin contraseña, por tal es imprescindible si se realiza una conexión por IP que el ordenador tenga una IP compatible.
- Al dar click en "Connect" Winbox empieza a descargar los plugins necesarios del dispositivo contra el cual se va a conectar, con ello terminado se podrá realizar las configuraciones iniciales, el proceso de descarga de plugins puede tomar cierto tiempo dependiendo el tipo de conexión y no es que se realice una solo vez sino pueden ser varias dependiendo la versión el equipo a conectarse.
- La venta inicial de conexión será la siguiente.

Figura 2.15. Winbox, ventana principal de administración.

Fuente: Los Autores, Winbox Aplicación de Administración RouterOS, 2013

- El primer paso recomendable si la conexión no se realizó por IP y se la hizo a nivel de capa 2 es agregar la IP, ya que muchas configuraciones realizadas a veces no son aplicadas, para ello dirigirse a la pestaña IP >>> Address y agregar la IP determinando la interfaz a la cual va a asignar la misma Ejm.

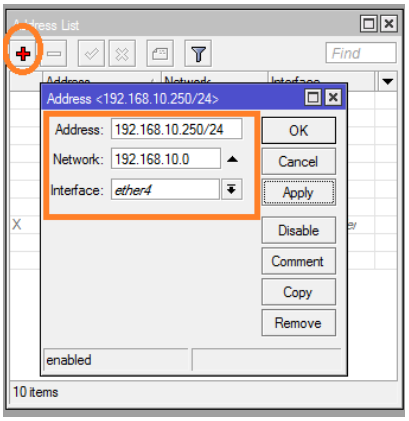


Figura 2.16. Winbox, agregar IP RouterOS

Fuente: Los Autores, Winbox Aplicación de Administración RouterOS, 2013

O mediante línea de comandos en consola de la siguiente forma:

```
[RouterOS@RouterUPS] >ip address add address=192.168.10.250/24
interface=ether1
```

Dentro de Winbox es importante también conocer el submenú de opciones básicas disponibles tales como:

Figura 2.16. Winbox, submenú de opciones Winbox (Adress – List)

Fuente: Los Autores, Winbox Aplicación de Administración RouterOS, 2013

	Agregar un nuevo elemento a la lista
	Remover un elemento de la lista
	Habilitar un elemento de la lista
	Deshabilitar un elemento de la lista
	Agregar un comentario a un elemento de la lista.
	Filtrar la vista de la lista.

Tabla 2.6. Funciones de Opciones principales en Winbox

Fuente: Los Autores, Winbox Aplicación de Administración RouterOS, 2013

Terminado de setear los parámetros de conexión se realiza la conexión utilizando la IP configurada en la interfaz aplicada y empezar con el proceso de carga de Licencia.

Para cargar la licencia existen varios procedimientos, pero dentro de este trabajo se tomarán algunos o las importantes en cuenta, para ello se asume tener una licencia valida disponible en la cuenta de Mikrotik, o a su vez haber comprado la licencia a un revendedor y posterior introducirla con el respectivo Soft-ID.

- Ingresar dentro del navegador a la siguiente URL:
  http://www.mikrotik.com/

  Luego a la pestaña >>> account
- Se procede a registrar los datos solicitados, realizado dicho paso se notificará con un mail para que se confirme los datos previamente ingresados.

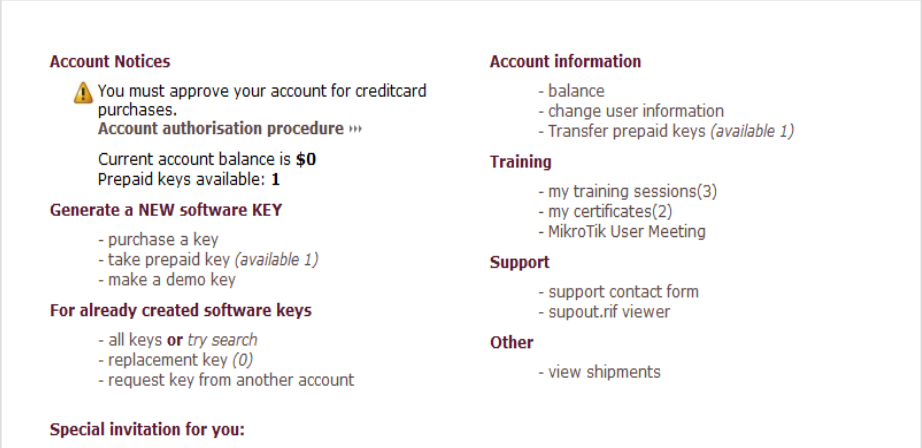


Figura 2.17. Panel de Administración de Cuenta Mikrotik.
Fuente: Los Autores, Administración de Cuenta Mikrotik, 2013

Siendo posible generar una licencia demo nivel 1 utilizando el Soft-ID visible en la pantalla inicial de RouterOS donde con todas las limitaciones de acuerdo a la tabla anterior presentada, se podrá evaluar la funcionalidad de RouterOS antes de la compra de una licencia de mayor nivel. Basta dar click en créate a demo key y con el Soft-ID del equipo a probar, posteriormente ingresar y evaluar su funcionamiento sin la molestia de las 24 Hras disponibles en su versión sin licencia.

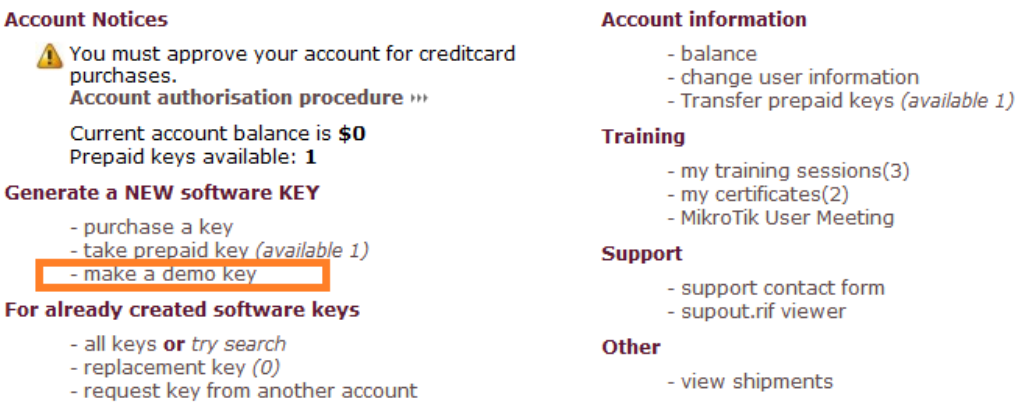


Figura 2.18. Creación de una llave demo desde la cuenta Mikrotik

Fuente: Los Autores, Administración de Cuenta Mikrotik, 2013

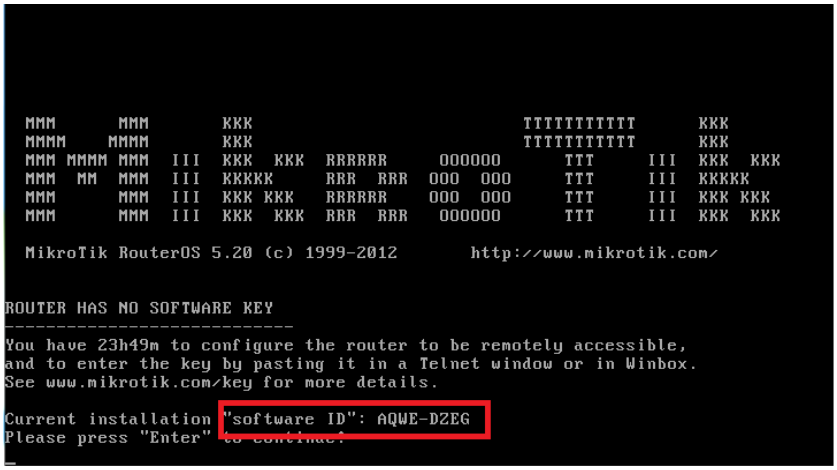


Figura 2.19. Visualización del Soft-ID en la Shell de RouterOS.

Fuente: Los Autores, Shell de RouterOS V.6.1, 2013

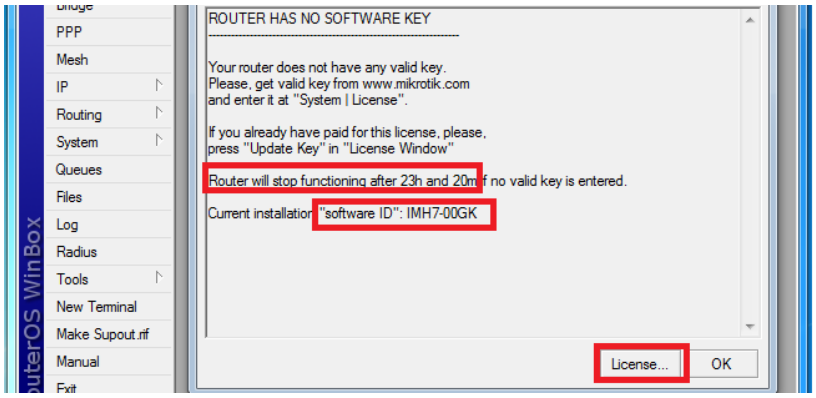


Figura 2.20. Mensaje de Aviso Winbox antes de pare de funcionalidad sin licencia.

Fuente: Los Autores, Winbox para RouterOS V.6.1, 2013

En el caso de querer realizar la compra dirigirse a la opción

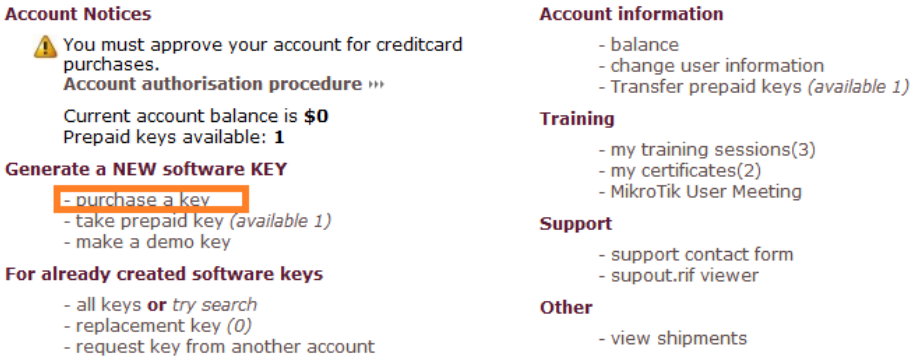


Figura 2.21. Crear una llave valida mediante un pago de la misma.

Fuente: Los Autores, Cuenta de administración Mikrotik, 2013

Luego se ejecuta el proceso de compra con las credenciales necesarias para la misma, seleccionando la licencia a adquirir y estableciendo el número de las mismas automáticamente se genera el total.

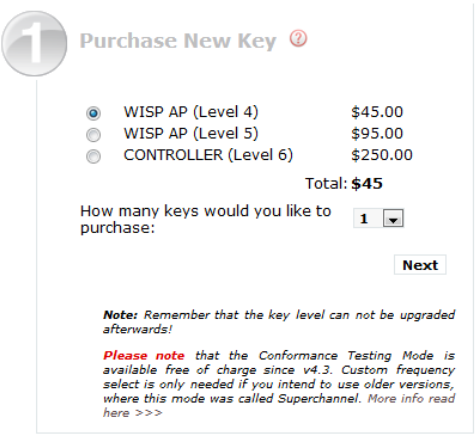


Figura 2.22. Procedimiento para compra de la llave.

Fuente: Los Autores, Cuenta de administración Mikrotik, 2013

En el siguiente paso es necesario que se introduzca el SoftID que como ya se lo ha mencionado en puntos anteriores, se visualiza al momento del Login en Router OS o desde Winbox abriendo una New Terminal.

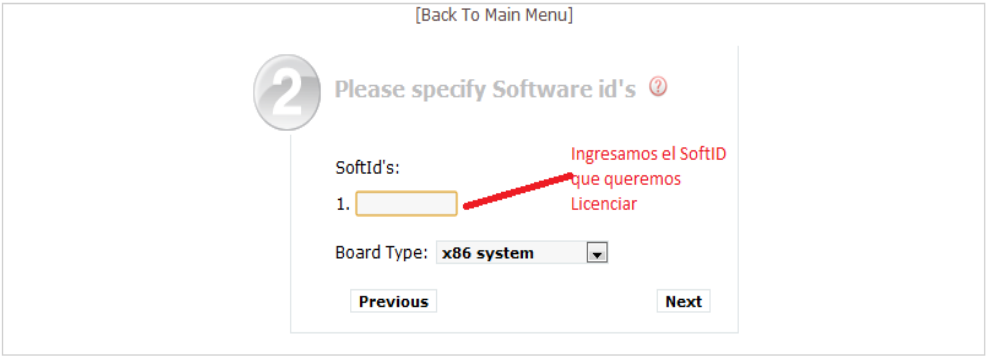


Figura 2.23. Introducción del Soft-ID para generar licencia validad.

Fuente: Los Autores, Cuenta de administración Mikrotik, 2013

Realizado el proceso de compra de la licencia, la misma se acreditara a la cuenta creada, luego se tendrá que tomar el Soft-ID para generar la licencia misma que será importada desde Winbox, desde la pestaña System >>> License, para ello se puede abrir la licencia desde un bloc de notas y seleccionarla toda completamente, realizar un ctrl + c, o copia y luego Winbox se encarga de pegar la misma por medio del import, validando la licencia y dejando de mostrar el tiempo de pare de funcionalidad y el nivel de licencia comprando.

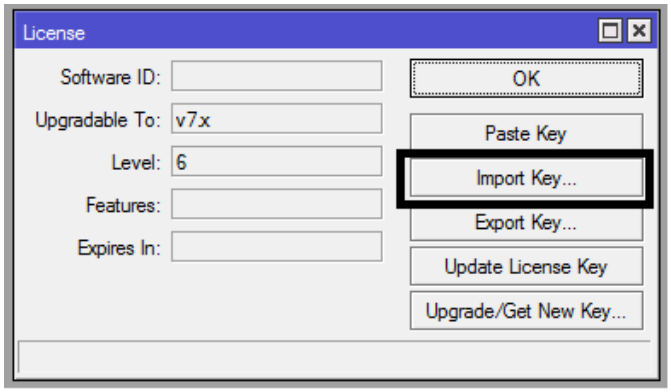


Figura 2.24. Importación de una llave valida desde Winbox.

Fuente: Los Autores, Winbox para RouterOS V.6.1, 2013

Por consola sería necesario arrastrar el archivo a la pestaña files y luego ejecutar el siguiente comando:

```
[RouterOS@RouterUPS] >system license import file-name=”NombreLicencia”
```

Entre las configuraciones básicas luego de la carga de licencia están:

En la pestaña System >>> Identity; especificar el nombre con el que será reconocido en la red el dispositivo y ante otros dispositivos RouterOS.

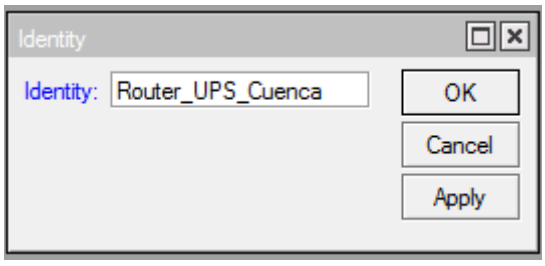


Figura 2.25. Asignación de Identidad al Router

Fuente: Los Autores, Winbox para RouterOS V.6.1, 2013

Por consola seria de la siguiente manera:

```
[RouterOS@RouterUPS] > system identity set name=Router_UPS_Cuenca
```

Si el equipo donde RouterOS es instalado no es un X86 y no dispone de una pila interna es necesaria la configuración de un cliente NTP para la obtención exacta de la hora, caso contrario este paso se podría omitir. Es importante sincronizar el Reloj interno del dispositivo no solo por sus configuraciones, ejecución de scripts o tareas sino para determinar posibles fallas a través de Log, para ello configurar en:
System >>> Clock; y seleccionar la zona horaria.

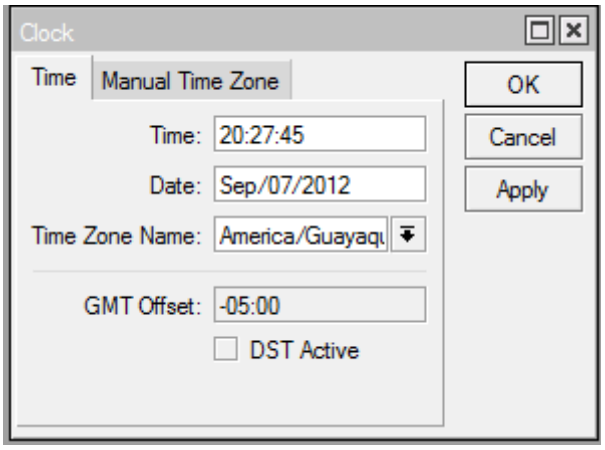


Figura 2.26. Asignación de Zona Horaria

Fuente: Los Autores, Winbox para RouterOS V.6.1, 2013

Comando por consola:

```
[RouterOS@RouterUPS] > system clock set time-zone-name=America/Guayaquil
date=
                                Sep/07/2012 time=20:27:45
```

Para que el proceso anterior tenga efecto es necesario sincronizar el NTP Client y así poder disponer de la hora exacta para ello lo hacer de la siguiente forma. System >>> NTP Client, y especificar las direcciones IP del servidor NTP por Ejm.

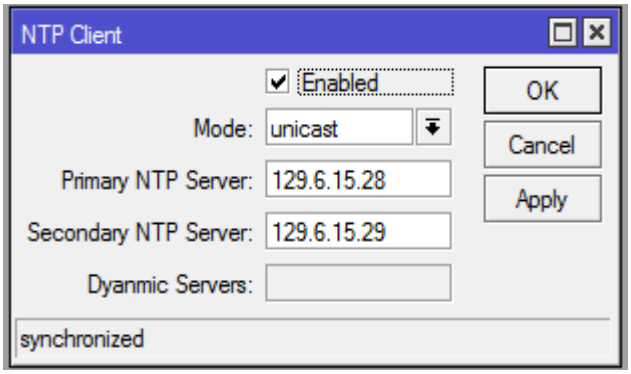


Figura 2.27. Asignación de NTP Cliente.

Fuente: Los Autores, Winbox para RouterOS V.6.1, 2013

Comando por consola:

```
[RouterOS@RouterUPS] > system ntp client set enabled=yes primary-ntp=129.6.15.
28 secondary-ntp=129.6.15.29 mode=unicast
```

2.2.2.4 ADMINISTRACIÓN DE ACTUALIZACIONES Y FORMAS DE OBTENERLO

Las actualizaciones tienen un esquema parecido a la administración de paquetes que se lo vera en el siguiente punto, es decir es necesario descargar desde la página oficial la actualización en formato en NPK de acuerdo a la arquitectura que se esté usando; es recomendable antes de proceder con la actualización revisar el changelog, que no es nada más que el documento de cambios y arreglos sobre la versión ya que en muchos casos en vez de mejorar el rendimiento puede terminar afectándolo, ya que una actualización es recomendable antes de catalogarse establece por la comunidad de testers haber transcurrido cierto tiempo.

Por ende se detalla el procedimiento de la siguiente forma:

1.-Descargar los archivos de actualización desde la página oficial, asumiendo que nuestra arquitectura de trabajo es en este caso PC / X86
http://www.mikrotik.com/download

Figura 2.28. Descarga de Actualización RouterOS para X86/PC

Fuente: Mikrotik, Actualización para RouterOS V.6.1, 2013, http://www.mikrotik.com/download

2.-Descargado el archivo entonces es necesario subirlo a RouterOS para proceder con la actualización, para esto se tiene varias formas la primera utilizando Winbox y otra utilizando un cliente FTP para subir la misma. Con Winbox simplemente basta con arrastrar el archivo de actualización a la pestaña Files y luego reiniciar el Router para constatar que dicho proceso sea haya realizado satisfactoriamente pudiéndolo verificar en la ventana inicial en la parte superior izquierda.

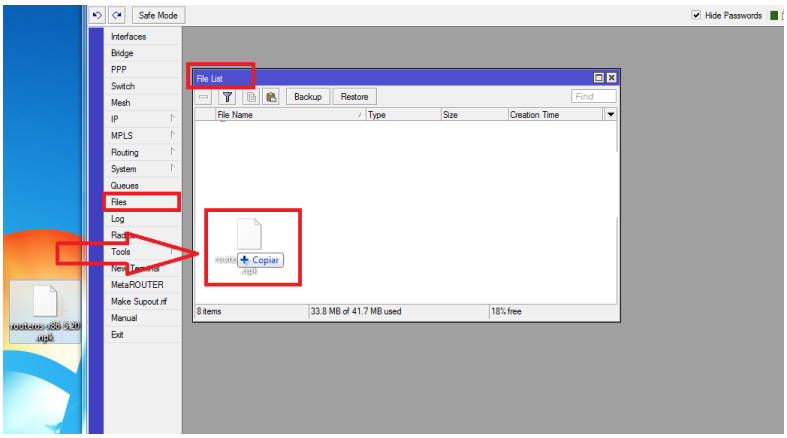


Figura 2.29. Actualización de RouterOS mediante archivo NPK y Winbox.

Fuente: Los Autores, Actualización para RouterOS V.6.1, 2013

3.-La forma alternativa podría usarse un cliente FTP o SFTP tales como Filezilla o WinSCP, en este módulo no se explica estas opciones pero son completamente validas igual en el proceso de actualización, la carga se realizaría con las herramientas antes descritas.

2.2.2.5 MANEJO DE PAQUETES DEL SISTEMA.

Las políticas de administración de paquetes dentro de RouterOS es altamente flexible, ya que si por algún motivo en la instalación inicial no se instaló alguno, es posible volver a instalarlo e incluso desinstalarlo con tan solo dirigirse a la página de Mikrotik y descargar el comprimido con los paquetes, luego seleccionar los paquetes a instalar y arrastrarlos hacia Winbox dentro de la pestaña Files, para proceder con la instalación, con los paquetes dentro de Winbox para empezar a disponer de ellos será necesario un reinicio del sistema y el mismo será agregado, además algo a tener en consideración especialmente con los RouterBoards, es necesario siempre realizar un proceso de verificación el espacio disponible en el disco ya que muchas veces puede ser una limitante para que dichos paquetes no sean instalados.

Por ende el procedimiento se establece de la siguiente forma:

1.-Descarga el comprimido de acuerdo a la arquitectura a instalar.

http://www.mikrotik.com/dowload

2.-El archivo por defecto tiene la extensión .zip, con nombre “All Packages”
3.-Descomprimir el archivo, seleccionar los paquetes a instalar y arrastrarlos a la pestaña files, programar un reinicio y verificar la instalación del paquete.
4.-Si la instalación no fue satisfactoria se debería tomar en consideración del punto anterior relacionado al espacio disponible.
5.-Verificar los paquetes instalados en Winbox desde la opción “Packages” o vía Shell utilizando el siguiente comando.

```
[RouterOS@RouterUPS] >system package print
```

2.2.2.6 PROCEDIMIENTO DE BACKUP Y RECUPERACIÓN.

Los procedimientos de “Respaldos - Backups” y recuperación en RouterOS hacen que las tareas del administrador sea mucho más fáciles en caso de desastres, migraciones o procesos de recuperación y contingencia, es posible disponer de “Respaldos” de configuraciones especificas o de determinados servicios de red como por ejemplo solo firewall, nat o encolamiento, etc. El propósito de los respaldos se centra en compilar en un archivo todas las configuraciones que necesitan ser respaldas, siendo posible editar el archivo y modificarlo a entero gusto, no en tanto para un Respaldo Global, el proceso implica generar un archivo donde se encuentren respaldadas todas las configuraciones de los diversos servicios y parámetros seteados sobre el Hardware y RouterOS a nivel Global, el mismo es un archivo binario y legible solo para RouterOS, para el caso de recuperaciones es importante tener en cuenta la versión de RouterOS sobre la cual se va a realizar la carga del Backup, ya que puede causar que el proceso de carga del respaldo no se realice adecuadamente o con errores. Para obtener un Backup Global, mediante Shell o Línea de comandos, se define la siguiente estructura de comando especificando al final del mismo el nombre que se le dará al archivo de respaldo.

```
[RouterOS@RouterUPS] > system backup save name=Global
```

En tanto para obtener una configuración de determinado servicio de red como por ejemplo el firewall navegar por la shell de la siguiente forma y utilizando el comando export se creará el respaldo solo de determinado servicio el mismo puede ser editable utilizando un editor de texto para modificar determinadas configuraciones en el caso

de ser necesario, más adelante serán explicados a detalle el uso de cada comando dentro de RouterOS.

```
[RouterOS@RouterUPS] > ip firewall filter export file=filter
```

Para el ejemplo anterior, la línea describe, utilizando el comando export respaldar todas las configuraciones en RouterOS dentro de "Filter" perteneciente al servicio "Firewall" cuyo nombre del archivo será filter, ejecutada esta línea de comandos podremos dirigirnos al Winbox a la opción Files y desde ahí arrastrar el archivo hacia cualquier ubicación dentro del ordenador, lugar donde se guardará el respaldo de dicho archivo.

En el caso de querer recuperar dicho archivo y las configuraciones específicas o globales en el mismo equipo u otro simplemente se invocaría el uso del comando import y previamente el archivo haya sido importado al Router a través de la pestaña Files y definiendo el nombre del archivo de Backup.

En el caso de una configuración especifica.

```
[RouterOS@RouterUPS] > ip firewall filter import file=filter
```

En el caso de una configuración global.

```
[RouterOS@RouterUPS] > system backup load name=Global
```

Incluso automatizar dichas actividades mediante el uso de scripts posibilitando el envío de dichos archivos a un servidor de correo o FTP, mismos que se detallarán más adelante y evitará a la larga muchos dolores de cabeza al administrador de red, por ende dicha parte debe ser tomada a consideración.

2.2.2.7 FIREWALL.

El Firewall en RouterOS es una implementación poderosa dentro de este segmento su función como ya se lo ha visto anteriormente es proteger el Router y la red de

clientes contra accesos no autorizados, y consiste en reglas definidas por el usuario que trabajan con el principio condicional:

SI (COINCIDE >>> ENTONCES)

Todas las reglas son ordenadas en cadenas para facilitar la administración de las mismas de manera más ordenada, aquí mantener el orden es muy importante ya que RouterOS procesa cada regla desde el inicio al final en forma ordenada, por lo tanto se afirma que hay cadenas predefinidas (las establecidas por RouterOS) y las cadenas creadas por el usuario. (Se puede crear cadenas adicionales a partir de las cadenas por defecto)

RouterOS utiliza las siguientes 3 cadenas por defecto que son:

INPUT: Procesa paquetes que tiene como destino el Router.

OUTPUT: Procesa paquetes enviados del Router.

FORWARD: Procesa paquetes que atraviesan el Router.

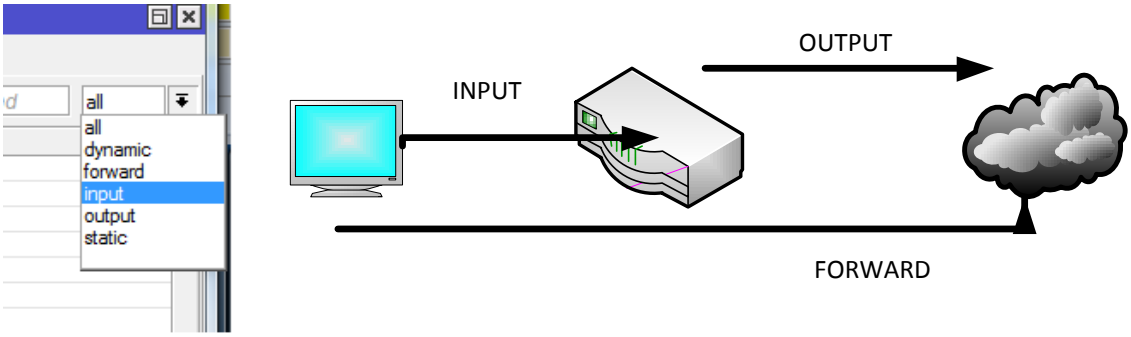


Figura 2.30. Esquema General de cadenas Firewall en RouterOS.

Fuente: Los Autores, Winbox opción Firewall V.6.1, 2013

Las cadenas INPUT contiene reglas de filtrado que protegen al Router, en cambio las cadena FORWARD contiene las reglas que controlan los paquetes que atraviesan el Router, y las OUTPUT las que salen del Router, por ende para entenderlas un poco mejor y comprender lo explicado es necesario visualizar el siguiente diagrama simplificado del Firewall de RouterOS.[15]

[15] Mikrotik, Packet Flow Firewall, 19 de Marzo del 2013, http://wiki.mikrotik.com/wiki/Manual:Packet_Flow

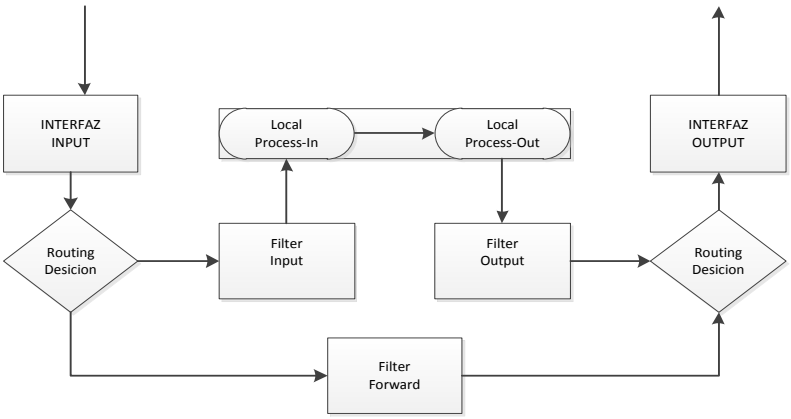


Figura 2.31. Diagrama simplificado de Firewall

Fuente: Mikrotik, Packet Flow Firewall, 2012, http://wiki.mikrotik.com/wiki/Manual:Packet_Flow

Las tácticas conocidas a nivel de Firewall son:

- Bloquear lo conocido y aceptar el resto.
- Aceptar lo conocido y bloquear el resto.

2.2.2.8 ADMINISTRACIÓN DE ESTADO DE CONEXIONES.

Es importante saber que muchas de las conexiones generadas desde o hacia el Router son rastreadas utilizando el administrador de estado de conexiones, conocido con el nombre de Connection-Tracking es el corazón del Firewall, y se encarga de recopilar o manejar todas las conexiones, cada entrada generada en la tabla representa un intercambio bidireccional de datos, este módulo usa muchos recursos de la CPU, pero sin embargo puede ser de gran utilidad para detección de anomalías dentro del Router, es posible desactivarlo pero de hacer ello la opción de Nat en el Router se desactivaría.

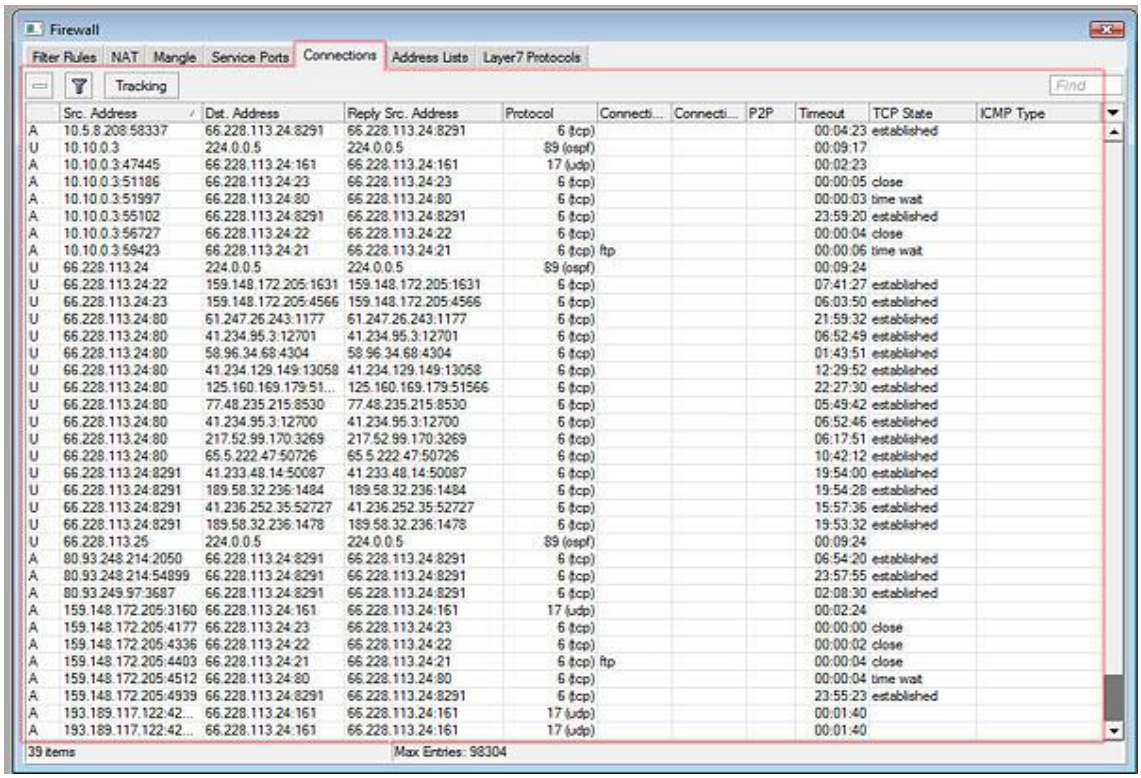


Figura 2.32. Estado de Conexión (Connection Tracking)

Fuente: Los Autores, Estado de Conexion, 2013

También existen tareas necesarias básicas a realizar para que un firewall este optimizado en referencia a sus conexiones:

- Es necesario agregar una regla de eliminación para todas aquellas conexiones inválidas, luego para las conexiones establecidas que las mismas sean aceptadas y finalmente relacionadas de la misma forma, dejando que el firewall opere solo con las conexiones nuevas y evite carga de procesamiento innecesaria, para lograr ello utilizar el parámetro connection-state en la categoría Firewall >> Filter que permitirá realizar dicha tarea.

- Otra opción relevante es el mantenimiento que se le dé al mismo, es importante documentar cada regla agregando un comentario, en cada regla, verificar las estadísticas generadas por cada una, es una buena opción para determinar si la misma está cumpliendo con el propósito establecido, ubicando correctamente cada una en el orden correspondiente para que sea ejecutada, así como también es importante utilizar la acción Log en

determinados casos para tener datos más específicos ante cualquier vulnerabilidad o error.

2.2.2.9 CALIDAD DE SERVICIO EN UN WISP.

En la actualidad la convergencia de servicios en la red es decir el tráfico de voz, video y datos sobre una misma infraestructura han exigido que muchos de los proveedores de Internet adapten sus redes para poder brindar un servicio eficiente, el tema calidad de servicio toma más relevancia incluso en un WISP ya que el medio de última milla hacia el cliente es inalámbrico, aunque ahora la diversa variedad de productos existentes y las técnicas de control de acceso al medio empleadas para optimizar el espectro no garantizan un servicio como el cableado, el objetivo es mitigar al máximo siempre las congestiones y asegurar un óptimo servicio.

Es necesario realizar un plan de calidad de servicio adaptado a las necesidades de la red, y considerando parámetro tales como pérdida de paquetes, Jitter, Latencia, Througput, Uptime, y protocolos a priorizar, que más tarde permitan aplicar las técnicas necesarias para la aplicación de QoS sobre la red de datos.

La regulación del servicio de Internet en cualquiera de los proveedores de Internet es completamente necesaria y debe cubrir siempre aspectos tales como precio, acceso y calidad, que necesitan ser correctamente direccionados para levantar una política de QoS viable, buscando como fin una red de datos altamente eficiente.

2.2.2.10 PROTOCOLOS DE ENRUTAMIENTO.

Los protocolos de enrutamiento son considerados como un conjunto de reglas a base de algoritmos de enrutamiento tanto en Hardware como Software para un Router, que especifican la forma o esquema de comunicación entre dos o más Routers, con el propósito de poder compartir información detallada o no de enrutamiento, tanto al interior(administrando redes dentro de un único sistema autónomo como: RIP, EIGRP, IGRP y OSPF) como al exterior(encargado de manejar rutas que conectan con diferentes sistemas autónomos como: BGP o EGP), considerando un sistema autónomo (SA) como un determinado grupo de redes, o routers que mantienen una

política de enrutamiento en común bajo una administración de igual forma y permitiendo decidir cuál es la mejor ruta que debe seguir un datagrama o paquete para llegar a su destino.

Los protocolos de enrutamiento se clasifican en:

Protocolo	Descripción
Estático	La gestión de rutas son manejadas manualmente por un administrador de red, que es el encargado de introducir las políticas de enrutamiento en un Router, además dicho enrutamiento necesita de un mantenimiento constante en el caso de actualizaciones e ingreso de nuevas rutas sobre la topología de red, su uso se aplica idealmente cuando no existen rutas con redundancia, o incluso cuando las redes son pequeñas, entre sus características relevantes se encuentra que es: Seguro, adecuado para topologías simples, no hace uso de excesivos recursos del hardware, y no requiere conocimientos avanzados.
Dinámico	Es un protocolo versátil cuyas rutas son construidas por información intercambiada entre los diversos protocolos de enrutamiento, mismo que se encargan de distribuir información que dinámicamente ajustan las rutas reflejadas sobre la red, tales como en el caso de redes con múltiples caminos a un mismo destino pueden requerir el uso de un protocolo de enrutamiento dinámico, ya que incluso su tiempo de respuesta es mucho más rápido que si un administrador lo estuviese haciendo de forma estática, entre sus características relevantes se encuentra que es: Adecuado para topologías simples y complejas, además que se adapta a los cambios de la topología de forma

	automática.

Tabla 2.7. Clasificación de los Protocolos de Enrutamiento.

Fuente: Deepankar Medhi, "Network Routing:Algoritms, Protocols and Arquitectures", Morgan Kauffman, 2007, p56

La clasificación de los protocolos de enrutamiento se especifica de la siguiente forma:

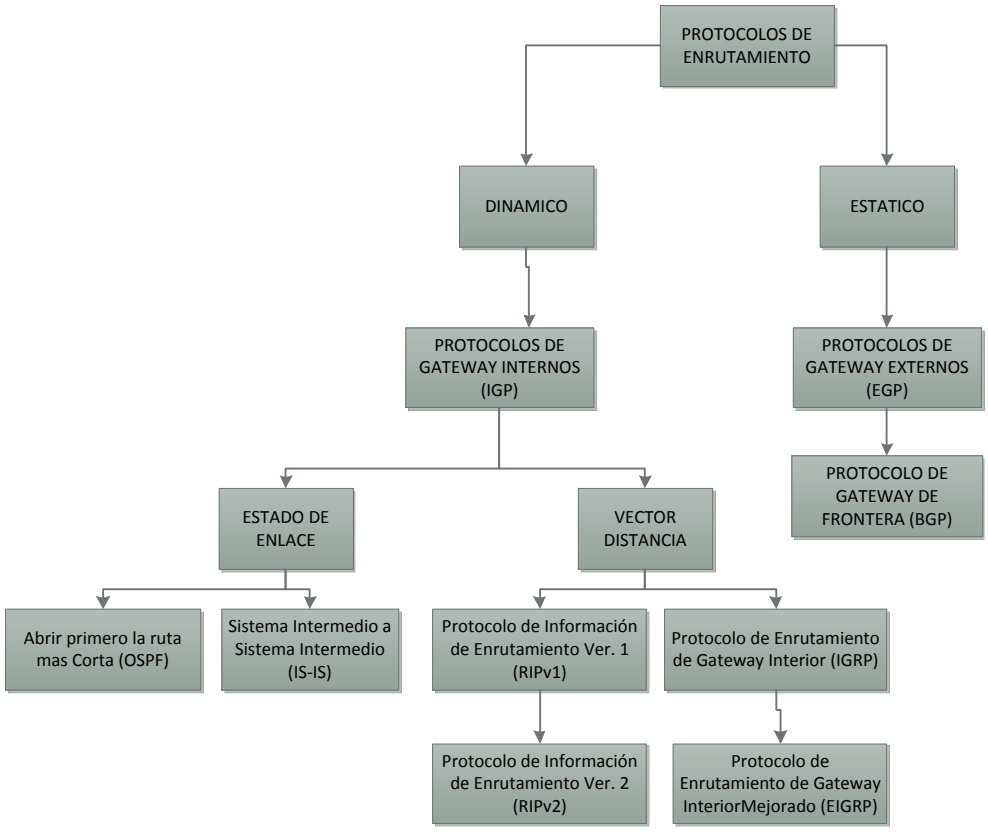


Figura 2.33. Clasificación de los Protocolos de Enrutamiento

Fuente: Deepankar Medhi, "Network Routing:Algoritms, Protocols and Arquitectures", Morgan Kauffman, 2007, p56

2.2.2.10.1. OSPF como protocolo de enrutamiento en un WISP, aspectos generales, funcionamiento y ventajas.

- **Aspectos Generales.-**

Se lo conoce como Open Short Path First, es un protocolo de enrutamiento interno creado en respuesta a necesidades presentes por parte de R.I.P, pensado para distribuir información de rutas entre Routers que pertenecen a un mismo Sistema Autónomo implementado generalmente en redes corporativas medianas, grandes o de cualquier tipo y envergadura. Su uso en entornos como los proveedores de servicios inalámbrico WISP generalmente era mínimo hasta hace algunos años atrás debido a su escaso conocimiento y alta complejidad de configuración requerida, o bien al alto costo que implicaba levantar dicha protocolo sobre la red.

Entre sus aspectos generales se detallan los siguientes:

- Protocolo estándar de enrutamiento interior basado en el RFC2328.
- Opera como protocolo de estado de enlace a nivel de protocolo de enrutamiento.
- Hace uso del algoritmo Dijkstra para calcular la ruta más corta a su diferente red de destino.
- Implementable sobre cualquier red de todo tipo y tamaño, aun así sin demandar una configuración más compleja que otros protocolos.
- Su métrica de enrutamiento se considera como el costo de los enlaces, parámetro calculado en función del ancho de Banda.
- Establece adyacencias con los dispositivos vecinos, enviando periódicamente paquetes HELLO.
- Es de estándar abierto, permitiendo estar disponible en casi cualquier Sistema Operativo que opere a nivel de red, tales como: Cisco, Linux, RouterOS, Windows Server etc.
- Cuando un enlace cambia de estado, dicho protocolo inunda la red notificando dicho cambio, así como cada 30 minutos envía a los dispositivos vecinos una actualización de contenido de todos los cambios de estado.

Entre sus ventajas se puede considerar:

- No esta propenso a bucles de enrutamiento.
- Puede soportar VLSM y CIDR.
- Altamente escalable incluso en redes de gran tamaño.

- Converge con mucha más rapidez que los protocolos de vector distancia, enviando actualizaciones pequeñas que no implican enviar toda la tabla de enrutamiento
- Diseñado para adaptarse al máximo a los protocolos TCP/IP.
- Los mensajes OSPF se encapsulan en datagramas IP, como protocolo de transporte numero 89 (TCP=6, UDP=17).

Su funcionamiento general se describe como:

OSPF como protocolo de estado de enlace se fundamenta en la existencia de un mapa de la red el cual es poseído por todos los nodos y que es actualizado periódicamente, siendo necesario que la red pueda almacenar en cada nodo el mapa de la red, y lo esencial que ante cualquier cambio en la estructura de la red poder actuar rápidamente, evitando así el riesgo de la creación de bucles y teniendo en cuenta posibles particiones o uniones de la red.

Cada Router con OSPF habilitado gestiona una tabla donde, las filas representan a un Router de Red; y todo cambio que se materialice sobre dicho dispositivo se verá reflejado en el registro de la tabla por medio de los registros de descripción, no en tanto las columnas representan los atributos de un Router que son almacenados por cada nodo, siendo los principales atributos de cada nodo: El número de Enlace, la métrica y un indicador de interface.

Con toda esta Data en cada Router el objetivo se centra en que cada Router sea capaz de administrar su propio mapa de la red, evitando así como ya se mencionó anteriormente problemas muy relevantes como la creación de bucles.

- Para el descubrimiento de vecinos se encarga la tarea al protocolo HELLO, mismo que es el encargado de llevar dicho mensaje a otros Routers OSPF conectados a su misma subred.
- Se ejecuta el intercambio de la base de datos topológica de OSPF:DB Link-state, donde cada router mantiene dicha información de estado de

enlaces con la topología completa de cada router, dichas tablas principales son:

- Router Link State: Información de cada una de las interfaces de todos los Routers.
- Network Link State: Información de las subredes a las que están conectados, todos los RouterOSPF

- El algoritmo Dijkstra procesa localmente la tabla de enrutamiento partiendo de la Base de datos de la topología de la red.
- Si se dan cambios en la topología, se envían mensajes del estado del enlace con información sobre los vecinos. [16]

Uso en un WISP.-

OSPF es y ha sido un protocolo de enrutamiento cuyas bondades y características hablan por sí solas, su lenta adopción anteriormente se debía a los elevados precios en Hardware para su implementación y terminales o CPE que lo soporten, y quizá de cierta forma el grado de complejidad y conocimiento que demandan para su puesta en marcha eficiente, es así como muchos WISP en sus inicios, incluso algunos hasta la actualidad han mantenido redes de datos sin una arquitectura de operación definida, siendo netamente grandes bridges lógicos, asociados a las problemáticas que ello conlleva. La adopción del protocolo aún no se da en su totalidad en los proveedores de servicio de Internet Inalámbricos o WISP, pero eso no implica que muy pronto se empiece a ver dicha transacción en progreso, debido a que Mikrotik está poniendo dicha tecnología al alcance de todos y volviéndola lo más asequible posible con su diversidad de productos RouterBoard que mes a mes se incrementa más y más.

[16] Routing in the Internet Second Edition",Christian Huitema, Pretince Hall, 3 de Diciembre del 1999.

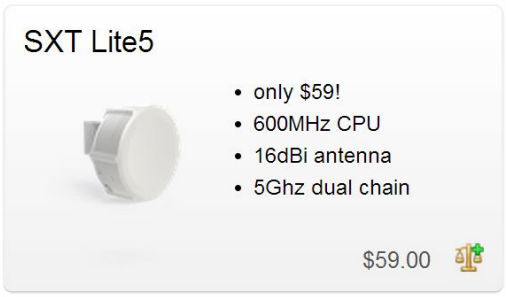


Figura 2.34. CPE RouterBoard Modelo SXT Lite 5 Ghz con RouterOS y soporte OSPF

Fuente: Mikrotik, Lista de Productos RouterBoard, 2013, http://www.mikrotik.com/

Por tal razón Sigsignet no ha decido quedarse atrás y OSPF es una de sus implementaciones a quedar funcionales a corto plazo, aunque ello implica el cambio físico de equipamiento en los Nodos con soporte para dicho protocolo que se describirán en capítulos posteriores.

2.2.2.10.2. MPLS, aspectos generales, funcionamiento y ventajas.

En este subcapítulo se va a hablar de una técnica de transporte de data denominada MPLS cuyas siglas denotan (Multiprotocol Label Switching), el objetivo no es tratar de ahondar en dicho subtema ya que el mismo comprende un tema de estudio sumamente amplio por ende se va a considerar los puntos más relevantes de este subtema, aplicándolos al proceso de restructuración dentro de la empresa Sigsignet; en si MPLS es un mecanismo de transporte de datos bajo RFC 3031, que dentro del modelo OSI trabaja a nivel de la capa de enlace de datos y la capa de red, siendo uno de los modelos de transporte que hasta la actualidad otorga gran nivel de rendimiento.

MPLS desde ya hace algunos años atrás es una tecnología que aún se encuentra en adopción pero cuyos beneficios se pueden palpar, no solo por el alto rendimiento que este tipo de redes acumulan sino por su gran versatilidad y escalabilidad, se la considera una red privada IP, que conjuga la gran ventaja de las comunicaciones PTP o mejor conocida como punto a punto sin olvidar la capacidad para ofertar niveles de

rendimiento diferenciados, priorización del tráfico, aplicaciones de voz y multimedia establecido todo en una misma red.

Entre sus principales características y ventajas se denotan las siguientes:

- Uso de una infraestructura de red unificada.
- Flujo de tráfico óptimo.
- El proceso de "Forwarding" de paquetes se basa en el contenido de una "etiqueta", en lugar de realizar un proceso complejo de lookup basado en IP destino.
- Soporte para ingeniería de tráfico.
- Los servicios basados en MPLS pueden reducir costes, frente a tecnologías como Frame Relay y ATM, alcanzado niveles de hasta un 40%.
- Recuperación ante desastres, ya que soportan conexiones redundantes a la Nube MPLS, y a través de ella, a otros sitios de red.
- MPLS intenta conseguir las ventajas de ATM, pero sin sus inconvenientes.
- Se asigna una etiqueta a los datagramas de cada flujo una etiqueta única que permite una conmutación rápida en los Routers intermedios.
- Las etiquetas son inyectadas entre en el encabezado de capa 3 y el encabezado de capa 2.

Funcionamiento.-

Una red con soporte para MPLS, funciona cambiando las etiquetas sobre un paquete con una etiqueta ya establecida. Cuando se envía un paquete desde un punto A hasta un punto B por una ruta MPLS se define el siguiente recorrido.

El funcionamiento Básico de MPLS se establece de la siguiente forma:

- Crear y distribuir las etiquetas entre los Routers.
- Creación de tablas en cada enrutador.
- Creación de LSP (Label Switched Path).

- Agregar etiquetas a los paquetes con la información de la tabla.
- Envió del paquete.

Los elementos que intervienen en la comunicación son:

LER (Label Edge Router).- Establecidos a los extremos de la red MPLS, Inicia o termina el túnel, establece o remueve cabeceras, se entiende como el elemento de entrada/salida en la red MPLS, conocido como Ingress Router al dispositivo de entrada, y al Egress Router como el dispositivo de salida, y se los conoce como LER.

LSR (Label Switching Router).- Componente encargado de conmutar las etiquetas.

LSP (Label Switched Path).- Se le conoce como un camino unideraccional MPLS determinado para cierto tráfico o FEC, un túnel definido entre los extremos.

LDP (Label Distribution Protocol).- Protocolo encargado de la distribución de etiquetas MPLS entre los equipos de la red.

FEC (Forwarding Equivalence Class).-Trafico asociado y que viaja encaminado bajo una etiqueta.

2.2.2.10.3. Calidad de servicio en MPLS

Cada día las redes IP van centrando sus esfuerzos en quizá antes lo que se consideraba un aspiración un tanto desmesurada y fuera de lo común, donde se afirmaba la convergencia de todos los servicios de telecomunicaciones; hoy en día prácticamente dicha idea ha cambiado a tal punto que la convergencia de servicios se está dando a un nivel tan amplio que incluso ya la podemos palpar, tal es así que hoy por medio de la línea de acceso a datos o internet se disfruta de múltiples servicios tales como TV, Telefonía, Internet, Video Conferencias entre otras cosas, quizá en sí porque los diversos ISP quieren mitigar en cierta parte las inversiones realizadas en infraestructura.

Si bien antes la red durante sus inicios mantenía un alto grado de subsidio hoy el panorama ha cambiado a tal punto que los servicios de transporte de información

tiene un costo, mismo que muchas de las veces se torna difícil de cuantificar cuando no es posible asegurar una calidad de servicio adecuada.

MPLS al ser hoy por hoy un protocolo con altas expectativas en mejora de performance sobre redes IP, desde su concepción en de la década de los 90, es el que hasta hoy mejores resultados ha demostrado sobre redes IP.

Una arquitectura MPLS está definida bajo el RFC 3031. Y se compone de los Label Edge Router situados en la frontera de la red y mejor conocidos como LER, así como los LSR (Label Switched Router) o denominados enrutadores, y su funcionamiento es asignarse a las tramas que circulan por la red una identificación que se le indique a los Routers una ruta que los datos deban seguir.

La calidad de servicio sobre una red MPLS es quizá tan relevante como una red convencional IP, el hecho de que MPLS otorgue notables mejoras sobre la capa de transporte no significa que no necesite calidad de servicio, al contrario la aplicación de este es muy relevante pudiendo aplicar calidad de servicio bajo este protocolo, siendo netamente considerada la calidad de servicio como la habilidad de la red para administrar determinados servicios por cierto tráfico que utilicen un grado de priorización permitiendo evitar congestiones y cuellos de botella y así poder brindar un servicio de calidad. Por lo tanto se consideran 3 tipos de calidad de servicio de acuerdo a como las aplicaciones permiten la transmisión de datos tal como en un modelo de servicio diferente se lo aplicaría en un escenario donde exista transmisión de datos como audio, videoconferencia incluso telefonía IP, así como se aplicaría para otro modelo tal es el caso de transferencia de archivos y relacionados, por lo tanto se definen los siguientes modelos de Calidad de Servicio:

- **BestEffort (Mejor Esfuerzo).-** Utiliza el tipo de encolamiento FIFO, y no garantiza el arribo de los datos a su destino, aplicando dicho método se considera que todos los usuarios reciben el mejor servicio posible.

- **IntServ (Servicio Integrado).-**Se establece como un método que garantiza una calidad de servicio, ya que de cada extremo tanto del que envía como el que recibe datos realiza reservas de recursos.

- **DiffServ (Servicios Diferenciados).-** Un método aplicado a redes de gran tamaño, analizando varios flujos de datos al mismo tiempo, estableciendo negociaciones llamadas como Acuerdos de Nivel de Servicio (SLA) donde se establecen las clases de tráfico que serán provistos y garantías otorgadas por cada una de ellas.

Además se puede establecer un mecanismo de Calidad en servicio en MPLS que hacen posible que la misma sea altamente eficiente, determinado para tal cinco consideraciones a tomar en cuenta que son:

- **Control Latencia.-** Consiste en establecer colas para administrar el tráfico sobre una Interfaz, estableciendo el tráfico en cada cola identificando antes que nada el tipo de tráfico.
- **Anulación de Latencia.**-En el caso de colas llenas este mecanismo empieza el descartado de paquetes sobre las colas al momento de encontrarse estos llenos.
- **Control de Admisión.**-Mecanismos que filtran un tráfico especifico, basados en las características que este muestra.
- **Acondicionamiento de tráfico.**-Se encargan de limitar el tráfico a un determinada velocidad o incluso lo encola en base a los diferentes algoritmos existentes para cumplir dicha tarea.
- **Control de eficiencia de enlace.**-Permite el incremento de performance del enlace utilizando tanto técnicas de comprensión de cabecera de paquetes como fragmentado de los mismos, con el único fin de volver al medio lo más eficiente posible.

2.2.2.11 ROUTEROS COMO ADMINISTRADOR DE ANCHO DE BANDA EN UN WISP

RouterOS hoy por hoy es quizá de las soluciones con una relación beneficio/costo altamente competitiva en comparación con otras soluciones propietarias presentes en

el mercado así también su progresivo desarrollo, soporte y versatilidad sobre la solución la están convirtiendo cada día más en una plataforma altamente eficiente.
Pero la pregunta radica en ¿Por qué se está volviendo tan popular RouterOS como administrador de Ancho de Banda? Lo hace en primer lugar como ya se mencionó por su relación beneficio/costo, segundo su elaborado desarrollo e incluso algoritmos propietarios para administrar el ancho de banda que hacen que RouterOS sea considerada como una solución altamente eficiente, tercero su facilidad de configuración, atrás quedaron quizá aquellos días donde prácticamente casi todas las configuraciones se las hacia mediante una consola aunque con ello no se afirma que ninguna configuración se lo pueda hacer mediante esta vía, al contrario queda a elección del usuario definir la mejor vía de configuración dentro de RouterOS y finalmente su alto nivel de integración con Sistemas Externos por medio de su API posibilitando elaborar soluciones Ad-Hoc con un alto nivel de rendimiento dentro de este campo.

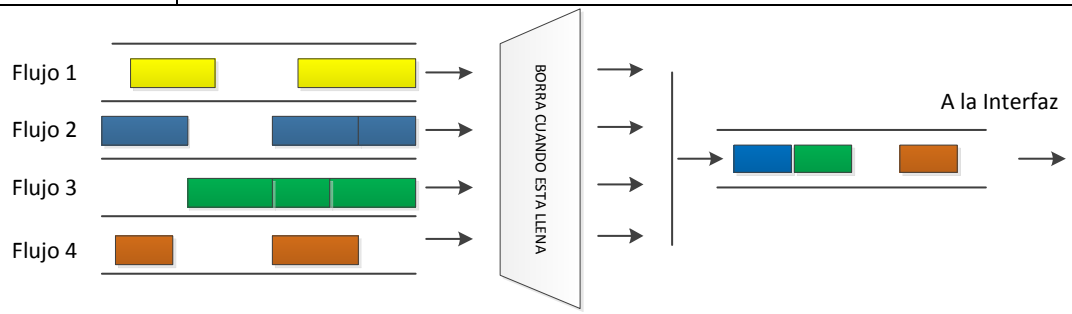
En si quizá el administrador de ancho de banda es el talón de Aquiles de cualquier empresa de tipo WISP, pero por medio de RouterOS y si se lo sabe aplicar y configurar de momento será una solución que beneficiará significativamente, para tal en RouterOS se puede utilizar las diversas formas de encolamiento y algoritmos que permitirán establecer políticas de administración del ancho de banda efectivas.

Es importante recalcar que las colas en RouterOS son utilizadas para limitar e incluso priorizar el tráfico, pudiendo establecer límites por direcciones IP, subredes, protocolos, puertos y parámetros adicionales con un marcado previamente establecido para su posterior tratamiento, incluso como límites en función del tiempo, puntos determinante que en un ISP son altamente usados.

RouterOS basa sus políticas de administración de Ancho de Banda bajo un algoritmo de amplio uso en entornos Linux con ciertas mejoras de por medio conocido como HTB (Hierachy Token Bucket), que aparte de distribuir el tráfico, utiliza una Jerarquía de colas y su relación. En los siguientes puntos se explicará cuáles son los mecanismos con los que RouterOS trabaja y un repaso breve a su funcionamiento.

2.2.2.11.1. Algoritmos de Encolamiento.

Conocidos también en su término inglés como Queuing, es un mecanismo aplicado en el control de ancho de banda o paquetes dentro de RouterOS, que retrasa, varia, o entrega oportunamente un caudal de paquetes encolados en una interfaz, y apoya las siguientes disciplinas:

Tipo Queue	Descripción
Bfifo	Es una disciplina de encolamiento avanzada basada en fifo (Primer en Entrar Primero en Salir) de tipo Scheduler, poco conocida que permite limitar y priorizar el tráfico reordenando el flujo de paquetes, su función es limitar paquetes mas no velocidad, este tipo de encolamiento se mide en bytes.
 **Figura 2.35. Modelo de Encolamiento BFIFO.** **Fuente:** Mikrotik, Queue Type, 2013, http://www.mikrotik.com/	
Mq pfifo	Permite el soporte para múltiples colas de transmisión, así mismo está basando en fifo (Primer en Entrar Primero en Salir), es beneficioso en interfaces Ethernet con soporte y driver para dicho encolamiento.
Pcq	Conocida como (Per-Connection Queueing), es disciplina de encolamiento de tipo shaper ampliamente usada en los proveedores de Internet destinada a controlar la velocidad del flujo datos, permiten subdividir el ancho de banda general o total de forma equitativa y en función de la demanda o incluso de acuerdo al número de usuarios o por interfaz.

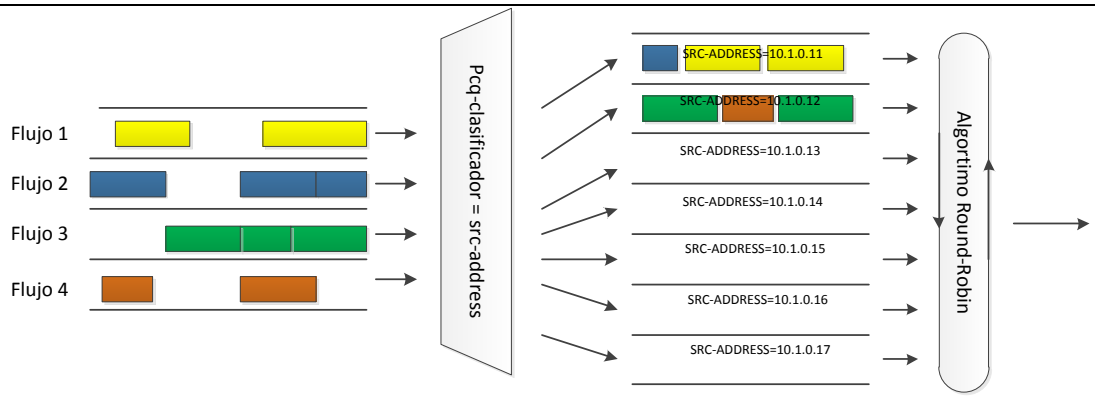


Figura 2.36. Modelo de Encolamiento PCQ.

Fuente: Wiki Mikrotik, Queue Type, 2013, http://www.mikrotik.com/

Pfifo	Es una disciplina de encolamiento avanzada basada en fifo (Primer en Entrar Primero en Salir) y quizá poco conocida que permite limitar y priorizar el tráfico, pero que se mide en paquetes.
Red	Conocida como (Random Early Detection), permite el descarte aleatorio temprano de paquetes, encola tanto paquetes como pueda y simplemente borra los que no se pueda encolar, se lo puede considerar también como de tipo Scheduler actuando como un encolamiento a nivel de reordenar paquetes.

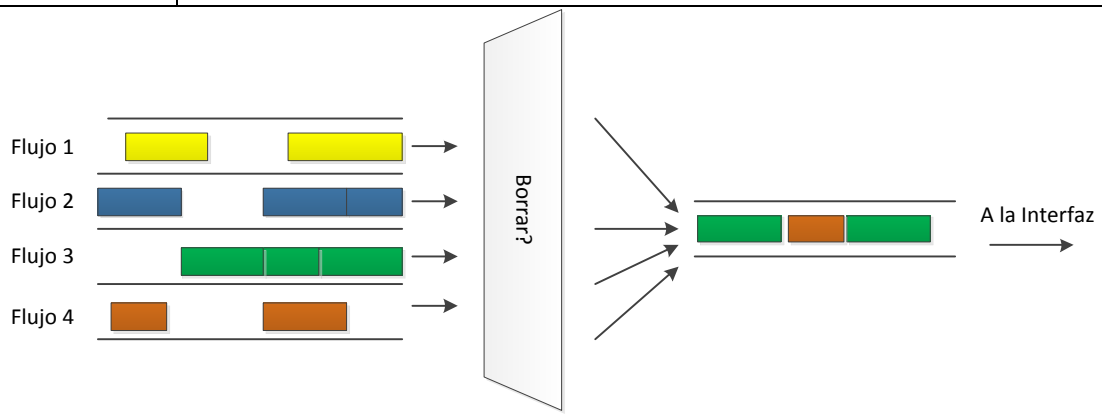


Figura 2.37. Modelo de Encolamiento RED.

Fuente: Wiki Mikrotik, Queue Type, 2013, http://www.mikrotik.com/

Sfq	Conocida como (Stochastic Fairness Queuing Server), es un algoritmo de cola justo, diseñado para prevenir que un solo flujo se apodere del uso de la red, utilizando para ello un algoritmo Round Robin (WRR)

	que le asigna un turno a cada flujo para su respectiva salida de la cola.

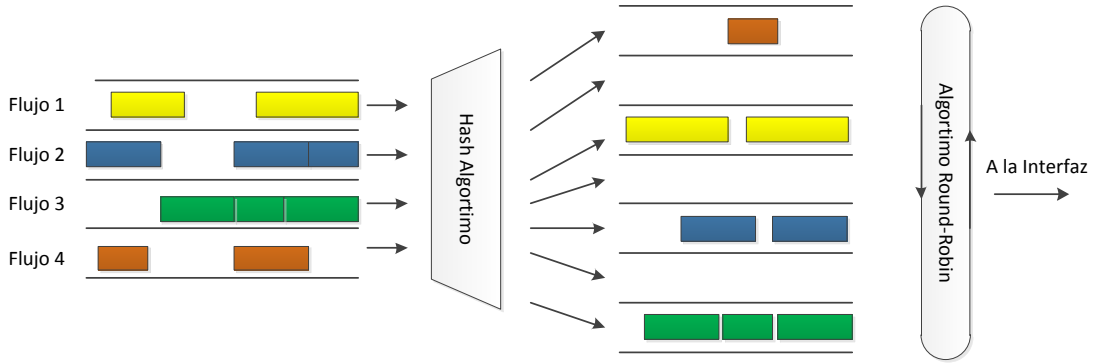


Figura 2.38. Modelo de Encolamiento SFQ.

Fuente: Wiki Mikrotik, Queue Type, 2013, http://www.mikrotik.com/

Tabla 2.8. Tipo de Queues

Fuente: Mikrotik, Queues, 2013, http://wiki.mikrotik.com/wiki/Manual:Queue

Para entenderlo más a detalle se los podría clasificar de la siguiente manera:

Tipo Shaper: Destinados a controlar la velocidad del flujo de Datos dentro de esta disciplina se encuentran:

- PCQ
- HTB

Tipo Scheduler: En cambio estos se destinan a reordenar y limita el flujo de paquetes, más no la velocidad y dentro de esta disciplina se encontrarían los siguientes algoritmos.

- RED
- FIFO
- SFQ

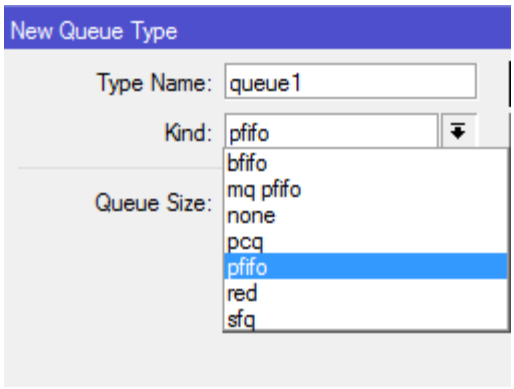


Figura 2.39. Tipos de Encolamiento Disponibles en RouterOS.

Fuente: Los Autores, Queue Type, 2013.

Así mismo es importante acuñar términos relevantes dentro del control de tráfico como son:

- **Scheduling.-** Mecanismo que permite ordenar o desordenar los paquetes antes de ser encolados tanto al ingreso como salida de la cola.
- **Shaping.-** Es el encargado de retardar los paquetes para poder satisfacer con una velocidad dada.
- **Classifying.-** Conocidos como clasificadores, encargados de ordenar o separar el tráfico entre colas con el fin de tener diferentes tratamientos e incluso diferentes colas de salida.
- **Policing.-**O también llamados "Policers" encargados de limitar y medir el tráfico de una cola específica, en si no es más que un mecanismo basado en algoritmos que limitan el tráfico, por ejemplo en el caso que este exceda una velocidad fijada o incluso que el trafico sea descartado.
- **Dropping.-** Descarte de paquetes, un flujo o una clasificación.
- **Making.-** O marcado de paquetes consiste en establecer marcas dentro de un paquete, para su posterior uso y tratamiento incluso con otros routers de un mismo dominio administrativo.

2.2.2.11.2. Colas Simples.-

Antes de empezar con la temática de colas simples es necesario recalcar que parte del software de RouterOS está compuesto por soluciones Open Source debidamente trabajadas e incluso, mejoradas y adaptadas, en el caso del encolamiento por medio de colas simples se debe mencionar que el mismo está basado en HTB(Hierarchical Tocken Bucket) que es un mecanismo que permite limitar o dividir el ancho de banda tanto para una o múltiples direcciones IP y subredes. Desde RouterOS se puede realizar incluso configuraciones un tanto más elaboradas, desde especificar incluso tiempos de ráfaga que son incrementos en el caudal de paquetes durante breves lapsos de tiempo programado e incluso trabajar con algoritmos de encolamiento, los cuales se han mencionado anteriormente, quizá uno de los mayores inconvenientes que tenía hasta la versión 5.X es que con cientos de reglas de encolamiento, el equipo empezaba a perder rendimiento por lo tanto requería disponer de un hardware altamente eficiente, ya que el proceso de ejecución y cumplimiento de cada regla dentro de Mikrotik es secuencial, provocando muchas de las veces en hardware con escasos recursos pero con alto número de usuarios deje de funcionar adecuadamente, incluso ahora RouterOS en sus nuevas versiones 6.X es ya posible elaborar un proceso de doble encolamiento esto quiere decir que ahora se puede realizar un marcado de paquetes para flujos de protocolos y otro destinado al tráfico de los usuarios, pudiendo luego brindar la limitación de usuarios con sus respectivas marcas y calidad de servicio con flujo de protocolos en el mismo dispositivo.

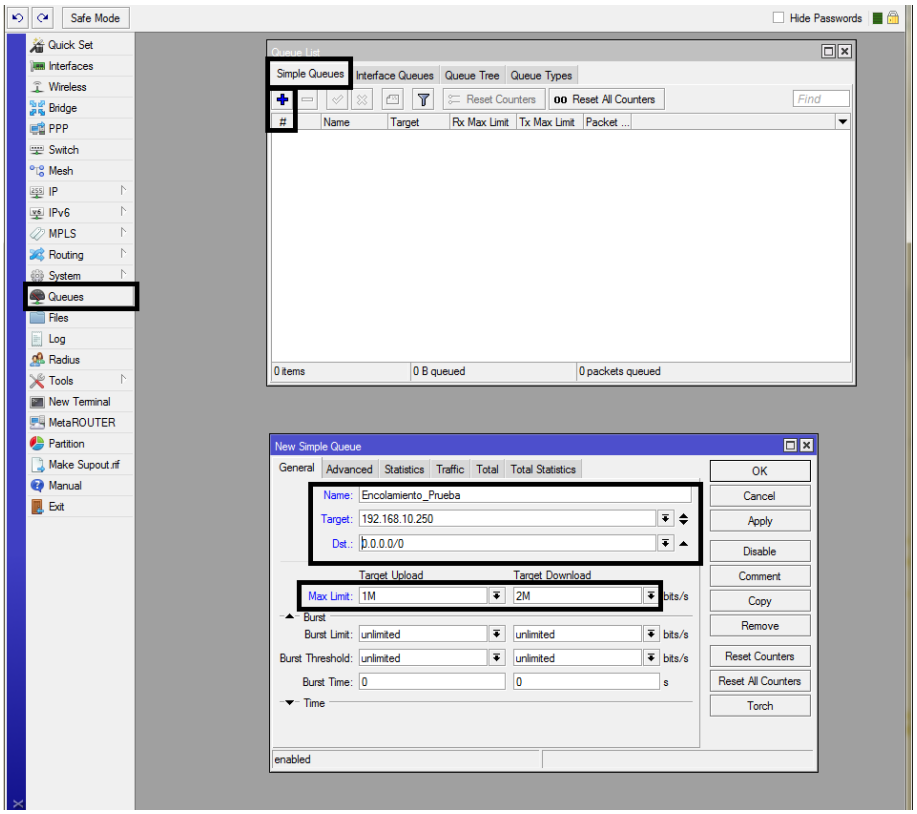


Figura 2.40. Creación de un encolamiento simple básico dentro de RouterOS

Fuente: Los Autores, Simple Queue, 2013.

2.2.2.11.3. Arboles de Colas

El mecanismo de árboles de colas dentro de RouterOS es quizá una de las opciones con mayor grado de rendimiento y la que mejores resultados trae en cuanto a limitación, repartición del ancho de banda y priorización así como la anterior está basada en HTB y es unidireccional[17], la diferencia con el encolamiento simple es que aquí todo el tráfico es procesado simultáneamente mas no de forma secuencial como las colas simples, además de ser posible emplear todas las disciplinas de encolamiento antes mencionadas, y pudiendo aplicarlos en entornos con gran volumen de tráfico sin una pérdida significativa de rendimiento en el Hardware, quizá una de las mayores desventajas para aplicar este tipo de mecanismo es que todas las colas hijas necesitan disponer de una marca de paquete previamente configurada e incluso pudiendo definir un nivel de prioridad entre las colas que

[17] Colas Simples, 20 de Mayo del 2013, http://wiki.mikrotik.com/wiki/Manual:Queue

distribuyen hacia las colas hijas, dichos nombres se manejan así ya que al hacer uso de HTB consideramos que este tipo de encolamiento es Jerárquico, por tal existen "colas padre" llamadas a las colas que distribuyen el ancho de banda "colas Hija" a las colas que consumen el ancho de banda, pero para comprender estos términos y familiarizarse un poco más es necesario antes de profundizar definir los siguientes términos relevantes tales como:

CIR (Committed Information Rate): Es considerado en un escenario de compartición de ancho de banda como el peor de los casos establecidos, donde al menos asegurara un mínimo de tráfico disponible, el ancho de banda no debe caer por debajo de esta tasa asignada.

MIR (Maximum Information Rate): Es considerado en un escenario de compartición de ancho de banda como el mejor de los casos establecidos, ya que se asegura la tasa de datos máxima disponible para un flujo dentro del ancho de banda o tasa asignada.

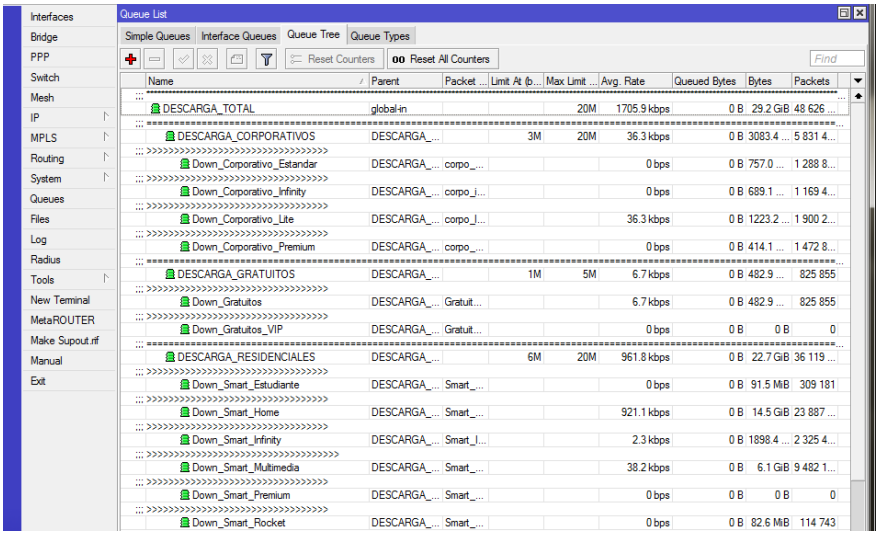


Figura 2.41. Ventana de Administración de Árbol de Colas RouterOS.

Fuente: Los Autores, Queue Tree, 2013.

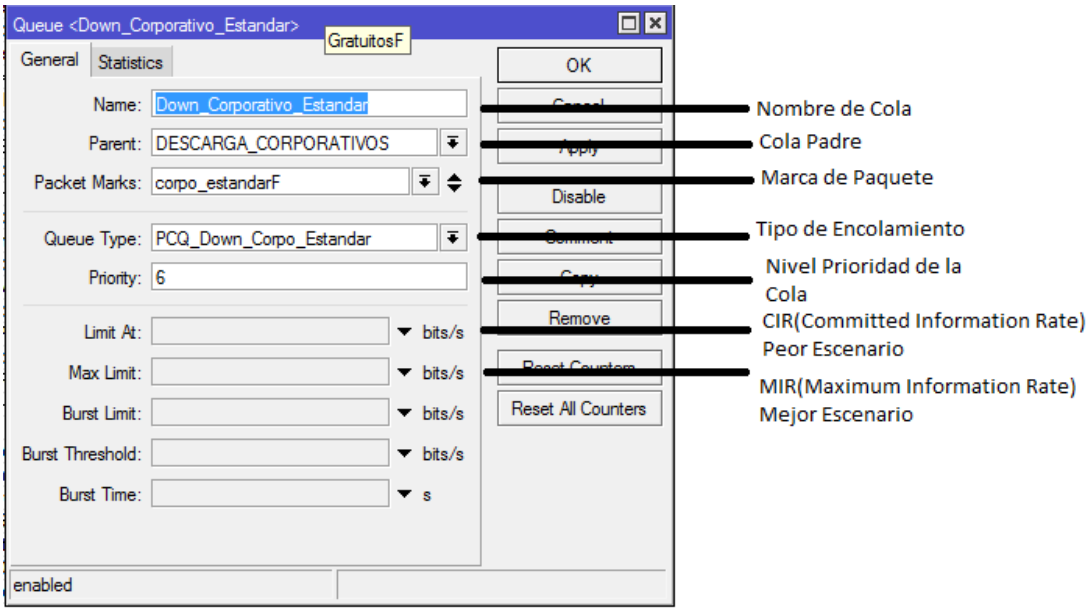


Figura 2.42. Creación de una Cola mediante Árbol de Colas.

Fuente: Los Autores, Queue Tree, 2013.

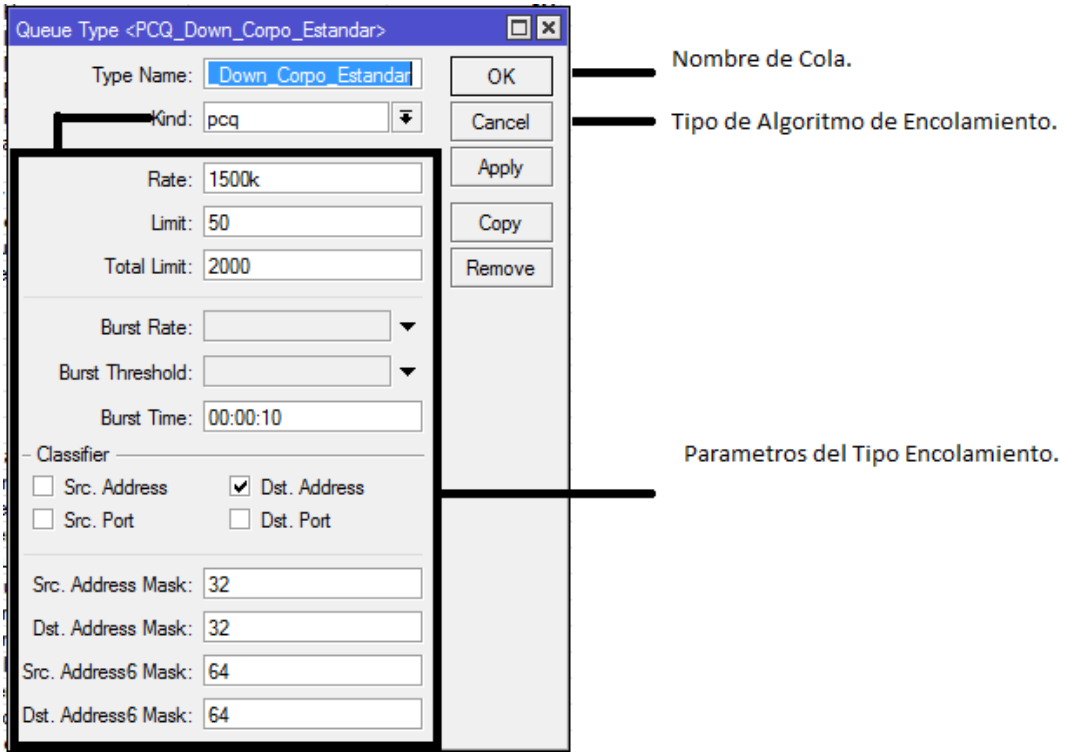


Figura 2.43. Creación de un Tipo de Cola y Parámetros.

Fuente: Los Autores, PCQ Queue, 2013.

2.2.2.12 WIRELESS E IMPLEMENTACIÓN DE PUNTOS DE ACCESO Y CPE.-

Hoy por hoy RouterOs soporta una amplia variedad de tecnologías inalámbricas tanto emergentes como las ya tradicionales como lo son: 802.11 y su completo soporte para 802.11a/b/g/n e incluso ac el nuevo estándar que está revolucionado el mercado Wireless por su capacidad para transportar grandes cantidades de datos, además su gran variedad de modulaciones como lo son: DSSS (Direct Sequence Spread Spectrum) o CCK (Complementary Code Keying) etc, que hacen relación al conjunto de técnicas elaboradas para el transporte de la información sobre una onda portadora y el objetivo de este punto no es detallar dichos aspectos técnicos a profundidad porque el mismo comprende un estudio de amplia envergadura, pero si generalizar aspectos relevantes que han apoyado en este proceso de reingeniería de la empresa Sigsignet, en fin la gran versatilidad de radios Mikrotik, le han permitido soportar múltiples configuraciones con una amplia variedad de usos que van desde Puntos de Acceso, hasta modo CPE e incluso enlaces punto a punto o porque no mencionar una característica que le ha dado gran relevancia como es el Hotspot embebido que dispone. Configurar una estación en cualquiera de los modos de operación antes mencionados, y en las nuevas versiones de RouterOs es completamente sencillo incluso para una persona con escasos conocimientos, pero ello no significa que el modo avanzado no esté disponible, al contrario dicho modo se lo puede apreciar si se desea un configuración más precisa y puntual, desde la versión 5.X de RouterOs se incluyó un gestor de configuración o Wizard para facilitar las configuraciones básicas en RouterOS, además características relevantes a tomar en cuenta como lo son sus protocolos propietarios tales como: Nstreme en sus dos versiones, cuya tarea es mejorar el desempeño de los enlaces inalámbricos reduciendo el tiempo de acceso y aumentando la velocidad de transmisión, o incluso el uso de la tecnología MIMO bajo el estándar 802.11n, que mediante múltiples antenas transmisoras y receptoras permite mejorar el desempeño permitiendo manejar más información, una característica que llama la atención y de suma utilidad es el virtual AP que permite manejar varios SSID con diferentes encriptaciones en un AP que hereda el mismo canal de frecuencia usada por el nativo

o de la interfaz, incluso la administración de redes MESH o tipo malla que permite incrementar el espacio de cobertura, sin olvidar que permite manejar varios estándares de seguridad muy conocidos como son WEP (Wired Equivalente Privacy), WAP (Wireless Aplication Protocol), WAP2, posibilitando también integrarse con casi cualquier tipo Radius (Remote Authentication Dial-In User Server) que maneje estándares globales, elevando aún más el nivel de seguridad.
El procedimiento para configurar un Punto de Acceso en RouterOS se detalla usando el gestor Quickset y setear las configuraciones elementales o directamente sobre la interfaz donde se pueden definir parámetros avanzados y un nivel de configuración y funcionamiento elevado.

1.-Ingresar dentro de Winbox y dirigirse a la opción QuickSet, se visualizará la pantalla de asistente que permite configurar un equipo con soporte inalámbrico en los siguientes modos establecidos por defecto que son:

AP.- Access Point o Punto de Acceso, usado para enlaces multipunto.
CPE.- Customer Premises Equipment o Equipo Local de Cliente
Home AP.- Punto de Acceso Residencial.
PTP Bridge.- Usado para enlaces punto a punto.

El asistente permite establecer determinados parámetros sobre la interfaz sin necesidad de tener elevados conocimientos de acuerdo al modo de operación que dicho dispositivo vaya a realizar, por tal se puede poner a funcionar un equipo Mikrotik en apenas pocos minutos, utilizando Quickset para Modo AP o punto de acceso, tan solo requiere ingresar los siguientes parámetros que son: Protocolo Inalámbrico, Dirección IP, Gateway, SSID, frecuencia sobre la que se va a irradiar, banda y método de seguridad y encriptación.

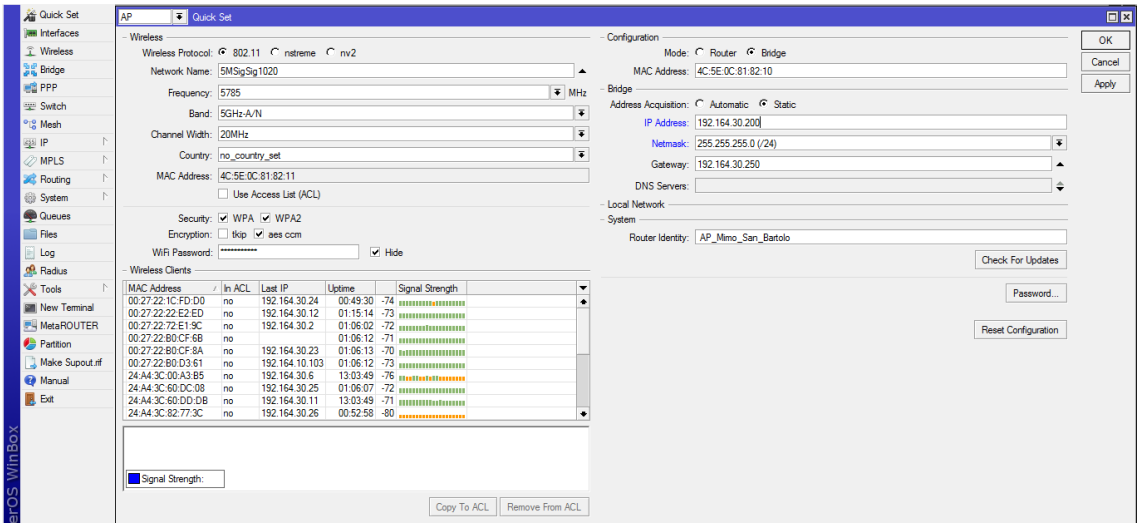


Figura 2.44. Herramienta Quickset de RouterOS para modo AP.

Fuente: Los Autores, Quickset y RouterOS, 2013.

En tanto la configuración para un CPE el asistente tan sólo requiere identificar la red inalámbrica o SSID a la que se desea conectar, el ancho de canal, el ingreso de la seguridad y el método de adquisición de IP y operación del equipo.

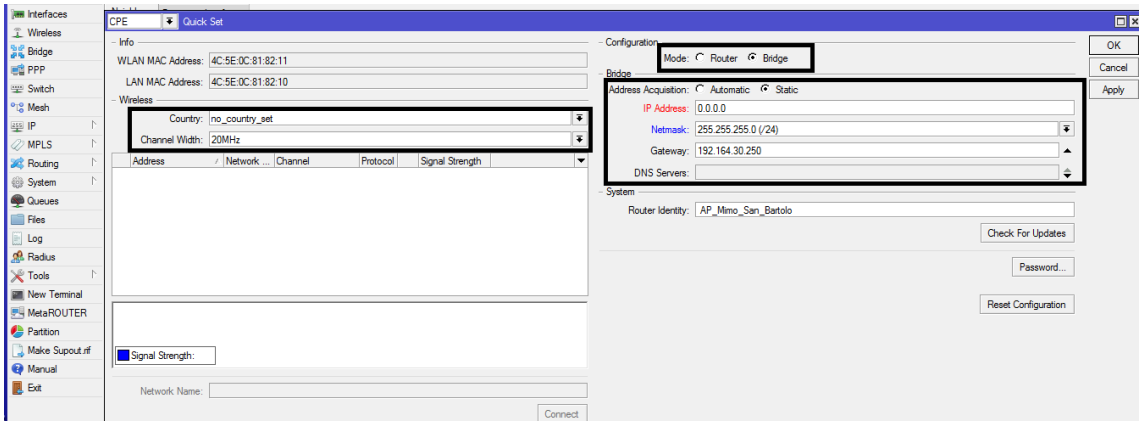


Figura 2.45. Herramienta Quickset de RouterOS para modo CPE.

Fuente: Los Autores, Quickset y RouterOS, 2013.

Como se mencionaba anteriormente si el modo de operación demanda configuraciones especiales para entornos a medida o una geografía de un lugar poco común, el QuickSet ya no sería una forma óptima de configurar la estación para ello

se tendrá que setear cualquier parámetro desde la Interfaz Inalámbrica, ingresando desde Winbox en la pestaña Wireless y en la pestaña interfaces seleccionar con doble clic la interfaz sobre la cual se aplicará la configuración, donde se podrá disponer de dos modos de configuración una simple y otra avanzada, siendo la única diferencia la visualización de campos adicionales que demandan un elevado conocimiento sobre protocolos inalámbricos dentro del modo avanzado.

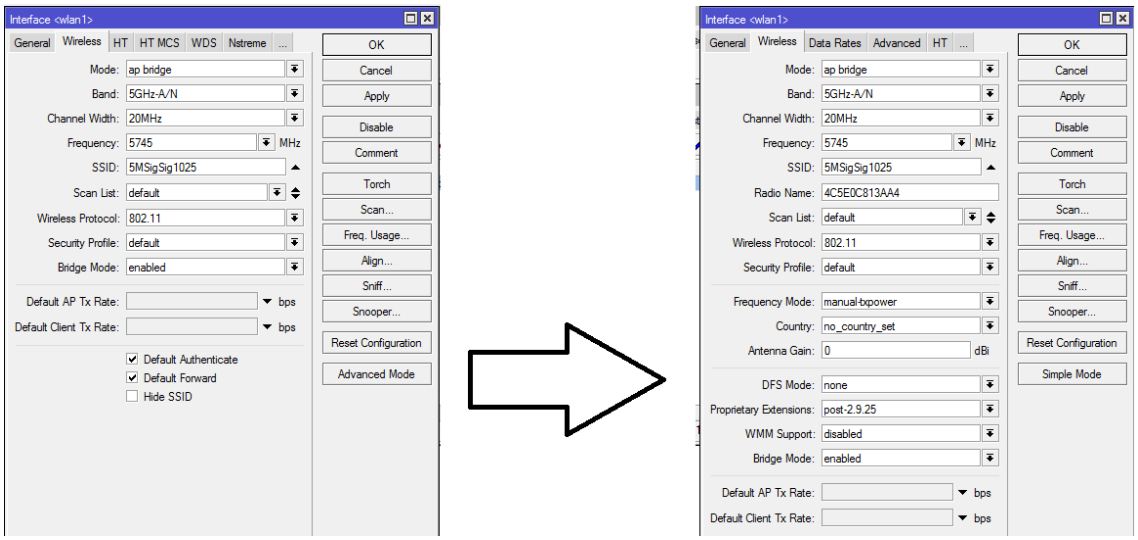


Figura 2.46. Configuración de Interfaz Wireless, vista en modo simple y avanzado

Fuente: Los Autores, Quickset y RouterOS, 2013.

2.2.2.13 SERVICIOS DE RED PRINCIPALES DISPONIBLES EN ROUTEROS.

RouterOS como tal fue concebido como una solución altamente versátil, el sistema brinda la posibilidad de que el usuario sea quien defina las funciones elementales y servicios de red a usar, en tanto soluciones propietarias de otros vendedores no aportan la flexibilidad necesaria, ya que si es necesario una solución para Firewall la misma se vende indistintamente de una para Ruteo o para hotspot etc., incrementando aún más los costos de implementación, no obstante Mikrotik es aquí donde suma puntos a favor ya que es posible habilitar o bien el mínimo de servicios de red cargados por defecto con el sistema o todos a su vez siendo la descarga de paquetes adicionales, incluso utilizar los mismos de forma independiente. Muchos de estos servicios de red son encontrados en sus respectivos paquetes generalmente al

adquirir una solución con Hardware Mikrotik dichos equipos traen ya de por si instalado una versión estable de RouterOS con los paquetes por defecto del sistema, siendo posible desde Winbox en la opción Packages inhabilitar, desinstalar o instalar paquetes con sus respectivos servicios de red.

System >>> Packages

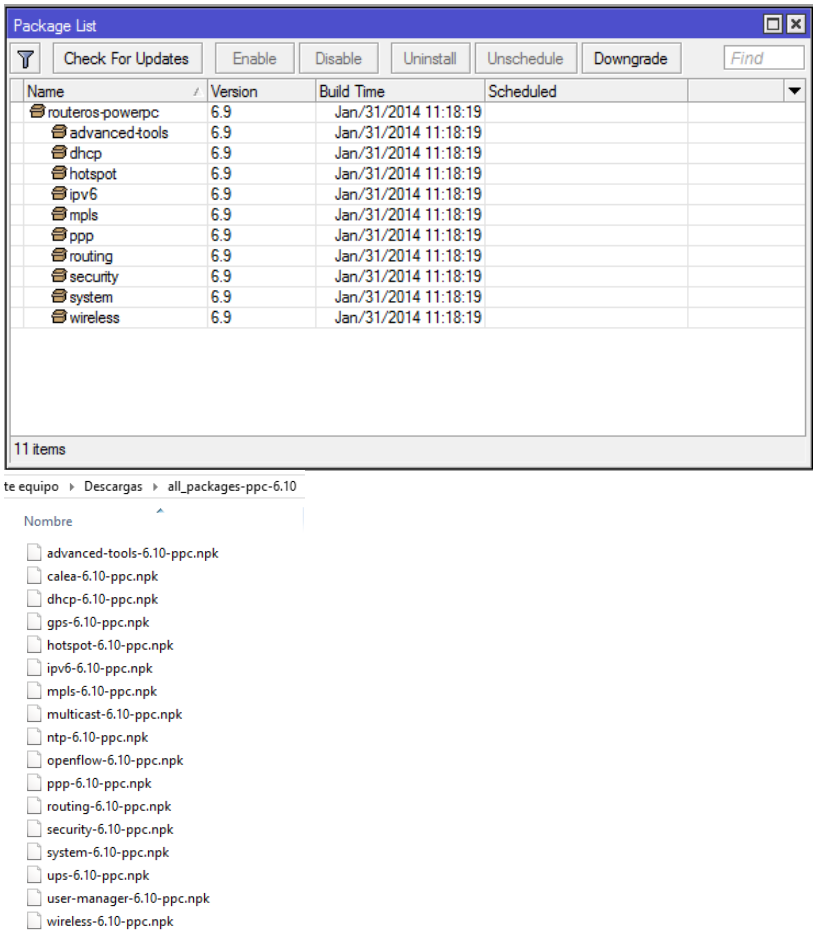


Figura 2.47. Ventana de Lista de Paquetes en RouterOS con servicios de red

Fuente: Los Autores, Packege List, 2013.

Los diversos niveles de licenciamiento que Mikrotik otorga, establecen una limitante a nivel lógico en algunos por determinados servicios de red como límite de túneles establecidos por el servicio PPoE por ejemplo, o que puede ser ilimitados si el nivel de licencia es el máximo, pero aun siendo posible disponer de todos los servicios de red establecidos para RouterOS, aunque la mayoría de ISP en sus inicios y en redes

relativamente pequeñas tienden a usar un solo aplicance con todos los servicios de red habilitados y sin ser necesaria una alta inversión hasta cuando la red haya escalado lo necesario y demande temas como alta disponibilidad, óptima calidad de servicio, transporte de datos etc., pueden ser implementados progresivamente e inclusive independizando los diversos servicios de red en appliances independientes.

Mikrotik por medio de RouterOS ofrece un repertorio completo de servicio de red que van desde, un servidor DHCP, DNS, FTP, NFS un servicio para almacenamiento de archivos en red etc., los mismos por defecto vienen instalados pero cuyos servicios no se están ejecutando.

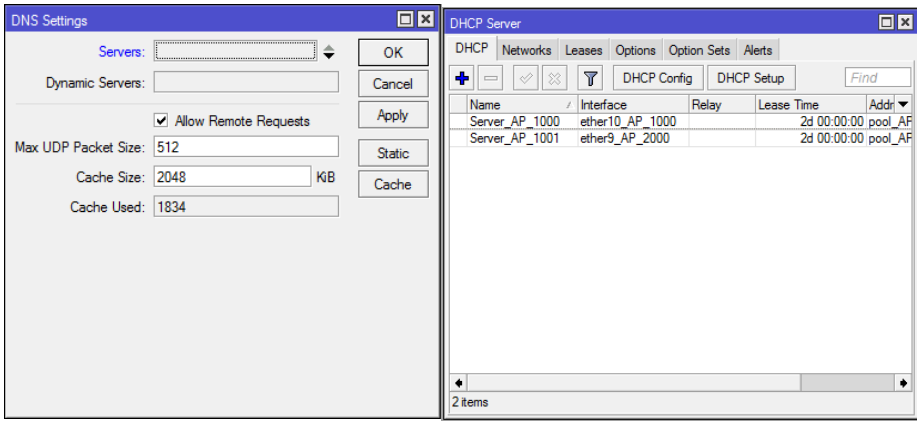


Figura 2.48. Servicios de red DNS & DHCP Server.

Fuente: Los Autores, DHCP Server & DNS, 2013.

2.2.2.14 CREACIÓN DE SCRIPTS EN ROUTEROS Y REGLAS DE EJECUCIÓN.

El uso de scripts dentro de cualquier sistema operativo es casi una tarea imprescindible y más aún cuando se trata de sistemas dedicados a trabajo en redes de datos ya que estos pueden actuar directamente con el Sistema Operativo o componentes en sí, Mikrotik ha implementado dicha funcionalidad desde sus inicios y hasta la actualidad lo ha convertido en una solución bastante atractiva permitiendo disponer de su propio lenguaje de scripting, que permite automatizar tareas manuales a veces muy tediosas de forma muy eficiente.

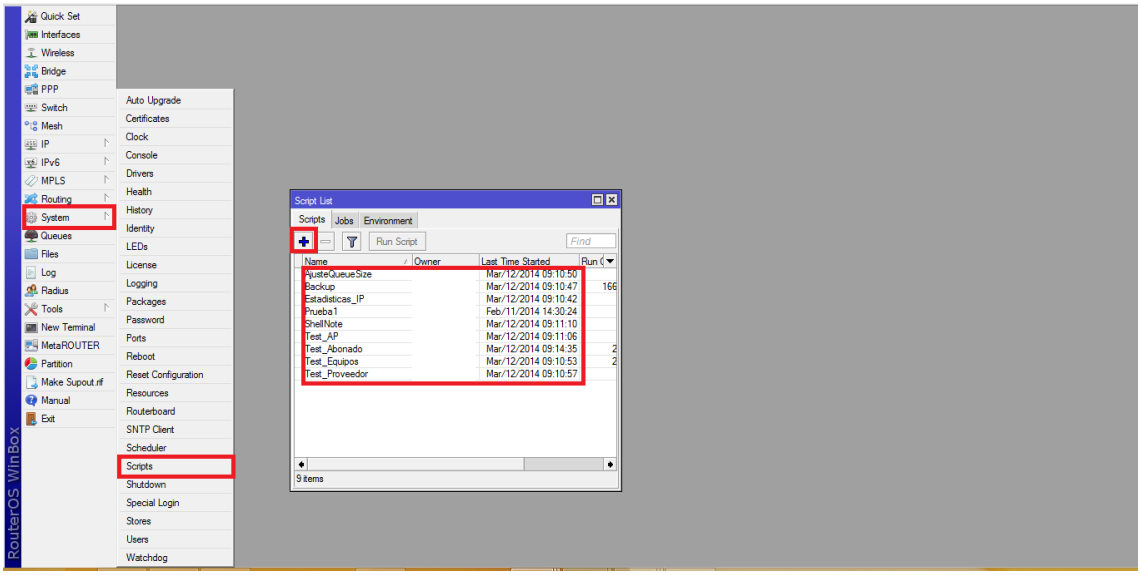


Figura 2.49. Creación de Scripts dentro de RouterOS utilizando WinBox

Fuente: Los Autores, Scripting Mikrotik, 2013.

Scripting en Mikrotik - RouterOS proporciona una vía para automatizar diversas tareas de mantenimiento del Router, incluso la ejecución de los mismos ante determinados eventos, dentro de RouterOS dichos scripts o bien puede ser almacenados para su posterior ejecución o ejecutados directamente sobre una Shell, todo script dentro de RouterOS sigue un proceso de ejecución secuencial que va uno por uno hasta el final o hasta que se genere algún tipo de error.

Dentro de Sigsignet y el proceso de reingeniería el uso de scripts está apoyando significativamente a los procesos manuales que se venían realizando por el departamento técnico en especial el personal encargado de soporte nivel 1, se han desarrollado soluciones que han apoyado en diversos campos como el soporte directo al usuario, permitiendo crear un proceso de test de conexión de un cliente de servicio donde se asocian todos los procedimientos necesarios para verificación de la calidad de conexión junto con respuesta interpretadas, es decir los resultados de dichas pruebas interpretados para personal sin elevados conocimiento de TCP/IP pero que puede colaborar en la etapa de soporte técnico reduciendo el tiempo de respuesta ante eventuales problemas suscitados por el servicio o diversos factores sobre el ámbito de TPC/IP, incluso scripts capaces de evaluar día a día el nivel de conexión contra el

proveedor y enviar estadísticas puntuales por correo electrónico, o realizar ajustes acorde a las condiciones actuales.

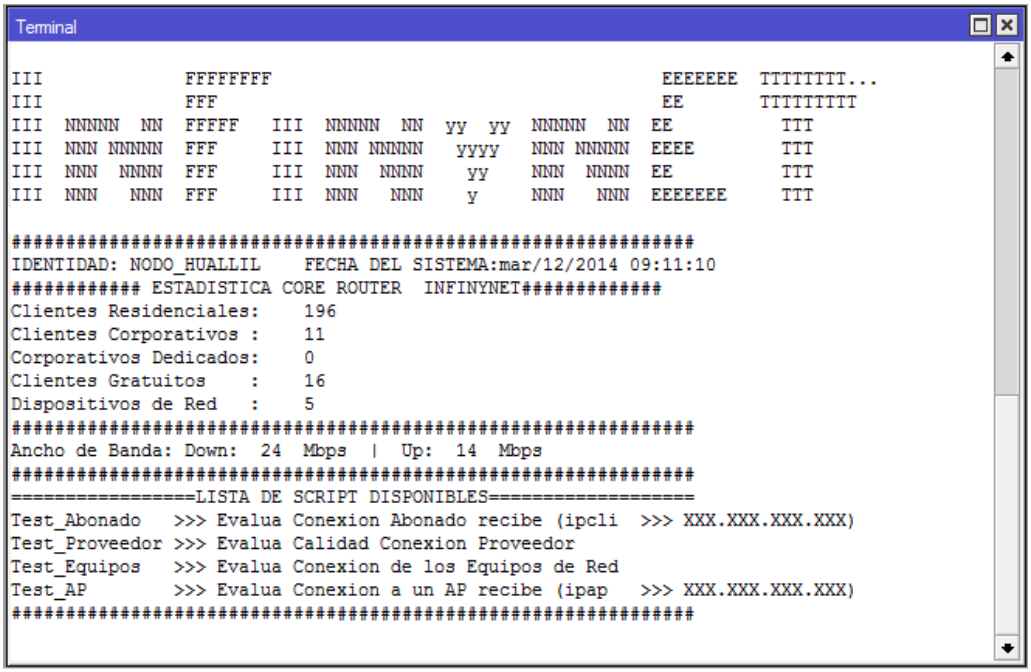


Figura 2.50. Shell modificada para la ejecución de script con variables dinámicas.

Fuente: Los Autores, Mikrotik – RouterOS, 2013.

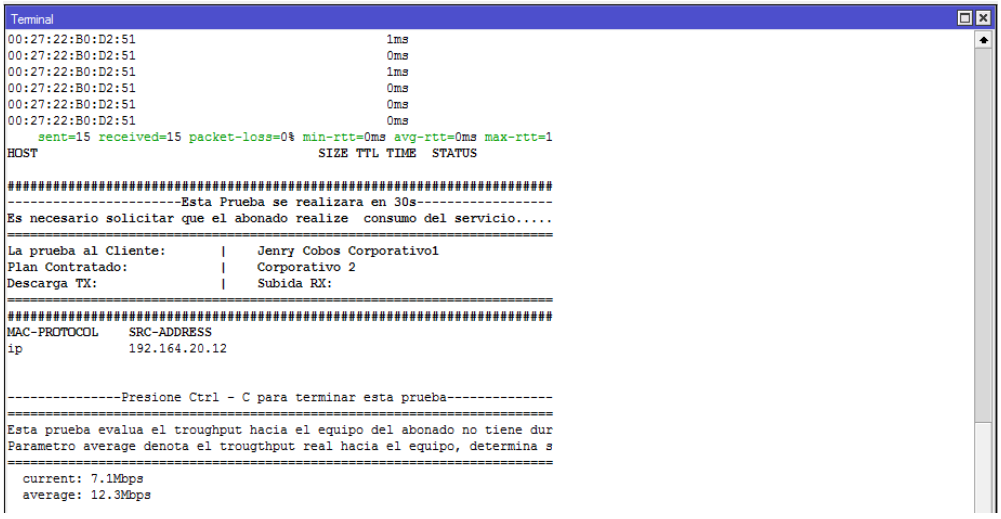


Figura 2.51. Ejecución de Script para test de conexión de un abonado.

Fuente: Los Autores, Mikrotik - RouterOS, 2013.

Es importante antes de elaborar un script entender la sintaxis que el lenguaje de scripting que RouterOS emplea y su estructura, con dicho conocimiento previamente obtenido el proceso de crear un script por medio de Winbox contempla lo siguiente:

- Crear el Script desde Winbox >>> System >>> Script >>> (+)

-

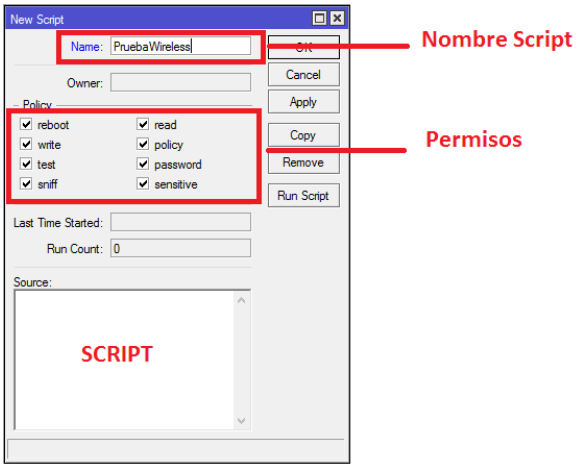


Figura 2.52. Ventana de creación de un nuevo script.

Fuente: Los Autores, Scripts, 2013.

- Verificación y ejecución, necesarios para comprobar la funcionalidad del mismo, es posible ejecutar un script desde la misma ventana de creación pero es recomendable usar la Shell ante cualquier proceso de debug sobre errores presentes en el script, por lo tanto desde un Shell en RouterOS o Winbox se digitaría lo siguiente.

```
[RouterOS@RouterUPS] > system script run Test_Abonado;
```

2.2.2.15 ROUTEROS, API Y SERVICIOS DISPONIBLES

Muchos sistemas y soluciones de Networking, están abriendo sus plataformas para integración con sistemas externos por tal razón se ha puesto en auge el uso de API's o librerías que posibilitan un canal de comunicación directa y en tiempo real con cualquiera de estos dispositivos, quizá una de las más grandes ventajas de la disponibilidad de un API a nivel de un proveedor de servicios de Internet es poder

crear aplicaciones personalizadas utilizando dichos equipos como medios de acción que permitan automatizar tareas que antes eran completamente manuales evitando ya los tradicionales y anticuados procesos donde la sincronización a determinadas horas era un término muy común, y causante algunas veces de transacciones fallidas o no realizadas.

Para activar el API dentro de RouterOS basta ingresar por medio de Winbox y dirigirnos a la opción IP >> Services >>> Seleccionar (API) y habilitarlo.

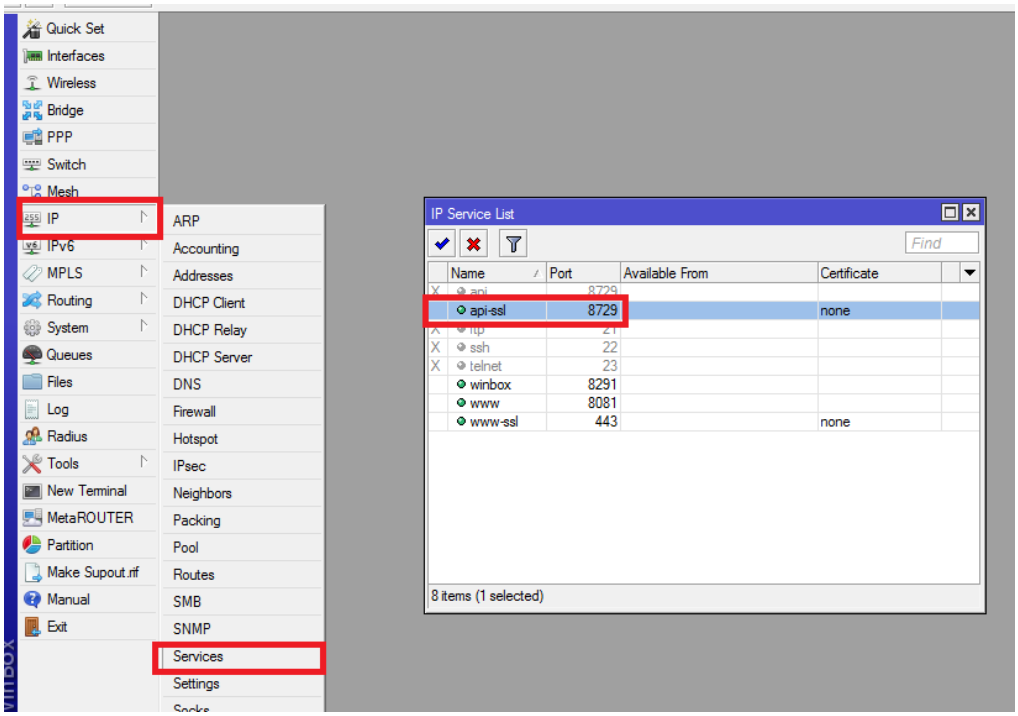


Figura 2.53. Ventana de Lista de Servicios de administración de RouterOS

Fuente: Los Autores, IP Services, 2013.

Así también su respectiva configuración mediante línea de comandos.

```
[RouterOS@RouterUPS] > ip service enable api;
```

El API al ser un Puerto de comunicación que usa RouterOS puede ser incluso cambiado ya que por defecto viene configurado como puerto escucha el 8728 y como medida de protección adicional que emplea el puerto en la lista de servicios se puede configurar con una IP o un rango de acceso exclusivo, inclusive la posibilidad de usar encriptación sobre dichos canales por medio de SSL previniendo con el mismo posibles intrusiones no deseadas, es importante recalcar que en el proceso de

comunicación con el sistema externo y el API valida también las credenciales de acceso previamente creadas en el Router por medio de un usuario y password caso contrario la comunicación no se podrá establecer.

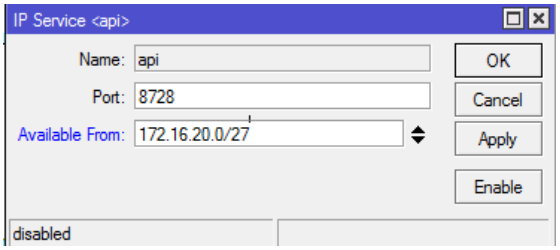


Figura 2.54. Ventana de configuración de servicio API en RouterOS.

Fuente: Los Autores, IP Services, 2013.

Así también su respectiva configuración mediante línea de comandos.

```
[RouterOS@RouterUPS] > ip service set api port=8729 address=172.16.20.0/27
certificate=none;
```

La lista de servicios IP disponibles para acceso a administración y gerenciamiento de un equipo Mikrotik – RouterOS son diversos, van desde la posibilidad de acceder al equipo por Winbox con su popular herramienta de administración grafica o incluso hoy en día el acceso por su API como ya se ha mencionado anteriormente, de ahí también las ya tradicionales vías de acceso, que van desde acceso por SSH o consola, telnet, web y sus variantes que incluyen encriptación que son WEB por SSL y API con SSL, en su configuración por defecto todos los puertos disponibles viene activos, es necesarios siempre como primer paso antes de su funcionamiento su protección por firewall o a su vez su inhabilitación.

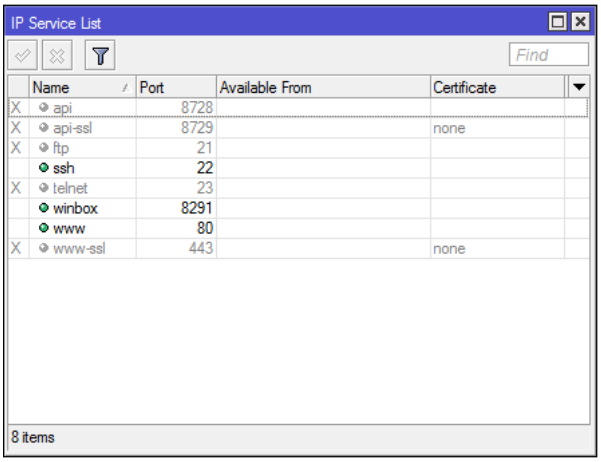


Figura 2.55. Lista de Servicios de Red disponibles en Mikrotik para acceso a RouterOS

Fuente: Los Autores, IP Service List, 2013.

En línea de comandos los podemos listar de la siguiente forma:

```
[RouterOS@RouterUPS] > ip service print
```

Nombre Servicio	Puerto por Defecto	Descripción
API	8729	Puerto de Interfaz de programación de aplicaciones, para integración con sistemas externos.
API-SSL	8729	Puerto de Interfaz de programación de aplicaciones, para integración con sistemas externos, protegido por encriptación
FTP	21	Protocolo de transferencia de archivos bajo TCP destinado para la descarga de archivos, pero no muy seguro
SSH	22	Conocido como Secure Shell, protocolo para acceso remoto al Router o cualquier dispositivo de red, permitiendo administrar el equipo remoto a

		entera disposición, similar a telnet pero con beneficios de encriptación.
TELNET	23	Es un protocolo de red similar a SSH pero sin los beneficios del mismo ya que no maneja un nivel de encriptación.
WINBOX	8291	Puerto de acceso a Winbox, interfaz de administración gráfica, creada para manipular RouterOS de manera segura y fácil, facilitando las tareas de administración sobre el dispositivo y brindando estadísticas puntuales.
WWW	80	Puerto de administración Web corriendo sobre RouterOS, posibilita la configuración y administración de RouterOS a través de una página WEB0.
WWW-SSL	443	Similar al anterior pero con la capacidad de poder agregar encriptación e incluso el uso de certificados de autoridad.

Tabla 2.9. Servicios y Puertos

Fuente: Los Autores, Servicios y Puertos, 2013.

2.2.2.16 CLI Y LÍNEA DE COMANDOS ROUTEROS.

Denominada como interfaz de línea de comandos por sus siglas en inglés (CLI), accesibles vía Telnet, SSH, cable serial o nativamente con teclado o monitor si el Router dispone de una interfaz VGA, permite configurar las opciones del Router utilizando comandos de texto, debido a la gran cantidad de comandos disponibles en RouterOS, los mismos se organizan de modo jerárquico en niveles de menús, siendo posible incluso hacer uso de comodines de ayuda o la opción de auto complementado método que agilita la configuración de cualquier equipo Mikrotik por medio de dicha vía, incluso la visualización por color de comandos, como ayuda visual de por medio

simplificando aún más dicho proceso de administración y configuración de forma intuitiva.

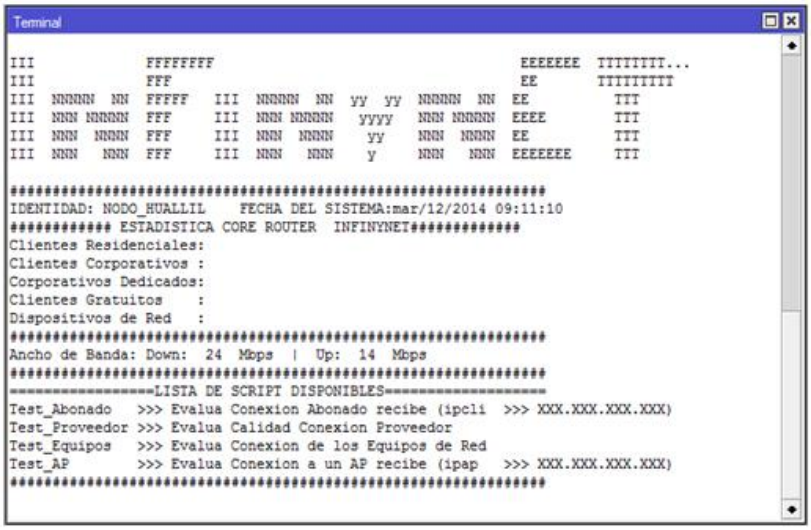


Figura 2.56. CLI o Shell Mikrotik RouterOS

Fuente: Los Autores, Console, 2013.

Para tal no todos los comandos pueden estar disponibles en una u otra instalación de RouterOS a veces es necesario instalar algunos paquetes adicionales para disponer de los mismos ya que generalmente no todos los servicios puede venir instalados por defecto, en el caso de no disponer de un amplio conocimiento en el CLI de RouterOs se puede hacer uso de comodines de ayuda en el teclado utilizando la tecla <TAB> donde seguido a presionar la misma podemos visualizar los comandos disponibles para su ejecución, o incluso donde muchas de las veces no es necesario utilizar la palabra completa del comando sino más bien su diminutivo como por ejemplo la regla a continuación describe una tarea para grabar un ip en una lista y se puede observar que se la puede realizar de dos formas una con el comando completo y la otra con su diminutivo, siendo las dos opciones completamente válidas.

[RouterOS@RouterUPS] > **ip firewall address-list** add list=spammers address=8.8.8.8

[RouterOS@RouterUPS] > **ip fire address** add list=spammers address=8.8.8.8

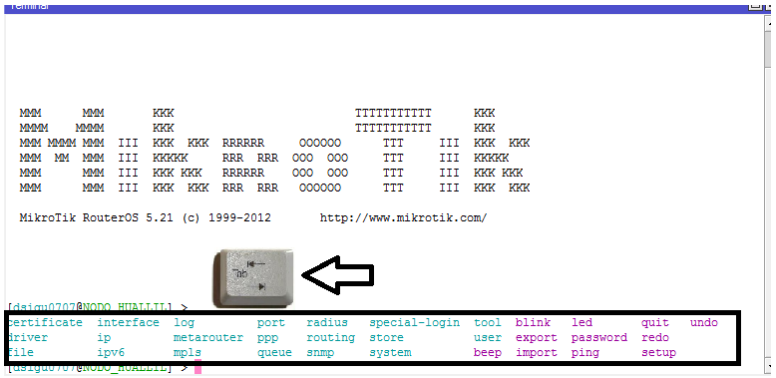


Figura 2.57. Comandos RouterOS listados a partir de comodín tecla TAB.

Fuente: Los Autores, Función Autocomplemento RouterOS, 2013.

O similar con el comodín interrogación presionado la tecla < ? > interrogación se desplegará un menú contextual con la descripción puntual de cada comando permitiendo, en caso de no conocer bien el CLI determinar la función y tarea del comando.

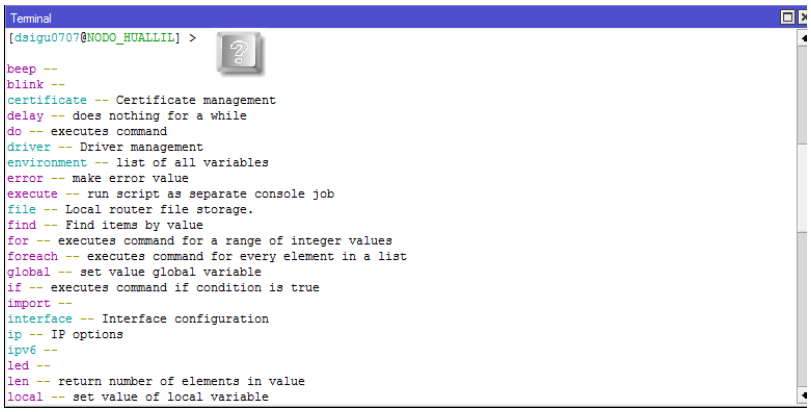


Figura 2.58. Lista de Comandos RouterOS con descripción utilizando comodín <?>

Fuente: Los Autores, Comodín de Ayuda, 2013.

2.2.2.17 ROUTEROS COMO CONCENTRADOR DE VPN.

El uso de las VPN o mejor conocidas como redes privadas virtuales sobre redes de datos públicas donde se simula tener una línea privada por medio de un túnel que atraviesa una red pública, cada vez su uso está volviéndose más común hoy en día, y

no solo por su amplio uso que dan las empresas sino porque los usuarios comunes y corrientes ya lo consideran una forma esencial de conexión incluso para la tele presencia o trabajo virtual hacia sus oficinas remotas o incluso proveedores de acceso de internet cuya última milla es entregada mediante este modelo de conexión, RouterOs por tal desde sus inicios lo ha considerado como una importante opción a estar presente en su sistema operativo y como parte de sus servicios. Por tal existe una amplia variedad de protocolos mejor conocidos como protocolos de tunneling implementados sobre RouterOS algunos de ellos operan sobre capa 3 de acuerdo al modelo OSI siendo posible no solo realizar tareas de enrutamiento sino control puntual de trafico así como de QoS o calidad de servicio, e incluso posibilitando mantener canales cifrados con niveles de encriptación altamente eficaces como lo son estándares como 3Des o AES-256 bits, encriptaciones para protección de datos de estado critico o encriptaciones básicas a nivel de conexión para hogares como MPPE 128 muy comúnmente usadas en domicilios, o incluso protocolos propietarios de Mikrotik como lo es L2TP con una capa de cifrado adicional denominada IPSec. Generalmente los más comunes para realizar transmisiones en modo túnel son VPN e IPSec (Secure IP) con alternativo ESP (carga útil de encapsulamiento de seguridad.)

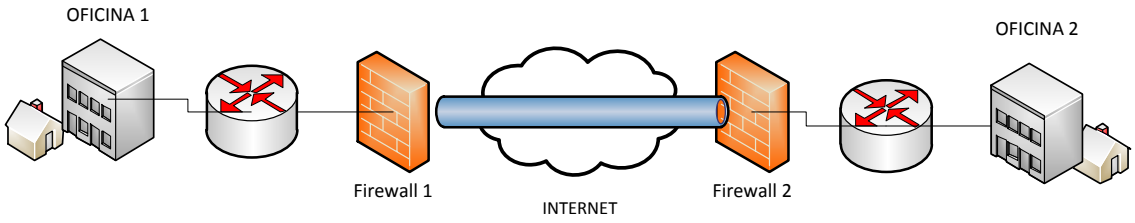


Figura 2.59. Topología de Túnel VPN a través de Internet.

Fuente: Los Autores, Topología de Túnel, 2013.

En RouterOS una forma básica de VPN o tunneling es a través PPTP (Point to Point Tunneling Protocol) ampliamente usado en clientes Windows para conexión con redes privadas virtuales, el servidor es configurable en tan solo unos pasos y tendremos levantado un servidor VPN PPTP para ello se dirige en el menú Winbox a la opción PPP >>> PPTP Server (Click en el check Enabled) y luego registrar un Secret estableciendo nombre de usuario, contraseña y demás parámetros.

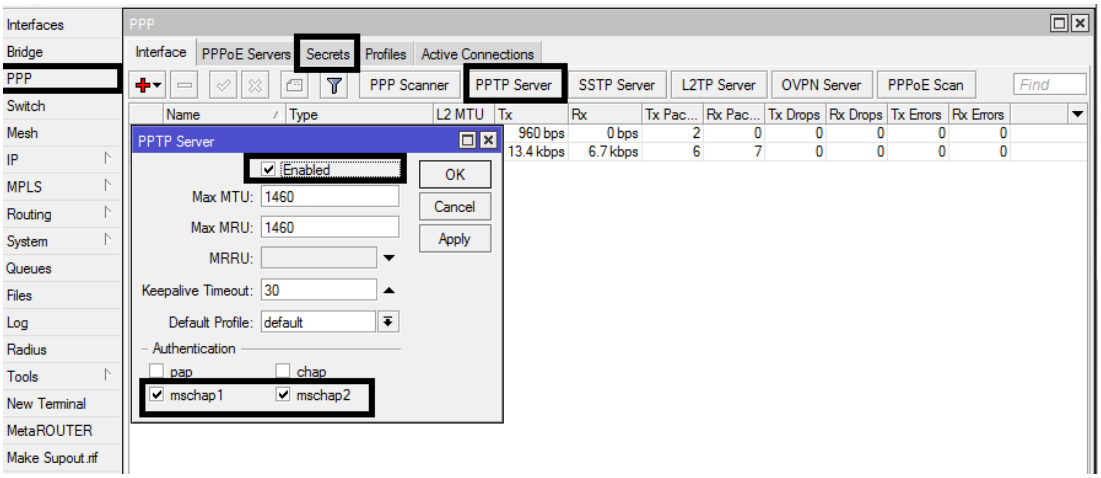


Figura 2.60. Ventana de activación servidor PPTP y servidores Túneles.

Fuente: Los Autores, PPP, 2013.

Si se quiere establecer perfiles de conexión también se lo puede definir previamente y establecerlos luego a nivel de PPP Secret, cabe recalcar que los perfiles de conexión ayudan a poder administrar las conexiones al servidor de forma más ordenada siendo posible agregar una conexión a una lista o incluso establecer políticas de uso y de tratamiento de dichas conexiones de una forma especial pudiendo determinar incluso el uso de protocolos de encriptación, compresión u otros, sin olvidar que al mismo tiempo es posible controlar la sesión mediante a nivel de ancho de banda y tiempo válido de usuario y contraseña antes de su caducidad.

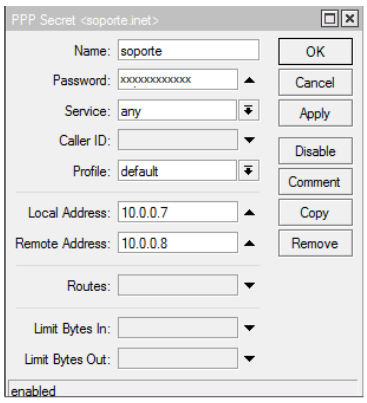


Figura 2.61. Ventana de creación de Secret en Perfil de Túnel.

Fuente: Los Autores, PPP, 2013.

2.2.2.18 ROUTEROS COMO SWITCH CAPA 2 Y CAPA 3.

Entre una de sus principales utilidades en RouterOS desde la versión 4.X en adelante existe la posibilidad de realizar tareas de switching tanto a nivel de capa 2 como de capa 3, así como emular el funcionamiento de Switch administrable utilizando software, o incluso poder funcionar como un hardware dedicado gracias a las características integradas en su hardware denominado Routerboard que algunas de sus variantes ya se integran los tan afamados chip Switch que son componentes electrónicos dedicados a tareas de Switching por hardware evitando así que en el proceso de emulación por software y por ende el consumo excesivo de recursos de hardware, incrementando significativamente el número de paquetes por segundo traficados por interfaz. Al hospedar dicho hardware a RouterOS le da la posibilidad incluso de poder convertir como ya se mencionó sea por hardware o software al equipo en un dispositivo de switching incluso con soporte para capa 3 según el modelo OSI y todas las características agregadas que van desde realizar tareas de enrutamiento avanzadas e incluso el filtrado de paquetes en cualquiera de sus dos capas.

Entre las características básicas que ya se incluyen en RouterOS dedicadas al switching son:

- Puerto de Conmutación.-Función de switching que permite el tráfico de datos a velocidad del cable que pasa entre un grupo determinado de puertos.
- Port Mirroring.- Capacidad para espejar el tráfico de un puerto a otro.
- Host Table.-Contiene entradas MAC dinámicas y estáticas para la asignación de puertos.
- Tabla de Vlan.-Especifica determinadas reglas para el reenvió de paquetes que tienen 802.1q.

Desde hace casi un par de años atrás Mikrotik ha estado trabajando en una versión dedicada y exclusiva para productos de switching por tal ahora ya es posible incluso hablar de SwitchOS, un sistema operativo dedicado a tareas de switching comercializados ya con su hardware respectivo “Cloud Router Switch”, en dicha

versión ya es posible incluso encontrar características destacables como en otras soluciones de renombre, que incluyen la posibilidad de controlar tormentas broadcast o bucles de red, inundaciones de trafico etc., pero que dicho tema no contempla un análisis profundo de esta solución.

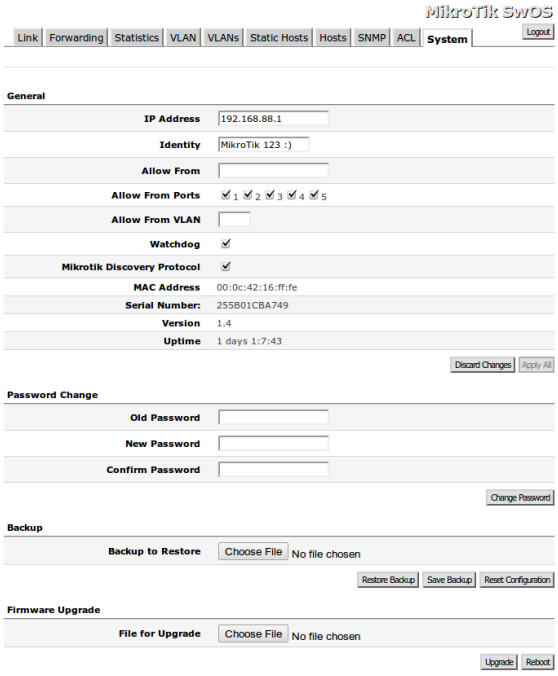


Figura 2.62. Configuración Web SwitchOS Mikrotik.

Fuente: Mikrotik, SwOS, 2013, http://wiki.mikrotik.com/wiki/SwOS

En la versión con la que se han realizado las pruebas para el desarrollo de esta tesis se ha empleado un Hardware dedicado Routerboard modelo RB1200 AHx2 que incluye un chip switch Atheros 8327 con capacidad para Port Switching, Port Mirroring, Host Table de hasta 2k entradas, Vlan Table de hasta 4096 entradas, pudiendo el equipo ser capaz de trabajar como un switch administrable dedicado, su utilización es tan sencilla en otras versiones ajenas a la que se ha trabajado solo requiere la activación de dicho paquete, aunque para futuras versiones Mikrotik lo piensa manejar con su propio Sistema Independiente, dotándolo con RouterOS para dotarlo de las bondades de la capa 3.

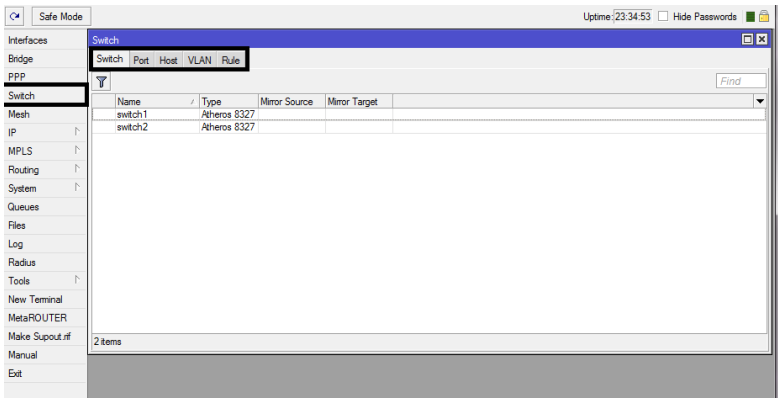


Figura 2.63. Ventana de configuración de Switch en RouterOS y Características.

Fuente: Mikrotik, SwOS, 2013, http://wiki.mikrotik.com/wiki/SwOS

2.3. GNU LINUX Y SUS APLICACIONES EN UN WISP.

Es un tema que hoy en día está tomando gran relevancia y no solo por el beneficio en ahorro de pago de licencias y reducción de costos que ello implica en cualquier entorno, empresa o negocio sino por el establecimiento de grandes comunidades de usuarios que apoyan casi cualquier proyecto de este tipo y la funcionalidad ofrecida, las aplicaciones en un WISP puede ser muy variadas, integrando proyectos que van desde la monitorización de la red, servidores de correo, servidores de cache, servidores web, base de datos entre otros, por tal razón su uso casi se encuentra justificado en este tipo de empresas, e incluso su implementación debe tener un estudio previo que permitan no solo asegurar un buen funcionamiento sino un nivel de seguridad óptimo para los mismos, ya que muchas soluciones Open Source requieren una base de conocimiento sólida, antes de su puesta en marcha.

2.3.1 DEFINICIÓN.

Se puede acuñar el termino GNU/Linux como la interacción entre un Kernel o Núcleo Linux y un grupo de aplicaciones o Software desarrollados bajo estándares de licenciamiento libres tales como por mencionar uno de ellos con amplio uso como lo es GPL (Licencia Pública General) que buscan compartir (copiar), modificar, pero siempre proteger cualquier trabajo desarrollado sobre esta política de licenciamiento.

2.3.2 CARACTERÍSTICAS.

Quizá las características de más renombre basadas en experiencias personales son las siguientes que podemos encontrar en este ecosistema:

- Robusto, estable y altamente configurable.
- Gratuito, cero costo de pago de licencias.
- Multiplataforma siendo posible usarlas hoy en día en Hardware como ARM, MIPS entre otros.
- Gran comunidad de usuarios que dan soporte a través de foros a las distintas plataformas.
- Soporte para virtualización y configurable para trabajo como servidor dedicado.
- Amplia variedad de Software con soporte de una extensa comunidad.

2.3.3 SERVICIOS Y APLICACIONES DENTRO DE UN WISP.

Son variados los servicios y aplicaciones en un entorno para un proveedor de servicio inalámbrico que pueden apoyar en las tareas de gestión y administración de la red otorgando herramientas esenciales como:

- Monitorización de Protocolos y Servicios en la Red.
- Monitorización de Consumo y Ancho de Banda.
- Servidores de Cache Dinámico & Estático.
- Radius Server
- IPS / IDS.
- Servidores Web y Base de Datos para aplicaciones externas.

2.3.3.1 NTOP COMO MONITOR DE RED.

Ntop así como herramientas similares tiene una trascendencia importante en la monitorización de la red y mucho más sobre un proveedor de servicios de Internet, ya que es una herramienta destinada al control de usuarios y aplicaciones a través de la generación de estadísticas que permiten detectar anomalías notificando cualquier

problema mediante determinadas señalas visuales, y que actúa como ayuda en la toma de decisiones correctivas o preventivas sobre la red. El mismo se instala o configura sobre una plataforma web y puede funcionar tanto en entornos Windows como Linux, según el fabricante es capaz de monitorizar protocolos como: TCP/UDP/ICMP, ARP, IPX, DLC, Decnet, AppleTalk, Netbios, y dentro de TCP/UDP es capaz de agruparlos por FTP, HTTP, DNS, Telnet, SMTP/POP/IMAP, SNMP, NFS, X11.

Para este tema de tesis y sus respectivas pruebas la instalación se realizará utilizando Ubuntu Server en su versión 12.04 sin entorno grafico para tal el proceso de instalación se realizará en dicha versión y del lado del servidor de Red Mikrotik – RouterOS en su versión 6.09.
Ubuntu Server puede ser obtenible desde:

http://www.ubuntu.com/download/server

1.-Asumir que el Sistema Operativo está instalado y previamente actualizado con sus repositorios por defecto empezamos el proceso de instalación abriendo una terminal y digitando:

```
sudo apt-get update
sudo apt-get install ntop
```

2.-Luego de terminar el proceso de instalación es necesario configurar el password del administrador NTOP para ello se hace uso del siguiente comando:

```
sudo ntop --set-admin-password
```

3.-Para terminar el proceso de instalación es necesario reiniciar el servicio:

```
sudo /etc/init.d/ntop restart
```

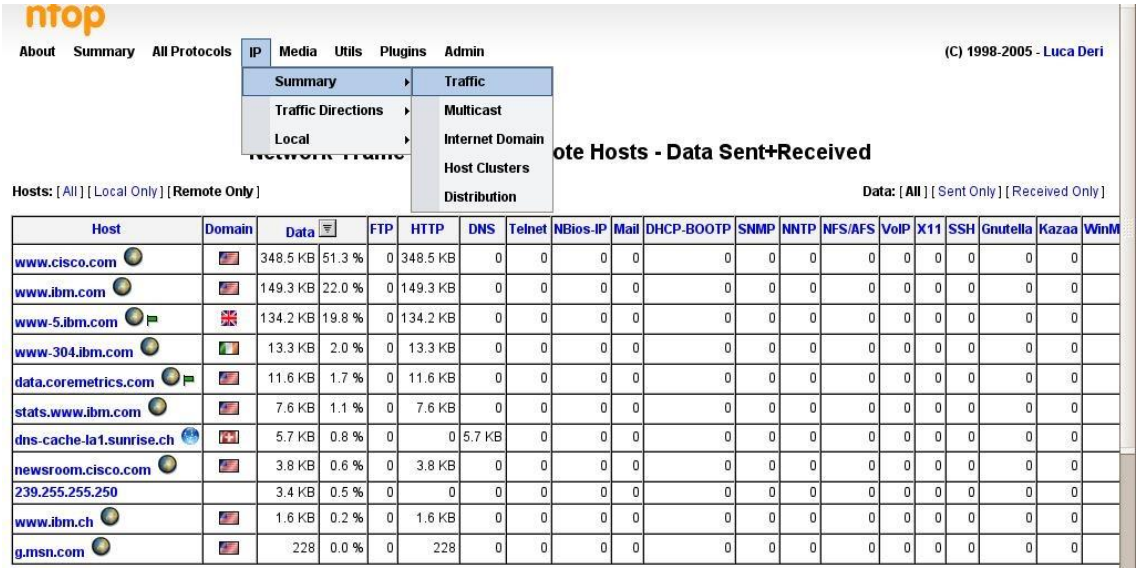
4.-Para acceder a las estadísticas de red ingresamos al siguiente link:

```
http://localhost:3000[18]
```

[18] Ubuntu, 2013, http://www.ubuntu.com/download/server

Localhost se pude reemplazar por la IP del servidor en el caso de que quiera ser accedido desde otra máquina dentro de una misma red.

Del lado del servidor de red Mikrotik necesitamos habilitar el protocolo Traffic-Flow con soporte en sus versiones 1, 5 y 9 que se encarga de proveer de todas las estadísticas informativas al servidor NTOP y el que más tarde les dará su debido tratamiento e interpretación, siendo posible en base a las mismas la optimización global de toda la red, cabe recalcar que el protocolo traffic-flow es compatible con Cisco NetFlow posibilitando su uso con herramientas diseñadas para Cisco NetFlow, como por ejemplo netflowanalyzer.



Host	Domain	Data		FTP	HTTP	DNS	Telnet	NBios-IP	Mail	DHCP-BOOTP	SNMP	NNTP	NFS/AFS	VoIP	X11	SSH	Gnutella	Kazaa	WinM
www.cisco.com		348.5 KB	51.3 %	0	348.5 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	
www.ibm.com		149.3 KB	22.0 %	0	149.3 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	
www-5.ibm.com		134.2 KB	19.8 %	0	134.2 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	
www-304.ibm.com		13.3 KB	2.0 %	0	13.3 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	
data.coremetrics.com		11.6 KB	1.7 %	0	11.6 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	
stats.www.ibm.com		7.6 KB	1.1 %	0	7.6 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	
dns-cache-la1.sunrise.ch		5.7 KB	0.8 %	0	0	5.7 KB	0	0	0	0	0	0	0	0	0	0	0	0	
newsroom.cisco.com		3.8 KB	0.6 %	0	3.8 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	
239.255.255.250		3.4 KB	0.5 %	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	
www.ibm.ch		1.6 KB	0.2 %	0	1.6 KB	0	0	0	0	0	0	0	0	0	0	0	0	0	
g.msn.com		228	0.0 %	0	228	0	0	0	0	0	0	0	0	0	0	0	0	0	

Figura 2.64. Vista General de Tráfico IP desde NTOP.

Fuente: NTOP, Summary Traffic IP, 2013, http://openmaniak.com/cacti_plugins.php

2.3.3.2 SNMP Y CACTI COMO HERRAMIENTAS DE GENERACIÓN DE ESTADÍSTICAS DE CONSUMO DE DISPOSITIVOS.

SNMP o mejor conocido como Simple Network Management Protocol en su traducción (Protocolo Simple de Administración de Red), establecido en la capa de aplicación de acuerdo al modelo OSI, es el encargado de intercambiar información

de administración entre dispositivos de red, y su modelo de interacción se basa en Administrador/Agente siendo el ultimo el encargado de la colecta de datos y envió, el administrador es el que procesa y da tratamiento a los mismos, para ello en una red administrada SNMP consta de 4 Partes como:[19]

- Sistemas Administrados: Cualquier dispositivo capaz de enviar información de estado y ejecutar un agente.
- Estaciones Administradoras.-Computadoras con Software de administración interno, que permiten comunicarse con agentes SNMP por medio de una red, enviando comandos y recibiendo respuestas.[20]
- Información de Administración.-Todo dispositivo es capaz de describir su estado por medio de una o más variables de estado (objetos) donde se da la base de la información de administración MIB (Management Information Base)

En tanto Cacti se puede considerar como una Suite completa destinada a la generación de gráficos estadísticos haciendo uso de la funcionalidad de RRDTool, capaz de generar gráficos de gran complejidad, empleando SNMP en sus diferentes versión con plantillas predefinidas para algunos casos y en otros siendo posible desarrollarlos desde cero, con un amplio uso en los proveedores de Internet, siendo incluso elementos esenciales en reclamos del servicio ante la venta de un bien no tangible.

2.3.3.2.1. Esquemas o Mapa Conceptual.

En el análisis de protocolos y metodologías para el monitoreo y control de ancho de banda se plantean el siguiente modelo conceptual.

2.3.3.2.2. MIB (Manager Information Base).

Entendida como una base de datos completa y bien definida de Información de administración, con una estructura en árbol dedicada para el manejo y administración

[19] MAURO DOUGLAS, SCHMIDT KEVIN, Essential SNMP, Second Edition

[20] UNIVERSIDAD DEL AZUAY, SNMP, 18 de enero de 2013, http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/snmp.htm

de grupos de objetos con identificadores exclusivos, pudiendo por medio de este acceder a información no solo de hardware, sino estadísticas de rendimiento, etc.[21]

2.3.3.2.3. Versiones, Estructura y Grupo MIB y MIB II.

Las versiones hasta el momento de MIB comprenden el MIB I y MIB-II, pero la más completa se centra en la MIB-II no solo porque es la de más amplio uso por los fabricantes de hardware sino por el hecho que pueden desarrollar sus propias MIBs con la ventaja de que puedan obtener completa autoridad de los objetos, y contemplando así descripciones específicas, en tanto el formato de la estructura de gestión de la Información SMI, en forma de árbol jerárquico global, en el que:

- Un nodo representa un objeto, cuyo identificador único asociado es un OID, proveniente de los nodos del árbol y formado exclusivamente por números enteros, separados por puntos.

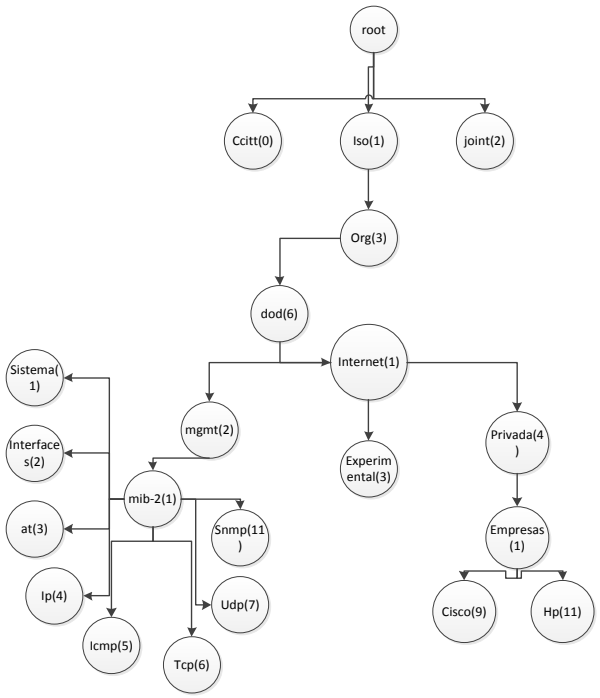


Figura 2.65. Estructura Grafica de la MIB-II.

Fuente: D. Guerrero, Management Information Base MIB, 15 de Agosto de 2013, http://www.linuxfocus.org/Castellano/January1998/article21.html

[21] SNMP, un protocolo de simple gestión, J. Manuel Huidrobo, 16 de Marzo de 2009, http://www.coit.es/publicac/publbit/bit102/quees.htm

En cuanto a los grupos MIB II se comprenden detalladamente 3 niveles adicionales detallados a más de los 8 que incorporan tanto el MIB I como MIB II.

Nivel 1 Systems.- Detalla información genérica del sistema administrador
Nivel 2 Interfaces.- Muestra toda la información de interfaces y objetos en el sistema y sus respectivas estadísticas, y como estos son conectados a la red.
Nivel 3 Address translation.- En este nivel se puede visualizar aquellos objetos apropiados en el mapeo de las direcciones de red a las direcciones físicas.
Nivel 4 IP.- Tablas de rutas y estadísticas IP almacenadas.
Nivel 5 ICMP.- Aquí se almacena todos los contadores ICMP tanto salientes como entrantes y adicionales los paquetes de errores que pudieron haberse suscitado.
Nivel 6 TCP.-Se detalla toda la información relativa al protocolo y las estadísticas puntuales que pudieron haber surgido.
Nivel 7 UDP.- Se especifica estadísticas del protocolo UDP tanto enviados, como recibidos y entregados.
Nivel 8 EGP.- Se detalla a este nivel la información acerca del número de mensajes EGP generados y recibidos.
Nivel 9 CMOT.- Especifica la arquitectura de gestión de red usando los protocolos CMIS/CMIP sobre el modelo OSI sobre la familia de protocolos de internet, definiendo un canal para intercambio de información de control y monitorización.
Nivel 10 Transmisión.- Contiene información acerca de los esquemas de transmisión y protocolos de acceso.
Nivel 11 SNMP.- Contiene y guarda información relevante sobre el protocolo SNMP y su implementación y operación.

Comprendidas las MIB y su estructura y funcionamiento es ahora importante detallar el protocolo SNMP y su forma de trabajo, quizá un tema muy esencial ya que dentro de un Proveedor de Servicios de Internet dicho protocolo comprende un amplio uso en varios aplicativos.

2.3.3.2.4. Protocolo SNMP: Definición, características y versiones.

Definido como Protocolo Simple de administración de red que opera en la capa de Aplicación de acuerdo al modelo OSI, permitiendo el intercambio de información de

administración entre uno o más dispositivos de Red, siendo el más utilizado en la actualidad para el monitoreo de la red, por tal razón casi todo fabricante de equipos con conexión Ethernet o similar incluyen soporte para SNMP, permitiendo su fácil administración y gestión.[22]

Entras las características más destacadas podemos encontrar:

- Envió de alertas o notificaciones en casos de fallos o afines.
- No es necesario disponer de grandes recursos en la red.
- Fácil de implementar y actualizar.
- Estadísticas puntuales de hardware e interfaces de red.

Además entre las versiones disponibles se tiene 3, de las cuales la más usada es la versión 2, aunque la 3 haya incrementado la seguridad no ha tenido gran acogida por tal se detalla las versiones en la siguiente manera:

SNMPv1.-Autentificacion por nombre de comunidad, lista de control de acceso sobre direcciones IP, mantiene un problema con las sobrecargas en la transferencia de datos.

SNMPv2.-Utiliza la autentificación de la primera versión, pero resolviendo el problema de la primera, e incorpora RMON para monitorización remota junto con un mecanismo de recuperación de información en bloques (bulk request).

SNMPv3.- La última versión disponible que engloba a la versión 2 y adiciona seguridad y administración , aportando integridad en los mensajes y autentificación , estableciendo un modelo USM (User-Based Security Model) que no solo especifica autentificación y privacidad sino niveles de encriptación.

2.3.3.2.5. Componentes y Metodologías SNMP.

Se establece un modelo de 3 componentes sobre SNMP que consisten en:

[22] Protocolo SNMP, 17 de diciembre 2013, http://neo.lcc.uma.es/evirtual/cdd/tutorial/aplicacion/snmp.html

- **Dispositivos Administrados.-**Son los dispositivos que intervienen en la red y ejecutan un agente SNMP que reside sobre en una red administrada, recogiendo y almacenando información de administración.
- **Agentes SNMP.-** Modulo que se hospeda sobre un dispositivo administrado, recolectando la información de dicho dispositivo desde la MIB, pudiendo realizar tareas tanto de consulta como de modificación a la MIB.
- **Agentes Proxy.-** Requiere que el producto cuente con una función administradora, ya que por medio de ella se comunicará mediante los debidos protocolos, hoy en día prácticamente en desuso.

En cuanto a la metodología empleada en la monitorización de la red bajo uso del protocolo SNMP se establece de la siguiente forma:

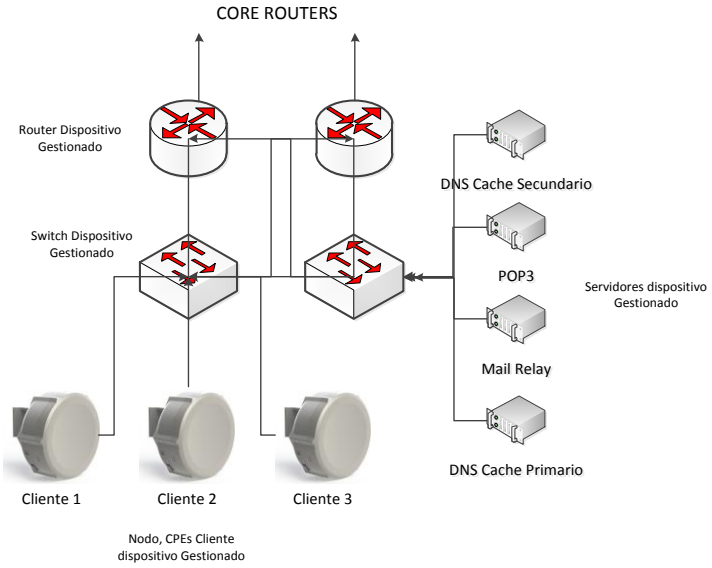


Figura 2.66. Metodología SNMP WISP.

Fuente: Los Autores, Metodología de Monitorización SNMP, 2013.

2.3.3.2.6. Funcionamiento del Protocolo SNMP.

Como ya se observó anteriormente el modo de operación de SNMP era sobre una arquitectura cliente/servidor, encargado de habilitar la comunicación entre agentes y administrador de red, y en si el protocolo describe 4 operaciones esenciales que son:

- **SET**.- Para escritura.

- **GET**.- Para Lectura.
- **GET-NEXT.-** Para realizar recorridos sobre el árbol jerárquico.
- **TRAP**.-Exclusivo para notificaciones.

Es importante describir también todos los mensajes que se gestionan por medio de SNMP que son:

- **GET REQUEST.-** Solicita el valor de un objeto dentro del MIB
- **GET NEXT REQUEST.-** Este mensaje es similar al GET BULK con la diferencia de ser menos eficiente, su función es usar el siguiente objeto luego de que el primero ya se usó, así también permitiendo el descubrimiento de objetos de la MIB.
- **GET BULK.-** Disponible desde la versión 2, solicita el siguiente atributo de un objeto cuando el anterior ya se ha usado, usado también para descubrir objetos de la MIB.
- **SET REQUEST.**-Este mensaje se orienta a modificar en la MIB un valor de un objeto.
- **GET RESPONSE.-**Respuesta de un agente en la red que contiene valores requeridos por un Get o Set.
- **TRAP.-**Generados por los agentes con el fin de notificar alertas.
- **INFORM, NOTIFICATION, REPORT.-** Funcional desde la versión 2 intercambia mensajes de información, confirmación etc., de un dispositivo administrador a otro.

2.3.3.2.7. CACTI como generador de estadísticas.

Cacti es una herramienta suite completa en la generación de estadísticas y dedicadas al monitoreo a base de plantillas preestablecidas, siendo posible en el caso de que las mismas no existan poderlas implementar, su funcionamiento se basa en recopilar datos de los diversos dispositivos agregados a una red, y gracias a RRDTool`s (Round-Robin Database Tool), almacenar y luego procesar dicha data empleando algoritmos y técnicas que permitan visualizar la información adecuadamente, que luego serán mostrados e interpretados sobre una interfaz intuitiva y fácil de usar. Pudiendo disponer de información en tiempo real de casi cualquier dispositivo de

Red y estadísticas que van desde tráfico de datos, porcentaje de consumo de CPU, temperaturas, etc.

Su amplio uso en proveedores de Internet se encuentra más que justificado, ya muy aparte de la monitorización de dispositivos es posible obtener estadística de consumo de ancho de banda puntuales, y que al ser un bien intangible muchas veces es objeto de reclamo sobre problemas en el servicio.

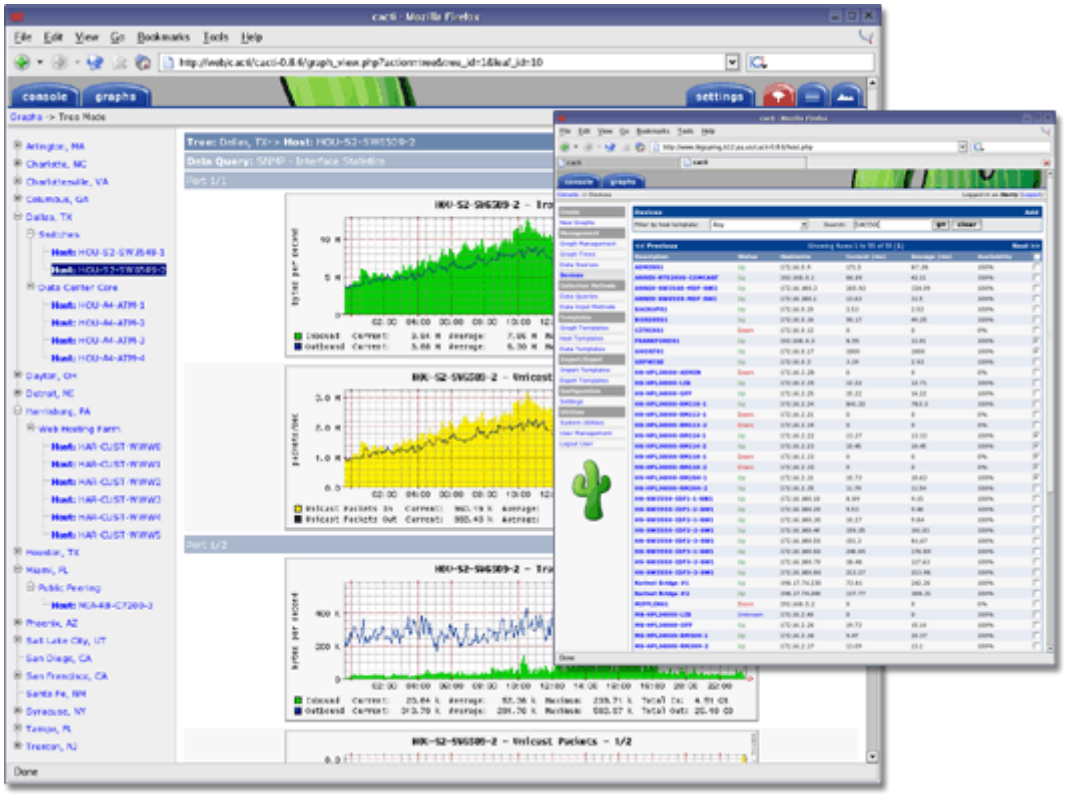


Figura 2.67. Vista principal sistema de Monitoreo Cacti.

Fuente: Los Autores, Estadísticas de Monitorización, 2013.

2.3.3.2.8. Aplicaciones de CACTI en un WISP.

El monitor Cacti cubre un amplio uso dentro de un entorno WISP, de los cuales su primer uso y el más relevante se orienta a poder generar estadísticas de monitorización de dispositivos de red como Puntos de Acceso, Switch, Router y elementos de hardware de Networking usados dentro de un WISP, pudiendo

monitorizar aspectos claves a nivel de rendimiento y determinantes para brindar un nivel de operatividad optimo en la red de datos, adicional se orienta a la a la generación de estadísticas de consumo, punto relevante ya que el Internet al ser un bien no tangible, dicho medio faculta a poder monitorizar adecuadamente el servicio incluso con problemas suscitados en tema de cortes, Mikrotik es una tecnología por medio de RouterOS que incorpora muchas herramientas como SNMP o su propio servidor de estadísticas para interpretar el tráfico de datos tanto desde el NOC como desde el CPE del cliente final, posibilitando un toma de decisiones acertadas en gestión y administración del tráfico, quizá muchas de las veces una de las problemáticas presentes con Cacti es la creación de templates para RouterOS o sistemas emergentes y monitorización de determinados aspectos del sistemas y su versionamiento que muchas de las veces hace necesaria la actualización de dichos templates, al momento desde cacti es posible utilizar templates para monitorizar:

- **Sistema**
    - Carga de CPU
    - Tiempo de Uptime
    - Uso de Disco
    - Uso de Ram
    - Temperatura.
    - Voltaje
- **IP**
    - Conexiones PPP
    - Entradas ARP
    - DHCP Server Leases
    - Count Neighbor

- **Interfaces de Red.**
    - TX/RX Bits/Bytes
    - TX/RXPackets

- **Wireless**
    - Intensidad de señal
    - TX/RX Rate

- Frecuencia 802.11a/b/g

- **Queues**
  - Simple Queue Packets
  - Queue Tree Packets

2.3.3.3 CACHE DINÁMICO Y ESTÁTICO.

Los sistemas de cache o proxy han sido elementos de red clave en algunas empresas e ISP desde hace algunos años atrás y que ahora su uso se ha visto incrementado notablemente, el hecho radica en que el acceso a Internet se ha vuelto más común por lo tanto miles de personas que quizá hace un par de años atrás no podían acceder a la gran red, ahora lo hacen sin problema alguno y que suponemos que ese número en años posteriores se verá duplicado o triplicado con facilidad, prácticamente convirtiendo ahora el servicio en un necesidad y dado los contenidos generados por web 2.0 que son cada vez más pesados y demandan mayor ancho de banda, generando grandes problemas a los proveedores de acceso a Internet tales como incremento de saturación de canales o latencia, por tal muchas empresas desarrolladoras de Software ha visto en esta como una actividad económica muy lucrativa desarrollando soluciones orientadas al cacheo dinámico y estático y reducir costos notables en pagos sustanciosos de ancho de banda, y la gran ventaja de por si brindar al usuario final una experiencia asegurada, muchas soluciones propietarias incluso son más costosas que la contratación de ancho de banda ya que sus políticas de licenciamiento son poco flexibles y representan costos significativos ya que casi todos detallan un valor especifico de su licencia por el número de peticiones generadas mas no un precio fijo, por tal algunos ISP han optan por trabajar en sus propias versiones con una base en software libre ya realizada, trabajando tan bien como una propietaria, aunque lógicamente hay diferencias notables en cuanto al tratamiento de la forma de cache y el empleo de algoritmos más eficientes.

El funcionamiento se basa en que un servidor intermediario recibe peticiones de los usuarios o aplicaciones, este se encarga de procesar la petición verificando si dentro del contenido solicitado se solicita algún objeto que este en el cache local y pueda ser

resuelto y entregado por este mismo o caso contrario generar la petición hacia el Internet para descargar el objeto y dejar una copia local en el cache, es importante recalcar que no todos los proxies son utilizados como cache sino algunos como Gateways que controlan el paso del tráfico por medio de ellos facilitando así el cumplimiento de funciones de seguridad, e incluso muchos de ellos emplean modelos de comportamiento complejos que analizan la generación de enlaces dinámicos, como en el caso de videos dinámicos.

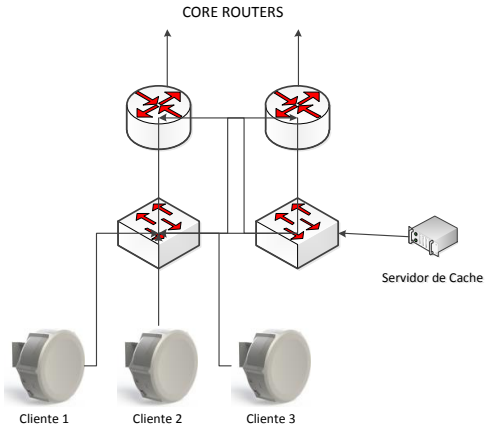


Figura 2.68. Modelo de topología para ubicación de Servidor Cache.

Fuente: Los Autores, Topología de Ubicación de Cache, 2013

La estructura de la topología puede variar según la forma en cómo vaya a operar el Sistema de Cache de tal forma que es posible hasta Jerarquizarlos, e incluso el soporte para operar en modo transparente e indetectable, cabe recalcar es necesario que para que haya un funcionamiento dedicado el mismo debería operar sobre un Hardware con altas prestaciones o de carácter dedicado que posibilite un procesamiento de peticiones y despacho inmediato reduciendo al mínimo tiempos de latencia.

Sigsignet ha visto necesaria su implementación ya que siendo, Sígsig un Cantón donde al acceso a Internet para su reventa se encuentra Limitado y cuyas capacidades de Internet manejadas se dan por medios limitados se ha optado por dichas soluciones para poder brindar una experiencia más satisfactoria en el servicio. En la actualidad existen muchas soluciones propietarias y Open Source, que varían

exclusivamente es su forma de procesamiento del contenido almacenado y su distribución, siendo actualmente usada en los WISP la solución de BMSoftware mejor conocida como ThunderCache, ya que al ser una solución propietaria su constante desarrollo justifica un producto de calidad y se adapta a los constates cambios que la red genera, quizá su política de licenciamiento es poco flexible ya que la misma se realiza por conexiones generadas, el sistema como tal ha evolucionado increíblemente a tal punto que antes era necesario el desarrollo de plugins o componentes por dominio o sitio web que permitan realizar el caching de dichos objetos provenientes de esos sitios web, o quizá la interacción que se la hacía antes con soluciones Open Source como en sus inicios lo es Squid un sistema para realizar caching estático.

Conclusiones del Capítulo II

Culminado el desarrollo de este capítulo en donde se han dado a conocer aspectos teóricos técnicos necesarios para ampliar el campo de visión en el proceso de restructuración de la empresa de Sigsignet, además de divisar las capacidades de Mikrotik - RouterOS y su apoyo en el proceso de reestructuración que sigue la empresa Sigsignet, por ende una sólida base de conocimientos y las diversas soluciones que contemplan el medio para dar solución al problema es importante antes del proceso de reestructuración.

CAPÍTULO III: estudio y analisis del estado actual y deseado de la red y servicios.

Objetivos:

- Realizar un completo estudio y análisis del estado actual de la red y servicios de la empresa Sigsignet, determinando en dicho análisis un estado presente y el deseado del mismo.

Objetivos Específicos:

- Conocer la infraestructura de la empresa y políticas vigentes sobre la red de datos.
- Analizar la topología de red física-lógica actual y definir un modelo deseado de la misma.
- Evaluar el rendimiento actual de la red utilizando indicadores clave que permitan determinar la salud actual de la red.
- Emplear DUDE como software gratuito de Mikrotik para monitorización de enlaces y generación de estadísticas.

3.1 ANALISIS DE LA INFRAESTERUCTURA ACTUAL Y DESEADA

El tema central de este capítulo es poder realizar un análisis de la condición actual de la red y todos sus servicios, con el objetivo planteado de que el proceso de reacondicionamiento se lo lleve de la mejor manera y la nueva red permita no solo abarcar mayor capacidad sino llevar la misma a nuevo nivel, posibilitando poder brindar un servicio de calidad y con estándares de prestación de servicios eficientes cumpliendo las exigencias.

3.1.1 MODELO DE RED

El modelo de red usado y el deseado en la red de datos de la empresa Sigsignet, tomará un giro completo ya que al momento no se contempla una distribución ideal y menos aún en su implementación inicial se ha seguido normas o topologías modelo que aseguren y garanticen una distribución ideal del tráfico y ubicación ideal de los dispositivos, su infraestructura de distribución al momento está contemplada de la forma más básica y elemental para dar conectividad a los abonados que a su vez ha permitido brindar un servicio de calidad, pero dado su exponencial crecimiento dicho modelo ya no es capaz de abastecer.

Para tal en la nueva red, se pretende separar y aislar las capas de tal forma que se puedan volver sistemas autónomos cuya funcionalidad se encuentre bien definida, estableciendo un modelo de red jerárquico en capas explicados a continuación.

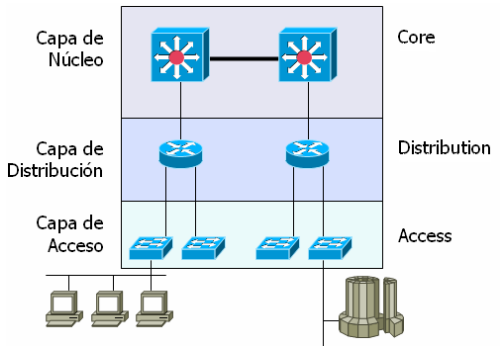


Figura 3.1 Modelo Jerárquico 3 Capas de Cisco.

Fuente: Luis R., El modelo jerárquico de 3 Capas de Cisco, 28 de Noviembre de 2008, http://www.cisco.com/web/LA/soluciones/educacion/cs_edu_networkers.html

3.1.1.1 CAPA DE ACCESO

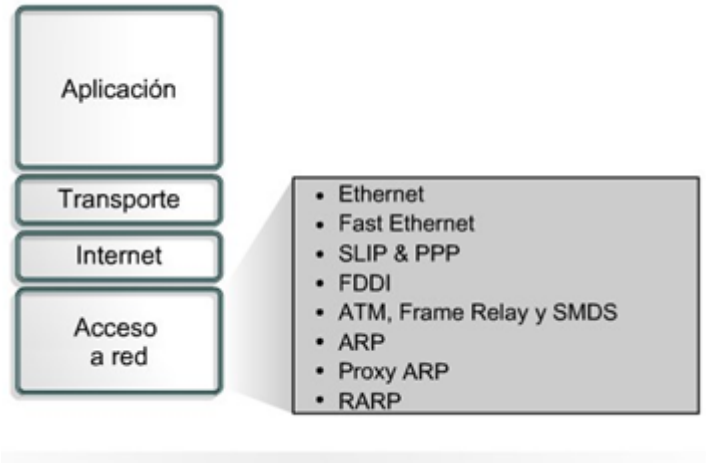


Figura 3.2 Capa de acceso

Fuente: Jimmy Hernandez, Introducción a TCP/IP(La capa de acceso de red), 18 de Junio de 2008, http://expertoccna.blogspot.com/2008/06/la-capa-de-acceso-de-red-tambin-se.html

La capa de Acceso de Red (Network Access Layer) es la capa inferior de la jerarquía de protocolos de TCP/IP. Es equivalente a la capa 1 y 2 del modelo OSI (con algunas funciones de la capa 3). Encapsula Datagramas en Frames y mapea direcciones IP a direcciones físicas. Esta capa se construye con la tarjeta de red, los drivers y los programas asociados.

Nº de capa	OSI
7	Aplicación
6	Presentación
5	Sesión
4	Transporte
3	Red
2	Enlace de datos
1	Física

TCP/IP	Nº de capa
Aplicación	4
Transporte	3
Internet	2
Acceso a la red	1

Figura 3.3. Modelos de Referencia

Fuente: Universidad Veracruzana, Adair Santos G., La Seguridad Informatica en Redes Inalambricas, Xalapa-Enríquez, Veracruz Agosto 2008, p. 26

En la condición inicial la empresa Sigsignet, esta capa se encuentra construida inicialmente por dos tarjetas de red D-Link 10/100/1000 Mbps conjuntamente con sus respectivos controladores montados sobre un servidor Linux Ubuntu 8.04, en el estado deseado de la nueva red se pretende reemplazar por hardware Mikrotik con su variedad de soluciones y appliances dedicadas y sobre todo los beneficios de RouterOS ya descritos en capítulos anteriores.

La capa Core Descrita en el estado actual y deseado será establecida de la siguiente forma.

Periodo	Tarjeta	Plataforma
2003-2012	D-Link 10/100/1000 Mbps	Ubuntu Desktop 8.04
2012 en adelante	RB110AHx2 power PC	Mikrotik v6.9

Tabla 3.1. Interfaces de Red

Fuente: DLink, Network Interface Gigabit DLink, Enero 2013,

http://www.dlink.com/es/es/support

3.1.1.2 CAPA DE DISTRIBUCIÓN

Es el medio de comunicación entre la capa de acceso y el Core. Las funciones de esta capa son proveer ruteo, filtrado, acceso a la red WAN y determinar que paquetes deben llegar al Core. Además, determina cuál es la manera más rápida de responder a los requerimientos de red, por ejemplo, cómo traer un archivo desde un servidor.

Aquí además se implementan las políticas de red, por ejemplo: ruteo, Access-list, filtrado de paquetes, cola de espera (Queuing), se implementa la seguridad y políticas de red (traducciones NAT y firewalls), la redistribución entre protocolos de ruteo

(incluyendo rutas estáticas), ruteo entre VLANs y otras funciones de grupo de trabajo, se definen dominios de broadcast y multicast[23].

En la plataforma inicialmente utilizada (Ubuntu 8.04), y en la condición actual de la red, la capa de distribución se encontraba configurada de la siguiente manera:

SCRIPT DE CONFIGURACION DE IPTABLES

#!/bin/bash
#Dispositivo de red de internet

EXIF="eth1"
#Dispositivo de red local

INIF="eth0"
 # Puertos tcp que se desean redirigir (separados por espacios) puertos TCP="7778"
 # Puertos udp que se desean redirigir (separados por espacios) puertos
UDP="7779"

 # ip a la que se le redirigen los puertos

pc2="192.168.0.2"
fail=0
[-f /etc/default/rcS] && . /etc/default/rcS

. /lib/lsb/init-functions

log_begin_msg "Aplicando Reglas de Firewall..."

Borrado de reglas anteriores

iptables -F || fail=1

iptables -X || fail=1

[23] Luis R., Modelo Jerárquico 3 capas de Cisco, 11 de Noviembre de 2008, http://ipref.wordpress.com/2008/11/28/modelo-jerarquico-de-red/

iptables -Z || fail=1

iptables -t nat -F || fail=1

Establecemos política por defecto

iptables -P INPUT ACCEPT || fail=1

iptables -P OUTPUT ACCEPT || fail=1

iptables -P FORWARD DROP || fail=1

iptables -t nat -P PREROUTING ACCEPT || fail=1

iptables -t nat -P POSTROUTING ACCEPT || fail=1

 # Marcar paquetes salientes con su ip de origen

iptables -t nat -A POSTROUTING -o $EXIF -j MASQUERADE || fail=1

 # Reenvío de IP

echo 1 > /proc/sys/net/ipv4/ip_forward || fail=1

 # Aceptar paquetes para reenviar procedentes de la red local

iptables -A FORWARD -i $INIF -o $EXIF -j ACCEPT || fail=1

 # Aceptar paquetes para reenviar procedentes de internet de conexiones ya establecidas

iptables -A FORWARD -i $EXIF -o $INIF -m state --state RELATED,ESTABLISHED -j ACCEPT || fail=1

##Se redirigen los puertos configurados arriba

for puerto in $puertosTCP

do

iptables -A FORWARD -i $EXIF -o $INIF -p tcp --dport $puerto -j ACCEPT || fail=1

iptables -t nat -A PREROUTING -i $EXIF -p tcp --dport $puerto -j DNAT --to $pc2:$puerto ||

fail=1

done

for puerto in $puertosUDP

do

iptables -A FORWARD -i $EXIF -o $INIF -p udp --dport $puerto -j ACCEPT || fail=1

iptables -t nat -A PREROUTING -i $EXIF -p udp --dport $puerto -j DNAT --to $pc2:$puerto || fail=1

done

 # Se muestran los resultados

log_end_msg $fail

if [$fail -eq 0]

then

log_success_msg "Verifique que lo que se aplica con: iptables -L -n."

else

log_warning_msg "Se ha producido un error al aplicar alguna de las reglas"

fi

FIN SCRIPT DE CONFIGURACION DE IPTABLES

Segmentación de Ancho de Banda.

La segmentación de ancho de banda en la condición actual de la red Sigsignet se encuentra implementada mediante el algoritmo CBQ destinado a gestión tráfico, que permite ayudar a compartir el ancho de banda por igual pero que a su vez demanda una noción básica sobre bash y arquitectura acerca de CBQ, dividiendo el tráfico de usuarios en una jerarquía de clases, basadas en cualquier combinación de direcciones IP, protocolos y tipo de aplicaciones. En el mismo servidor no es más que un guión escrito en BASH y que forma parte del paquete IPROUTE, a continuación se presenta el script utilizado para la red SIGSIGNET, con las segmentaciones y prioridades asignadas desde sus inicios con apenas mínimas modificaciones sobre la marcha.

```
#!/bin/sh

# Script de Segmentación de Ancho de Banda Utilizando CBQ
# < http://sourceforge.net/projects/cbqinit/ >

#####################
# VARIABLES ########
#####################
# COMANDOS
IPTABLES="/sbin/iptables -t mangle"
TC=/sbin/tc
CBQ=/sbin/cbq

# INTERFACES
WAN="0/0"
DEVWAN="eth0"
DEVLAN="eth1"

# VELOCIDAD DE INTERFACES DE RED
ETH0_BW="100Mbit"
ETH1_BW="100Mbit"
```

```
# PUERTOS
PROXY_PORT="8080"
SMTP_PORT="25"
P2P_PORT="4662"

####################
# ANCHOS DE BANDA###

####################
BW24="24Kbit"
BW32="32Kbit"
BW48="48Kbit"
BW64="64Kbit"
BW96="96Kbit"
BW128="128Kbit"
BW256="256Kbit"
BW512="512Kbit"

####################
# PRIORIDADES ######
####################
NORMAL="5"
ALTA="2"
BAJA="8"

####################
# CLIENTES #########
# RED 192.168.1.0/24
####################

# CLIENTE 1
LAN1="192.168.1.2/32"

# CLIENTE 2
LAN2="192.168.1.3/32"
```

##########

 # INICIO #

##########

$CBQ stop

$IPTABLES -F

$IPTABLES -X

$TC qdisc add dev $DEVWAN root handle 1: cbq bandwidth $ETH0_BW avpkt 1000 cell 8

$TC qdisc add dev $DEVLAN root handle 2: cbq bandwidth $ETH1_BW avpkt 1000 cell 8

####################

 # CLIENTES #########

####################

 # CLIENTE 1

$IPTABLES -A PREROUTING -s $LAN1 -d $WAN -i $DEVLAN -j MARK --set-mark 1

$IPTABLES -A FORWARD -s $WAN -d $LAN1 -i $DEVWAN -o $DEVLAN -j MARK --set-mark 2

$IPTABLES -A OUTPUT -d $LAN1 -p tcp --sport $PROXY_PORT -o $DEVLAN -j MARK --set-mark 2

$TC class add dev $DEVWAN parent 1:0 classid 1:1 est 1sec 2sec cbq bandwidth $ETH0_BW rate $BW12 allot 1514 cell 8 weight 1 prio $NORMAL maxburst 20 avpkt 1000 bounded

$TC class add dev $DEVLAN parent 2:0 classid 2:1 est 1sec 2sec cbq bandwidth $ETH1_BW rate $BW24 allot 1514 cell 8 weight 1 prio $NORMAL maxburst 20 avpkt 1000 bounded

$TC filter add dev $DEVWAN protocol ip handle 1 fw classid 1:1

$TC filter add dev $DEVLAN protocol ip handle 2 fw classid 2:1

 # CLIENTE 2

$IPTABLES -A PREROUTING -s $LAN2 -d $WAN -i $DEVLAN -j MARK --set-mark

3

$IPTABLES -A FORWARD -s $WAN -d $LAN2 -i $DEVWAN -o $DEVLAN -j MARK --set-mark 4

$IPTABLES -A OUTPUT -d $LAN2 -p tcp --sport $PROXY_PORT -o $DEVLAN -j MARK --set-mark 4

$TC class add dev $DEVWAN parent 1:0 classid 1:2 est 1sec 2sec cbq bandwidth $ETH0_BW rate $BW12 allot 1514 cell 8 weight 1 prio $NORMAL maxburst 20 avpkt 1000 bounded

$TC class add dev $DEVLAN parent 2:0 classid 2:2 est 1sec 2sec cbq bandwidth $ETH1_BW rate $BW24 allot 1514 cell 8 weight 1 prio $NORMAL maxburst 20 avpkt 1000 bounded

$TC filter add dev $DEVWAN protocol ip handle 3 fw classid 1:2

$TC filter add dev $DEVLAN protocol ip handle 4 fw classid 2:2

echo "ANCHOS DE BANDA ASIGNADOS"

 # FIN DEL ARCHIVO #

##################################

Proxy Cache Squid y Administración de Usuarios.

- En la configuración inicial del servidor de Sigsignet también se encuentra Squid que sirve como un Servidor Intermediario (Proxy), cache de contenido de Red para los protocolos HTTP, FTP, GOOPHER, WAIS, Proxy de SSL, cache transparente, WWCP, aceleración HTTP, cache de consultas DNS, filtrado de contenido y control de acceso por IP y por usuario.

La arquitectura de SQUID es similar a la descrita en el capítulo II en proxy cache, siendo la principal diferencia el proceso de caching en SQUID con objetos estáticos y con Thundercache con objetos dinámicos.

- La configuración de proxy cache de manera transparente se encuentra implementada mediante SQUID, a continuación se muestra el contenido del archivo squid.conf

http_port 3128 transparent

cache_mem 100 MB

cache_dir ufs /var/spool/squid 150 16 256

acl red_local src 192.164.10.0/24

acl localhost src 127.0.0.1/32

acl all src all

http_access allow localhost

http_access allow red_local

En la implementación posterior se la realiza con Mikrotik 6.9 en paralelo a ThunderCache una solución propietaria e independiente, la cual cuenta con notables mejoras en comparación con Ubuntu 8.04. En esta capa una de las principales diferencias es la implementación del Firewall el cual permite personalizarlo a un nivel muy detallado y con una complejidad mínima.

A continuación se muestra algunas configuraciones realizadas en esta capa:

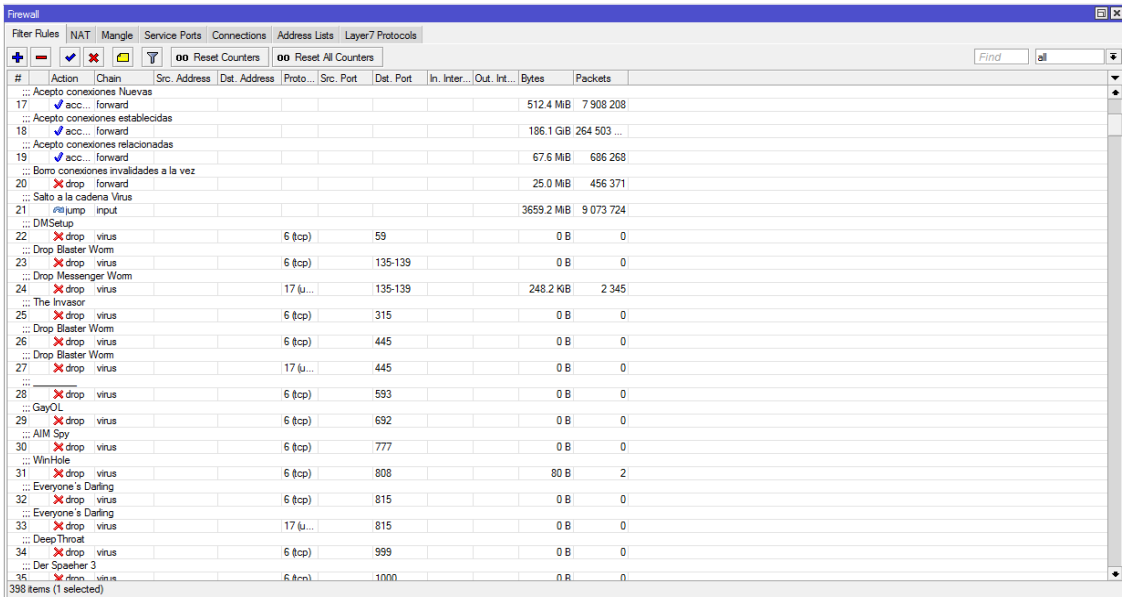


Figura 3.4. Firewall-Filter Rules

Fuente: Los Autores, Firewall Filter RouterOS, 2013.

En la Figura 3.4 se puede observar algunas de las reglas de filtrado que se han implementado en la nueva plataforma Mikrotik en donde constan bloqueos de direcciones invalidas, spammers, ataques DDoS, Virus, Ataques de Fuerza Bruta, Accesos desde IP Autorizadas etc. Buscando siempre brindar un valor agregado en temas de seguridad sobre la red de datos de la empresa y a sus clientes. Es por tal razón que la parte de Firewall ha requerido un amplio trabajo, análisis incluso experiencias acumuladas para elaborar una solución permisiva pero a su vez eficiente a nivel de protección ya que ningún ISP tiene como objetivo el bloqueo de puertos o servicios simplemente su respectivo control y buen uso.

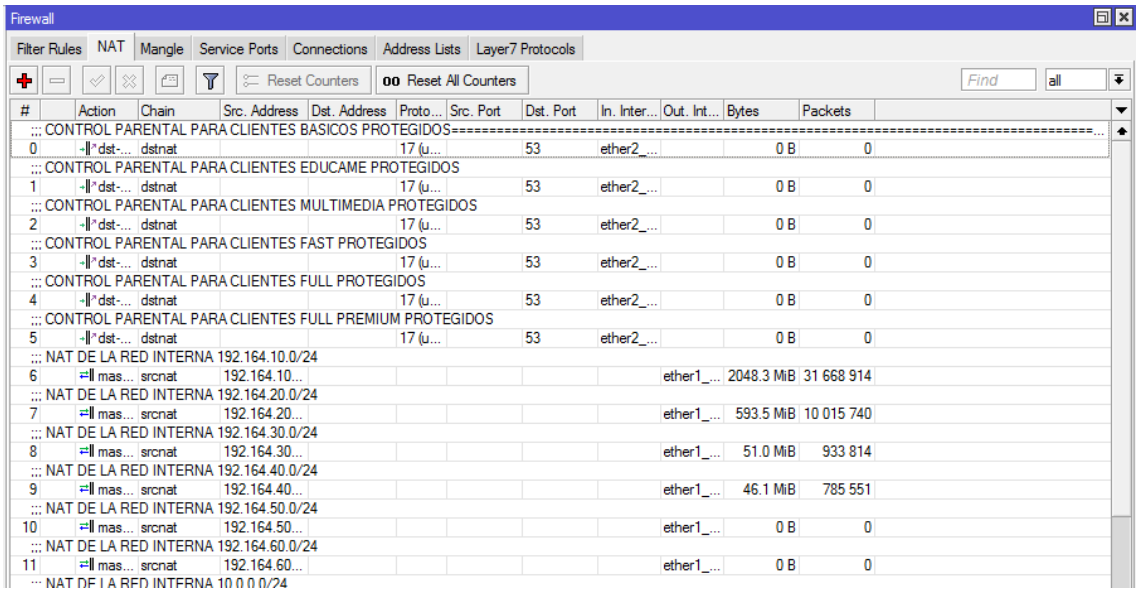


Figura 3.5. Firewall-NAT

Fuente: Los Autores, Firewall NAT RouterOS, 2013.

En la Figura 3.5 se muestra la configuración del NAT para las subredes específicas que la empresa maneja y que realizan la traducción de direcciones privadas a públicas, complementado con reglas DST-NAT dedicadas a brindar un servicio de control parental que la empresa ofrece por cada uno de sus planes de Internet.

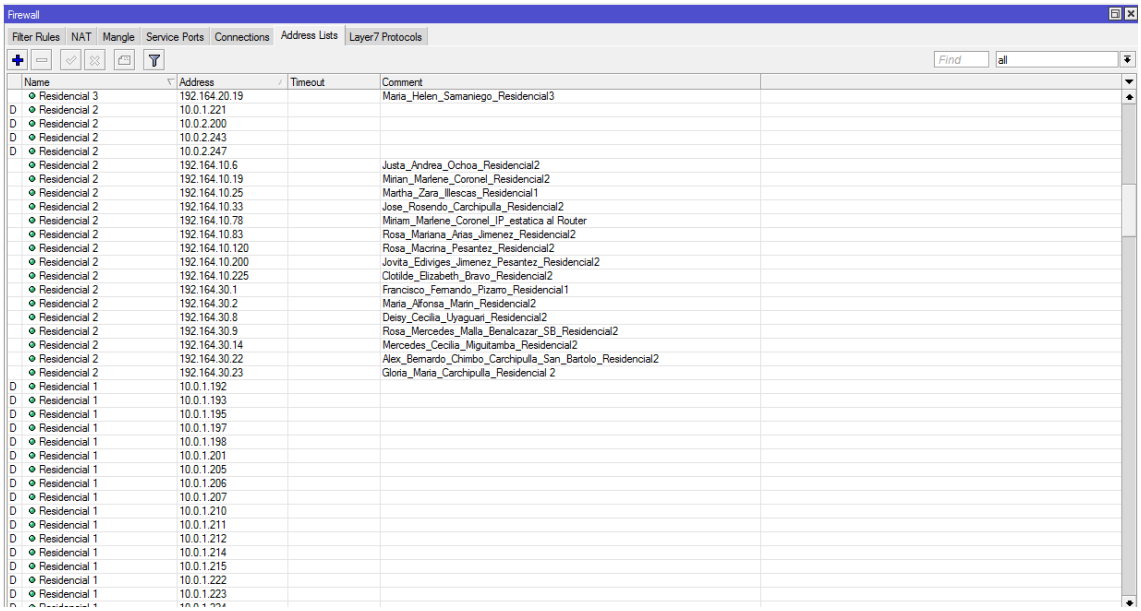


Figura 3.6. Firewall-Address Lists

Fuente: Los Autores, Firewall Address List RouterOS, 2013.

La figura 3.6 muestra la forma en como los clientes son asignados a sus respectivos planes de Internet por ende su respectiva segmentación de ancho de banda, algunos de los clientes se entrega la capacidad por medio de IP estáticas en tanto que otros por medio de IP Dinámicas, siendo mucho más sencillo la administración y soporte que en comparación con Ubuntu 8.04 o la forma en como se venía ya administrando la red, además de llevar la lista de los clientes o abonados también se puede llevar la lista de los equipos AP´s que se tienen instalados y equipos de red en sí, para poder administrar su correcto funcionamiento e incluso en temas de monitorización.

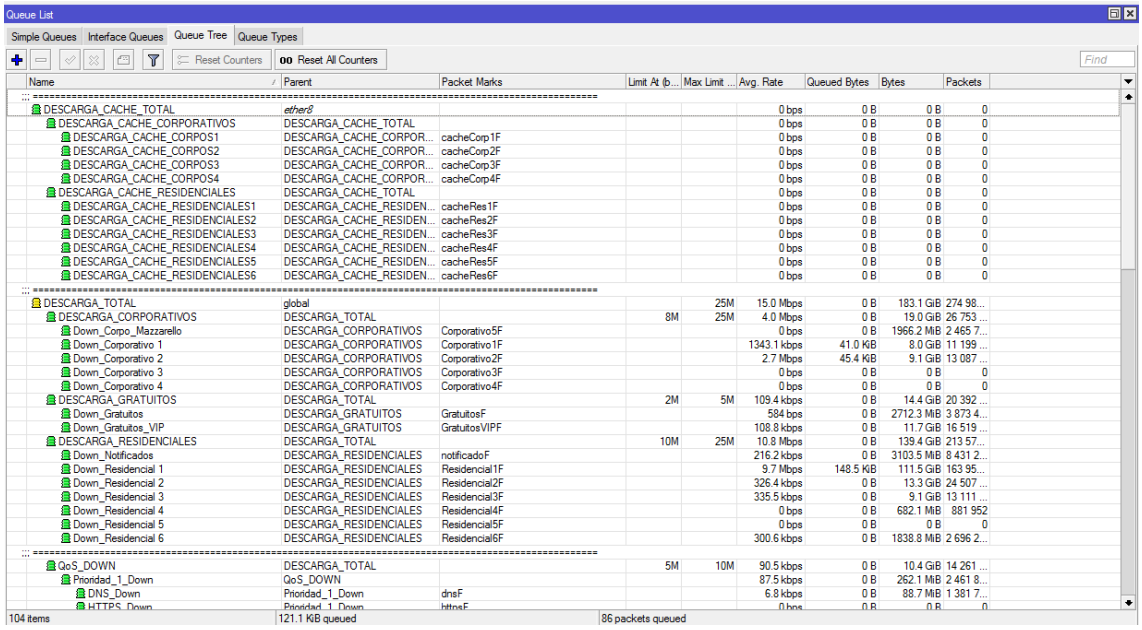


Figura 3.7. Encolamiento Queue Tree

Fuente: Los Autores, Queue Tree RouterOS, 2013.

La figura 3.7 muestra el árbol de colas que se ha creado para segmentar el ancho de banda, en esta parte se toma en cuenta el ancho de banda tanto de subida como el de bajada así como también sus prioridades aplicadas a los diversos protocolos que van del 1 al 8 siendo el de más baja prioridad el 8 y el de más alta prioridad el 1, así como también la distribución equitativa la segmentación de cache, ya que el mismo al poder distribuir cantidades elevadas de ancho de banda si de por medio no hay una distribución o encolamiento podría causar que los diversos puntos de acceso que distribuyen el servicio se saturen recayendo en una pérdida de rendimiento significativa.

3.1.1.3 CAPA CORE

En el análisis de esta capa se ha pretendido comparar entre las soluciones actuales y las deseadas de la red de Sigsignet con la cantidad actual de abonados y lo que se pretende alcanzar en un futuro cercano.

	Actual	Deseado
		
Modelo	Switch D-Link 8 ptos 10/100 modelo: DES-1008D/A	SG 200-26P
Puertos	8 (10/100Base-TX)	24 x 10/100/1000 + 2 x Gigabit SFP combinado
Estándares	IEEE 802.3 10Base-T Ethernet Repeater, IEEE 802u 100Base-TX class II Fast Ethernet repeater y ANSI/IEEE Std 802.3 Nway auto-negotiation.	IEEE 802.3, IEEE 802.3u, IEEE 802.3z, IEEE 802.1D, IEEE 802.1Q, IEEE 802.3ab, IEEE 802.1p, IEEE 802.3af, IEEE 802.3x, IEEE 802.3ad (LACP), IEEE 802.1w, IEEE 802.1x
Interfaces	RJ-45	12 x 10Base-T/100Base-TX/1000Base-T - RJ-45 12 x 10Base-T/100Base-TX/1000Base-T - RJ-45 - PoE 2 x SFP (mini-GBIC)
Transferencia	10/100 Mbps Full Duplex, autodetect	Capacidad de conmutación : 38.69 Mpps Rendimiento de reenvío (tamaño de paquete de 64 bytes) : 52 Gbps
Método de Acceso	CSMA/CD	RMON, HTTP, TFTP
LEDs	Por puerta: link/activity, velocidad 100Mbps, Full-duplex	Actividad de enlace, velocidad de

indicadores	collision. Por switch : Power	transmisión del puerto, sistema, PoE
Fuente de poder	Externa	Interna
Consumo	8-12 Watts Máximo [24]	12 Watts Máximo[25]

Tabla 3.2. Cuadro comparativo de Switchs en la Capa Core

Fuente: Loa Autores, Modelos de Switch, 2012.

La capa núcleo o capa core a menudo se denomina Backbone de la red. Los routers y los switches en la capa núcleo proporcionan conectividad de alta velocidad. En una LAN empresarial, la capa núcleo puede conectar múltiples edificios o sitios, además de proporcionar conectividad a la granja de servidores. La capa núcleo incluye uno o más enlaces a los dispositivos en el margen empresarial a fin de admitir Internet, redes privadas virtuales (VPN), extranet y acceso a la WAN[26].

La implementación de una capa núcleo reduce la complejidad de la red, lo cual facilita la administración y la resolución de problemas.

Objetivos de la capa núcleo

El diseño de la capa núcleo permite la transferencia de datos eficiente y de alta velocidad entre una y otra sección de la red. Los objetivos principales del diseño en la capa núcleo son:

- Proporcionar un 100% de tiempo de actividad

[24] D-Link, DES-1008D Características Técnicas, 2012, http://www.dlinkla.com.ec/des-1008d

[25] Cisco, Switches inteligentes Cisco de la serie 200 Cisco Small Business, finales de 2013. http://www.cisco.com/c/dam/en/us/products/collateral/switches/small-business-100-series-unmanaged-switches/data_sheet_c78-634369_Spanish.pdf

[26] Luis R., Modelo Jerárquico 3 capas de Cisco, 11 de Noviembre de 2008, http://ipref.wordpress.com/2008/11/28/modelo-jerarquico-de-red/

- Maximizar el rendimiento
- Facilitar el crecimiento de la red

Tecnologías de capa núcleo

Entre las tecnologías que se utilizan en la capa núcleo se incluyen:

- Routers o switches multicapa que combinan el enrutamiento y la conmutación en el mismo dispositivo
- Redundancia y balanceo de carga
- Enlaces de alta velocidad y agregados
- Protocolos de enrutamiento escalables y de rápida convergencia, como el Protocolo de enrutamiento de gateway interior mejorado (EIGRP) y el protocolo Abrir primero el camino más corto (OSPF).[27]

Sigsignet en la implementación de su red inicial, la capa de distribución comprendida entre Switchs y Routers que se utilizan no era de carácter dedicado y con soporte para manejar capacidades de tráfico significativas no solo por las pocas prestaciones de hardware que dichos equipos ofrecían como por ejemplo un Switch empleado modelo D-Link 8 ptos 10/100 modelo: DES-1008D/A en el nodo Sígsig y otro de los mismo en el nodo Huallil que cumplían hasta la fecha el trabajo de distribución en dicha capa, que durante sus inicios cumplían las expectativas deseadas pero que conforme la red crecía, el rendimiento se veía comprometido. En la actualidad la mejora de esta capa viene por parte de la mano de Cisco System, fabricante de soluciones de Networking con ya varios años en el mercado y notable reconocimiento sobre dicho segmento que en complemento en este caso con Mikrotik pretende dar la solución a este problema presente, para tal se pretende colocar un switch administrable modelo SG200-26 el cual ya cuenta con características relevantes en la capa de distribución y que pretende mejorar y elevar el rendimiento de la misma, agregando además características de seguridad y control sobre capa 2 y su completo set de funcionalidades con las que cuenta.

El cuanto a nivel del Router también se pretende asegurar el rendimiento por la solución de Mikrotik, al ser un appliance de carácter dedicado el nivel de operación ininterrumpido se asegura aún más, además las prestaciones de Hardware contra el tradicional Servidor Ubuntu que la empresa venia manejado, pretende dar una solución definitiva y concreta, basado en un hardware con procesadores y recursos dedicados, e incluso buscando alta disponibilidad.

Distribución de los Puntos de Red, Enlaces y Áreas de Cobertura

La red actual cuenta con dos puntos de red principales para dar cobertura al cantón Sígsig:

- **Nodo Sígsig:** este nodo se encuentra en el centro de Sígsig y cuenta con un AP Tranzeo 802.11b/g (2.4 GHz) TR6 Router con una antena Externa de 19 dBi sumada con una potencia que nos da mayor ganancia y rango de cobertura.

- **Nodo Huallil:** en este nodo se encuentran 3 AP´s los cuales cubren la mayor parte del cantón Sígsig, el primer AP es otro Tranzeo 802.11b/g (2.4 GHz) TR6 Router que consta con dos paneles sectoriales de 120 grados el uno apuntando a la parroquia Cutchil y el otro apuntando a la parte central del cantón Sígsig y también acogiendo gran parte de comunidades aledañas. Un segundo AP NanoStation 5 con un plato de gran alcance y cobertura con una ganancia de 23 dBi que cubre también la parte central sur del cantón Sígsig. Y un cuarto AP NanoStation 5 con una antena externa de tipo grilla que se encuentra apuntando a la parte norte de Sígsig para dar cobertura a un cliente corporativo.

  En la actualidad, la distribución de Puntos de Red, enlaces y áreas de cobertura tiene mucho por mejorar, quizá la ubicación geográfica del Nodo Actual tiene una posición aventajada pero sobre ello inconvenientes como la mala administración del espectro en la zona por la competencia y la poca regulación sobre el órgano estatal de telecomunicaciones no permiten aun brindar un

servicio de calidad, por tal razón incrementar soluciones más elaboradas son necesarias como el uso de script mediante equipos que monitorean constantemente la saturación de los canales y espectro y realicen procedimientos automáticos de cambio de canales para mantener un servicio estable, se ha planteado como soluciones a dichas problemáticas.

3.1.2 SERVIDORES Y EQUIPOS DE RED ACTUALES Y DESEADOS.

Comprende los equipos actualmente usados por la Empresa Sigsignet y los que se pretende usar en el modelo de red deseado y que contemplan como solución al fabricante Mikrotik, por su clara relación beneficio/costo y análisis posteriores definidos en el capítulo anterior, y especificados en la siguiente tabla.

	Actual	**Deseado**
		
Arquitectura	PC X86	PowerPc
Procesador	Intel Dual Core (E5700)	PowerPC P2020 dual core network CPU with IPsec accelerator
Frecuencia Procesador	3.0 GHz	1066MHz
Motherboard	Marca Gigabyte GA-G41MT-S2 DDR3	Mikrotik Routerboard
Soporte POE	NO	SI (12-24V)

Memoria RAM	DDR2 2GB Kingstone	2GB
Monitor Voltaje, Temperatura	NO	SI
Almacenamiento	500GB SATA 7200 rpm 16MB	One microSD slot
Case	Case ATX	Rackeable
Sistema Operativo	Ubuntu Optimizado	RouterOS V6.9
Unidad Óptica	DVD+/-RW SATA Súper Multi Doble Capa	
Interfaz de Red	D-Link 10/100 Mbps	13 , 10/100/1000 Mbit/s Gigabit Ethernet with Auto-MDI/X Includes switch to enable Ethernet bypass mode in two ports[28]
Precio Mercado	510 USD	379 USD
Actualización de Software	Por parte del comunidad, sin fechas y calendarios establecidos.	Constantes y en caso de corrección de errores inmediato.

Tabla 3.3. Cuadro comparativo de Servidores29

Fuente: Mikrotik & Intel, Modelos de Router, 2012.

[28] Mikrotik DataSheet RB1100AHx2, 2011, http://www.mikrotik-mexico.com.mx/assets/doctos/RB100AHx2.pdf

Ventajas y desventajas de la plataforma actual.

Ventajas.

- No existe pagos de licencia, se instala los repositorios el software que se necesite y se lo usa.
- Amplia base de conocimientos en foros, blogs, web entre otros.
- Alto nivel de automatización de servicios y tareas por medio de Bash.
- Millones de usuarios distribuidos en comunidades.

Desventajas.

- Complicadas y laboriosas configuraciones ante eventuales cambios en temas como calidad de servicio u otros servicios acorde la demanda de la red. Poco Flexible.
- Estadísticas de la red y tráfico necesitan de la ejecución de servicios adicionales como medidores de las mismas.
- La seguridad muchas veces se puede ver comprometida por la ejecución de servicios innecesarios.
- No se asegura funcionamiento ininterrumpido, no hay soporte para fuentes redundantes y sistema operativo no optimizado para tolerar fallos.
- Pocas vías de administración al servidor.
- Demanda una base sólida de conocimientos en Linux.

EQUIPOS DE RED.- Equipos Terminales de Clientes.

Los terminales CPE o mejor conocido como equipo local de cliente, son los encargados de brindar conectividad final al usuario en la última milla, son equipos sumamente imprescindibles no solo por la función que cumplen sino porque de ello depende poder brindar un servicio de calidad y asegurar un rendimiento óptimo sobre la red, y además el impacto sobre todo en costos finales generados por la instalación de servicio, Sigsignet desde sus inicios a confiado su servicio en terminales basados en tecnología Ubiquiti, muy

reconocidos por la calidad de sus radios pero limitados por la funcionalidad de sus sistema operativo "AirOS" en comparación a Mikrotik por medio de RouterOS que son significativas, el proceso de restructuración contempla utilizar las dos variedades como CPE pero exclusivamente Mikrotik en los puntos de distribución o AP, el proceso de reestructuración contempla el uso de equipos previamente evaluados y acorde a las capacidades requeridas por los clientes y situación geográfica el ultimo factor por el hecho de que Sigsignet es un proveedor de servicios de internet inalámbrico y el medio como tal siempre representa un punto a tomar en consideración por sus limitaciones. Al momento en los CPE de uso común del proveedor y dentro del proceso de reestructuración contemplan los siguientes terminales con sus respectivas características y consolidadas para clientes residenciales que basan su conexión por compartición de canal y dedicadas cuyo acceso al medio no tiene compartición, algunos ya descontinuados por el fabricante pero en actual uso por la red de Sigsignet, para cual se plantean las siguientes topologías de instalación.

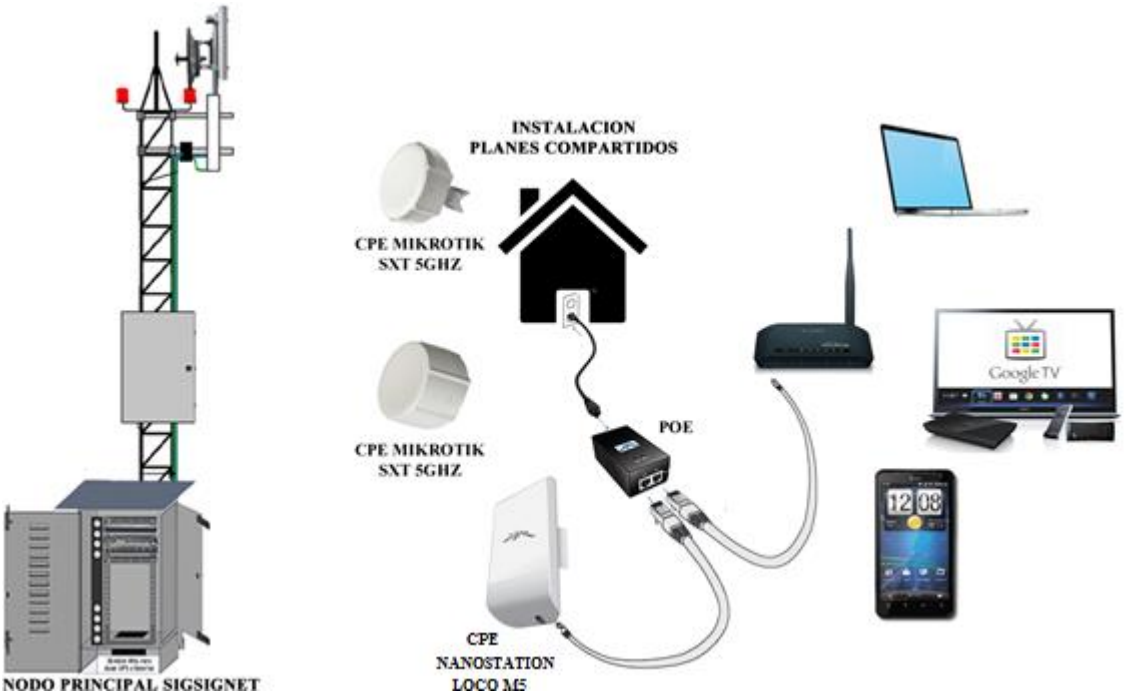


Figura 3.8. Topología de Instalación de CPE para Planes Compartidos

Fuente: Infinynet Cia. Ltda, Topología Planes Compartidos, 2014.

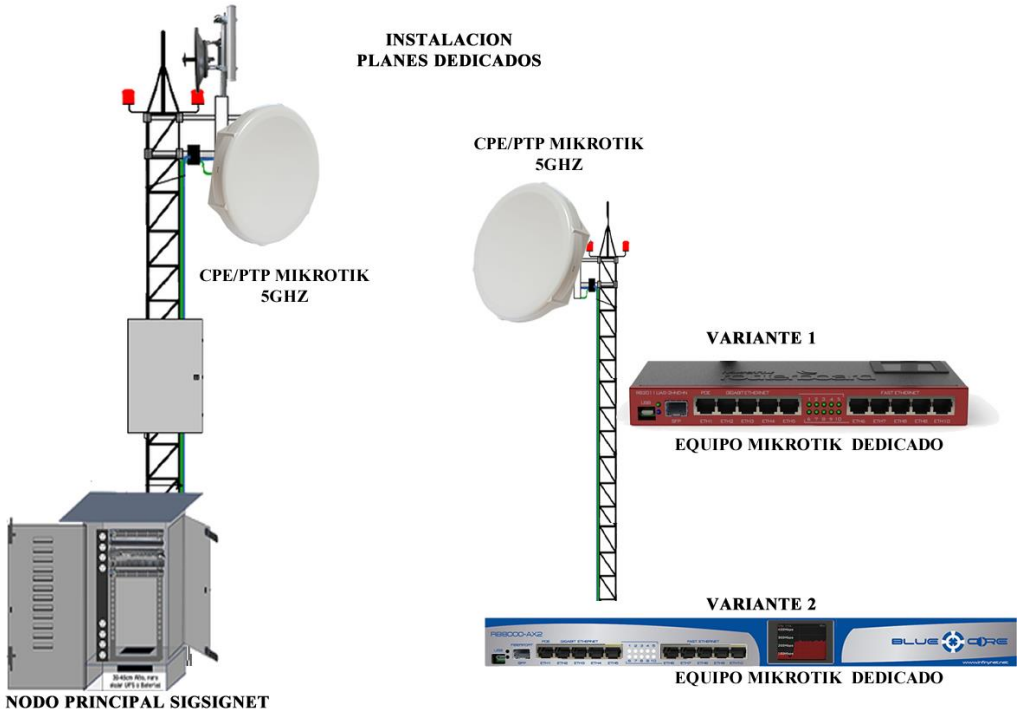


Figura 3.9. Topología de Instalación de CPE para Planes Dedicados

Fuente: Infinynet Cia. Ltda, Topología Planes Dedicados, 2014.

Además se definen los modelos de CPE en actual uso y los nuevos a usar en el proceso de reestructuración en la siguiente tabla.

Características **Modelos**	**CPU**	**Core**	**Wireless**	**Ram**	**Red**	**POE**	**O.S.**
UBIQUITI							
NanoStation Loco 2 & 5 (Descontinuado) Medio: Radio	Atheros	1(180 Mhz)	2.4 Ghz 5.8 Ghz a/b/g 8 Dbi	16 MB	10/100 Base TX	SI	AirOS

			1 Antena PTM				
NanoStation 2 & 5 (Descontinuado) Medio: Radio	Atheros	1(180 Mhz)	2.4 Ghz 5.8 Ghz a/b/g 10 Dbi 1 Antena PTM	16 MB	10/100 Base TX	SI	AirOS
NanoStation Loco 2 & 5 (En Uso Medio) Medio: Radio	Atheros MIPS	1(400 Mhz)	2.4 Ghz 5.8 Ghz a/n 8-13 Dbi 2 Antena PTM	32 MB	10/100 Base TX	SI	AirOS
NanoStation 2 & 5 (En Uso Medio) Medio: Radio	Atheros MIPS	1(400 Mhz)	2.4 Ghz 5.8 Ghz a/n 11-16 Dbi 2 Antena PTM	32 MB	10/100 Base TX	SI	AirOS
MIKROTIK							
RouterBoard SXT-Lite5 (En Uso	Atheros MIPS-BE	1(600 Mhz)	5.8 Ghz a/n 16 Dbi	64MB	10/100 Base TX	SI	Router OS Nivel 3

Continuo) Medio: Radio			2 Antena PTM				
RouterBoard SXT-HG (En Uso Continuo) Medio: Radio	Atheros MIPS-BE	1(600 Mhz)	5.8 Ghz a/n 17 Dbi 2 Antena PTM	64MB	10/100/1000 Base TX	SI	Router OS Nivel 4
RouterBoard SEXTANT G 5HPnD (En Uso Continuo) Medio: Radio	Atheros MIPS-BE	1(600 Mhz)	5.8 Ghz a/n 18 Dbi 2 Antena PTP	32MB	10/100/1000 Base TX	SI	Router OS Nivel 3
RouterBoard RB750 GL (En Uso Continuo) Medio: Cableado	Atheros MIPS-BE	1(400 Mhz)	No	64MB	10/100/1000 Base TX	NO	Router OS Nivel 4
RouterBoard RB2011UiAS-RM (En Uso Continuo) Medio: Cableado	Atheros MIPS-BE	1(600 Mhz)	No	128 MB	10/100/1000 Base TX	NO	Router OS Nivel 5

RouterBoard RB1100AHx2-LM (En Uso Continuo) Medio: Cableado	Power PC	1(1 Ghz)	No	152 MB	10/100/1000 Base TX	SI	Router OS Nivel 6

Tabla 3.4. Modelos de CPE empleados para instalaciones servicio de Internet

Fuente: Mikrotik - RouterBoard, Lista de Dispositivos, 2014, http://wiki.mikrotik.com

Estos dispositivos son los que se encuentran trabajando actualmente como lista de equipamento CPE`s conjuntamente con AP`s compatibles a sus respectivas tecnologías, Dado el exponencial crecimiento de las redes inalámbricas el uso del espectro incluso en frecuencias antes poco explotadas se ha visto en serios aprietos generando perdida de rendimiento sobre la red, por tal razón el proceso de reestructuración ha comprendido también delimitar un tiempo de vida útil sobre las tecnologías ya en uso de la empresa Sigsignet, y las nuevas con el fin de estar en constante renovación procurando siempre brindar un servicio de calidad.

3.1.3 DIRECCIONAMIENTO IP Y MÉTODOS DE ASIGNACIÓN ACTUALES Y DESEADOS

El direccionamiento IP en un Proveedor ISP o mejor conocido en Ecuador como SVA y dado el agotamiento de IPv4 ha hecho que la entrega de IP'S Publicas por cada cliente se vea limitado, por ello muchas técnicas como NAT o traducción de direcciones Privadas en Publicas sean de gran uso actualmente, o la lenta adopción de IPv6 que aún no terminan de completar la transición, dentro de la red de datos de Sigsignet no se contaba con ninguna política sobre direccionamiento IP, desde sus inicios la misma ha utilizado NAT y mediante asignación estática de IP en los CPE y

así posibilitar su interconexión, aun con la problemática que NAT conlleva al compartir varios usuarios una misma IP en específico sobre determinados servicios de Internet. Sin embargo siempre se ha mantenido disponible un rango público aunque no se lo ha dado uso, mismo que en el proceso de restructuración se contempla su uso y asignación para clientes que contraten el servicio dedicado, sobre la red actual al ser un gran bridge lógico no existía proceso de enrutamiento alguno, pero dado su exponencial crecimiento y las desventajas que una red de datos grande genera al estar en esa configuración y centrados en el proceso de reestructuración se ha procedido no solo en reemplazar tecnologías anteriores ya obsoletas en los puntos de acceso por Mikrotik, permitiendo aplicar procesos de enrutamiento avanzados como OSPF gracias a RouterOS y sus beneficios agregados incluso disponer de soporte para MPLS.

El proceso de direccionamiento IP en el proceso de reestructuración contempla un método de asignación de IP dinámico basado en un servidor DCHP gestionados por un servidor centralizado para asignación de IP por los diversos nodos que la empresa tiene y utilizando diversos pool de IP privadas, no obstante con los clientes dedicados la asignación de IP se realizara de manera estática utilizando un rango de direcciones públicas, todo enlace punto a punto que parten desde el nodo principal y sirven como medio para dar acceso a un multipunto utilizaran un rango /30 incluso por temas de seguridad ya que solo se cuenta con dos direcciones IP por dicho rango, respectivamente enrutadas, las direcciones IP publicas será gestionadas por OSPF para su asignación en tanto los clientes residenciales se contemplara diversos pool de direcciones privadas manejadas por Puntos de Acceso e incluso para evitar temas de saturación mismo que contemplan subredes con /26 con soporte hasta 62 IP validas por punto de acceso divididos en varios pools de IP.

3.1.4 POLÍTICAS DE SEGURIDAD ACTUALES Y DESEADAS CONTRA INTRUSIÓN NO AUTORIZADA A DISPOSITIVOS DE RED Y LA RED DE DATOS

Las políticas de seguridad dentro de todo Proveedor de Servicios de Internet, tiene una función vital ya que no solo protegen a los abonados de amenazas externas sino también contra accesos no autorizados a la red e infraestructura de la empresa

estableciendo un barrera lógica que permita un funcionamiento ininterrumpido y optimo, por ende es necesario utilizar estrategias de seguridad adecuadas, que pueden ir desde una defensa en profundidad hasta una negociación por defecto, estrategias de amplio uso en un ISP la primera destinada a establecer varios niveles de seguridad de tal forma que si uno falla siempre habrá uno de respaldo y la segunda negar todo y permitir lo que se conoce, en fin complementos que colaboran creando mecanismo de seguridad adaptados a las necesidades para brindar la seguridad deseada.

Sigsignet contempla algunas necesidades en la red deseada que van desde protección de acceso a equipos terminales de clientes CPE mediante contraseña y por capa 2 y 3 de acuerdo al modelo OSI, acceso a Core y puntos de distribución, cifrado del canal inalámbrico, validación de conexión frente a sistemas externos tipo Radius Server para autorizar conexión, acceso desde redes o IP autorizadas, en si una serie de capas que actúen como barreras y ayuden a resguardar e incrementar los niveles de seguridad y ante todo brindar la protección necesaria para brindar un óptimo servicio.

3.1.4.1 FIREWALL LAYER 2,3 Y 7

Son diversas las capas sobre las que puede operar un firewall a nivel lógico según el modelo OSI, y actuar como barrera ante amenazas externas o internas manteniendo a buen resguardo infraestructura o sistemas de estado crítico, los pequeños WISP en sus inicios no comprenden lo valioso y funcional que puede ser un firewall; por tal razón entre muchos de los factores de los pequeños ISP como causante de problemas de perdida de rendimientos solo la ausencia de mecanismos de protección como Firewall en sí; Sigsignet en sus inicios no disponía de una solución en Firewall robusta que aplicara las dos o tres capas pero si una de ellas, a nivel de capa 2, pero que dado el crecimiento exponencial sobre la red su uso se fue justificando cada vez más y más, solución que la actual plataforma no la realiza de forma eficiente dado la complejidad que la misma demandaba para tener un sistema con el nivel de protección deseado.

La problemática actual en Sigsignet comprende dar una solución no solo a nivel Físico por medio de Hardware especializado sino a nivel lógico contemplando una solución que abarque una protección completa sobre capa 2 y 3 y lo más importante que no termine afectando el buen rendimiento del servicio, y el bloqueo de puertos o servicios innecesarios.

En cuanto a capa 7 la filosofía que se plantea es mitigar de cierta forma protocolos que a veces viene encapsulados bajo TCP en puertos de común uso, siendo necesario en esos momentos desmantelar los paquetes para analizarlo a nivel de capa de aplicación y poder darles su respectivo tratamiento, a pesar de sus altos consumos de Hardware es necesario realizar dicho procedimiento ya que muchas veces al no tener control puntual como P2P se tiende a generar problemas en la red, que puede terminar afectando el rendimiento de la red.

A continuación se detallan características deseadas en la solución de Firewall deseada y una comparativa con la red actual.

Característica	Red Actual	Red Deseada
Protección contra SPAM	Básica. Bloqueo de Puerto	Reglas Filter por número de conexiones en determinado tiempo hacia el puerto 25.
Protección contra virus conocidos.	Ninguna	Reglas Filter, bloqueos por puertos y protocolos específicos y por cantidad de tráfico.
Protección Equipos Infraestructura	Ninguna	Listas de Acceso para IP permitidas.

P2P Mitigación exceso consumo.	Básico	Reglas Filter con determinado número de conexiones.
Bloqueo de servicio a clientes en Mora.	Básico, por MAC en puntos de acceso.	A nivel lógico por capa 2 y capa 3.
IP Duplicada.	Ninguna	Script Lista dinámica creada y aviso de duplicado.
Amarre por MAC & IP	Ninguna	Avanzado, desde IP - ARP
Protección contra DDoS	Ninguna	Avanzado, reglas filter.

Tabla 3.5. Características Deseadas y Actuales de la solución Firewall para Sigsignet.

Fuente: J.Michael,Stewart, Network Security, Firewalls and VPNS, 27 Agosto 2010.

La protección sobre capa 3 es una de las más trascendentales, por tal razón es necesario antes de plasmar cualquier solución sobre la misma, comprender cuatro elementos vitales, su solo entendimiento permitirá implementar reglas elaboradas, un firewall por capa 3 basa su mecanismo en un dirección de origen que es la IP del equipo que está queriendo realizar una conexión hacia una red externa por un puerto especifico en tanto la dirección destino es la IP del host a la cual el equipo, computador u otro dispositivo de red quiere acceder y que por medio del puerto de destino, siendo estas cuatro piezas las que definen una conexión, misma que a su vez pueden adquirir los siguientes estados

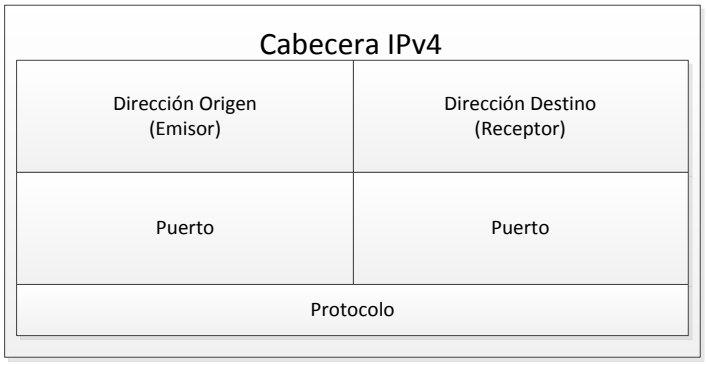


Figura 3.10. Cabecera IPv4, estructura Básica.

Fuente: Stheper Discher, RouterOS by example, 30 Noviembre 2011.

Un Firewall puede generar las siguientes conexiones que son de tipo:

- **Nuevas.-** La primera vez que la combinación de conexión entre puerto, direcciones de origen, dirección de destino, y puerto de destino ha sido realizada.
- **Establecidas.-** Combinación de conexiones conocidas.
- **Relacionadas.-** Parte de la combinación de una conexión conocida.
- **Inválidas.-** No parte de ninguna conexión conocida y ninguna nueva.

Sobre estas premisas armar un firewall consiste en el uso adecuado de reglas o mejor conocidas como chains que son las que van construyendo al Firewall, junto con los demás elementos que lo compone como son Packet Mactchers y Acciones mencionados en capítulos anteriores.

- **Input.-**Siendo dicha regla la que controla tráfico que va hacia el firewall o Router (Protege al Router)
- **Forward.-** Tráfico que pasa por el Router (Protege a los clientes)
- **Output.-**Tráfico generado por el Router. (Menos comúnmente usada en soluciones de Firewall sencillas)

3.1.4.2 POLÍTICAS DE ACCESO A DISPOSITIVOS PARA ADMINISTRACIÓN DE LA RED

La seguridad es un elemento y parte fundamental como herramientas para brindar un servicio de calidad sobre un proveedor de servicios de Internet, teniendo siempre como objetivo el buen resguardo y sobre todo tener el control absoluto de la misma, esta se centra en definir estrategias de métodos de acceso seguros desde el Exterior, o a su vez por medio de dispositivos intermedios de interconexión en el Interior o directamente desde el subscriptor, evitando intrusiones no deseadas que causen problemas sobre la red o peor interrumpan el continuo servicio.

La Arquitectura de Sigsignet en cuanto a control sobre el acceso a los diversos dispositivos de red se contemplaba como una solución muy permisiva y con un solo nivel de seguridad basado en autentificación por Login y contraseña desde los equipos de los subscriptores y en cuanto a los diversos equipos de administración ubicados en el Core y Puntos de Distribución los acceso se daban por medio del protocolo telnet con posibilidad de ser accedidos desde cualquier parte de la red con las herramientas adecuados, si bien sin registrar hasta el día de hoy problemas de seguridad serios sobre la marcha pero que a futuro se contemplaba un serio problema, de tal forma que la arquitectura actual de la red se define de la siguiente forma.

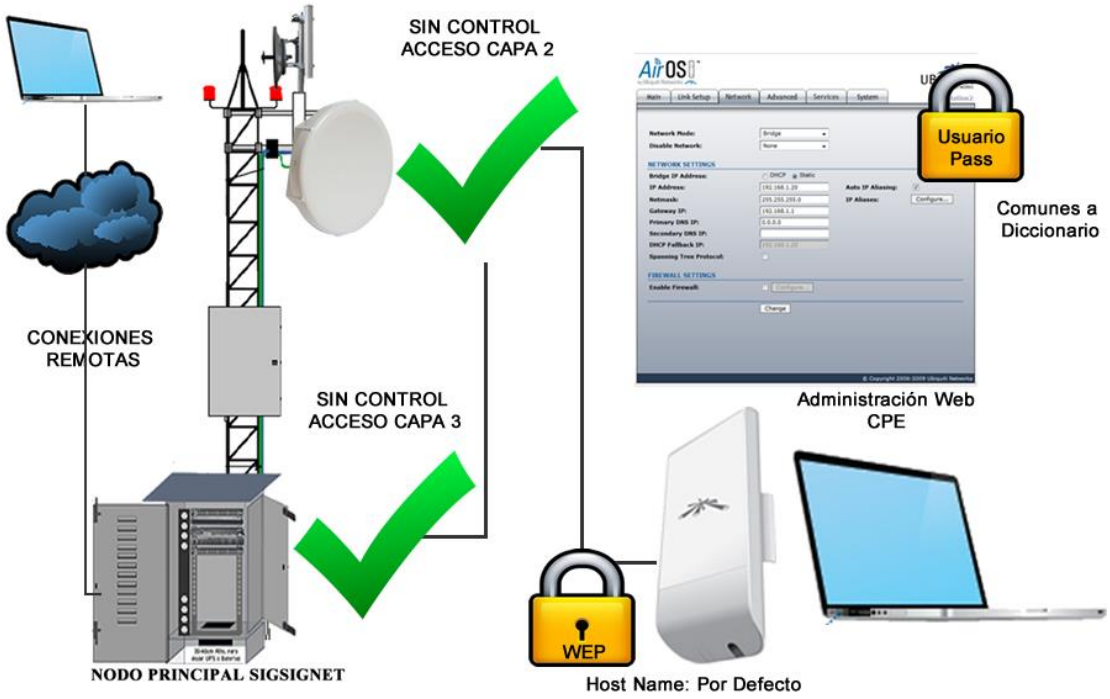


Figura 3.11. Arquitectura Actual sobre Control de Acceso a la Red

Fuente: Los Autores, Arquitectura Control de Acceso Actual Sigsignet, 2013

En tanto la solución para la Red Deseada contempla políticas de acceso más específicas, políticas que contemplan mecanismos que van desde usuarios y contraseñas en los CPE más robustas y poco comunes, control de acceso por los Puntos de Distribución hasta validación de dispositivos por MAC, a sabiendas que es un hecho el conocer que haya sistemas 100% seguros en estos casos, se ha buscado una solución acoplada a las necesidades actuales de la empresa y que pueda aportar un alto grado de seguridad sobre la nueva red de datos, dando niveles agregados de seguridad que dificultaran mucho intrusiones por acceso no autorizados en el caso de existirlas, posibilitando brindar un servicio de calidad.

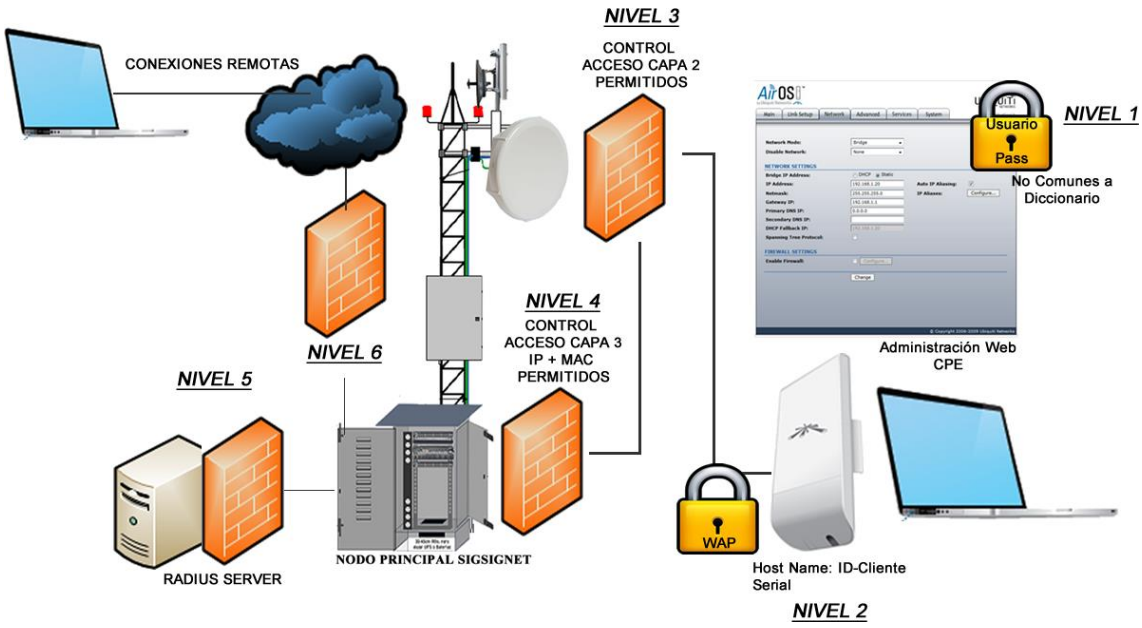


Figura 3.12. Arquitectura Deseada sobre Control de Acceso a la Red

Fuente: Los Autores, Arquitectura Control de Acceso Actual Sigsignet, 2014

3.1.4.3 PROTOCOLOS DE SEGURIDAD Y ENCRIPTACIÓN 802.11

Los protocolos de encriptación y seguridad en el caso de Proveedores de Servicio de Internet Inalámbrico es un factor muy serio, ya que al ser un medio de fácil acceso y no de uso exclusivo, su resguardo es aún más importante, al estar transmitiendo datos de manera inalámbrica se está también conscientes de los riesgos que esto conlleva, por ende hablar de protocolos de seguridad es quizá uno de los temas más relevantes dentro de la red.

La empresa SigsigNet ha implementado como seguridad el algoritmo WEP (Privacidad Equivalente al Cable) desde sus inicios. El protocolo WEP es un sistema de encriptación estándar implementado a nivel de capa 2 y ampliamente soportado por la mayoría de soluciones inalámbricas, quizá con algunas deficiencias que muchas de las veces han comprometido la seguridad sobre diversas redes inalámbricas e incluso la de Sigsignet pero que optimizadas adecuadamente y en complemento con TKIP (Protocolo de Integridad de Clave Temporal) protocolo

encargado de cambiar las claves a medida que se usa el sistema de forma dinámica y que junto con un vector de inicialización mucho más grande evita los ataques de recuperación de fuerza bruta a los que es muy susceptible el protocolo WEP haciéndola más robusta.

En la red actual el escaso soporte para protocolos WPA 1 y 2 y WEP con TKIP es claramente visible, si bien elevar el nivel de encriptación corresponde un gasto de recursos de Hardware significativo el mismo se justifica sobre el nivel de protección otorgado sobre el medio, aunque el mismo se ve complementado por los niveles de seguridad agregados explicados en el capítulo anterior, por ende es necesaria la utilización de protocolos de encriptación robustos como WPA (Acceso a Wifi Protegido) una de las opciones más viables al momento con alto grado de confiabilidad y que corrige las deficiencias de WEP (Wired Equivalent Privacy), la misma es basada en el estándar 802.11i, posibilitando incluso el uso de un servidor de autentificación RADIUS, mismo que se encarga de distribuir claves diferentes a cada usuario, además desde la versión 2 de WPA apoyó el uso del algoritmo de cifrado AES (Advanced Encryption Standard) una notable mejora en seguridad y elevando aún más el grado de intrusión. Son pocas las técnicas conocidas hasta el momento para Cracking de WPA y WPA2, entre ellas el ataque mediante fuerza bruta ejecutando una serie de combinaciones de credenciales de autentificación hacia exploits hallados en algunas variedades de Routers de casa con soporte para WPS es quizá la más conocida al momento, es por ello que el uso de contraseñas robustas, que empleen hasta 8 caracteres o combine letras y números, los primeros tanto en mayúsculas como minúsculas y la inclusión de caracteres no alfanuméricos permitirán definir una contraseña con un alto grado de seguridad. Ante tal el proceso de reestructuración contempla una actualización sobre los puntos de distribución con un Hardware con soporte para los tipos de cifrado antes mencionados, donde claramente Mikrotik sigue siendo aquí unas de las opciones más viables y como amplio soporte en dichos protocolos y como solución concreta en el proceso de reestructuración.

3.1.4.4 POLÍTICAS DE SEGURIDAD DE ACCESO A LA RED

Se emplearan políticas de seguridad de acceso a la red en diferentes niveles para evitar tanto intrusión de usuarios no permitidos como para evitar accesos innecesarios a dicha red.

Ingresos a equipos localmente:

- Se permitirá el ingreso a los AP's solo al administrador de enlaces en caso de existir saturación del canal utilizado por dicho AP.
- Se permitirá el ingreso a los CPE's solo al personal encargado de realizar las instalaciones y al administrador del enlace para realizar las configuraciones respectivas.
- Se deberá ingresar a los CPE's solo en caso de existir pérdida de paquetes superior a un 3% por minuto.
- En caso de recibir quejas por parte de los abonados, esta se deberá comunicar inmediatamente al administrador de enlaces para su verificación.

Encriptación a nivel de enlaces.

- De ahora en adelante la encriptación que se manejará en los enlaces serán WPA2 ya que esta cumple con los más altos estándares de seguridad a nivel de gobiernos federales.
- Los enlaces configurados anteriormente con encriptación WEP deberán ser reemplazados con WPA2 dado un plan de migración paulatino de los CPE's que estén conectados a este tipo de encriptación.

Uso de ACL's en AP's

- En el caso de los CPE's que no se puedan migrar a WPA2 se crearan ACL's en los AP's que estén enlazados con estos en caso de soportar esta configuración.

Uso de VPN

- Solo los usuarios previamente autorizados podrán utilizar los beneficios del Sistema VPN, los que además, serán los responsables del correcto uso del sistema.
- Es de responsabilidad del usuario con privilegios VPN, asegurarse que ninguna otra persona utilice su cuenta de acceso, entendiendo que es de uso exclusivo para quienes se les ha asignado dichos privilegios.
- El uso del sistema VPN debe ser controlado utilizando una contraseña de autenticación fuerte.
- Cuando esté conectado activamente a la red, el sistema VPN obligará a todo el tráfico hacia y desde el equipo computacional pasar a través del túnel de VPN, el resto del tráfico será denegado.
- Multiplicación de túneles NO ESTÁ permitido, sólo una conexión está permitida.
- Las puertas de enlace VPN serán configuradas y administradas por el grupo de seguridad informática.
- Todos los computadores conectados a las redes internas vía Sistema VPN o cualquier otra tecnología deberá utilizar el software antivirus más actualizado, además de los equipos computacionales personales conectados al sistema.
- Los usuarios del Sistema VPN serán automáticamente desconectados de la red, una vez que hayan pasado 30 minutos de inactividad. El usuario deberá logearse nuevamente para reconectarse a la red. Procesos artificiales informáticos como el "PING" no deben ser utilizados para mantener la sesión abierta.
- El concentrador VPN está limitado para un tiempo de conexión absoluta de 24 horas.
- Mediante el uso de la tecnología VPN con el equipo computacional personal, los usuarios deben entender que sus máquinas son una extensión de la red, y como tales están sujetos a las mismas normas y reglamentos que se aplican a los equipo computacionales de la empresa, es decir sus máquinas deben ser configuradas para cumplir con las políticas de seguridad de la empresa.

3.1.4.5 SISTEMAS DE ADMINISTRACIÓN EXTERNOS

Los sistemas de administración externos elementos claves para la gestión y administración de usuarios y transacciones realizadas por los mismos y sobre servicios ofertados por Sigsignet, la interacción con el Hardware directamente y el soporte para crear aplicaciones personalizadas por medio de los API disponibles por el fabricante, posibilitando ejecutar acciones en tiempo real e incluso generar reportes de estadísticas detallados sobre el servicio, o incluso la calidad de servicio que un cliente tiene, abriendo una serie de infinitas posibilidades. Sigsignet desde sus inicios no ha concretado una solución clara que apoye la gestión y administración de usuarios, dicho procedimiento se lo ha venido desarrollando de forma manual, por medio de herramientas ofimáticas como lo es Excel con un determinado nivel de personalización.

- **iNet Control V1.0:** Es la respuesta y solución contemplada en el proceso de restructuración, como sistema de gestión y administración Web basado en JAVA creado para control de abonados y gestión de planes de Internet en el WISP Sigsignet con soporte para integración con Mikrotik - RouterOS, su desarrollo personalizado empleando tecnologías Open Source de última generación complementados con estándares de desarrollo adecuados y en capas, ha establecido una solución aún en proceso de desarrollo que contempla una serie de módulos que van desde Facturación Electrónica, Gestión de Planes de Internet, Gerenciamiento y Planificación de Nodos de la Empresa, Control de Inventario, módulo de monitoreo, puntos de recaudación para terceros, soporte para integración de servicios de terceros complementados con su interfaz amigable e intuitiva reduciendo tiempos incluso sobre soporte directo con el cliente y otorgando mayor control sobre la red y transacciones realizadas por los usuarios.
-

Figura 3.13. iNet Control v1.0, sistema de gestión y administración para ISP

Fuente: Los Autores, iNet Control v1.0, 2014

- **Escalabilidad y modelo de crecimiento Actual y Deseado**

La red actual de Sigsignet se reestructurará lógica y físicamente de tal manera que busca ser escalable. Como principal prioridad y en el proceso de planificación de crecimiento dentro de la red deseada se ha priorizado la completa cobertura del cantón Sígsig así como también el poder cubrir sectores aledaños como Zhotor, Dacte, Curin, San Bartolomé, Zhimbug, Zhuzho, Malpad, Reron, Garau, Piruncay, Cuhil Capilla, Sondeleg y Pueblo Viejo.

Para tal hecho la infraestructura con la que se cuenta en la actualidad impiden que dicha ampliación se realice de forma exitosa por ende la red se encuentra limitada en su crecimiento no solo por su estructura lógica sino por su capacidad. Es por eso que el proceso de reestructuración contempla la implementación de nuevos enlaces Punto a Punto y Multipuntos soportados por hardware de mayor capacidad en conjunto con el software que den soporte al uso de nuevos protocolos de red, en pro de elevar el nivel de rendimiento de la misma y su escalabilidad.

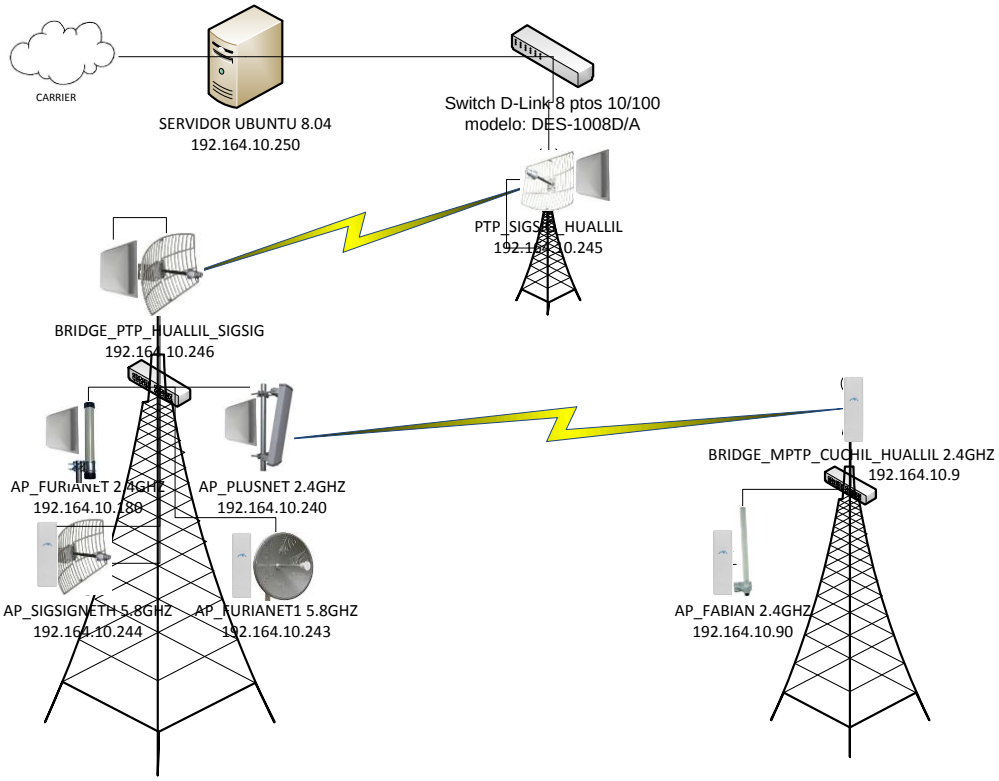


Figura 3.14. Arquitectura actual de red Sigsignet

Fuente: Sigsignet, Departamento Networking, 2013

Como se muestra en la figura 3.14 el rango de cobertura es muy direccional ya que las antenas colocadas limitan la misma y su mala ubicación recae en una irradiación poco eficaz y sobre todo nivel lógico la red es un gran bridge con los problemas y complicaciones que ello conlleva.

En tanto la solución para la red deseada contempla soluciones a nivel de Wireless, estableciendo una ubicación adecuada de las antenas, muchas veces causantes de series conflictos por generación de ruido, posicionados en una topología en forma de corona posibilitando una cobertura de 360° sobre el nodo la misma cubierta con 4 antenas sectoriales de 90° cada una, debidamente distanciadas, en tanto el control de los puntos de acceso de ahora en adelante los realizará Mikrotik – RouterOS con todas sus características para control de redes inalámbricas, los enlaces punto a punto que comunicarán con nodos secundarios se los dejara en manos de Mikrotik igualmente, buscando incrementar su rendimiento incluso si el caso amerita el uso

de frecuencias poco comunes no licenciadas como es el caso de los 24 Ghz asegurando aún más la calidad de los mismo, todos estos nodos estarán debidamente monitorizados desde una oficina central ubicada en la ciudad de Cuenca, velando por su continua operatividad y correcto funcionamiento.

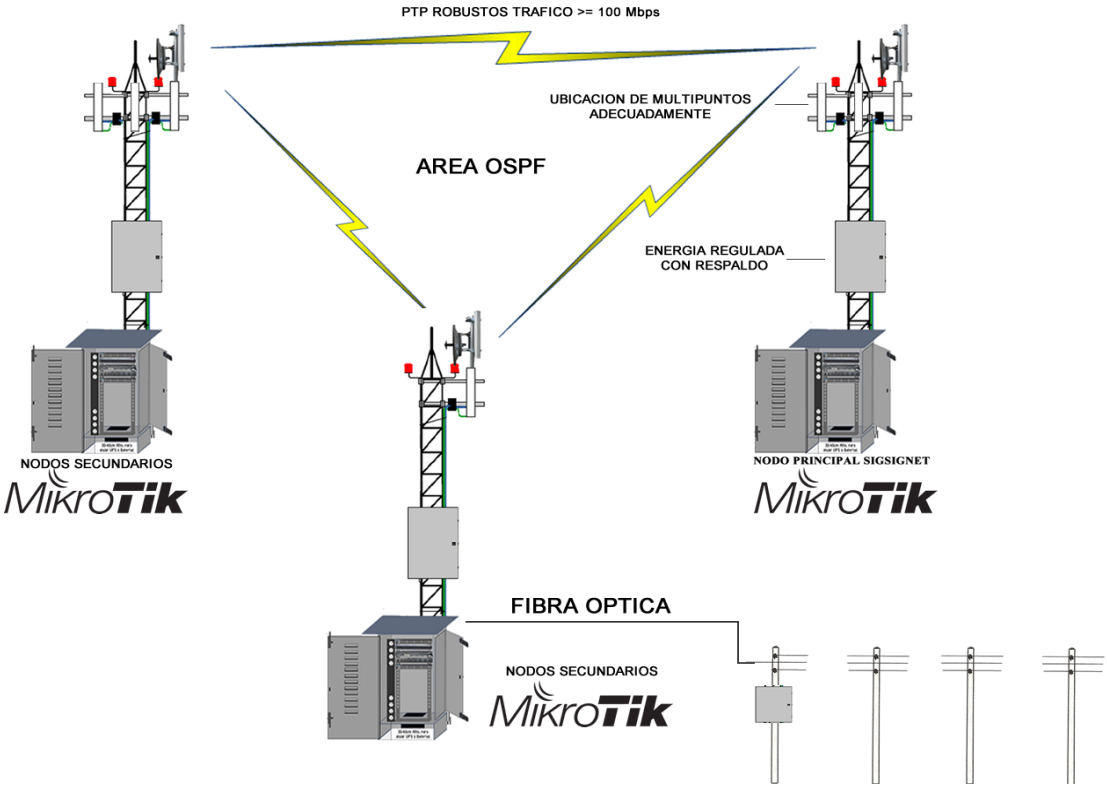


Figura 3.15. Arquitectura de red la red Deseada Sigsignet

Fuente: Los Autores, Modelo de Red Deseada, 2014

3.2 TOPOLOGÍA DE LA RED ACTUAL Y DESEADA

3.2.1 TOPOLOGÍA FÍSICA DE LA RED.

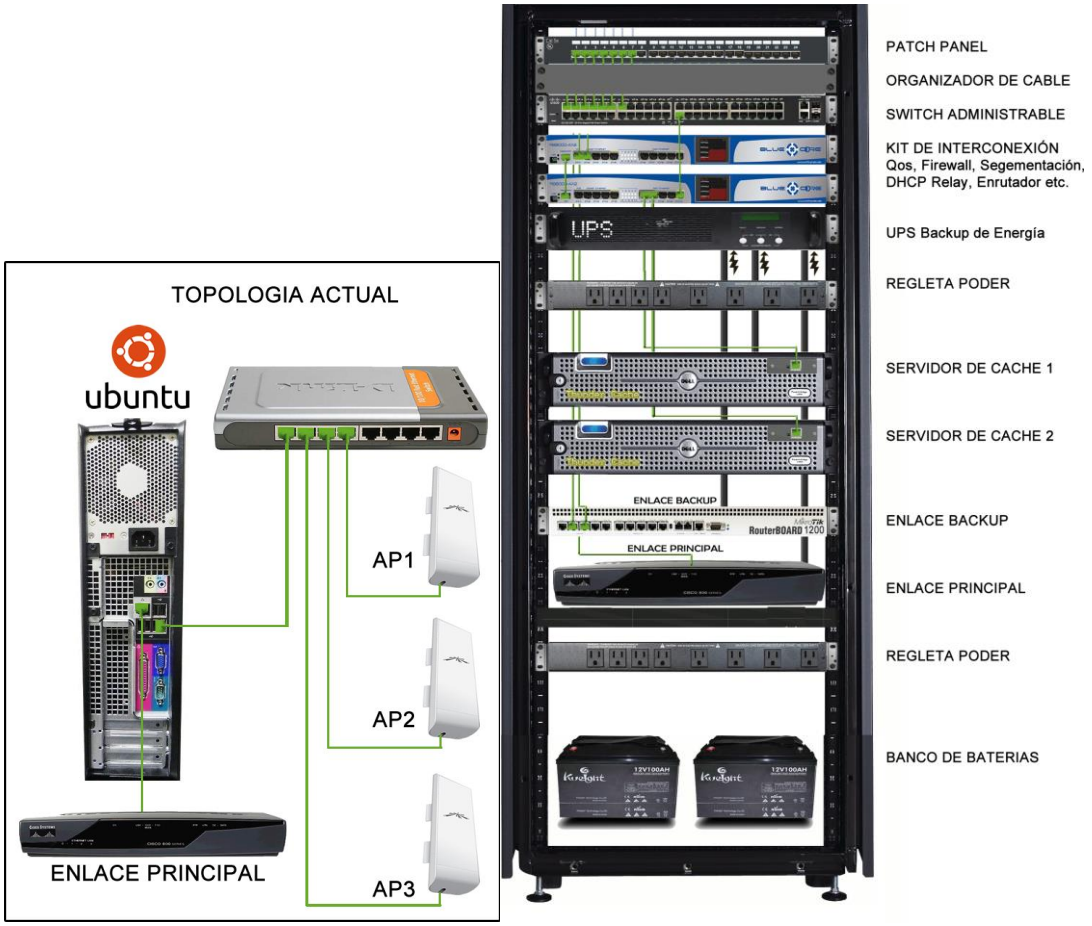


Figura 3.16. Topología Física Actual y Deseada de la Red Sigsignet

Fuente: Los Autores, Topología Física Actual y Deseada Sigsignet, 2013

Como se puede evidenciar en la Figura 3.16. entre la topología Física de la estructura de la red actual y deseada existen notables diferencias, que pretende mediante la misma elevar la calidad de servicio y brindar un servicio ininterrumpido, problemáticas antes constantemente presentes y solucionadas en la red deseada. Se determina una topología de tipo Estrella en la red actual y una topología Malla en la red Deseada, permitiendo con la última, asegurar la calidad y operación constante, además para tal el nodo principal contara no solo con Hardware Redundante, sino con energía de respaldo posibilitando un funcionamiento 24x7, la organización de los

dispositivos en la red está contemplada, así como el uso de un enlace de contingencia, servidores de cache etc., todo funcional sobre Hardware dedicado.

3.2.2 TOPOLOGÍA LÓGICA DE LA RED

Caso similar al punto anterior, se describe en la siguiente imagen la topología lógica de la empresa Sigsignet y el estado actual de su red, donde se puede observar su direccionamiento IP y estructura lógica en forma “Estrella”.

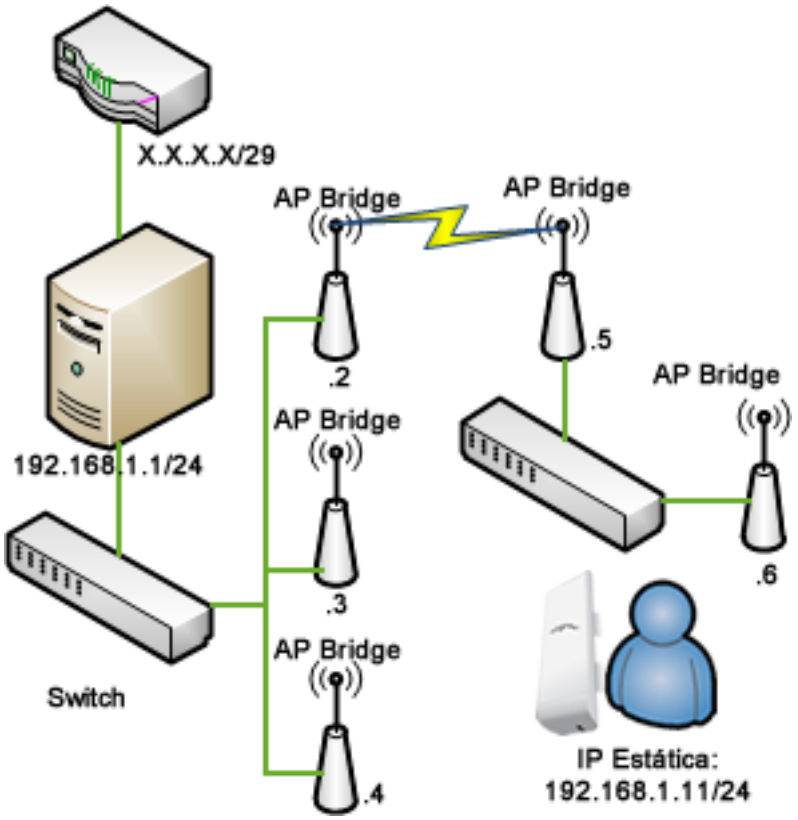


Figura 3.17. Topología Lógica de la Red Actual Sigsignet

Fuente: Sigsignet, Departamento Networking, 2013

En tanto la topología Deseada, pretende dar solución tangible a problemas generados en entornos grandes funcionales como grandes bridges lógicos, como es el caso de tormentas broadcast entre otros, aparte la asignación de rangos IP Públicos asignados al cliente, en este caso encargados bajo el protocolo OSPF, todos los enlaces Punto a

Punto gozarán de un rango /30 con dos IP disponibles para su enlace agregando un nivel de seguridad adicional, sobre la nueva topología lógica y con Mikrotik – RouterOS se posibilita disponer de diversos servicios de red y protocolos como el uso de VLAN, MPLS, OSPF, Ingeniería de Trafico etc., asegurando un nivel de rendimiento óptimo, y brindando una calidad de servicio eficiente.

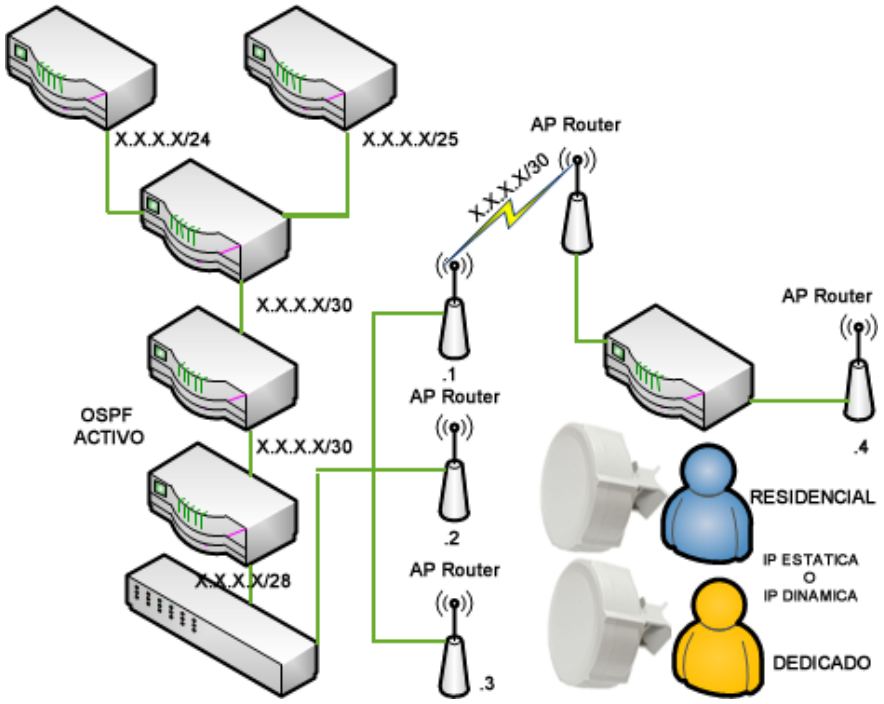


Figura 3.18. Topología Lógica de la Red Deseada Sigsignet

Fuente: Sigsignet, Departamento Networking, 2013

3.2.3 ANÁLISIS DE TRAFICO DE ENLACES, NOC Y CAPACIDAD TOTAL ACTUAL Y DESEADA.

El propósito de este punto es realizar un análisis de tráfico de Enlaces, NOC y capacidad actual administrada por el Backbone, con el fin de determinar posibles cuellos de botella, que luego en el modelo de red deseado nos permitan tomar en cuenta dichas problemáticas para evaluar y determinar posibles mejoras. Para este punto el tráfico se monitorizó en capa 2 y 3 de acuerdo al modelo OSI, para dichas pruebas en primera instancia se ha utilizado estadísticas generadas por el protocolo SNMP recolectadas mediante DUDE sistema Gratuito de Mikrotik disponible para su

descarga en su última versión, adicional el cálculo de capacidad de los enlaces Punto a Punto se ha cuantificado por medio de IPerf y Mikrotik Bandwidth Test V0.1, de forma tal que permita saturar el enlace y tener noción de tráfico del troughput soportado por los mismos y posibles cuellos de botella divisados y que en correlación con datos recolectados por el SNMP poder determinar resultados puntuales, cabe mencionar que IPerf fue empleado a la par con Mikrotik Bandwidth Test, asegurando aún más que los resultados sea lo más reales y fiables posibles.

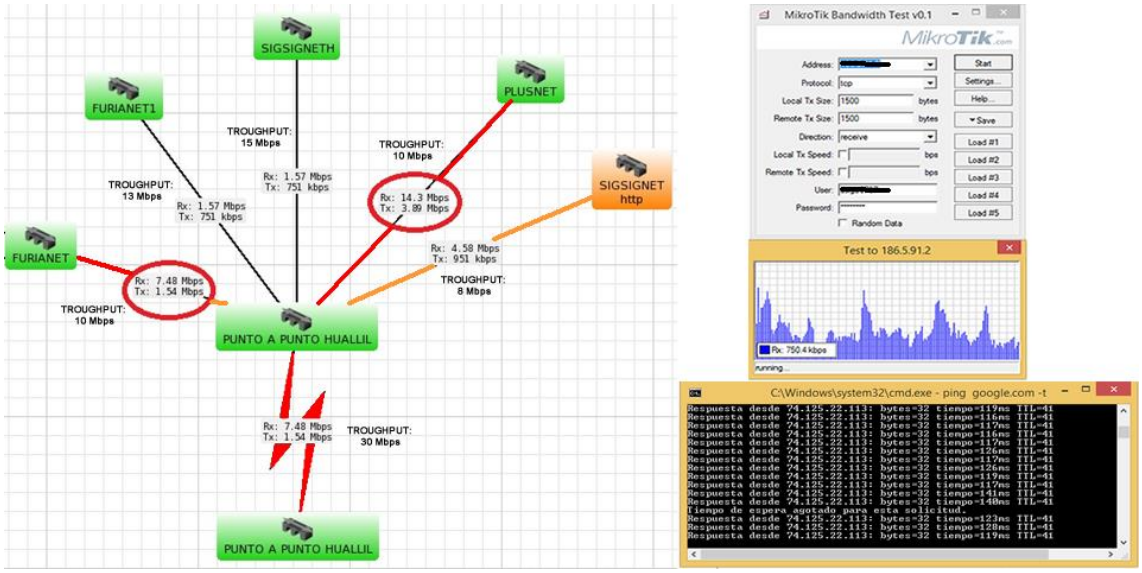


Figura 3.19. Análisis de Trafico de Enlaces y NOC Red Actual Sigsignet

Fuente: Sigsignet, Departamento Networking, 2013

Se realiza un análisis del tráfico y latencia generado en los enlaces y en el centro de operaciones y se puede notar que existe saturación en ciertos enlaces con evidentes cuellos de botella en el enlace Sigsig – Huallil, esto debido a que desde el NOC hacia el nodo de distribución existen un enlace de radio en los 5Ghz cuyas limitaciones de Hardware están alcanzando su máximo en horas pico generando un cuello de botella notable que recae en pérdida de rendimiento sobre la red, incrementando los tiempos de latencia.

En tanto sobre la red actual, se ha simulado un escenario en la misma infraestructura utilizando tecnología Mikrotik – RouterOS bajo el uso del protocolo 802.11 sin activar soporte para NStreme V2 en esta etapa de pruebas, vale mencionar que la misma es una característica wireless de RouterOS basada en TDMA propietaria, que otorga notables mejoras sobre el incremento de troughput y haciendo más eficiente el canal, aplicada sobre los enlaces Punto a Punto, en la misma evaluación la reubicación del Nodo Principal se ha movido hacia el Punto de Distribución ubicado en el Cerro Huallil, con el fin de garantizar la entrega de la capacidad Internacional 25 Mbps 1:1 y disminuir aún más la latencia generado de por si por el enlace Sigsig – Huallil, siendo el nodo Principal para estas pruebas el Nodo Huallil, por tal para constatar y como pruebas establecidas de rigor IPerf y Mikrotik Bandwidth Test nos servirán para evaluación y cuantificación de los resultados junto con herramientas como ping, y el monitoreo de tráfico por interfaz, sobre la red simulada utilizando para ello Hardware real, cabe mencionar que los equipos fueron facilitados para sus pruebas por la empresa Infinynet Cia. Ltda. y poder así disponer de un escenario aún más real, y montados a la par sobre la infraestructura actual disponible para dicho nodo.

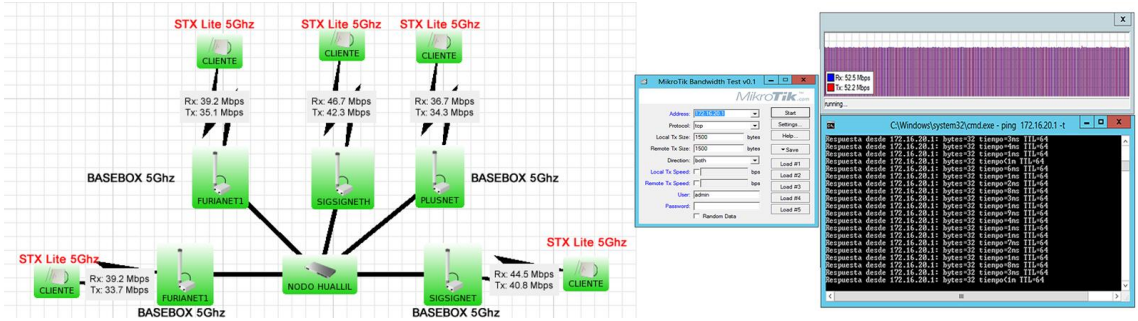


Figura 3.20. Análisis de Trafico de Enlaces y NOC Red Deseada Sigsignet

Fuente: Los Autores, Red Deseada Sigsignet, 2013

A continuación se detallan resultados de pruebas básicas de conectividad y test de capacidad para establecer una comparativa entre la condición actual y deseada de la red.

Prueba	*Red Actual*	*Red Deseada*
Pruebas de Latencia		
Latencia al Gateway	80 ms (Promedio) Variable	2 ms (Promedio) Estable
Latencia google.com	123 ms Variable	16 ms (Promedio) Estable
Latencia Facebook.com	197 ms Variable	120 ms (Promedio) Estable
Prueba de Capacidad		
Prueba de Capacidad Enlace Huallil – Sigsig 1	RX:8 Mbps TX: 7 Mbps	RX:31 Mbps (Promedio) TX:23 Mbps (Promedio)
Prueba de Capacidad Enlace Huallil – Sigsig 2	RX:14 Mbps TX:11 Mbps	RX:52 Mbps (Promedio) TX:48 Mbps (Promedio)
Prueba de Capacidad Enlace Huallil – San Bartolo	RX:13 Mbps TX: 9 Mbps	RX:49 Mbps (Promedio) TX: 47 Mbps (Promedio)

Tabla 3.6. Tabla de Resultados de pruebas de Stress de Latencia y Capacidad.

Fuente: Los Autores, Pruebas de Stress red actual y Deseada, 2013.

3.2.4 ANÁLISIS DE TRÁFICO POR PROTOCOLOS Y APLICACIONES ACTUAL Y DESEADA

El análisis de tráfico es una tarea de vital importancia en redes de datos, más aun si la misma es una red de un proveedor de servicios de Internet, el análisis de tráfico faculta disponer de una captura o histórico del estado de salud de la red y su condición en dicho momento, facilitando la detección de anomalías y actuando como una herramienta de condición preventiva y correctiva. Las diversas soluciones para

análisis de tráfico presentes en el mercado, unas de carácter propietario otras open Source como Wireshark pueden resultar de gran utilidad detectando, analizando y correlacionando tráfico con el fin de identificar potenciales amenazas para que en etapas posteriores poder limitar su impacto.

Para este punto se dispone de un escenario sobre la red actual de la empresa Sigsignet y sobre la red simulada, utilizando Wireshark como herramienta para dicho análisis en complemento con NTOP por su amplia gama de soporte para protocolos de red.

Es necesario antes de iniciar con dichas pruebas disponer de un servidor para colectar la información, mismo que tendrá Wireshark y Ntop corriendo sobre Ubuntu Desktop en su última versión disponible, corriendo sobre la siguiente topología.

Sobre la red actual el mismo se conectará al Switch del Nodo Principal para realizar la captura de tráfico y uso con Wireshark, en tanto para la red deseada se utilizará la función de Mikrotik – RouterOS denominada Traffic Flow compatible con el protocolo Netflow de Cisco empleado en el monitoreo de tráfico de la red, actuando como un Port Mirroring, y enviando el tráfico hacia un servidor de captura de tráfico, cabe mencionar que las dos herramientas son opciones válidas para realizar este tipo de prueba pero destacando a Wireshark pos sus funciones, características y suite de protocolos TCP y UDP más completas, cumpliendo el objetivo de manera simultánea con las dos y generando una captura del estado de salud de la red actual y deseada. Las topologías empleadas para la captura del tráfico se detallan a continuación.

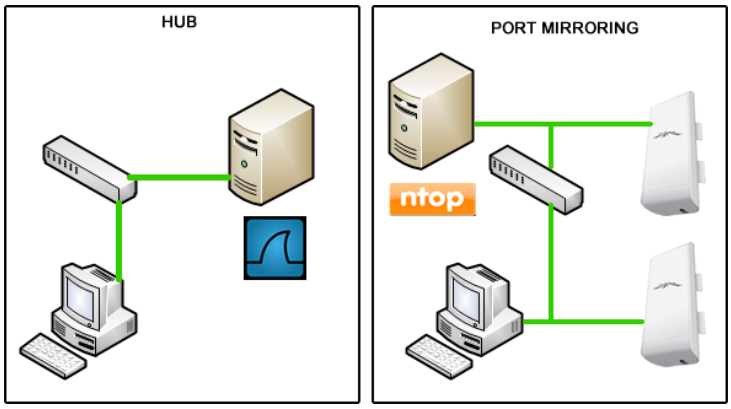


Figura 3.21. Modos de Captura de tráfico

Fuente: Los Autores, Topología de Captura de tráfico, 2013

Con ello implementado es necesario ya solo empezar a realizar la captura del tráfico y posterior su análisis minucioso en busca de anomalías sobre el mismo y su posterior estrategia de mitigación.

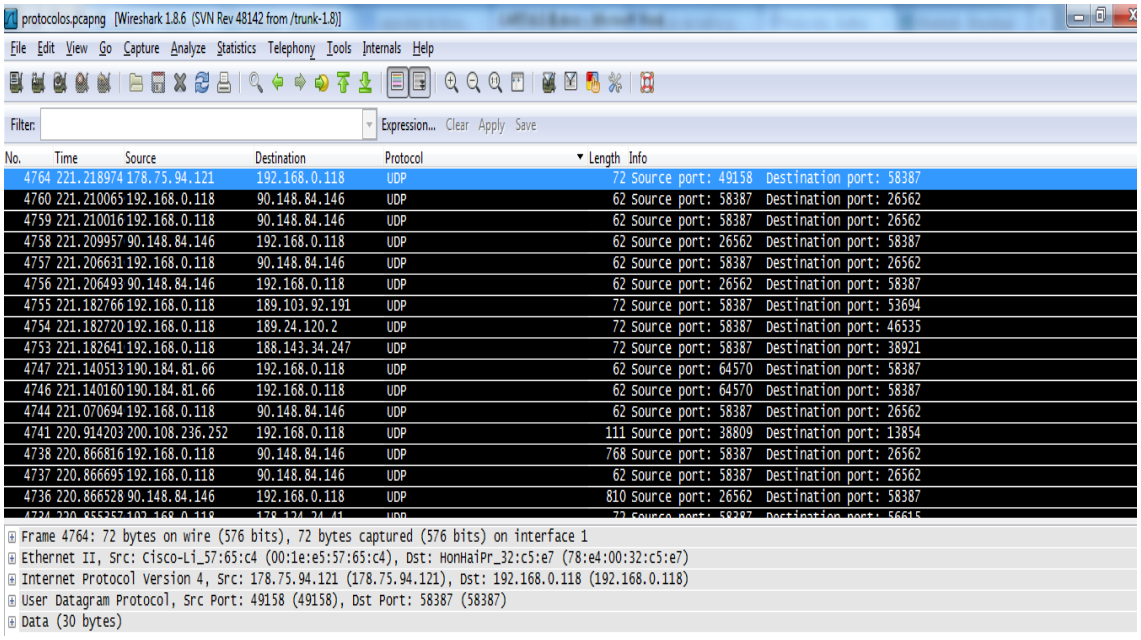


Figura 3.22. Análisis de Tráfico por Protocolos mediante Wireshark

Fuente: Los Autores, Captura de tráfico Red Actual Sigsignet, 2013

Su análisis inicial muestra notables consumos generados por el uso del protocolo P2P sin control establecido sobre la red actual y que puede ser causante de perdida de rendimiento en el servicio durante determinados horarios, así como la falta de control de SPAM generado por el puerto 25 y su ausencia de procesos claros de mitigación, si bien la red de datos de la empresa actual es pequeña en comparación a proveedores de mayor envergadura, los problemas se consideran como irrelevantes quizá la ausencia de problemas más significativos es por la cultura de los habitantes de dicha zona o por la falta de conocimientos en dicho campo que hayan hasta el momento evitado generar molestias y problemas más significativos.

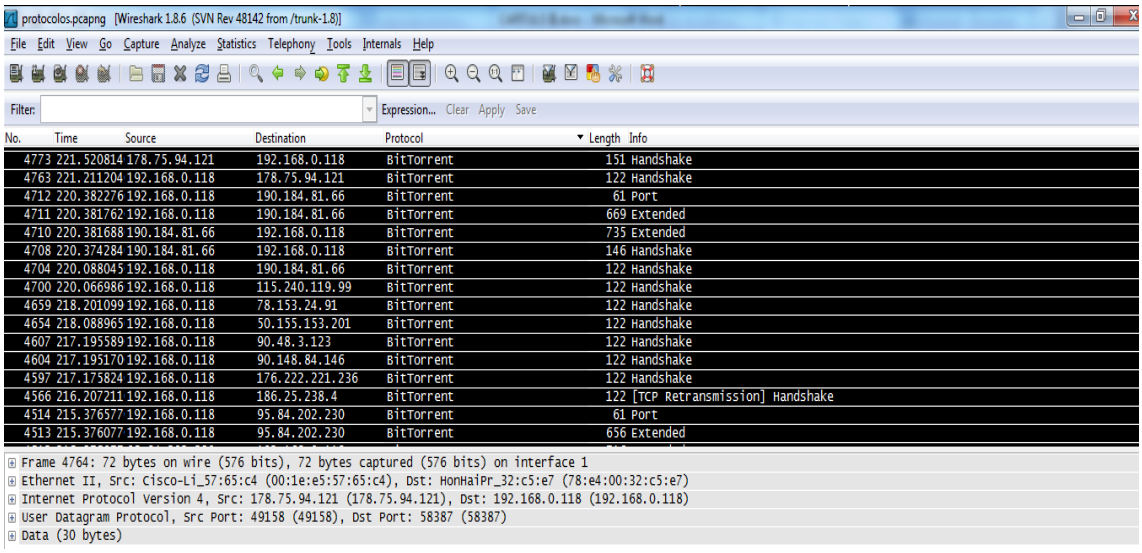


Figura 3.23. Análisis de Tráfico por Aplicación mediante Wireshark

Fuente: Los Autores, Captura de Tráfico Red Actual Sigsignet, 2013

El análisis de resultados tanto de la red de datos actual y deseada es bastante favorable, más aun en la deseada ya que se corrigen sobre los mismos problemas presentes en la red actual, mediante las diversas herramientas que brinda Mikrotik – RouterOS, como la función Firewall, Filter, Encolamiento, Control de Protocolos sobre capa 7 etc., además en correlación con los resultados obtenidos y de fácil interpretación no se divisan anomalías o problemas de mayor relevancia en primera instancia sobre la red actual que sea necesarios una medida correctiva de carácter urgente, a pesar de ello dicha base de conocimiento permitirá los problemas de momento divisados tomar acciones correctivas sobre la red deseada.

3.2.5 VERIFICACIÓN Y SIMULACIÓN DE CÁLCULOS DE ENLACES UTILIZANDO RADIO MOBILE

El proceso de verificación y simulación es imprescindible como herramienta de planificación para la creación de nuevos enlaces y optimización de los que ya se tienen, antes poco usada dentro de la empresa Sigsignet, evitando así prácticas empíricas, adicional a esto es que uno de los aspectos de brindar una calidad óptima del servicio recae en ello, por tal su uso se encuentra más que justificado. La empresa al momento dispone de varios nodos de largo alcance que dentro del proceso de reestructuración deberán ser sometidos a un nuevo proceso de simulación y recalculo, medida en la cual se determinará la factibilidad o no del Hardware actual y su posible reemplazo.

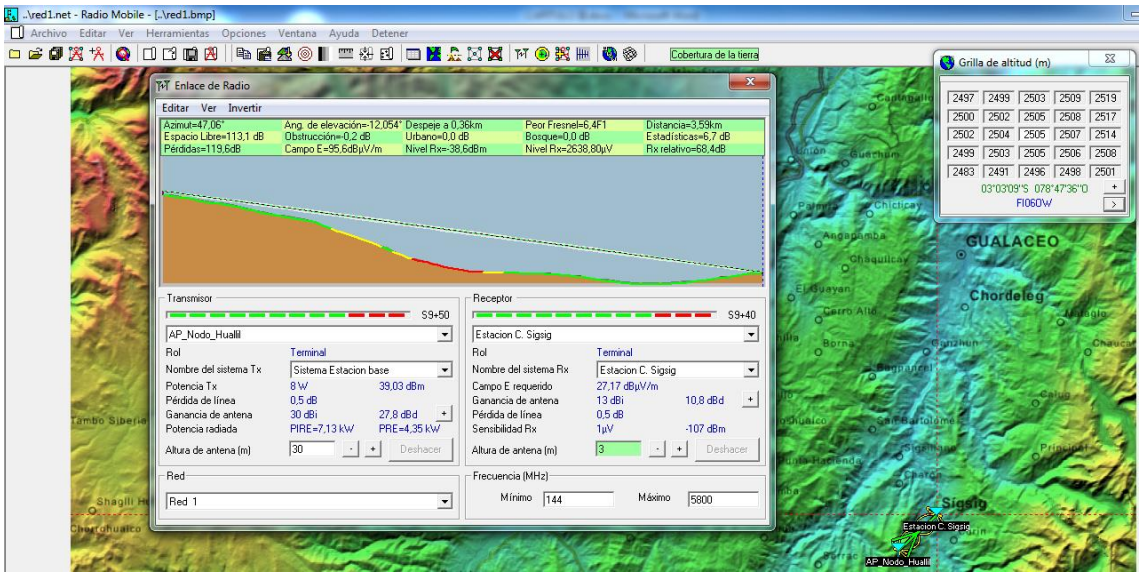


Figura 3.24. Vista global de la simulación del enlace Huallil-Sígsig

Fuente: Los Autores, Simulación Enlace Huallil- Sigsig, 2013

Entre la simulación y cálculo del enlace actual Huallil – Sigsig, la misma arroja resultados positivos en cuanto a línea de vista óptima, quizá la limitada capacidad del

Hardware de momento han permitido ante análisis de capacidad previamente realizado que dicho enlace presente problemas de latencia, para tal se sugiere dado la factibilidad del carrier la reubicación del Nodo Principal ubicado en el Sígsig al Cerro Huallil o a su vez el empleo de hardware de mayores prestaciones, siendo la primera la opción más viable con mínimos gastos generados.

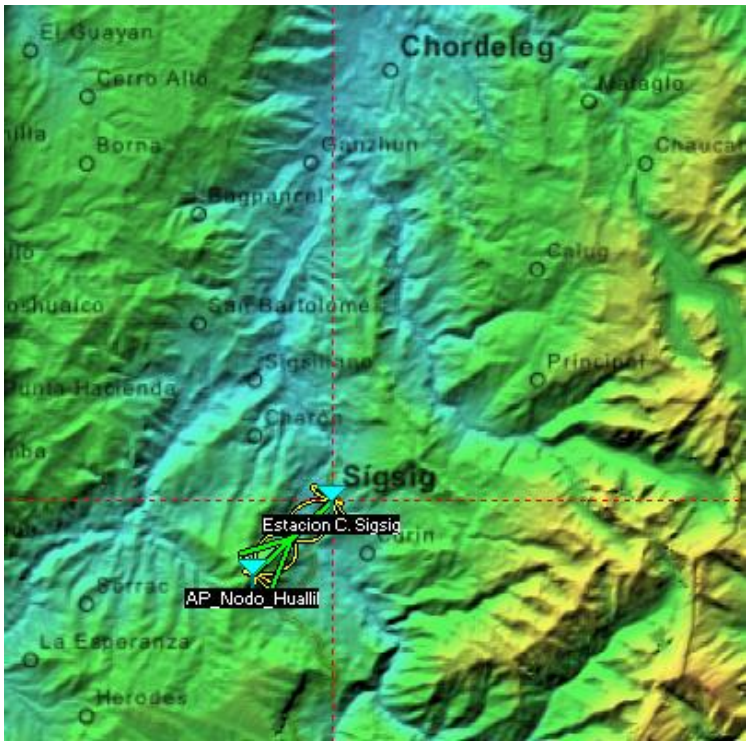


Figura 3.25. Geo posicionamiento del Enlace Huallil-Sígsig

Fuente: Los Autores, Simulación Enlace Huallil- Sigsig, 2013

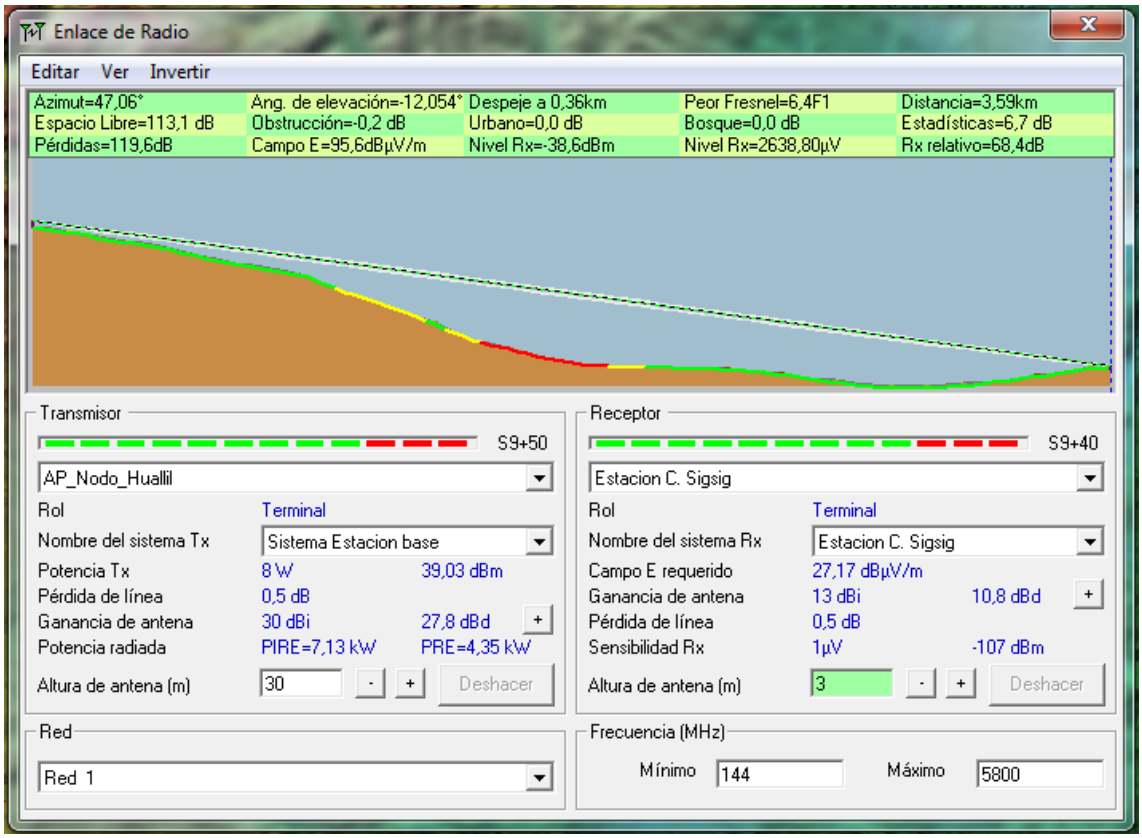


Figura 3.26. Resultados Radiomobile Calculo Enlace Huallil-Sígsig

Fuente: Los Autores, Simulación Enlace Huallil- Sigsig, 2013

De la misma forma el proceso aplicado para simulación del enlace principal es aplicado para los enlaces secundarios arrojando resultados similares, que sugieren una optimización sobre los puntos de distribución o AP'S a nivel de Hardware, es necesario también recalcar que la competencia es un tema a considerar, ya entre los parámetros usados para esta prueba denotaron un mal uso de las frecuencias por parte de los mismos, pudiendo ser un factor que a futuro podría causar serios problemas afectando el buen rendimiento sobre el servicio, por tal una solución clara sería una administración ordenada de las mismas en acuerdo con la competencia siendo la más viable o la utilización de frecuencias no libres la menos viable por los costos derivados de pago por su uso.

3.2.6 MEDICIÓN Y EVALUACIÓN DEL ESTADO Y RENDIMIENTO DE LA RED ACTUAL Y DESEADA

3.2.6.1 ANCHO DE BANDA

Según Wikipedia se define como la cantidad de datos que se pueden transmitir en una unidad de tiempo, cuyas unidades de medidas se establecen en bits por segundo o sus derivados (bps), (Kbps), (Mbps), ligada al término canal de compartición referido al número de usuarios que comparten el ancho de banda en un mismo medio de transmisión.

Sigsignet en sus inicios, siendo una empresa nueva en el mercado del cantón el Sígsig inició con una capacidad Internacional contratada de 2Mbps 1:1, determinados y adecuados a la cantidad de usurarios que en aquel tiempo disponía. Hace algunos años atrás los costos de acceso Internacional en Ecuador eran muy elevados a comparación de los anchos de banda ofrecidos, relación que con el pasar del tiempo fue cambiando, los elevados anchos de banda que demandaban la llegada de la Web 2.0 y los nuevos medios de transporte que posibilitaban transmitir más capacidad por la misma vía como por ejemplo la fibra óptica, cambiaron radicalmente el panorama, reduciendo dichos costos pero a su vez demandando mayor capacidad de conexión. Por tal el proceso de redimensión de la capacidad contratada a los carriers es constante en este tipo de negocios, por tal razón uno de los talones de Aquiles de muchas de estas empresas es la administración del preciado ancho de banda, su manejo optimo puede representar el éxito o fracaso, ya que conforme la red crece el caudal necesario para satisfacer una conexión banda ancha optima también, estableciendo entre estas dos variantes una relación exponencial.

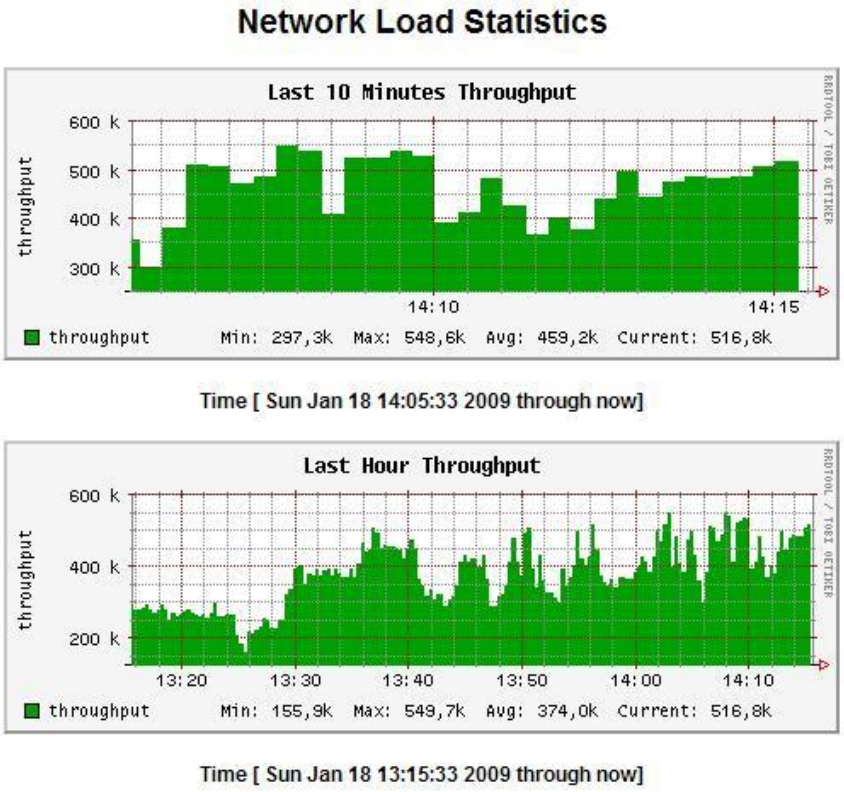


Figura 3.27. Estadísticas de Consumo Sigsignet

Fuente: Sigsignet, Estadísticas de Consumo, 2009

Como se ha mencionado la capacidad internacional contratada es proporcional, misma que se ha visto incrementado desde sus inicios, en la siguiente imagen se presenta una captura consolidada tomada en el año 2009 con cerca de 60 subscriptores y planes del servicio con soporte para más capacidad a los iniciales.

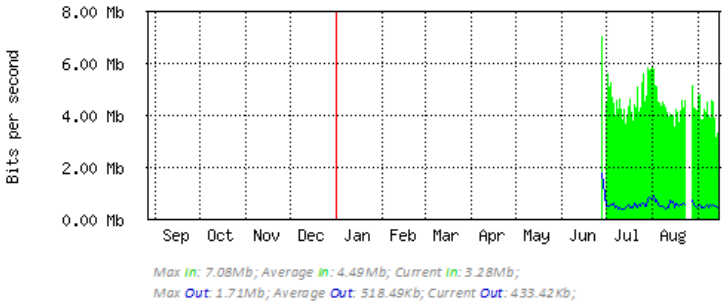


Figura 3.28. Estadísticas de Consumo Sigsignet

Fuente: Sigsignet, Estadísticas de Consumo, 2012

Actualmente la capacidad administrada del Nodo central se limita a 25 Mbps 1:1, limitados por la capacidad de su red interna, para dar cabida a administrar una mayor capacidad, por tal el plan de reestructuración contempla el incremento del mismo facilitando en primera instancia administrar unos 100 Mbps sin problema alguno, mismo que podrá escalar con el pasar del tiempo, además se contempla un nuevo medio de acceso contrario al utilizado actualmente, denominada FTH o fibra óptica residencial, buscando elevar el nivel de fiabilidad sobre la red deseada.

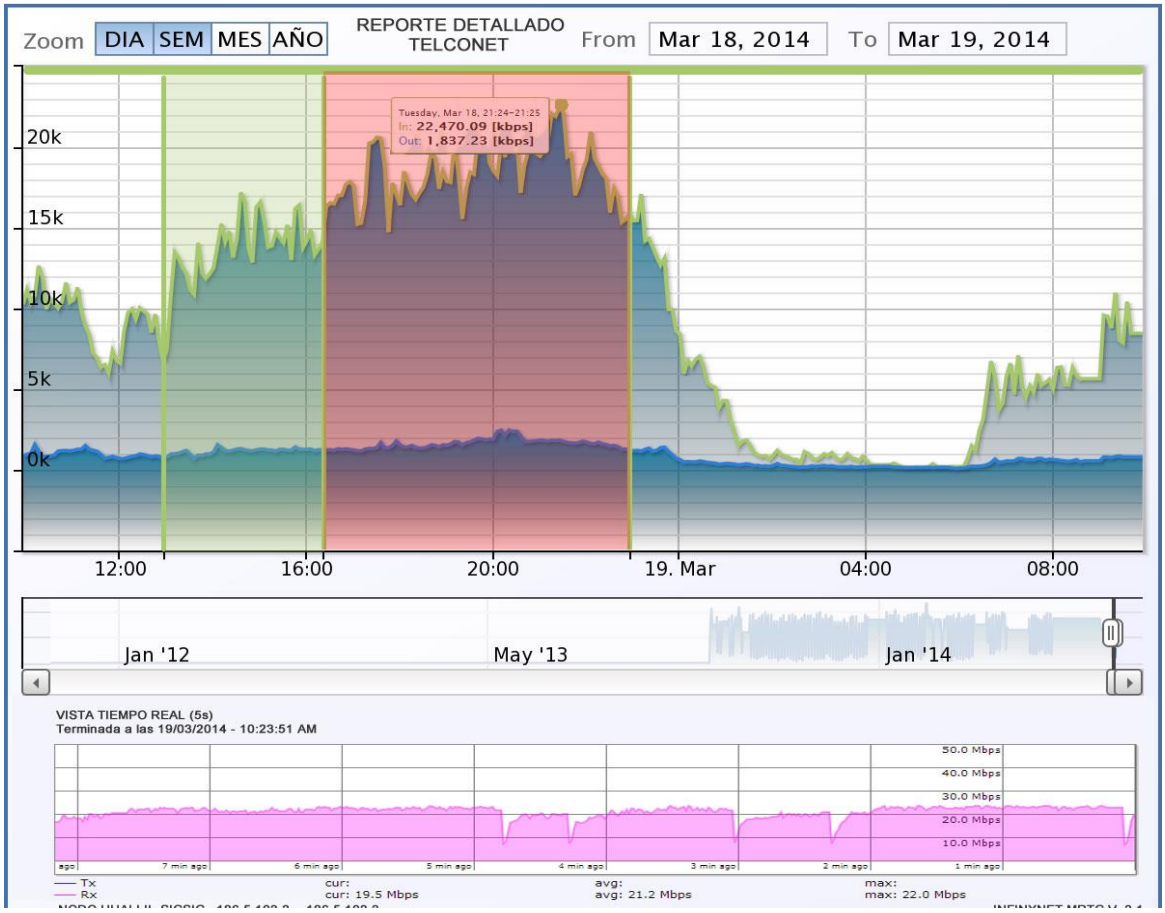


Figura 3.29. Estadísticas de Consumo Sigsignet

Fuente: Sigsignet, Estadísticas de Consumo, 2014

3.2.6.2 JITTER

Definido como la variación de retardo entre los paquetes que arriban, generalmente causado por diversos factores como la congestión de la red, pérdida de

sincronización o por las diferentes rutas seguidas por los paquetes para llegar al destino, conocido también como señal de ruido no deseada, factor que dentro de una red de datos es un problema muy relevante, aplicable también sobre una red Wireless, por congestión de frecuencias o redes vecinas que de una u otra manera interfieren en la señal que se está emitiendo, hoy seriamente agravado sobre frecuencias de uso doméstico establecida en los 2.4 GHz, la disponibilidad de canales en esta está muy limitada, lo que hace que uno o varios equipos utilicen el mismo canal de transmisión ocasionando que exista pérdida de paquetes ya sea porque estos llegan demasiado pronto o demasiado tarde, esto se ve mayormente afectado en aplicaciones de tiempo real como lo son radio, telefonía IP, video conferencias, etc., especialmente sensibles y comúnmente más notorio sobre enlaces lentos o congestionados, cabe recalcar que mecanismos como la calidad de servicio o QoS, enlaces de alta velocidad etc., son capaces de mitigar en cierta forma dicho problema.

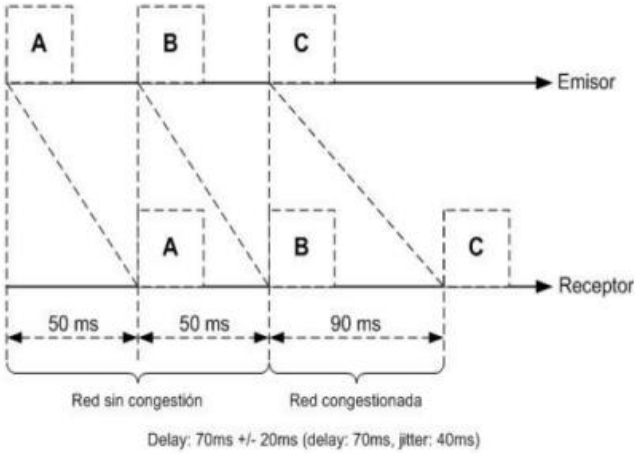


Figura 3.30. Jitter

Fuente: D. A. Howe; T. N. Tasset, "Clock Jitter Estimation based on PM Noise Measurements", Boulder, CO 80305, 2003.

En la imagen anterior, se puede observar como los paquetes A y B llegan a su destino cada 50 ms en comparación al paquete C que muestra un retraso de 40 ms que los paquetes antes mencionados.

En la red actual de la empresa Sigsignet, durante las etapas de análisis de tráfico y protocolos mediante herramientas como Wireshark se denoto notables inconvenientes a nivel de Jitter, que si bien no son de carácter critico si merecen ser tomados en consideración, la problemática se divisa por la ausencia de mecanismos de encolamiento no disponibles en la plataforma de gestión y control actual, mecanismos esenciales que actúan como buffers descartando los mismos si no se encuentra en la cola o su vez como un almacén temporal recibiendo y emitiendo paquetes con un mínimo retraso, mismos que son controlados sobre la red deseada, utilizando herramientas como encolamiento por árbol de colas o colas simples, imprescindibles para establecer un control puntual a este problema si bien no lo elimina completamente pero de cierta forma lo mitiga al máximo, dichos mecanismos actúan en conjunto con una serie de algoritmos para manejo de colas propietarios y genéricos para llevar a cabo dichas tareas, tales como por ejemplo PCQ, PFIFO, RED etc., por ende su correcta implementación es de vital importancia para un funcionamiento eficiente.

3.2.6.3 RETARDO PUNTO A PUNTO

Conocido como latencia definido como la diferencia que existe entre la instancia que una señal es transmitida y el momento de su arribo, considerado como un problema existente en casi todas las redes de datos.

Sobre la infraestructura de la red actual de la empresa Sigsignet, previo análisis realizados en puntos anteriores, se ha determinado causales relevantes que están ocasionado una pérdida de rendimiento significativa sobre la red, como lo es el retardo punto a punto existente, que si bien no contempla una solución sencilla, en ocasiones dicho inconveniente puede ser mitigado por el Hardware encargado de pasar el tráfico de la red o a su vez la implementación de políticas de control de tráfico adecuadas dentro de la red, como el marcado de paquetes y su priorización o

la reserva necesaria de ancho de banda, siendo medidas que de una u otra forma colaboran a optimizar dicho retardo, reduciendo su impacto al mínimo.

Uno de los retardos detectados en la evaluación a la red actual de la empresa y el más significativo se encuentra sobre entre el punto a punto Sigsig – Huallil, punto de recepción del servicio de internet donde se recepta la capacidad internacional contratada por parte del proveedor y el nodo principal de difusión, ubicado en el cerro Huallil, lugar donde se difunde el servicio hacia las diversas zonas aledañas. El problema de este retardo se debe al límite de capacidad que los equipos receptores y emisores han alcanzado generando este inconveniente, en tanto la red deseada, no solo utilizada hardware de mayores prestaciones sino las características que RouterOS permite aplicar configuraciones adicionales para dar tratamiento a este tipo de problemas y como ya se dijo reducir al mínimo su impacto, por eso se realizan pruebas de latencia utilizando herramientas del mismo sistema operativo como el comando ping o pingPlotter sobre la red actual y simulada en diferentes horarios del día, cabe recalcar que debido al medio sobre el cual se distribuye el acceso el factor climático y geografía son elementos a tomar en consideración pero que previos análisis en la simulación se ha descartado afectación al menos de la parte geográfica, reflejando los siguientes resultados.

	Red Actual		*Red Deseada*	
	Mañana	***Tarde***	***Mañana***	***Tarde***
Test en el Punto a Punto Sigsig - Huallil	75 ms (Promedio) 1% perdida de paquetes	179 ms (Promedio) 5% perdida de paquetes	Salto Eliminado (0 ms) 0% perdida de paquetes	Salto Eliminado (0 ms) 0% perdida de paquetes
Test Cliente – AP Sigsig 1	80 ms (Promedio) 2% perdida de	185 ms (Promedio)	3 ms (Promedio) 0% perdida de	15 ms (Promedio) 0% perdida de

	paquetes	6% perdida de paquetes	paquetes	paquetes
Test Cliente – AP Sigsig 2	73 ms (Promedio) 2% perdida de paquetes	195 ms (Promedio) 5% perdida de paquetes	4 ms (Promedio) 0% perdida de paquetes	12 ms (Promedio) 0% perdida de paquetes
Test Cliente – AP San Bartolo	84 ms (Promedio) 1% perdida de paquetes	172 ms (Promedio) 2% perdida de paquetes	2 ms (Promedio) 0% perdida de paquetes	3 ms (Promedio) 1% perdida de paquetes

Tabla 3.7. Tabla de Resultados de pruebas de Retardo Punto a Punto.

Fuente: Los Autores, Pruebas de Retardo Punto a Punto red actual y Deseada, 2013.

3.2.6.4 PÉRDIDA DE PAQUETES

La pérdida de paquetes en enlaces de radio es casi un problema que muchos WISP lo tienen muchos por latencia generada en sus equipos o por la configuración no adecuada de los mismos, en cierta forma al ser equipos inalámbricos donde cuyo acceso al medio es compartido sin capacidad de diferenciación puede generar que por ejemplo una aplicación de voz, sufra pérdidas o retardos elevados, ya que el medio de por no emplea garantías sobre dicho tráfico, incluso a veces el mismo entorno pueden ser factores determinantes para afectar la transmisión de paquetes sobre el medio, causando que cuando dicho problema surja la perdida de velocidad en cuanto a la entrega del servicio de Internet sea un problema relacionado.

Las posibles soluciones para evitar este tipo de problemas quizá un análisis del espectro constante en búsqueda de frecuencias o canales limpios que no generen interferencias, además el uso de protocolos robustos que empleen técnicas de acceso

al medio como lo es TDMA, NStreme en RouterOS, Airmax desde haciendo más eficiente el uso del canal.

3.2.6.5 THROUGHPUT DE ENLACES PRINCIPALES Y SECUNDARIOS

El análisis resultante de la evaluación de troughput sobre enlaces principales y secundarios tanto en la red actual como en la red deseada se detalla de la siguiente manera, para dichas pruebas se generó pruebas de stress específicas que permitan saturar la red al máximo y determinar un caudal real más el valor teórico dado por el fabricante en los diversos datasheet de los equipos, e incluso los servicios de red que los mismos tenga habilitados como firewall, encolamiento etc.

Prueba	*Red Actual*	*Red Deseada*
Prueba de Capacidad		
Prueba de Capacidad Enlace Huallil – Sigsig 1 Multipunto	Marca: Tranzeo Modelo: Tr-SL2 Frecuencia: 2.4 Ghz RX:8 Mbps TX: 7 Mbps Uso recursos Hardware 75% promedio	Marca: Mikrotik Modelo: BaseBox Frecuencia: 2.4 Ghz RX:31 Mbps (Promedio) TX:23 Mbps (Promedio) Uso recursos Hardware 25% promedio
Prueba de Capacidad Enlace Huallil – Sigsig 2	Marca: Tranzeo Modelo: Tr-5a-20 Frecuencia: 5.8 Ghz RX:14 Mbps TX:11 Mbps	Marca: Mikrotik Modelo: BaseBox Frecuencia: 2.4 & 5.8 Ghz RX:52 Mbps (Promedio)

	Uso recursos Hardware 97% promedio	TX:48 Mbps (Promedio) Uso recursos Hardware 50% promedio
Prueba de Capacidad Enlace Huallil – San Bartolo	Marca: Tranzeo Modelo: Tr-5a-20 Frecuencia: 5.8 Ghz RX:13 Mbps TX: 9 Mbps Uso recursos Hardware 90% promedio	Marca: Mikrotik Modelo: BaseBox Frecuencia: 2.4 & 5.8 Ghz RX:49 Mbps (Promedio) TX: 47 Mbps (Promedio) Uso recursos Hardware 30% promedio

Tabla 3.8. Tabla de Resultados de pruebas de Troughput de Enlaces

Fuente: Los Autores, Pruebas de Troughput de Enlaces, 2013.

3.2.6.6 ANÁLISIS DE APLICACIONES TIEMPO REAL, PÁGINAS WEB E ICMP

El proceso de análisis de aplicaciones en tiempo real, apertura de páginas web e ICMP, basa su fundamento de la prueba en un procedimiento empírico apoyado de una base conceptual sólida, por ejemplo el tiempo de resolución de un nombre de Dominio y por ende su posterior tiempo de carga, utilizando nombres de dominios establecidos como los más visitados por los usuarios, evaluando los mismos en horas de congestión y horas sin la misma, para efecto de dicha prueba se dispone de un ordenador libre de amenazas, virus, o aplicación que se ejecuten en segundo plano o que a su vez consuman ancho de banda, adicional un enlace con compartición 8:1 residencial basico de la empresa Sigsignet cuyo valor de descarga es 1.2 Mbps y 850 Kbps de subida evaluados sobre la red actual, y una segunda prueba de similares

condiciones sobre la red deseada, en diferentes horarios tanto sobre horas de congestión y sin la misma en la red, arrojando los siguientes resultados.

Prueba	Indicadores de Rendimiento	
	Red Actual	**Red Deseada**
Tiempo de apertura de Dominios más visitados: Youtube, Facebook, Instagram, Twitter, Vimeo etc.	Hasta 5 seg.	Hasta 2 seg
Calidad de conexión sobre protocolo UDP en Video llamadas o llamadas VoIP	Regular, presenta intermitencias y denota ausencia de calidad.	Optima, en horas de saturación se mantiene la calidad con mínimas intermitencias.
Streaming de video en línea, Youtube, Vimeo, Dailymotion.	Deficiente, intermitencias constantes en sus diversos planes, definición por defecto 360p en youtube.	Óptima, sin intermitencias en sus diversos planes, definición por defecto 720p youtube.
Pruebas de ICMP con saturación completa del canal, hacia el mundo.	Presenta una tasa promedio de 3% de perdida de paquetes.	No presenta perdida de paquetes.

Tabla 3.9. Tabla de Resultados de pruebas de Análisis de calidad de conexión.

Fuente: Los Autores, Pruebas de calidad de conexión, 2013.

3.2.6.7 ANÁLISIS DE QOS.

La calidad de servicio o QoS establecidas como un conjunto de características relacionadas con la provisión de uno o más servicios hacia un usuario, aplicación informática etc., que buscan asegurar la entrega del caudal o ancho de banda y la diferenciación del servicio dentro de una red de datos. Dado el notable acceso a Internet y los nuevos servicios que por dicho medio se ofertan como el soporte para majeo de audio, video y diverso tráfico multimedia, han sido pautas para establecer modelos de QoS para satisfacer diversas necesidades, considerando parámetros de vital importancia como lo es el ancho de banda o la latencia, permitiendo y asegurando fiabilidad durante periodos de congestión, por lo tanto se consideran algunos modelos a seguir según la IETF misma que define lineamientos para transferir información a través de la red que son los siguientes.

- Diff-Serv (Servicios Diferenciales)
- Int-Serv (Servicios Integrales)
- MPLS (Multiprotocolo de conmutación de etiquetas)
- Ingeniería de Trafico.

Herramientas complementadas con mecanismos para hacer uso adecuado de los recursos de la red siempre y cuando se tenga presente el requerimiento de los usuarios, si bien no se detalla un análisis a fondo sobre esta temática por su amplio contenido, se contempla en el proceso de reestructuración como herramienta para control de QoS el modelo Diff-Serv, como mecanismo a ser aplicado dentro de Mikrotik y sobre la nueva red de datos, para tal se propone establecer marcas sobre el tráfico utilizando “Mangle” para su posterior tratamiento y asignación de prioridad o a su vez por ToS utilizando el encabezado del paquete IP como medio de clasificación y asignación de marca, cuyos niveles de precedencia definidos en 8 peldaños, van desde Normal o Rutinario hasta Control de red, siendo el ultimo el más prioritario.

Por lo tanto, mecanismos dentro de RouterOS ya explicados previamente como Queue Tree, han permitido en base a dicho modelo conceptual “Diff-Serv” armar una

propuesta de QoS, es claro que su análisis es una tarea de carácter delicado y contempla el uso de diversas herramientas tales como ping, Torch, ping speed etc., propietarias de Mikrotik así como las estadísticas generadas por el árbol de colas, y en el caso de ping de los clientes Windows o Linux y metodologías empíricas como el índice de satisfacción del usuario e incluso pruebas externas como speedtest o visualware.

3.3 DUDE COMO HERRAMIENTA DE MONITORIZACION DE ENLACES.

Mejor conocido como Sistema Centralizado de Monitorización y Administración de Red, Servicios y Protocolos, Dude es una herramienta libre elaborada por Mikrotik diseñada para representar la estructura de una red mediante un diagrama gráfico, que está ganando muchos adeptos, ello debido no solo a su nivel de personalización sino debido al nivel de parametrización soportado y más que nada su muy intuitiva y fácil interfaz, la herramienta se integra adecuadamente con RouterOS para su monitorización y generación de estadísticas pero es posible monitorizar equipos de otros vendedores por medio del uso de protocolos como SNMP en cualquiera de sus versiones y así utilizar una plataforma desarrollada por Mikrotik con otros dispositivos. Se puede monitorizar y establecer dos estados como de caído o activo de cualquier dispositivo de red empleando ICMP o Ping para dicha monitorización, así como también es posible la generación de estadísticas puntuales otorgadas por el protocolo SNMP y almacenadas por Dude, nivel de tráfico por interfaz, intensidad de señal, ruido con equipos bajo 802.11, algunas de las funciones de alerta usadas por dude son las notificaciones bajo correos electrónicos o mediante el uso de SMS siendo todas partes del paquete Dude, es posible correr el mismo directamente desde Windows es decir funcionando como servidor o a su vez utilizarlo como host para una conexión remota a un servidor Dude, además su instalación dentro del Hardware dedicado de Mikrotik conocido como RouterBoard se lo realiza por medio de un paquete, también puede ser instalado en sistemas operativos Linux.

Al ejecutar por primera vez dude pedirá definir el idioma por defecto en el cual se mostrará la aplicación, seguido se observará al cliente dude mostrando los

parámetros de conexión a setear para conectarse o bien en modo servidor o modo cliente.

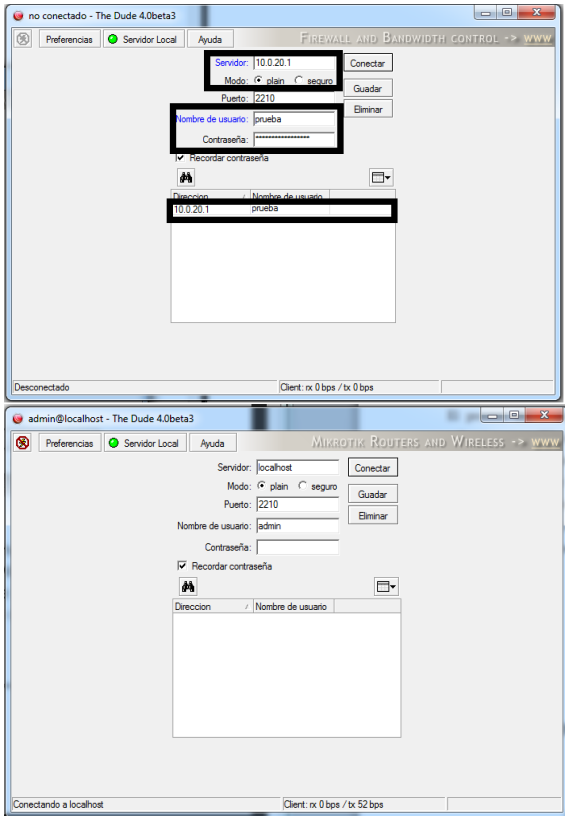


Figura 3.31. Ventana Login Monitor Dude

Fuente: Los Autores, Mikrotik Dude Login, 2013

Es posible guardar los parámetros de conexión al servidor Dude, para poder más tarde realizar conexiones fáciles sin necesidad de volver a introducir los parámetros de conexión, además bajo topologías extensas y amplias se puede usar el concepto de agentes Dude, que no es nada más que un servidor que actúa detrás de un servidor primario, el agente se configura para obtener información estadística a donde el servidor primario no puede llegar en dicha subred pero donde el agente lo hace sin problema alguno.

Como se ha mencionado Dude tiene dos modos de conexión la primera que puede actuar como cliente en donde será necesario definir la IP del servidor Dude y su

respectivo Usuario y Password, y la otra opción que es actuar como servidor local para ello hace uso del parámetro localhost, además es importante definir el tipo de conexión si es plano o seguro haciendo uso de un protocolo cifrado para su conexión, sin mencionar el puerto por defecto dude se ejecuta que es el puerto 2210, pero es posible levantar dicho servicio sobre otro puerto, e incluso una tarea esencial luego de conectar el cambio por defecto del usuario admin dentro de Dude ya que los usuarios manejados por RouterOS son diferentes a los que maneja Dude, si el servidor dude ha sido alojado como un paquete de RouterOS.

Una vez dentro de Dude se tiene un set de opciones imprescindibles por los cuales se mencionará los más relevantes.

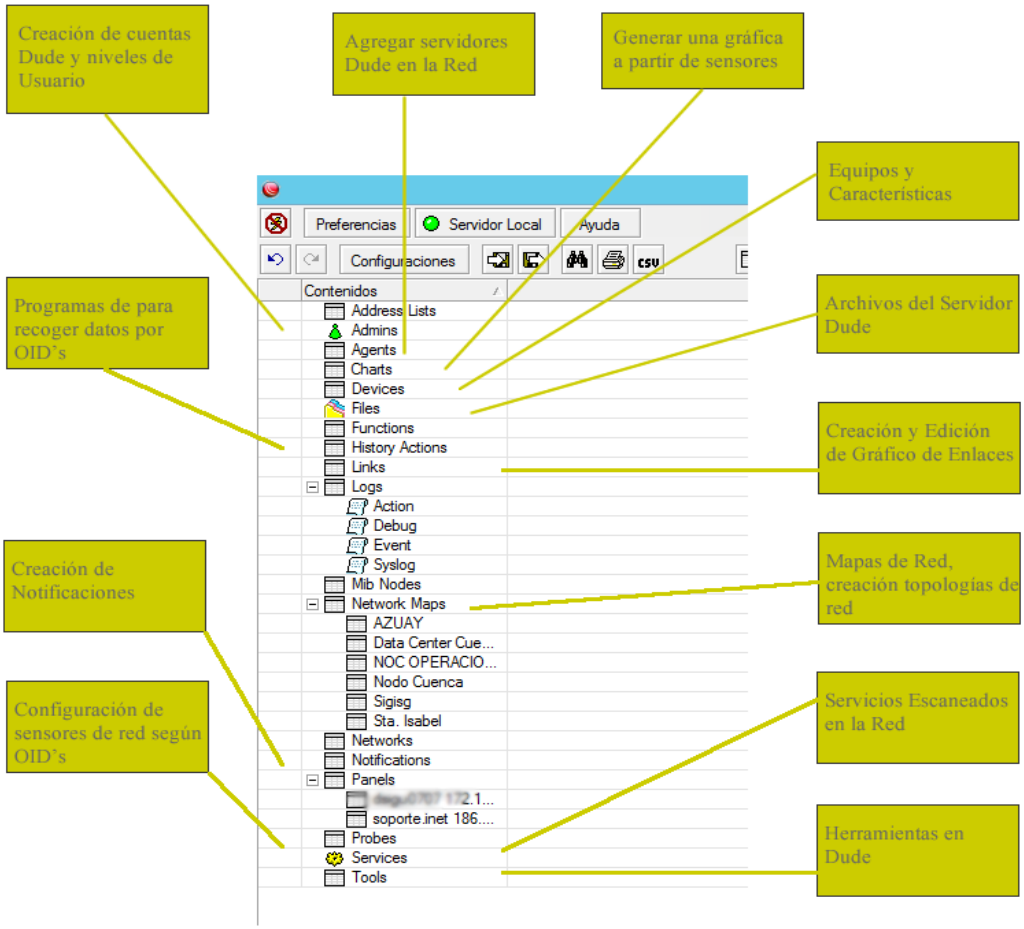


Figura 3.32. Pestaña de configuración de Preferencias de Dude

Fuente: Los Autores, Configuración de "The Dude" como network managment system, 2013

El botón preferencias define parámetros orientados a como se establece la conexión, donde se ubican iconos, su ejecución dentro del sistema operativo y lenguaje por defecto a usar.

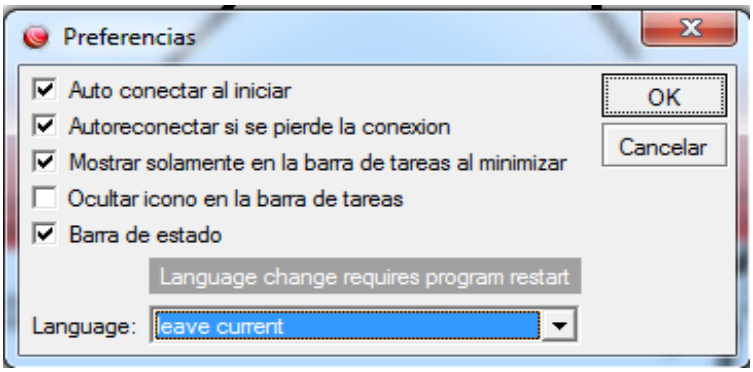


Figura 3.33. Pestaña de configuración de Preferencias de Dude

Fuente: Los Autores, Mikrotik Dude, 2013

En tanto el botón configuraciones, se puede establecer parámetros orientados a definir ya configuraciones más específicas como agentes de monitoreo dentro de las redes remotas, servidor SMTP para notificaciones vía correo electrónico, puertos de acceso para monitoreo por medio de la web, servidor log, parámetros de conexión para equipos RouterOS y entre otros más.

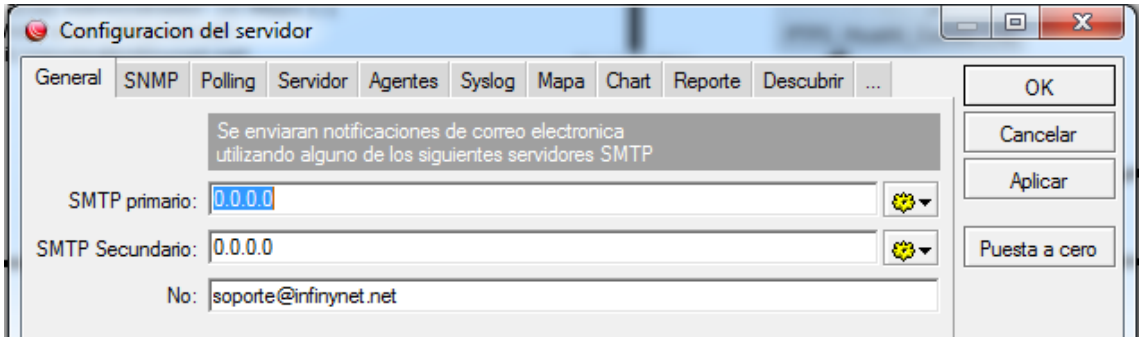


Figura 3.34. Pestaña de configuración General de Dude

Fuente: Los Autores, Mikrotik Dude, 2013

En tanto en el panel de contenidos se puede encontrar:

- Address Lists.- Se lista todas las IP agregadas en una Lista de IP dentro de equipos RouterOS.
- Admins.-Se agregar todos los grupos y usuarios con privilegios o no para el acceso a Dude.
- Charts.-Se pueden identificar las fuentes de datos asociadas para la generación de datos estadísticos en los diagramas.
- Devices.- Podemos visualizar dispositivos que han sido agregados tanto por medio del escaneo automático o la asignación manual de host, en el caso de dispositivos RouterOS podemos visualizar determinados parámetros solo visibles si dichos equipos monitoreados tiene RouterOS como tal, y finalmente un mapeo completo de direcciones MAC.
- Funciones.-Es posible definir funciones específicas definidas por el usuario para que realicen tareas específicas como retornar propiedades de un dispositivo.
- Log.-Dude puede actuar como un servidor Log, donde además de colectar todos los logs de los equipos Monitorizados y administrar una base de log unificada.
- Network Maps.- Es aquí donde se establecen los gráficos de los mapas y submapas asociados.
- Notifications.-Aquí se definen las notificación en caso de alertas pudiendo tener desde notificaciones auditivas hasta por medio de sms, incluso es posible crear notificaciones personalizadas y poderlas agendar o planificar para su ejecución.

  El proceso para agregar dispositivos a monitorizar se lo puede hacer por dos formas por medio de un escaneo automático o por medio de una agregación manual, en el caso del escaneo automático en el menú superior de la opción Network Map podemos utilizar el botón Descubrir para realizar dicha tarea, en donde se definirá la red ha escanear e incluso si lo vamos hacer por medio de un agente, además podemos setear configuraciones solo de ese grafico de

la red como colores, fondos etc., siendo posible también la opción de exportación desde el botón utilidades en formato de imagen tipo jpg, bmp etc.

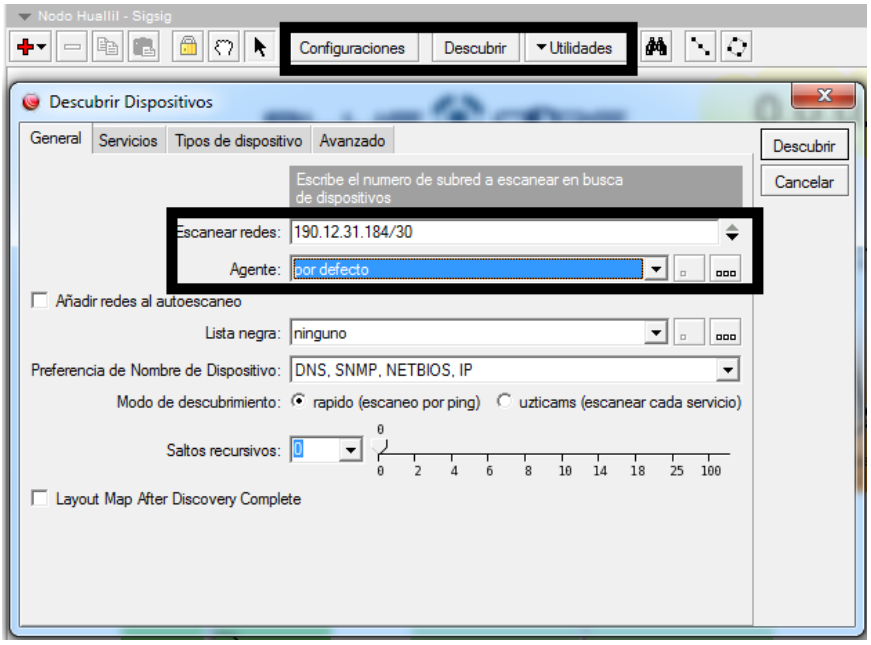


Figura 3.35. Pestaña de agregación de subredes y dispositivos a monitorizarde Dude

Fuente: Los Autores, Mikrotik Dude, 2013

En cambio la agregación manual del dispositivo se la puede realizar utilizando el botón (+) dentro de la opción Network Map o sobre el área de trabajo dando click izquierdo para poder visualizar un submenú con las siguientes opciones.

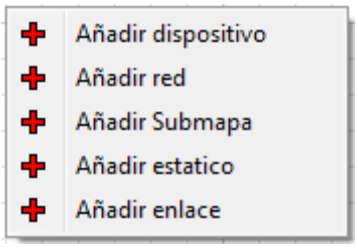


Figura 3.36. Opción para agregación de elementos en Dude

Fuente: Los Autores, Mikrotik Dude, 2013

Siendo posible agregar desde dispositivos de red por medio de una IP, o una red completa, cuando agregamos dispositivos hay una característica relevante como el poder asociar a este dispositivo con sus credenciales si es RouterOS, permitiéndonos de cierta forma utilizarlo como un winbox remoto o incluso aperturar al mismo sin ser necesaria cada vez el ingreso de sus credenciales.

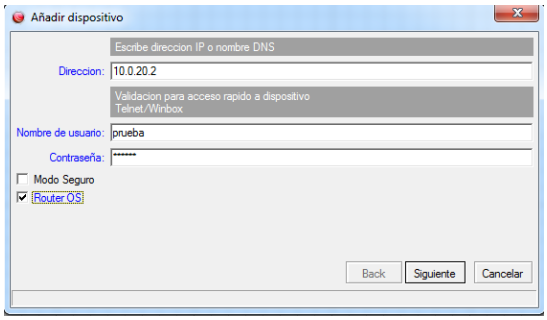


Figura 3.37. Pestaña para agregar dispositivos

Fuente: Los Autores, Mikrotik Dude, 2013

Un procedimiento importante es la agregación de enlaces lógicos que representan como se encuentra relacionados y en si su uso después por medio de la generación de estadísticas bajo la forma o protocolo de monitorización para la obtención de estadísticas puntuales como tráfico por Interfaz e incluso en el caso de Punto de Acceso Wireless Niveles de señal y ruido.

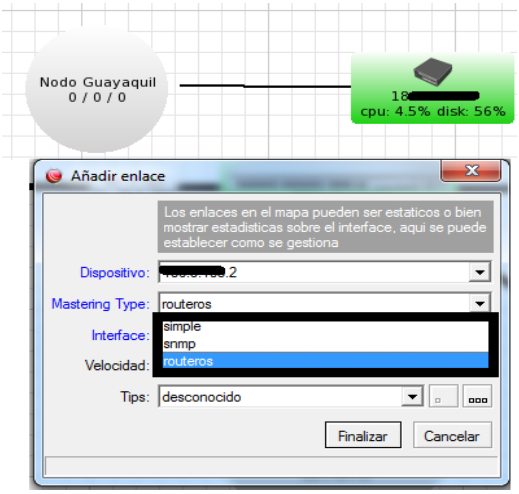


Figura 3.38. Pestaña para agregar enlaces

Fuente: Los Autores, Mikrotik Dude, 2013

Desde la parte Wireless y por medio de dude se puede utilizar herramientas como el spectral scan y las soportadas por RouterOS y porque no también bajo SNMP la obtención de estadísticas wireless.

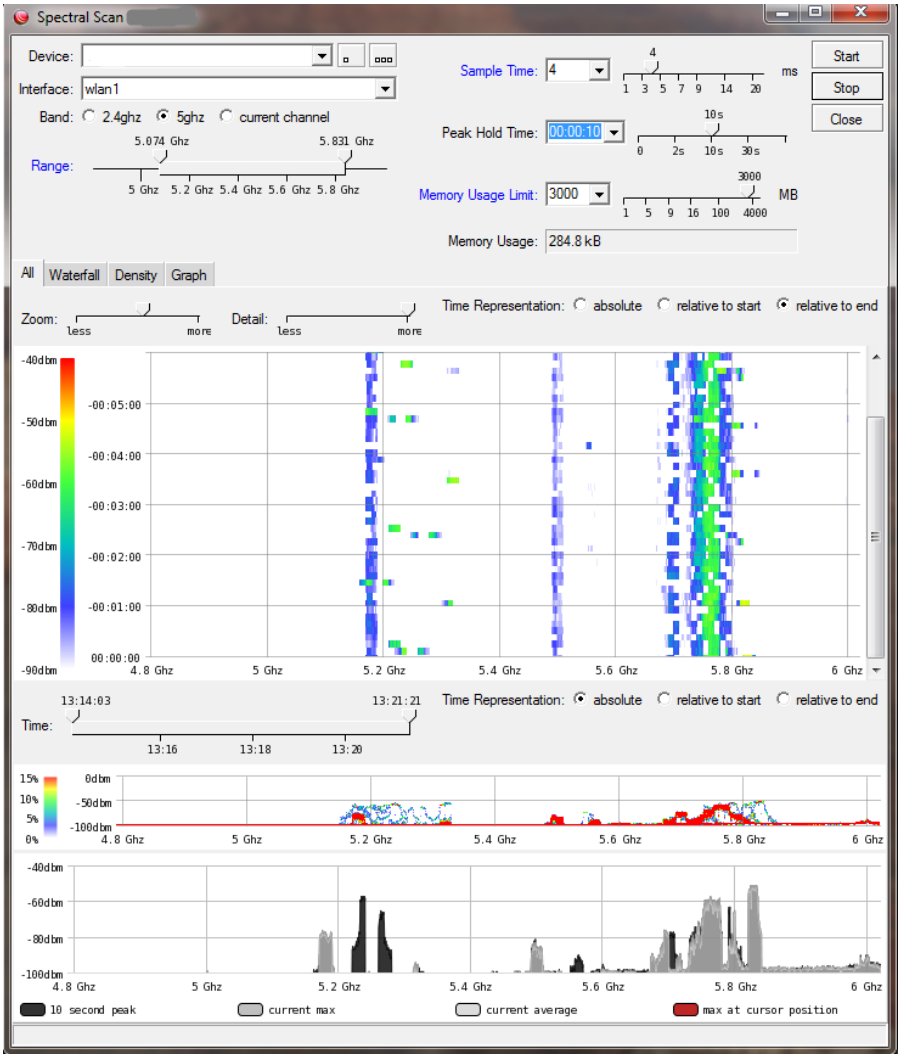


Figura 3.39. Pestaña para monitorización de Espectro.

Fuente: Los Autores, Mikrotik Dude, 2013

3.3.1 INSTALACIÓN Y CONFIGURACIÓN INICIAL EN ARQUITECTURAS X86 Y ROUTERBOARD.

El proceso de Instalación es relativamente sencillo, si trabajamos con una RouterBoard para convertirlo en un servidor Dude será necesaria la descarga desde sus repositorios de la versión actual soportada para dicha arquitectura generalmente

asociada con archivos de extensión .npk, se debe tener presente que los RouterBoard soportan diversas arquitecturas sobre sus placas madre, las mismas pueden ir desde arquitecturas tipo mipsbe, Power PC, Tilera entre otras., en el caso de querer trabajar con nuestras PC será necesaria descarga la versión o instalable para Windows, pudiendo instalar incluso las versiones en estado Beta, es posible desde el Host o cliente Dude hacer que el servicio se ejecute en Background, o desde los RouterBoard con solo instalar el paquete el servicio se mantendrá en ejecución, como se mencionó el cliente dude o host puede conectarse tanto localmente como remotamente al Servidor, se ha podido comprobar según experiencias personales en este trabajo que operar sobre un arquitectura X86 y RouterOS a bordo junto con Dude como paquete instalado dentro de este, su funcionamiento es más estable, por el hecho de poder disponer más memoria y espacio en disco a diferencia de las RouterBoard.

Los requerimientos mínimos en un sistema X86 son:

- Memoria RAM mínima 64 Mb y recomendada 128 MB
- OS: Windows 2000/XP con permisos de Administrador, no funciona con (Windows 95/98/Me)
- Resolución de Video 800x600

Para este caso vamos utilizar el instalador Dude en su versión 4.0 en estado beta versión 3, obtenido desde la página Mikrotik .com sección dowloads, una vez descargado dicho paquete cuya extensión es .npk, será necesario aperturar Winbox y arrastrar el mismo a la pestaña Files dentro de este, para que RouterOS agende la instalación de dicho paquete y pueda el equipo empezar a actuar como servidor Dude.

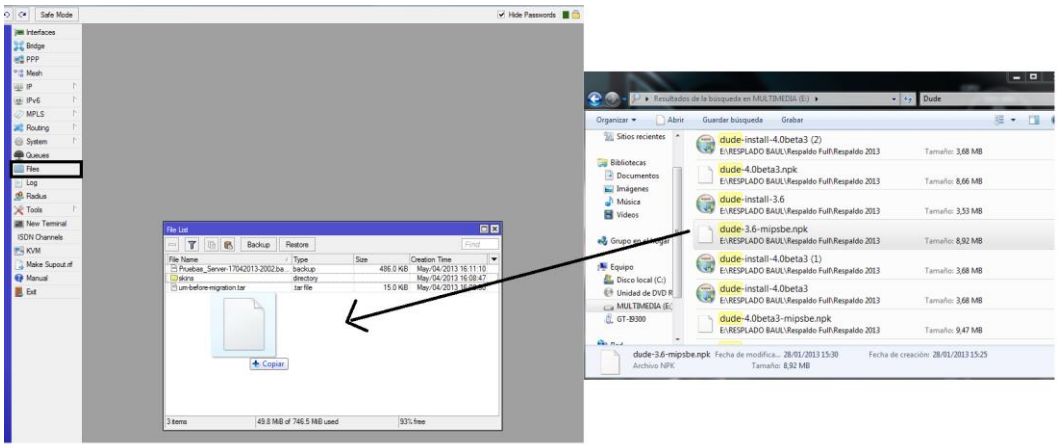


Figura 3.40. Proceso de instalación de Paquete Dude en Winbox.

Fuente: Los Autores, Mikrotik Dude, 2013

Una vez realizado ello bastara un Reinicio del dispositivo y el servicio Dude estará en ejecución, ahora será turno de la instalación del cliente Dude mismo que se conectara al servidor, para ello deberemos solo bajar la versión adecuada similar a la instalada en el paquete y podremos realizar la instalación.

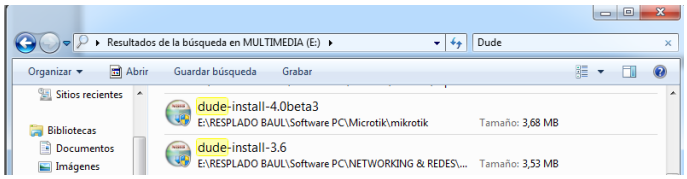


Figura 3.41. Instalación de Cliente Dude en Winbox.

Fuente: Los Autores, Mikrotik Dude, 2013

El proceso de instalación de Dude es relativamente sencillo tanto como otras aplicaciones en Windows, ya que sus Wizard o asistentes hacen que dicho procedimiento sea relativamente sencillo, en primer lugar agregar los términos de la licencia, y seleccionar los componentes a instalar, es posible instalar el cliente y el servidor al mismo tiempo, al continuar el proceso se nos pedirá la ubicación o path donde se instalara el servidor Dude, esto en el caso de instalar Dude en diferentes versiones y sobre diferentes redes.

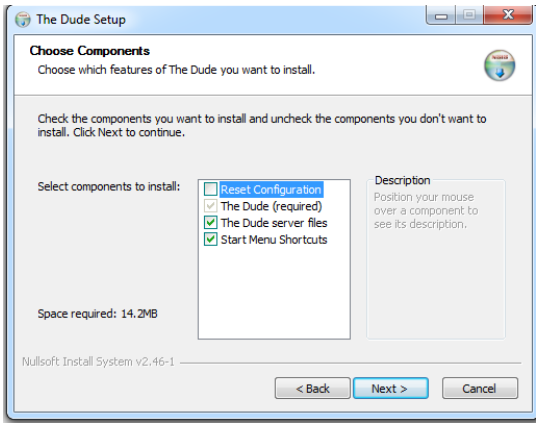


Figura 3.42. Wizard de instalación Cliente Dude en Winbox.

Fuente: Los Autores, Mikrotik Dude, 2013

3.3.2 MODELOS DE TOPOLOGÍAS Y APLICACIONES.

Diversas son las topologías empleadas que se aplican en redes datos para su respectiva monitorización, aunque no existen lineamientos sobre cómo se deben armar estructuras de monitorización puntuales si se puede emitir recomendaciones que ayudaran a mantener no solo un orden sino la colección de estadísticas puntuales usadas posteriormente para la toma de decisiones, para tal identifiquemos las siguientes imágenes y su notable diferencia.

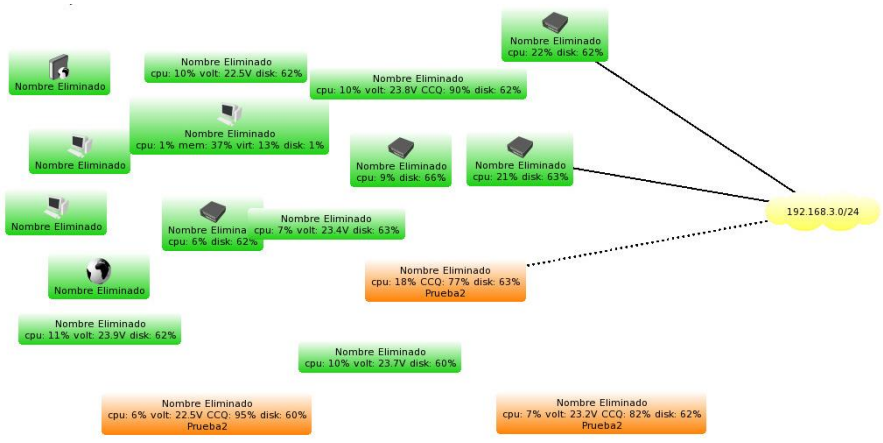


Figura 3.43. Topología Autogenerada en Dude mediante función Descrubrir.

Fuente: Foro Ryohnosuke, Configuración de "The Dude" como network managment system, 2013

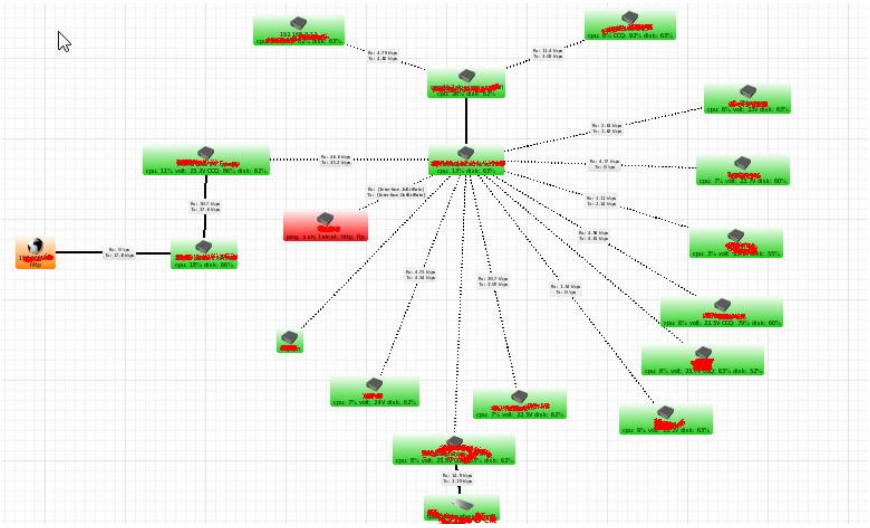


Figura 3.44. Topología Generada Manualmente en Dude.

Fuente: Foro Ryohnosuke, Configuración de "The Dude" como network managment system, 2013

- La función Autodescrubrir si bien elabora una topología de la red rápidamente y sus dispositivos muchas de las veces no genera una estructura optima de la red creando un desorden en sí.
- Al ser una herramienta desarrollado por Mikrotik y gratuita soporta protocolos como SNMP en sus diversas versiones, pero a su vez la integración con equipos RouterOS, dando la opción para monitorizar en tiempo real parámetros de vital importancia como clientes Wireless de un Punto de Acceso etc.
- Elementos para agrupar dispositivos en Dude son de mucha ayuda, ya que evitan tener un caos sobre la topología a monitorizar.
- El uso adecuado de etiquetas nos ayuda a identificar rápidamente el tipo de equipo al que se está monitorizando, de mucha ayuda en topologías grandes.
- Crear el enlace de dos o más dispositivos utilizando el medio adecuado, es decir un medio de radio, fibra, Ethernet etc, para luego obtener estadísticas generadas entre los dispositivos enlazados si bien sea por SNMP o los dispositivos RouterOS.

- Al igual que Winbox Dude para equipos RouterOS es capaz de almacenar Usuarios y Contraseñas con el propósito de autentificar para extraer data de los dispositivos y generar estadísticas o a su vez la ejecución de tareas específicas como Bandwdith Test sin ser necesario el acceso por Winbox.

3.3.3 IMPLEMENTACIÓN DE DUDE EN EL ENTORNO DE LA RED

La implementación de Dude dentro de la nueva Red de la empresa Sigsignet ha sido todo un éxito, no solo por el caso que factores que antes no eran monitorizados como el ancho de banda manejado por enlace sino la disponibilidad de los equipos para ante eventuales problemas pode dar una respuesta rápida por parte del departamento técnico, hoy es posible ya tener incluso un servidor de log completamente centralizado sobre la red, que permitirá al administrador poder tener detalles puntuales sobre la misma, además se manejan alertas sonoras para el personal responsable de la operación, así como notificaciones que van desde él envió de SMS, Mail y ventanas emergentes, todo ello con un esquema ordenado e incluso la generación de alertadas especificas por dispositivo.

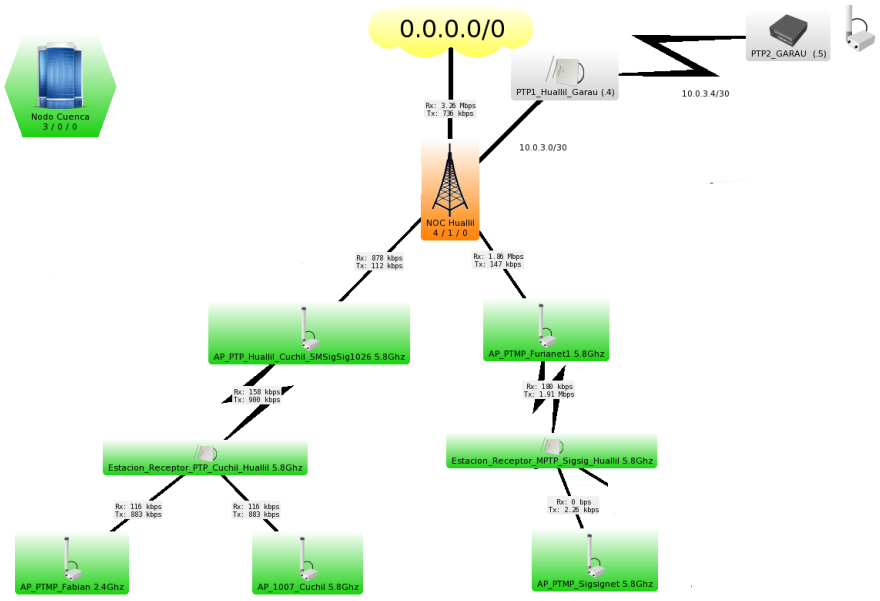


Figura 3.45. Topología de Monitorización empleada en Dude para Sigsignet

Fuente: Los Autores, Mikrotik Dude, 2013

Conclusiones del Capítulo 3

Al terminar este capítulo, parte importante de este procesos de reestructuración que la empresa Sigsignet lleva a cabo, nos ha permitido identificar diversas falencias en la condición actual de la red y a su vez establecer las diversas estrategias correctivas a tomar sobre la nueva infraestructura, la importancia de las pruebas aquí realizadas y sus resultados obtenidos nos han permitido ampliar nuestra perspectiva sobre la estructura de la red actual, y sobre lo que se debería trabajar para mejorar. Es claro que Mikrotik por su relación Beneficio / Costo llegará a ser una solución muy rentable para la empresa, a su vez posibilitando brindar nuevas servicios e incluso elevando el nivel de calidad de servicio actualmente brindado.

CAPÍTULO IV: IMPLEMENTACION DE ROUTEROS Y SOFTWARE OPEN SOURCE COMO SOLUCIÓN DE RED PROPUESTA

Objetivos:

- Implementar las configuraciones necesarias sobre RouterOS y Software Open Source que permitan establecerse como solución de red propuesta.

Objetivos Específicos:

- Establecer todas las configuraciones pertinentes bajo RouterOS que permitan implementar los nuevos servicios y anteriores sobre esta solución utilizando hardware dedicado.
- Conocer la funcionalidad de todas las herramientas disponibles en RouterOS para una administración correcta de la red, y ante eventuales fallas e inconvenientes.
- Comprender los servicios y procedimientos esenciales en RouterOS.
- Implementar CACTI como colector de estadísticas de tráfico y NTOP como monitor de red.

4.1 INTRODUCCION

La implementación de RouterOS como solución propuesta no solo nace por la gran acogida que Mikrotik por medio de RouterOS ha alcanzado, sino en parte por sus grandiosas cualidades, características y directamente relación beneficio/costo que ha permitido que la marca y su sistema operativo en conjunto con su hardware como tal se consoliden y posicionen como una opción altamente eficiente, llegando a ser competencia directa de grandes del mercado con grandes como por mencionar: Cisco, Juniper entre otros.

La solución por factibilidad se presenta como la adecuada para el entonto en el proceso de reingeniería y reacondicionamiento de la red de datos de la empresa Sigsignet, misma que conjuntamente con soluciones Open Source debidamente integradas serán elementos claves para la nueva gestión y administración de la red, y en la mejora y optimización de servicios de red clave que por esta se brindan.

4.2 Configuraciones Básicas en RouterOS.

Asegurar un óptimo funcionamiento de los dispositivos que gestionan y administran una red de datos es una tarea esencial por tal razón hay procedimientos iniciales considerados como elementales que debe ser realizados para asegurar no solo un buen funcionamiento sino una fácil administración y un nivel de seguridad elemental por tal en RouterOS se describen los siguientes procedimientos:

- Asignación de un nombre de identidad al dispositivo de red RouterOS para identificación dentro de la misma y con dispositivos del mismo tipo, para tal dentro de RouterOS abrimos una consola y digitamos lo siguiente:

```
[admin@NODO_HUALLIL] > system identity set name=FirewallSigsignet
```

- En el caso de RouterBoard o Hardware dedicado Mikrotik casi todas sus variantes no disponen de una pila interna por tal necesitamos establecer la hora del sistema utilizando un cliente NTP (Protocolos para sincronización de

relojes por Internet conocido como Network Time Protocol), se debe tener presente que tanto la hora como fecha del sistema son esenciales en tareas de auditoria, registro y análisis de estadísticas de conexión sobre el dispositivo y otros de similar función de ahí su importancia de configuración, para tal lo configuraremos de la siguiente forma abriendo una terminal dentro de RouterOS y escribiendo lo siguiente:

```
[admin@NODO_HUALLIL] > system ntp client set enabled=yes primary-ntp=129.6.15.28 secondary-ntp=129.6.15.29 mode=unicast
```

Donde es necesario definir las IP's o dominios del servidor primario y secundario NTP de su confianza o algunos disponibles en Internet, y en el campo mode establecer el método de difusión de dicho servidor NTP para lo cual disponemos de los siguientes modos de sincronización:

Modo	Descripcion.
Broadcast	En el modo Broadcast el cliente NTP escucha mensajes enviados por servidor NTP , y luego de recibir el mensaje de difusión, primero el cliente sincroniza el reloj local utilizando el modo unicast y luego no envía ningún paquete al servidor NTP.
Manycast	En realidad es similar al modo unicast, pero con una dirección IP desconocida del servidor NTP, por tal el mismo servidor antes de empezar a enviar mensajes de configuración el cliente tiene que descubrir al servidor NTP enviando para tal mensajes multicast, si el servidor se configura para escuchar estos mensajes de manycast antes que nada, luego el mismo responderá, y finalmente el cliente recibirá una respuesta, entrando en modo unicast y sincronizándose con el servidor NTP, luego el cliente en paralelo seguirá buscando más servidores NTP mediante el envío de mensajes de multidifusión de forma periódica.
Multicast	Similar al modo Broadcast solo que en vez de recibir mensajes de Broadcast (IP 255.255.255.255) se reciben mensajes de multicast

	(IP 224.0.1.1)
Unicast	El cliente se conecta al servidor NTP especificado por IP o dominio y envía periódicamente solicitudes comprendidas entre los (64 ... 1024 seg) para sincronizar el reloj.

Tabla 4.1. Modos de Operación Servidor NTP en Mikrotik.

Fuente: Los Autores, Network Time Protocol, 2013

Una vez realizado dicho configuración, ahora es necesario digitar el nombre de la zona horaria y los valores tanto de fecha como de hora se actualizarán automáticamente

```
[admin@NODO_HUALLIL] > system clock set time-zone-name=America/Guayaquil
```

- La protección de los equipos por medio de una credencial de acceso es una tarea muy importante a realizar, en incluso el nivel de privilegios que se le puede autorizar y las diversas formas de acceso a RouterOS en cualquiera de sus modos de trabajo u operación, que van desde armar temas personalizados para administración web con determinadas opciones habilitadas para un usuario en específico por tal a nivel de seguridad en acceso lo primero que tenemos que empezar creando es grupos de usuarios y definiendo las políticas de acceso en el grupo como tal se definen grupos con acceso total para los administradores del sistema de la siguiente forma:

```
[admin@NODO_HUALLIL] > user group add name=administradores policy=api,ftp,local,password,policy,read,reboot,sensitive,sniff,ssh,telnet,test,web,winbox,write
```

Grupo de usuarios destinados al soporte en la red:

```
[admin@NODO_HUALLIL] > user group add name=soporte policy=local,policy,read,reboot,sensitive,sniff,ssh,telnet,test,web,winbox,write
```

Y finalmente terminado creando los usuarios y asignado a los grupos respectivos.

[admin@NODO_HUALLIL] > user add name=administrador password=prueba group=administradores

[admin@NODO_HUALLIL] > user add name=soporte password=prueba_soporte group=soporte

Además es posible incrementar aún más el nivel de seguridad restringiendo el acceso a RouterOS desde determinada dirección IP o direcciones, elevando aún más el nivel de seguridad pero que por cuestiones de funcionalidad optaremos por procedimientos más eficaces como la inclusión de dichas políticas en el firewall, pero que para ejemplo detallamos la configuración:

[admin@NODO_HUALLIL] > user add name=administrador password=prueba group=administradores address=192.168.1.5

- Por defecto RouterOS trae habilitado determinados servicios de red para conexión con el dispositivo corriendo bajo puertos específicos por ende si no se ha establecido un firewall adecuado para solventar ello la mejor forma de prevenir es deshabilitándolos o a su vez realizando el cambio de puerto por defecto, para asegurar un grado más de seguridad sobre el equipo e incluso la serie de ataques, amenazas e intrusiones no deseadas, para tal empezamos listando que servicios están activos y los puertos sobre los cual está operando utilizando el siguiente comando:

admin@NODO_HUALLIL] > ip service print

El mismo listará los siguientes puertos y utilizando un flag “X” que permitirá identificar si dicho puerto se encuentra habilitado o no y lógicamente su dirección de puerto, para este caso práctico habilitaremos determinados servicios y se cambiará la dirección de puerto.

Flag	Nombre	Dirección Puerto
Desactivado (X)	telnet	
Desactivado (X)	ftp	
Activado	www	Por Defecto Puerto 80 Ahora 8082
Activado	ssh	Por Defecto Puerto 22 Ahora Puerto 2223
Desactivado (X)	www-ssl	Por Defecto Puerto 443
Desactivado (X)	api	Por Defecto Puerto 8728 Sera habilitado en condiciones específicas para integración con Sistemas Externos de gestión y administración.
Activado	winbox	Por Defecto Puerto 8291 Ahora Puerto 8292

Tabla 4.2. Servicios Disponibles en RouterOS

Fuente: Los Autores, IP - Services, 2013

El cambiar o alterar los números de puertos no garantiza que el Router esté completamente protegido al contrario es considerada una medida valida pero de mediano impacto ya que cualquier intruso podría escanear los puertos y servicios corriendo en el dispositivo, lo ideal sería combinar dichas medidas con soluciones más eficientes como el uso de un firewall incluso como en el caso del punto anterior "usuarios y grupos", es posible habilitar dichos servicios para ser acezados solo desde un IP o un rango específicos de las mismas, asegurando conexiones confiables, pero que en muchas ocasiones tiende a ser algo tedioso la autorización de IPS en cada servicio se puede tornar confuso, y hasta muchas veces irritante, aunque existe formas de hacer lo mismo y mejor por medio de un firewall, pero es importante comprenderlas en este punto como configuraciones básicas a realizar, por lo tanto la forma en como desactivaremos un puerto será la siguiente:

```
[admin@NODO_HUALLIL] > ip service set disabled=yes  nombre_servicio
```

Y en caso de setear la nueva dirección de un Puerto solo bastara con ejecutar el siguiente comando:

```
[admin@NODO_HUALLIL] > ip service set port=XXXX nombre_servicio
```

Donde nombre de servicio representa los servicios disponibles para acceso al Router definidos en la tabla anterior y XXXX el nuevo número de puerto a definir.

4.3 Implementaciones RouterOS aplicadas a un WISP.

RouterOS como tal puede tener muchas aplicaciones como servidor de red, y en si múltiples configuraciones disponibles y modos de trabajo, hay quienes piensan que por las grandes bondades que RouterOS brinda en un mismo entorno, se tiene la idea equivocada de que un equipo con buenas características puede realizar casi todo, con ello se hace referencia a que se cree que serán capaces de levantar un firewall, enrutamiento, calidad de servicio, QoS, WebProxy, Servidor VPN o algún método de tunneling, DHCP Server entre otros, y no por el hecho que no sea posible al contrario es completamente realizable, pero para nuestra situación y lo que abarca este tema de estudio está claro que un proveedor de acceso a Internet donde prácticamente la calidad de servicio y el funcionamiento ininterrumpido tiene que estar asegurado, es ahí donde temáticas como la alta disponibilidad, redundancia y afines, entran a la partida y por lo tanto dicha recomendación pueda a futuro evitar grandes dolores de cabeza.

4.3.1 Marcado de conexiones.

Es proceso de marcado de conexiones o mejor conocido como “Mangle” en RouterOs consiste en aplicar una determinada “marca” a los paquetes con el fin de posteriormente dar un determinado tratamiento interno a dicha marca, dentro de los diversos estados y módulos que un paquete puede atravesar a lo largo de su travesía por el Router o dispositivo de red Mikrotik, donde más tarde dichas marcas serán de

utilidad en procedimientos tanto de ruteo, calidad de servicio, distribución de ancho de banda etc., además el mangle tiene capacidades especiales como la posibilidad de modificar ciertos campos en el encabezado del paquete IP como por ejemplo TOS (ó DSCP), y TTL, y una configuración adecuada del mismo en un entorno como un WISP asegura en sus etapas posteriores un 50% de una buena calidad de servicio, por tal es necesario empezar a comprender más a detalle su funcionamiento utilizando el siguiente diagrama.

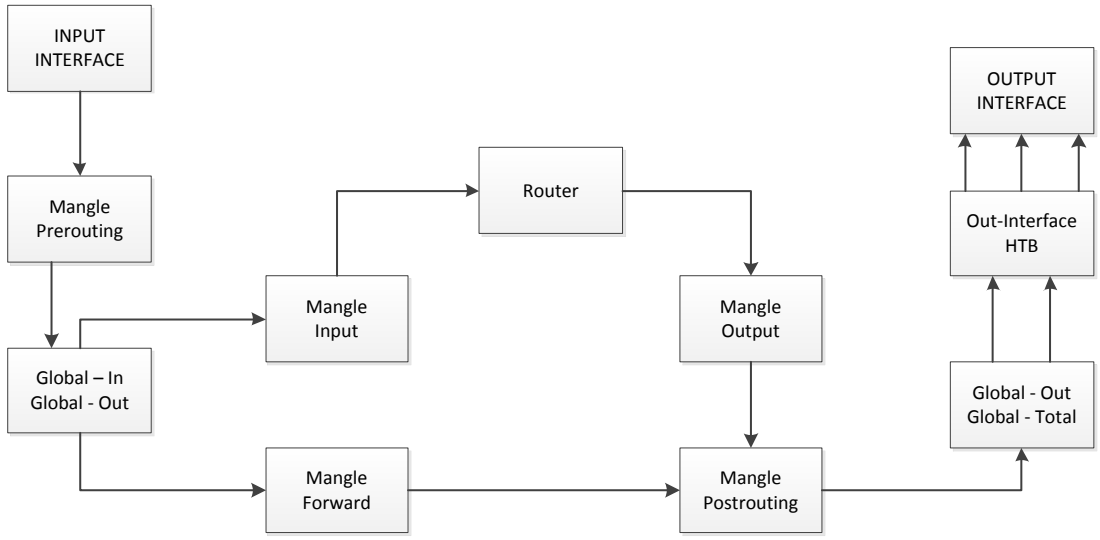


Figura 4.1. Diagrama simplificado Estructura del Mangle RouterOS Ver. 5.X

Fuente: Los Autores, Pack Flow Mangle, 2013

Todas las reglas de mangle se organizan en cadenas, por lo tanto se definen 5 cadenas por defecto:

- Prerouting: Marca todo lo que ingresa al Router.
- Postrouting: Marca todo lo que sale del Router.
- Input: Marca todo lo que tiene como destino el Router.
- Forward: Marca todo lo que atraviesa el Router
- Output: Marca todo lo que origina el Router.

Es importante recalcar que desde la versión 6.X en estado beta de RouterOS la estructura en el diagrama simplificado ha sufrido un cambio importante, la misma no

ha sido considera en este tema de estudio para el desarrollo de este proyecto por su estado de desarrollo pero que promete muchas mejoras importantes.

En el proceso de marcado de conexiones también se pueden definir algunas acciones realizadas sobre esta como son:

- Mark-Connection: Marca solo el primer paquete.
- Mark-Packet: Marca paquetes para políticas de QoS.
- Mark-Routing: Marca paquetes para políticas de ruteo.
- Change MSS: Cambia el tamaño máximo del segmento (similar al MTU)
- Change DSCP (ToS): Cambia el tipo de servicio.
- Change TTL: Cambia el tiempo de vida.

Siendo importante acuñar una regla o norma esencial dentro del Mangle en que primero se marca un paquete y luego un flujo asociado a dicha paquete, además dichas marcas de conexión permiten identificar una o un grupo de conexiones asociadas a una marca específica, dichas marcas son almacenadas en una tabla denominada “connection tracking”, siendo posible establecer solo una marca de conexión para cada conexión.

También es importante conocer que el mangle dispone de una vista avanzada donde podemos realizar procedimiento de marcado de conexión en capa 7 de acuerdo al modelo OSI, o utilizando listas IP en el caso de segmentación de ancho de banda, o en la vista extra marcado por horas o tiempo específico pudiendo activar determinadas marcas en cierto horario, o incluso el uso listas IP, que en este caso no serán de utilidad para el marcado de conexión de abonados y su posterior segmentación, es importante también mencionar que muchas marcas de conexión no requieren la primera marca establecida que corresponde a marca de paquete sino directamente al flujo, esto debido al tipo de protocolo que se está gestionando en la conexión como por ejemplo el caso de ICMP es necesario solo detallar la marca de flujo mas no la del paquete.

Para el ejemplo de una marca utilizando listas IP para este caso dicha lista lleva el nombre de Smart Home, que se relaciona con el nombre de uno de los planes empleados en la empresa Sigsignet, además dicho procesamiento se lo realizara al prerouting, es decir al momento que la conexión ingresa al Router y la marca del paquete llevara como nombre Smart_HomeF, es importante mencionar que el passtroung en esta primera etapa de marcado deberá estar habilitado y cuando se marque el flujo de dicha regla se lo desactive con el fin de que las conexión gestionados en esa regla coincidan y no detenga el procesamiento de otras reglas subsiguientes.

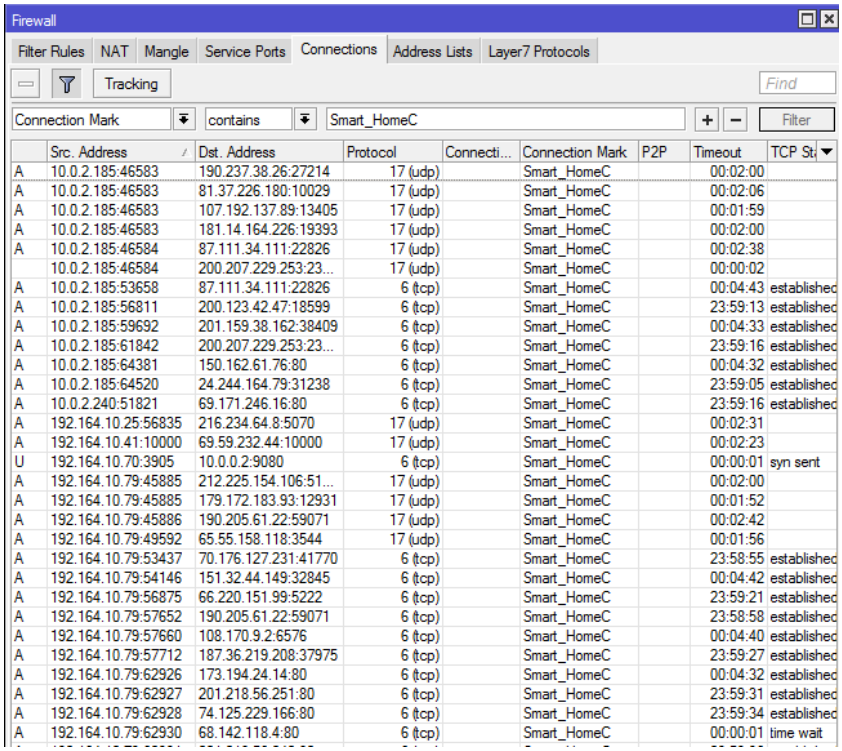
```
[admin@NODO_HUALLIL] > ip firewall mangle add chain=prerouting src-address-list="Smart Home" passthrough=yes comment=Plan Residencial Smart Home action=mark-connection new-connection-mark=Smart_HomeC

[admin@NODO_HUALLIL] > ip firewall mangle add chain=prerouting connection-mark=Smart_HomeC action=mark-packet new-packet-mark=Smart_HomeF passthrough=no
```

Para que dichas reglas hagan efecto necesitamos definir un cliente que tenga conexión a través del servidor Mikrotik y haber agregado su IP a una lista IP como por ejemplo de la siguiente forma:

```
[admin@NODO_HUALLIL] > ip firewall address-list add address=10.0.2.185 list="Smart Home" comment=Usuario_UPS
```

Apenas se empieza a navegar desde el cliente con la IP de ejemplo antes listado se podrá dirigir al Connection Tracking desde Winbox y divisar que el campo Connection Mark ha empezado a ser marcado, método que nos indica que el procedimiento de marcado está realizándose con éxito, el módulo connection tracking es considerado como el firewall, ya que es el encargado de recopilar y manejar todas las conexiones, representado cada entrada un intercambio bidireccional de datos, al deshabilitar connection tracking desde el botón Tracking el

sistema pierde la capacidad de hacer NAT, como así gran parte de las condiciones de filtrado y marcado.



	Src. Address	Dst. Address	Protocol	Connecti...	Connection Mark	P2P	Timeout	TCP St
A	10.0.2.185:46583	190.237.38.26:27214	17 (udp)		Smart_HomeC		00:02:00	
A	10.0.2.185:46583	81.37.226.180:10029	17 (udp)		Smart_HomeC		00:02:06	
A	10.0.2.185:46583	107.192.137.89:13405	17 (udp)		Smart_HomeC		00:01:59	
A	10.0.2.185:46583	181.14.164.226:19393	17 (udp)		Smart_HomeC		00:02:00	
A	10.0.2.185:46584	87.111.34.111:22826	17 (udp)		Smart_HomeC		00:02:38	
	10.0.2.185:46584	200.207.229.253:23...	17 (udp)		Smart_HomeC		00:00:02	
A	10.0.2.185:53658	87.111.34.111:22826	6 (tcp)		Smart_HomeC		00:04:43	established
A	10.0.2.185:56811	200.123.42.47:18599	6 (tcp)		Smart_HomeC		23:59:13	established
A	10.0.2.185:59692	201.159.38.162:38409	6 (tcp)		Smart_HomeC		00:04:33	established
A	10.0.2.185:61842	200.207.229.253:23...	6 (tcp)		Smart_HomeC		23:59:16	established
A	10.0.2.185:64381	150.162.61.76:80	6 (tcp)		Smart_HomeC		00:04:32	established
A	10.0.2.185:64520	24.244.164.79:31238	6 (tcp)		Smart_HomeC		23:59:05	established
A	10.0.2.240:51821	69.171.246.16:80	6 (tcp)		Smart_HomeC		23:59:16	established
A	192.164.10.25:56835	216.234.64.8:5070	17 (udp)		Smart_HomeC		00:02:31	
A	192.164.10.41:10000	69.59.232.44:10000	17 (udp)		Smart_HomeC		00:02:23	
U	192.164.10.70:3905	10.0.0.2:9080	6 (tcp)		Smart_HomeC		00:00:01	syn sent
A	192.164.10.79:45885	212.225.154.106:51...	17 (udp)		Smart_HomeC		00:02:00	
A	192.164.10.79:45885	179.172.183.93:12931	17 (udp)		Smart_HomeC		00:01:52	
A	192.164.10.79:45886	190.205.61.22:59071	17 (udp)		Smart_HomeC		00:02:42	
A	192.164.10.79:49592	65.55.158.118:3544	17 (udp)		Smart_HomeC		00:01:56	
A	192.164.10.79:53437	70.176.127.231:41770	6 (tcp)		Smart_HomeC		23:58:55	established
A	192.164.10.79:54146	151.32.44.149:32845	6 (tcp)		Smart_HomeC		00:04:42	established
A	192.164.10.79:56875	66.220.151.99:5222	6 (tcp)		Smart_HomeC		23:59:21	established
A	192.164.10.79:57652	190.205.61.22:59071	6 (tcp)		Smart_HomeC		23:58:58	established
A	192.164.10.79:57660	108.170.9.2:6576	6 (tcp)		Smart_HomeC		00:04:40	established
A	192.164.10.79:57712	187.36.219.208:37975	6 (tcp)		Smart_HomeC		23:59:27	established
A	192.164.10.79:62926	173.194.24.14:80	6 (tcp)		Smart_HomeC		00:04:32	established
A	192.164.10.79:62927	201.218.56.251:80	6 (tcp)		Smart_HomeC		23:59:31	established
A	192.164.10.79:62928	74.125.229.166:80	6 (tcp)		Smart_HomeC		23:59:34	established
A	192.164.10.79:62930	68.142.118.4:80	6 (tcp)		Smart_HomeC		00:00:01	time wait

Figura. 4.2. Connection Tracking en Winbox con marcado de paquete.

Fuente: Los Autores, Winbox Mikrotik, 2013

En el caso de que queramos ir agregando más usuarios y que las marcas sigan funcionando de igual forma, bastara con agregar en la lista las IP's.

4.3.2 Firewall Capa 3 y capa 7.

RouterOS desde su versión inicial incorpora un servidor de seguridad operable tanto en capa 3 como en capa 7 según OSI, con todas las funciones de su clase, que van desde autorizar trafico bajo ciertas condiciones o denegar y filtrar diferentes tipos de tráfico entre redes, basando ello en un conjunto de reglas o políticas, o incluso evitar el acceso no autorizado al Router o la protección de determinadas redes o equipos

que requieren medidas de seguridad de estado crítico, toda la estructura de reglas son definidas por el usuario y que trabajan bajo el principio condicional:.

SI COINCIDE >>>> ENTONCES

Siendo el orden de las mismas muy importante ya que su procesamiento es secuencial, además dichas reglas son ordenadas en cadenas, pudiendo existir cadenas predefinidas y las creadas por el usuario, entre las cadenas por defecto tenemos las siguientes:

CADENA INPUT: Procesa paquetes que tienen como destino final el Router, dicha cadena contiene las reglas de filtrado que protegen al Router mismo.

CADENA OUTPUT: Procesa paquetes enviados por el Router, en si esta cadena contiene las reglas de filtrado que salen del Router.

CADENA FORWARD: Procesa paquetes que atraviesan el Router.

CADENA PREDEFINIDAS: El hecho de que se listen las 3 cadenas por defecto no significa que no se puedan añadir más, es posible crear cadenas con cualquier nombre que se desee, basta con cambiar el nombre por el nombre de la cadena por defecto (INPUT, OUTPUT, FORWARD), pero para que dicha cadena sea procesada es necesario acompañar a la regla de un salto o jump hacia dicha cadena.

SALTO DE CADENAS: Es utilizado para saltos a cadenas creadas por el usuario, esto con el fin de mantener un orden en las reglas de firewall, generalmente tiende a ubicarse debajo de las cadenas predefinidas.

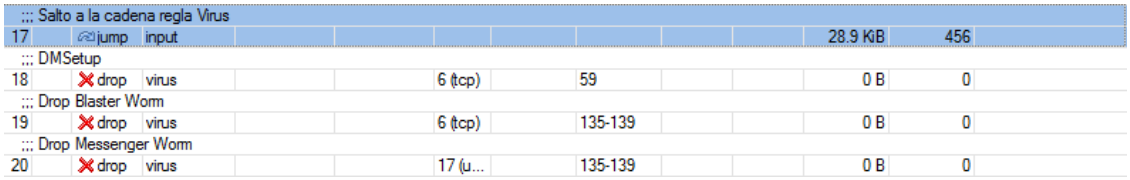


Fig. 4.3. Regla de Salto (Jump) a una cadena predefinida (virus).

Fuente: Los Autores, Winbox Mikrotik, 2013

El diseño posterior del Firewall aplicable en un ISP las cadenas INPUT nos servirá para proteger el servidor y las FORWARD para la protección de los abonados o clientes.

Para tal es necesario entender el siguiente diagrama simplificado de Firewall en RouterOS.

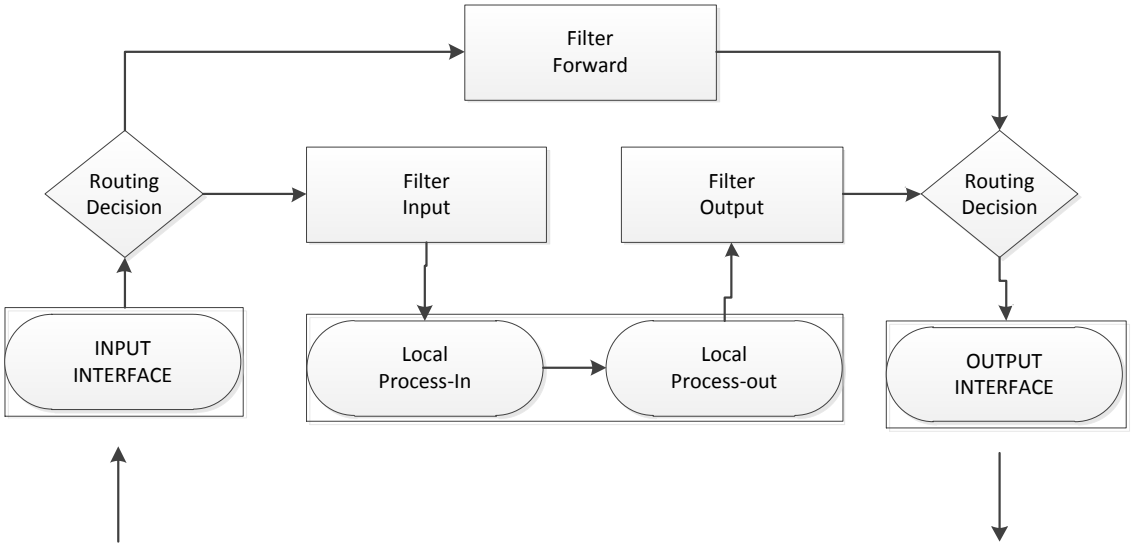


Figura 4.4. Diagrama simplificado de Firewall RouterOS.

Fuente: Los Autores, Firewall RouterOS, 2013.

Siempre durante el proceso de construcción de reglas de firewall deberemos considerar el diagrama simplificado de firewall para una estructuración de reglas adecuada en base a un flujo utilizado, además se debe considerar que tácticas o políticas se deben emplear en la administración de un Firewall como son:

- Política de Bloquear lo conocido.- El mismo específico que todo está bloqueado por defecto, y solo es habilitado el tráfico conocido para su paso por el firewall.
- Política de Aceptar lo conocido.-Comprende en acepar el tráfico conocido que entra y sale por el firewall y el resto se bloquea.

La primera política se la podría considerar como la técnica o táctica más segura a emplearse en la creación de un Firewall, pero como se ha mencionado su uso es

dependiente del caso en que lo vayamos a implementar, definiendo como la táctica más valida sería la primera específicamente, aunque ello implique un elevado conocimiento como base, ya que la interacción con los protocolos, puertos se vuelve más complicada y algunas veces difícil de gestionar, por tal un administrador de red debe pensar dos veces en emplear dicha táctica porque en el caso de no dominar o tener un conocimiento base la misma nos creara más conflictos que beneficios.

En cuanto al filtrado en capa 7 es similar al proceso de filtrado ya visto, con la diferencia que el trafico gestionado ya no es IP, es decir que haga uso de un determinado protocolo, puerto y dirección IP sino más bien este esté orientado a capa 7 según el modelo OSI utilizando puertos comunes para el envió de información maliciosa o netamente el poder restringir aplicaciones como el tan molesto P2P operando sobre dicha capa, incluso muchos problemas a nivel de seguridad se origina por dicha capa siendo casi imposible detectarlos en capa 3, por tal razón Mikrotik dispone en RouterOS la posibilidad de trabajar con Firewall utilizando capa 7, tal proceso tiene un coste para el Hardware el procesamiento de reglas por capa 7 implica el uso de más recursos de procesamiento ya que en capa 4 de un paquete procesado se tiene a buscar en los primeros 40 bits o los datos del encabezado TCP haciendo que el procesamiento en dicha capa sea extremadamente rápido no en tanto en capa 7 se tiene a buscar en el paquete entero por lo tanto la cantidad de datos a procesar va desde 20 bytes a 1500 bytes, por ejemplo el trafico bittorrent en capa 7 seria identificado de la siguiente manera:

```
^(bittorrent protocol|azver$|get/scrape\?info_hash=)|d1:ad2:id20:|'7P\)[RP]
```

Por lo tanto ahora es necesario definir las sentencias y comandos para crear reglas básicas de firewall en RouterOS, es importante mencionar que tres reglas consideradas como reglas de oro deben ser creadas en toda implementación de Firewall o netamente en cualquier dispositivo RouterOS de acuerdo al estado de

conexiones que se pueden manejar, es decir pudiente tener conexión de tipo: Invalidas, nuevas, establecidas y relacionadas, indicándole al firewall procesar solo paquetes nuevos y evitar de cierta forma el tráfico no deseado y en si evitando el consumo excesivo de recursos como CPU y RAM, para tal establecemos las siguientes configuraciones:

- Reglas de Oro Básicas para procesar solo tráfico nuevo y no invalido.

```
[admin@NODO_HUALLIL] > ip firewall filter add chain=forward action=accept connection-state=established
```

```
[admin@NODO_HUALLIL] > ip firewall filter add chain=forward action=accept connection-state=related
```

```
[admin@NODO_HUALLIL] > ip firewall filter add chain=forward action=drop connection-state=invalid
```

El operador Drop se orienta dentro de RouterOS como la acción para borrar o eliminar determinado tráfico, dichos comandos se especificaran más a detalle en el capitulo 5.

Además entre las operaciones elementales del Firewall debe estar presentes opciones para:

- Prevención de Spam: Como tal el spam es un método de envío masivo de correos basura o no solicitados cuyo remitente es desconocido, siendo un gran problema en los proveedores de acceso a Internet, volviéndose muchas de las veces una tarea completamente difícil su mitigación ya que se tiene a encubrir algunas veces con usuarios que está recibiendo y enviando correos válidos, generalmente una opción válida es el control de spam definiendo un número de conexiones establecidas por medio del puerto 25 que utiliza el protocolo TCP, para tal antes que definir un número de conexiones es necesario poner una analogía, en que un usuario residencial nunca generan más de cinco conexiones TCP en el puerto 25 hacia afuera dicho esto si se

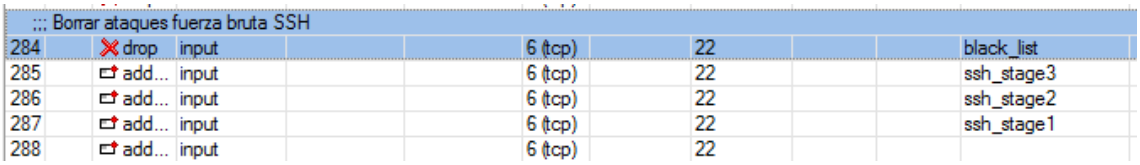
habla de un entorno corporativo pues bueno solo será cuestión de empezar a multiplicar, en muchas ocasiones esta es un tarea de suma importancia ya que existen usuarios a los cuales ni cuenta se dieron pero de pronto un gusano o alguna variedad de virus ingreso en su computador sin autorización alguna y empezó a enviar spam, por tal definimos la siguiente configuración como medida para mitigar la misma, está por demás mencionar que la estructura de regla puede ser reacondicionada o mejorada según se crean conveniente mas no representa un proceso puntual o norma contra la mitigación de spam.

[admin@NODO_HUALLIL] > ip firewall filter add chain=forward action=add-src-to-address-list protocol=tcp address-list=Sobre_5_Conexiones_SMTP address-list-timeout=2h dst-port=25 connection-limit=5,32 comment=Proteccion_Spam

admin@NODO_HUALLIL] > ip firewall filter add chain=forward action=drop address-list=Sobre_5_Conexiones_SMTP

- Otra norma esencial que debe cubrir un firewall es la protección ante los ataques de fuerza bruta, generalmente sobre puertos necesarios para la administración del Router donde se tiene a probar mediante un diccionario que contiene una base de datos de usuarios y passwords e intentar acertar las credenciales de acceso a un dispositivo de red, generalmente dichos ataques se realizan a través del puerto SSH, telnet o FTP, existen muchos procedimientos para mitigar esto como tal es el caso en los puntos anteriores la posibilidad de agregar direcciones IP para acceder a dichos servicios en específico pero la mejor opción se orienta desde el Firewall, por ejemplo para el caso creando un regla de conexión nueva hacia uno de estos puertos y separándoles por etapas o fases, donde en una primera etapa estarán los usuarios reales, pero si el mismo intenta acceder varias veces erróneamente pasara a listarse en una etapa 2 por un lapso de tiempo de 5 a 6 minutos no podrá establecer conexión con el Router, si los intentos siguen desmedidamente y dejo de considerarse un usuario real sino un atacante

pasara a su vez a una nueva lista en la fase 3 donde prácticamente todo el tráfico hacia el Router proveniente de dicha IP será eliminado, impidiendo de por si nuevamente generar conexión al Router por Días.



;;; Borrar ataques fuerza bruta SSH								
284		drop	input		6 (tcp)	22		black_list
285		add...	input		6 (tcp)	22		ssh_stage3
286		add...	input		6 (tcp)	22		ssh_stage2
287		add...	input		6 (tcp)	22		ssh_stage1
288		add...	input		6 (tcp)	22		

Figura 4.5. Reglas de contramedida para protección contra ataque fuerza bruta por SSH.

Fuente: Los Autores, Winbox Mikrotik, 2013

- Ataques DOS/POD, son dos tipos de ataques comúnmente vistos, DOS o ataque de denegación de servicios, el mismo actúa enviando miles de peticiones TCP SYN, a una dirección IP única, pudiendo representar esta un servidor web, servicio de red o algún protocolo orientado a conexión que funcione sobre dicho servicio de red, haciendo que el servidor de red o similar se sobrecargue con solicitudes SYN, evitando que el mismo funcione adecuadamente, para tal dicho problema puede ser mitigado en primer lugar identificando el tipo de conexiones TCP y utilizando una bandera SYN en el estado de nueva conexión, permitiendo identificar todas estas conexiones que están intentando abrirse, y luego especificando un límite en el número de paquetes por segundo que deseamos permitir, especificando un rango entre 300-400 paquetes por segundo como máximo, y cualquiera que exceda este límite sea asignado a una lista de direcciones IP para su posterior bloqueo de conexión, el segundo ataque más relevante a ser considerado en una configuración de firewall adecuada es conocido como POD o ping de la muerte, utiliza un gran número de ordenadores a nivel mundial con el fin de enviar paquetes ICMP extremadamente grandes con el fin de colapsar sistemas o servidores, por tal una medida a considerar para controlar este problema puede establecerse entre limitar el tamaño de paquetes ICMP o ping o bien bloquearlos completamente.

Adicional un parámetro muy poco difundido en RouterOS es el uso del modo seguro durante el proceso de creación de cadenas y reglas en firewall, ya que muchas veces suele suceder que durante el proceso de creación de reglas sobre dispositivos remotos y la poca experiencia se tiende a perder acceso con los dispositivos remotos ante tal Mikrotik ha implementado un modo denominada seguro, que consiste en el caso de perder conexión con la última regla creada la elimina y la vuelve a un estado anterior permitiendo retomar conexión y alterar la regla errónea para tal se tiene dos formas de activar desde Winbox.

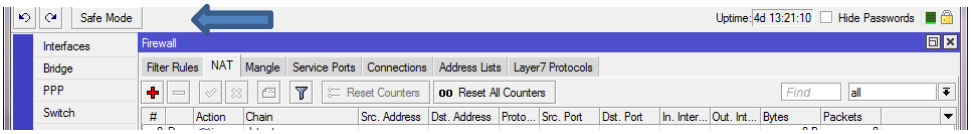


Figura 4.6. Activación Safe Mode RouterOS desde Winbox.

Fuente: Los Autores, Winbox Mikrotik, 2013

O Ingresando en la consola y presionado tan solo Ctrl + x para activar dicho modo.

4.3.3 Cadenas de NAT.

NAT es un protocolo de traducción de red, creado para el intercambio de paquetes entre dos redes que asignan mutuamente direcciones incompatibles[30], al igual que el Firewall, las reglas de NAT trabajan con el principio condicional

SI COINCIDE >>>> ENTONCES

Siendo procesadas de igual forma que el firewall es decir en forma secuencial, para tal como ya se ha mencionado NAT es un protocolo de traducción de IPs públicas a privadas y viceversa que dentro de RouterOS dicha función solo esta útil con el módulo de connection tracking activado y además mantienen dos tipos de cadenas que son:

[30] Mikrotik, (n.d.). Network Address Translation, http://es.wikipedia.org/wiki/Network_Address_Translation

- Dstnat.-Es una cadena NAT que traduce una dirección Publica en una dirección privada, cambiando el destino de un paquete ip o puerto, usado generalmente para la redirección de tráfico desde Internet a un servidor en nuestra red Interna, aquí se aplica un tipo de DST-Nat denominado redirect que permite actuar como proxy de servicios DNS, HTTP; Redireccionando los paquetes al Router (Se sobrescribe la dirección IP y/o puerto de origen)

Figura 4.7. Topología SRC-Nat RouterOS

Fuente: Los Autores, Topología SRC-Nat, 2013

- Srcnat.- Es una cadena de NAT que traduce una dirección IP origen y su puerto a una dirección pública y su puerto respectivamente, permitiendo a un IP privada aparecer como una IP pública, permitiendo tener acceso público a una red privada, para ello empleando un tipo de src-nat denominado masquerade o enmascaramiento cuyo fin es cambiar el origen de los puertos (Se sobrescribe la dirección IP y/o puerto de Destino)

Figura 4.8. Topología DST-Nat RouterOS

Fuente: Los Autores, Topología DST-Nat, 2013

RouterOS ofrece una completa suite de funciones relacionadas a NAT, no en tanto otras soluciones ofrecen la función de NAT pero limitada exclusivamente a la traducción de IP y puertos nada más, por tal razón para comprender su

funcionamiento es necesario entender el siguiente diagrama simplificado de su funcionamiento.

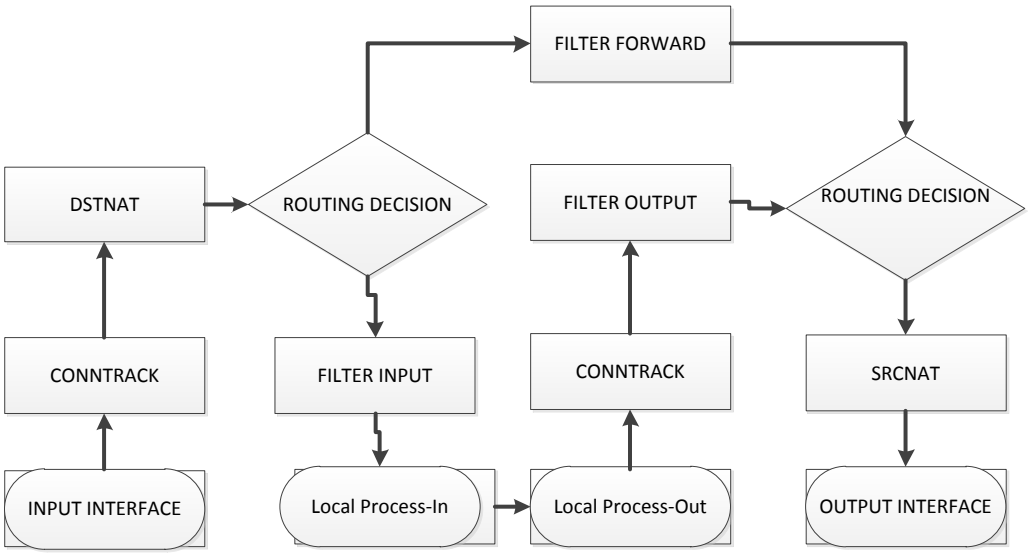


Figura 4.9. Diagrama simplificado NAT en RouterOS

Fuente: Los Autores, NAT RouterOS, 2013.

Además un función esencial de NAT se lo conoce como NAT 1-1, empleada muy comúnmente por ISP a quienes les proveen un pool de IP´s públicas no enrutadas para su respectiva utilización, permitiendo la asignación de una IP pública a través de una privada, teniendo que definir 2 reglas puntuales y la de enmascaramiento para todos los abonados para ello que son:

- Src-Nat para el cliente.
- Dst-Nat particular para la IP pública.

Entre las limitaciones de NAT se establecen que algunos protocolos necesitan la ayuda de NAT-Helpers o Nat-Transversal para poder trabajar adecuadamente estando establecidos por defecto en RouterOS siendo posible solo desactivarlos mas no crearlos o eliminarlos, además la problemática de que algunos servicios TCP trabajaran en modo pasivo, e incluso del lado del cliente la posibilidad de no disponer de una verdadera comunicación punto a punto no pudiendo iniciar conexiones remotas o externas.

Por lo tanto las configuraciones esenciales dentro de RouterOS son las que se detallan a continuación:

Para Src-Nat asumiendo que se pretende dar salida a un grupo de abonados con un rango de direcciones IP determinado para el caso 10.0.10.128/25 y que el Router disponga de una interfaz cuya boca recibe la conexión a Internet con nombre ether1_wan la regla se especifica de la siguiente forma:

```
[admin@NODO_HUALLIL] > ip firewall nat add chain=srcnat src-address=10.0.10.128/25 out-interface=ether1_wan action=masquerade
```

En el caso de un Dst-Nat en el cual se quiera por medio de una IP pública publicar un servidor web que tiene un servicio web ejecutándose por el puerto 80 en la red interna con una IP privada asumiendo que la misma para el ejemplo es la 192.168.50.200/24 se lo realizará de la siguiente forma:

```
[admin@NODO_HUALLIL] > ip firewall nat add chain=dstnat dst-address=186.5.103.2 protocol=tcp dst-port=80 action=dst-nat to-addresses=192.168.50.200 to-ports=80
```

Para el caso del NAT 1:1, donde se asignará una dirección pública única a una IP privada única para tal se describe el siguiente proceso:

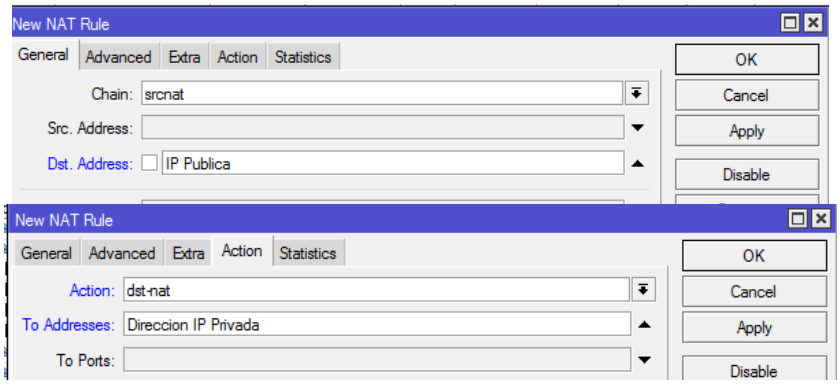


Figura 4.10. Dst-Nat particular para la IP pública.

Fuente: Los Autores, Winbox Dst-Nat, 2013

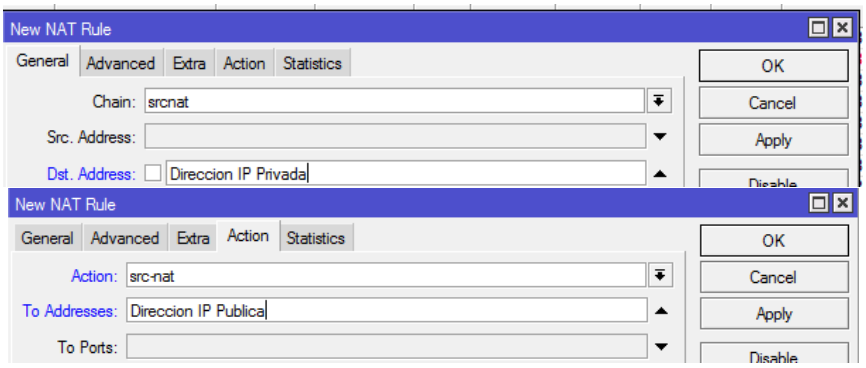


Figura 4.11. Src-Nat para el cliente.

Fuente: Los Autores, Winbox Dst-Nat, 2013

4.3.4 Servidor DHCP y configuraciones esenciales.

Es un protocolo de configuración de host dinámico ampliamente usados del lado de los proveedores de acceso a Internet se basa en el RFC 2131 y usa UDP en los puertos 67 del lado del servidor y 68 del lado del cliente como protocolo de transporte y lógicamente operar tanto en modo cliente como servidor, del lado del servidor se encarga de enviar parámetros de configuración de IP, Defaul Gateway, DNS, NTP Server y más de 100 otras opciones personalizadas, a los clientes que a su vez se encargan de recibir los mismos para entablar comunicación con el servidor y diversos protocolos de red. RouterOS así también tiene la capacidad de convertirse en un Servidor DHCP, pudiendo tener múltiples servidores DHCP en distintas interfaces conforme el mismo equipo las tenga, con restricciones como es el caso que solo se puede tener un servidor DHCP en una interfaz, o el hecho de no ser posible levantar un servidor DHCP en una interfaz que es parte de un bridge lógico en RouterOS, y su implementación debe realizarse sobre redes que se consideren confiables debido a su poco grado de seguridad; Dado el desarrollo de Winbox cuyo objetivo es facilitar las tareas de administración en la red, se cuenta con un asistente o wizard que puede ayudar a levantar un servidor DHCP en apenas unos pocos minutos, se debe tener en cuenta que existen muchos parámetros a considerar cuando se levanta un DHCP tales como a nivel de seguridad la problemática de poder encontrar DHCP Rogue o clones que puedan hacerse pasar por el real y empezar a

delinquir sobre la Red o a su vez la entrega de IP a personas no autorizadas para dicho capitulo contemplara algunas medidas para mitigar dichos problemas.

Para crear un DHCP en RouterOS, ejecutar Winbox y dirigirse a IP >> DHCP Server y dar clic, para posterior visualizar el asistente de configuración, donde se realiza los siguientes procedimientos:

1.-Definir la interfaz por donde se va a ejecutar el servidor DHCP, antes que nada habiendo registrado la IP de la interfaz sobre la cual se levantará el servidor DHCP.

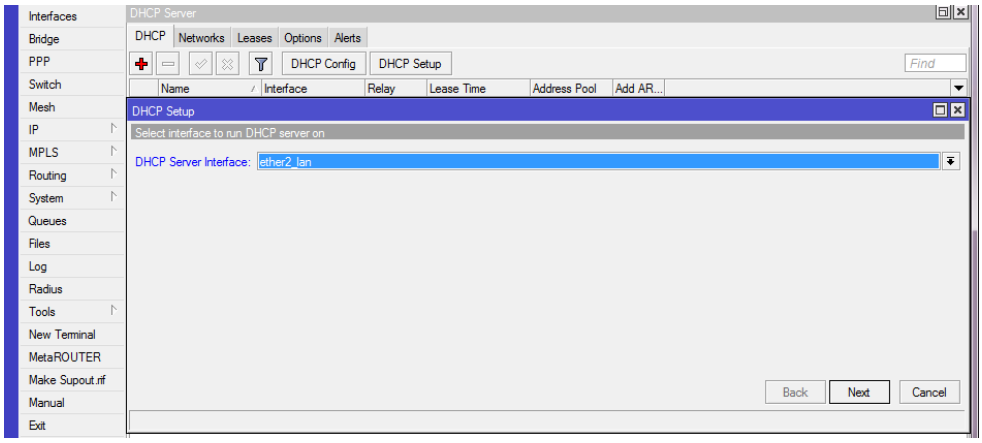


Figura 4.12. Ventana de Asistente o Wizard de Creación de un Servidor DHCP

Fuente: Los Autores, Winbox Wizard creación servidor DHCP, 2013

2.-Determinar la red de trabajo sobre la que operará el servidor DHCP, generalmente el Wizard detecta la IP sobre la interfaz y automáticamente especifica la dirección de red de trabajo del DHCP Server.

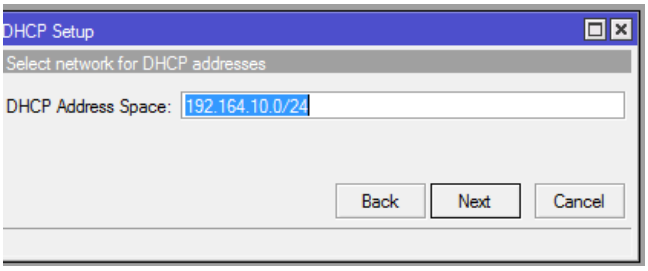


Figura 4.13. Wizard de Creación de un Servidor DHCP – Direccionamiento.

Fuente: Los Autores, Winbox Wizard creación servidor DHCP, 2013

3.-El siguiente punto es la especificación del Gateway sobre el cual DHCP brindará conectividad.

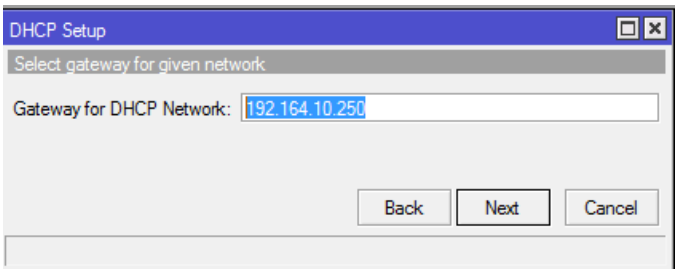


Figura 4.14. Ventana de Asistente o Wizard DHCP – Especificación de Gateway.

Fuente: Los Autores, Winbox Wizard creación servidor DHCP, 2013

4.-Luego determinar el o los Pool validos de IP's a ser consumidos por el Servidor DHCP pudiendo especificar los que se crea convenientes.

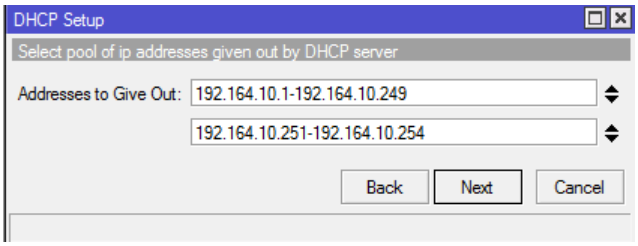


Figura 4.15. Ventana de Asistente o Wizard DHCP – Especificación de Pool IP.

Fuente: Los Autores, Winbox Wizard creación servidor DHCP, 2013

5.-Es necesario también establecer los Servidores de Nombres de Dominios validos que permitirán entablar conectividad y la resolución de nombres de Dominio.

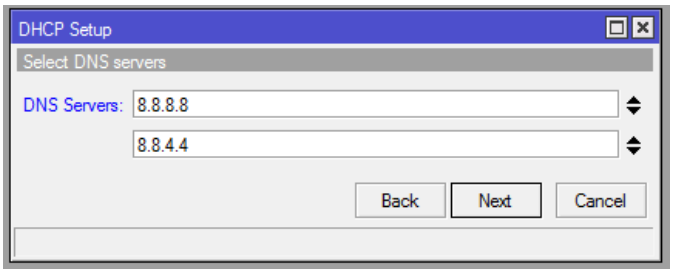


Figura 4.16. Ventana de Asistente o Wizard DHCP – Determinacion servidores DNS.

Fuente: Los Autores, Winbox Wizard creación servidor DHCP, 2013

6.-Sin olvidar el Lease Time o tiempo establecido para renovar la concesión de una IP, cuyo formato se establece en Días: Horas: Minutos: Segundos

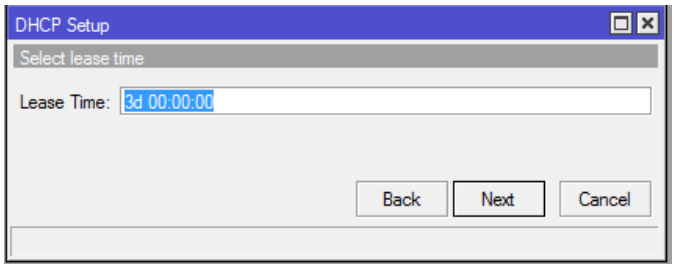


Figura 4.17. Ventana de Asistente o Wizard DHCP – Asignación Lease Time DHCP.

Fuente: Los Autores, Winbox Wizard creación servidor DHCP, 2013

Generalmente el Wizard se recomienda para configuraciones de usuarios con poca experiencia ya que durante el proceso se omiten muchos parámetros de importancia pero que como tal es una opción válida para levantar un DHCP server en su mínima expresión por tal se puede configurar el mismo siguiendo el procedimiento anterior y luego realizar los ajustes requeridos, basta con dar doble clic sobre el servidor configurado.

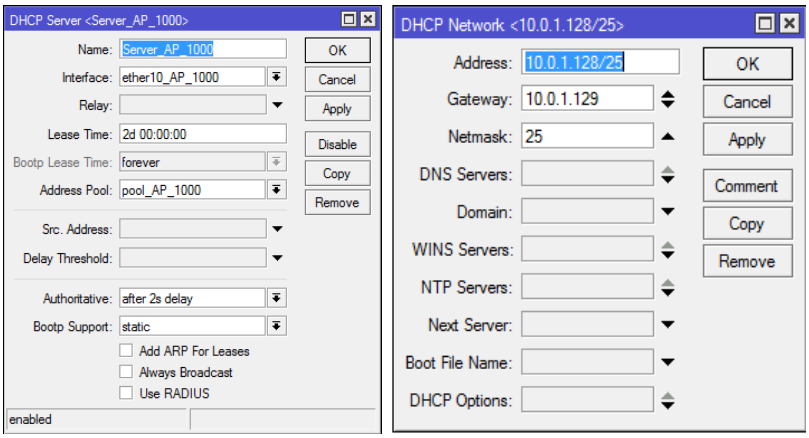


Figura 4.18. Parámetros de configuración DHCP en RouterOS.

Fuente: Los Autores, Parámetros de Configuración DHCP, 2013

Así también es posible la asignación de entradas estáticas con el fin de entregar a determinado host parámetros específicos como la misma IP, basta con dirigirse desde Winbox a:

IP >> DHCP Server >> Leases y seleccionar la entrada a realizarla estática, estableciendo una vez la misma se haya vuelto estática darle diversos tratamientos como la asignación a un address-list para brindarle un QoS o un determinado ancho de banda mediante un cola simple apenas se realice la conexión.

Es importante mencionar que Mikrotik incorpora un módulo de alerta sobre DHCP Server que permite detectar anomalías sobre dicho servicio como por ejemplo DHCP no autorizados, y personalizar una respuesta ante dicho evento mediante la ejecución de un script personalizados, tal como un regla de bloqueo o aviso etc.

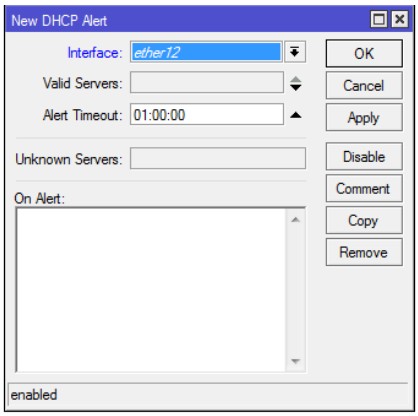


Figura 4.19. DHCP Alert en Mikrotik - RouterOS.

Fuente: Los Autores, DHCP Alert, 2013

4.3.5 OSPF como protocolo de enrutamiento en un ISP.

Haciendo una recapitulación del capítulo 2 acerca del protocolo dinámico de enrutamiento OSPF, se debe tener en claro que es un protocolo de enrutamiento Dinámico y de estado de enlace cuyas siglas de su algoritmo describen en inglés (Open Shortest Path First) y cuya traducción denota protocolo de enrutamiento jerárquico de pasarela interior o conocido como IGP (Internet Gateway Protocol), que utiliza el algoritmo Dijkstra mismo que permite calcular el camino más corto a todas las redes conocidas ; con un amplio uso hoy en día en redes corporativas no solo por sus grandes beneficios que aporta sino debido a su arquitectura y flexibilidad, encargado de enviar actualizaciones constantes rápidamente tanto de enrutamiento como de estado de interfaz, muy poco conocido sobre proveedores de acceso a internet inalámbricos algunos por el hecho de que los CPE o dispositivos terminales no soportan el uso del protocolo y otros por desconocimiento del mismo y su forma de uso. OSPF como tal ha sido estructurado para el entorno de Internet junto con su pila de protocolos TCP/IP, entendido como un protocolo de ruteo interno encargado de distribuir información entre Routers de una red Interna agrupadas en lo que se conoce como Sistema Autónomo, la intención de este punto del capítulo como tal no es ahondar en un tema de amplio estudio sino detallar sus aspectos básicos y evaluar su uso en proveedores de Internet Inalámbricos y como tal plantear su implementación para futuro ya que por el momento la red actual de la

empresa Sigsignet y sus dispositivos terminales no soporta el empleo de dicho protocolo; entre quizá sus grandes características se establecen como:

- La seguridad aportada ante los cambios, especificando que todos los cambios manejen un esquema de autentificación.
- Soporte de Múltiple métricas.
- Rápida respuesta sin bucles ante cambios.
- Mayor fiabilidad frente a protocolos como RIP.

Como se mencionó su uso en Proveedores de acceso a Internet inalámbrico está recién en auge, a raíz del surgimiento de tecnologías de bajo coste con soporte para dicho protocolo ya que anteriormente el uso del mismo se veía relegado a tecnologías cuyos costes era inaccesibles para posibilitar el acceso de última milla por tal utilizando dicho protocolo; Mikrotik hoy por hoy y sus variadas propuestas de hardware con RouterOS está posibilitando su rápida adopción en tales redes que en un futuro no muy lejano podrán hacer uso de todas sus bondades y muchas más.

Por esto es necesario ahora entender ciertos conceptos puntuales acerca de OSPF para tener una noción más clara acerca del protocolo y como base o sustento para su posterior implementación de una red de datos.

- El concepto de área está ligado a optimizar la distribución y agrega estabilidad.
- Todos los Routers dentro de OSPF se agrupan como áreas.
- La estructura del área es invisible fuera de ella.
- El área ID debe ser único en el sistema autónomo.
- Las áreas son identificadas por medio de un identificador de 4 Bytes (0.0.0.0 – 255.255.255.255).
- Existe una área 0 llamada Backbone, responsable de distribuir la información entre las áreas no-backbone
- Dentro de un área se definen también los IR o Routers Internos.

- También están los Routers que se conectan al área Backbone y otras áreas denominados ABR, así como los ASBR (Autonomous System Boundary Routers) encargados de la redistribución de información de ruteo entre OSPF y otros protocolos de ruteo.
- Áreas no-backbone pueden ser conectadas al área backbone con un virtual-link.

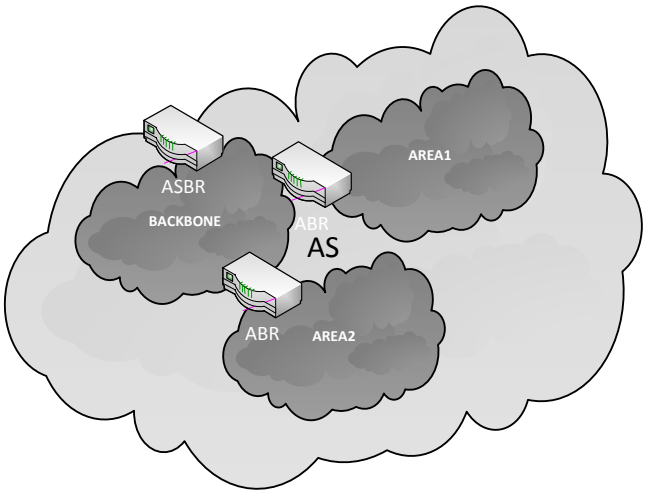


Figura 4.20. Topología y Elementos OSPF estándar.

Fuente: Los Autores, Parámetros de Configuración DHCP, 2013

Su implementación puede diferir de acuerdo a la topología pero su principio de funcionamiento y su configuración sobre Mikrotik será la misma, por tal para este punto se plantea una topología de ejemplo sobre la cual se implementara OSPF para interconectar la misma y evaluar su rendimiento y factibilidad, y que denotara como laboratorio para la puesta en marcha de dicho protocolo sobre la red reestructurada de la empresa Sigsignet, otorgando un encaminamiento de paquetes de forma más eficiente, y el soporte para añadir redundancia con un corto tiempo de respuesta ante eventuales fallos, por tal describiendo el siguiente procedimiento de configuración:

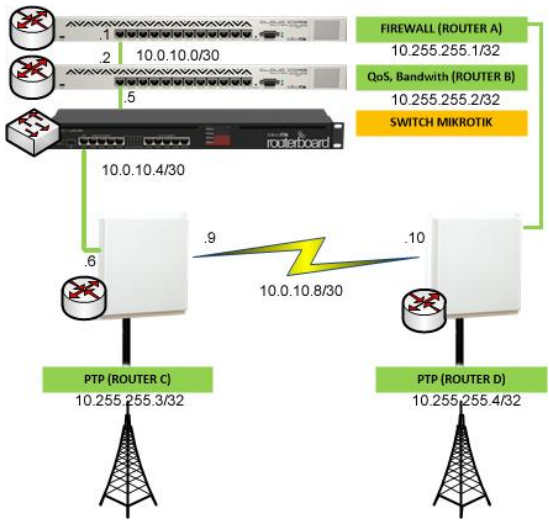


Figura 4.21. Topología de Ejemplo para implementación de OSPF.

Fuente: Los Autores, Topología Ejemplo para OSPF, 2013

1.-Es necesario la creación de una interfaz de tipo loopback sobre cada uno de los enrutadores Mikrotik, evitando que la identificación de cada Router se dé por su interfaz física sino más bien por una interfaz de tipo lógico, pero curando la misma este siempre activa, cabe recalcar que no es necesario asignar ninguna interfaz física al bridge.

```
[admin@ROUTERA,B,C,D] > interface bridge add name=loopback
```

Luego de la creación de cada una de las interfaces en todos los Enrutadores es necesaria la asignación de un IP a la misma, para su identificación como se mencionó en el punto anterior.

```
[admin@ROUTERA] > ip address add address=10.255.255.1/32 interface=loopback

[admin@ROUTERB] > ip address add address=10.255.255.2/32 interface=loopback

[admin@ROUTERC] > ip address add address=10.255.255.3/32 interface=loopback

[admin@ROUTERD] > ip address add address=10.255.255.4/32 interface=loopback
```

En cuanto a los enlaces punto a punto entre Enrutadores se utiliza la red 10.0.10.0/24 con un CIDR a /30, definiendo dos host por red y evitando el desperdicio de direcciones IP.

```
[admin@ROUTERA] > ip address add address=10.0.10.1/30 interface=ether1

[admin@ROUTERB] > ip address add address=10.0.10.2/30 interface=ether1

[admin@ROUTERB] > ip address add address=10.0.10.5/30 interface=ether2

[admin@ROUTERC] > ip address add address=10.0.10.6/30 interface=ether1

[admin@ROUTERC] > ip address add address=10.0.10.9/30 interface=ether2

[admin@ROUTERD] > ip address add address=10.0.10.10/30 interface=ether1
```

Luego de la asignación de todos las direcciones IP sobre las interfaces físicas y que forman OSPF, el siguiente paso es la configuración de OSPF, se usa la instancia establecida por defecto dentro de RouterOS cuyo nombre es default y contiene al área "Backbone" que existe de forma predeterminada, la misma que ya tiene establecida parámetros por defecto y existe en todo enrutamiento OSPF. Pudiendo si se cuenta con una base sólida de conocimientos la creación de una nueva instancia desde cero y por ende la definición de nuevas áreas. Es necesario para llevar a cabo este proceso desde una consola en Winbox, asociar la identificación del Router con su instancia.

```
[admin@ROUTERA] >  routing ospf instance set default router-id=10.255.255.1 redistribute-connected=as-type-1

[admin@ROUTERB] >  routing ospf instance set default router-id=10.255.255.2 redistribute-connected=as-type-1

[admin@ROUTERC] >  routing ospf instance set default router-id=10.255.255.3 redistribute-connected=as-type-1

[admin@ROUTERD] >  routing ospf instance set default router-id=10.255.255.4 redistribute-connected=as-type-1
```

Paso seguido será necesario que los enrutados inicien con la publicación de sus redes con el resto de enrutadores estableciendo la pertenencia de cada red sobre las redes publicadas.

```
[admin@ROUTERA] > routing ospf network add network=10.0.10.0/30 area=backbone
```

```
[admin@ROUTERB] > routing ospf network add network=10.0.10.0/30 area=backbone
```

```
[admin@ROUTERB] > routing ospf network add network=10.0.10.4/30 area=backbone
```

```
[admin@ROUTERC] > routing ospf network add network=10.0.10.4/30 area=backbone
```

```
[admin@ROUTERC] > routing ospf network add network=10.0.10.8/30 area=backbone
```

```
[admin@ROUTERD] > routing ospf network add network=10.0.10.8/30 area=backbone
```

Con dicho proceso terminado, finalmente solo queda comprobar las adyacencias con los diferentes vecinos listando los mismos, para esto ejecutar, en cualquiera de los enrutadores, pudiendo evaluar conectividad con los vecinos por medio del comando ping

```
[admin@ROUTERB] > routing ospf neighbor print
```

Si es necesaria dar salida a dicha red a Internet, previo haber configurado en el Enrutador la IP y su respectivo gateway sobre la Interfaz que brinda el acceso bastará solo publicar para su distribución y luego evaluar su conectividad.

[admin@ROUTERA] > routing ospf instance set default distribute-default=if-installed-as-type-1

4.3.6 MPLS.

MPLS (Multi-Protocol Label Switching) también ya hablado en el capítulo 2, compendia una red privada IP que combina la flexibilidad de las comunicaciones punto a punto o Internet y la fiabilidad, calidad y seguridad de los servicios Prívate Line, Frame Relay o ATM.

Ofrece niveles de rendimiento diferenciados y priorización del tráfico, así como aplicaciones de voz y multimedia. Y todo ello en una única red. Se cuenta con distintas soluciones, una completamente gestionada que incluye el suministro y la gestión de los equipos en sus instalaciones (CPE). O bien, que sea usted quien los gestione

- MPLS (Multiprotocol Label Switching) intenta conseguir las ventajas de ATM, pero sin sus inconvenientes
- Asigna a los datagramas de cada flujo una etiqueta única que permite una conmutación rápida en los routers intermedios (solo se mira la etiqueta, no la dirección de destino)
- Las principales aplicaciones de **MPLS** son:
    - Funciones de ingeniería de tráfico (a los flujos de cada usuario se les asocia una etiqueta diferente)
    - Policy Routing
    - Servicios de VPN
    - Servicios que requieren QoS
- MPLS se basa en el etiquetado de los paquetes en base a criterios de prioridad y/o calidad (QoS).
- La idea de MPLS es realizar la conmutación de los paquetes o datagramas en función de las etiquetas añadidas en capa 2 y etiquetar dichos paquetes según la clasificación establecida por la QoS en la SLA.

- Por tanto MPLS es una tecnología que permite ofrecer QoS, independientemente de la red sobre la que se implemente.
- El etiquetado en capa 2 permite ofrecer servicio multiprotocolo y ser portable sobre multitud de tecnologías de capa de enlace: ATM, Frame Relay, líneas dedicadas, LANs. [31]

Con el soporte de Mikrotik para MPLS y con la nueva infraestructura disponible luego del proceso de reestructuración utilizando tecnología Mikrotik, bastará las respectivas configuraciones sobre los equipos para el funcionamiento de dicho protocolo, en dicho proceso y en esta etapa la misma permitirá brindar a sus dueños y demás personal técnico que labora en la empresa un visión general sobre el protocolo y beneficios que representa mas no su implementación o adopción inmediata en dicho proceso de reestructuración, para este caso similar al anterior se usará una topología de la red de ejemplo usada para la puesta en marcha del protocolo OSPF **Figura 4.21.** sobre la cual se realizarán dichas configuraciones y su posterior evaluación, por tanto el procedimiento usado para enrutamiento será aplicado como requisito previo para su implementación, y definiendo las siguientes configuraciones en el ámbito de MPLS.

Sobre Enrutador A.

```
[admin@ROUTERA] >  mpls ldp set enabled=yes lsr-id=10.255.255.1 transport-address=10.255.255.1

[admin@ROUTERA] >  mpls ldp interface add interface=ether1

[admin@ROUTERA] >  mpls ldp interface add interface=ether2
```

Sobre Enrutador B.

[31] Luis Morales, Universidad de las Américas de Puebla, (n.d.). Redes VPN con tecnología MPLS, http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/morales_d_l/indice.html

[admin@ROUTERB] > mpls ldp set enabled=yes lsr-id=10.255.255.2 transport-address=10.255.255.2

[admin@ROUTERB] > mpls ldp interface add interface=ether1

[admin@ROUTERB] > mpls ldp interface add interface=ether2

Sobre Enrutador C.

[admin@ROUTERC] > mpls ldp set enabled=yes lsr-id=10.255.255.3 transport-address=10.255.255.3

[admin@ROUTERC] > mpls ldp interface add interface=ether1

[admin@ROUTERC] > mpls ldp interface add interface=ether2

Sobre Enrutador D.

[admin@ROUTERD] > mpls ldp set enabled=yes lsr-id=10.255.255.3 transport-address=10.255.255.3

[admin@ROUTERD] > mpls ldp interface add interface=ether1

[admin@ROUTERD] > mpls ldp interface add interface=ether2

Con ello culminado es necesario verificar la tabla de enrutamiento OSPF y su perfecto funcionamiento, y a su vez verificar la tabla de forwarding de etiquetas en MPLS.

4.3.7 Wireless en RouterOS.-

La parte de Wireless en RouterOS es quizá hoy por hoy una de las partes fuertes que Mikrotik ha desarrollado y lo sigue haciendo en cada versión nueva del Sistema Operativo, y es quizá una de las razones de porque los proveedores de servicio de Internet hayan optado por RouterOs como infraestructura fundamental para proveer

el acceso a Internet por lo tanto se va a detallar los procedimientos de configuración y sus diversos modos de Operación.

RouterOs cumple con los estándares IEEE 802.11, con soporte a,b,g y n y es posible muy pronto se llegue a ver el nuevo estándar ac, junto con niveles de encriptación WPA, WPE bajo cifrados tkip o aes, además los diversos modos de operación soportados(CPE, Punto de Acceso, Bridge etc), protocolos propietarios de alto rendimiento como NStreme o NStreme V2, y la posibilidad de trabajar en las bandas más usadas tanto en el spectro de los 5 Ghz o los 2.4 Ghz, que pueden desplegar canales acorde el dominio regulatorio o no según lo que exigen o demanda la ley.

Otras características asociadas a la parte de Wireless de Mikrotik es el apoyo al estándar IEEE 802.11 RTS/CTS (Solicitud de envió / Listo para enviar) mecanismo destinado a reducir las colisiones de marco introductorio asociado al problema de nodo oculto o mejor conocido como problema del terminal oculto, que se refiere a nodos que están fuera de otros nodos o de una colección de nodos, además el soporte para NStreme Version 2, protocolo basado sobre la tecnología más difundida como lo es TDMA (Multiplexación por División de Tiempo), que no es nada más que ocupar un canal de gran capacidad a partir de distintas señales fuentes, o mejor dicho que varios usuarios compartan el mismo canal dividiendo la señal en varios intervalos de tiempo.

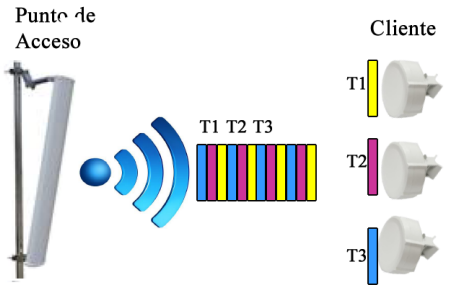


Figura 4.22. TDMA y acceso al medio.

Fuente: Los Autores, Acceso al medio por TDMA, 2013

NStreme Versión 2 está destinado para uso con chips de radio Atheros 802.11, además soporta QoS con un número variable de colas de prioridad, desde la versión 5.0 soporta ya cifrado de datos y funciones de autenticación por medio de un Radius, puede coexistir con dispositivos regulares 802.11, pero la NV2 solo podrá estar disponible entre dispositivos RouterOS mas no entre otros fabricantes. Además una de las características determinantes en NV2 es que no existe ACK por marco en NV2 permitiendo elevar el rendimiento en enlaces de larga distancia y reducir la latencia.

El uso de MIMO sobre 802.11n sobre el medio, por medio del uso de múltiples antenas y radios para obtener ventaja de la multitrayectoria permite el incremento del rango y troughput, y casi todos los fenómenos presentes en protocolos anteriores como refracción, difracción, absorción etc., son aprovechados completamente, por lo tanto utilizando múltiples transmisores permiten transmitir más datos por medio de la mutiplexación caso similar pasa con la recepción a diferencia se incrementa la relación señal/ruido

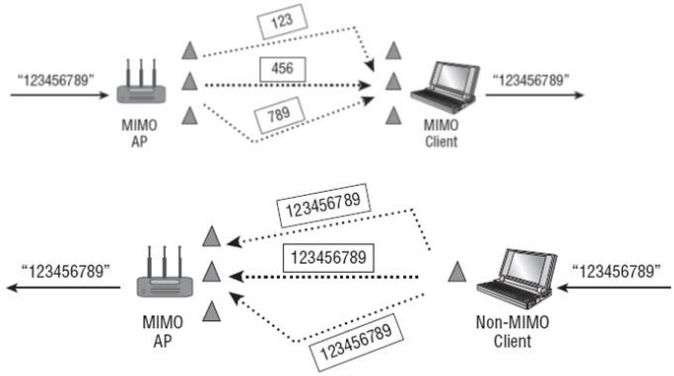


Figura 4.23. Metodología de transmisión y recepción sobre medios inalámbricos con soporte MIMO en 802.11.

Fuente: PERAHIA ELDAD, STACEY ROBERT, Next Generation Wireless LANs: 802.11n and 802.11ac, 2013

Además toda esta parte se completa con el uso de herramientas esenciales para la gestión de enlaces inalámbricos entre los cuales tenemos opciones como "Scan", permite realizar un escaneo de canales y frecuencias sobre la interfaz inalámbrica

permitiendo ver Puntos de Acceso Disponibles para Conexión y algunos parámetros adicionales.

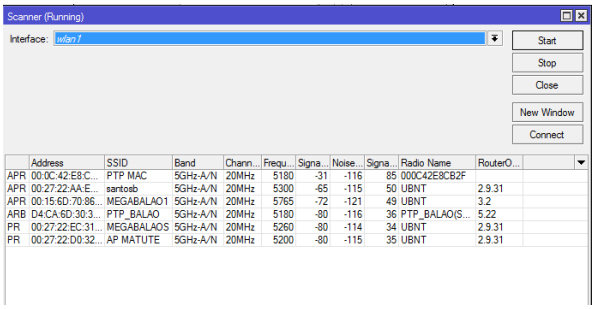


Figura 4.24. Herramienta Scanner en Winbox para Escaneo de Canales y Frecuencias.

Fuente: Los Autores, Herramienta Scanner, 2013

Incluso herramientas para monitorización de uso del espectro de la banda y sus determinadas frecuencias, generalmente muy útil para determinar canales limpios libres de interferencia.

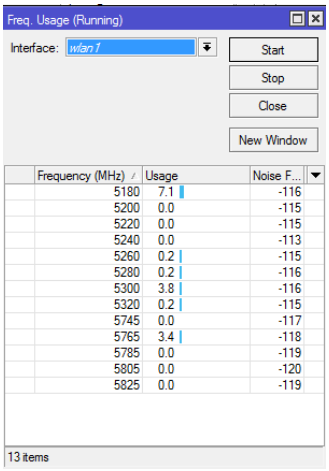


Figura 4.25. Herramienta Freq. Usage para detección del Espectro.

Fuente: Los Autores, Freq. Usage, 2013

En tanto la herramienta Snooper permite monitorizar el uso de la frecuencia, y que dispositivos la están ocupando, mostrando estadísticas puntuales como la cantidad de datos y paquetes, ancho de banda real utilizado por cada canal.

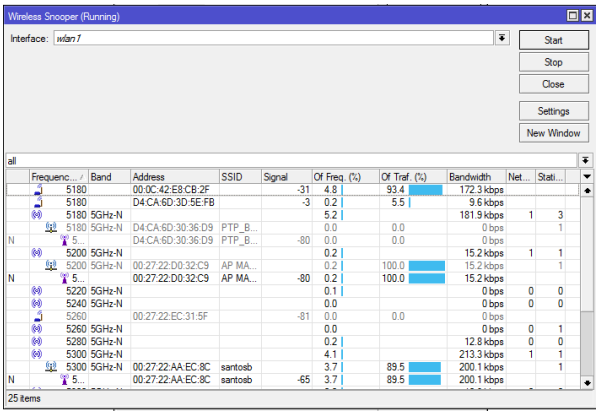


Figura 4.26. Herramienta Wireless Snooper.

Fuente: Los Autores, Wireless Snooper, 2013

O la herramienta Sniff, capaz de capturar el tráfico y analizar paquetes que van a salir o pasar por el Router, a excepción del tráfico que pasa por el chip switch o chip de conmutación, para luego ser analizado por herramientas como Wireshark o similares.

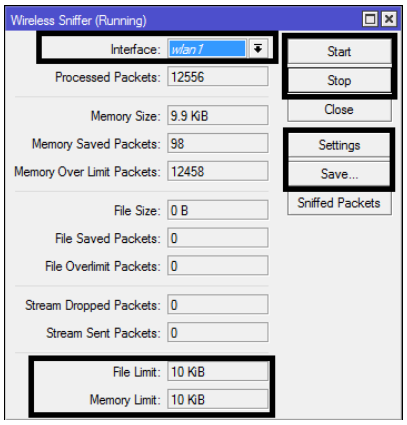


Figura 4.27. Herramienta Wireless Sniffer.

Fuente: Los Autores, Wireless Snooper, 2013

4.3.7.1 Puntos de Acceso

Desde sus inicios Sigsignet ha confiado su infraestructura para distribución del acceso a Ubiquiti, por los beneficios que en aquellos tiempos dicha solución presentaba, pero conforme la red crecía la solución empleada se quedaba algo corta

no por el hecho que fuera de mala calidad al contrario Ubiquiti es un vendedor referente de conectividad con enlaces de radio robustos y componentes de buena calidad, en cambio Mikrotik por su poderoso sistema Operativo con capacidades para levantar topologías, escenarios complejos, bajo protocolos como OSPF o MPLS y su bajo costo esta revolucionado el mercado y la forma en como proveer el servicio de Internet, aunque no por ello significa que con Mikrotik no podemos tener enlaces de calidad, al contrario pueden ser muy robustos y eficientes quizá para usuarios convencionales la facilidad de configuración que presenta ubiquiti en su frot – end, no necesita de muchos conocimientos para levantar un punto a punto a multipunto, en cambio en Mikrotik existe la posibilidad de hacer uso de un Wizard denomida "Quick Set" pero que muchas de las veces no permite setear parámetros base para armar un radioenlace de calidad y acorde a las necesidades establecidas.

Por lo tanto se tiene en consideración algunos instructivos claves a la hora de configuración para poder disponer de puntos de acceso adecuado.

1.-A nivel de 802.11 se ha constatado que el protocolo nstreme busca mejores velocidades de transmisión y fiabilidad en la comunicación, ya que mejora notablemente la modulación, codificación y la forma en como la señal se procesa, sumado a esto el soporte MIMO para por medio del uso de múltiples antenas poder transmitir y recibir al mismo tiempo, el uso adecuado del estándar 802.11n en combinación con NV2, garantizará una mayor eficiencia de tiempo aire, permitiendo tener una mayor concurrencia de clientes simultáneos, incremento de throughput, por tal bajo tecnologías Mikrotik se vuelve relativamente importante la activación del protocolo basado en TDMA denominado "Nstreme" en su versión 2, como se mencionó su activación es acertada cuando se trabaja con equipos Mikrotik, además la selección del Ancho de Canal que van desde los 5Mhz, 10 Mhz, 20 Mhz y 40 Mhz mismos que posibilitan según el ancho del canal, poder manejar un mayor troughput, además utilizar las herramientas tanto de escaneo de frecuencias como la monitorización de las mismas puede ayudar a elegir frecuencias en canales muy limpios y poder brindar así una comunicación y enlace fiables.

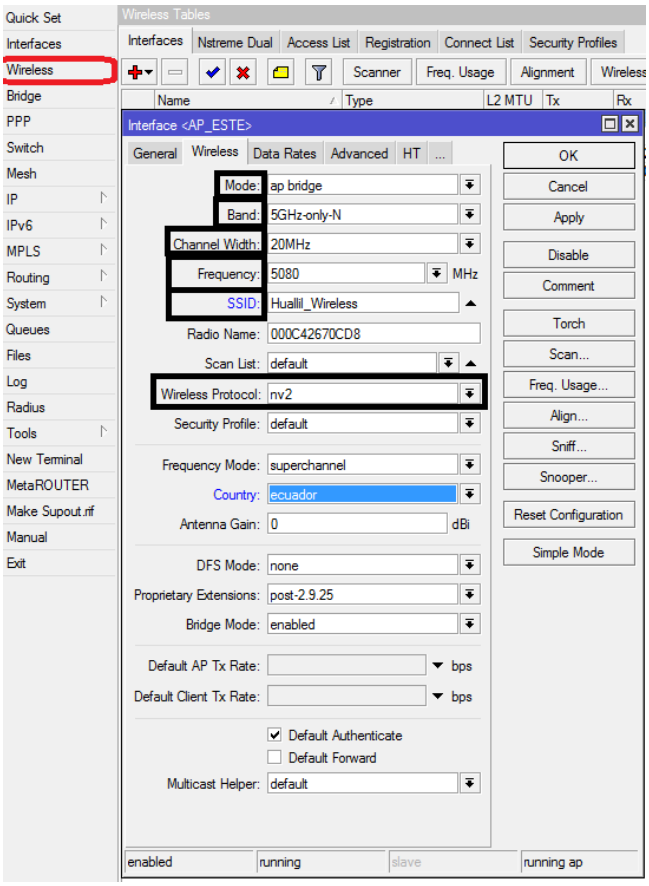


Figura 4.28. Ventana de Configuración de Interfaz Wireless en RouterOS

Fuente: Los Autores, Ventana de Configuración Wireless Mikrotik, 2013

En cuanto a la determinación del protocolo Wireless para comprender un poco más acerca de los mismos se detalla la siguiente tabla.

Valor	AP	Cliente (CPE)
Unspecified	Establece nstreme o 802.11 basado en la configuración de tiempo Nstreme	Conectarse a Nstreme o 801.11 basado ajuste tiempo NStreme
Any	Mismo que unspecified	
802.11	Establece protocolo	Conecta solo a redes

	802.11 sobre la red	802.11
Nstreme	Establece una red bajo protocolo NStreme	Conecta solo a redes NStreme
Nv2	Establece una red bajo protocolo NStreme Versión 2	Conecta solo a redes NStreme Versión 2
Nv2-nstreme-802.11	Establece una red NStreme Versión 2	Primero busca redes NV2, si la red adecuada es encontrada se conecta, caso contrario buscara las redes NStreme y se conectara, o si en su defecto se encuentra una red 802.11 se conectara a la misma.
Nv2-nstreme	Establece una red NStreme con soporte para Versión 2	Primero busca redes NV2, si la red adecuada es encontrada se conecta, caso contrario buscara las redes Nstreme y se conectara.

Tabla 4.3. Soporte de Protocolo Wireless en Mikrotik.

Fuente: Los Autores, Protocolos Wireless en Mikrotik, 2013.

Además el paramento HT dentro de la interfaz inalámbrica conocida como “High Troughput” es un modo de operación que ofrece mejoras para obtener ancho de banda elevados utilizando “frame aggregation” y por tal sus mejoras en capa MAC, reducción de transmisión de encabezados y espacio entre tramas, haciendo en

realidad un mejor uso del ancho de banda del espectro de la radio frecuencia, empleando para ello canales superiores en ancho de banda de radiofrecuencia como los (20 Mhz o los 40 Mhz), y además al operar con tecnología MIMO requiere el uso de múltiples radios y antenas para sacar ventaja a la multitrayectoria , por tal se convierte en necesario activar las chains o antenas disponibles, dicha configuración también puede ser configurado como enlaces punto a punto y obtener resultados altamente eficientes; con dichas recomendaciones no se pretende establecer un modelo de configuración puntual, ya que la activación o desactivación de determinados parámetros variara o dependerá la situación geográfica, y pueda en dichos casos no ser una opción eficiente.

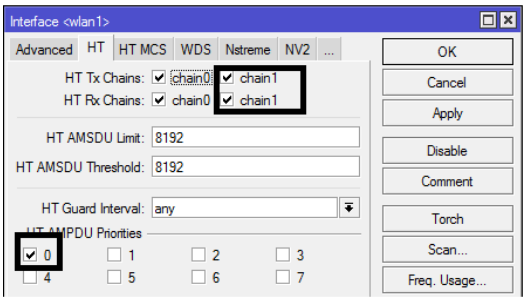


Figura 4.29. Ajustes de Parámetros High Troughput en Interfaz Wireless.

Fuente: Los Autores, Ventana de Configuración Wireless Mikrotik, 2013

La reducción de la potencia Tx es otro factor a controlar importante definiéndolo a un valor menor del establecido por defecto, ya que muchos de los casos el exceso de potencia termina en la generación de interferencia que en una buena comunicación.

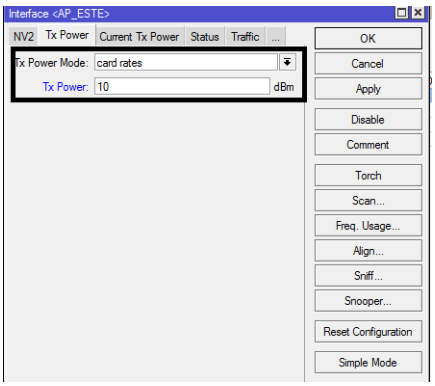


Figura 4.30. Ajustes de Parámetros TX Power en Interfaz Wireless.

Fuente: Los Autores, Ventana de Configuración Wireless Mikrotik, 2013

La selección del rate es otro factor vital, por defecto dentro de la pestaña Data Rates en vista modo Avanzado dentro de la Interfaz inalámbrica el rate viene activada por "Default" en modo avanzado, además se consideran dos modos de selección de rate:

Legacy.-

- Funciona cuando la conexión inalámbrica es buena en todo los datarates.
- No se cambia tan bien del protocolo B a G, debido a las tasas de datos estándar.
- No se cambia de A/G para velocidades de datos N, donde es posible usar "Frame Aggregation"

Avanzado.-

- El siguiente data-rate se calcula-prueba simultáneamente en todos los data-rate "bloques" disponibles, y se usa el mejor de los resultados obtenidos.
- Para un enlace corriente de 20 Mhz el cambio al protocolo N es más rápido de utilizar y permite "Frame Aggregation"
- El data-rate puede incrementarse rápidamente sin sufrir ningún tipo de problemas.

Figura 4.31. Ajustes de Parámetros Data Rates en Interfaz Wireless.

Fuente: Los Autores, Ventana de Configuración Wireless Mikrotik, 2013

Para el caso de Ubiquiti las consideraciones en la configuración de los puntos de acceso a nivel inalámbrico se establecen de la siguiente forma, algunos puntos sobre protocolos y relacionados no se ahondaran debido a que ya se los ha explicado en temas anteriores por tal se establecerán puntos clave.

Lo primero Ubiquiti no maneja una interfaz de administración como Winbox mas bien las configuraciones se las pueden setear por su interfaz de administración web o si se tiene algo experiencia haciendo uso de ssh y bajo consola, por tal para este caso optamos por la primera opción.

Por lo tanto desde el navegador ingresar al equipo por la IP que esté asignada al mismo.

1.-Definir el modo de Operación del Dispositivo tales como Station, Access Point o AP Repeater para este caso de la configuración del Multipunto Access Point.

2.-Definir el SSID que será difundido por medio de este punto de acceso.

3.-El modo de operación se establece al momento de seteo por primera vez durante la pestaña login del campo Country Name o País, para el caso el modo establecido es A/N combinado.

4.-Es necesario establecer el ancho de canal de la frecuencia que se va a operar, para este caso 20 Mhz y luego establecer la frecuencia sobre la que va a operar, al igual que el caso anterior con los equipos Mikrotik el parámetro TX Power es necesario reducir para evitar generar problemas de comunicación o interferencia, así como el parámetro MCS o mejor conocido como Sistema de Modulación y Codificación, siendo como para el caso anterior sobre Mikrotik una combinación de modulación determinada tales como (BPSK, QPSK, 64-QAM) la tasa de codificación (1/2/3/4) entre otros parámetros más, todos los puntos de acceso bajo el estándar n deben soportar como mínimo MCS0 hasta 15 desde MCS0 hasta MCS7, por defecto viene seleccionado en modo automático pero se recomienda establecer un valor MCS

estático con el fin de poder manejar rates bajo modulación considerados estables y que otorgan un nivel de perfomance adecuado.

5.-Finalmente establecer el protocolo de cifrado y su clave es imprescindible.

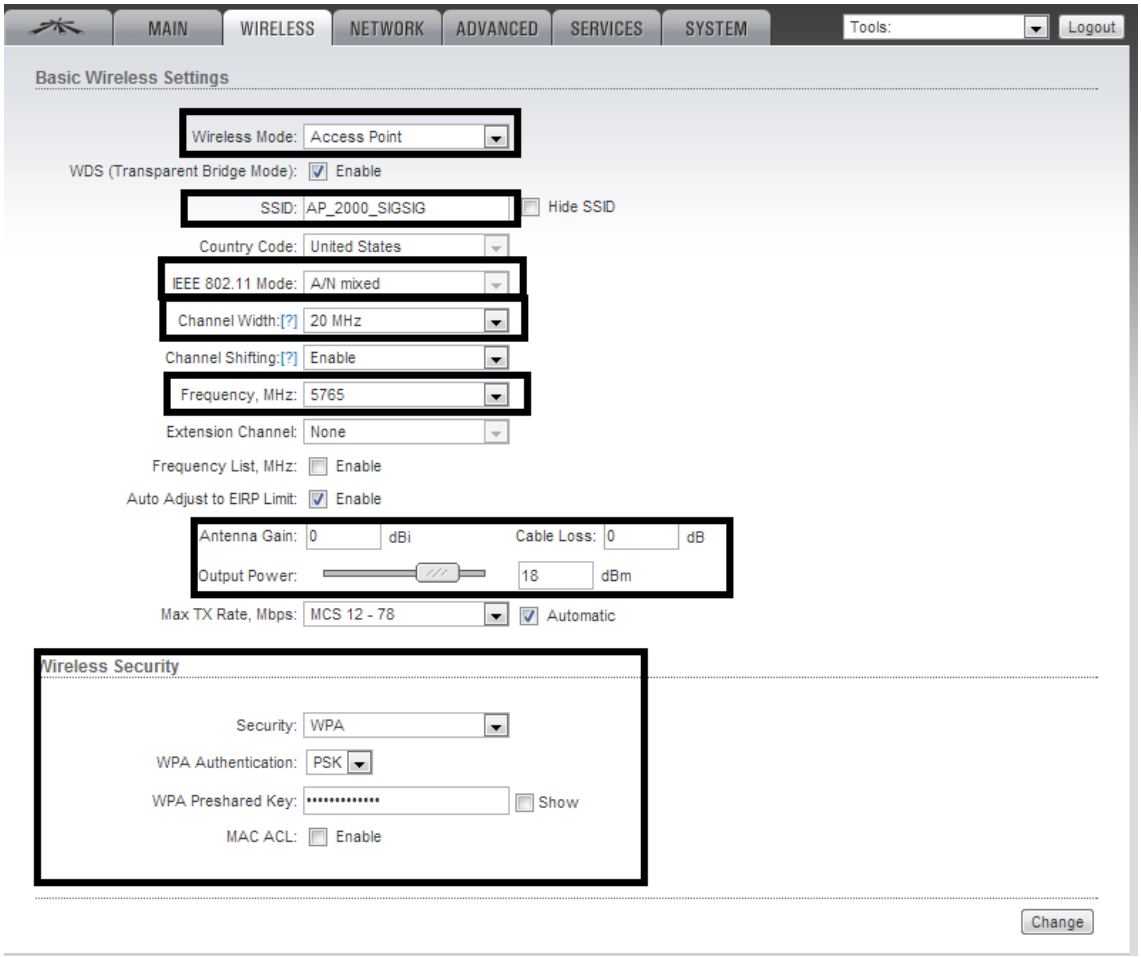


Figura 4.32. Ajustes de Parámetros Wireless en AP Ubiquiti Nanostation.

Fuente: Los Autores, Ventana de Configuración Wireless Ubiquiti, 2013

En la pestaña avanzada ahora es necesario realizar las siguientes configuraciones.

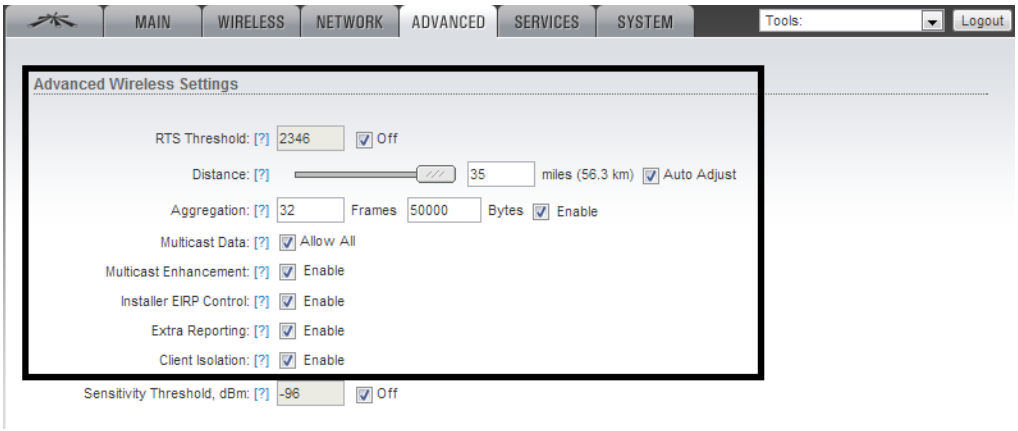


Figura 4.33. Ajustes de Parámetros Advanced en AP Ubiquiti Nanostation.

Fuente: Los Autores, Ventana de Configuración Advanced Ubiquiti, 2013

4.3.7.2 Configuración de CPE Mikrotik y Ubiquiti.

La configuración de las estaciones cliente es de vital importancia ya que determina la calidad de conexión, la configuración deseada al momento de instalar un cliente se la muestra en las siguientes figuras, cabe recalcar que depende la ubicación del cliente y las condiciones de visibilidad, geográficas y ambientales sus configuraciones variaran dependiendo el entorno por tal en este punto se estable una configuración genérica que podría someterse a cambios dependiendo el entorno.

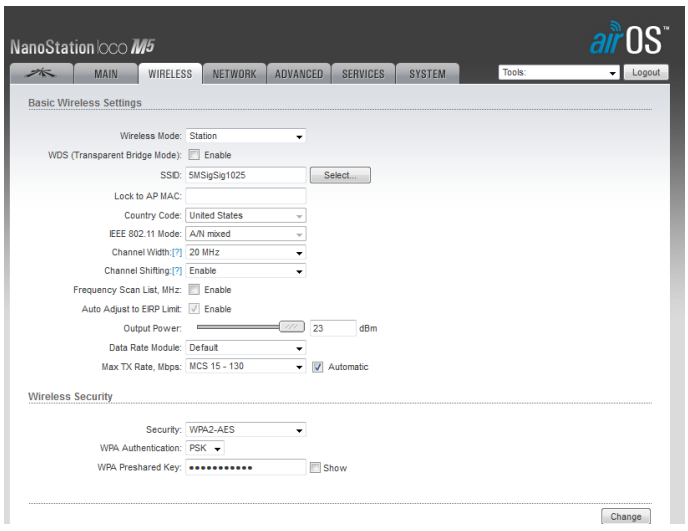


Figura 4.34. Ajustes de Parámetros Wireless en CPE Ubiquiti Nanostation.

Fuente: Los Autores, Ventana de Configuración Wireless Ubiquiti, 2013

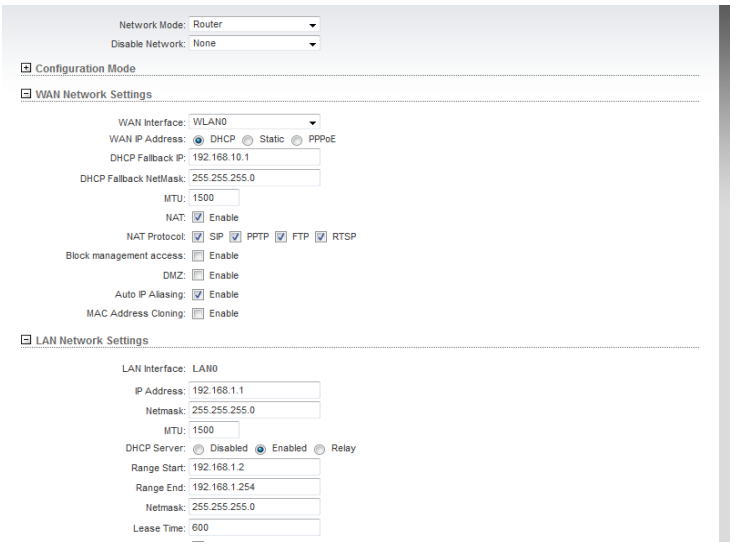


Figura 4.35. Ajustes de Parámetros Network en CPE Ubiquiti Nanostation

Fuente: Los Autores, Ventana de Configuración Network Ubiquiti, 2013

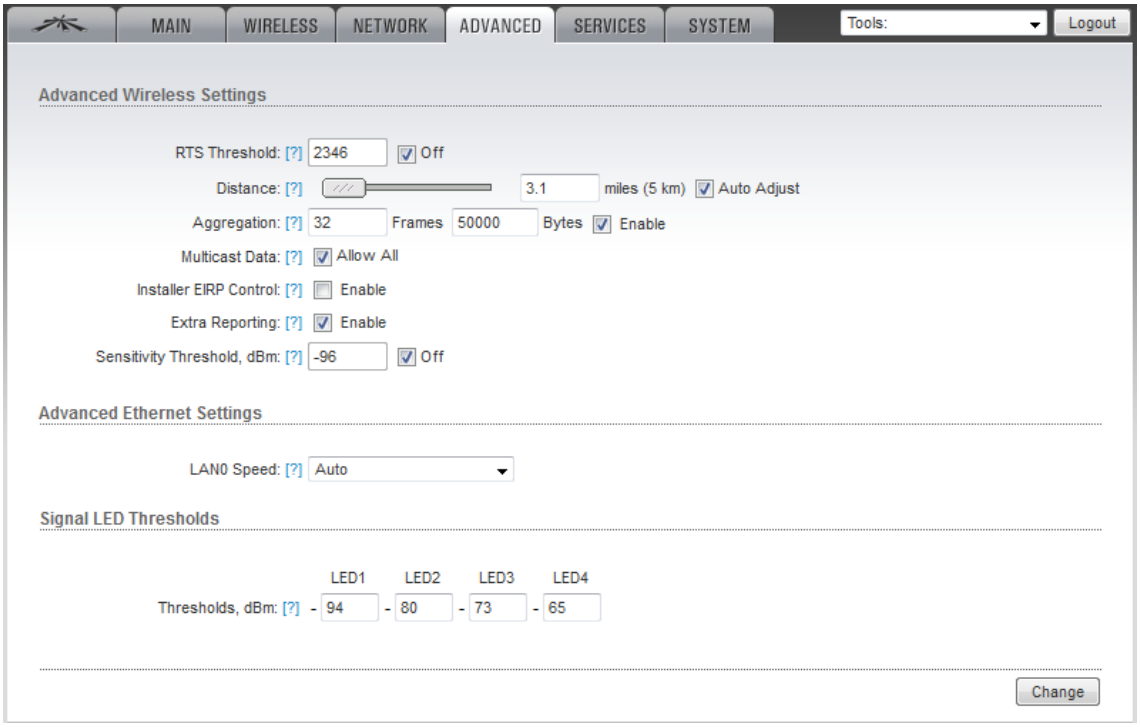


Figura 4.36. Ajustes de Parámetros Advanced en CPE Ubiquiti Nanostation.

Fuente: Los Autores, Ventana de Configuración Network Advanced, 2013

En tanto la configuración para CPE de la marca Mikrotik maneja la siguiente configuración, misma que puede ser realizada por la herramienta Quick Set o Directamente sobre la Interfaz, siendo necesario determinar el protocolo sobre el cual se va a establecer conexión en el caso Mikrotik Nstreme en cualquier de sus variantes.

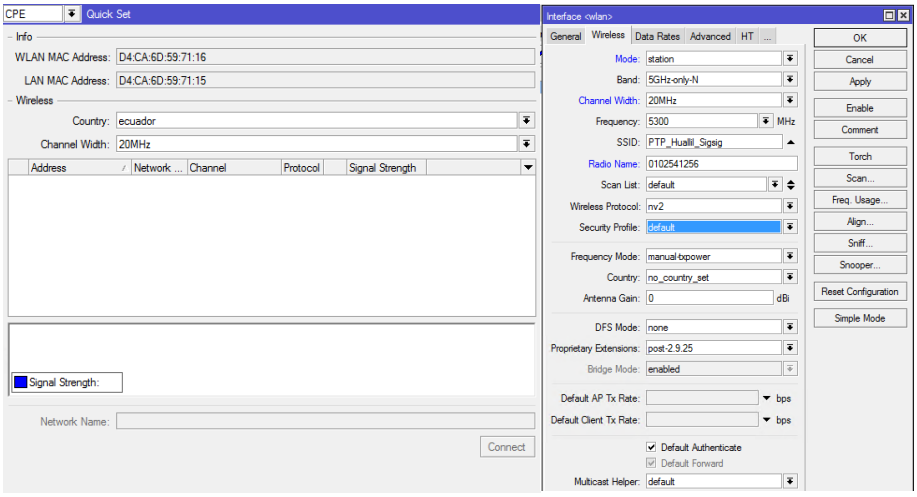


Figura 4.37. Ventana de Configuración Wireless Mikrotik para modo CPE.

Fuente: Los Autores, Ventana de Configuración Wireless Mikrotik Modo CPE, 2013

4.3.8 Administrador de Ancho de Banda con colas simples y árboles de colas.

La administración de Ancho de Banda en los proveedores de Internet es muchas veces su talón de Aquiles, los factores que recaen en problemáticas son diversos, algunos que van desde configuraciones mal elaboradas, limitaciones del Hardware - Software o soluciones demasiadamente costosas para ser implementadas. Por tal Mikrotik ha presentado un clara propuesta siendo como ya se ha mencionado en ocasiones anteriores su principal factor la relación beneficio / costo, y que a su vez lo complementa con la diversidad de disciplinas de encolamiento soportados tales como pfifo, fifo, pcq, red etc., con el único fin de poder dotar de diversos mecanismos para tareas de administración de ancho de banda. Dentro de la empresa Sigsignet son algunas premisas que a ser tomadas en consideración y con las cuales se pretende

consolidar una clara solución utilizando Mikrotik como herramienta para dicho fin, y en específico sobre la red deseada:

- Limitación del ancho de banda disponible por usuario o por tipo de contrato subscrito.
- Priorización de determinados servicios en comparación a otros (QoS), dejando fluir paquetes de alta prioridad y descartando paquetes de baja prioridad si viene demasiadamente rápido.
- Evitar la monopolización de tráfico por un usuario.
- Bursting sobre tráfico HTTP, y denotar una mejor experiencia de navegación sobre el usuario.
- Control Trafico Malicioso.

Para tal es necesario comprender las modalidades a emplearse en gestión de tráfico, temas vitales para la estructuración y configuración de los mecanismos de control y administración de ancho de banda.

- **Traffic Shapping.-** Busca limitar el Rate sobre un caudal de tráfico a un determinado valor, almacenando en buffer los paquetes excedentes.

Figura 4.38. Grafica de limitación de Rate basada en Traffic Shapping
Fuente: Alfredo Giordano, QoS in RouterOS v6.x, MUM Italia 2014, p 8

- **Traffic Priority.-** Busca clasificar el trafico basado en aplicación, permitiendo fluir rápidamente a paquetes con alta prioridad y controlando a los de menos prioridad.

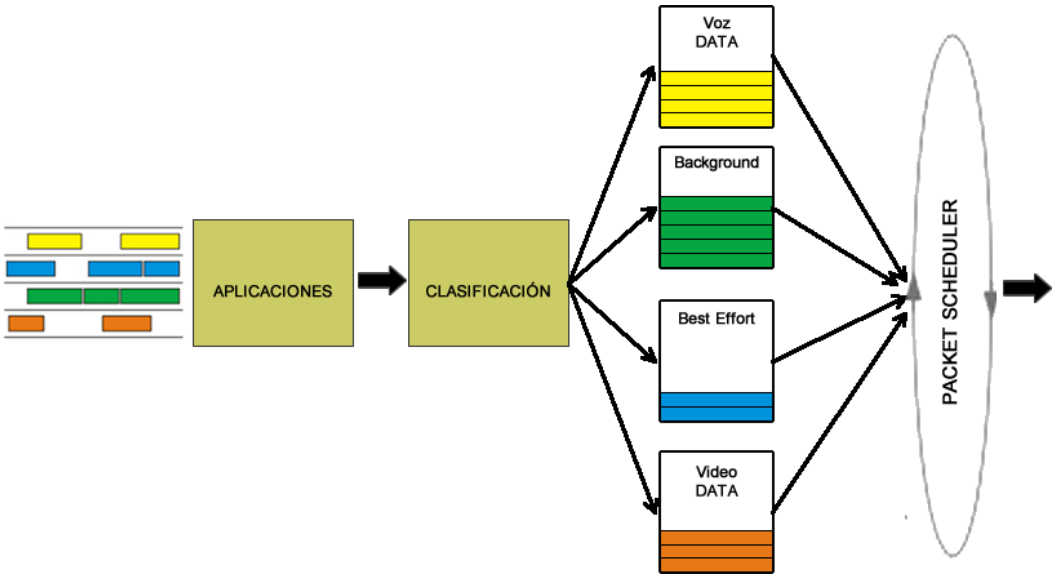


Figura 4.39. Clasificación de Tráfico Basado en Aplicación.

Fuente: Alfredo Giordano, QoS in RouterOS v6.x, MUM Italia 2014, p 8

Es posible dentro de RouterOS emplear dos técnicas de control de Ancho de Banda la primera mediante un Árbol de Colas o mejor conocido como "Queue Tree" y la otra por "Simple Queue" o colas simples, la primera técnica o Árbol de Colas, se orienta por construir un estructura jerárquica con colas padres e hijas donde los padres se encargan de distribuir el tráfico y las hijas lo consumen, en tanto el encolamiento simple hace una limitación del caudal sin ser necesarias marcas sobre el mismo para su procesamiento, limitando o contralando el trafico sea por medio de dts-address (IP) o por interface, en versiones anteriores a las 6.X su modo de operación sobre cantidades significativas de colas simples representaba un significativo consumo de recursos, pero que desde liberación de la versión 6.0 en adelante el problema fue solucionado pudiendo tener actualmente miles de colas sin sufrir un exceso de consumo de recursos, o incluso la posibilidad de disponer de una doble calidad de servicio (QoS) en un mismo equipo, siendo posible usar Árbol de Colas para elaborar una completa calidad de servicio y encolamiento simple para la limitación de ancho de banda por usuario o tipo de contrato subscrito, con tales consideraciones cabe recalcar que Mikrotik es una potente herramienta con el cual se puede construir un sistema de gestión de tráfico extremadamente sofisticado que nos permite brindar un servicio de calidad.

4.3.8.1 Colas Simples

Es la forma más sencilla de establecer un control o límite de velocidad de datos para direcciones específicas y/o subredes, siendo posible también trabajar con marcado de tráfico mediante Mangle, definir prioridades, manejar Bursting o incluso definir diferentes límites de rates basados en horarios, el empleo de colas simples se establece para la limitación del rates sobre los diversos planes que la empresa oferta hacia los subscriptores de tal forma que evite la monopolización de tráfico, no controlada en la red actual y posibilite un asignación personalizada de rate en el caso de clientes corporativos con canales dedicados.[32]

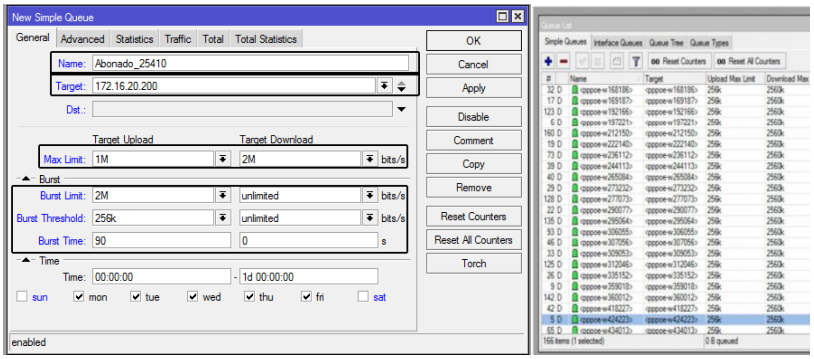


Figura 4.40. Encolamiento Simple "Simple Queue" en RouterOS.

Fuente: Los Autores, Simple Queue, 2013

El proceso de creación de las mimas es relativamente sencillo, utilizando Winbox:

- Winbox >> Simple Queue >> (+) Add

Dentro de la ventana simple queue, en la pestaña "General" los parámetros a configurar serán:

- **Name:** Establece un nombre a dicha Cola.
- **Target:** La subred, dirección IP o interfaz a la que se pretende realizar la limitación.
- **Max-Limit:** Considerado tanto para la subida como la descarga respectivamente, se encargaran de limitar el caudal al valor establecido.

[32] DISCHER, STEHHEN R.W, "RouterOS by example", Learn Mikrotik, 2011, p 100

- **Burts:** Grupo de parámetros definidos para la asignación de ráfagas, empleado sobre tráfico HTTP, generando un rate superior al limitado por determinado periodo de tiempo.

Además es importante mencionar, que el proceso de crear un cola no solo implica una actividad manual sino el mismo puede ser de forma automática, es decir si los subscriptores emplearan métodos de conexión, como por ejemplo los basados en PPPoE o mediante DHCP dichas colas pueden ser creadas de forma automática por Mikrotik, sin ser necesario un proceso manual de creación, cada vez que una cola es creada mediante un proceso automático el FLAG o Bandera en "Simple Queue" adjunta un carácter que asocia la letra "D" de Dinámico, indicando que la misma ha sido creada de forma automática, muy útil en determinados escenarios.

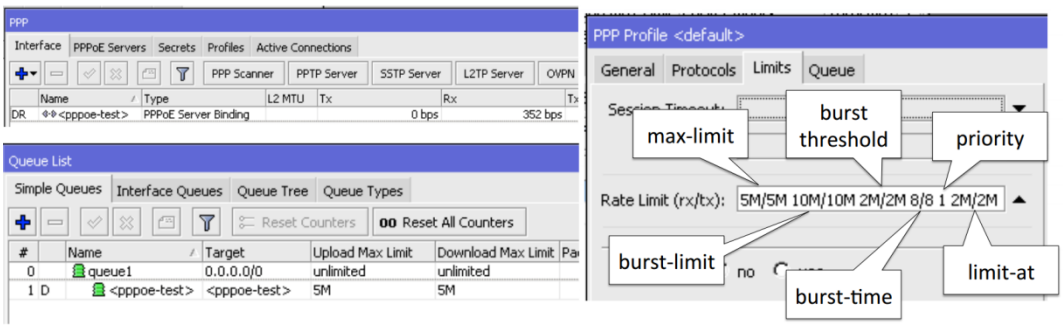


Figura 4.41. Creación Automáticas de Colas Simples bajo perfil de conexión PPPoE.

Fuente: Mikrotik, Interface PPPoE, 2013, http://wiki.mikrotik.com/wiki/Hotspot,_apply_different_limits_and_different_traffic_priorities

4.3.8.2 Arboles de Colas

Como ya se ha mencionado en capítulos anteriores Queue Tree es una implementación de Mikrotik basada en HTB formando una estructura jerárquica de colas, estableciendo niveles de colas tanto padres como hijas, posicionando las

ultimas en el nivel más bajo y siendo estas las encargas de consumir el tráfico, no en tanto así las colas padres cuya función es la distribución del caudal de tráfico entrante, además HTB implementa dos mecanismos de limite sobre el rate conocidos como “limit-at” y “max-limit” relacionados con CIR y MIR respectivamente ya comentados en puntos anteriores pero si parámetros influyentes al momento de la distribución del caudal, siendo CIR o “limit-at”, la tasa de rate a garantizar, que en complemento con el parámetro prioridad ejecutan la distribución de tráfico restante entre las colas hijas, siendo uno la prioridad más alta y 8 la más baja.

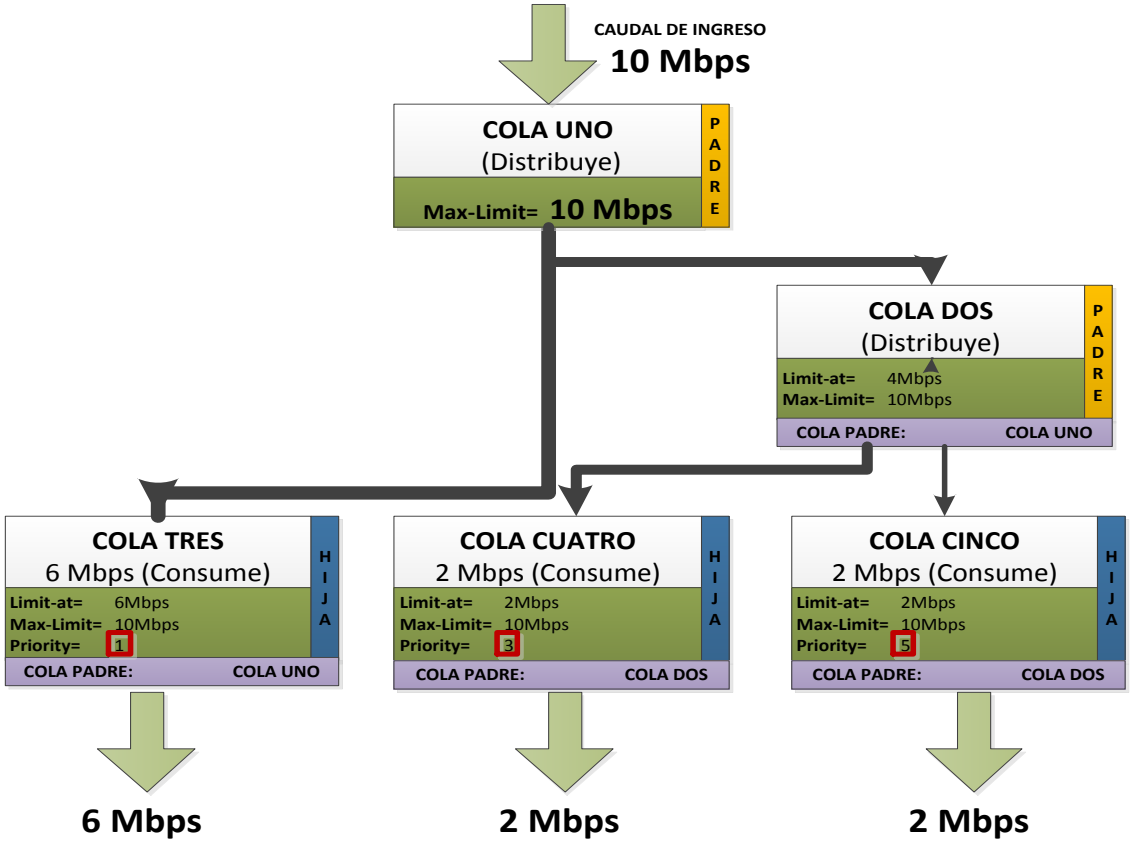


Figura 4.42. Caso de Uso de Jerarquía de Colas bajo HTB.

Fuente: Los Autores, HTB, 2013

El mecanismo de árbol de colas en Mikrotik y su aplicación sobre la red de la empresa Sigsignet se plantean como solución sobre la red deseada, destinada al control y gestión de calidad de servicio (QoS), su uso se ve complementado con Mangle, herramienta utilizada para identificar el tráfico y establecer marcas sobre los

paquetes para su posterior priorización o tratamiento sea tanto en “Queue Tree” o sobre las diversas instancias en las cuales dicho trafico tiene que fluir. Antes de adentrarnos sobre configuraciones puntuales es importante conocer para ello el Diagrama de Flujo de Paquetes en RouterOS, funcional desde la versión 6.X o superior, definido de la siguiente forma:

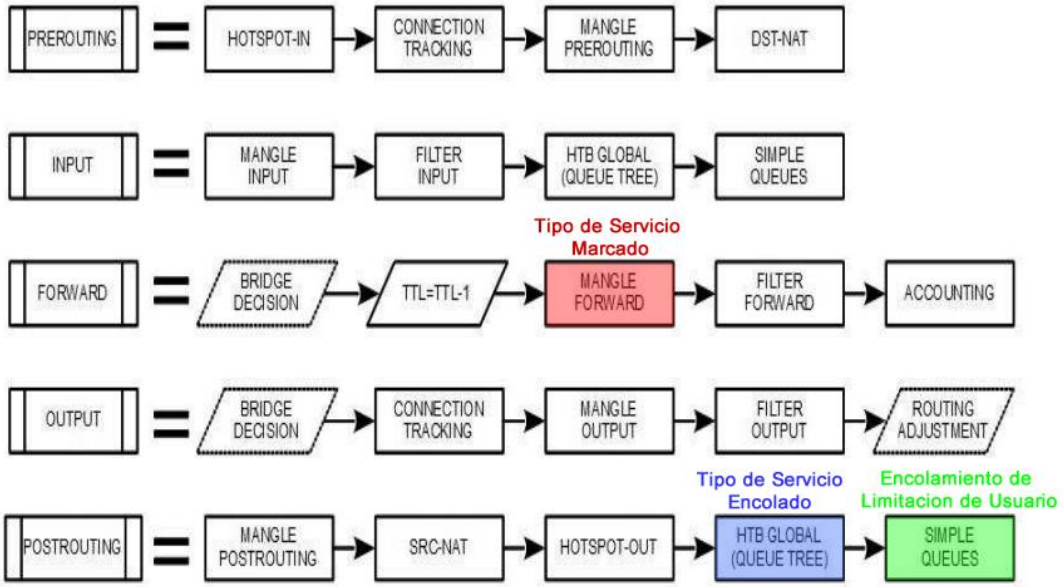


Figura 4.43. Diagrama de Flujo de Paquetes para RouterOS V6.X.

Fuente: Mikrotik, Packet Flow V6, 2014,
http://wiki.mikrotik.com/wiki/Manual:Packet_Flow

Según el “Packet Flow” y como medio para establecer una calidad de servicio optima, las marcas de paquetes asignadas a los distintos tipos de tráfico se establecerán dentro Mangle sobre la cadena “FORWARD”, para su posterior encolamiento y clasificación de dicho tráfico y por ende su priorización sobre Queue Tree, dejando la limitación de rate por usuario / plan contratado a través de encolamiento simple, por tal es necesario tener en claro el tráfico que se intenta priorizar, que va desde determinar servicios de red y los puertos sobre los que estos corren así como el protocolo utilizado por estos sea TCP o UDP.

Port	Protocol	Comments
20/21	tcp	FTP
53	tcp/udp	DNS
22	tcp	SSH,SFTP
80	tcp	HTTP
123	udp	SNTP
443	tcp	HTTPS
500	udp	IPSec
1701	udp	L2TP
1723	tcp	PPTP

Figura 4.44. Puertos de Servicios de Red Básicos.

Fuente: Red de Centros SAT, Medidas de seguridad básicas: Los puertos de tu router, 2 de Mayo de 2014, https://www.fundacionctic.org/sat/articulo-medidas-de-seguridad-basicas-los-puertos-de-tu-router

Es necesario conocer que cada red de datos es mundo diferente y no siempre un procedimiento establecido de QoS para una red puede funcionar sobre otra distinta, las necesidades muchas de las veces puede variar, por tal se describe el procedimiento sobre RouterOS para elaborar una calidad de Servicio y su respectiva limitación de rate para los usuarios o planes contratados, para el siguiente ejemplo se intenta priorizar los puertos 22 y 23 bajo el protocolo TCP , utilizando Winbox para dicha configuración definiendo el siguiente procedimiento:

1.-Determinar puerto y protocolo, y establecer marca conexión para dicho servicio de red, para tal asignamos un nombre a dicha marca de conexión, en este caso "protocolosremotosC"

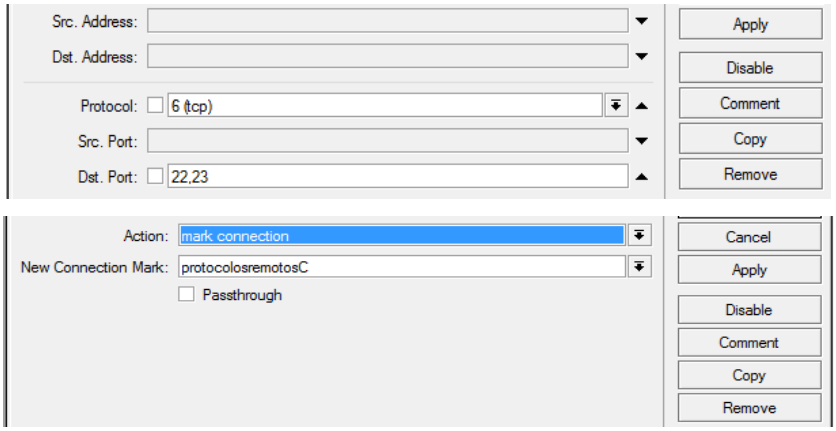


Figura 4.45. Marca de Conexión en Mangle.

Fuente: Los Autores, Marca de conexión Mangle, 2013

2.-Marcar el flujo de paquetes de dicha conexión para su posterior priorización, para tal utilizamos el nombre de la Marca de Conexión anterior y se asigna un nombre a la marca del Flujo de Paquetes “protocolosremotosF”.

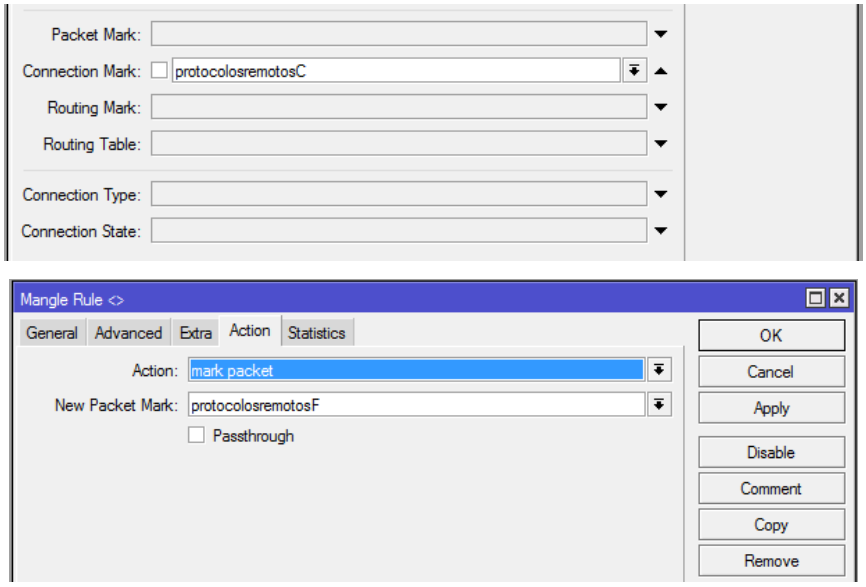


Figura 4.46. Marca de Flujo de Paquetes en Mangle.

Fuente: Los Autores, Marca de Flujo de Paquetes en Mangle, 2013

3.-Con dicha Marca establecida es necesario realizar la priorización del Flujo de Paquetes utilizando Queue Tree, por tal basta ubicar el nombre de la Marca de Paquetes, asignar la cola padre en caso de haberla, establecer la prioridad de dicho flujo, y la asignación de un nombre, con ello realizado se posibilita que dicho servicio(s) de red en horas de congestión no se vea afectado(s) o peor aún ininterrumpido(s), así basta como ya se mencionó anteriormente establecer los protocolos y puertos a priorizar.

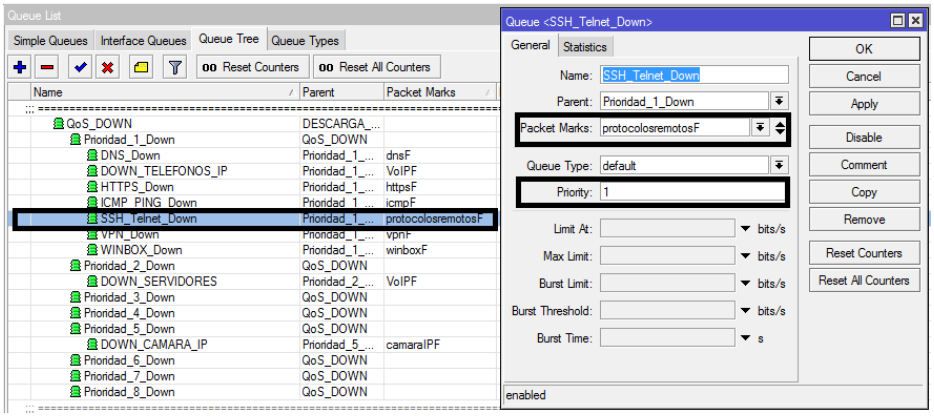


Figura 4.47. Queue Tree, Priorización de Flujo de Paquetes.

Fuente: Los Autores, Priorización de Flujo de Paquetes, 2013

4.3.9 Lista de Direcciones

Mejor conocido dentro de Winbox como “Address List”, dentro de esta es posible asignar múltiples direcciones o rangos a una misma regla de firewall reduciendo el número de reglas e incrementando la perfomance del Router, incluso puede ser asociado reglas de NAT o marcas del mangle para más tarde dar un tratamiento específico a dichas direcciones dentro del Router, el address-list puede ser creado de forma automática por medio de servicios de red como Hotspot, DHCP, Radius o PPP Profile. Para hacer uso de la lista de dirección dirigirse en Winbox a la opción

IP >> Firewall >> Address–List. (Add), basta con asociar la IP(s) a la lista para su posterior tratamiento.

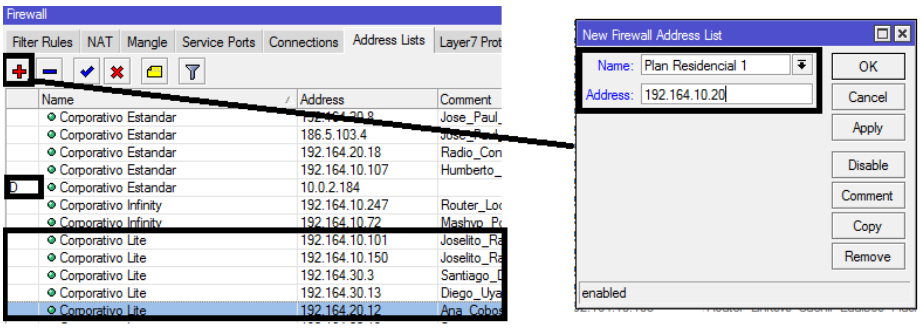


Figura 4.48. Ventana para agregar IP en Address-list

Fuente: Los Autores, Ventana de agregación IP en Adress-list, 2013

4.3.10 VPN y Concentradores de VPN

Por razones de soporte y mantenimiento sobre la red deseada de la empresa Sigsignet, y al tener diversas redes independientes y autónomas que necesitan tener un control centralizado y en vista de la necesidad de acceso continuo a la misma 24 horas del día 7 días de la semana, el uso de VPN para dichas tareas es administración se consolida como una solución de vital importancia, RouterOS para tal da soporte a una serie de protocolos para "tunneling" que van desde Open VPN, L2TP, SSTP, PPTP e IPSec, algunos de los cuales operan tanto en capa 2 otras sobre capa 3, de los cuales L2TP y para el caso en particular de la empresa Sigsignet es el protocolo elegido no solo porque incorpora menos jitter sino por el poco consumo de recursos de Hardware, siendo posible agregar a futuro sobre la misma cifrado de tipo IPSec protegiendo aún más dichas conexiones en el caso de ser requerido, por tal se considera el siguiente escenario de la empresa.

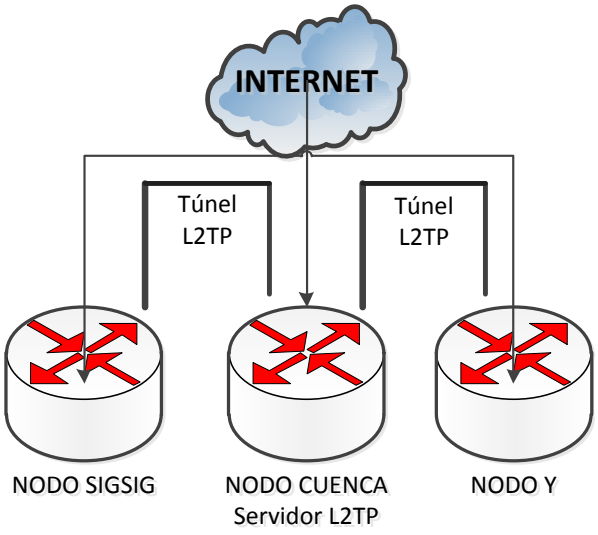


Figura 4.49. Topología de Túneles VPN para le Empresa Sigsignet

Fuente: Los Autores, Topología de Túneles VPN, 2013

El proceso de configuración sobre RouterOS se da de la siguiente forma.

Se establecen las credenciales de acceso, utilizando Winbox dentro de la opción Secrets, en tanto desde el lado del Servidor basta con habilitar el servicio, y los clientes que establecen la conexión al servidor es necesario crear una interface

cliente L2TP desde Winbox dentro de la Opción PPP, indicando la IP a la cual se va a realizar el marcado así como su usuario y contraseña previamente establecidos.

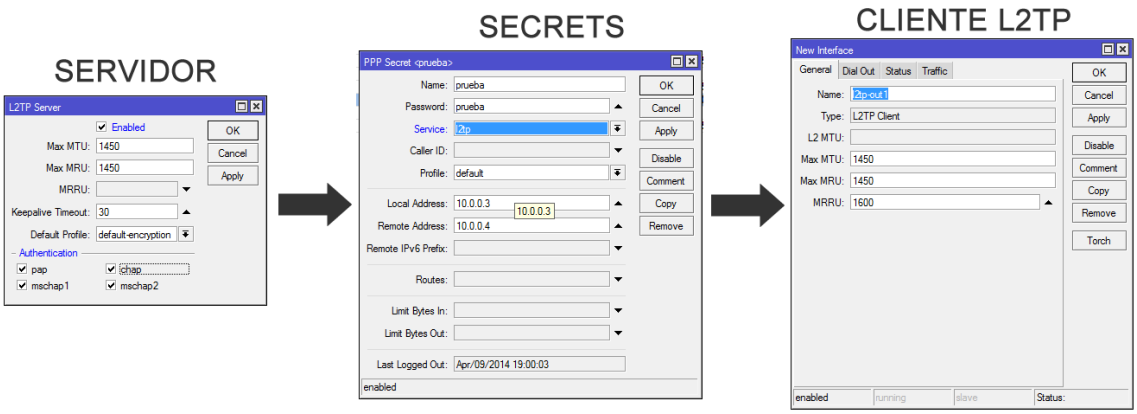


Figura 4.50. Proceso de configuración de Túnel L2TP.

Fuente: Los Autores, Configuración de Túnel L2TP, 2013

4.3.11 Herramientas esenciales de análisis Mikrotik.

Las herramientas de análisis de red son imprescindibles dentro de RouterOS y cualquier dispositivo equipado para tareas y servicios sobre una red de datos, a tal punto que nos permiten no solo evaluar el comportamiento de la red sino su rendimiento general en sí, y porque no detectar falencias sobre la misma e inclusive mitigar las mismas.

4.3.11.1 Ping.

El protocolo ping que viene del acrónimo Packet Internet Groper, permite evaluar el estado de conexión entre un host local y un remoto, o dentro de un grupo de host, haciendo uso de paquetes ICMP siendo estos de solicitud o respuesta; en ámbito de Networking dicho protocolo es sumamente utilizado ya que permite no solo determinar la calidad de una red de datos sino además el estado y la velocidad.[33]

Dentro de RouterOS se implementa dicha utilidad con algunos parámetros disponibles como son los siguientes:

[33] UTN, Facultad Regional la Plata-Argentina, Comandos de Red, 2005, p 1, www.frlp.utn.edu.ar/materias/redesdeinformacion/tp4red.doc

Desde Winbox nos dirigimos a Tools >>> Ping

Donde podremos visualizar la venta de ping con dos vistas diferentes la primera Pestaña General donde disponemos de todos los parámetros esenciales durante tareas de prueba de conectividad, en donde poder encontrar los siguientes parámetros escenciales en las tareas de gestión y administración:

- Ping To: Especifica la dirección IP en capa 3 o MAC Address del host a evaluar conectividad si se desea evaluar conectividad en capa 2.
- Interface: La interfaz física o virtual por la que vaya a realizarse la prueba de conectividad no es necesario seleccionar la misma ya que puede quedar por defecto como esta, salvo ciertos casos como el uso de ARP Ping.
- ARP Ping: Opera sobre capa 2 y capa 3 sobre modelo OSI, utilizando adicionalmente ARP para sondear los Host, siendo de mucha utilidad para la detección de IP`S duplicadas.
- Packet Size: Se define como el tamaño del paquete utilizad para evaluar conectividad.

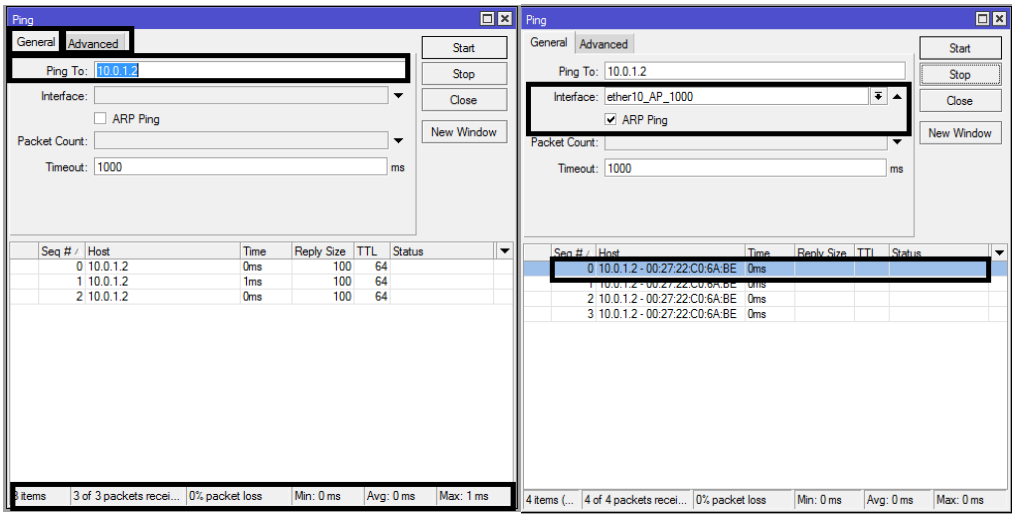


Figura 4.51. Herramienta Ping dentro de RouterOS.

Fuente: Los Autores, Ventana de Test Ping Mikrotik, 2013

Otra variante que utiliza ICMP dentro de sus herramientas y ping en si hablando generalmente dentro de RouterOS, se denomina “Ping Speed”, accesible desde Winbox desde Tools >>> Ping Speed; nos permite evaluar el ancho de banda ICMP o velocidad de ping que permite evaluar el rendimiento hacia cualquier equipo remoto y poder determinar con el mismo cuellos de botella presentes en la red.

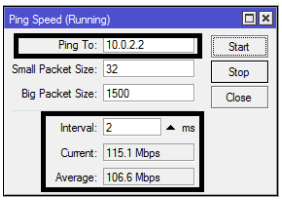


Figura 4.52. Herramienta para prueba velocidad de Ping RouterOS “Ping Speed”

Fuente: Los Autores, Ventana de Test Ping Speed, 2013

Así también dentro de las herramientas Winbox nos podemos encontrar con la opción Flood Ping que envía paquetes ICMP aleatoriamente a un servidor remoto, al igual que los anteriores con la única variante que tan pronto recibe una respuesta envía la siguiente solicitud, incluso con fines de saturar una línea de comunicación con un número excesivo de paquetes ICMP suficientemente grandes, causando una degradación de los servicios prestados por otros protocolos, la herramienta tiene fines netamente de evaluación mas no su creación se orienta a tareas de saturación o para ataques mal intencionados.

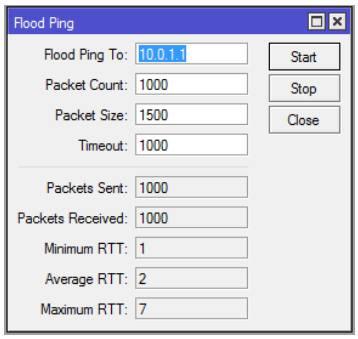


Figura 4.53. Herramienta Flood Ping RouterOS

Fuente: Los Autores, Ventana de Test Flood Ping, 2013

4.3.11.2 Torch

Es una herramienta parametrizable incluida dentro de RouterOS destinada a monitorizar el tráfico en tiempo real o controlar el flujo de tráfico a través de una Interfaz, pudiendo mostrar las tasas de datos de TX/RX y total de paquetes gestionados para las mismas, incluso por Interfaz o protocolo; Dentro de un proveedor de servicio de Internet es ampliamente usando tanto como método de evaluación y determinación de consumo de ancho de banda e incluso la determinación de problemas orientados a conexión, conexión sospechosas asociadas, e incluso la posibilidad de determinar el consumo que se genera tanto entre una IP de origen como una IP de destino, y los diversos puertos y protocolos usados generados en dicha conexión, obteniendo estadísticas puntuales.

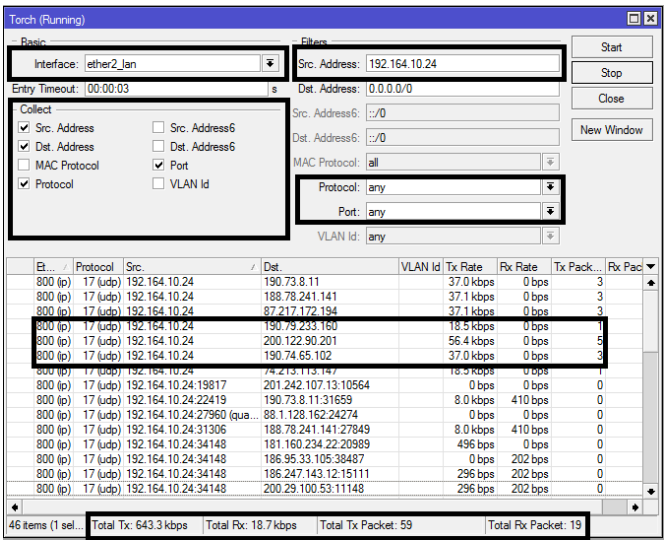


Figura 4.54. Herramienta Torch Monitorización Ancho de Banda en RouterOS.

Fuente: Los Autores, Ventana de Monitor de Consumo "Torch", 2013

4.3.11.3 BTEST Server

Una herramienta desarrollada por Mikrotik e incluida en RouterOS que permite entre equipos del mismo tipo, realizar una evaluación o test de ancho de banda y determinar una capacidad aproximada de tráfico a ser manejado por el medio de interconexión o los equipos en sí, cabe recalcar que si tenemos de por medio una segmentación de ancho de banda previamente configurada, para el caso de pruebas

remotas haciendo uso de enlaces contratados este test reflejara el rate máximo contratado mas no la velocidad del medio soportada o procesado por equipos RouterOS.

Para tal efecto es necesario activar dentro de Winbox dirigirnos a la pestaña Tools >>> BTest Server donde existen dos opciones que podemos seleccionar la primera "Enable" permite actuar a dicho dispositivo como servidor para pruebas de Ancho de Banda locales como remotas y el segundo parámetro "Authenticate", que permite que desde la opción Bandwidth Test sea necesario para realizar la prueba de ancho de banda introduciendo antes un usuario y contraseña, realizado ello desde el cliente se podrá dirigir al botón sessions y poder divisar todas las sesiones actuales que en ese momento estén realizando una prueba o test de ancho de banda hacia el servidor.

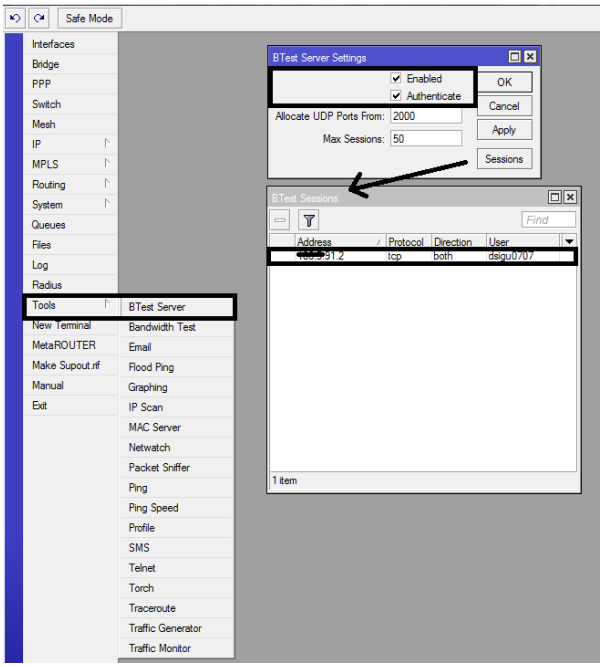


Figura 4.55. Herramienta Servidor de Prueba de Ancho de Banda (BTest Server)

Fuente: Los Autores, Herramienta Banwidth Test Server, 2013

4.3.11.4 Graphing

Es una herramienta dedicada a la generación de gráficos estadísticos para la monitorización de determinados parámetros en RouterOS, pudiendo mostrar desde los niveles de voltaje, temperatura, hasta gráficos de estadísticas de tráfico asociadas por interfaces o por colas simples, su estructura consta de dos partes, donde la primera parte recoge la información y datos afines y luego son procesados para ser mostrados en una interfaz web accesible desde http://[direccion_ip_router] /graphs/, es importante mencionar que si el puerto por defecto al 80 es cambiando desde Winbox en la opción IP >>> Services; será necesario para acceder a dichos gráficos establecer la dirección IP del Router acompañado de dos puntos y el puerto por donde está corriendo el protocolo "www" quedando de la siguiente forma por ejemplo:

http://10.0.1.2:8082 /graphs/ o en su defecto con el puerto 80 habilitado.

http://10.0.1.2 /graphs/

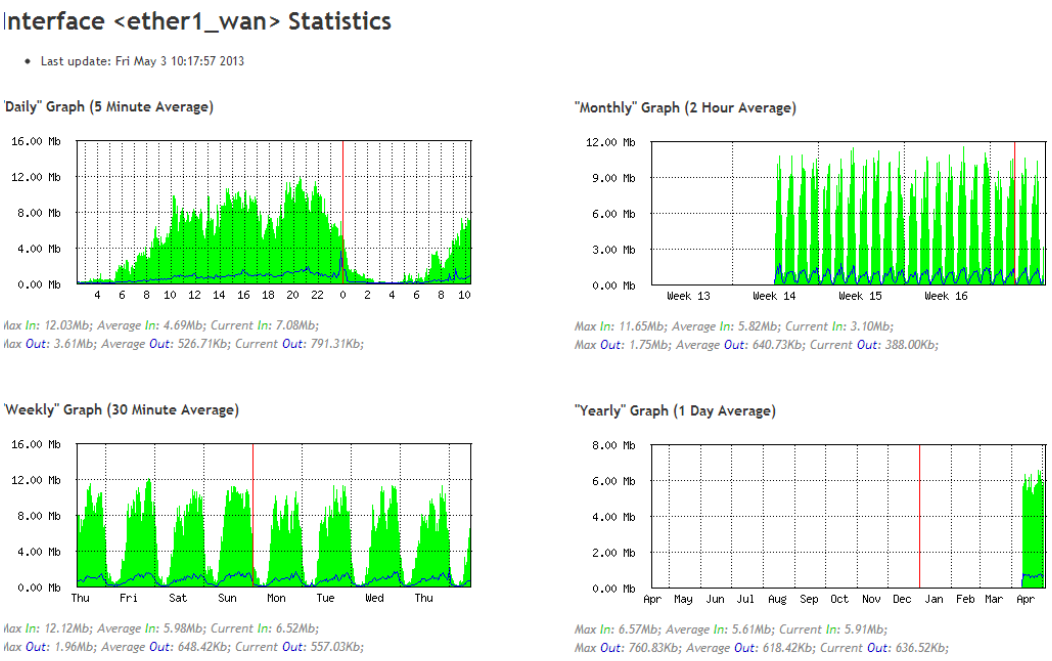


Figura 4.56. Generación de gráficos estadísticos de tráfico por Interfaz en RouterOS.

Fuente: Los Autores, Herramienta Graphs Mikrotik, 2013

Como se puede observar en la figura anterior dichos gráficos son de gran utilidad en el ámbito de monitorización ya que se pueden divisar estadísticas puntuales que colaboran en una administración de la red óptima.

4.3.11.5 Bandwith Test.

Utilizada en complemento con Bandwith Server, es el cliente encargado de evaluar el troughput de un enlace o entre equipos RouterOS, para realizar dicho procedimiento es necesario ingresar la IP del Servidor de Test de Ancho de Banda remoto, el protocolo con el cual se va a evaluar siendo este TCP o UDP, y como se mencionó en el punto anterior si en el servidor Test esta activada la opción authenticate ingresar usuario y password para realizar el test caso contrario no se realizara la misma, además es importante determinar la dirección de prueba tanto como paquetes enviados, o solo recibidos o incluso bidireccional, siendo posible en dicho test la opción para limitar la velocidad de la prueba, en el caso de querer evaluar anchos de banda especifico.

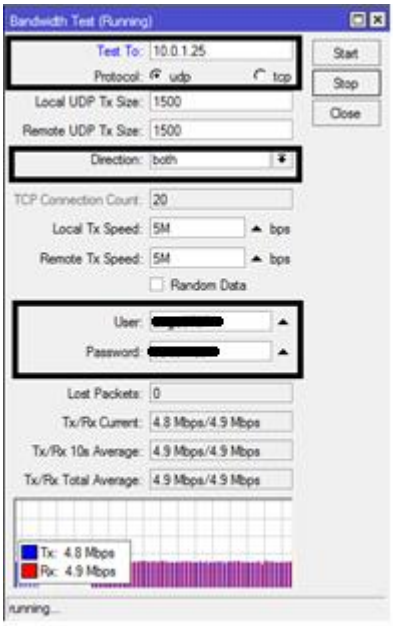


Figura 4.57. Cliente de Prueba Bandwith Test.

Fuente: Los Autores, Herramienta Bandwidth de Test, 2013

4.3.11.6 Netwatch.

Es una herramienta destinada a monitorizar el estado de los dispositivos de red, a través del uso del protocolo ICMP o ping, a una dirección IP o direcciones previamente especificadas, siendo posible ejecutar comandos o scripts en el caso de determinado evento, además es esencial para que dicha herramienta funcione bien, establecer el intervalo de tiempo para envió de los paquetes ICMP, sus comandos adicionales se los detallan en los capítulos posteriores, es importante además mencionar que se consideran dos estados de identificación cuando se levanta una regla Netwatch que son:

Up: Cuando el host o dispositivo de red está respondiendo a los paquetes ICMP, es decir el mismo está activo,

Down: Es el contrario al punto anterior aquí se entiende que el host esta caído y no tiene comunicación.

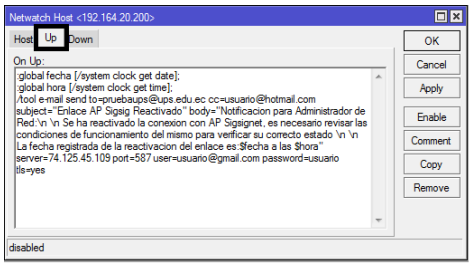


Figura 4.58. Inserción de Script en Herramienta Netwatch.

Fuente: Los Autores, Herramienta Netwatch, 2013.

Por tal dentro de cada estado podemos especificar algún comando de RouterOS, tal como por ejemplo se envié un mail indicando el estado o un sms, o a su vez incrustar el uso de scripts.

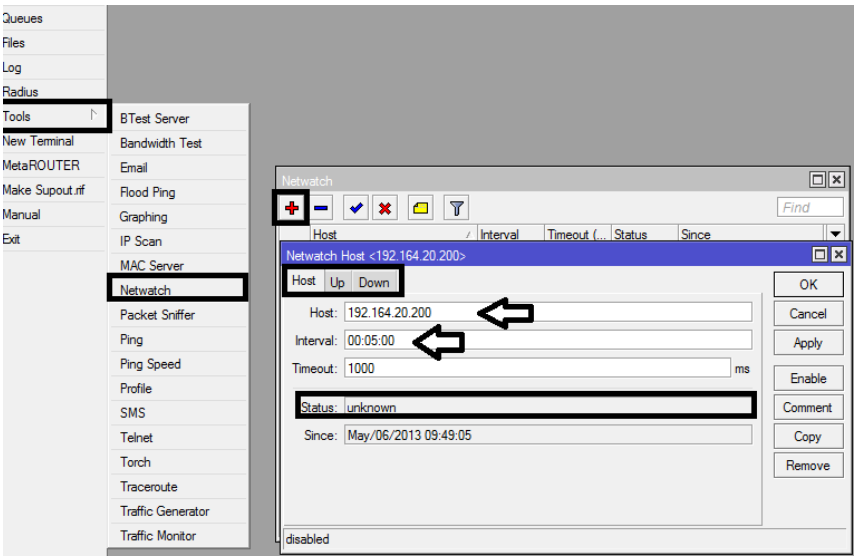


Figura 4.59. Herramienta Netwatch para monitorización de Host o Dispositivos de Red.

Fuente: Los Autores, Ventana de Monitorización de Host Mikrotik, 2013

4.3.11.7 Telnet

El uso de telnet como protocolo cliente / servidor de administración remota en RouterOS aún tiene vigencia a pesar de mejores y más seguras opciones como SSH, por defecto utiliza el puerto 23 bajo el protocolo TCP, su habilitación, uso e incluso protección contra accesos no autorizados la podemos parametrizar desde winbox dirigiéndonos a IP >>> Services; donde encontraremos todos los protocolos listados para administración o conexión Remota contra el Router siendo posible incluso cambiar o alternar el número de puerto y las IP o rango de IP's autorizadas para realizar dicha conexión, pudiendo considerarse como un método seguro de nivel medio para autorizar y de cierta forma proteger el uso de determinado puerto y servicio corriendo por el mismo a determinada IP.

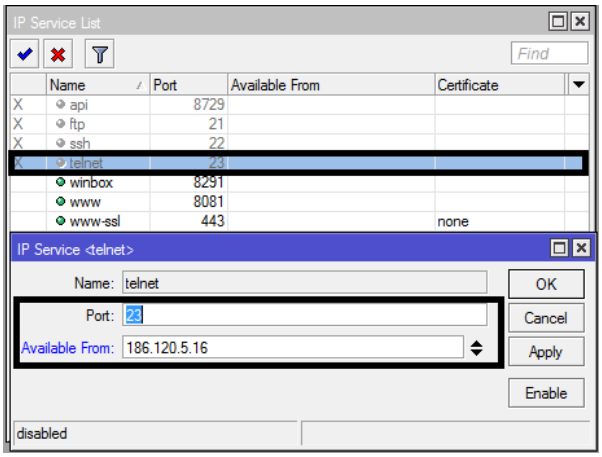


Figura 4.60. Lista de Servicios Disponibles en RouterOS para conexión Remota.

Fuente: Los Autores, IP Service List Mikrotik, 2013

4.3.12 Servicios y Procedimientos Básicos en RouterOS

Los servicios y procedimientos básicos a configurar en RouterOS son procedimientos iniciales de vital importancia para otorgar una funcionalidad básica al dispositivo, y que permiten asegurar un funcionamiento óptimo.

4.3.12.1 NTP Server

Su instalación dentro de RouterOS se la realiza como un paquete separado para tal es necesario antes que nada descargar el mismo y agregar a la pestaña files dentro de Winbox tan solo con arrastrarlo, su habilitación dentro de RouterOS es sencilla, una vez descargado el paquete es necesario reiniciar al Router para su respectiva habilitación y luego basta con seleccionar en la pestaña Enable y el servidor NTP estará ya disponible para su respectivo uso, respondiendo a peticiones NTP luego con la fecha y hora del Reloj, dentro de los proveedores de Internet Inalámbricos es ampliamente usada ya que permite como tal setear el reloj y fecha de los Puntos de Acceso, permitiendo a los mismos mantenerlos sincronizados no solo para tareas de mantenimiento sino análisis de logs y afines.

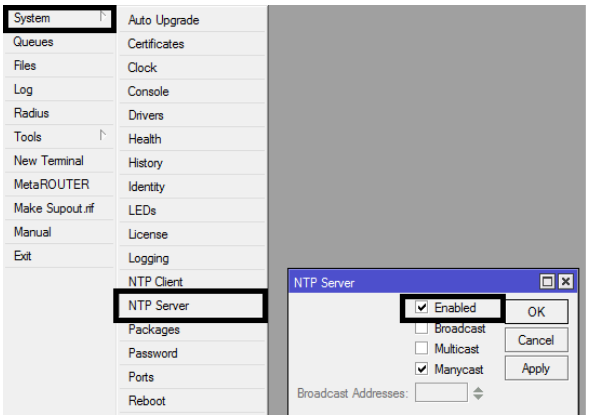


Figura 4.61. Habilitación Servidor NTP en RouterOS

Fuente: Los Autores, Ventana de Habilitación NTP Server, 2013

4.3.12.2 Administración de Paquetes

Es un punto muy relevante dentro de RouterOS como tal ya que permite la habilitación de determinadas funciones que utiliza el sistema de paquetes como de servicios de red e incluso la desinstalación completa de los mismos, siendo posible también el poderlos bajar de versión en caso de problemas de bugs con versiones actuales, generalmente algunos de los paquetes se instalan vienen precargados en el caso de las RouterBoards por defecto pero en el caso de arquitecturas x86 es posible determinar que paquetes durante la instalación serán configurados y utilizados, además existen paquetes como el Wireless que funciona específicamente sobre RouterBoard y en x86 sobre determinados chips Wireless como por ejemplo Atheros.

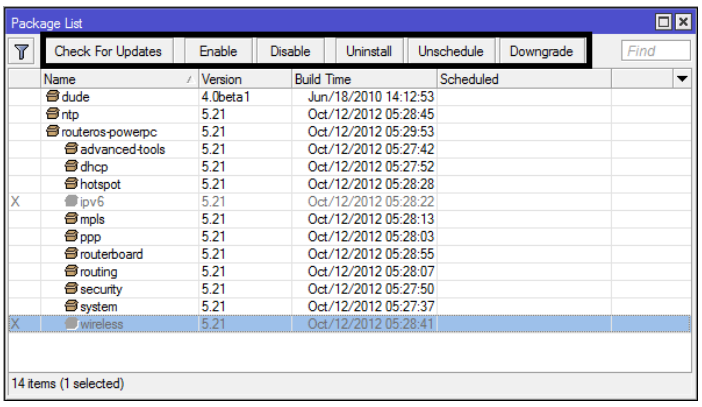


Figura 4.62. Administración de paquetes sobre RouterOS

Fuente: Los Autores, Administración de paquetes sobre RouterOS, 2013

Es posible realizar una actualización de paquetes directamente desde la Opcion Check For Updates, y establecer todos los paquetes a la última versión disponible directamente desde Mikrotik, teniendo una vista de un completo changelog y su historial de cambios, por versión.

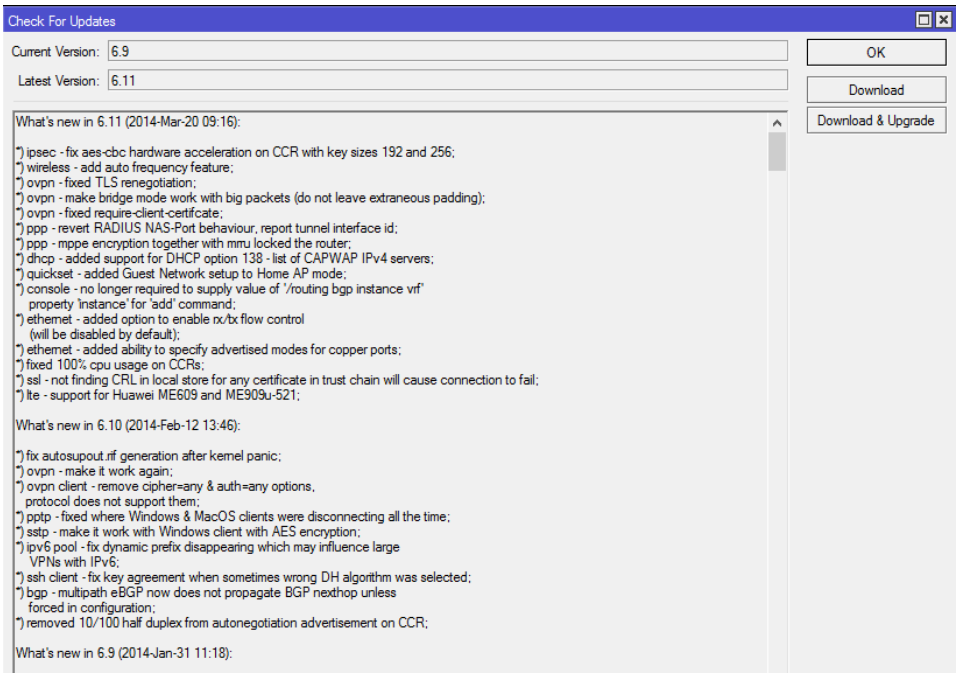


Figura 4.63. Ventana de Revisión de Actualizaciones de RouterOS.

Fuente: Los Autores, Administración de paquetes sobre RouterOS, 2013

4.3.12.3 Administración de Backups del Sistema

La gestión y administración de Backup en el sistema son procedimientos esenciales y extremadamente útiles que permiten mantener copias de respaldo de configuraciones sobre archivos binarios realizadas dentro RouterOS, dichas configuraciones pueden ser de tipo globales donde se realiza una copia de todo el sistema en si o específicas donde se puede realizar copias solo de determinados servicios de red en RouterOS como firewall, Nat etc., y que a futuro en el caso de averías de los equipos nos permiten recuperar dichas configuraciones inmediatamente.

Los archivos pueden ser descargados por medio de un servidor FTP o por medio de Winbox y su gestor de archivos, incluso existe la posibilidad de automatizar dichas tareas por medio de scripts y enviar a correos electrónicos o concentrarlos directamente en un servidor de archivos.

Para elaborar un Backup General de todo el Sistema dirigirse a la Opción Files y dar clic en el Botón Backup, donde se generará un nombre asociado a la identidad del Router y cuya extensión será .backup

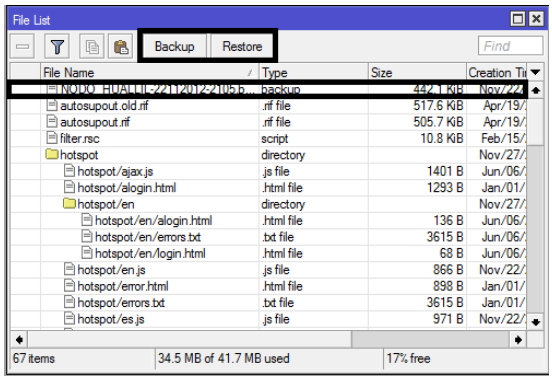


Figura 4.64. Ventana de administración de Archivos y Backup General de RouterOS

Fuente: Los Autores, Administración de archivos y Backup en Mikrotik, 2013

Para el caso de backup de configuraciones específicas abrir un Shell o consola puede ser ésta desde winbox, donde se ubica con el promp al servicio de red al cual se pretende sacar el Backup para este ejemplo se va a realizar un backup del Firewall por tal la sentencia se determina usando el comando export y definiendo un nombre al archivo a exportarse, el mismo se genera con una extensión .rsc

```
[admin@NODO_HUALLIL] > ip firewall filter export file=Firewall_Huallil_2013
```

Una vez generado el archive de respaldo el mismo puede ser guardado dentro de una PC o algún lugar seguro, para tal basta solo con arrastrar desde Winbox el mismo a otra ubicación.

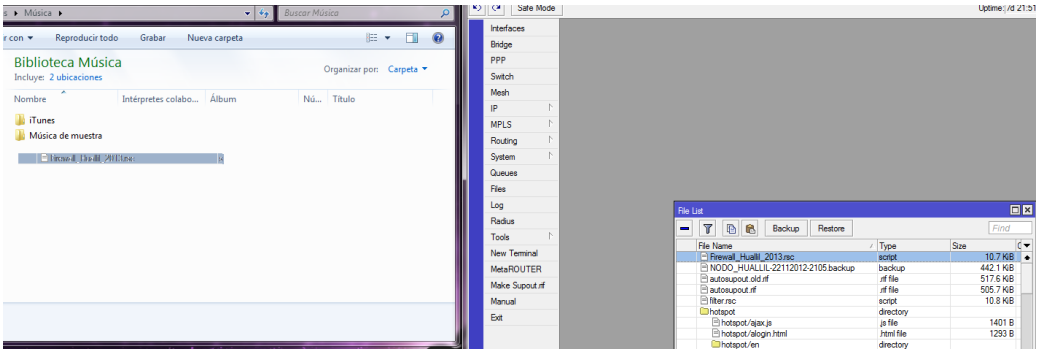


Figura 4.65. Generación de Backup específicos en RouterOS.

Fuente: Los Autores, Gestión y Almacenamiento de Backup en Mikrotik, 2013

4.3.12.4 Scheduler.

Scheduler o mejor conocido como planificador, es una herramienta que permite la ejecución de comandos RouterOS o scripts previamente elaborados, en determinadas fechas de inicio, horarios e intervalos, los mismos son agendados para ser ejecutados posteriormente o en un momento determinado, se establece un contador que permite registrar el número de veces que un script o determinado grupo de comandos agendados ha sido ejecutado por scheduler, el mismo se restablece a cero cada vez que el Router se reinicia, además si más de un secuencia de comandos se debe ejecutar de forma simultanea los mismos se ejecutan en el orden establecido o secuencialmente, o a su vez directamente desde un script, los proveedores de Internet inalámbrico pueden destinar varios usos tales como el reinicio de determinados equipos para obtener mejor perfomance a determinadas horas, o incluso la alteración de otros parámetros en RouterOS como cambio de valores en cuotas de simples para segmentación de ancho de banda en diferentes horas del día, también cada tarea a realizarse utilizando scheduler se puede definir políticas de ejecución por determinado script o grupo de comandos tales como que se evite la ejecución de determinados comandos que puedan comprometer el buen funcionamiento del Router, o el cambio de password etc.

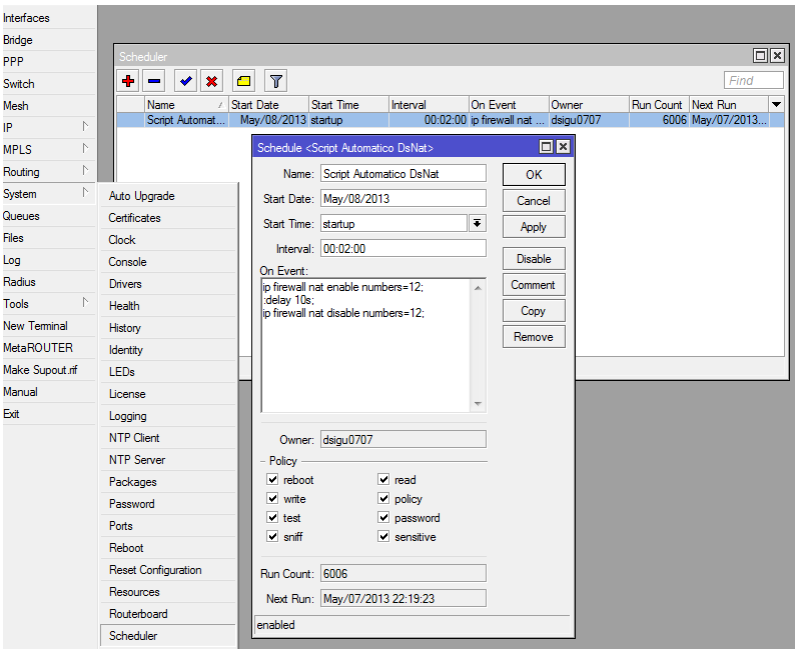


Figura 4.66. Herramienta Planificador de Tareas "Scheduler" en RouterOS.

Fuente: Los Autores, Gestión de Tareas en Mikrotik, 2013

4.3.12.5 Profile y actividad del Sistema

Es importante en todo sistema tener estadísticas y datos puntuales sobre la actividad del mismo, y sus diferentes procesos y servicios en ejecución, y como estos se encuentra siendo utilizados por el Hardware, en muchas veces son indicadores claros para detectar anomalías de mal funcionamiento o posibles ataques tales como DoS, o DDoS que estén haciendo mal uso de los recursos o sobrecargándoles, incluso posibles malas configuraciones sobre RouterOS que impiden un buen funcionamiento sobre el mismo.

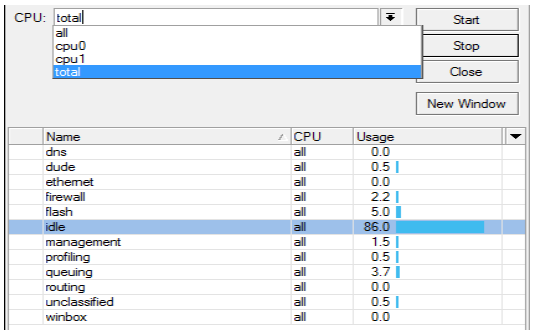


Figura 4.67. Ventana de Profile en RouterOS

Fuente: Los Autores, Gestión de uso de recursos con herramienta Profile, 2013

En la captura anterior se puede visualizar claramente el nivel de uso de CPU y su porcentaje de consumo por cada servicio en ejecución, incluso en el caso de que este pueda manejar varios Cores dentro del mismo CPU, se puede ejecutar la herramienta profile y evaluar el consumo por cada core en la CPU presente.

4.3.13 Administración de Usuarios.

La gestión de los usuarios en RouterOS debe ser considerada como un punto muy relevante, ya que son los usuarios a quienes se les permitirá el acceso al Router con los privilegios asignados, por defecto RouterOS viene sin contraseña y su usuario es admin, por lo tanto uno de los primeros procedimientos a realizar es el cambio del nombre de usuario y luego la asignación de un password para esto se lo hace de la siguiente forma:

```
[admin@NODO_HUALLIL] > user add name=usuarioups password=prueba123 group=full disabled=no
```

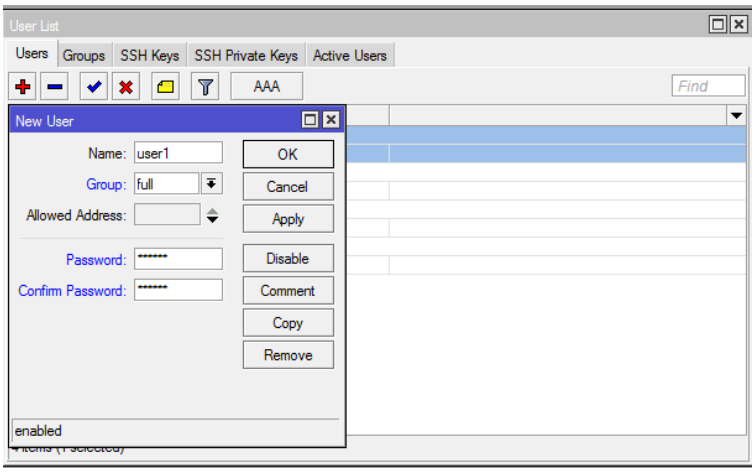


Figura 4.68. Creación de usuarios y grupos en RouterOS.

Fuente: Los Autores, Gestión de grupos y usuarios en RouterOS, 2013

Para el ejemplo se ha creado un usuario "usuarioups" con todos los privilegios de administrador, y asignado al grupo por defecto creado por RouterOS denominado Full, que dispone de acceso total al Router, cabe mencionar que agregar un usuario

por consola puede representar un problema ya que el password no tiene medida de protección visual aunque internamente la misma es encriptada, así también siendo posible su modificación, des habilitación o eliminación, es recomendable para mantener un orden y una escala de privilegios, y más que nada si existen diferentes usuarios que no se necesiten disponer de un acceso total se pueda configurar grupos con diferentes políticas de acceso, tales como a determinados grupos de usuarios darles acceso en Full en tanto a otros que no requieran elevados niveles de privilegios asignarlos a grupo con políticas solo de lectura mas no de escritura, o de acceso por medio del web mas no de winbox, e incluso con la posibilidad de no cambiar passwords, por tal se pueden considerar 3 tipos de grupos por defecto Full, lectura, y escritura, los cuales pueden determinadas políticas del sistema como Reboot, que como su nombre lo dice se asigna la potestad para reiniciar al Router, o sniff que permite a los usuarios a la detección de paquetes.

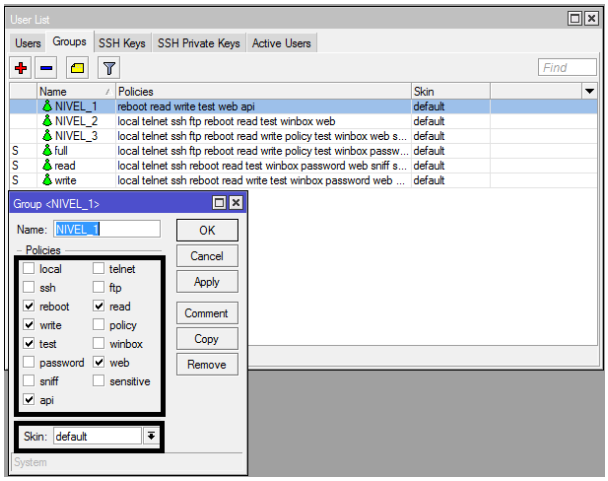


Figura 4.69. Asignación de Políticas de conexión de usuarios por Grupos

Fuente: Los Autores, Gestión de Políticas de conexión de usuarios en RouterOS, 2013

Además en el caso de usuarios inexpertos existe la posibilidad de personalizar la administración del Router por medio del web para ello definiendo skin, mismos donde se puede establecer que parámetros podrán ser visibles cuales se ocultaran e incluso personalización a nivel de nombres de campos ya que por defecto la administración web opera sobre idioma Inglés como lengua establecida mas no otros idiomas, por ende para realizar ello lo primero que debemos hacer es con privilegios

Full acceder a la administración web o "webfig" por medio de la IP introducir el usuario y password y una vez ahí dirigirnos a la opción Desing Skin.

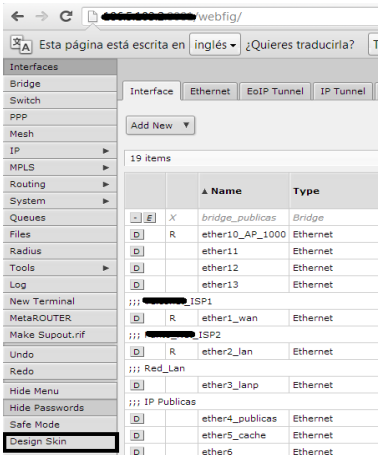


Figura 4.70. Diseño de Skin personalizados por medio de Webfig.

Fuente: Los Autores, Diseño de Skin personalizados en RouterOS, 2013

Al Dar Clic sobre el Diseño de Skin, todos los botones y texto asociado podrá ser alterado o incluso omitido para el diseño de ese skin basta con seleccionar o deseleccionar de la lista, mismo que al terminar su edición deberá ser guardado con un nombre respectivo y luego desde Winbox o por consola asociado al grupo de usuario que hará uso de dicha plantilla.

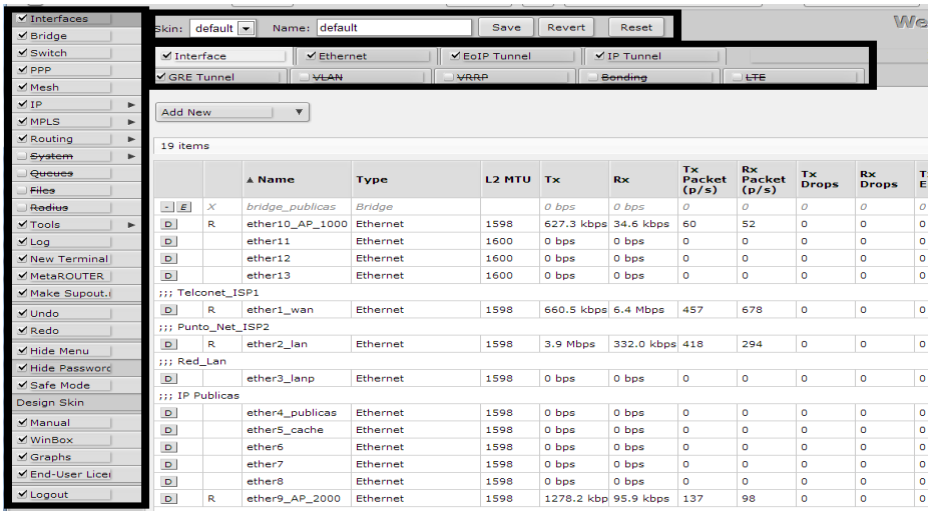


Figura 4.71. Diseño de Skin personalizados por medio de Webfig.

Fuente: Los Autores, Habilitación de campos en Webfig y personalización de plantilla, 2013

Toda la administración puede ser altamente personalizable como se mencionó hasta tal punto de cambiar el idioma o incluso los encabezados textualmente por lo que se desee poner.

Figura 4.72. Opción para Edición de Lenguaje en WebFig

Fuente: Los Autores, Personalización de idioma en Webfig, 2013

Dejando un Skin de administración prácticamente con solo herramientas y nombres personalizados para determinado grupo de personas y una administración y orientación puntual.

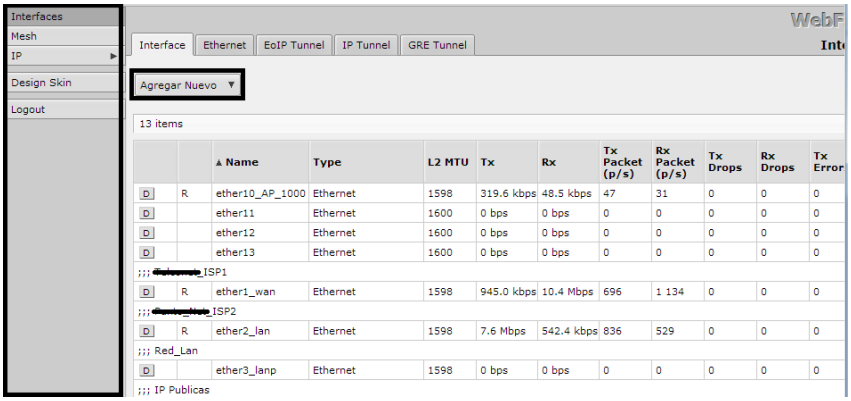


Figura 4.73. Vista del Skin terminado en Webfig.

Fuente: Los Autores, Modelo de Skin Personalizado, 2013

Finalmente como se mencionó en el párrafo anterior solo resta desde winbox asignar al grupo de usuario al respectivo skin.

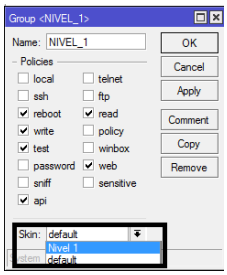


Figura 4.74. Asignación del Skin al Grupo Respectivo.

Fuente: Los Autores, Asignación de Skin a usuario para acceso por vía Web, 2013

Además para control de conexión sobre el Router el mismo dispone de un control de conexiones sobre el mismo, pudiendo especificar via de conexión del usuario, grupo asignado, y vía de conexión si por ejemplo el mismo de Winbox, Web, Api, Ssh etc.

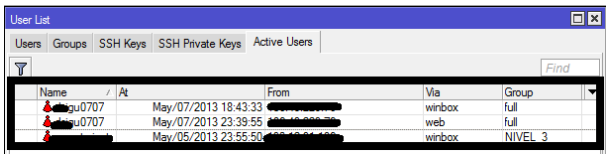


Figura 4.75. Vista de Usuarios Activos en Winbox y su forma de conexión.

Fuente: Los Autores, Vista de Usuarios activos conectados, 2013

Y finalmente dentro de este punto se encuentra el uso de claves SSH para autenticar sesiones sin necesidad de utilizar un nombre de usuario y contraseña, para tal es necesario disponer de un archivo de clave previamente generado y luego impórtalo haciendo uso de la opción Files en Winbox o a su servidor FTP embebido en RouterOS.

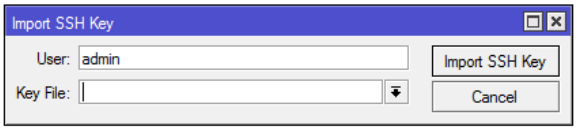


Figura 4.76. Ventana de importación para llaves Públicas y Privadas SSH.

Fuente: Los Autores, Importación de llaves Publicas y Privadas en SSH, 2013

4.3.14 Manejo y Administración de Seguridad en la red

La seguridad dentro de un WISP es un ámbito esencial por distintos motivos, evitar el uso no autorizado del servicio, la protección a clientes finales, el control de

accesos no autorizados a la infraestructura del proveedor, medidas preventivas y correctivas contra ataques, deberían ser consideradas cuando se requiere proteger una red de datos, por tal el hecho de que un proveedor de Internet pueda brindar un servicio de calidad con un nivel de seguridad adecuado es elemental.

Hoy en día la seguridad se ha convertido en tema de gran polémica no porque no se pueda brindar sino porque es complicado definir políticas que pueda abarcar y controlar casi cualquier amenaza.

Las primeras políticas deberían centrarse en el ámbito inalámbrico que es el primer camino que un atacante dentro de un WISP podría centrarse para obtener un acceso no autorizado a la red, una forma de mitigar ello es haciendo el uso de encriptación segura y no descifrable como en el caso de por ejemplo, en el estándar 802.11, hacer uso de cifrados tipo WPA WPA2 – PSK con cifrados del tipo aes (Advanced Encryption Standar), también se debe considerar que cifrados demasiadamente elevados o poco adecuados puede causar los puntos de acceso tiene a causar pérdidas de perfomance ya que el mismo emplea gran porcentaje de CPU para dichas tareas por tal es necesario usar un cifrado adecuado, además el mismo podría verse complementado mediante el uso de un servidor Radius (Remote Authentication Dial-In User Server) como factor de autentificación e incrementando aún más el nivel de seguridad.

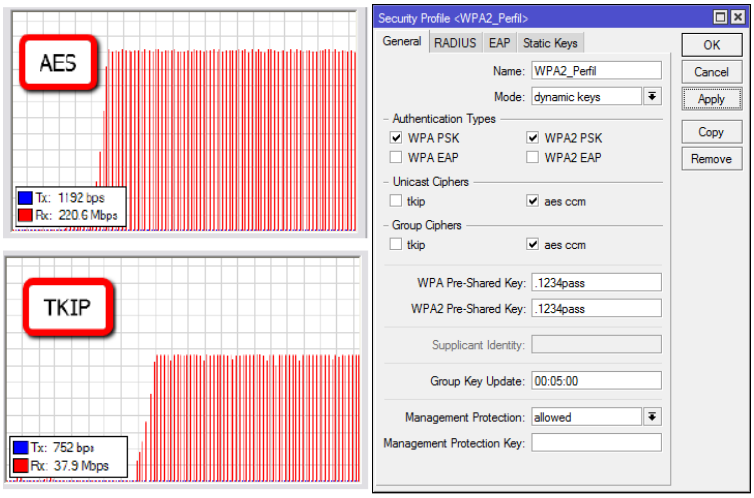


Figura 4.77. Modelo de Cifrado y velocidad 802.11 con encriptación.

Fuente: Los Autores, Velocidad de transmisión con cifrado AES y TKIP, 2013

Además determinadas configuraciones deben estar seteadas en RouterOS sobre la interfaz inalámbrica para dar un agregado más de seguridad, aunque parecieran a simple vista insignificante es de suma importancia, antes que nada nos dirigimos a la configuración de la interfaz Wireless desde Winbox es necesario deshabilitar el Default Authenticate para que solo puedan autenticar clientes existentes en la lista de acceso y como tal poder validar la conexión utilizando la MAC del mismo y Default Forward para que no pueda haber forwarding entre los clientes, además algo recomendable se orienta a ocultar el SSID de la red, para que no pueda ser visible ante demás dispositivos que operen sobre la misma Banda, para ello se puede hacer uso del parámetro Hide SSID, cuando se activa NV2 (NStreme Version 2) protocolo propietario de Mikrotik dicho parámetro es ocultado ya que por defecto las redes sobre el protocolo NV2 son solo visibles entre las mismas.

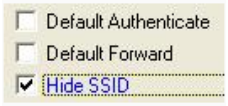


Figura 4.78. Check para ocultar el SSID en RouterOS

Fuente: Los Autores, Opción para ocultar SSID en RouterOS, 2013

Después se pueden empezar a registrar las direcciones MAC a las que se quiera dar acceso en el caso de clientes autorizados, en la pestaña Access List se empieza a crear las entradas.

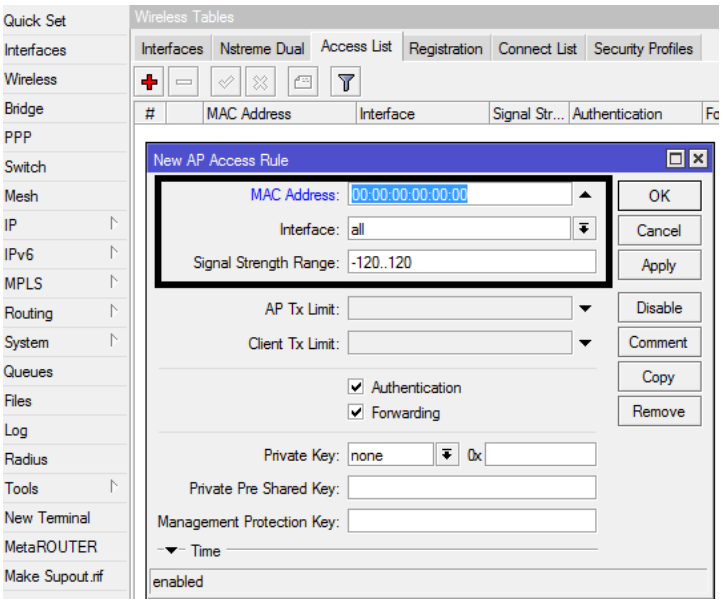


Figura 4.79. Lista de Control de Acceso Wireless en RouterOS

Fuente: Los Autores, Reglas de Control de Acceso RouterOS, 2013

Una vez registrada cada entrada asociada a un usuario autorizada también es posible definir parámetros de conexión tales como autorizar solo a ciertos usuarios con un numero de señal especifico y desconectar a usuarios con mala que puedan causar conflictos en performance del punto de acceso y clientes con buena señal puedan resultar afectados, pero que en este punto no se ahondara sobre el mismo.

Otro método de seguridad establecido desde el CPE o cliente similar al Connect List, se le dice a la estación a que dirección física de un Access Point en particular se debe este conectar, es necesario como el punto anterior quitar la opción Default Authenticate, ya que el resto de opciones en modo estación o CPE no están habilitadas.

Figura 4.80 Check para quitar autentificación por Defecto Interfaz Wireless en RouterOS

Fuente: Los Autores, Desactivación Autentificación por Defecto RouterOS, 2013

Al agregar una entrada desde el CPE se tiene los siguientes parámetros, como por ejemplo porque Interface se realizará la conexión, la MAC Address del AP, el SSID del AP, incluso el nivel de señal como el caso anterior el protocolo asociado Wireless y definir un perfil de seguridad.

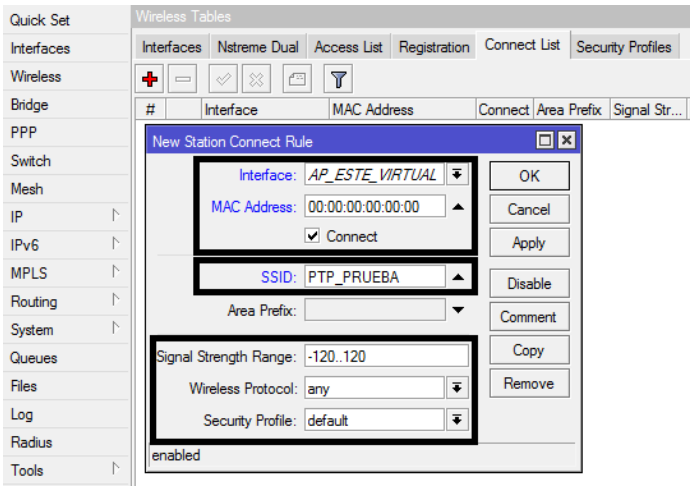


Figura 4.81. Lista de Connect List en RouterOS

Fuente: Los Autores, Lista de Conexión RouterOS, 2013

Ahora nivel inalámbrico se ha definido algunos métodos o barreras para asegurar la intrusión no deseada a la red, las redes de datos que ofertan los proveedores de Internet inalámbrico son la mayor parte Nateadas en muchos casos la configuración básica en Mikrotik es enmascarar todas las redes por defecto conectadas al equipo Mikrotik, generando así un problema de seguridad ya que cualquier red que se conecte tendrá acceso a Internet, una eventual solución ante ello fácil y practica es Natear Redes pero siempre y cuando están provengan de una dirección origen conocida.

Nat de red Básica:

```
[admin@NODO_HUALLIL] > ip firewall nat add chain=srcnat out-interface=ether1
action=masquerade
```

Nat de red con Dirección Src. Address:

```
[admin@NODO_HUALLIL] > ip firewall nat add chain=srcnat out-interface=ether1
action=masquerade src-address=192.164.10.0/24
```

Complementado con el Uso de un Firewall y las listas de direcciones de IP permiten establecer otro nivel de seguridad más, ya que por ejemplo se puede establecer que si una IP que no se encuentra en la lista de IP esta no estará autorizada a navegar y será bloqueado por el firewall, esto en el caso de que la asignación de IP sea estática o inclusive por DHCP, PPoE o hotspot.

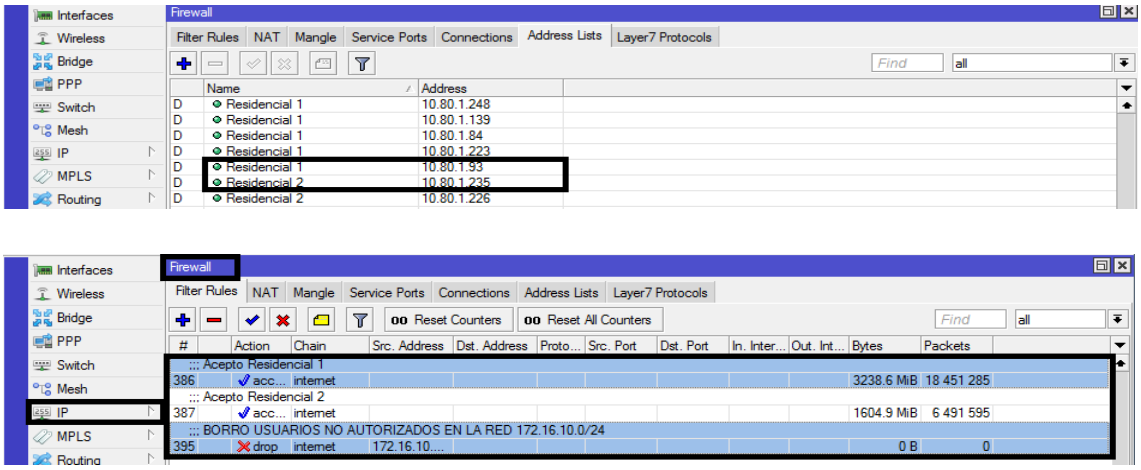


Figura 4.82. Permitir navegación de IP's por medio de listas IP.

Fuente: Los Autores, Regla Firewall para autorizar navegación usuarios, 2013

4.3.15. Manejo y administración de scripts RouterOS

En RouterOS es muy sencillo el manejo y administración de scripts los cuales sirven para automatizar algunas tareas que son necesarias, o que puedan en algún momento ser primordiales tenerlas. Para ello simplemente debemos ir al Menu System/Scripts, se abre la ventana de administración de scripts. Luego dar clic en el icono (+) y configurar la ventana con los datos que se desee que hacer el script.

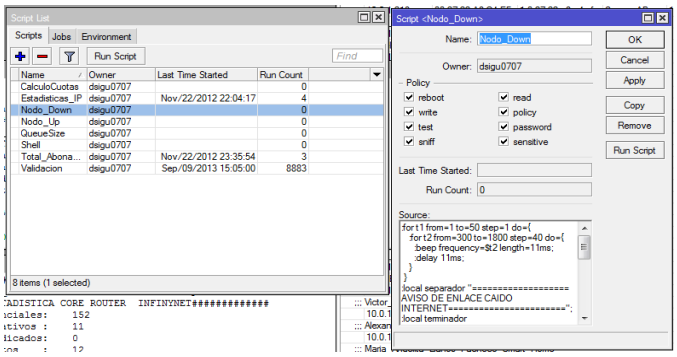


Figura 4.83. Ejemplo de configuración de Scripts.

Fuente: Los Autores, Ventana de configuración de Scripts RouterOS, 2013

4.3.16 Tareas de Mantenimiento

Como parte de las mejoras en la red de Sigsignet se debe tener previsto un mantenimiento periódico de la misma y esto se logra mediante la creación de un script el cual enviará una orden a todos los AP´s que se reinicien cada cierto tiempo para evitar la saturación de su memoria RAM y el sobrecalentamiento de su procesador. Esto ayudará a mejorar el rendimiento de la red y evitará que se inhiban los equipos.

También como parte del mantenimiento se creará un script que reinicie de manera automática el servidor de red RB1100AHx2 cuando este presente pérdidas de paquetes hacia el proveedor de manera constante, con el fin de descartar la probabilidad de que el fallo sea en el servidor.

Se realizarán envíos de mensajes hacia el correo electrónico y hacia el celular en caso de pérdida de conexión de algún equipo que funciona como AP o de algún otro servicio que sea prioritario.

4.3.17 RouterOS con NTOP.

Como ya se ha mencionado NTOP es un sniffer de Red, empleado en tareas de monitorización y destinado al análisis de protocolos, host, y cualquier aplicación que generen consumo de recursos de red, generando para tal gráficos estadísticos mediante una interfaz amigable, posibilitando un análisis a detalle de la red, su uso dentro de la red de la empresa Sigsignet contempla:

- Establecer un análisis detallado del tráfico de red.
- Informe de protocolos de red generados por cada host.
- Host que contactan con mayor frecuencia a servidores externos.
- Determinar host con consumos de tráfico sobre lo normal.

Por esto se establecen los siguientes pasos dentro de RouterOS para su integración con NTOP:

1.-Dentro de RouterOS es necesario habilitar Traffic-Flow en el Router, para reenviar así todo el flujo de trafico UDP.

```
[RouterOS@RouterUPS] > ip traffic-flow set enabled=yes
```

2.-Es necesario especificar una dirección IP y el puerto del host o servidor ntop que recibirá el flujo de tráfico (UDP) de estadísticas de paquetes generadas por el Router

```
[RouterOS@RouterUPS] > ip traffic-flow target add address=IP:2055 version=9
```

3.- Proceso similar a los puntos anteriores haciendo uso de Windox y digitando los siguientes parámetros, cabe recalcar que el parámetro versión es imprescindible para tal por Traffic Flow se denotan 3 versiones:

- **Versión 1.-**La primera versión de Formato de datos de Netflow, poco usada.
- **Versión 5.-**Posibilita la inclusión de BGP AS e información de numero de secuencia de flujo.
- **Versión 9.-**El nuevo formato y más extendido al momento

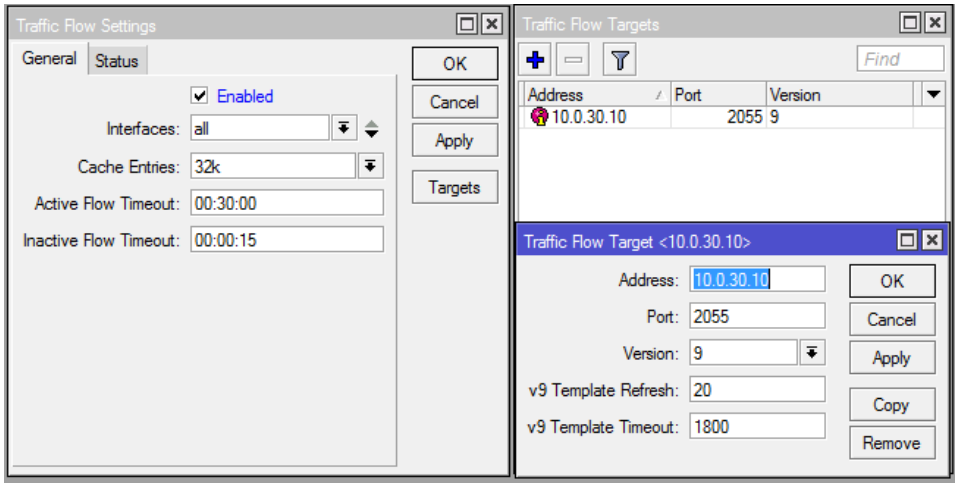


Figura 4.84. Configuración de Traffic Flow para Ntop.

Fuente: Los Autores, Ventana de configuración de Traffic Flow en RouterOS, 2013

Con las configuraciones anteriores realizadas basta solo con ingresar a NTOP desde http://IPServer:3000/, e inmediatamente se podrá empezar a hacer uso de las herramientas que dispone para análisis de tráfico.

4.3.18 CACTI junto a RouterOS y CPE's.

La parte de monitorización es y ha sido siempre un tema de suma importancia y sobre todo en proveedores de servicio de Internet Inalámbrico, las estadísticas detalladas que sistemas como Cacti generan colaboran constantemente en la toma de acciones preventivas o correctivas dentro de una red de datos.

Al ser Cacti una plataforma madura con un larga trayectoria y completamente abierta, ha sido una opción clara destinada al monitoreo de tráfico y recursos del sistema, generando gráficos estadísticos muy detallados, por lo tanto se plantean algunas premisas destinadas a la monitorización sobre la red deseada de la empresa Sigsignet que son las siguientes:

- Monitorización de Tráfico a interfaces de red de CPE bajo el protocolo SNMP para abonados con planes Dedicados y Corporativos, generando datos de tipo TX/RX Bits/Bytes, TX/RX Packets.
- Monitorización de parámetros de Sistema a los CPE de clientes corporativos y dedicados, que van desde carga de CPU, Uptime, Uso de Ram, Uso de Disco e intensidad de señal en CPE Wireless.
- Sobre los puntos de acceso que dan abasto a clientes residenciales se pretende monitorizar el Número Total de estaciones registradas, Estaciones por AP, ruido de Piso, CCQ, Trafico por colas "Simple Queue", así como tráfico generado por "Queue Tree", SNR.

Cacti incluye templates por Defecto para la monitorización de determinados parámetros como por ejemplo el tráfico TX/RX Bits/Bytes, TX/RX Packets, pero en parámetros como Intensidad de Señal, Trafico de "Simple Queue" etc., dichos templates muchas de las veces necesitan ser programados desde cero o en el mejor de los casos mejorados, y lo principal acoplados a las versiones del Sistema Operativo del CPE, no es lo mismo tener un template funcional para colectar estadísticas del Encolamiento Simple en la versión 5.1 de RouterOS que en la V 6.5.

Antes de establecer el proceso de configuración, es necesaria la ubicación del servidor en la topología de la Empresa.

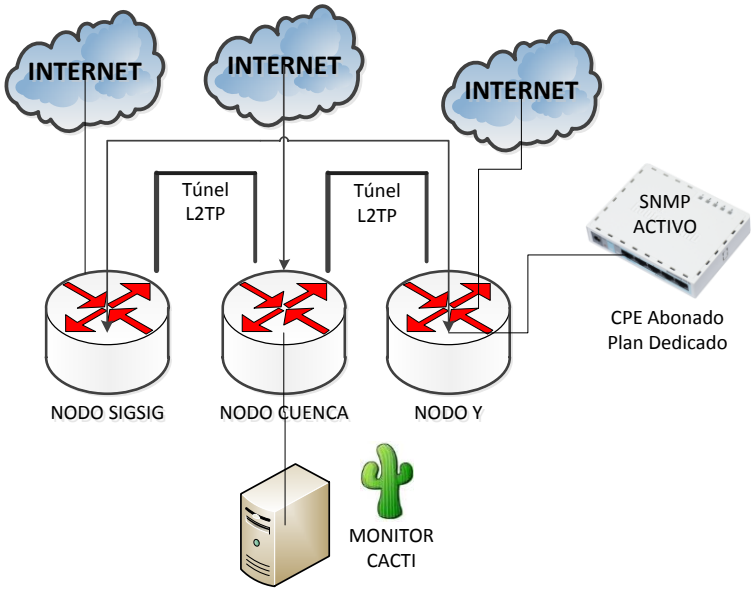


Figura 4.85. Topología Ubicación Servidor Cacti en la Red Deseada Sigsignet

Fuente: Los Autores, Topología de Ubicación Servidor Cacti, 2014

Cabe recalcar que Cacti se aloja sobre un Linux Ubuntu Server 13.10, su instalación es realmente sencilla basta con ingresar a la Shell y con privilegios sudo digitar lo siguiente:

"sudo apt-get install cacti-spine"

Una vez dentro de Cacti se necesitará agregar los host(s) que se desean monitorizar y asociar a sus respectivos templates, para definir que parámetros se desean monitorizar, teniendo en cuenta que el protocolo SNMP este activo del lado del CPE y debidamente agregado a la comunidad de pertenencia. Mantener la seguridad sobre dicho protocolo es esencial, ya que el mismo puede revelar información muy importante e incluso una potencial amenaza para comprometer la infraestructura y servicios de red ante ataques externos o internos, por tal mecanismos incluidos en RouterOS y soportados por el protocolo SNMP permiten mantener a buen resguardo dicha información, como por el uso de un password en la comunidad establecida, así como el uso de un canal encriptación, mecanismos que si bien parecen irrelevantes a

simple vista a futuro podrían evitarnos grandes dolores de cabeza y peor aún ver comprometida la red.

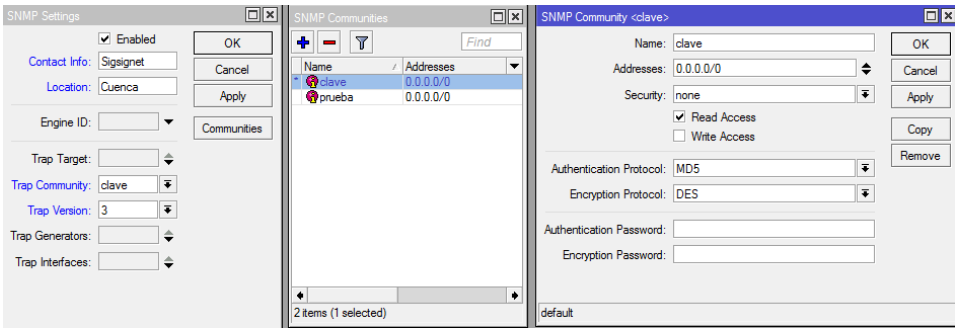


Figura 4.86. Ventana de Configuración de SNMP en RouterOS.

Fuente: Los Autores, Configuración de SNMP en RouterOS, 2013

En tanto en Cacti, como ya se dijo bastaría agregar el host a monitorizar desde la pestaña Devices >> Add Device, y posterior establecer los templates de los parámetros que se pretende monitorizar, es posible para ciertos casos como ya se mencionó utilizar templates por defecto, en otros utilizar templates creados por la comunidad o programados, todo ello dependerá que intentamos monitorizar de nuestros dispositivos.

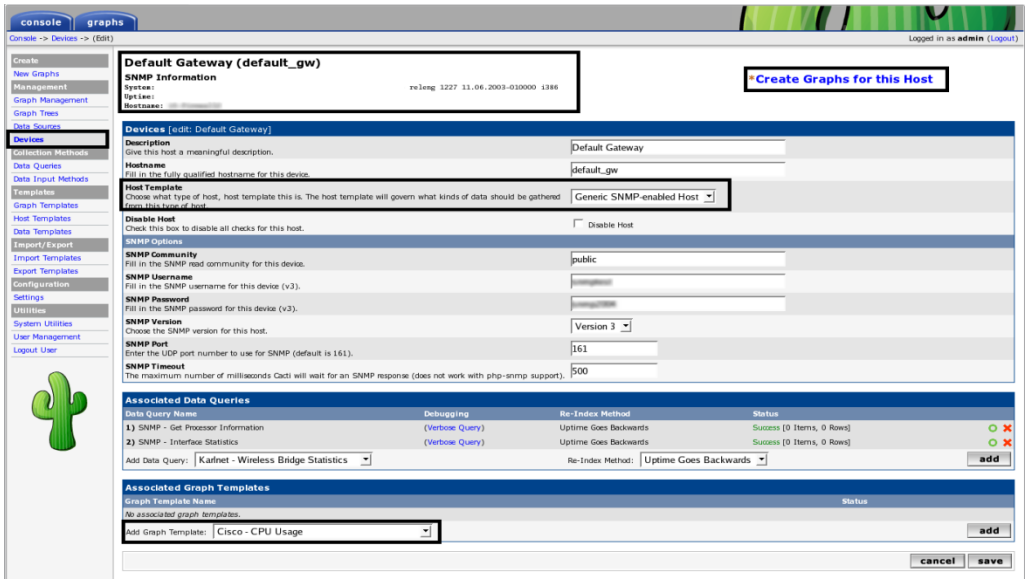


Figura 4.87. Agregación de un Dispositivo a Cacti para su monitorización.

Fuente: Los Autores, Agregar Dispositivos para Monitorización Cacti, 2013

Así también es posible asociar gráficos a esos dispositivos por medio de los diversos templates que se dispongan, consolidando así un gráfico general, es decir obteniendo como resultados en el mismo formulario gráficos estadísticas de tráfico, intensidad de señal, carga de CPU, RAM etc.

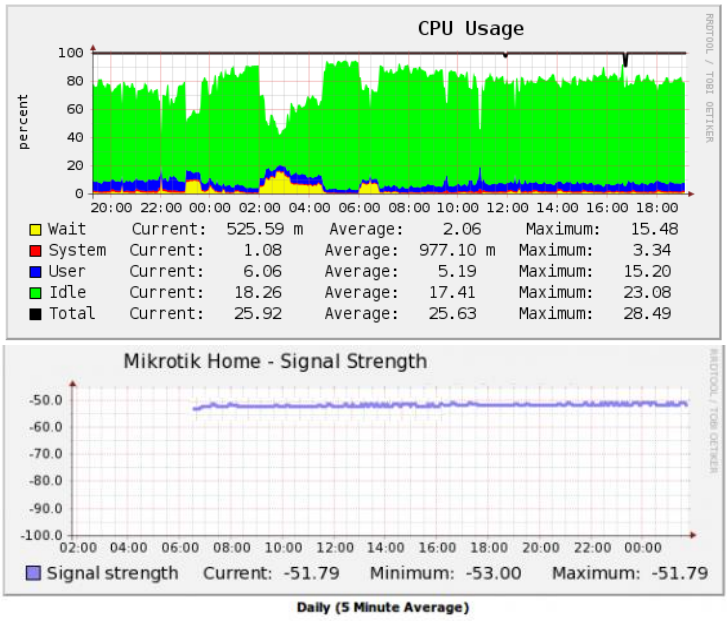


Figura 4.88. Gráficos Estadísticos Generados por Cacti

Fuente: Sergio Hernando, Instalación de la herramienta de monitorización Cacti en FreeBSD, 26 de febrero de 2008, http://www.sahw.com/wp/archivos/2008/02/26/instalacion-de-la-herramienta-de-monitorizacion-cacti-en-freebsd/

Conclusiones del Capítulo 4

El presente capitulo nos ha permitido comprender agregados de funcionalidad de RouterOS además de su completa suite de herramientas y características que apoyaran el proceso de reestructuración, complementado con los diversos procedimientos de configuración de servicios de red y parámetros, estableciendo una base de conocimiento como referente, así también la importancia del uso de herramientas Open Source como Cacti o Ntop en complemento con Mikrotik que apoyen a la administración y soporte de la red, buscando consolidar una red de datos altamente escalable y eficiente para la empresa Sigsignet.

CAPÍTULO V: INTEGRACION DEL SISTEMA DE ADMINISTRACION WEB PARA CONTROL DE ABONADOS Y GESTION DE PLANES DE INTERNET JUNTO A ROUTEROS.

Objetivos:

- Integrar un Sistema de administración Externo utilizando el API disponible de RouterOS para control de Abonados y Planes de Internet.

Objetivos Específicos:

- Entender el API de RouterOS y las diversas formas de comunicación con sistemas externos.
- Entender las estructura de comandos, sentencias y atributos disponibles en RouterOS.
- Integrar iNetControl V 1.0 como sistema de administración web para control de abonados y gestión de planes de Internet.

5.1 INTRODUCCION

En este capítulo se tratará sobre el manejo del API de Mikrotik y su integración con una aplicación personalizada acorde al negocio del WISP, se dará a conocer sobre las funciones y comandos más utilizados con el fin de integrar el sistema de manera eficiente y evitar errores en cuanto al manejo de ancho de banda y de precios por planes. En este capítulo se toma principal interés ya que en base a esto se manejara la logística del negocio y se estandarizaran procesos para el ingreso de un nuevo abonado, cortes de servicio, soporte, etc.

5.1.1 API en RouterOS y formas de comunicación con sistemas externos

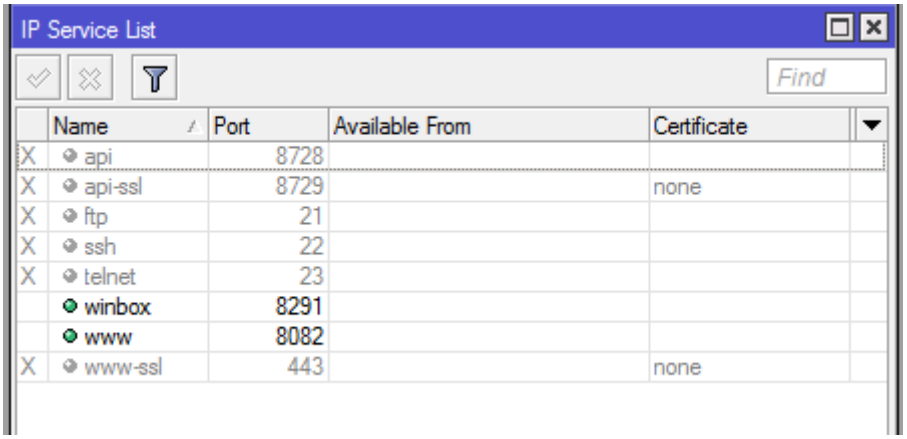


Figura 5.1. IP Services List – API

Fuente: Los Autores, IP Service List Winbox, 2013

Interfaz de programación de aplicaciones (IPA) o API (del inglés Application Programming Interface) es el conjunto de funciones y procedimientos (o métodos, en la programación orientada a objetos) que ofrece cierta biblioteca para ser utilizado por otro software como una capa de abstracción. Son usadas generalmente en las bibliotecas (también denominadas vulgarmente "librerías").[34]

[34] Wikipedia, Interfaz de programación de aplicaciones (n.d.), 9 de febrero del 2013, http://es.wikipedia.org/wiki/Interfaz_de_programaci%C3%B3n_de_aplicaciones

El API de RouterOS se encuentra en IP--->Services y se puede observar claramente que trabaja con el puerto 8728, este es un servicio que se encuentra inicialmente deshabilitado y para utilizarlo obviamente se lo debe activar, este servicio es de gran utilidad para empresas que requieran utilizar una aplicación web o de escritorio para interactuar directamente con RouterOS, esto con la finalidad de llevar a cabo la administración de clientes, planes de ancho de banda, control de pagos, manejo de servicios, monitoreo de consumo, etc., de una manera sencilla y centralizada en una sola aplicación, para que todo tipo de usuario lo pueda manejar sin la necesidad de que tenga grandes conocimientos sobre este sistema operativo. Lo que se pretende realizar en este proyecto es automatizar la gestión de los cobros más que nada de tal manera que si no se registra pago alguno en la base de datos entonces automáticamente se realice una notificación al abonado, dado que esto se lo hace manualmente y resulta muy tedioso ir notificando cliente por cliente y al tener una gran cantidad de clientes esto va a resultar cada vez más complicado y generando también pérdida de tiempo además que se puede cometer muchos errores como lo es notificar a un cliente que si está puntual en los pagos.

5.1.2 Estructura del API y Protocolos

El API se comunica con el Router Mikrotik mediante el envío de frases y este a su vez envía una o más sentencias a cambio, este API está estructurado por oraciones que no son más que una secuencia de palabras que terminan en una palabra de longitud cero. Una palabra es parte de una sentencia que se encuentra codificada de alguna manera y que solamente escrita de manera correcta el RouterOS entenderá el tipo de orden que se le está enviando, y así podrá responder de la manera que se desea.

5.1.2.1 Sentencias

La sentencia es el conjunto de palabras reservadas por el sistema operativo complementadas con uno o más comandos para poder ejecutar una orden y recibir una respuesta. Las sentencias son el objeto principal de comunicación con el API, a continuación se describe algunas características de funcionamiento de las sentencias:

- Las sentencias vacías son ignoradas
- La sentencia se procesa luego de recibir una palabra de longitud cero
- Hay un límite en el número y el tamaño de clientes y sentencias que puede enviar antes de que haya iniciado sesión
- El orden de las palabras atributo no debe ser invocado. Como el orden y la cuenta es cambiable por el atributo "proplist".

La estructura de la sentencia es la siguiente:

- La primera palabra debe contener la palabra de comando;
- Debe contener la palabra de longitud cero para terminar la frase;
- Puede contener ninguna o varias palabras de atributos. No hay ningún orden en particular en lo que las palabras de atributo tiene que ser enviado en la sentencia

5.1.2.2 Comandos

Es una instrucción o una orden que el usuario del sistema operativo le da desde una línea de comandos o desde una llamada de programación.

En esta sección nos limitaremos a listar solamente los comandos más usados y populares:

Comandos "set", "add" y "remove" sirven para poder cambiar, agregar o remover reglas desde la línea de comandos respectivamente, estos comandos son de gran utilidad al momento de realizar la configuración del firewall en caso de no contar con un computador que nos facilite utilizar winbox para realizar los cambios mediante una interfaz gráfica.

Comandos "enable" y "disable" son utilizadas para habilitar y deshabilitar respectivamente reglas, direcciones IP y otros servicios que ofrece Mikrotik sin la necesidad de removerlas de la configuración.

Comando "move" sirve para mover algunas reglas que lo permitan y así cambiar el orden de ejecución de las diferentes configuraciones.

Comando “comment” es el más utilizado en casi todas por no decir todas las configuraciones ya que esto permite realizar una breve explicación de lo que se hace en las diferentes configuraciones.

Tipos de Datos.

Operador	Descripción
Number	Tipo de dato entero de 64 bits
Boolean	Tipo de dato booleano puede tomar valor de “verdadero” o “falso”
String	Tipo de dato cadena o secuencia de caracteres
IP	Dirección IP
Internal ID	Identificador interno con un prefijo “*”. Cada elemento del menú tiene un identificador único.
Time	Valor de fecha y hora
Array	Secuencia de valores organizados en una matriz
Nil	Valor por defecto tipo variable en caso de no tener un valor asignado.

Tabla 5.1. Tipos de Datos

Fuente: Mikrotik, Tipos de datos, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Secuencias de Escape.

Operador	Descripción

\”	Insertar comillas dobles
\\	Insertar barra invertida
\N	Insertar un salto de línea
\R	Insertar un retorno de carro
\T	Insertar un tab horizontal
\$	Salida de carácter. De lo contrario se utiliza para vincular variable
\?	Salida de carácter. De lo contrario se utiliza para imprimir ayuda en la consola.
\ _	Espacio
\A	Bel (0x07)
\B	Retroceso (0x08)
\F	Formulario de alimentación (0xFF)
\V	Insertar tabulación vertical
\Xx	Imprime carácter de valor hexadecimal. El número hexadecimal debe utilizar letras mayúsculas.

Tabla 5.2. Secuencias de escape

Fuente: Mikrotik, Constante de secuencias de escape, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Operadores Aritméticos.

Operador	Descripción	Sintaxis
“+”	Adición binaria	:Put(3+4);

“-”	Sustracción binaria	:Put(5-6);
“*”	Multiplicación binaria	:Put(6*2);
“/”	División binaria	:Put(10/5); :Put((10)/2);
“-”	Negación unitaria	{: Local a 1; : put (-a);}

Tabla 5.3. Operadores Aritméticos

Fuente: Mikrotik, Operadores aritméticos, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Operadores Relacionales.

Operador	Descripción	Sintaxis
“<”	Menor que	:Put(2<3);
“>”	Mayor que	:Put(4>3);
“=”	Igual que	:Put(5=5);
“<=”	Menor o igual que	:Put(4<=4);
“>=”	Mayor o igual que	:Put(6>=6)
“!=”	Diferente que	:Put(5!=3);

Tabla 5.4. Operadores Relacionales

Fuente: Mikrotik, Operadores Relacionales, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Operadores Lógicos.

Operador	Descripción	Sintaxis
“!”, “not”	No lógico	:Put(!true);

“&&”, “and”	And lógico	: Put (true && true)
“||”, “or”	Or lógico	: Put (true | | false);
“in”	Dentro de lógico	: Put (1.1.1.1/32 en 1.0.0.0 / 8);

Tabla 5.5. Operadores Lógicos

Fuente: Mikrotik, Operadores Lógicos, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Operadores Bit a Bit.

Operador	Descripción	Sintaxis
“~”	Inversion de bit	: Put (~ 0.0.0.0)
“|”	OR bit a bit. Realiza la operación OR lógica en cada par de bits correspondientes. En cada par, el resultado es "1" si uno de los bits o ambos bits son "1", de lo contrario el resultado es "0".	
“^”	XORbit a bit. Lo mismo que or bit a bit, pero el resultado en cada posición es "1" si dos bits no son iguales, y "0" si los bits son iguales.	
“&”	AND bit a bit. En cada par, el resultado es "1" si el primero y segundo bit es "1". De lo contrario el resultado es "0".	
“<<”	desviación a la izquierda por determinada cantidad de bits	
“>>”	desplazamiento a la derecha por determinada cantidad de bits	

Tabla 5.6. Operadores Bit a Bit

Fuente: Mikrotik, Operadores Bit a Bit, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Operadores de Concatenación.

Operador	Descripción	Sintaxis
“.”	Concatena dos cadenas	:Call(“Concatenar”. “”.“Cadena”);
“,”	Concatena dos matrices o añade elementos a la matriz	: Put ({1, 2, 3}, 5);

Tabla 5.7. Operadores de Concatenación

Fuente: Mikrotik, Operadores de Concatenación, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Operadores Adicionales.

Operador	Descripción	Sintaxis
“[]”	Comando de sustitución. Puede contener solo una línea de comando	:put [:len "my test string";];
“()”	Sub expresión u operador de agrupación	:put ("El valor es " . (4+5));
“$”	Operador de sustitución	:global a 5; :put $a;
“~”	operador binario que coincide con el valor en contra de POSIX extendido de expresiones regulares	Imprime todas las rutas del waterway que terminan con 202 ip route print where gateway~"^[0-9 \\.]*202"

Tabla 5.8. Operadores Adicionales

Fuente: Mikrotik, Otros Operadores, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Variables.

Variable	Descripción
Global	Accesible desde todos los scripts creados por el usuario, definida por la palabra clave “global”;
Local	Accesible sólo dentro del actual ámbito de aplicación, definido por la palabra clave “local”.

Tabla 5.9. Variables

Fuente: Mikrotik, Variables, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Comandos Globales.

Comando Globales	Descripción	Sintaxis
/	Situarse en el menú raíz	
..	Retroceder un nivel del menú	
?	Lista los comandos disponibles con una breve descripción	
global	Define una variable global	:global myVar "algo"; :put $myVar;
local	Define una variable local	{ :local myLocalVar "Yo soy local"; :put $myVar; }
beep	Beep de altavoz incorporado	:beep <freq> <length>
delay	No hace nada por un determinado periodo de tiempo	:delay <time>

put	Colocar el argumento suministrado en la consola	:put <expression>
len	Regresar la longitud de la cadena o el recuento del elemento de la matriz	:put [:len "length=8"];
typeof	Retorna el tipo de dato de la variable	:put [:typeof 4];
pick	Retorna el rango de elementos o subcadenas. Si la posición final no se ha especificado, se devolverá solo un elemento de una matriz	:put [:pick "abcde" 1 3]
log	Escribe un mensaje de registro del sistema . Temas disponibles son "debug, error, info and warning"	:log info "Imprimo desde el script";
time	Retorna intervalo de tiempo necesario para executar el comando	:put [:time {:for i from=1 to=10 do={ :delay 100ms }}];
set	Asigna un valor a la variable declarada	:global a; :set a true;
find	Regresa a la posición del elemento de la matriz o subcadena	:put [:find "abc" "a" -1];
enviroment	Imprime información de la variable inicializada	:global myVar true; :environment print;
terminal	Terminal de comandos relacionados	
error	Genera error en la consola y	

	detiene la secuencia de ejecución de comandos	
parse	Analiza la cadena y retorna a la consola los comandos analizados	:global myFunc [:parse ":put hello!"]; $myFunc;
resolve	Retorna la dirección up del nombre o nombres del DNS	:put [:resolve "www.mikrotik.com"];
toarray	Convierte la variable a array	:toarray <var>
tobool	Convierte la variable a booleana	:tobool <var>
toid	Variable para convertir ID interno	:toid <var>
Toip	Variable para convertir la dirección IP	:toip <var>
toip6	Variable para convertir direcciones IPv6	:toip6 <var>
tonum	Convertir variable a entero	:tonum <var>
tostr	Convertir variable a cadena	:tostr <var>
totime	Convertir variable a tiempo	:totime <var>

Tabla 5.10. Comandos Globales

Fuente: Mikrotik, Comandos Globales, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Comandos Comunes.

Comando Comunes	Descripción	Sintaxis
add	Agrega un nuevo ítem	add

		<param>=<value>..<param>=<value>
remove	Elimina el ítem seleccionado	Remove <id>
enable	Habilita el elemento seleccionado	Enable <id>
disable	Deshabilita el ítem seleccionado	Disable <id>
set	Cambia el parámetro seleccionado, pueden ser seleccionados más de un elemento	set <id> <param>=<value>..<param>=<value>
get	Obtiene el valor del parámetro seleccionado	get <id> <param>=<value>
print	Imprime los elementos del menú, la salida depende de los parámetros de impresión especificados.	print <param><param>=[<value>]
export	Exporta la configuración del menú y submenús. La extensión del archivo será ".Rsc". Los comandos exportados pueden ser importados.	export [file=<value>]
edit	Edita los items seleccionados	edit <id> <param>
find	Encuentra los elementos por la expresión dada	find <expression>
comment	Agrega un comentario para	

	describir el item.	
unset		
move	Mueve de posición el item seleccionado	
reset-counters	Encera los contadores	
reset-counters-all	Encera todos los contadores de estadísticas	
release (DHCP-Client)	Borra las direcciones de los clientes DHCP	
renew (DHCP-Client)	Renueva las direcciones de los clientes DCHP	

Tabla 5.11. Comandos Comunes

Fuente: Mikrotik, Comandos Comunes, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Comandos de Impresión de Parámetros.

Comando Impresión	Descripción	Sintaxis
as-value	Salida de impresión como una matriz de parámetros y sus valores	:put [/ip address print as-value]
brief	Imprime una breve descripción	
detail	Imprime una descripción detallada, este es útil para ver	

	todos los parámetros.	
count-only	Imprime solo un conteo de los elementos del menú	
File	Imprime la salida en un archivo	
follow	Imprime todas las entradas actuales y rastrea las entradas nuevas hasta que ctrl-c es presionado, es útil cuando se visualiza el registro de las entradas.	/log print follow
follow-only	Imprime y realiza un seguimento solo de las nuevas entradas hasta que ctrl-c es presionado	/log print follow-only
from	Imprime solo los parámetros del elemento especificado.	/user print from=admin
interval	Imprime continuamente la salida en el intervalo de tiempo seleccionado.	/interface print interval=2
terse	Muestra los detalles de la maquina en formato amigable	
value-list	Muestra los valores uno por línea	
without-paging	Si la salida no cabe en la pantalla de la consola y no se detiene, imprime toda la información en una sola pieza	
where	Las expresiones seguidas por el parámetro “where”, se puede utilizar para filtrar las entradas	/ip route print where interface="ether1"

	coincidentes.	

Tabla 5.12. Impresión de Parámetros

Fuente: Mikrotik, Impresión de parámetros, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Bucles y Sentencias Condicionales.

Bucles y Condicionales	Descripción	Sintaxis
do..while	Ejecuta comandos hasta que una determinada condición se cumple	:do { <commands> } while=(<conditions>); :while (<conditions>) do={ <commands> };
For	Ejecuta comandos a través de un numero dado de iteraciones	:for <var> from=<int> to=<int> step=<int> do={ <commands> }
foreach	Ejecuta comandos para cada elemento de la lista	:foreach <var> in=<array> do={ <commands> };
If	Si una determinada condición es “true” entonces ejecutar comandos en el bloque “do”, de lo contrario ejecuta comandos en el bloque “else” si se especifica	:if(<condition>) do={<commands>} else={<commands>} <expression>

Tabla 5.13. Bucles y sentencias condicionales

Fuente: Mikrotik, Bucles y sentencias condicionales, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Gestión de Scripts.

Comando Script	Descripción	Sintaxis
name	Nombre de la secuencia de comandos	name (string; Default: "Script[num]")
policy	Lista de políticas aplicables	policy (string; Default:)
source	Script de código fuente	source (string;)
last-started	Fecha y hora desde que el script fue invocado por última vez	last-started (date)
owner	Usuario que creo el script	owner (string)
run-count	Contador que cuenta el número de veces que la secuencia de comandos se ha ejecutado.	run-count (integer)
run	Ejecutar el script especificado por ID o por nombre.	run (run [id|name])
name	Nombre de la variable	name (string)
user	Usuario quien define la variable	user (string)
value	Valor asignado a la variable	value ()

Tabla 5.14. Comandos de Gestión de Scripts

Fuente: Mikrotik, Scripts, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Tareas (JOB).

Comandos	Descripción	Sintaxis

Comunes		
Owner	Usuario quien está ejecutando el script	owner (string)
policy	Lista de todas las políticas aplicados al script	policy (array)
started	Fecha y hora cuando el script fue iniciado	started (date)

Tabla 5.15. Tareas (JOB)

Fuente: Mikrotik, Tareas, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Comandos de Administración Interfaz(es).

Comando	Descripción	Sintaxis
6to4	Cambia al contexto `netsh interface 6to4'	/interface 6to4 add mtu=1280 name=ipng-tunnel local-address=62.157.9.98 remote-address=192.88.99.1 disabled=no
bonding	sumar dos conexiones o más interfaces de red como un enlace virtual único.	[admin@Router1] interface bonding> add slaves=ether1,ether2
bridge	Establece la interface en modo bridge para interconectar los diferentes enlaces.	interface bridge add name=wds-bridge
eoip	Protocolo que crea un túnel Ethernet entre dos enrutadores en la parte superior de una	add name="eoip-remote" tunnel-id=0 \

	conexión IP	
eoipv6	Protocolo que crea un túnel Ethernet entre dos enrutadores en la parte superior de una conexión IPv6	
ethernet	Estándar de conexión de red	Interface ethernet edit ether1 10.0.1.1/30
Gre	Protocolo de encapsulación de enrutamiento genérico	ip tunnel add netb mode gre remote 172.19.20.21 local 172.16.17.18 ttl255
gre6	encapsulación de enrutamiento genérico, túnel a través de red IPv6	/interface gre6 add local-address=2001:db8:bad:ee1::a remote-address=2001:db8:f00:baa::b keepalive=5
Ipip	IPIP túnel es un protocolo simple que encapsula los paquetes IP en IP para hacer un túnel entre dos routers	interface ipip> /ip address add address=1.1.1.1/24 interface=ipip1
ipipV6	IP/IPv6 más la función de túnel IPv6 se añade en v5RC6 y se configura desde otro menú, utiliza las mismas propiedades como IPv4.	
l2tp-client	Cliente del protocolo de túnel seguro para el transporte de tráfico IP mediante PPP	/interface l2tp-client>add name=l2tp-hm user=l2tp-hm password=123 \
l2tp-server	Servidor del protocolo de túnel seguro para el transporte de	interface l2tp-server server> set enabled=yes

	tráfico IP mediante PPP	
mesh	Configura la red multipunto a multipunto o malla	/interface wireless set wlan1 disabled=no ssid=mesh frequency=2437 band=2.4ghz-b/g mode=ap-bridge
ovpn-client	Configura el cliente de open vpn	/interface ovpn-client> add connect-to=10.1.101.1 user=test password=123 disabled=no
ovpn-server	Configura el servidor de open vpn	/interface ovpn-server server> set enabled=yes
ppp-client	Configura al cliente del túnel ppp	interface ppp-client add profile=defaul
ppp-server	Administra las conexiones	interface ppp-server enable
pppoe-client	crea una interfaz cliente PPPoE	interface pppoe-client add name="PPPoE-e2H" user=e2h password=pipo interface=ether1 service-name="Internet" disabled=no add-default-route=yes use-peer-dns=yes
pppoe-server	crea una interfaz servidor PPPoE	interface pppoe-server server add service-name="Internet" interface=ether1 default-profile="PPPoE-profile" disabled=no one-session-per-host=yes
pptp-Client	Configura la interfaz cliente para trabajar en modo pptp	/interface pptp-client>add name=pptp-hm user=pptp-hm password=123 \

pptp-Server	Concentrador de acceso pptp para permitir a usuarios remotos conectarse por medio del túnel encriptado	interface pptp-server server> set enabled=yes
sstp-Client	Configura el cliente sstp	/interface sstp-client>add user=sstp-test password=123 \
sstp-Server	Configura el servidor de conexiones sstp	interface sstp-server server> set enabled=yes
traffic-eng	Monitorea el tráfico del túnel TE	interface traffic-eng> monitor 0
virtual-Ethernet	Comando para virtualizar una interface de red	interface virtual-ethernet add
vlan	Red de área local virtual	Interface vlan add name=vlan1 vlan-id=11 interface=ether1
vpls	Servicio de red de área local virtual privada y permite implementar servicios LAN-to-LAN entre sedes de clientes, sobre el backbone MPLS existente.	/interface vpls add name=A1toA2 remote-peer=9.9.9.5 mac-address=00:00:00:00:00:a1 vpls-id=10 disabled=no
vrrp	Protocolo redundante de red virtual	interface vrrp add name=vrrp1 interface=ether1

Tabla 5.16. Comandos de Administración de Interfaz(es)

Fuente: Mikrotik, Manual: Interface, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Comandos Principales de Interfaz Wireless.

Comando	Descripción	Sintaxis

access-list	Configura la lista de acceso de los clientes wireless	interface wireless access-list print
aling	Configura la el tipo de alineación que se utilizará para la antena wireless	interface wireless align set active-mode=yes audio-max=-20 audio-min=-100 audio-monitor=\ 00:00:00:00:00:00 filter-mac=00:00:00:00:00:00 frame-size=300 \ frames-per-second=25 receive-all=no ssid-all=no
connect-list	Muestra la lista de Access point que están disponibles dentro del rango de alcance	
info	Muestra información del log del sistema	Log info message= mensaje
manual-tx-power-table	Define la patencia de transmisión de la interfaz	interface wireless manual-tx-power-table>set 0 \manual-tx-powers=1Mbps:10,2Mbps:10,5.5Mbps:9, 11Mbps:7
nstreme	Configura la interfaz wireless en modo Nstreme	interface wireless nstreme set wlan1 enable-nstreme=yes enable-polling=yes framer-policy=best-fit framer-limit=3200
nstreme-dual	Configura la interfaz wireless en modo Nstreme-dual	interface wireless set wlan1 mode=nstreme--dual--slave
registration-table	Permite ver que clientes están conectados al AP	Interface wireless registration-table print
security-	Define los perfiles de	security-profile=default

profiles	seguridad que se	
sniffer	Configura el rastreador de paquetes inalámbrico	interface wireless sniffer
snooper	Controla la carga de tráfico en cada canal	Interface wireless snooper
wds	Configura el enlace inalámbrico con bridge transparente	set wlan1 wds-mode=dynamic

Tabla 5.17. Comandos de Administración de Interfaz Wireless.

Fuente: Mikrotik, Interface Wireless, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Comandos Adicionales Wireless.

Comando	Descripción	Sintaxis
packet	Marca los paquetes	ip firewall mangle add action=mark-connection chain=prerouting comment="CONTROLE ICMP" disabled= no new-connection-mark=ICMP-Conexao passthrough=yes protocol=icmp add action=mark-packet chain=prerouting comment="" connection-mark= ICMP-Conexao disabled=no

		new-packet-mark=ICMP-Pacotes passthrough=yes
monitor	Muestra el estado de las interfaces	/interface wireless monitor wlan1
reset-configuration	Resetea la configuración del RouterOS a los valores de fábrica	/system reset-configuration
scan	Escanea los dispositivos inalámbricos	/interface wireless scan wlan1
spectral-history	Realiza un análisis espectral de todas las frecuencias admitidas por la tarjeta inalámbrica	/interface wireless spectral-history <wireless interface name>
spectral-scan	Monitorea continuamente los datos espectrales	/interface wireless spectral-scan <wireless interface name>
test-audio	Prueba del sonido emitido por Mikrotik	
frequency-monitor	Monitorea las frecuencias de la interfaz inalámbrica	/interface wireless frequency-monitor wlan1

Tabla 5.18. Comandos Adicionales Wireless

Fuente: Mikrotik, Manual: Interface/Wireless, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Comandos Bridge

Comando	Descripción	Sintaxis
calea	Herramienta de recolección de datos	/ tool calea add action=pcap intercept-port=5555 case-id=100

		intercept-ip=192.168.0.254
filter	Agrega un filtro para bloqueo o aceptación de puertos, direcciones IP, direcciones MAC, etc.	/ip firewall filter add chain=input protocol=tcp dst-port=8728 action=accept
host	Indicador del anfitrión a ser tratado	add host=10.0.0.217 interval=10s timeout=998ms up-script=gw_2 down-script=gw_1
nat	Redirige puertos para las diferentes redes	ip firewall nat add in-interface=LAN dst-port=80 protocol=tcp action=redirect to-ports=8080 chain=dstnat
port	Establece el puerto a tratar	ip proxy set enabled=yes port=8080

Tabla 5.19. Comandos Bridge

Fuente: Mikrotik, Manual: Interface/Bridge, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Comandos PPP

Comando	Descripción	Sintaxis
aaa	Permite ajustar cuentas RADIUS y autenticación	/user aaa
active	Para ver los clientes pppoe conectados	/ ppp active> print
profile	Permite crear un perfil ppp para el servidor y los clientes	/ ppp profile set default local-address=192.168.0.1

secret	método para crear usuarios en la base de datos local de nuestro RouterOS	ppp secret add name=12343 password=1234 service=pppoe profile=PPPoE-profile

Tabla 5.20. Comandos PPP

Fuente: Mikrotik, Manual: Interface/PPP, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Comandos de Administración IP.

Comando	Descripción	Sintaxis
accounting	Activa el conteo de IP's	/ip accounting set enabled=yes
address	Asigna una dirección IP a la interface	ip address add interface=ether1 address=1.1.1.1/30
arp	responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP	/ arp -a
dhcp-client	Configura la dirección ip entrante como dinámica	/ ip dhcp-client add interface=ether2 disabled=no
dhcp-relay	Configura un proxy en la interfaz	ip dhcp-relay add name=Local1-Relay interface=Local1
dhcp-server	Configura el servidor dhcp para que reparta direcciones IP	/ip dhcp-server add interface=To-DHCP-Relay relay=192.168.1.1

dns	Configura los DNS a utilizar	/ip dns static add 200.93.192.148
firewall	Configura las reglas de nat, bloqueo, aceptación, etc.	/IP FIREWALL NAT add chain=srcnat action=masquerade out-interface=ether1
hotspot	Proporsiona la autenticación de los clientes antes del acceso a la red	/ip hotspot setup
ipsec	es un conjunto de protocolos definidos por el Internet Engineering Task Force (IETF) para garantizar un intercambio de paquetes a través de redes no protegidas IP/IPv6 como Internet.	Ip ipsec propuesta ajustar [encontrar default = yes] = ENC-algoritmos 3DES, AES-128, AES-192, AES-256
neighbor	Muestra todos los clientes vecinos conectados	/ ip neighbor print
packing	ofrece servicio de empaquetamiento de paquetes en los enlaces de la red. Permite la agregación simple de paquetes en paquetes más grandes y compresión de los contenidos de paquetes.	/ip packing add interface=ether1 aggregated-size=1500 packing=simple unpacking=none
pool	Reserva el pool de IP's que serán tomadas por el servidor DHCP para asignar automáticamente	/ip packing add interface=ether1 aggregated-size=1500 packing=simple unpacking=none
proxy	Configura el proxy transparente	ip proxy set enabled=yes port=8080

route	Configura las rutas del RouterOS	/ip route add gateway=10.1.0.1
service	Activa o desactiva los servicios de Mikrotik	/ip service enable api
smb	proporciona acceso a las carpetas de uso compartido de archivos configurados del router	/ip smb user add read-only=no name=mtuser password=mtpasswd
socks	Servidor proxy que permite que los datos de aplicaciones basadas en TCP transmitan a través del servidor de seguridad, incluso si el servidor de seguridad podría estar bloqueando los paquetes	ip socks> set enabled=yes
ssh	Permite realizar conexiones bajo ssh	/system ssh 192.168.88.1 user=lala
tftp	Trivial File Transfer Protocol es un protocolo muy simple que se usa para transferir archivos	/ip tftp add req-filename=file.txt real-filename=/sata1/file.txt allow=yes read-only=yes
traffic-flow	Es un sistema que proporciona información estadística sobre los paquetes que pasan por el Router	ip traffic-flow> set enabled=yes
upnp	Permite la comunicación de datos entre dos dispositivos al mando de cualquier dispositivo de control de la red	ip upnp> set enable=yes

Tabla 5.21. Comandos de Administración IP

Fuente: Mikrotik, Manual: IP, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos IP Accounting.

Comando	Descripción	Sintaxis
snapshot	Recolecta y visualiza tráfico de datos	ip accounting snapshot> take
uncounted	Almacena los paquetes no contabilizados.	ip accounting uncounted> print
web-access	Habilita o deshabilita el acceso vía web al servidor	/ip accounting web-access set accessible-via-web=yes address=0.0.0.0/0

Tabla 5.22. Sub-Comandos IP Accounting

Fuente: Mikrotik, Manual: IP/Accounting, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos IP DHCP-client.

Comando	Descripción	Sintaxis
release	Borra las direcciones ip del cliente que han sido concedidas dinámicamente	/ ip dhcp-client release
renew	Renueva las direcciones ip del cliente que han sido concedidas dinámicamente	/ ip dhcp-client renew

Tabla 5.23. Sub-Comandos IP DHCP-client

Fuente: Mikrotik, Manual: IP/DHCP_Client, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos IP DHCP-server.

Comando	Descripción	Sintaxis
alert	Alerta de la detección de servidores dhcp falsos tan pronto como aparecen en la red	ip dhcp-server alert>/log print
config	Permite configurar con qué frecuencia los arriendos DHCP se almacenaran en el disco	/ ip dhcp-server config
lease	El tiempo que un cliente puede utilizar la dirección asignada	/ip dhcp-server lease print
network	Configure el rango de red que se utilizará	/ ip dhcp-server network add address=192.168.0.0/24 gateway=192.168.0.1
option	Añade más opciones de dhcp	add address = 10.1.0.0 gateway = 10.1.0.1 dhcp-option = Opción Nombre de host DNS-server = 159.148.60.20
setup	Configura el servidor dhcp-server con un asistente	/ ip dhcp-server setup

Tabla 5.24. Sub-Comandos IP DHCP-server

Fuente: Mikrotik,Manual: IP/DHCP_Server, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos DNS.

Comando	Descripción	Sintaxis

cache	Configura el dns cache transparente	/ ip dns cache
static	Configura el dns estático	/ip dns static add address=8.8.4.4 disabled=no name=www.google.com ttl=1d

Tabla 5.25. Sub-Comandos DNS

Fuente: Mikrotik, Manual: IP/DNS, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos IP Firewall.

Comando	Descripción	Sintaxis
address-list	Muestra las direcciones IP con sus nombres y planes establecidos en las queues	/ ip firewall address-list print
calea	Asistente para el cumplimiento de la Ley de comunicaciones para interceptar y registrar el tráfico de red	/ ip firewall calea add action=sniff-pc chain=forward sniff-id=100 sniff-target=10.9.1.250 sniff-target-port=5555 \ src-address=192.168.0.10
connection	Muestra los dispositivos conectados al routerOS	/ ip firewall connection print
filter	Configura reglas de conexión y de estado	ip firewall filter add connection-state=established action=accept chain=input
layer7-protocol	Método de búsqueda de patrones en las corrientes de ICMP / TCP / UDP	/ip firewall layer7-protocol add comment="" name=bittorrent regexp="^(\\x13bittorrent protocol|azver\\x01\$\ |get

		/scrape\\\?info_hash=|get /announce\\\?info_hash=|get/client/bitcomet\ /|GET /data\\\?fid=)|d1:ad2:id20:|\\x08'7P\\)[RP]"
mangle	Prioriza los servicios para mejorar el QoS	/ ip firewall mangle add chain=forward dst-address=192.168.0.2 action=mark-packet-mark=VOIP disable=no
nat	Agrega reglas de nat al servidor	/ip firewall nat add chain=dstnat action=netmap dst-address=10.10.10.2-10.10.10.10 to-addresses=192.168.2.2-192.168.2.10 place-before=0
service-port	Activa o desactiva los puertos de diferentes servicios	ip firewall service-port set ftp disabled=no ports=21 set tftp disabled=no ports=69 set irc disabled=no ports=6667 set h323 disabled=no set sip disabled=no ports=5060,5061 sip-direct-media=yes set pptp disabled=no

Tabla 5.26. Sub-Comandos IP Firewall

Fuente: Mikrotik, Manual: IP/Firewall, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos Hotspot.

Comando	Descripción	Sintaxis
active	Muestra todos los usuarios autenticados vía hotspot	/ ip hotspot active print
cookie	Menú contiene todas las cookies enviadas a los clientes HotSpot	/ip hotspot cookie
host	muestra todos los equipos conectados al servidor de HotSpot	/ ip hotspot host print
Ip-binding	permite configurar estáticamente Uno a Uno traducciones NAT,	/ ip hostspot ip-binding

	permite eludir los clientes específicos HotSpot sin ningún tipo de autenticación, y también permite bloquear determinados hosts y subredes de la red de HotSpot	
profile	Configura los perfiles de los usuarios del hotspot	/ ip hotspot profile print
service-port	Configura los puertos que podrán estar activos para los usuarios de hotspot	/ip hotspot service-port print
user	Configura los usuarios del hotspot	/ip hotspot user set admin profile=default
walled-garden	Libera las paginas no autorizadas por el hotspot	/ip hotspot walled-garden add action=allow comment="" disabled=no dst-host=lineff.com dst-port=80
reset-html	El comando sobrescribe el servlet del hotspot existente con el archivo original HTML	/ip hotspot reset-html
setup	Configura en servidor de hotspot en el router	/ ip hotspot setup

Tabla 5.27. Sub-Comandos Hotspot

Fuente: Mikrotik, Manual: IP/Hotspot, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos IPSec.

Comando	Descripción	Sintaxis

installed-sa	proporciona información sobre las asociaciones de seguridad instalados, incluyendo las llaves.	/ip ipsec installed-sa
key	Lista todas las claves importadas, públicas y privadas que se pueden utilizar para la autenticación entre pares	/ip ipsec key print
peer	Se utiliza para negociar claves y algoritmos	/ip ipsec peer add address=192.168.80.1/32 port=500 auth-method=pre-shared-key secret="test"
policy	Determina si la configuración de seguridad se debe aplicar a un paquete.	/ip ipsec policy dump-kernel-policies
proposal	Información que será enviada por el demonio IKE para establecer asociaciones de seguridad para esta directiva	/ip ipsec proposal set [find default=yes] enc-algorithms=3des,aes-128,aes-192,aes-256
remote-peers	Proporciona varias estadísticas acerca de interlocutores remotos que en la actualidad se han establecido las conexiones de fase 1 con este router.	/ip ipsec remote-peers kill-connections
statistics	Muestra varias estadísticas de ipsec	/ip ipsec statistics

Tabla 5.28. Sub-Comandos IPSec

Fuente: Mikrotik, Manual: IP/IPsec, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos Neighbor.

Comando	Descripción	Sintaxis
discovery	facilita la configuración y la gestión al permitir que cada router Mikrotik para descubrir otros routers conectados	/ip neighbor discovery set vlan6 disabled=yes

Tabla 5.29. Sub-Comandos Neighbor

Fuente: Mikrotik, Manual: IP/Neghbor discovery, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos IP Pool.

Comando	Descripción	Sintaxis
used	Muestra todas las direcciones ips utilizadas del pool de ips creadas	/ ip pool used print

Tabla 5.30. Sub-Comandos IP Pool

Fuente: Mikrotik, Manual: IP/Pools, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos IP Proxy.

Comando	Descripción	Sintaxis
access	Bloquea o permite el acceso a url's o a url's que contengan ciertas palabras	/ip proxy access add dst-host=www.facebook.com action=deny

cache	Especifica que solicitudes tienen que estar almacenadas localmente por el web proxy y cuales no	/ ip proxy cache
cache-contents	Muestra el contenido que hay en cache	/ ip proxy cache-contents print
connections	Contiene la lista de conexiones actuales que el proxy está proveyendo	/ip proxy connections
direct	Lista de acceso directo al proxy que van a ser negados o permitidos	/ip proxy direct
inserts	Muestra las estadísticas de los objetos almacenados en cache	/ip proxy inserts
lookups	Muestra las estadísticas de los objetos leídos de cache	/ip proxy lookup
refreshes	Actualiza la lista disponible en el proxy	/ ip proxy refreshes print
clear-cache	Limpia automáticamente los datos de cache en caso de inconsistencias	/ ip web-proxy-cache transparente
reset-html	Para personalizar la página por defecto del RouterOS, ejecuta un reset sobre cualquier	/ip proxy reset-html

	configuración realizada.	

Tabla 5.31. Sub-Comandos IP Proxy

Fuente: Mikrotik, Manual: IP/Proxy, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos IP Route.

Comando	Descripción	Sintaxis
cache	Configura el almacenamiento en cache	/ip route cache print cache-size: 3644 max-cache-size: 65536 increasing started with out decreasing any more after more than 100 onlines
nexthop	Configura el siguiente salto que se dará en el enrutamiento	/ ip route nexthop print
rule	Configura una regla en la ruta	/ ip route rule print
vrf	Permite crear multiples instancias virtuales de enrutamiento	/ip route vrf add routing-mark=red route-distinguisher=111:500 import-route-targets=111:500,111:999 \ export-route-targets=111:500 interfaces=ether1.500

Tabla 5.32. Sub-Comandos IP Route

Fuente: Mikrotik, Manual: IP/Route, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos IP Traffic-Flow.

Comando	Descripción	Sintaxis

target	proporciona información estadística sobre los paquetes que pasan por el router	ip traffic-flow> set enabled=yes

Tabla 5.33. Sub-Comandos IP Traffic-Flow

Fuente: Mikrotik, Manual: IP/Traffic Flow (n.d.). 17 de febrero del 2013.

Comandos de MPLS.

Comando	Descripción	Sintaxis
forwarding-table	Comprueba que existe intercambio de etiquetas.	/ mpls forwarding-table print
interface	Este menú permite configurar MTU incluidos los encabezados MPLS que la interfaz puede reenviar sin fragmentación.	/ mpls interface print
ldp	Protocolo definido para la distribución de etiquetas	/ mpls ldp
local-bindings	Este submenú muestra las etiquetas asociadas a las rutas a nivel local en el Router.	/mpls local-bindings
remote-bindings	Sub-menú muestra las ligaduras de etiqueta para las rutas recibidas de otros Routers. Esta tabla se usa para construir tabla de reenvío	/ mpls remote-bindings
traffic-eng	Criterio de diseño de red que permite que el tráfico tome automáticamente la ruta más	/mpls traffic-eng interface

	óptima según en cuál encuentre ancho de banda disponible.	

Tabla 5.34. Comandos de MPLS

Fuente: Mikrotik, Manual: MPLS, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos MPLS LDP.

Comando	Descripción	Sintaxis
accept-filter	Lista de las ligaduras de las etiquetas que deben ser aceptadas por los vecinos del LDP.	/mpls ldp accept-filter
advertise-filter	Lista de las ligaduras de las etiquetas que deben ser objeto de publicidad a los vecinos del PLD.	/mpls ldp advertise-filter
interface	Lista de interfaces que se conectan a los routers de conmutación de etiquetas.	/mpls ldp interface
neignbor	Lista de todos los vecinos ldp	/mpls ldp neignbor print

Tabla 5.35. Sub-Comandos MPLS LDP

Fuente: Mikrotik, Manual: MPLS/LDP, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos MPLS TRAFFIC-ENG.

Comando	Descripción	Sintaxis

interface	Configura la interfaz de ingeniería de tráfico	/mpls traffic-eng interface
path-state	Monitorea el estado del túnel	/mpls traffic-eng path-state
resv-state	Monitorea el estado de los recursos reservados	/mpls traffic-eng resv-state print
tunnel-path	Define la ruta para el túnel	/mpls traffic-eng tunnel-path add name=tun-second-link use-cspf=no hops=192.168.33.13:strict,192.168.33.10:strict,192.168.33.9:strict

Tabla 5.36. Sub-Comandos MPLS TRAFFIC-ENG

Fuente: Mikrotik, Manual: Interface/Traffic Engineering, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Comandos de Routing.

Comando	Descripción	Sintaxis
bfd	Detecta fallas en el camino bidireccional entre dos motores de reenvío	/routing bfd
bgp	Enrutamiento dinámico solo con una opción por pares BGP para permitir BFD	/routing bgp peer add remote-address=x.x.x.x remote-as=xxxxx use-bfd=yes
filter	Filtra las redes de enrutamiento	/routing filter

mme	Protocolo de enrutamiento IP en redes malladas inalámbricas	/routing mme
ospf	Enrutamiento dinámico ospf para encaminar de forma más eficiente los paquetes	/routing ospf
ospf-v3	Protocolo de enrutamiento ospf para IPv6	/routing ospf-v3 interface add interface=ether1 area=backbone add interface=ether2 area=backbone
prefix-lists	Compara los prefijos de las rutas con los que figuran en la lista de prefijos	/routing prefix-list print
rip	Intercambio de información de enrutamiento en un sistema autónomo	/routing rip
ripng	Protocolo de enrutamiento rip para IPv6	routing ripng interface add interface=ether1

Tabla 5.37. Comandos de Routing

Fuente: Mikrotik, Category: Routing, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos Routing BGP.

Comando	Descripción	Sintaxis
advertisements	Muestra los prefijos que el router está redistribuyendo a sus compañeros	routing bgp advertisements> print 10.0.11.20
aggregate	Permite redistribuir un prefijo	routing bgp aggregate print

	grande en lugar de varios pequeños	
instance	Configura la instancia de BGP	/routing bgp instance set default as=100 redistribute-static=no
network	Permite especificar algunos prefijos arbitrarios que se anuncian sin condiciones	/routing bgp network add network=192.168.0.0/24
peer	Establece una conexión TCP entre uno y otro router	/routing bgp peer add remote-address=10.20.1.210 remote-as=65534
vpnv4-route	Prefijo de ruta distinguidora de red IPv4	/routing bgp vpnv4-route

Tabla 5.38. Sub-Comandos Routing BGP

Fuente: Mikrotik, Manual:Routing/BGP, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos Routing MME.

Comando	Descripción	Sintaxis
interface	Inicializa el protocolo MME en una interfaz	/routing mme interface add interface=wlan1
network	Determina que red se anuncia vía MME	/routing mme> network add network=1.2.3.0/24
originators	Contiene información acerca de los nodos vecinos activos	/routing mme originators

Tabla 5.39. Sub-Comandos Routing MME

Fuente: Mikrotik, Manual:Routing/MME, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos Routing OSPF & OSPFv3.

Comando	Descripción	Sintaxis
area	Agrupa a una colección de routers	/routing ospf area
as-border		
instance	Configura y ejecuta una instancia OSPF	/routing ospf instance
interface	Configura la interfaz en modo OSPF	/routing ospf interface
lsa	Configura el algoritmo de estado de enlace para encontrar la ruta mas corta	/routing ospf lsa
nbma-neighbor	Configuración manual para el acceso de múltiples canales no retransmitidos vecinos	/routing ospf nbma-neighbor
neighbor	Configura los vecinos que serán usados para formar la conexión ospf	/routing ospf Neighbor
ospf-router	Lista de todos los routers de frontera de área	/routing ospf ospf-router
route	Configura la ruta ospf	/routing ospf route
virtual-link	Configura un enlace virtual entre dos routers a través de un área común llamada zona de tránsito teniendo que estar conectado uno	/routing ospf virtual-link

	de ellos al backbone	

Tabla 5.40. Sub-Comandos Routing OSPF & OSPFv3

Fuente: Mikrotik, Manual:Routing/OSPF, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos Routing RIP

Comando	Descripción	Sintaxis
interface	Configura la interfaz sobre la cual correra el enrutamiento rip	/routing rip interface
keys	Configura las cadenas de clave de autenticación	/routing rip keys
neighbor	Define los routers vecinos para intercambiar información de enrutamiento	/routing rip neighbor
network	Define las redes en las que se ejecutaran RIP	/routing rip network
route	Configura las rutas rip	/routing rip route

Tabla 5.41. Sub-Comandos Routing RIP

Fuente: Mikrotik, Manual:Routing/RIP, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Comandos de Sistema.

Comando	Descripción	Sintaxis

backup	Guarda toda la configuración del router en un archivo de copia de seguridad	/system backup
clock	Configura la zona horaria, fecha y hora del sistema	/system clock
console	Habilita o desbilita la salida por consola	/system console
default-configuration	Configura el router a su configuración por defecto	/system default-configuration
health	muestra el actual voltaje de entrada y el status del ventilador	/system health print
history	Muestra el historial de las acciones realizadas en el sistema	/system history print
identity	Configura la identidad del router que será mostrada antes de la línea de comandos	/system identity print
leds	Configura la actividad de los leds de la manera que desee el usuario	/system leds
license	Configura la licencia en el router	/system license
logging	Especifica las acciones del sistema que figuran en el menú de acciones	/system logging
note	Permite asignar notas de texto arbitrario o mensajes que se mostrarán en cada inicio de sesión	/system note
ntp	Configura el servidor y el cliente ntp	/system ntp server set broadcast=no enabled=yes manycast=yes multicast=no

package	Lista los paquetes instalados en el router	/system package print
resource	Muestra el espacio libre en el HDD del router	/system resource print
routerboard	Muestra las características del routerboard	/system routerboard print
scheduler	Planifica la ejecución de un script en un instante de tiempo determinado	system scheduler> add name=run-1h interval=1h on-event=log-test
script	Lista los scripts creados	/system script print
upgrade	Permite la actualización del routerOS	/system routerboard upgrade
watchdog	Este menú permite configurar el sistema para reiniciar el kernel panic, cuando una dirección IP no responde, o si el sistema se ha bloqueado	/system watchdog
check-disk	Comprueba que el disco duro este libre de errores	/system check-disk
check-installation	Revisa el funcionamiento del sistema operativo RouterOS	/system check-installation
reboot	Reinicia el router	/system reboot
reset-configuration	Resetea la configuración del router a los valores de fabrica	/system reset-configuration
serial-terminal	Acceso a un dispositivo mediante el puerto serial	/system serial-terminal serial0
shutdown	Apaga el router	/system shutdown

ssh	Permite conectarse a otro router o computador usando ssh	/system ssh
sup-output	Contiene información o ayuda sobre el routeOS	/system sup-output
telnet	Permite conectarse a otro royuter o computador via telnet	/system telenet

Tabla 5.42. Comandos del Sistema.

Fuente: Mikrotik, Category: System, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos NTP.

Comando	Descripción	Sintaxis
client	Configura el cliente ntp	/system ntp client set enabled=yes mode=unicast primary-ntp=129.6.15.28 secondary-ntp=\ 129.6.15.29
server	Configura el servidor ntp	PRIMARY NTP SERVER = 159.148.60.2

Tabla 5.43. Sub-Comandos NTP

Fuente: Mikrotik, Manual: System/Time, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos RESOURCE.

Comando	Descripción	Sintaxis
cpu	Muestra el estado del cpu del router	/system resource cpu print
irq	Muestra que IRQ se utilizan actualmente por hardware	/system resource irq print
pci	Verifica los controladores que soporta nuestro router mikrotik	/system resource pci print
usb	Muestra todos los puestos usb disponibles por el router	/system reosource usb print

Tabla 5.44. Sub-Comandos Resource.

Fuente: Mikrotik, Manual: System/Resource, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos SCRIPT.

Comando	Descripción	Sintaxis
environment	Contiene todas las variables definidas por el usuario y sus valores asignados	/system script environment print
job	Contiene una lista de todos los scripts en ejecución	/system script job print

Tabla 5.45. Sub-Comandos Script

Fuente: Mikrotik, Manual: Scripting, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos UPGRADE.

Comando	Descripción	Sintaxis
mirror	Muestra desde un puerto lo que esta pasando en otro puerto	/system upgrade print
Upgrade-package-source	Añade la fuente para futuras actualizaciones	/system upgrade upgrade-package-source add address=172.16.0.2 user=admin

Tabla 5.46. Sub-Comandos Upgrade

Fuente: Mikrotik, Manual: Upgrading RouterOS, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Comandos de Queues.

Comando	Descripción	Sintaxis
interface	Cambia el tipo de cola de la interfaz	/queue interface
simple	Configuración de colas simples	/queue simple add dst-address=192.168.0.0/24 interface=ether1 limit-at=128000
tree	Configuracion de árbol de colas	/queue tree print
type	Configuración de los tipos de colas	/queue type add name=CUSTOMER-def kind=red red-min-threshold=0 red-burst=0

Tabla 5.47. Comandos de Queues

Fuente: Mikrotik, Manual: Upgrading RouterOS, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Comandos de Herramientas.

Comando	Descripción	Sintaxis
bandwidth-server	Habilita el servidor de prueba de ancho de banda	/tool bandwidth-server set enabled=yes
e-mail	Permite configurar el servidor smtp que se utilizará	/tool e-mail set server=10.1.1.1 port=25 from="router@mydomain.com"
graphing	Monitoriza diversos parámetros del routerOS	/tool graphing
mac-server	Habilita el servidor MAC para sesiones telnet	/tool mac-server add interface=ether1 disabled=no
netwatch	Monitorea el estado de las estaciones conectadas a la red	/tool netwatch print
sms	Configura el envio de mensajes mediante un modem GSM	/tool sms
sniffer	Captura y analiza paquetes enviados y recibidos por la interfaz especificada	tool sniffer start
traffic-generator	Realiza pruebas de rendimiento de trafico	/tool traffic-generator quick tx-template=r12,r13,r21,r23,r31,r32 packet-size=60 mbps=300

traffic-monitor	Muestra estadísticas del tráfico generado por la interfaz	/tool traffic-monitor
bandwidth-test	Mide el rendimiento contra otro Router o estación cliente	/tool bandwidth-test protocol=udp user=admin password="" direction=both address=10.0.1.5
dns-update	Actualiza los DNS que son dinámicos	/tool dns-update
fetch	Copia archivos desde cualquier dispositivo de red a un Router Mikrotik a través de HTTP o FTP	/tool fetch address=192.168.88.2 src-path=conf.rsc user=admin mode=ftp password=123 dst-path=123.rsc port=21 host="" keep-result=yes
flood-ping	Escanea los puertos contra ataques de DoS o DDoS	/tool flood-ping address=192.164.10.244
ip-scan	Permite escanear la red basada en algún prefijo de red o mediante el establecimiento de una interfaz de escucha	/tool ip-scan
mac-scan	Detecta todos los dispositivos que soportan el protocolo telnet MAC en la red dada.	/tool mac-scan
mac-telnet	Accede por MAC a otro Router de la red	/tool mac-telnet 00:15:F9:36:C2:XX
ping-speed	Realiza una prueba de velocidad de respuesta a una dirección específica	/tool ping-speed address=192.164.10.244
profile	Muestra el uso de CPU para cada proceso que se ejecuta	/tool profile

	en RouterOS. Ayuda a identificar qué proceso está utilizando la mayor parte de los recursos de CPU.	
torch	Monitoriza el tráfico en tiempo real para controlar el flujo de tráfico a través de una interfaz	/tool torch ether1 src-address=10.0.0.144/32 protocol=any
traceroute	Determina cuantos paquetes se enrutan a un host en particular	/tool traceroute 10.255.255.1
wol	Enciende el dispositivo por medio de la red local (wake on lan)	/tool wol mac=08:00:27:e8:02:6b interface=LAN

Tabla 5.48. Comandos de Herramientas

Fuente: Mikrotik, Category: Tools, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos MAC-SERVER.

Comando	Descripción	Sintaxis
interface	Habilita o desabilita el acceso telnet MAC por dicha interfaz	/tool mac-server add interface=ether1 disabled=no

Tabla 5.49. Sub-Comandos Mac-server

Fuente: Mikrotik, Mac Access, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Sub-Comandos TRAFFIC-GENERATOR.

Comando	Descripción	Sintaxis

packet-template	Permite construir paquetes basándose en los parámetros proporcionados	/tool traffic-generator packet-template
port	Permite configurar los puertos que se asociarán a una interfaz y se utiliza para recibir/enviar paquetes generados	/tool packet-generator port
raw-port-template		
stats	Almacena todas las estadisticas a cerca de la prueba cuando el generador de tráfico no se está ejecutando en modo rápido	/tool traffic-generator stats
stream	Almacena las estadísticas ordenadas por streams	/tool traffic-generator stats stream
quick	Permite iniciar rápidamente el generador de paquetes e imprimir la salida de las estadísticas de la terminal.	/tool traffic-generator quick mbps=450
start	Inicia la herramienta de generador de tráfico	/tool traffic-generator start
stop	Para la herramienta de generador de trafico	/tool traffic-generator stop

Tabla 5.50. Sub-Comandos TRAFFIC-GENERATOR

Fuente: Manual: Tools/Traffic Generator, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Atributos

Los atributos en Mikrotik son más comúnmente utilizados como metadatos que no es más que datos de datos como lo es el caso del comando “comment” que contiene información adicional para identificar diferentes configuraciones realizadas en el sistema operativo, pero también son atributos las propiedades de los objetos como por ejemplo el tipo de dato de una variable (tipo date de la variable fecha).

5.1.2.3 Comandos de Respuesta

Los comandos de respuesta son aquellos que retornan un valor a consecuencia de una solicitud causada por otro comando que es llamado comando de consulta. Estos son comandos vitales para el correcto funcionamiento del sistema operativo.

5.1.2.4 Comandos de Consulta (Query)

Los comandos de consulta son aquellos que están destinados a realizar peticiones al sistema operativo para conocer acerca del estado de diferentes configuraciones, esto puede ser consultar el estado de una dirección ip si esta activada, desactivada, bloqueada, suspendida, etc. Estos son comandos que se utilizan con bastante frecuencia ya que la mayor parte del tiempo el usuario del sistema operativo realiza consultas sobre diferentes estados de las configuraciones hechas.

5.1.2.4.1 Descripción de comandos de Consulta

Los comandos de consulta están destinados solamente con propiedades de lectura tales como el comando print que lo que hace es mostrar el estado de configuración y funcionamiento del proceso creado o de la configuración de los diferentes parámetros del dispositivo en cuestión.

5.1.2.5 Tags

Es importante diferenciar las respuestas que los comandos envían luego de su ejecución cuando se ejecutan varios comandos simultáneamente, para esto se utiliza el parámetro “tag”.

Al incluir el parámetro “tag” se lo debe hacer con un valor no vacío en su sentencia para diferenciar entre una respuesta y otra, si se lo utiliza con un valor vacío no se podrá diferenciar entre una respuesta y otra.

Ejemplo:

Deshabilitar Interfaz

/interface/set=disabled=yes=.id=ether1.tag=interface.

5.1.2.6 Ejemplos de Comandos de Consulta

Ejemplo:

/interface ethernet print → Realiza una consulta al sistema operativo sobre el estado de las interfaces del sistema operativo.

/ping 192.164.10.210 → Consulta si la dirección IP 192.164.10.210 está enlazada o no a la red.

5.2 iNetControl V1.0 como sistema de administración Web para control de abonados y gestión de planes de Internet en el WISP Sigsignet

Dada la necesidad de mejorar la gestión y control de usuarios, planes de Internet y control de cobros en la empresa Sigsignet nace la idea de crear un sistema de gestión y administración para WISP orientado al Web y con integración a Mikrotik, de tal manera que permita automatizar procesos que antes eran realizados de forma

mecánica, y sobre todo brindar un control más preciso y estadísticas detalladas no solo de conexión sino pagos, este subtema no pretende abarca el proceso de creación del sistema y la metodología empleada para su desarrollo sino más bien comprende ser una solución a un problema latente como lo es la falta de control que la empresa tenía en disponer de un sistema de esta categoría que apoyara los diversos proceso que la empresa tiene no solo en cuanto a pagos sino estadísticas de conexión, averías etc.

5.2.1 Descripción y Objetivos del Sistema

El sistema estará compuesto de la siguiente manera:

- Acceso al sistema con un nombre de usuario y contraseña específico para cada usuario con su nivel de acceso.
- Administración de clientes
- Administración de contratos
- Servicio de pagos
- Reportes de Clientes
- Reporte de cobros
- Facturación de servicios
- Servicio Técnico

Los objetivos de la creación del sistema son:

- Facilitar y agilizar la gestión de cobros
- Llevar un inventario de todos los clientes que han ingresado y han salido de la empresa
- Dar una mejor atención al cliente
- Mostrar una nueva imagen con la manera de realizar los cobros
- Tener un control del área de servicio técnico en donde se pueda manejar diferentes estados (en espera, procesando, reparado).

5.2.2 Descripción de Topología de Red a ser implementada

Se tendrá un servidor de aplicaciones ubicado en la oficina Cuenca o Matriz con una IP Privada y con restricción de acceso solo para IP establecidas dentro del sistema y del Gateway, el servidor de aplicaciones será alojado dentro una DMZ, la comunicación con las diversas sucursales se la realizará por medio de un túnel L2TP con una capa de encriptación IPSec, para acceder al sistema bastará con estar conectado a la red interna y desde la IP autorizada en este caso serán de las oficinas de la sucursal del Sigsig. En el caso de querer acceder desde fuera de la red se tendrá creada una VPN con nombres de usuarios y contraseñas específicos para los administradores del sistema.

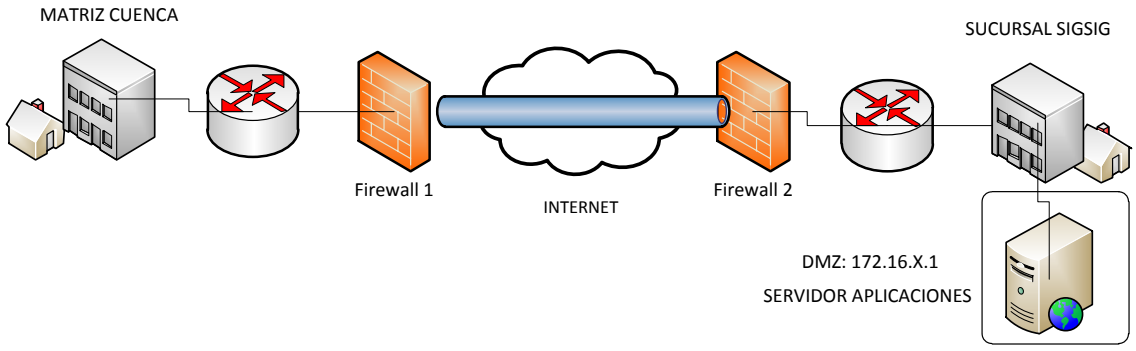


Figura 5.2. Topología de Ubicación de Servidor de Aplicaciones.

Fuente: Los Autores, Topología Ubicación Servidor de Aplicaciones, 2013.

5.2.3 Estructura y Funcionamiento lógico del Sistema

Si bien iNetControl en su versión 1.0 sigue aún en fase de desarrollo con algunos módulos funcionales y con constantes actualizaciones, desde sus cimientos se contempló en su estructura el control de diversos segmentos de negocios asociados a proveer servicios de Internet, y no solo ello sino toda la lógica de negocio implícita en la gestión y administración de un ISP, y sobre todo la integración con Mikrotik, con el fin de automatizar procesos antes desarrollados de forma manual.

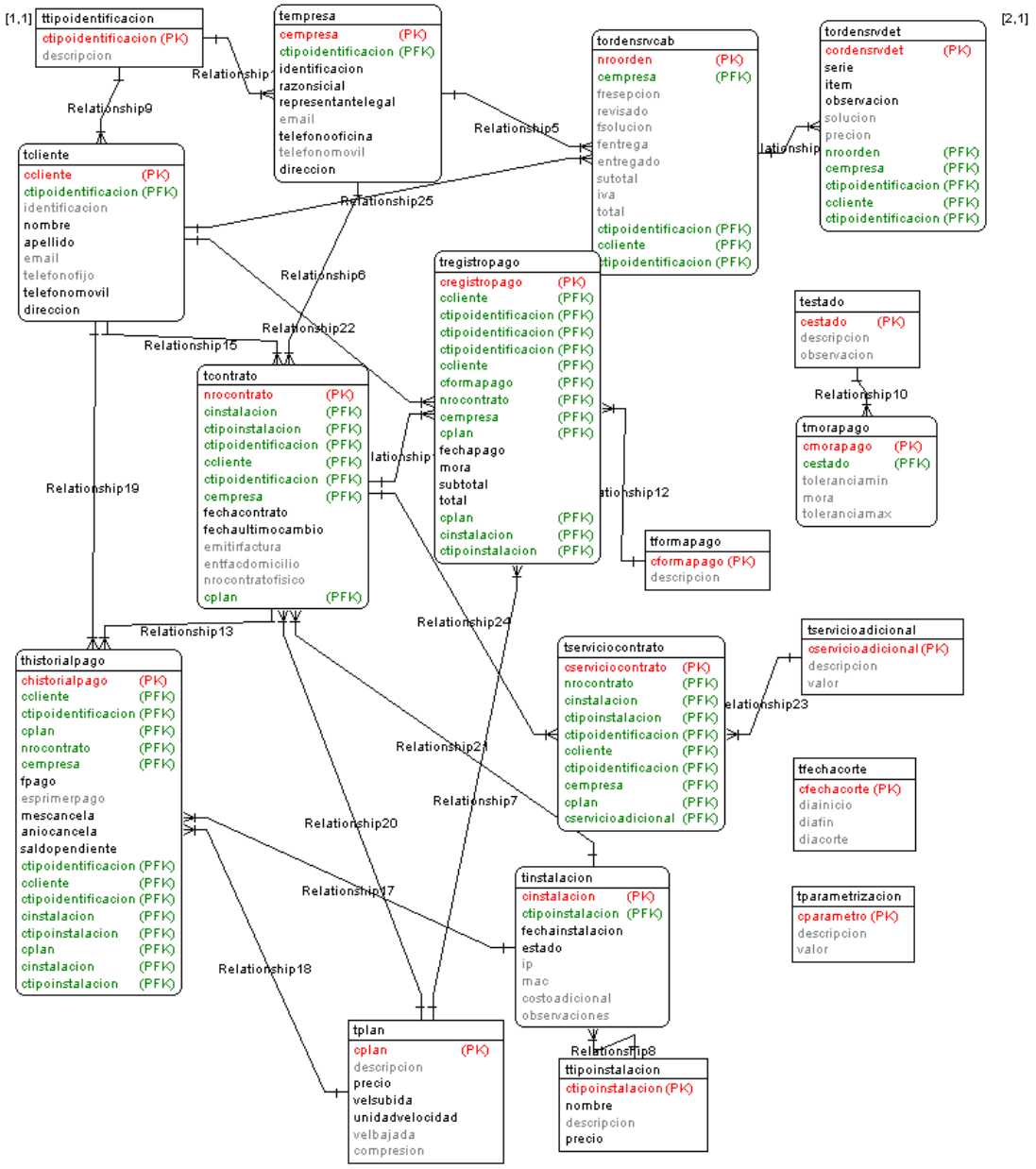


Figura 5.3. Modelo E-R de base de datos del sistema iNetControl.

Fuente: Los Autores, Diagrama E-R iNetControl, 10 de Diciembre 2013

5.2.3.1 Implementación del cliente de conexión para comunicación con RouterOS.

La arquitectura de desarrollo de esta aplicación desde sus inicios se contempló un modelo basado en capas, estableciendo una exclusivamente para comunicación con los equipos de red, posibilitando con ello desde la aplicación Web el envió de comandos así como la recolección de datos de los equipos de red y su posterior

almacenamiento en la base de datos, en el caso de Mikrotik el poder disponer de un API incluso con soporte para encriptación, se considera una funcionalidad de mucha ayuda hacia el sistema, no solo por la serie de herramientas y el completo acceso a estadísticas que de los equipos que se podría tener sino por el hecho de poder intercambiar información, y solo ello sino la automatización de algunos procesos antes llevados de forma manual como entre uno de ellas la suspensión del servicio por falta de pago automáticamente.

Lenguajes de programación a utilizar

El lenguaje de programación que se utilizará es Java por medio de un Framework denominado Play con el que se pretende reducir el tiempo de desarrollo de la aplicación en conjunto con una base de datos PostgresSQL, herramientas con las que se busca forma una solución robusta y confiable.

5.2.3.2 Plataforma base a utilizar.

La plataforma sobre la cual se desplegará el aplicativo es un JBoss Server en su versión 7 altamente robusta y eficiente, la misma será montada sobre un sistema operativo CentOS y sobre un Hardware dedicado utilizando Intel Xeon en el procesamiento, JBoss como tal se considera un servidor de aplicaciones para e-business con una arquitectura orientada a servicios SOA y con licencia GNU de código abierto, pudiendo el mismo ser descargado, utilizado y distribuido sin restricciones por la licencia.

5.2.4 Pruebas de Funcionamiento

A continuación se muestran las capturas de pantalla del sistema en funcionamiento que se ha puesto ya en marcha en las oficinas de Cuenca para la gestión de cobros y cortes automáticos del servicio a clientes en mora.

Para tal describiremos las siguientes pantallas de la aplicación:

El login de usuario permite dos modos de acceso uno por medio solo de cédula de identidad para consulta de facturas y otro con usuario y contraseña para acceso total al sistema y servicios adicionales, siendo necesario ingresar las credenciales entregadas en el contrato y a su vez enviadas al correo, modificables la primera vez que ingresa el usuario.

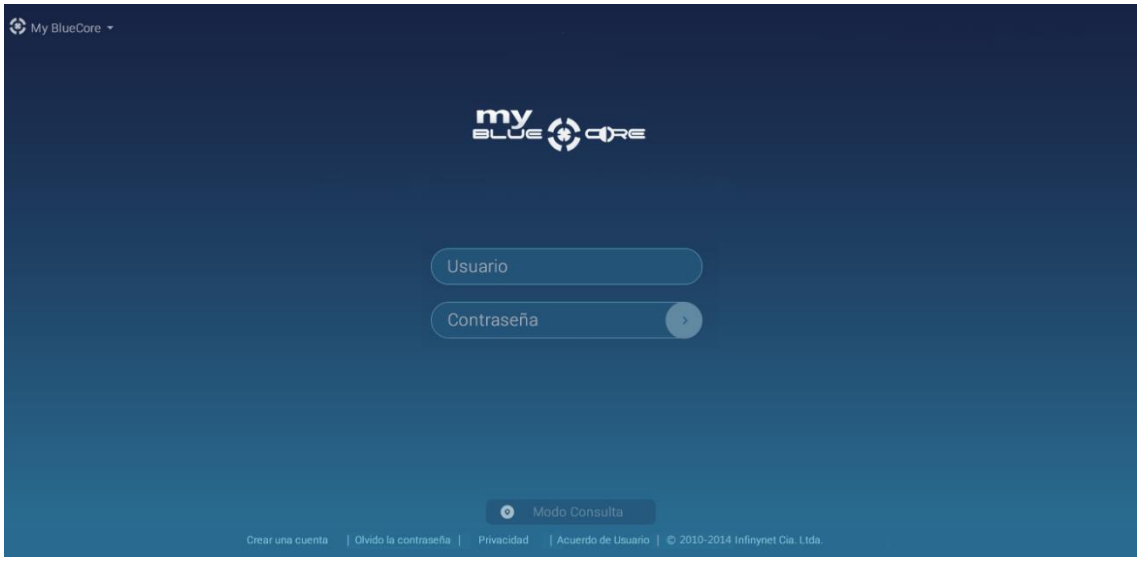


Figura 5.4. Página de acceso al sistema iNet.

Fuente: Los Autores. Login de Usuario iNetControl, 2013

Clientes.

Una vez que se haya ingresado al sistema con el usuario respectivo se tendrán varias opciones habilitadas acorde al rol de cada usuario. Como se puede observar en las Figuras 5.5. y 5.6. Al dirigirse a la pestaña “ADMINISTRACION” se puede sacar un reporte de todos los clientes que se han ingresado al sistema iNet.

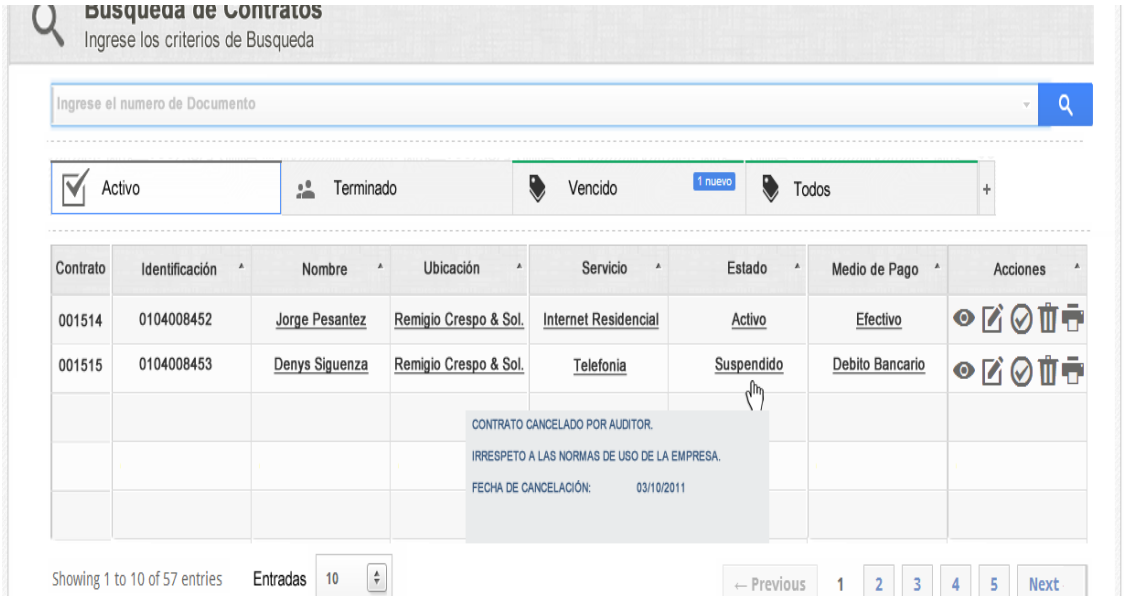


Figura 5.5. Reporte de clientes.

Fuente: Los Autores, Reporte de Cliente iNetControl, 2013

Nuevo contrato.

La creación de un nuevo contrato es realizada mediante un asistente o Wizard, dicha metodología contemplada con el uso de validaciones estricticas evita que los usuarios destinados a manejar la plataforma tengan problemas con el llenado del contrato en todo su proceso de manera tal que se pueda cumplir con todos los requisitos necesarios para dar de alta el contrato.

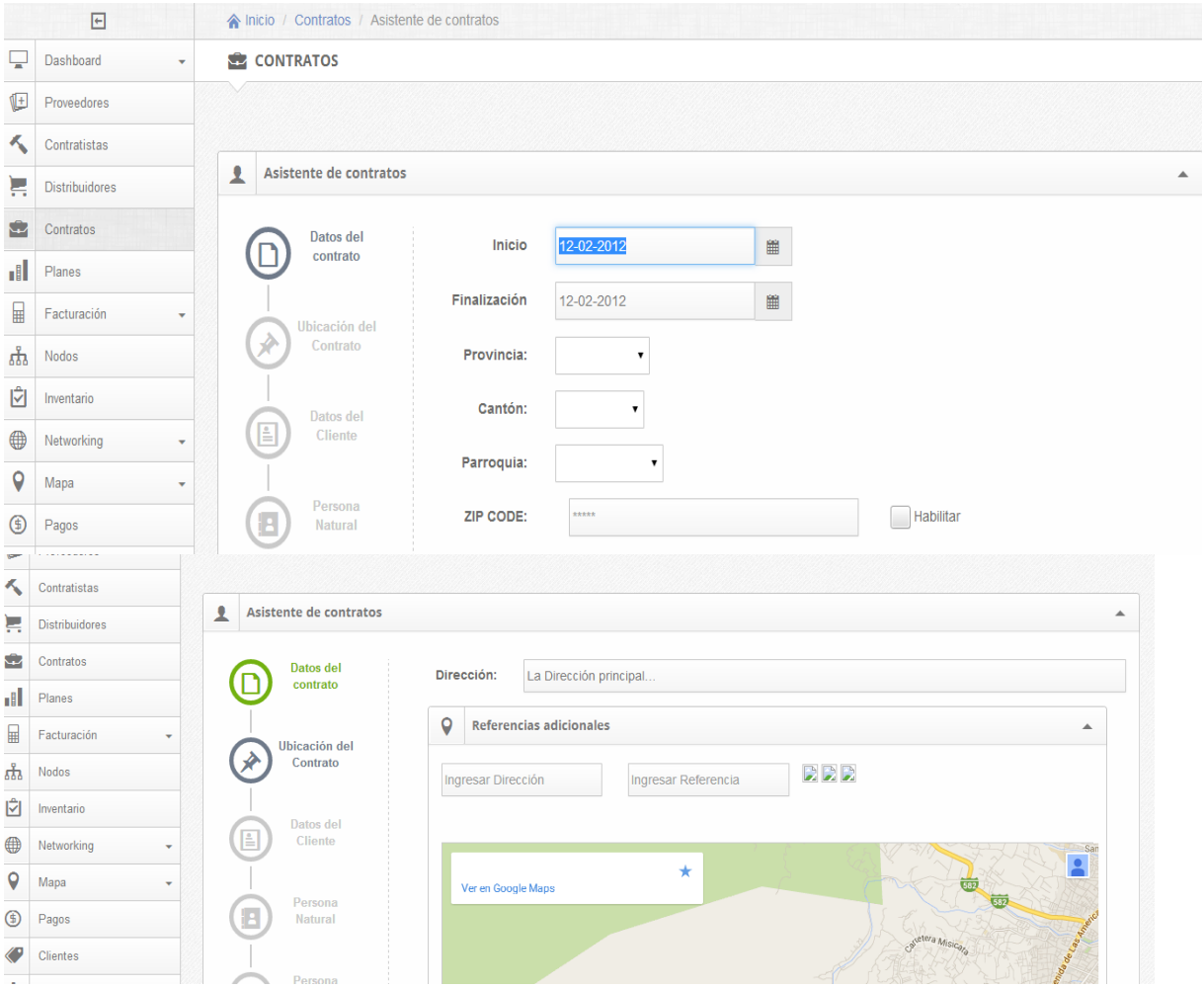


Figura 5.6. Asistente para creación de Nuevo Contrato.

Fuente: Los Autores, Nuevo Contrato, 2013

Búsqueda de contrato.

La parte de búsquedas en el sistema es imprescindible y procurando una experiencia de usuario amigable, se ha establecido en la misma opción de buscar campos de búsqueda avanzados que ayudarán a identificar rápidamente cualquier información necesaria.

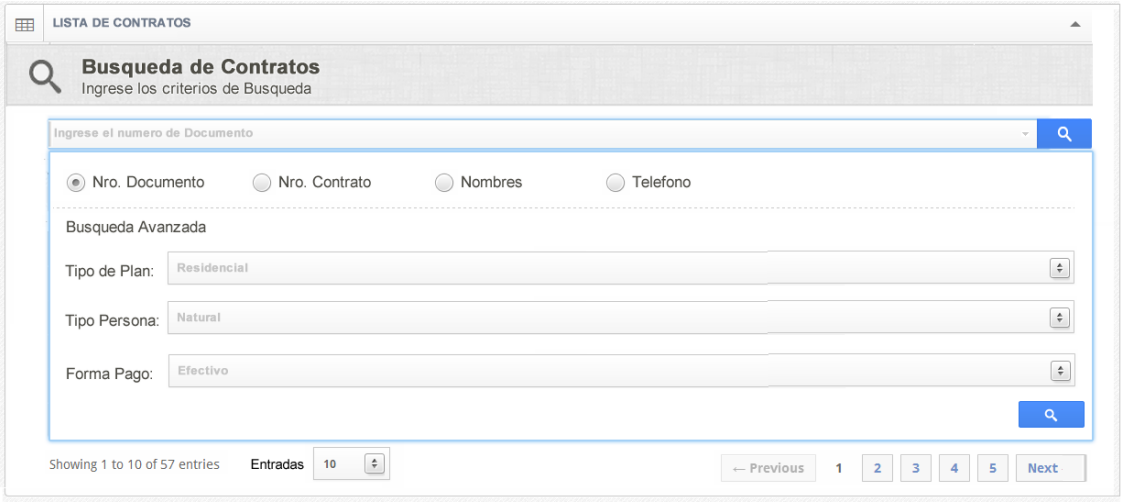


Figura 5.7. Búsqueda de Contratos.

Fuente: Los Autores, Búsqueda de Contrato, 2013

Pagos.

En la Figura 5.8. y 5.9. Se tiene la opción para ingresar y registrar un nuevo pago para los abonados. Este pago se registra y se coteja con la fecha de corte para enviar un comando a RouterOS que posibilitará mantener un estado de corte con notificación caso de registrar valores pendientes a pagar. Cabe recalcar que el sistema siempre registrará un primer pago adicional con un costo de instalación.

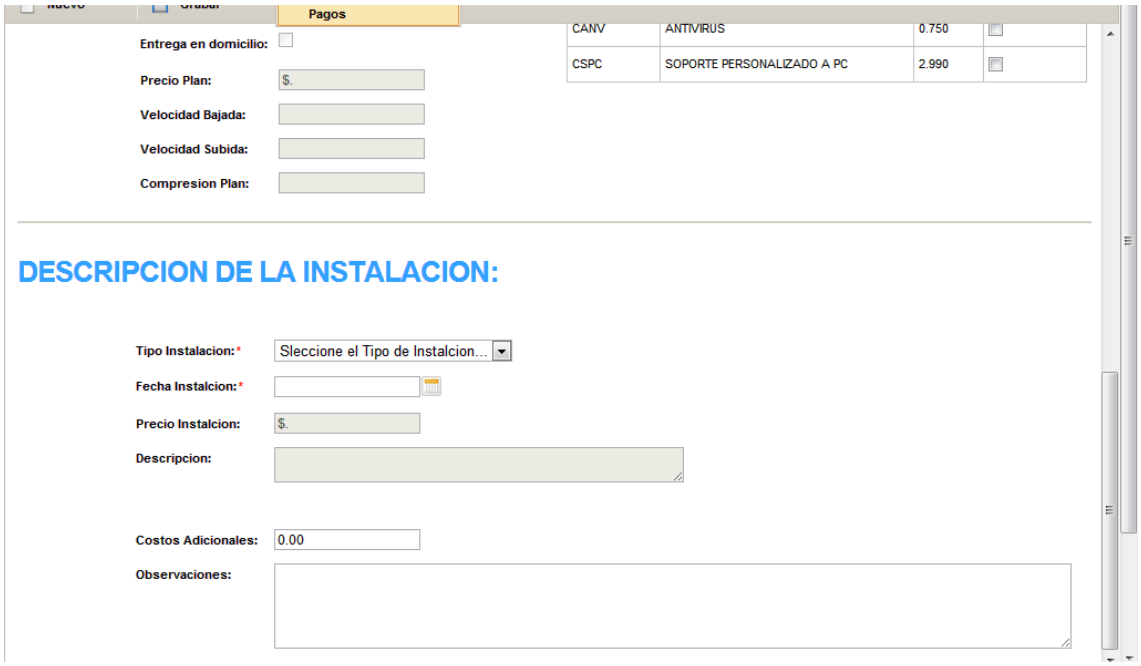


Figura 5.8. Opción de Pagos

Fuente: Los Autores, registro de Pagos, 2013

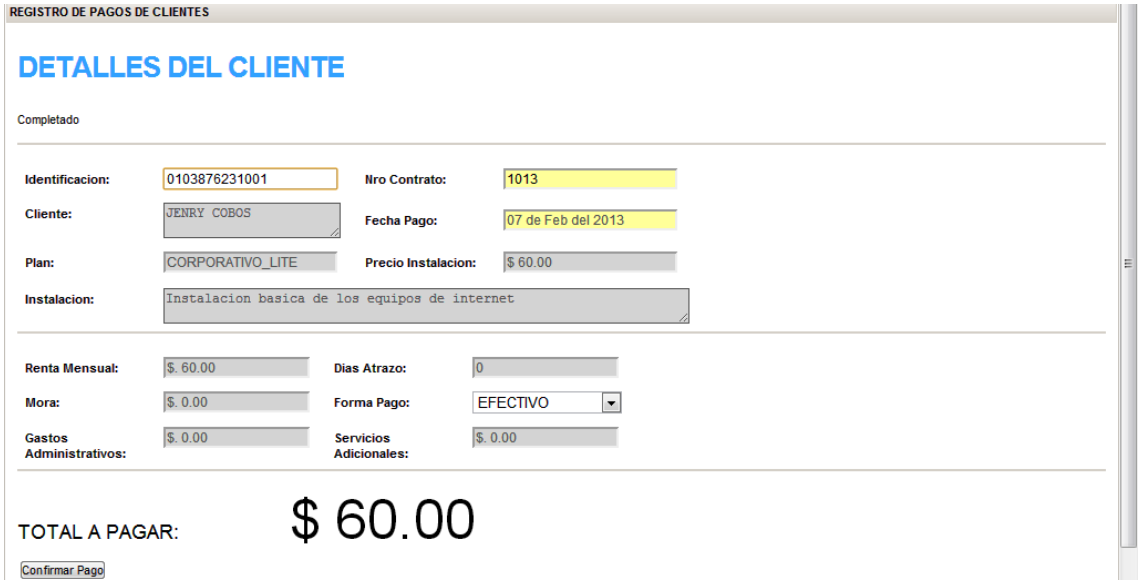


Figura 5.9 Registro de nuevo pago.

Fuente: Los Autores, registro de nuevo pago, 2013

Conclusiones del Capítulo 5

En este capítulo se puede decir que ha ayudado a entender de una mejor manera la estructura con la cual trabaja Mikrotik ya que se ha adentrado en un nivel más bajo dado que se pudo conocer sobre sus comandos más básicos hasta sus sentencias más complejas y de esta manera permite administrar desde un programa externo tan solo con la utilización de su API. La ayuda que presenta utilizar el sistema personalizado acorde al tipo de negocio que se tiene es significativa ya que sus recursos se están empleando de mejor manera y se aprovecha más el tiempo que se ahorra en dar soporte técnico en la oficina directamente.

CAPÍTULO VI: ANALISIS DE RESULTADOS.

Objetivos:

- Determinar un análisis de resultados entre la red actual y la deseada, que permitan como medio de verificación comprender las mejoras adoptadas y el nivel de rendimiento presente en la nueva red.

Objetivos Específicos:

- Establecer un cuadro comparativo de las mejoras implementadas dentro de la red.
- Elaborar un análisis de rendimiento de la nueva red y servicios.

6.1 INTRODUCCION

El análisis de resultados es una parte fundamental del desarrollo de este proyecto que busca determinar la efectividad en el proceso de implementación de la nueva red de datos en comparativa con la red actual del proveedor, dicho análisis comprende un grupo de pruebas debidamente estructuradas que buscan obtener indicadores de rendimiento puntuales y permitan a su vez denotar claros resultados entre las dos redes en comparativa.

Para la estructuración de dichas pruebas sobre la red deseada y con el fin de dotar de las condiciones necesarias a las que puede una red de datos estar sometida, herramientas como Traffic-Generator, Bandwith Test etc. de Mikrotik, han sido elementos clave para disponer de un ambiente con condiciones similares e incluso más exigentes que las que actualmente tiene la red de datos del proveedor y posibilitar así disponer de un escenario de iguales condiciones sin ser necesario el riesgo con la red de datos deseada de su temprana puesta en producción y el riesgo que ello conlleva con redes experimentales y el controlar de pequeños errores que puedan surgir en la marcha, que si bien pueden ser sencillos de corregir podrían afectar al continuo servicio que se brinda, sobre la red actual cabe recalcar que las pruebas serán llevadas a cabo a diversas horas del día y bajo condiciones de saturación y no saturación.

Descripción	Red Antigua	Red Actual
PRINCIPALES CARACTERISTICAS		
Control de Ancho de Banda	Script por CBQ desde Linux	Control eficiente del ancho de banda por PCQ y algoritmos relacionados. (Árbol de Colas y colas simples), implementación de calidad de servicio (QoS).
Enrutamiento	Sin Enrutamiento (Bridge Lógico)	Con Enrutamiento (Estático + OSPF)

Monitor de Red	Sin Monitor de Red	Monitor Dude personalizado para la Red, con soporte SNMP habilitado para monitoreo de recursos en los diversos dispositivos de red.
Servidor DNS	Con servidor DNS de terceros, tiempos de respuesta elevados.	Servidor DNS propietario, reducción de tiempos de respuesta.
Automatización de Tareas de Mantenimiento por medio Scripts	Sin automatización definida, altos tiempos de soporte.	Scripts de Definidos por medio de Mikrotik para tareas de ajustes de tipos de cola, estadísticas de consumo de IP, pruebas de conectividad automatizadas a Abonados, a Radio Bases y Proveedor de Última Milla.
Control de Cortes de Servicio por falta de pago automatizado.	(Corte Lógico) por punto de distribución o AP, tedioso y tiende a causar confusión u olvidos.	(Corte Lógico) Mediante sistema de control iNet Control, con notificaciones programadas de aviso por E-Mail
Alta Disponibilidad en el NOC	No presente	Presente en el NOC tanto mediante equipos de contingencia de Networking, enlaces de contingencia de última milla, así como por energía mediante sistemas de Backup por inversores

		y baterías.
Políticas y Sistema de Manejo de Backups de configuraciones de Equipos de Red.	No presente	Automatizado mediante Scripts y Correo Electrónico
SEGURIDAD & POLITICAS		
Control de Acceso a NOC	Control de acceso por ACL en AP's	Control de Acceso por Firewall, por AP y basado en reglas de conexión.
Control y Políticas de acceso externo a la red de datos y NOC para tareas de mantenimiento.	Sin Control Establecido	Por Firewall, acceso por medio de lista permitidos por servidor VPN.
Políticas contra ataques e Intrusiones no deseadas	Sin Políticas Establecidas	Políticas definidas a nivel de Firewall para prevención de servicios de red sensibles a ataques,
Políticas de Administración de Claves CPE	Sin Políticas Definidas (Un solo user y pass por todos los equipos)	Administradas por iNet Control y por contrato establecido.
WIRELESS		
Administración Espectro	Sin administración Establecida	Administración del Espectro por Mikrotik, complementada con Dude, y herramientas dedicadas de Mikrotik
Encriptación Wireless	Solo con soporte WEP	Con soporte WEP, WPA y WPA2.
Rate de Radio Bases Multipunto	Configuración por defecto	Configuración personalizada para manejar rates específicos, y evitar la saturación del espectro

Control de Conexiones Máximas por Radio Base	Sin Control	Se establece acorde troughput de la Base en relación a monitoreo de recursos de equipo como CPU y RAM así como el monitor de red y en relación con sistema de administración iNetControl, que detalla usuarios conectados a dicha base.
Habilitación de Protocolos basados en TDMA (Nstreme) para enlaces robustos entre radio base y estaciones CPE.	Sin Soporte para dicho protocolo	Habilitado con radio bases Mikrotik
Control de Ruido entre Bases en el mismo Punto de Distribución, relación Front – Back.	Sin Control	Control con separación adecuada y elementos materiales adicionales en los puntos de distribución.

Tabla 6.1. Cuadro comparativo de mejoras implementadas

Fuente: Los Autores, cuadro comparatio de mejoras implementadas, 2014

6.2 Análisis de rendimiento de la nueva red y servicios.

Para establecer un análisis cuantitativo sobre la red y sus servicios es necesario recolectar determinada información de relevancia establecida sobre la red de datos tanto actual como deseada, algunos resultados ya obtenidos en puntos anteriores, pero consolidados en esta, la parte final de este proyecto.

- **Latencia en el NOC y Backbone.**
    - Sobre dicho punto y previo análisis denotado en el capítulo 3, la latencia existente en uno de los enlaces del proveedor ubicado entre Sigsig y Cerro Huallil (Puntos de Distribución) es muy notorio y la más preocupante por ser parte del Backbone, según figura 3.19 y tabla 3.6, adicional a este algunos enlaces Multipunto ubicados denotados con los nombres de "Plusnet", "Sigsignet" y Furianet en el punto de distribución en el cerro Huallil con problemas similares, arrojando para tal los siguientes resultados ya denotados en el capítulo 3.

Latencia entre Enlace Sigsig-Huallil (Capacidad de Carga 20 Mbps)	**Red Antigua**	**Red Actual**
Latencia de enlace a máxima capacidad entre Enlace Proveedor y Equipo distribuidor o radio Base Huallil	- Promedio: 70 ms - Perdida de Paquetes 1% a 5% variable de acuerdo a congestión elevada.	(Reubicación Enlace directamente cerro Huallil) - Promedio: 0 ms - Perdida de Paquetes 0%
Latencia a Internet, dominio www.google.com	- Promedio: 90 ms	- Promedio: 27 ms
Latencia desde un abonado del servicio a Internet, dominio www.google.com	- Promedio sin Saturación : 115 ms - Promedio con Saturación : 140 ms, con pérdida de paquetes 3%	- Promedio sin Saturación : 40 ms - Promedio con Saturación : 60 ms, con pérdida de paquetes 0%
Latencia Bases: Sigsignet, Plusnet y Furianet, prueba ejecutada desde cliente Wireless a 2 Km distancia.	- Promedio sin Saturación: 70 ms (Muy Variable) 1% perdida de paquetes. - Promedio con Saturación: 110 ms, 4% perdida de	- Promedio sin Saturación: 2 ms 0% perdida de paquetes. - Promedio con Saturación: 10 ms, 0% perdida de paquetes.

	paquetes.	

Tabla 6.2 Latencia entre Enlace Sigsig-Huallil

Fuente: Los Autores, Latencia entre Enlace Sigsig-Huallil**,** 2014

- **Throughput de Radio Bases.**
  - Asociado al problema de latencia antes denotado son los cuellos de botella existentes se denotan por la saturación de recursos existentes en las radio bases, o a su vez por la mala administración del espectro explicados en el capítulo 3

Enlace	Red Antigua	Red Actual
Enlace 5.8 Ghz, Huallil - Sigsig	- Troughput promedio arrojado: 30 Mbps Consumo de Recursos: 90 - 100% - Sin variante de TDMA activa.	- Enlace reubicado, capacidad internacional adquirida directamente al NOC.
Enlace 2.4 Ghz Huallil – San Bartolo	- Troughput promedio arrojado: 10 Mbps Consumo de Recursos: 80 - 90% -Sin Control de Rates, CPE se conectan a la máxima tasa de rate. - Con variante de TDMA activa (Airmax).	- Troughput promedio arrojado: 50 Mbps Consumo de Recursos: 40-50% -Control de Rates por CPE - Con variante de TDMA activa (NV2)
Enlace 2.4 Ghz Huallil – Cutchil	- Troughput promedio arrojado: 13 Mbps Consumo de Recursos: 100%	- Troughput promedio arrojado: 50 Mbps Consumo de Recursos: 40-50%

	-Sin Control de Rates, CPE se conectan a la máxima tasa de rate. - Con variante de TDMA activa (Airmax).	-Control de Rates por CPE - Con variante de TDMA activa (NV2)

Tabla 6.3 Throughput de Radio Bases

Fuente: Los Autores, Throughput de Radio Bases, 2014

CONCLUSIONES

Indudablemente una red de datos debe estar en constante evolución y mejora y sobre todo en un proveedor de servicios de Internet, con la actual tendencia de elevados anchos de banda y el llamado “Internet de las Cosas” que busca conectar casi todo dispositivo electrónico a Internet, demandarán dichas mejoras que sean realizadas de forma constante, y no solo esto sino también el posibilitar brindar un servicio de calidad hacen un referente como proveedor del servicio en la zona. Como tal el propósito de este proyecto fue buscar una mejora sustancial sobre la condición actual de la red y evitar problemas latentes si bién que no aquejaron en un tiempo significativo pero que con el crecimiento de la red se hicieron presentes cada vez más y más.

RECOMENDACIONES

Para mantener siempre a flote un tipo de negocio como lo es un WISP se debe tener presente que la calidad de servicio se debe mantener en constante mejora y evolución tanto la infraestructura de red física asi como las configuraciones de la red de datos para que conforme la tecnología vaya avanzando y sus requerimientos sean cada vez mas altos la empresa pueda mantenerse siempre con un algo grado de confiabilidad por parte de sus clientes.

BIBLIOGRAFIA

equipoteccelaya, Norma, Estándar, Modelo, 07 de Febrero del 2009, http://equipoteccelaya.blogspot.es/1234029360/norma-est-ndar-modelo/

WordReference, protocolo-Definición, 3 de Septiembre del 2013, http://www.wordreference.com/definicion/protocolo

ALARCON HERRERA, ERIKA; CROVETTO HUERTA, CHRISTIAN, Redes de Computadoras y Conectividad, Editorial Megabyte, 20 de Diciembre del 2004,

TEXTOS CIENTIFICOS, TCP/IP y el modelo OSI, 02 de Octubre de 2006.

UCOL, Modelo OSI, 07 de Junio de 2001 http://docente.ucol.mx/al008353/public_html/tarea2.htm

Ms.Gonzalez, El switch: cómo funciona y sus principales característicasr, 08 de Noviembre de 2013, http://redestelematicas.com/el-switch-como-funciona-y-sus-principales-caracteristicas/

"Salvan: Cradle of Wireless, How Marconi Conducted Early Wireless Experiments in the Swiss Alps", Fred Gardiol & Yves Fournier, Microwave Journal, February 2006

UPV, Diagramas de Radiación, 13 de Enero de 2004, http://www.upv.es/antenas/Tema_1/diagramas_de_radiacion.htm

Iván Bernal, Revisión de Conceptos Básicos de Antenas y Propagación, 21 de Abril de 2006 http://clusterfie.epn.edu.ec/ibernal/html/CURSOS/AbrilAgosto06/Inalambricas/CLASES/AntenasParteI.pdf

INFOSATELITE, Diagrama de Zona de Fresnel, http://www.infosatelite.net/wifi.php.

José Paul Alvarado Robles, Zonas de Fresnel, QUETZALTENANGO, 22 DE OCTUBRE DE 2008, http://es.scribd.com/doc/55774691/zonas-de-fresnel

n/d, 30 de Mayo de 2010, Patrones de Radiación,
http://rdspako.blogspot.com/2010_05_01_archive.html

Conceptos Generales de Antenas, 2011,
http://www.edutecne.utn.edu.ar/wlan_frt/antenas.pdf

Wahba Y.; Madugula M. And Monforton G. "Evaluation of non-linear analysis of guyed antenna towers". Computers and Structures. 1998, vol. 68

DISCHER, STEHHEN R.W, "RouterOS by example", Learn Mikrotik, 2011

Mikrotik, Niveles de Licencimiento, Abril del 2013,
http://wiki.mikrotik.com/wiki/Manual:License_levels

Mikrotik, Download Mikrotik software products, 2013,
http://www.mikrotik.com/download

MIKROTIK, "Paquetes disponibles RouterOS", 2013,
http://wiki.mikrotik.com/wiki/System/Packages_spanish

Mikrotik, Packet Flow Firewall, 19 de Marzo del 2013,
http://wiki.mikrotik.com/wiki/Manual:Packet_Flow

Deepankar Medhi, "Network Routing:Algoritms, Protocols and Arquitectures", Morgan Kauffman, 2007

Routing in the Internet Second Edition",Christian Huitema, Pretince Hall, 3 de Diciembre del 1999.

Mikrotik, Lista de Productos RouterBoard, 2013, http://www.mikrotik.com/

Mikrotik, Queues, 2013, http://wiki.mikrotik.com/wiki/Manual:Queue

Mikrotik, SwOS, 2013, http://wiki.mikrotik.com/wiki/SwOS

Ubuntu, 2013, http://www.ubuntu.com/download/server

NTOP, Summary Traffic IP, 2013, http://openmaniak.com/cacti_plugins.php

MAURO DOUGLAS, SCHMIDT KEVIN, Essential SNMP, Second Edition

UNIVERSIDAD DEL AZUAY, SNMP, 18 de enero de 2013, http://www.uazuay.edu.ec/estudios/sistemas/teleproceso/apuntes_1/snmp.htm

SNMP, un protocolo de simple gestión, J. Manuel Huidrobo, 16 de Marzo de 2009, http://www.coit.es/publicac/publbit/bit102/quees.htm

D. Guerrero, Management Information Base MIB, 15 de Agosto de 2013, http://www.linuxfocus.org/Castellano/January1998/article21.html

Protocolo SNMP, 17 de diciembre 2013, http://neo.lcc.uma.es/evirtual/cdd/tutorial/aplicacion/snmp.html

Luis R., El modelo jerárquico de 3 Capas de Cisco, 28 de Noviembre de 2008, http://www.cisco.com/web/LA/soluciones/educacion/cs_edu_networkers.html

Jimmy Hernandez, Introducción a TCP/IP(La capa de acceso de red), 18 de Junio de 2008, http://expertoccna.blogspot.com/2008/06/la-capa-de-acceso-de-red-tambin-se.html

Universidad Veracruzana, Adair Santos G.,La Seguridad Informatica en Redes Inalambricas, Xalapa-Enríquez, Veracruz Agosto 2008

DLink, Network Interface Gigabit DLink, Enero 2013, http://www.dlink.com/es/es/support

Luis R., Modelo Jerárquico 3 capas de Cisco, 11 de Noviembre de 2008, http://ipref.wordpress.com/2008/11/28/modelo-jerarquico-de-red/

D-Link, DES-1008D Características Técnicas, 2012, http://www.dlinkla.com.ec/des-1008d

Cisco, Switches inteligentes Cisco de la serie 200 Cisco Small Business, finales de 2013. http://www.cisco.com/c/dam/en/us/products/collateral/switches/small-business-100-series-unmanaged-switches/data_sheet_c78-634369_Spanish.pdf

Luis R., Modelo Jerárquico 3 capas de Cisco, 11 de Noviembre de 2008, http://ipref.wordpress.com/2008/11/28/modelo-jerarquico-de-red/

Mikrotik & Intel, Modelos de Router, 2012.
Infinynet Cia. Ltda, Topología Planes Compartidos, 2014.

Mikrotik - RouterBoard, Lista de Dispositivos, 2014, http://wiki.mikrotik.com

J.Michael,Stewart, Network Security, Firewalls and VPNS, 27 Agosto 2010.

Stheper Discher, RouterOS by example, 30 Noviembre 2011.

Sigsignet, Departamento Networking, 2013

Sigsignet, Estadísticas de Consumo, 2009

Sigsignet, Estadísticas de Consumo, 2014

D. A. Howe; T. N. Tasset, "Clock Jitter Estimation based on PM Noise Measurements", Boulder, CO 80305, 2003.

Foro Ryohnosuke, Configuración de "The Dude" como network managment system, 2013

Mikrotik, (n.d.). Network Address Translation, http://es.wikipedia.org/wiki/Network_Address_Translation

Luis Morales, Universidad de las Américas de Puebla, (n.d.). Redes VPN con tecnología MPLS, http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/morales_d_l/indice.html

PERAHIA ELDAD, STACEY ROBERT, Next Generation Wireless LANs: 802.11n and 802.11ac, 2013

Alfredo Giordano, QoS in RouterOS v6.x, MUM Italia 2014, p 8

DISCHER, STEHHEN R.W, "RouterOS by example", Learn Mikrotik, 2011, p 100

Mikrotik, Interface PPPoE, 2013, http://wiki.mikrotik.com/wiki/Hotspot,_apply_different_limits_and_different_traffic_priorities

Red de Centros SAT, Medidas de seguridad básicas: Los puertos de tu router, 2 de Mayo de 2014, https://www.fundacionctic.org/sat/articulo-medidas-de-seguridad-basicas-los-puertos-de-tu-router

UTN, Facultad Regional la Plata-Argentina, Comandos de Red, 2005, p 1, www.frlp.utn.edu.ar/materias/redesdeinformacion/tp4red.doc

Sergio Hernando, Instalación de la herramienta de monitorización Cacti en FreeBSD, 26 de febrero de 2008, http://www.sahw.com/wp/archivos/2008/02/26/instalacion-de-la-herramienta-de-monitorizacion-cacti-en-freebsd/

Mikrotik, Tipos de datos, 14 de Febrero del 2014, http://wiki.mikrotik.com/wiki/Manual:Scripting

Mikrotik, Manual: IP/Traffic Flow. 17 de febrero del 2013

GLOSARIO

64-QAM tipo de modulación

3Des *Triple Data Encryption Standard,* algoritmo que hace triple cifrado del DES

A

ARM *Advanced RISC Machine*, Maquina avanzada RISC

API Interfaz de programación de aplicaciones

Arlan Provee soporte para tarjetas aironet arlan

ATM *Automatic Teller Machine*, cajero automatico

AP **Punto de Acceso**

ARP Address Resolution Protocol, Protocolo de resolución de

AirOS Sistema operativo airmax

ACL Lista de Control de Acceso

AES *Advanced Encryption Standard,* Estandar de encriptacion

ABR Autonomous Boundary Routers

ASBR Autonomous System Boundary Routers

ACK Acuse de recibo

B

BGP *Border Gateway Protocol,* Protocolo de Entrada Límite

BPSK Codificacion por cambio de fase binaria

C

CPE *Customer Premises Equipment.* Equipo local de cliente

CISC *Complex Instruction Set Computer,* Computador con Conjunto de Instrucciones Complejas

CD	Disco Compacto
CPU	Unidad de control de procesamiento
CIDR	*Classless Inter-Domain Routing*, enrutamiento entre dominios sin clases
CIR	*Committed Information Rate,* velocidad de datos garantizada
CCK	*Complementary Code Keying,* Codificacion por clave complementaria
CLI	interfaz de linea de comandos
CMOT	*Common Management Information Protocol over TCP/IP*, Información de Gestión Común Protocolo sobre TCP/IP
CBQ	Class Based Queueing, Encolamiento basado en clases

D

DMZ	Zona desmilitarizada
DHCP	*Dynamic Host Configuration Protocol,* protocolo de configuración dinámica de host
DB	Base de datos
DSSS	*Direct Sequence Spread Spectrum,* Espectro ensanchado por secuencia directa
DNS	Servidor de nombre de dominios
DDoS	Ataque de denegación de servicio distribuido
dBi	Decibel Isotrópico
DSCP	Punto de código de servicios diferenciados
DOS	Denegacion de servicios
Dijkstra	Algoritmo de caminos mínimos

E

EGP	*Exterior Gateway Protocol*, Protocolo de puerta de enlace Exterior
ESP	carga útil de encapsulamiento de seguridad

EIGRP	Protocolo de enrutamiento de gateway interior mejorado

F

Firewall	Cortafuegos
FTP	*File Transfer Protocol.* Protocolo de transferencia de archivos
FIFO	*First Input First Output.* Primero en entrar primero en salir
FTH	Fibra óptica residencial
FEC	*Forwarding Equivalence Class*, Reenvio de clase de equivalencia
F/B	Front/Back
FORWARD	Atravesar
FLAG	Bandera

G

GHz	Giga Herzios
Gateway	Puerta de enlace
GNU/Linux	Términos empleado para referirse a la combinación del núcleo o kernel libre similar a Unix denominado Linux con el sistema GNU.
GPL	Licencia Pública General
Gopher	Es un servicio de Internet consistente en el acceso a la información a través de menúes

H

Hz	Herzios
HTML	*HyperText Markup Language*, Lenguaje de Marcado de Hipertexto
HUB	Concetrador

HTB	*Hierachy Token Bucket*, Mecanismo de reparticion de carga
Home AP	Punto de Acceso Residencial

I

IP	Protocolo de internet
ISO	Organization internacional de estandarización
IT	Tecnologias de la Informacion.
ISP	Proveedor de servicios de internet
IPSec	*Secure IP*, IP segura
IMAP	permite acceder a varios clientes al mismo buzón
IPv6	Protocolo de internet versión 6
Isdn	Red digital de servicios Integrados
Input	entrada
IPROUTE	comando para rutas ip
ICMP	Protocolo de Mensajes de Control de Internet
IETF	Grupo de Trabajo de Ingeniería de Internet
IGP	*Internet Gateway Protocol*, Protocolo de puerta de enlace de internet
IR	Routers Internos

J

JunOS	Sistema Operativos Juniper
Jump	Salto

K

KVM	*Kernel-based Virtual Machine*. Maquina virtual basada en Kernel
KBPS	kilobits por segundo

L

LAN	*Local area Network.* Red de Area Local
Lcd	*Liquid Cristal Display,* representación visual por cristal líquido
LSP	*label switched path,* Intercambio de rutas por etiqueta
LER	*Label edge Router,* etiqueta de router extremo
LSR	*Label Switched router,* Elemento que conmuta etiquetas
LSP	*Label Switched Path,* Intercambio de rutas por etiquetas
LDP	*Label Distribution Protocol,* Protocolo de distribucion de etiquetas
L2TP	Layer 2 Tunneling Protoco, Protocolo de tunel de capa 2

M

Mhz	Mega Herzios
MAC	*media access control*, Control de acceso al medio
MIPS	*Microprocessor without Interlocked Pipeline Stages,* Microprocesador sin Inter bloqueado Etapas Pipeline
MPLS	*Multi-Protocol Label Switching,* Multiprotocolo de intercambio de etiquetas.
MBR	*Master Boot Record,* Registro maestro de arranque.
Mbps	Mega bits por Segundo
Mq	Multiples colas
MIR	*Maximun Information Rate*, velocidad máxima información
MIMO	*Multiple Input Multiple Output.* Multiples entradas Multiples Salidas
MPPE	*Microsoft Point-to-Point Encryption,* Encriptacion punto a punto Microsoft
MIB	*Management Information Base*, base de informacion gestionada
Mirroring	Efecto espejo
MTU	Unidad Maxima de transferencia
MSC	Centro de conmutación de servicios mobiles

N

Networking	Redes
NOC	Centro de Operaciones de red
Ntp	*Network transfer protocol.* Protocolo de tiempo de red
NFS	Network file system, sistema de archivos de red.
NStreme	protocolo propietario de MikroTik
NV2	NStreme Version 2
NAT	*Network Address Translation.* Traduccion de direcciones de red

O

Open Source	Código abierto
OSI	*Open Systems Interconnection,* Interconexión de Sistemas
OSPF	*Open Short Path First.* Primer camino más corto
Output	salida
OID	identificación de objeto único

P

PC	Computador Personal
Ppp	protocolo para administrar conexiones punto a punto
Ppc	*power Personal computer.* Encendido de computador personal
PTP	punto a punto
PCQ	*Per-Connection Queueing,* por conexion de colas
PTP Bridge	Usado para enlaces punto a punto
PPTP	*Point to Point Tunneling Protocol,* Protocolo de túnel punto a punto
PPP	Protocolo punto a punto
POP	descarga mensajes eliminandolos del servidor
P2P	Punto a punto
PPPoE	Protocolo Punto a Punto sobre Ethernet

Q

QoS	*Quality of Service*. Calidad de Servicio
Queuing	Encolamiento
QPSK	Codificacion por cambio de fase quadruple
Queue Tree	Arbol de colas

R

RouterOS	Sistema Operativo Router
RFC	*Requests from comment*. Solicitud de comentarios
RIP	Protocolo de Informacion de encaminamiento
RF	Radio Frecuencia
RISC	*Reduced Instruction Set Computer,* Computadora con Conjunto de Instrucciones Reducido
Routing	Enrutamiento
Red	*Random Early Detection,* deteccion aleatoria temprana
Radius	*Remote Authentication Dial-In User Server,* protocolo de autenticación y autorización para aplicaciones de acceso a la red o movilidad IP
RRDTool	*Round-Robin Database Tool*
RAM	Memoria de acceso aleatorio
RTS/CTS	Solicitud de envío / Listo para enviar

S

S.O.	Sistema Operativo
Soft_ID	Identificacion de software
Switch	Dispositivo que interconecta dos o mas dispositivos electronicos
SFTP	*Secure File Transfer Protocol,* Protocolo Seguro de Transferencia de Archivos
SA	Sistema Autónomo

SLA	Acuerdo de nivel de servicio
Sfq	*Stochastic Fairness Queuing Server*
SSID	*Service Set IDentifie*, nombre de la red
SSL	*Secure Sockets Layer*, capa de conexion segura
SSH	*Secure Shell*, protocolo para acceso remoto
SVA	Servicio de Valor Agregado
SwitchOS	Sistema operativo de Switch Mikrotik
SMI	Estructura de gestion de la informacion
SPAM	Correo electrónico no solicitado que se envía a un gran número de destinatarios con fines publicitarios o comerciales
Sniff	rastreador
Simple Queue	Cuotas simples
SSTP	Par trenzado blindado seguro
Scheduler	planificador
SNR	relacion señal/ruido

T

TCP/IP	*Transmission Control Protocol/Internet Protocol*, Protocolo de Control de Transmision/Protocolo de Internet
TV	Television
TELNET	Telecommunication Network, Protocolo de telecomunicacion de red
TX/RX	Transmicion/Recepcion
TKIP	Protocolo de Integridad de Clave temporal
TDMA	Multiplexacion por Division de Tiempo
ToS	Tratamiento de servicio
TTL	Tiempo de vida
TRAFFIC SHAPPING	Controla el trafico de una red
TRAFFIC PRIORITY	Priorizacion de trafico

U

UDP	*User Datagram Protocol*, Protocolo de datagrama de usuario

Ups	*Uninterruptible Power Supply,* Sistema de Alimentación ininterrumpida
URL	*uniform resource locator,* localizador de recursos uniforme
USM	*User-Based Security Model,* modelo de seguridad basada en el usuario

V

VPLS	*Virtual Private LAN Service,* Servicio privado LAN virtual
VLSM	*Variable Length Subnet Masks*, máscara de subred de longitud variable
VGA	Adaptador grafico de video
VPN	*Virtual Private Network,* Red privada virtual direcciones
VLAN	*Virtual Local Area Network,* Red de área local virtual

W

WISP	Proveedor de sercicios de internet inalámbricos
WiFi	Wireless-Fidelity, Mecanismo de interconexión de dispositivos electrónicos
Wimax	Tecnologia de bucle de usuario inalámbrico de banda ancha basada en el estándar IEEE 802.16
WEP	*Wired Equivalente Privacy,* Privacidad Equivalente a Cableado
WAP	*Wireless Aplication Protocol,* Protocolo de aplicaciones inalambricas
WINBOX	Interfaz grafica de usuarios mikrotik
WAIS	es un servicio de búsqueda de información en la red por palabra clave o frases
WPA	Acceso a wifi protegido avanzada
WPS	Wi-Fi Protected Setup, Configuracion Protegida Wi-Fi

X

X86	Arquitectura de 32 bits

ANEXOS

Anexo 1

PRESUPUESTO IMPLEMENTACIÓN DE NUEVA RED DE DATOS SIGSIGNET						
	REUQERIMIENTO	**CANTIDAD**	**COSTO REQ. ($)**	**MATERIAL ADICIONALES($)**	**OTROS COSTOS ($)**	**TOTAL**
HARDWARE REQUERIDO	Mikrotik RB1100AHx2	1.0	420.00 $	0.00 $	0.00 $	420.00 $
	Switch Administrable Cisco SG-200P-26	1.0	320.00 $	0.00 $	0.00 $	320.00 $
	Mikrotik BaseBox 5Ghz (Punto de Acceso)	4.0	368.00 $	50.00 $	30.00 $	368.00 $
	Mikrotik QRT-5	2.0	350.00 $	30.00 $	0.00 $	350.00 $
	Caja Metalica para Interperie 1.50 mtrs x 0.90 mtrs	1.0	165.00 $	20.00 $	20.00 $	165.00 $
	Conectores Panduit Cat. 6 (1 Funda x 100 Unidades)	1.0	49.00 $	0.00 $	0.00 $	49.00 $
	Bateria de Descarga Profunda Generica	1.0	115.00 $	0.00 $	0.00 $	115.00 $
	Inversor de Voltaje APC	1.0	135.00 $	0.00 $	0.00 $	135.00 $
	Servidor de Aplicaciones basado en Intel NUC	1.0	410.00 $	0.00 $	0.00 $	410.00 $
	Servidor de Cache basado en Intel NUC	1.0	410.00 $	0.00 $	0.00 $	410.00 $
	Rack Abierto 18 U	1.0	115.00 $	0.00 $	0.00 $	115.00 $
	Cable Red Panduit Cat. 6 para Interperie (Caja)	1.0	165.00 $	0.00 $	0.00 $	165.00 $
	Subtotal		**3,022.00 $**	**100.00 $**	**50.00 $**	**3,172.00 $**
EN MARCHA	Configuracion Servidor Aplicaciones	1.0	200.00 $	0.00 $	0.00 $	200.00 $

	Configuracion Mikrotik RB1100 Ahx2	1.0	250.00 $	0.00 $	0.00 $	250.00 $
	Configuracion PtP QRT-5	1.0	150.00 $	0.00 $	0.00 $	150.00 $
	Instalación & Cableado Estructurado	1.0	110.00 $	0.00 $	0.00 $	110.00 $
	Configuraciones Generales	1.0	100.00 $	0.00 $	0.00 $	100.00 $
	Subtotal		**810.00 $**	**0.00 $**	**0.00 $**	**810.00 $**
HERRAMIENTAS	Ponchadora	1.0	23.00 $	0.00 $	0.00 $	23.00 $
	Lan Tester	1.0	35.00 $	0.00 $	0.00 $	35.00 $
	Arnes de Seguridad	1.0	130.00 $	0.00 $	0.00 $	130.00 $
	Alicates & Kit de Destornilladores	1.0	45.00 $	0.00 $	0.00 $	45.00 $
	Kit Cables Patch	1.0	25.00 $	0.00 $	0.00 $	25.00 $
	Subtotal		**258.00 $**	**0.00 $**	**0.00 $**	**258.00 $**

ADMINISTRACIÓN DEL PROYECTO	Instalar el sistema	1.0	318.00 $	0.00 $	0.00 $	318.00 $
	Entrenar a los Tecnicos	1.0	318.00 $	0.00 $	0.00 $	318.00 $
	Realizar prueba de aceptación (Evaluar)	1.0	50.00 $	0.00 $	0.00 $	50.00 $
	Realizar revisión posterior al proyecto	1.0	0.00 $	0.00 $	0.00 $	0.00 $
	Proporcionar soporte técnico inicial	1.0	500.00 $	0.00 $	0.00 $	500.00 $
	Subtotal		**1,186.00 $**	**0.00 $**	**0.00 $**	**1,186.00 $**

OTROS COSTOS	Otros costos (Puesta Marcha)	1.0	200.00 $	0.00 $	0.00 $	200.00 $
	Subtotal		**200.00 $**	**0.00 $**	**0.00 $**	**200.00 $**

Subtotales	**5,476.00 $**	**100.00 $**	**50.00 $**	**5,626.00 $**
Riesgo (previstos)	300.00 $	0.00 $	200.00 $	**500.00 $**

Total (programado)	**5,776.00 $**	**100.00 $**	**250.00 $**	**6,126.00 $**

Tabla 1 Anexo 1. Presupuesto del Proyecto

Fuente: Los Autores, Presupuesto del Proyecto, 2014

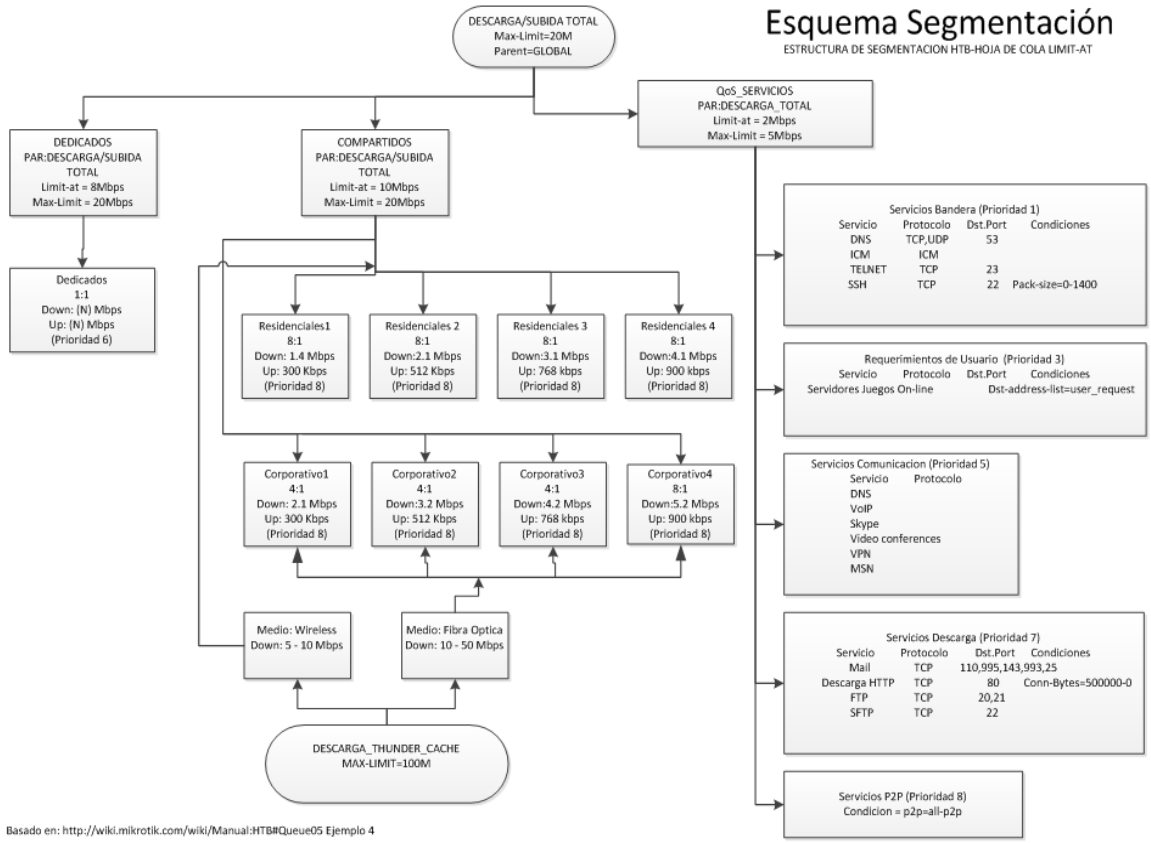


FIGURA 1 ANEXO 1. Segmentacion de ancho de banda

Fuente: Los Autores, Segmentacion de ancho de banda, 2014