ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

IMPLEMENTACIÓN DE ENLACES BACKHAUL PARA BACKBONE DE UN WISP MEDIANTE EL USO DEL SISTEMA OPERATIVO ROUTEROS.

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN ELECTRÓNICA Y TELECOMUNICACIONES

AUTOR: WASHINGTON SERGIO SARANGO ESPINOSA
sergio@ruidogris.com

DIRECTOR: ING. MÓNICA VINUEZA RHOR
monica.vinueza@epn.edu.ec

Quito, marzo del 2011

DECLARACIÓN

Yo Washington Sergio Sarango Espinosa, declaro bajo juramento que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional y que he consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedo mis derechos de propiedad intelectual correspondientes a este trabajo a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su reglamento y por la normatividad institucional vigente.

_____

W. Sergio Sarango Espinosa

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por W. Sergio Sarango Espinosa bajo mi supervisión,

_____

Ing. Mónica Vinueza Rhor

DIRECTOR DE PROYECTO

AGRADECIMIENTO

Agradezco de manera especial a mi madre L. Rocío Espinosa, por la oportunidad de permitirme participar de este gran viaje llamado vida, por su esfuerzo, sacrificio y apoyo a lo largo de este recorrido. A María Fernanda Torres, por la confianza, el respaldo y la paciencia brindada. A mi familia por ser un soporte siempre. Y a la memoria de todos aquellos seres anónimos de los que aprendí que cada amanecer trae su propio movimiento y con él una nueva oportunidad para empezar.

CONTENIDO

ANEXOS

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICOS

CAPÍTULO 1

CAPÍTULO 2

CAPÍTULO 3

CAPÍTULO 4

Resumen

El presente proyecto tiene como propósito introducir alternativas tanto en equipamiento como en la forma de gestión de una red de telecomunicaciones. Se analiza diversos tópicos que integran la infraestructura tanto en *backbone* como en el usuario final mediante la introducción del sistema operativo RouterOS de MikroTik como alternativa de equipamiento y administración de una red.

En el capítulo I se analiza el sistema RouterOS, sus características y funciones, modelos de placas RouterBoard, instalación de RouterOS, manejo de paquetes.

En el capítulo II cubre configuraciones relacionadas con la gestión de la red como es: configuración TCP/IP, configuraciones DHCP, enmascaramiento, direccionamiento de puertos, firewall, túneles, control de ancho de banda, etc.

En el capítulo III, se estudia las comunicaciones inalámbricas, se analiza los estándares IEEE 802.11x, su forma de funcionamiento tanto en la capa física como la capa enlace.

El capítulo IV analiza el diseño e implementación de enlaces de *backbone* , configuraciones de radio con RouterOS, factibilidad de enlaces, cálculos de desempeño de enlaces, presupuesto de pérdidas y ganancias de enlaces, configuraciones de enlaces punto a punto, configuración de enlaces redundantes, configuración de un punto de acceso, y un equipo CPE como router de frontera.

El capítulo V contiene las conclusiones y recomendaciones como consecuencia del trabajo realizado.

PRESENTACIÓN

Las telecomunicaciones y su principal red Internet en la actualidad tiene un carácter hegemónico global, se ha convertido en un recurso imprescindible en la mayoría de esferas de la sociedad, permitiendo el perfeccionamiento de herramientas que ayudan a las personas su desarrollo en el ámbito personal y profesional. El avance de Internet ha traído consigo un sin número de retos en los campos científico, tecnológico y humano que definirán de manera radical los parámetros sobre los cuales crecerán y se formarán las sociedades del futuro.

La buena elección de una plataforma de comunicaciones hará que una empresa tenga más posibilidades de asegurar una posición exitosa; en su implementación se consideran aspectos que permiten optimizar rendimiento y fiabilidad de toda la red. Muchas empresas encuentran limitaciones para ampliar o actualizar su infraestructura de comunicaciones por los elevados costos en el equipamiento, es por eso que este proyecto busca desarrollar una alternativa económica para su implementación, sin descuidar la capacidad y velocidades de transmisión, además de incorporar herramientas que permiten una mejor administración de la red

El presente trabajo surge de la necesidad de la empresa Stealth Telecom en investigar una nueva solución en equipo tecnológico que permita incrementar significativamente su manejo de ancho de banda en su red de *backbone*, así como su fiabilidad, flexibilidad en la arquitectura de la red, seguridad en los canales de transmisión y que además incluya los últimos protocolos para gestión y administración de la red.

CAPÍTULO 1.

ROUTEROS

1.1 DESCRIPCIÓN GENERAL

Stealth Telecom del Ecuador es una empresa de telecomunicaciones que cuenta con una red WAN con infraestructura inalámbrica propia, que comprende la región centro–norte del Ecuador brindando acceso a Internet y transmisión de datos a sus usuarios, mayoritariamente empresas en el sector rural, café nets, y usuarios del sector residencial. Su red de backbone en su totalidad es inalámbrica formando una topología mixta, integrando varios anillos redundantes.

La tecnología utilizada por los equipos de backbone lo componen plataformas como WiMAX basado en OFDM (*Orthogonal Frequency Division Multiplexing)*, y IEEE 802.11a/b/g/n, siendo Ethernet IEEE 802.3 el estándar de capa de enlace de todos los equipos. El uso de varias plataformas tecnológicas permite fortalecer la red de backbone minimizando interferencias debido a que varios de los equipos utilizados poseen modulaciones propietarias, lo que permite un mejor desempeño del espectro radioeléctrico frente a interferencias de otros operadores que trabajan en los mismos rangos de frecuencias.

Los equipos que componen la red de Stealth Telecom son principalmente Motorola - Canopy Backhaul (BH) para enlaces o unificación de los nodos y equipos punto – multipunto (AP Y SM) serie Advantage de hasta 20 Mbps de velocidad para acceso a clientes finales, además de equipos Cisco con su modelo Aironet como puntos de acceso, y Smart Bridges con su Modelo Nexus BH.

Estos equipos en primera instancia mejoraron significativamente el rendimiento del backbone, pero a medida que la red y la demanda de mayores anchos de banda crecían, estas soluciones resultaron limitadas y poco rentables; por ejemplo, la plataforma Motorola Canopy para su óptimo

funcionamiento requiere equipamiento adicional del mismo fabricante; en los nodos repetidores en la formación de clusters[1] *Access Point* (AP's), cuando se tiene instalado en similares rangos de frecuencia más de 3 equipos Access Point y equipos *Backhaul*[2] (BH), el fabricante sugiere la instalación de un equipo sincronizador con GPS (CMM micro – *Cluster Managment Module*), el cual se encargará de generar un pulso de sincronía para evitar la auto interferencia; además, para el manejo de ancho de banda en los equipos suscriptores en los clientes finales (Canopy SM), se requiere la implementación de un software de administración de equipos AP's y SM's (Prizm), todo este equipamiento adicional eleva los costos operativos y costos de instalación, y no resuelve problemas de gestión, administración, y control. Otra gran limitación que se presentó con el incremento de demanda de ancho de banda, es el manejo de paquetes por segundo (PPS), este parámetro se utiliza para medir el rendimiento de un equipo de red, Canopy soporta un máximo de 3500 PPS lo cual es un limitante cuando se requiere enlaces de *backbone* de por lo menos de 20000 PPS.

Con este trabajo se pretende plantear soluciones de enlaces inalámbricos de backbone confiables, eficientes y con altos niveles seguridad utilizando tecnología MBDA (Modulación Digital de Banda Ancha), en frecuencias no licenciadas que sean rentables en su implementación y operación mediante el uso del sistema RouterOS de MikroTik.

Realizando una análisis de costo versus beneficios de los principales fabricantes de equipamiento para *networking* se tiene que; un equipo de la marca CISCO serie 3800 con características de routeo MPLS, puertos Fast Ethernet, Gigabit Ethernet, implementación de Firewall, soporte de VPN, tiene un valor en el mercado de aproximadamente 4000 USD. El equipo RB1100 de la marca MikroTik posee similares prestaciones que el quipos CISCO, es decir; puede administrar MPLS, soporte de VPN's, Puertos Fast Ethernet, Gigabit Ethernet, Firewall etc., con un precio de mercado de 400 USD. Esta diferencia de precios se debe a que CISCO es una marca posicionada y con una amplia trayectoria en el mercado, mientras que la marca MikroTik es una empresa que está buscando darse a conocer en el mercado y ha resultado una respuesta

interesante en la implementación de pequeñas y medianas redes de telecomunicaciones (2000000 usuarios), hasta inclusive redes Metro.

Otra característica interesante que incluye MikroTik es el manejo de interfaces inalámbricas para levantamiento de WISP. Por ejemplo; una solución para un enlace punto a punto para un tráfico de 200 Mbps con equipos marca Motorola modelo PTP 600 tiene un costo promedio de 15000 USD. Esta solución puede ser realizada con equipos RouterBoard MikroTik RB411AH con un costo final promedio de 1200 USD y con prestaciones de tráfico similares a la solución de Motorola.

Es por esto que se ha realizado un minucioso estudio de alternativas de equipamiento para complementar o sustituir tecnología de infraestructura de la empresa Stealth Telecom del Ecuador.

1.2 ROUTEROS MIKROTIK[3]

RouterOS es un sistema operativo de la empresa MikroTik basado en Linux , que permite convertir un equipo x86 común o una placa RouterBOARD[4] en un router dedicado, con funcionalidades como: administrador de ancho de banda, un dispositivo inalámbrico, administrador BGP (*Border Gateway Protocol*), o cualquier otra cosa que sea relacionada con las necesidades de networking.

El sistema RouterOS fue creado por 2 estudiantes de Latvia país ex integrante de la Unión Soviética como tesis universitaria para diseñar un router basado en Linux que permita equiparar las funcionalidades de otros routers que se encontraban en el mercado. Con el pasar del tiempo se han integrado varias aplicaciones dentro del sistema, como: soluciones de telefónica IP, administración de protocolo BGP, integración de Ipv6, servidor de VPN's, administración de ancho de banda, calidad de servicio (QoS), administración de *hotspots*[5], puntos de acceso inalámbrico, *backhaul* inalámbrico, etc.

A partir del año 2002 se enfocaron en la creación del hardware que permita simplificar su operación, creando el RouterBOARD 230, luego desarrollaron una amplia gama de RouterBOARD RB, como: RB500, RB100, RB300, RB600, RB400 y RB1000, los cuales difieren entre sí en características

como: la velocidad del procesador, el número de puertos Ethernet, el número de slots mini-PCI, capacidad de memoria, capacidad de almacenamiento de datos, nivel de licencia, etc.

MikroTik es actualmente considerada como una de las grandes empresas de Networking, compitiendo con grandes fabricantes como Cisco, Juniper, 3Com, ó D-Link, etc., entre sus clientes y casos de éxito se pueden nombrar a: SIEMENS, IPASS, HP, ERICCSON, Mitsubishi, RIPE, El Departamento de Estado de los Estados Unidos de América, Motorola, Vodafone, FBI y la NASA[6].

La principal diferencia de MikroTik frente al resto de marcas en el mercado, es su bajo costo de sus licencias y la amplia capacidad de adaptación a operaciones de networking, con lo cual su uso se ha extendido de forma extraordinaria y rápidamente.

1.3 CARACTERÍSTICAS PRINCIPALES DE RouterOS[7]

RouterOS es basado en el Kernel 2.6 de Linux, soporta multi-core (varios núcleos), y computadores multi-CPU (SMP- *Symmetric Multiprocessing*), la instalación y ejecución puede ser desde discos IDE, HDDs, CF, memorias USB, SSD disk. Soporta varios métodos acceso a configuración: acceso local, con teclado y monitor, por consola mediante puerto serial, Telnet, *secure* SSH, interface WEB, además de una interface GUI (*graphical user interface*) propia llamada Winbox; también soporta una conexión a nivel de MAC address llamada Mac-Telnet.

1.3.1 FIREWALL[8]

El Firewall implementa filtrado de paquetes que es usado para administrar el flujo de datos a, desde y a través del router. Junto con el NAT *(Network Address Translation)* previene el acceso no autorizado a redes internas, autorizando solo el tráfico de salida, es decir el tráfico generado desde la red interna hacia el Internet, por ejemplo solicitudes HTTP (*Hypertex Transfer Protocol)* o envío de correo electrónico. RouterOS permite crear un *Firewall Stateful* lo que significa que realiza una inspección de estado de paquetes y realiza un seguimiento de estado de conexiones que pasan a través de él. También soporta *Source and Destination*

NAT *(Network Address Translation)*. El Firewall provee características para hacer uso de conexiones internas, ruteando y marcando paquetes. Permite detectar ataques por denegación de servicio (DoS)

El filtrado puede ser por direcciones IP, rango de direcciones IP, por puerto, rango de puerto, protocolo IP, DSCP *(Differentiated Services Code Point)* y otros parámetros. Soporta también direccionamiento IP estático y dinámico, además de implementar características de capa 7 *(Layer7).*

1.3.2 CALIDAD DE SERVICIO QOS

RouterOS puede implementar QoS (802.11Q):

- Tipo de colas: RED (*Random Early Detection*)**,** BFIFO (*Byte limited First In, First Out queue*)**,** PFIFO (*Packet limited First In, First Out queue*)**,** PCQ (*Packet Classification and Queuing*)
- Colas simples: por origen/destino de red, dirección IP de cliente, por interface
- Árboles de colas: por protocolo, por puerto, por tipo de conexión.

1.3.3 ROUTING[9]

RouteOS soporta ruteo estático, y una multitud de protocolos dinámicos de ruteo.

- Para IPv4 soporta RIP v1 y v2, OSPF (*Open Shortest Path First***)** v2, BGP (*Border Gateway Protocol)*
- Para IPv6 soporta RIPng, OSPF v3 y BGP

RouterOS soporta también *Virtual Routing y Forwarding* (VRF), ruteo basado en políticas, ruteo basado en interfaces, y ruteo ECMP *(Equal-cost multi-path routing*). Es posible usar el firewall para marcar conexiones específicas para hacer que el tráfico marcado use un diferente ISP (Internet Service Provider). Implementa el protocolo de ruteo MPLS (*Multiprotocol Label Switching)*, el cual trabaja entre la segunda y la tercera capa de red del modelo OSI, y es comúnmente utilizado para manejo y administración de redes de alto rendimiento.

Soporta BGP (*Border Gateway Protocol*) para la administración de sistemas autónomos.

RouterOS permite implementar *Bridging* en dos o más interfaces, es decir; refleja el tráfico que se genera en una de las interfaces, a otra u otras interfaces del mismo router, esto permite crear uno o más canales de datos dentro del mismo router.

RouterOS provee de un protocolo propietario para la implementación de túneles llamado EoIP el cual es un túnel Ethernet entre dos ruteadores sobre conexión IP.

1.3.4 WIRELESS[10]

RouterOS soporta una variedad de tecnologías inalámbricas, puede trabajar con diferentes configuraciones para diferentes aplicaciones, por ejemplo; *Backhaul* para enlaces punto a punto, *Access Point* para enlaces multipunto, *Hotspot.*

Soporta estándares IEEE802.11a/b/g/n, con modulaciones; OFDM (*Orthogonal frequency-division multiplexing):* BPSK (*Binary Phase Shift Keying*), QPSK (*Quadrature Phase Shift Keying*), 16 QAM (*Quadrature Amplitud Modulation*), 64QAM, DSSS (*Direct Sequence Spread Spectrum*): DBPSK (*differential binary phase shift keying)*, DQPSK (*Differential Quadrature Phase Shift Keying)*, CCK (*Complementary Code Keying)*. Maneja protocolos propietario: Nstreme[11] protocolo que permite extender el rango de cobertura y velocidad de lo radios y Nstream2 (dual) utiliza 2 tarjetas de radio una para transmisión y otra para recepción con lo cual se puede duplicar la capacidad de ancho de banda.

Mediante el uso de radios que soportan el estándar 802.11n, RouterOS tiene la capacidad de implementar la reciente tecnología MIMO (*Multiple-input Multiple-output)*, que permite mediante diversidad de antenas (dos antenas simultaneas en diferentes frecuencias) incrementar el ancho de banda hasta una velocidad teórica de 600 Mbps. Puede administrar redes *Wireless* MESH (malla) y HWMP (*Hybrid Wireless Mesh Protocol*) para incrementar zonas de cobertura de la red inalámbrica.

Soporta RTS/CTS (*Request to Send* / *Clear to Send*) para disminuir las colisiones, WDS (*Wireless Distribution System*) para extender una red Multipunto con varios puntos de acceso (AP's) con un mismo ssid (*service set identifier*) conservando las mismas direcciones MAC (*Media Access Control*) en los clientes.

Implementa seguridades WEP (*Wired Equivalent Privacy)*, WAP (*Wireless Application Protocol)*, WPA2 (802.11i), además incorpora una lista de control de acceso de clientes mediante filtrado de direcciones MAC con seguridad mediante un algoritmo de 104 bits con WEP, permite la creación de puntos de acceso virtuales utilizando las mismas característica de frecuencia que el AP primario.

1.3.5 CONTROL DE ANCHO DE BANDA[12]

El control de ancho de banda es un mecanismo que controla la asignación de la velocidad de los datos, tiempo de retraso, entrega oportuna de paquetes, confiabilidad en la entrega, es decir prioriza y da forma al tráfico de red. Algunas características de RouterOS para el control de tráfico son las siguientes:

- Limitación de tráfico por direcciones IP, subredes, por protocolo, por puerto, y otros parámetros.
- Limitación de tráfico peer to peer.
- Priorización de determinados flujos de paquetes sobre otros
- Uso de trafico de colas para mayor rapidez de navegación.
- Aplicación de colas en intervalos de tiempos fijos
- Manejo dinámico de cantidad de tráfico dependiendo de la carga del canal.
- RouterOS soporta *Hierarchical Token Bucket* (HTB), es un tipo de sistema jerárquico de calidad de servicio con CIR *(Committed Information Rate)* y MIR *(Maximum Information Rate)*, ráfagas de datos y prioridad

1.3.6 SERVIDOR / CLIENTE

RouterOS incorpora varios servicios como servidor o cliente:

DHCP *(Dynamic Host Configuration Protocol)*: usado para la asignación dinámica de direcciones IP.

Túneles tipo PPPoE *(Point to Point Protocolo over Ethernet)* utilizado para acceso DSL encapsulando tramas PPP dentro de tramas Ethernet.

Túneles PPTP *(Point to Point Tunneling Protocol)*: permite la transmisión de datos cliente – servidor sobre la plataforma TCP/IP.

Relay de DHCP (*Dynamic Host Configuration Protocol)*: utilizado para administrar reenvíos de solicitudes de asignación IP de un cliente DHCP hacia un servidor DHCP.

Cache web-proxy: utilizado para el almacenamiento temporal de archivos recurrentes.

Gateway de *Hotspot*: provee autenticación, autorización, y seguridad para el uso de una red inalámbrica de acceso público.

VPN *(virtual private network) Server*: permite establecer conexiones seguras sobre redes abiertas (sin seguridad), ó Internet.

1.3.7 LICENCIAMIENTO[13]

RouterOS para ser activado requiere una licencia de nivel de aplicaciones, es decir existen varias licencias con limitaciones o características adicionales dependiendo del tipo de aplicación de red que se requiera.

Las licencias de nivel 0 es una licencia demo, habilita todas sus funciones durante un periodo de 24 horas. La licencia de nivel 2 fue una licencia de transición e investigación, por lo que no se encuentran disponibles. La licencia de nivel 3 fue una licencia que operaba con características limitadas, y permitía el uso de interfaces inalámbricas solo para trabajar en modo cliente.

La principal diferencia entre las licencias de nivel 4, 5 y 6, son la cantidad de túneles permitidos por nivel, a continuación se muestra una tabla con los niveles y las características.

NIVEL	0 (Gratis)	1 (DEMO)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (Servidor Control)
Características						
PPPoE túneles	24h limite	1	200	200	500	ilimitados
PPTP túneles	24h limite	1	200	200	500	ilimitados
L2TP túneles	24h limite	1	200	200	500	ilimitados
HotSpot usuarios Activos	24h limite	1	1	200	500	ilimitados
Sesiones activas de administración	24h limite	1	10	20	50	ilimitados
EoIP túneles	24h limite	1	Ilimitados	ilimitados	ilimitados	ilimitados
OVPN túneles	24h limite	1	200	200	ilimitados	ilimitados
VLAN Interfaces	24h limite	1	Ilimitados	ilimitados	ilimitados	ilimitados
Colas QoS	24h limite	1	Ilimitados	ilimitados	ilimitados	ilimitados
Wireless AP	24h limite	-	-	sí	Sí	sí
Wireless Client y Bridge	24h limite	-	sí	sí	Sí	sí
RIP, OSPF, BGP protocolo	24h limite	-	Sí	sí	Sí	sí
RADIUS client	24h limite	-	Sí	sí	Sí	sí
Web proxy	24h limite	-	Sí	sí	Sí	sí
Sincrónicas interfaces	24h limite	-	-	sí	Sí	sí
Actualizable	-	no actualizaciones	ROS v4.x	ROS v4.x	ROS v5.x	ROS v5.x
Soporte online	-	-	-	15 días	30 días	30 días

Tabla 1.1 Licenciamiento RouterOS

Para el uso de BGP sobre x86 es necesario RouterOS v4x.

MikroTik periódicamente revisa y actualiza su sistema operativo, en cada actualización implementa o modifica características de RouterOS, estas actualizaciones son llamadas versiones y existen para cada tipo de licencia.

1.4 MODELOS DE PLACAS ROUTERBOARD[14]

Se ha fabricado varios modelos de placas MikroTik RouterBoard, los cuales varían entre ellos según la velocidad del procesador, el número de interfaces que admite cada placa, o el tipo de licenciamiento que viene de fábrica, con la posibilidad de cambiar la licencia en cualquier modelo. Al

momento de ser realizado este estudio se han considerado solamente los principales modelos que el fabricante promociona oficialmente, y los que serán útiles para el presente estudio

1.4.1 MODELO 433/AH

Este RouterBoard cuenta con un procesador con una velocidad de 300 MHz, posee 3 interfaces Ethernet, 3 interfaces Mini-PCI para interfaces inalámbricas, memoria RAM de 64 MB y licenciamiento RouterOS nivel 4, lo que le es ideal para funcionar como punto de acceso inalámbrico (Access Point). Existe un modelo 433AH que se diferencia de este modelo por incorporar un procesador de mayor velocidad 680 MHz, y un slot para memoria micro-SD, que puede ser usado para almacenamiento proxy.

CPU *speed* 680MHz

RAM 128MB *Architecture* MIPS-BE

LAN ports 3 MiniPCI 3 *Integrated Wireless*

1 *Memory card type microSD*

RouterOS License Level5

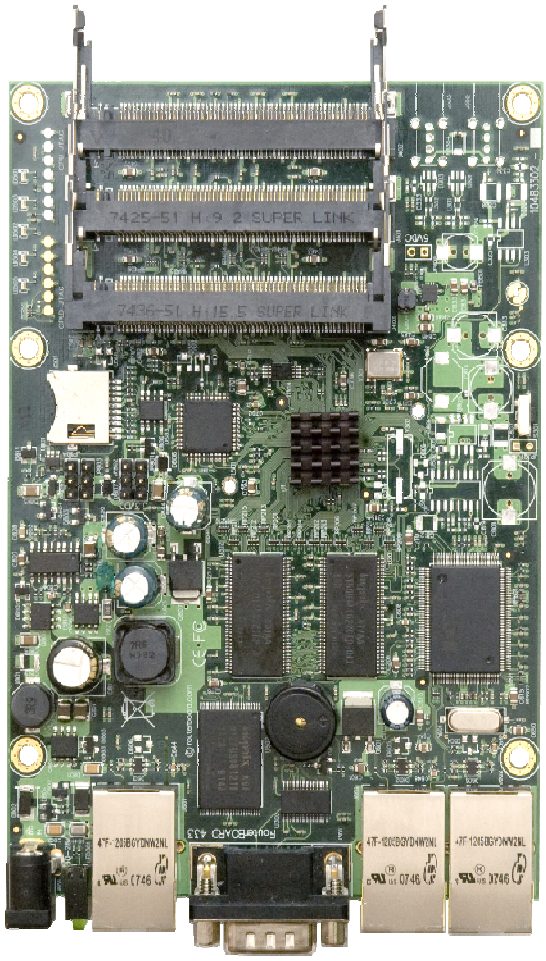


Figura 1.1 RouterBoard modelo 433/AH

1.4.2 MODELO 411/AH

Este RouterBoard tiene un procesador de velocidad de 300 MHz, posee un puerto LAN, un puerto Mini-PCI para interfaz inalámbrica y licencia nivel 3; el cual es ideal para CPE *(Customer Premises Equipment)*. El modelo 411AH difiere del modelo 411 por poseer un procesador de mayor velocidad 680 MHz, y licencia de nivel 4, por su mayor velocidad de procesamiento es ideal para ser usado en enlaces inalámbricos tipo *backhaul* (enlaces entre nodos).

CPU *speed* 680MHz

RAM 64MB *Architecture* MIPS-BE

LAN ports 1 MiniPCI

1 *Integrated Wireless*

RouterOS License Level4

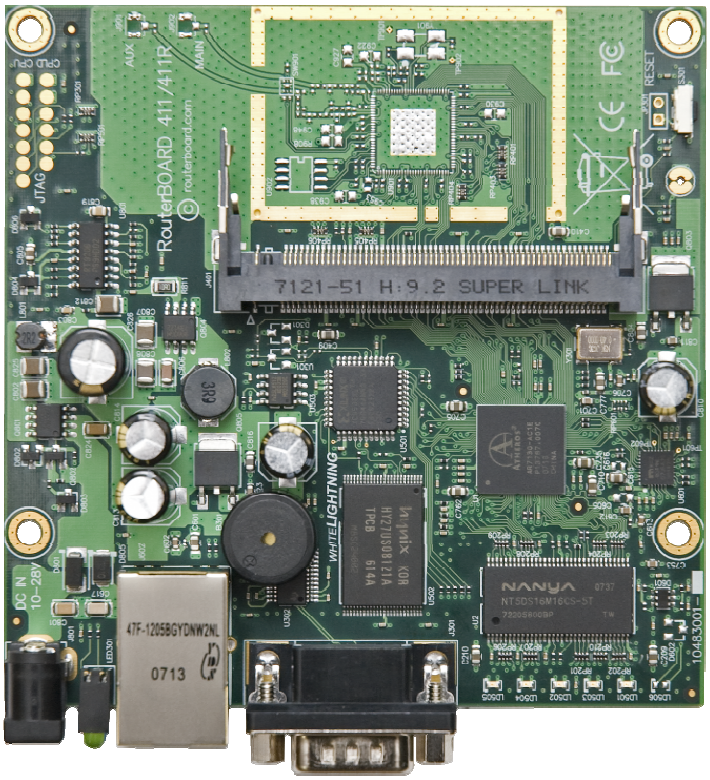


Figura 1.2 RouterBoard modelo 411/AH

1.4.3 MODELO 750G

Este equipo cuenta con un procesador con una velocidad de 680 MHz, está compuesto de 5 interfaces Gigabit Ethernet, y licencia nivel 4, por lo que es ideal para trabajar como router de frontera; además su licenciamiento le permite administrar la mayoría de tipos de ruteo incluyendo MPLS.

CPU *speed* 680MHz

RAM 32MB *Architecture* MIPS-BE

LAN ports 5 Gigabit

RouterOS License Level4

Figura 1.3 RouterBoard modelo 750G

1.5 INSTALACIÓN DE ROUTEROS MIKROTIK

RouterOS para su instalación en plataformas x86 (pc's) requiere un mínimo de características sobre las que pueda funcionar de manera estable. Un procesador mínimo de 100 MHz, 32 MB de memoria RAM, y 64 MB de memoria en disco rígido, con mejores características el rendimiento será mucho mayor.

Para instalar RouterOS MikroTik se puede descargar los paquetes de instalación directamente de la página oficial de MikroTik http://www.MikroTik.com. MikroTik muestra varias opciones de descarga para actualización de routerboards, y un ISO para la instalación de RouterOS sobre x86.

Una vez que se obtiene el paquete de instalación en CD, se elige la instalación del PC desde el lector de discos, al arrancar el PC indicará el menú de instalación con los paquetes que soportará RouterOS. Con las teclas "P" y "N" se puede desplazar entre el menú, o con las teclas "arriba" y "abajo". Para elegir o desmarcar una opción del menú se utiliza la tecla barra espaciadora.

Una vez escogidos los paquetes que se desea instalar se presiona la tecla "i" para iniciar la instalación o la letra "q" para cancelar la instalación. Si se cancela la instalación se regresará a la página de inicio de la instalación.

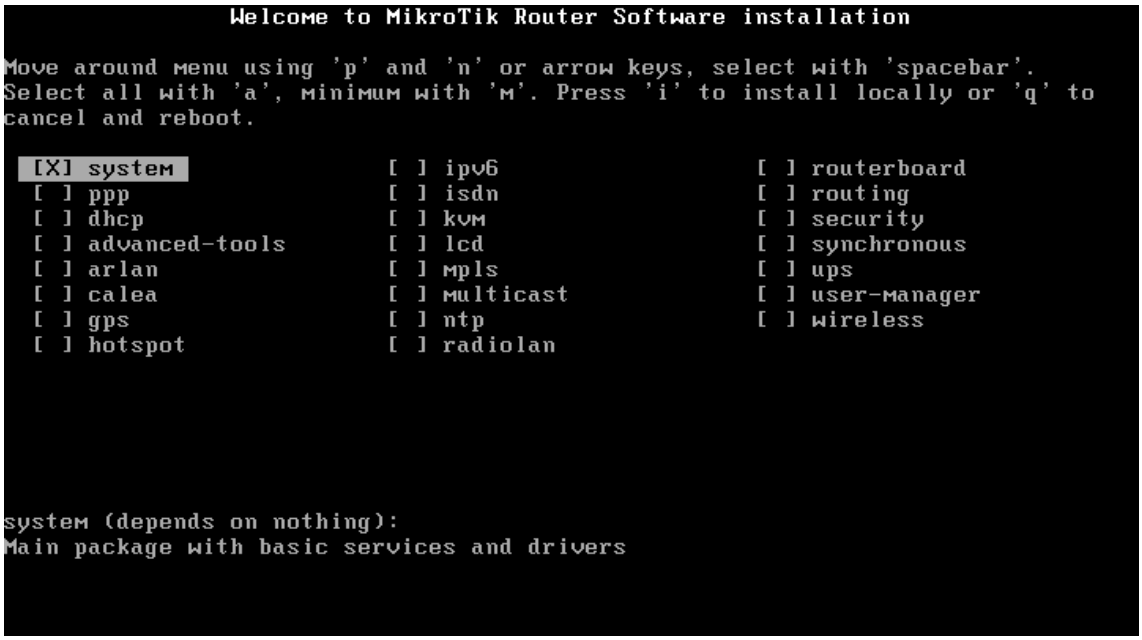


Figura 1.4 Pantalla de menú inicio instalación RouterOS

System: Provee los servicios básicos del sistema operativo, además de los drivers de las interfaces y periféricos.

PPP: Provee soporte para tuneles tipo PPP, PPTP, L2TP, PPPoE, e ISDN PPP.

DHCP: Paquete para servicio DHCP cliente / servidor.

Advanced-tools: Permite la utilización de herramientas avanzadas como: cliente de correo, ping avanzado, netwatch, ipscan, packet sniffer, torch, traceroute, monitor de tráfico, etc.

Arlan: Provee soporte para tarjetas aironet arlan

Calea: Es utilizado para interceptar y registrar tráfico de la red para facilitar el filtrado del firewall.

GPS: Mediante el uso de puerto serial se puede incluir un equipo GPS.

Hotspot: Provee las funciones para operar un Hotspot, proporcionando autenticaciones y autorizaciones para crear una red pública.

IPv6: Soporte para direccionamiento IPv6

ISDN: Usado para proporcionar conexiones digitales extremo a extremo para el uso de sistemas de voz

KVM: Provee el software necesario para el uso RouterOS sobre máquinas virtuales.

LCD: Soporte LCD para monitores y equipos LCD

MPLS: Soporte para MPLS *(Multiprotocol Label Switching)*.

Multicast: Soporte para trafico *Multicast* (difusión), utilizado para el envío de tráfico hacia un grupo determinado de usuarios, como puede ser video streaming o TV-pay, etc.

NTP: Soporte como servidor / cliente NTP *(Network Time Protocol)*, usado para sincronizar el reloj de servidores y equipos usuarios.

Radiolan: Soporte para equipos Radiolan.

Routerboard: Provee soporte para acceso y administración de RouterBOOT

Routing: Provee soporte para diferentes tipos de ruteo como RIP (*Routing Information Protocol)*, BGP, OSPF, BFD *(Bidirectional Forwarding Detection)*, filtros para rutas, etc.

Security: Provee soporte para IPSec, SSH, conectividad segura con Wibox

Synchronous: Soporte para tarjetas Farsync para el uso de equipos con conexiones síncronas

UPS: Permite el monitoreo mediante puerto serial de equipos APS (*Alternative Power Supply)*, *UPS (Uninterruptible Power Supply).*

User Manager: Soporte para User Manager un sistema de administración para HotSpot, usuarios PPP, usuarios DHCP, *Wireless users*, RouterOS clientes, es un paquete de software propio de MikroTik.

Wireless: Aplicación para la implementación de redes inalámbricas en diferentes modos y configuraciones.

A continuación pregunta si se quiere guardar las configuración anterior, a lo que se contesta que no, “N” [Y/N].

Figura 1.5 Pantalla de confirmación para guardar configuración antiguas

La siguiente pantalla advierte que los datos en el disco serán borrados y si se desea continuar a lo que se responde que si “Y”.

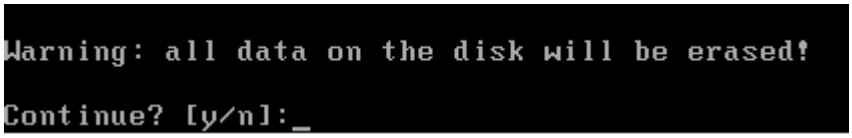


Figura 1.6 Confirmación de eliminación de datos

La instalación crea particiones y formatea el disco de forma automática, para concluir indica los paquetes que han sido instalados y solicita pulsar la tecla de ENTER para reiniciar el equipo.

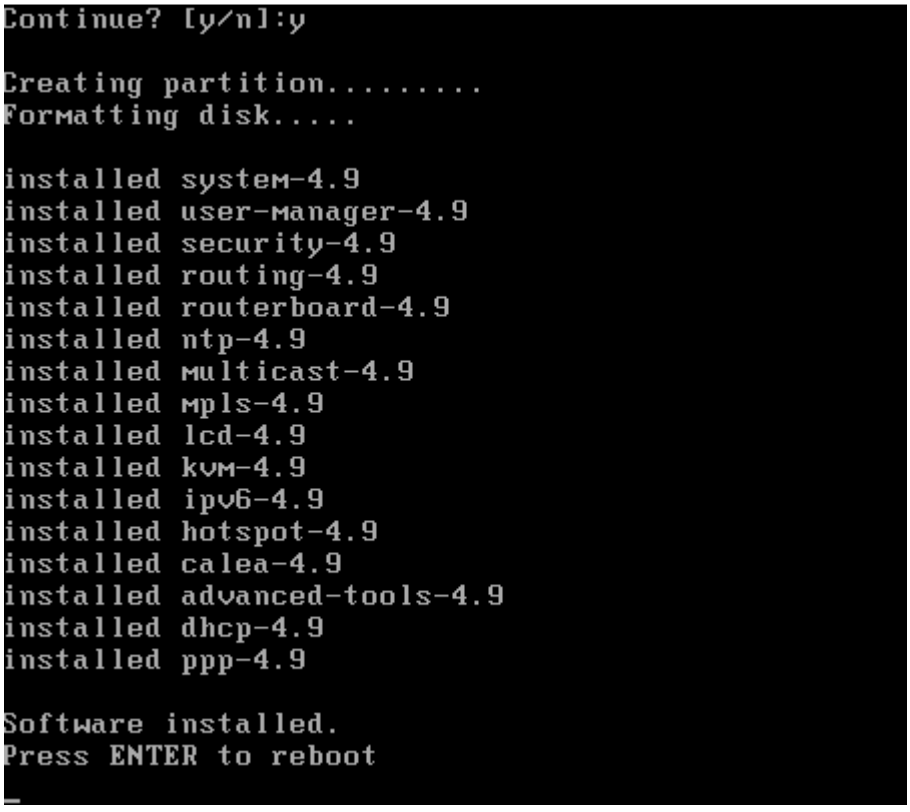


Figura 1.7 Progreso de paquetes instalados

Al reiniciarse el equipo pregunta si se quiere revisar la superficie del disco a lo que se responde que si “Y”, el tiempo que tarda revisar el disco es aproximadamente un minuto por cada Gigabyte del disco.

El sistema RouterOS ha sido instalado, a continuación solicita un usuario y una contraseña

Figura 1.8 Pantalla de usuario y contraseña

Por defecto el usuario es “admin”, y la contraseña se deja el campo vacio y se pulsa ENTER

Figura 1.9 Pantalla de inicio de RouterOS mediante CLI

1.6 INGRESO A ROUTEROS

Una vez realizada la instalación RouterOS este puede ser configurado mediante la interface CLI Interface de línea de comandos, también se puede acceder mediante telnet (capa3), SSH, interface web (webbox), mediante puerto serial, MAC - Telnet (usado solamente por equipos con RouterOS en capa 2) y por una interface propietaria MikroTik llamada WINBOX.

Winbox es una herramienta que ejecuta Telnet hacia el equipo a configurar, pero presenta una interface gráfica, lo que hace más cómoda e intuitiva la configuración del equipo.

Para el ingreso mediante Winbox se puede usar el IP del equipo asociado; para esto el equipo debe estar configurado dentro de la misma red IP o existir rutas hacia este equipo, caso contrario se puede usar el MAC Address del equipo para ingresar directamente por MAC – Telnet. Si no se conoce la dirección IP del equipo se puede hacer click en (…), esto hará que winbox busque el *MAC Address* del equipo instalado y ejecutando RouterOS

Figura 1.10 Pantalla de acceso por Winbox

Una vez ingresado al equipo (logging), en la barra de estado superior indica el IP o *MAC address* asociado al equipo, el nombre del equipo (si se encontraría configurado), la versión del software winbox que se está usando, y el tipo de arquitectura del procesador del equipo sobre el cual está instalado RouterOS, por ejemplo una placa RouterBoard o un equipo con procesador basado en x86.

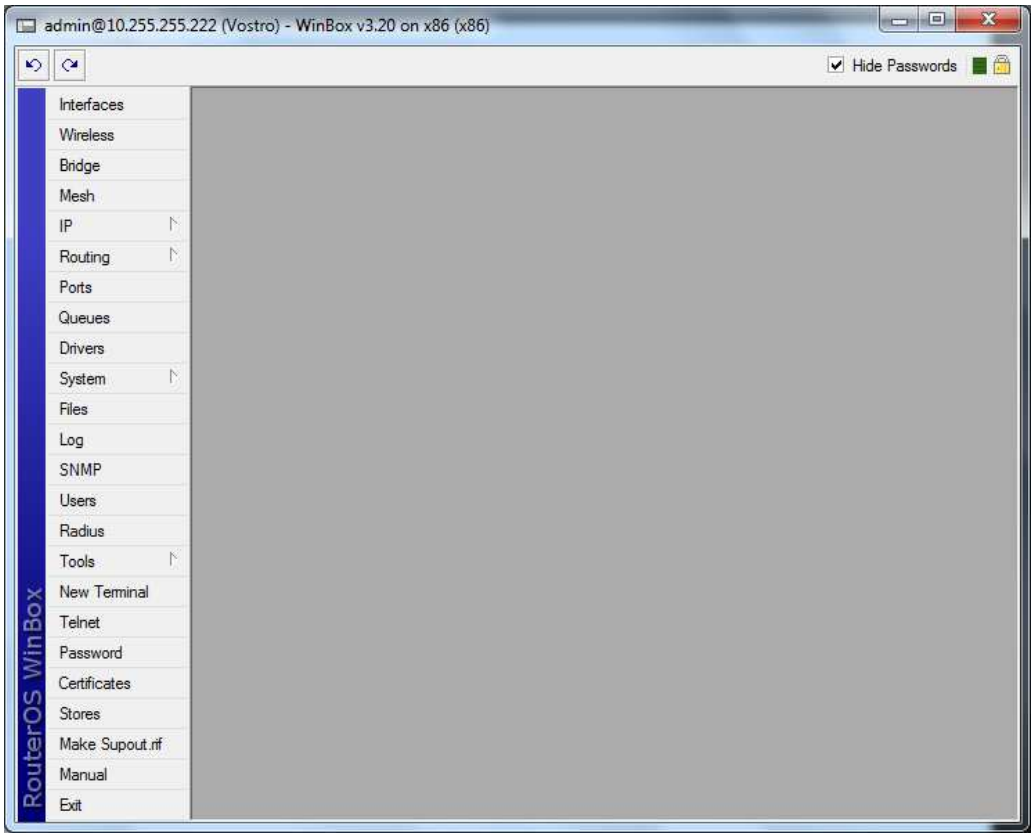


Figura 1.11 Entorno de RouterOS Winbox

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

Interface: Permite agregar, eliminar, habilitar, deshabilitar, definir diferentes tipos de interfaces a configurar como puede ser: Ethernet, *EoIP Tunnel, Mesh, Vlan, Bridge,* etc.

Wireless: Permite administrar las interfaces inalámbricas, modificar parámetros que guarden relación con el modo de funcionamiento de la tarjeta inalámbrica, como puede ser el modo: Access Point, Cliente, Bridge, Estación WDS, etc.

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

Mesh[I]*:* Permite configuración y administración de redes *Mesh*.

PPP: Permite habilitar tuneles tipo: PPP *(Point to Point Protocol)*, PPTP *(Point to Point Tunnelig Protocol)*, L2TP *(Layer 2 Tunneling Protocol)*, OVPN *(Open Virtual Private Network)*, PPPOE *(Point to Point Over Ethernet)* en diferentes modos, es decir como cliente o como servidor.

IP: Administra protocolos de capa 3 como: TC/IP, *Firewall*, DHCP, *Firewall*, DNS, *Hotspot*, IPsec, SNMP, DNS, etc.

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

VPLS[II]*:* Este protocolo permite la comunicación entre dos redes con un único dominio de *broadcast*, es decir permite trabajar dos redes remotas en la capa 2 del modelo OSI.

Routing: Permite el uso de protocolos de enrutamiento como: OSPF, RIP, BGP, MME *(Mesh Made Easy)*, este último utilizado para enrutar redes MESH, además permite la administración de filtros en el enrutamiento.

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

[I] ***Mesh networking*** es un tipo de red donde cada nodo puede actuar como un router independiente, independientemente si se encuentra conectado a otra red, lo que permite continuidad en la conexión.

[II] ***Virtual private*** **LAN** ***service*** (**VPLS**) es una forma de proveer Ethernet basado en comunicaciones multipunto a multipunto sobre redes IP/MPLS, esto permite redes geográficamente dispersas unirse dentro un mismo dominio de *broadcast*

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

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

Log: Permite tener guardar un historial de los cambios realizados en las configuraciones del router, además de ser una bitácora de actividad del router.

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

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

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

1.7 MANEJO DE PAQUETES DEL SISTEMA[15]

RouterOS permite la administración de paquetes que el sistema ejecutará, es posible habilitar o deshabilitar, añadir o remover paquetes de instalación; por ejemplo, si se tiene un servidor dedicado para control de ancho de banda, no será necesario que administre interfaces inalámbricas, por lo que este paquete de sistema se puede deshabilitarlo o removerlo.

Para habilitar o deshabilitar un paquete del sistema, se ingresa en el menú principal, se busca la opción *System*, dentro de *System* desplegará un submenú en el cual se busca *Package*. Dentro de la ventana *Package List* se busca el paquete que se desea deshabilitar o desinstalar. Para que los cambios que se han realizado sean válidos es necesario reiniciar el equipo.

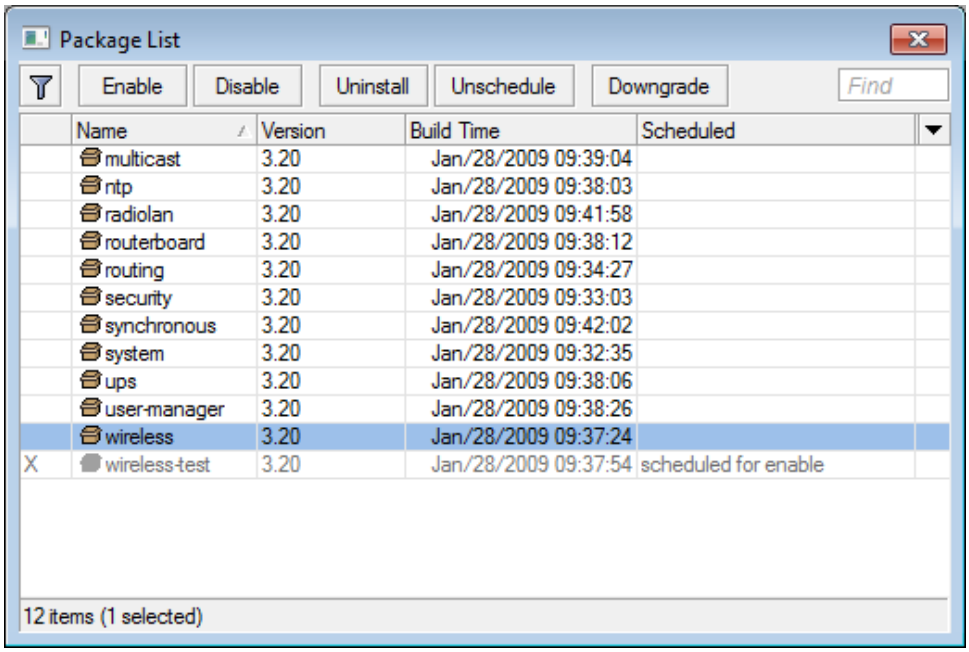


Figura 1.12 Paquetes instalados

CAPÍTULO 2

CONFIGURACIÓN DEL SISTEMA ROUTEROS

2.1 CONSIDERACIONES DEL SISTEMA ROUTEROS

Debido a la complejidad y lo extenso de los diferentes tópicos que encierra las redes de datos, se va a incluir ejemplos de configuraciones básicas y que incluyan la dificultad inherente a los temas que se está considerando.

La forma más sencilla e intuitiva para la configuración de RouterOS es mediante la herramienta gráfica WinBox, por lo que se partirá de este método para explicar su forma de configuración y eventualmente, y de ser necesario se incluirá configuraciones bajo línea de comandos.

Dentro de RouterOS y WinBox hay un número de lugares duplicados que permiten configurar un parámetro, por ejemplo si se desea configurar una interface inalámbrica se lo puede realizar a través de la sección interface o se puede realizar la misma configuración mediante la sección *wireless interface*

2.2 ADMINISTRACIÓN DE USUARIOS

Crear un listado de usuarios que tendrán acceso para administración o simplemente lectura de las configuraciones es importante a la hora de implementar seguridades en nuestro router, este listado contendrá usuarios que tienen permiso de administración; usuarios simplemente de lectura de las configuraciones, los cuales no pueden modificar configuraciones; o usuarios que pueden cambiar las configuraciones pero no pueden eliminar o cambiar usuarios.

Para crear un nuevo usuario, se ingresará en el menú principal del WinBox, se busca *System*, y dentro del submenú se busca *User*. En la nueva ventana se da clic el símbolo (+), y en la nueva ventana se llena los campos con el nombre del usuario, el grupo al cual pertenecerá que puede ser: *read*, - grupo de lectura, *full* - opción para administración completa, y *write* - para modificar configuraciones, y de ser necesario se puede definir las redes IP permitidas para la administración.

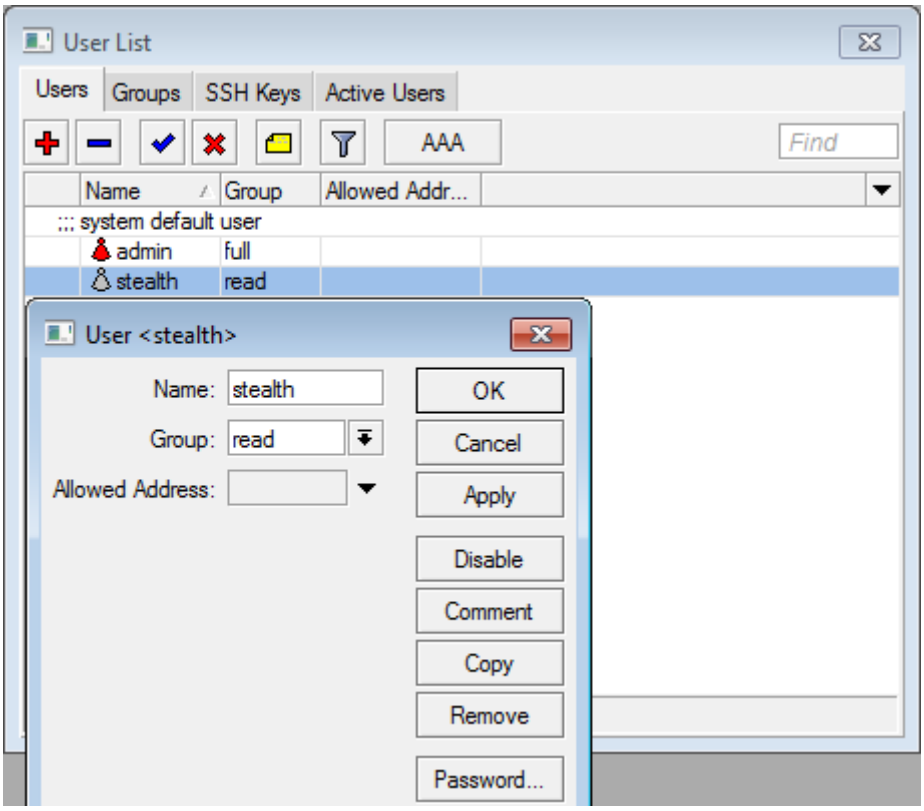


Figura 2.1 Lista de usuarios

Dentro de la opción *Groups* es posible crear un grupo que tenga permisos diferentes a los tres conocidos; por ejemplo, es posible considerar un grupo de usuarios a los cuales se les está permitido ingresar al equipo mediante la herramienta Telnet, para se creará un nuevo grupo en el que las políticas permita el uso de Telnet.

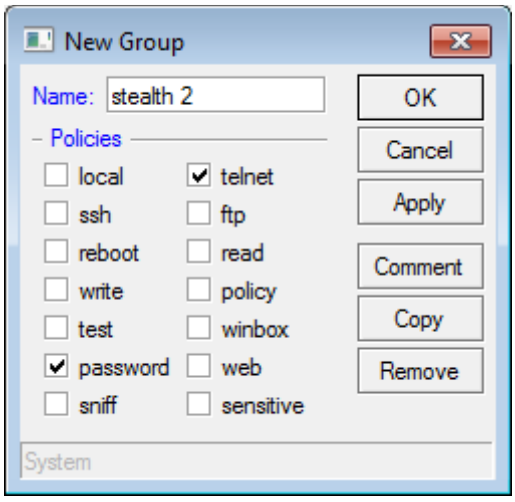


Figura 2.2 Lista de permisos para usuarios

Es posible determinar que usuarios se encuentran activos dentro del equipo mediante la vinieta *Active Users*, aquí indica la dirección IP desde la que se ingresa al router, y la forma de acceso al equipo (Telnet, WinBox, SSH, Webbox)

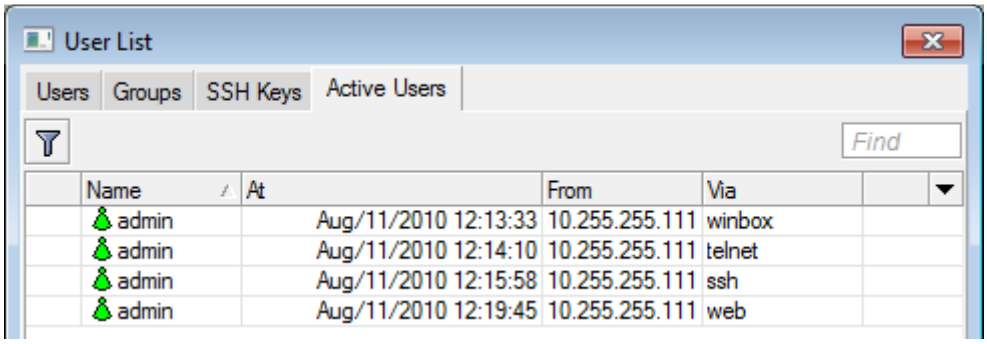


Figura 2.3 Lista de usuarios activos

2.3 CONFIGURACIÓN TCP/IP

2.3.1 CONFIGURACIÓN DE UNA DIRECCIÓN IP

Para el ingreso y configuración de cualquier tipo de router es necesaria la configuración de una dirección IP, en este trabajo no se incluirá el estudio del protocolo TCP/IP y subredes debido a la extensión del tema.

Para ingresar una nueva dirección IP, en el menú izquierdo se busca IP, y en el listado desplegado se escoge *Address*, se hace clic sobre el icono del signo (+); en la pantalla desplegada se indica cuatro campos: la dirección IP *(Address)*, la máscara de subred, el final del segmento de red, y la interface que va a asumir dicha IP. Se ingresa los datos de la dirección IP, la red y la interface, ya que la dirección *Broadcast* es calculada automáticamente.

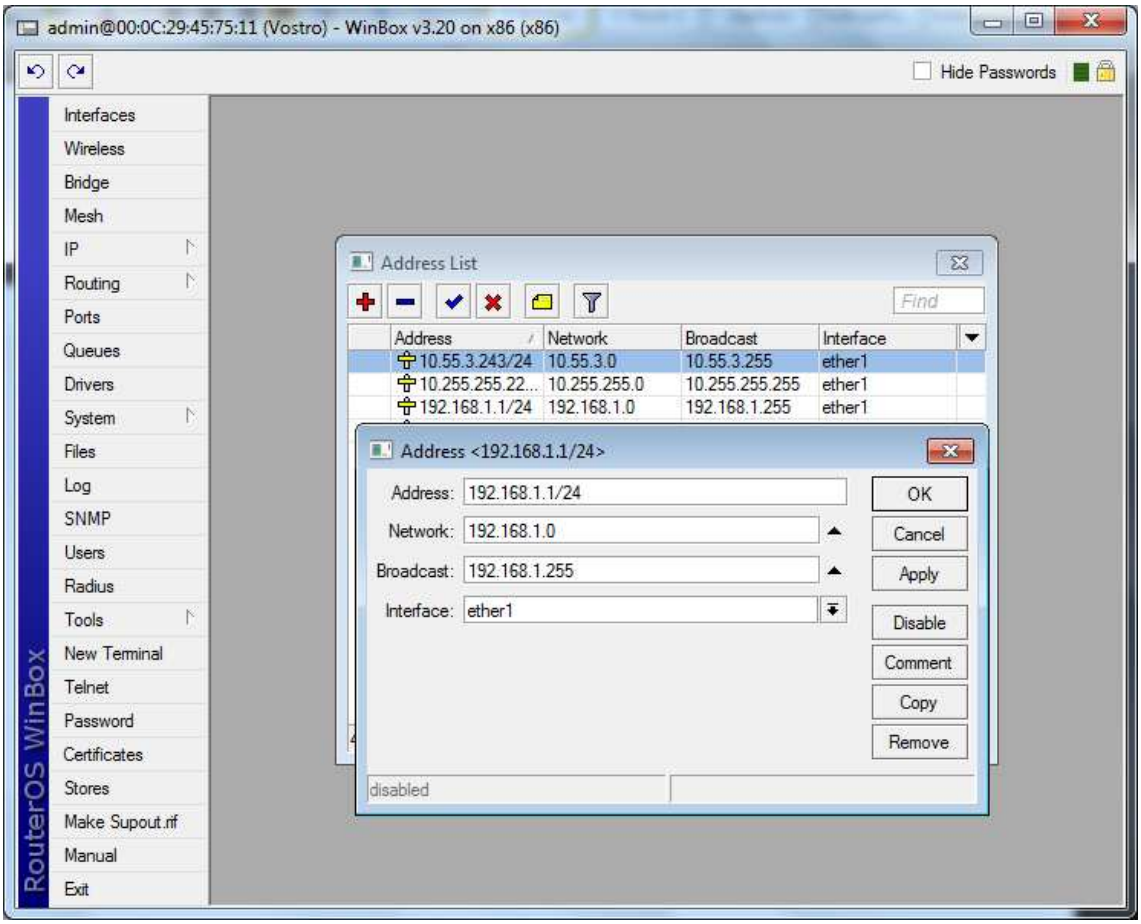


Figura 2.4 Configuración de dirección IP

Es también posible ingresar la dirección IP mediante notación decimal, es decir que la configuración de octetos en la máscara identifica los bits de red y los bits de host, por ejemplo 255.255.255.0 una típica clase C, pero es posible también la notación CIDR (*Classless Inter-Domain Routing*) en la que se ingresa el número de red seguido de una barra y un número que corresponde al número de bits que corresponde a la mascará de subred, por ejemplo 192.168.1.1/24 indica una red clase C.

Esta configuración se la puede realizar por consola mediante línea de comandos de la siguiente forma:

```
admin@Vostro] ip address> add address=192.168.1.1/24 interface=ether1
[admin@Vostro] ip address> print
Flags: X - disabled, I - invalid, D - dynamic
  #   ADDRESS            NETWORK         BROADCAST       INTERFACE
  0   192.168.1.1/24     192.168.1.0     192.168.1.255   ether1
  1   10.55.3.243/24     10.55.3.0       10.55.3.255     ether1
  2   10.255.255.5/24    10.255.255.0    10.255.255.255  ether1
```

Al momento de ingresar una dirección IP esta será asignada a una de las interfaces físicas, virtuales o inalámbricas que han sido creadas dentro del router, y estas son reflejadas en las interfaces del router. Para visualizar y/o modificar los valores de las interfaces se ingresa por Interface y en la ventana Interface indicará las interfaces detectadas en el router, en el lado izquierdo se indicará con una R *(Running)* en caso de que la interface se encuentre registrada, o tenga link.

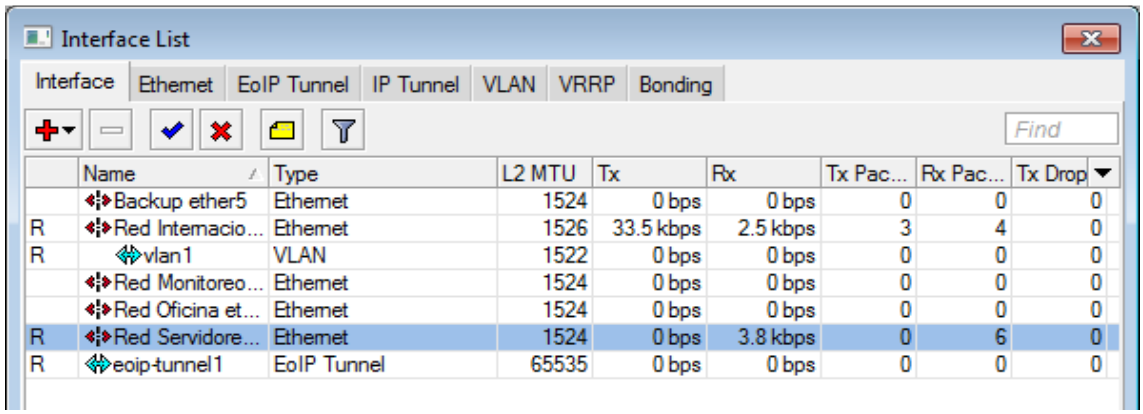


Figura 2.5 Lista de interfaces

Dentro de cada interface es posible monitorear, modificar o configurar parámetros propios del tipo de interface; por ejemplo en el caso de una interface Ethernet, es posible modificar la velocidad de negociación, el tipo de operación (full dúplex, half dúplex, auto negociación), el valor MTU *(Maximum Transfer Unit*, determina el tamaño de la unidad de datos IP), o asignar un valor de ancho de banda para la interface Ethernet.

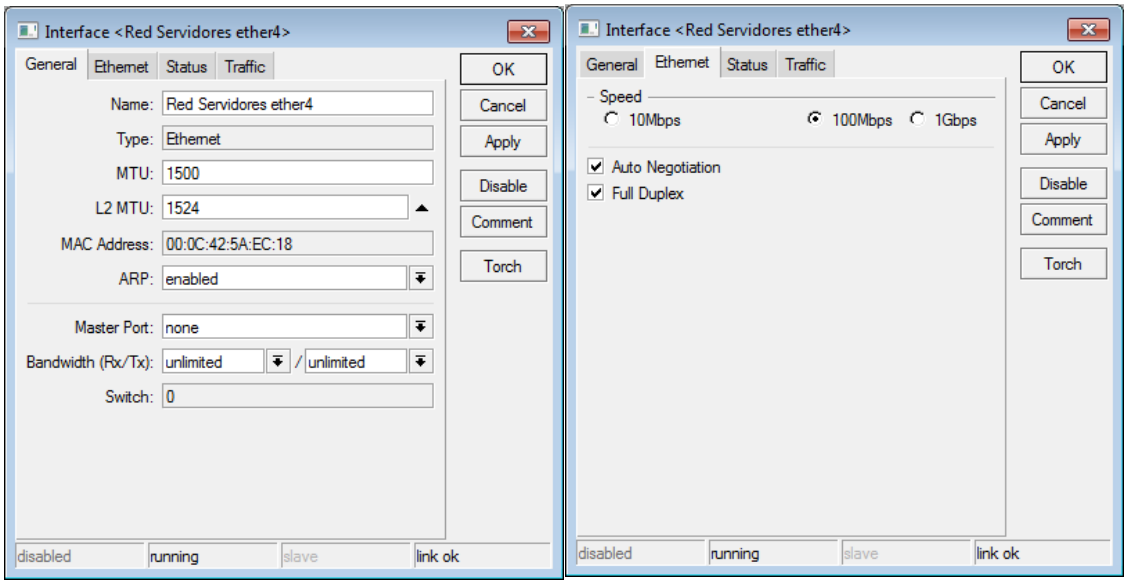


Figura 2.6 Interface Ethernet

2.3.2 PUERTA DE ENLACE (*GATEWAY*)

Una puerta de enlace es el equipo que permite la comunicación desde una red hacia otra red o grupo de redes, incluyendo Internet, especifica las rutas que deben seguir para alcanzar a un determinado host. Para ingresar un default Gateway o puerta de enlace, en el menú IP se busca Route, se da clic sobre el signo (+), y se ingresa los campos *destination* y *Gateway*.

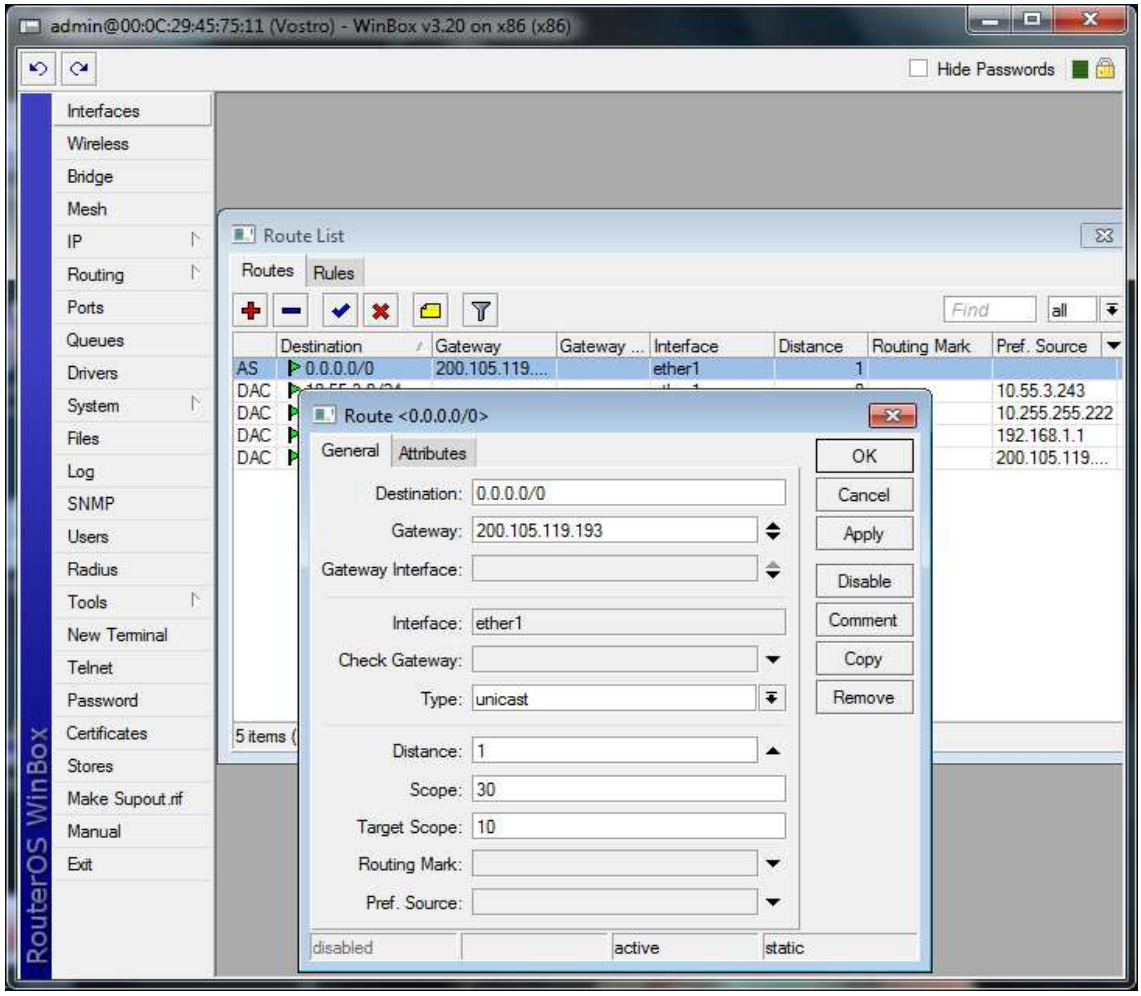


Figura 2.7 Configuración de puerta de enlace

RouterOS utiliza un "*default destination-address*" 0.0.0.0/0, los ceros indican que todas las redes con cualquier máscara pueden ser alcanzadas por el equipo, mediante el *Gateway* abajo especificado.

Esta configuración es posible mediante línea de comandos, para este ejemplo se usará Telnet mediante el programa Putty usado para administración de equipos remotos.

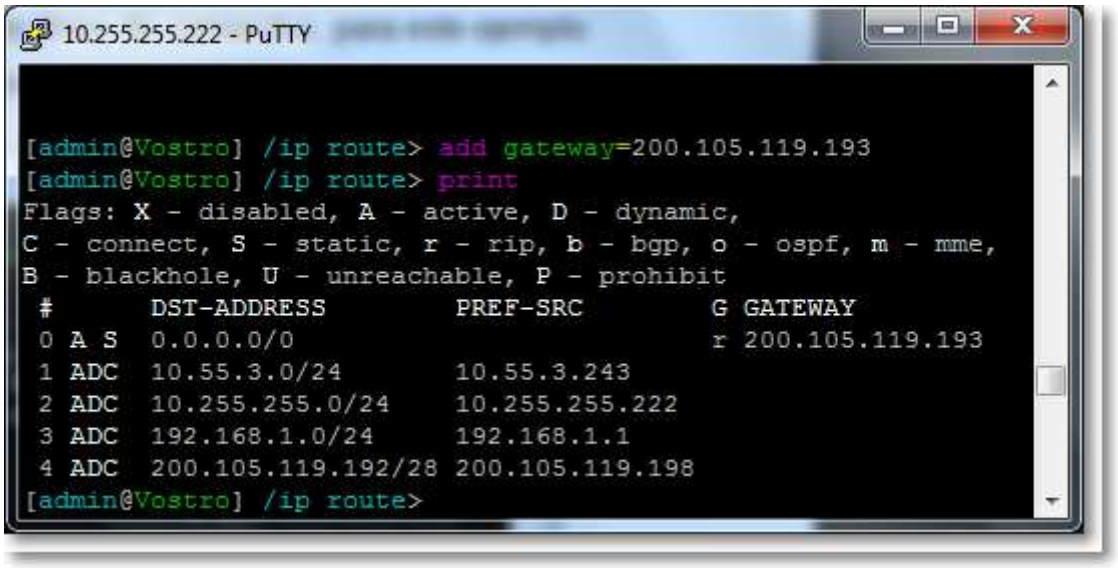


Figura 2.8 Configuración del Gateway mediante Telnet

2.3.3 DNS

Los servidores DNS *(Domain Name System)* permiten la traducción de direcciones de red inteligibles para humanos a dígitos binarios asociados a servidores host. RouterOS permite hacer DNS Caching, esto significa que RouterOS utiliza una sola vez los DNS's del ISP, y para los equipos conectados a él los entrega directamente, esto significa que un equipo conectado detrás del router con RouterOS no necesita ir hasta un servidor DNS del ISP *(Internet Sevice Provider)*, sino que realiza el traslado directamente del equipo RouterOS, en un tiempo mucho menor. Para ingresar servidores DNS en RouterOS, en el menú principal se busca IP, dentro de IP DNS, con el símbolo (+) se abre una ventana de configuración, en la cual se incluye el nombre del servidor DNS, y la dirección IP del servidor.

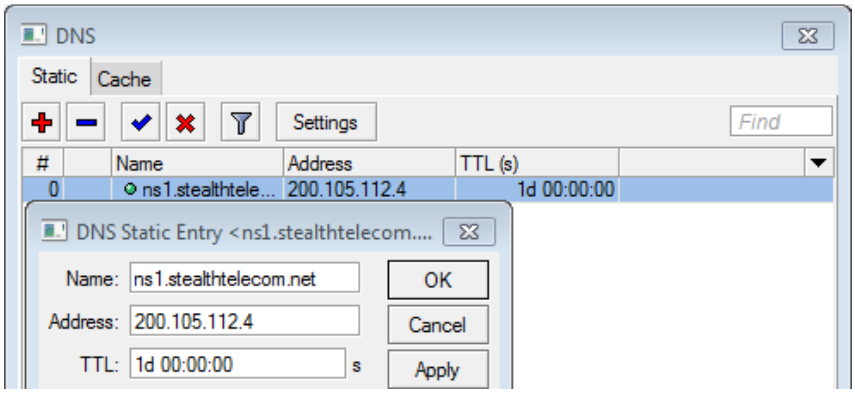


Figura 2.9 Configuración DNS

Configuración de los DNS's mediante línea de comandos a través de Telnet.

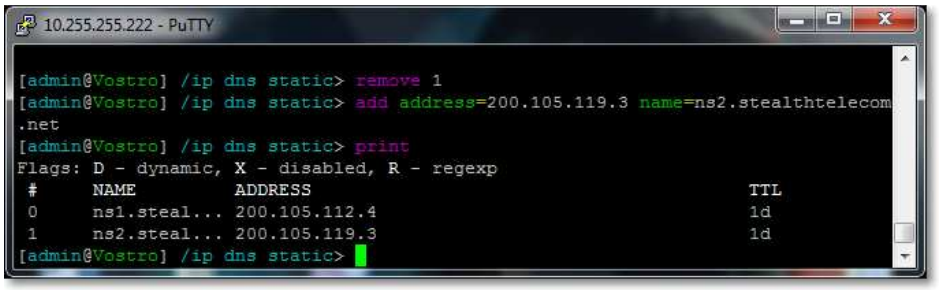


Figura 2.10 Configuración de DNS's mediante Telnet

2.3.4 CONFIGURACIÓN DE DHCP COMO CLIENTE.

Muchas veces los proveedores de Internet, permite a sus clientes obtener direcciones IP automáticamente vía DHCP *(Dinamic Host Configuration Protocol)*.

Para acceder al DHCP modo cliente, se ingresa mediante el menú IP se ingresa en DHCP-client, se da clic sobre el signo (+), la configuración más importante es la interface que se desea correr el DHCP *client*, el resto de configuraciones pueden no ser configuradas ya que no son parámetros importantes de funcionamiento, por ejemplo el NTP *(Network Time Protocol)* es utilizado para sincronización de husos horarios. El botón status muestra la dirección IP obtenida, el *Gateway*, dirección del servidor DHCP, DNS e información NTP, además indica el tiempo de validez de los datos obtenidos.

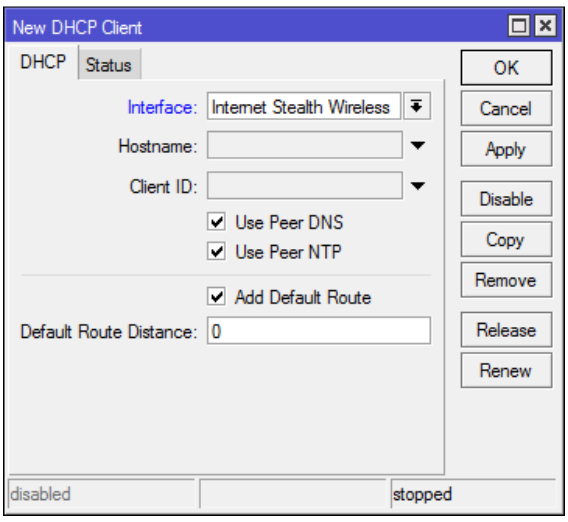


Figura 2.11 Configuración DHCP cliente

2.3.5 CONFIGURACIÓN DNS COMO SERVIDOR

RouterOS tiene la capacidad de funcionar como un servidor DHCP, y administrar múltiples servidores DHCP con diferentes direcciones IP, esto significa que se puede asignar toda la información necesaria a nuestros clientes de forma automática.

Se debe tomar en cuenta que cuando se habilita la opción de crear un servidor DHCP no es posible añadir dicha interface a un grupo en modo bridge (puente).

Para configurar un nuevo servidor DHCP dentro de RouterOS se ingresa IP, y se busca DCHP Server, se da clic en el signo (+), se busca el icono DHCP setup, esta es una forma sencilla e intuitiva de configurar un servidor DHCP.

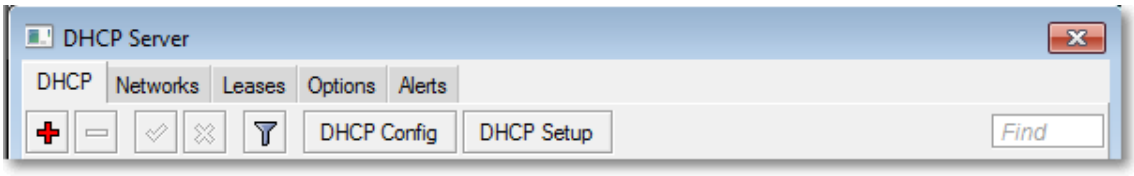


Figura 2.12 Configuración servidor DHCP

Aparecerá una pantalla solicitando la interface donde se va a crear el DHCP server, es importante tener en cuenta que el DHCP correrá sobre una interface.

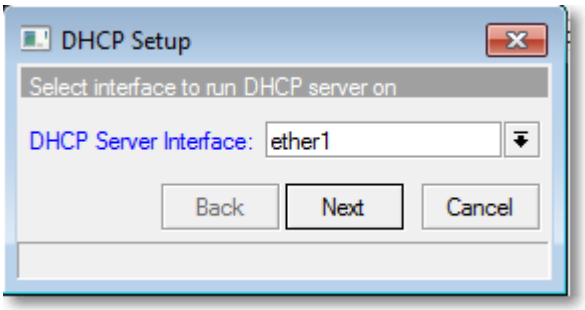


Figura 2.13 Interface DHCP servidor

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

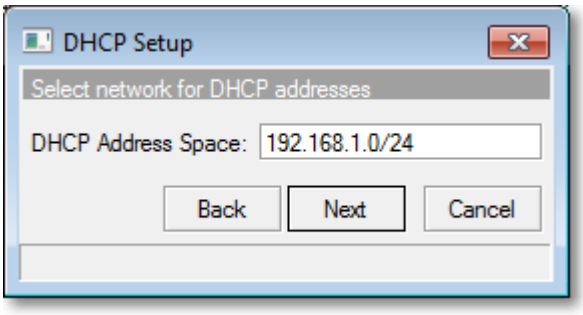


Figura 2.14 Asignación de red DHCP

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

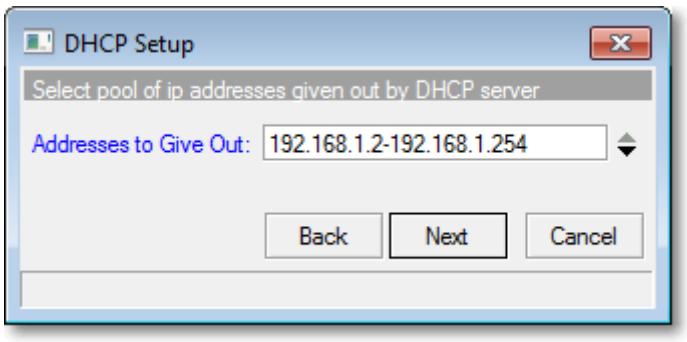


Figura 2.15 Configuración rango DHCP

Y al final los servidores DNS's.

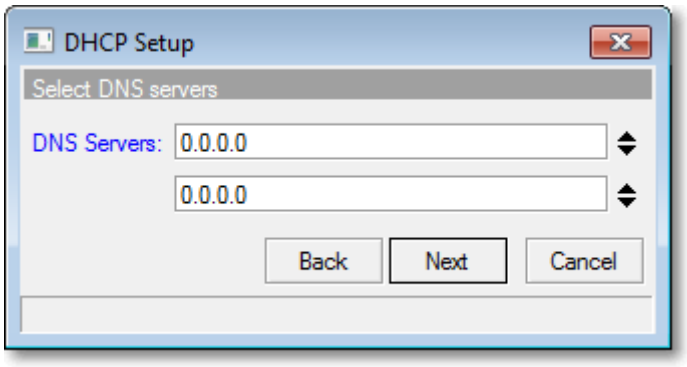


Figura 2.16 Configuración servidores DNS para DHCP

Finalmente se configurará el tiempo que el cliente guardará la dirección IP antes de ser reasignada automáticamente, y con esto indicará que la configuración ha sido completada satisfactoriamente.

Una vez que se ha finalizado con la configuración, en las diferentes viñetas de la pantalla principal indicará las configuraciones realizadas y el listado de equipos que han sido asignados con parámetros del DHCP server.

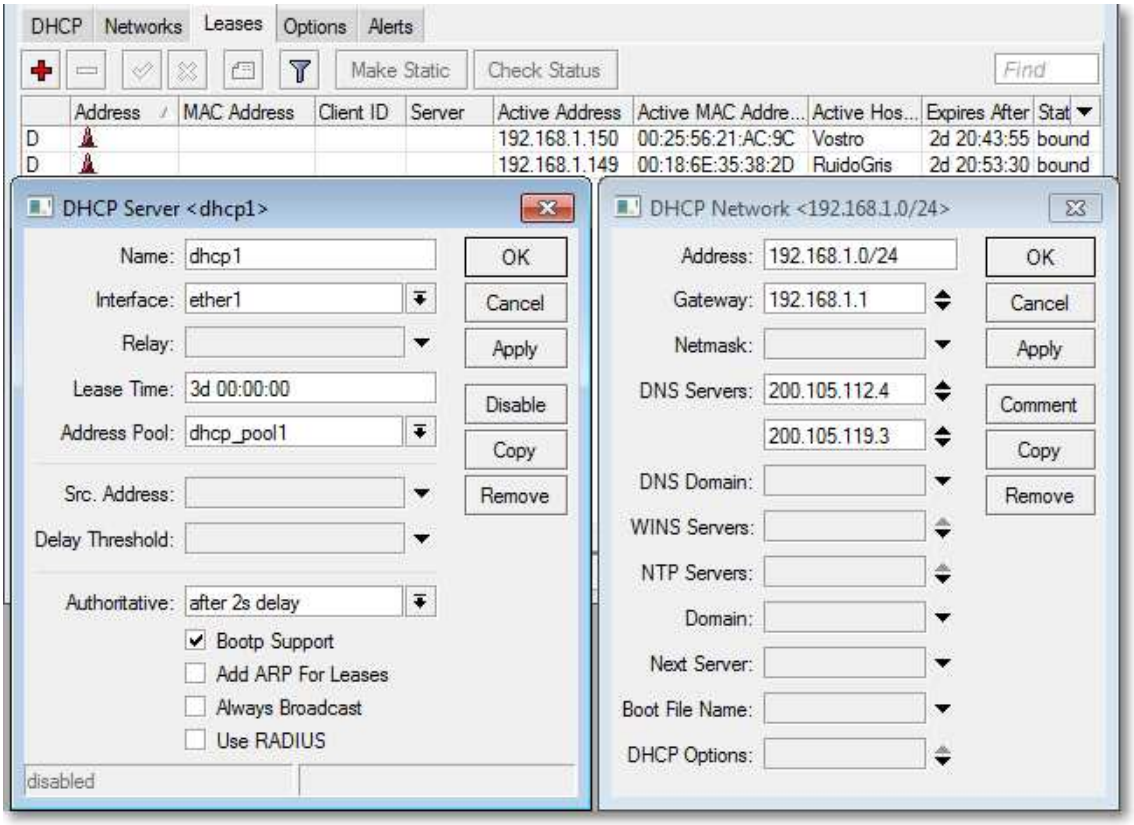


Figura 2.17 Pantalla configuración servidor DHCP

Dentro de la viñeta DHCP network es posible configurar DNS *Domain, WINS* en caso de trabajar con servidores de red internos, *Domain* para trabajar dentro de un dominio de red, NTP server para sincronizar la fecha en todos los equipos con asignación DHCP.

2.4 ENMASCARAMIENTO IP Y TRADUCCIÓN DE DIRECCIONES DE RED

2.4.1 ENMASCARAMIENTO / TRASLACIÓN DE DIRECCIONES DE RED (NAT)

Esta característica permite mediante una dirección IP pública que tienen acceso a Internet, trasladar el acceso a Internet a varios equipos con direcciones IP privadas. Esto debido a la escasez de direcciones IPv4 los proveedores de Internet están limitados de entregar direcciones IP a todos los

equipos de una red, pero mediante el uso de NAT o enmascaramiento se puede permitir que una red privada de equipos, pueda acceder a Internet a través de una única IP válida en Internet, de esta manera además se protege la red privada de ataques desde Internet.

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

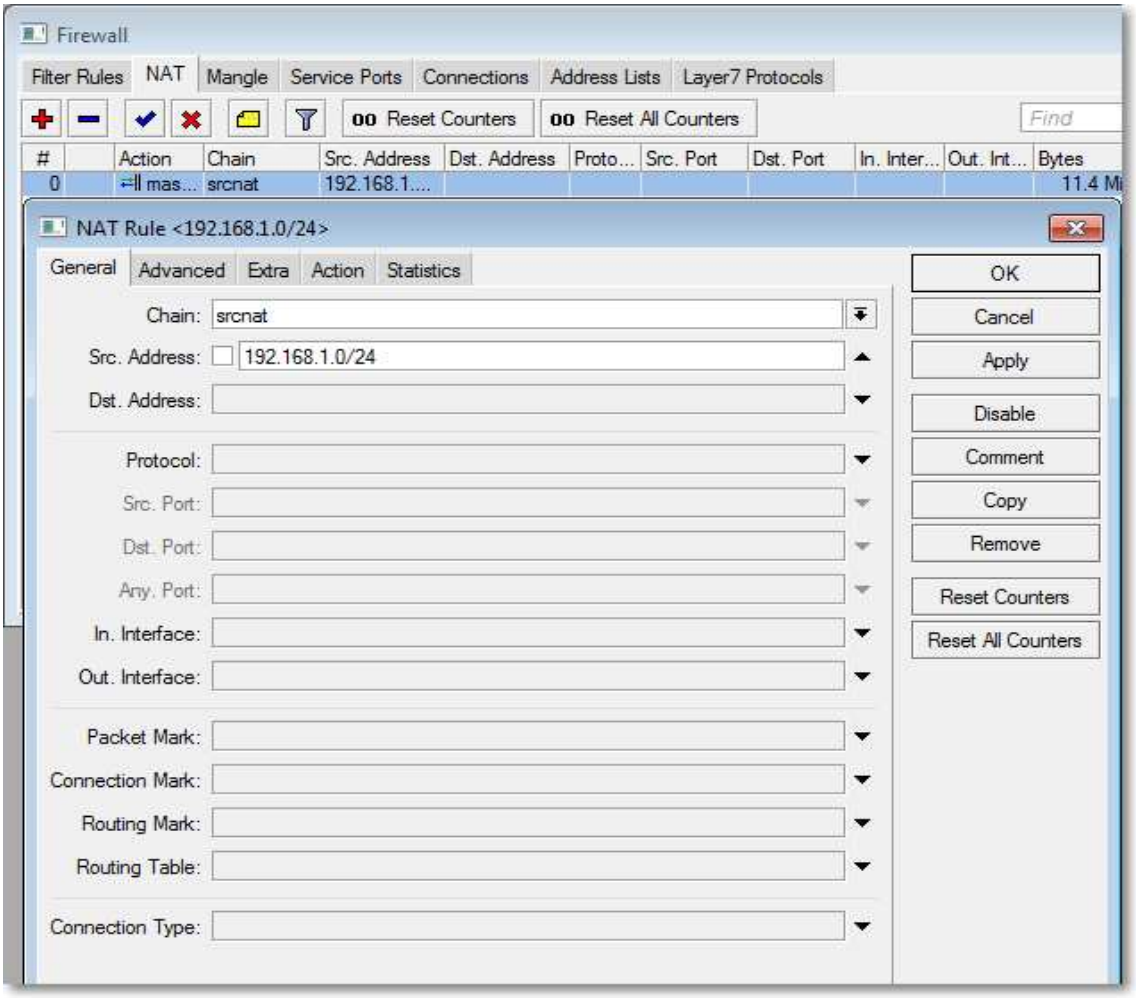


Figura 2.18 Configuración NAT

Para un ejemplo, la direccion fuente de red *o source address* es la red 192.168.0.0/24, que se encuentra previamente configurada en la interface ether 1, esto indica que toda la red clase C 192.168.0.0, va a ser enmascarada por la IP de la interface ether 2.

A continuación se escoge la acción que realizará la regla marcada, en este caso enmascaramiento *(masquerade)*

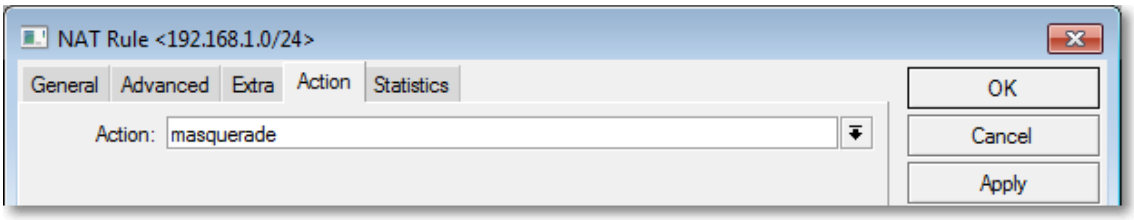


Figura 2.19 Enmascaramiento NAT

2.4.2 DMZ CON MIKROTIK *(DESMILITARIZED ZONE)*

Una DMZ es una zona que se encuentra entre la red local o red interna protegida por un firewall y una red externa que generalmente es la Internet, esto permite que equipos que se encuentran dentro en la DMZ puedan dar servicios hacia el exterior sin tener que exponer la red interna al ataque de intrusos esto ya que la red interna se encuentra detrás de un Firewall.

La utilización de DMZ's se lo realiza por lo general para permitir que servidores o equipos host que se encuentran detrás de un NAT puedan ser alcanzados desde la Internet, todo esto mediante la administración de un solo equipo ruteador que utilizará reglas de firewall dst-nat

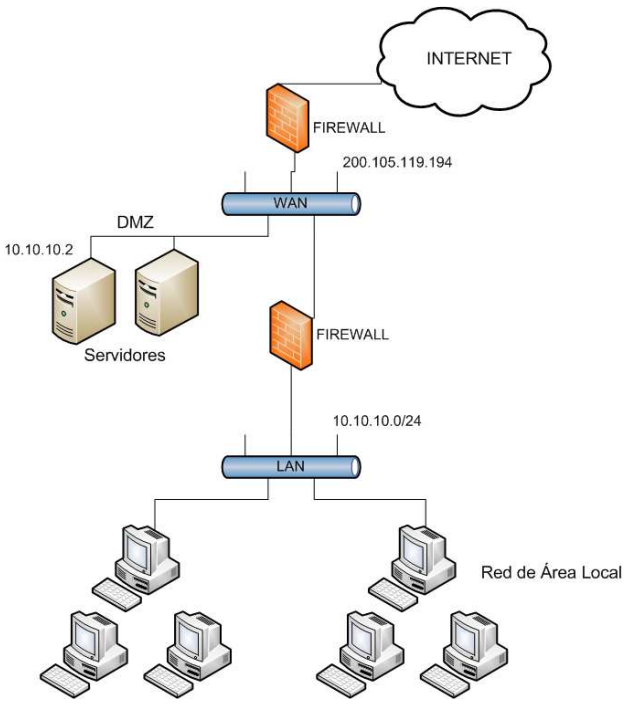


Figura 2.20 Configuración de una red con DMZ

Se crea un DMZ para un servidor el cual se encuentra dentro de la red interna 10.10.10.2/24, el cual será enmascarado por la dirección pública 200.105.119.194.

Se configura una interface del ruteador con la puerta de enlace para la red interna la cual se denominará DMZ-zona con la dirección IP 10.10.10.1, y una segunda interface llamada WAN con la dirección IP pública 200.105.119.194.

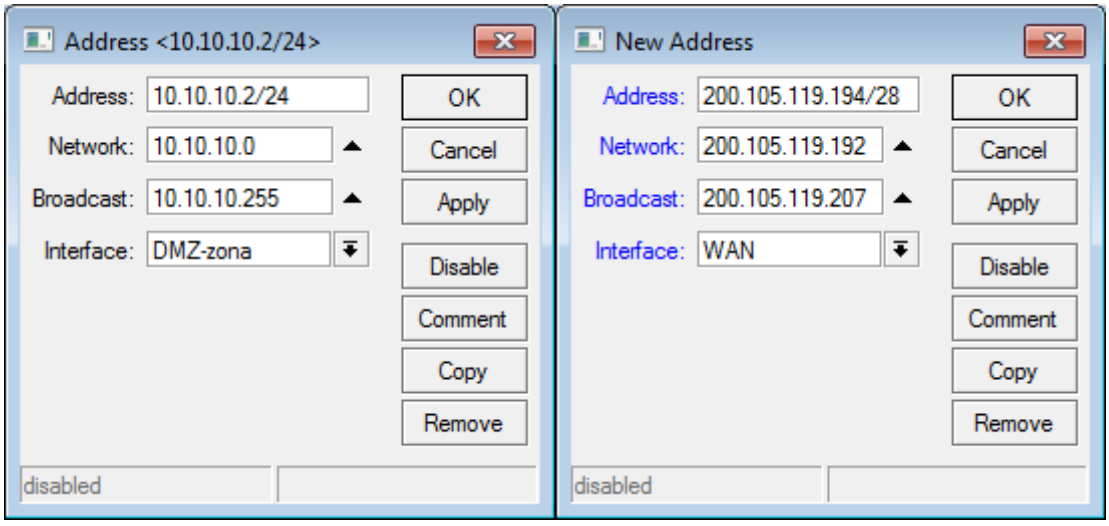


Figura 2.21 Direccionamiento DMZ

Dentro del Firewall/NAT se configura las reglas que permitirán el redireccionamiento de las direcciones IP, esto mediante el uso de la herramienta dst-nat. Esta regla indica que todo el tráfico que tenga destinado hacia la dirección IP 200.105.119.194/28 detrás de un NAT, sea redirigido hacia la dirección IP 10.10.10.2 de la red interna.

La configuración quedará de la siguiente manera:

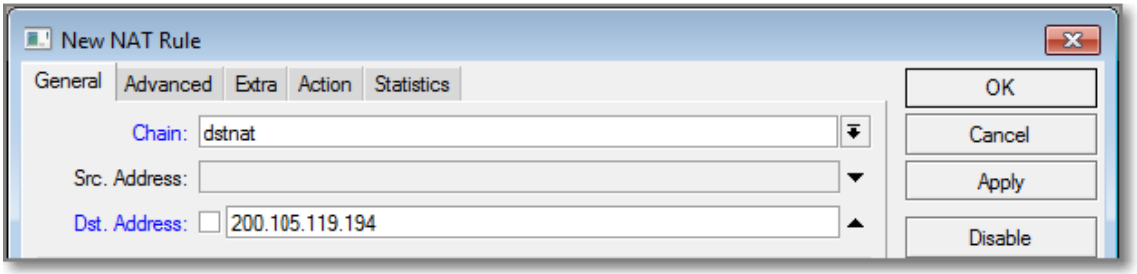


Figura 2.22 Redireccionamiento DMZ WAN

Y en la viñeta *Action* se indica el redireccionamiento:

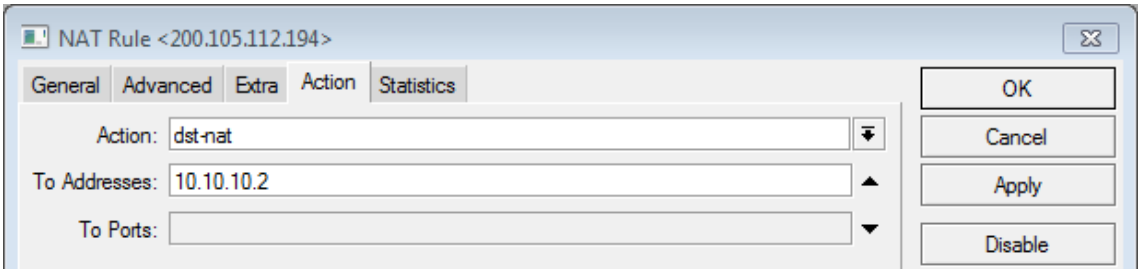


Figura 2.23 Redireccionamiento DMZ LAN

2.4.3 DIRECCIONAMIENTO DE PUERTOS

Esta técnica es usada para administrar, ejecutar o publicar varios servicios en Internet mediante el uso de una única IP pública configurada en un router de borde o frontera, por ejemplo; si se dispone de una IP pública en la empresa y se necesita exponer servidores de http, e-mail, ftp, etc., es posible realizarlo mediante el redireccionamiento de puertos hacia esta IP pública única.

Para aclararlo, se va a utilizar un ejemplo:

Se dispone de una única dirección IP pública 200.105.119.194, y se necesita publicar una página web, además se precisa exponer el servidor de correos y un servidor FTP.

El servidor de la página web tendrá que responder mediante el puerto TCP 80 a las solicitudes de Internet, el servidor de correo utilizará los puertos TCP 25 y 110 respectivamente para el envío y recepción de correos, y el servidor FTP usará el puerto TCP 21 para la transferencia de archivos.

Detrás del NAT, las direcciones IP's designadas para los servidores son las siguientes:

- Servidor HTTP: 10.10.10.2
- Servidor Email: 10.10.10.3
- Servidor FTP: 10.10.10.4

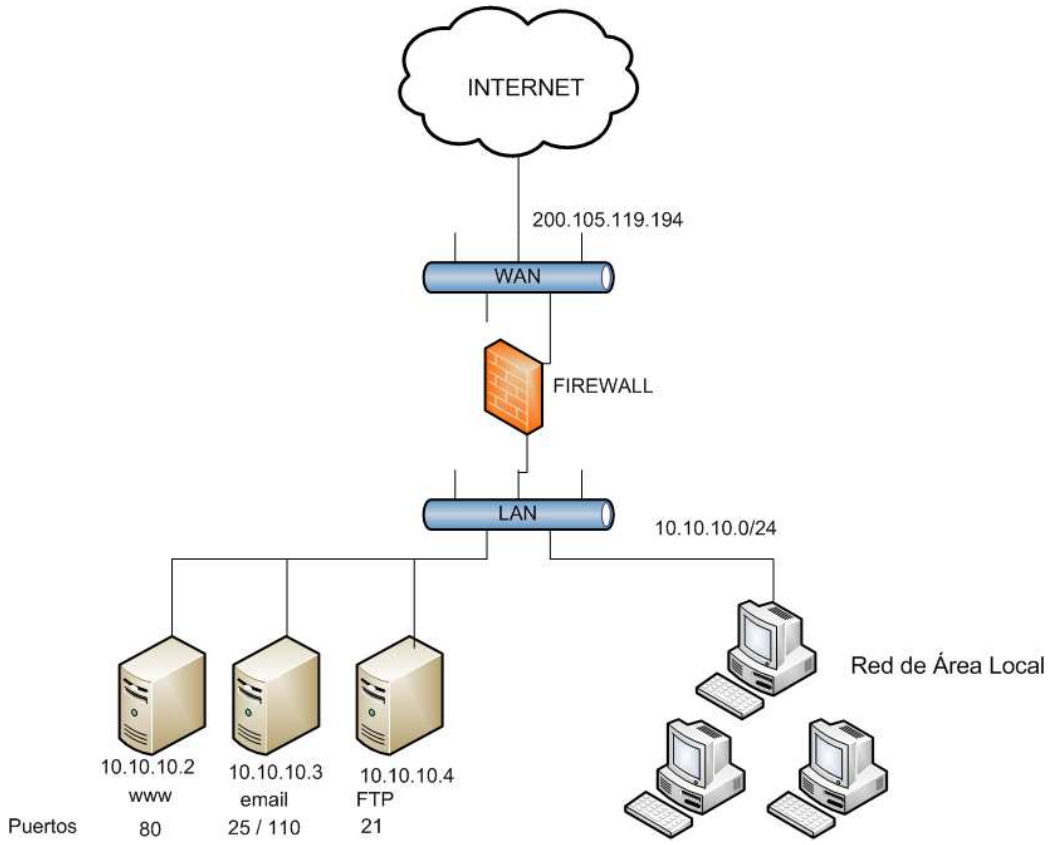


Figura 2.24 Esquema de redireccionamiento de puertos

Primero se agrega las direcciones IP a cada interface, en la interface Internet se configurará la IP pública 200.105.119.194, en la Interface Red Interna se agrega la IP 10.10.10.1 como puerta de enlace del área local.

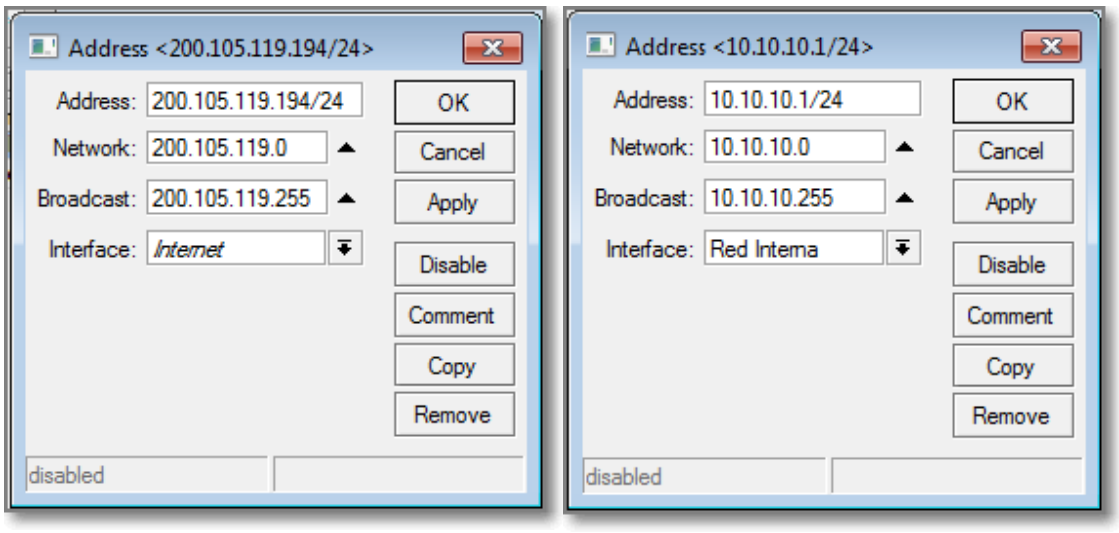


Figura 2.25 IP's con puertos redireccionados

2.4.3.1 Servidor WEB

A continuación se ingresa la regla de firewall que permitirá realizar el redireccionamiento de la IP pública hacia el servidor web mediante el puerto TCP 80.

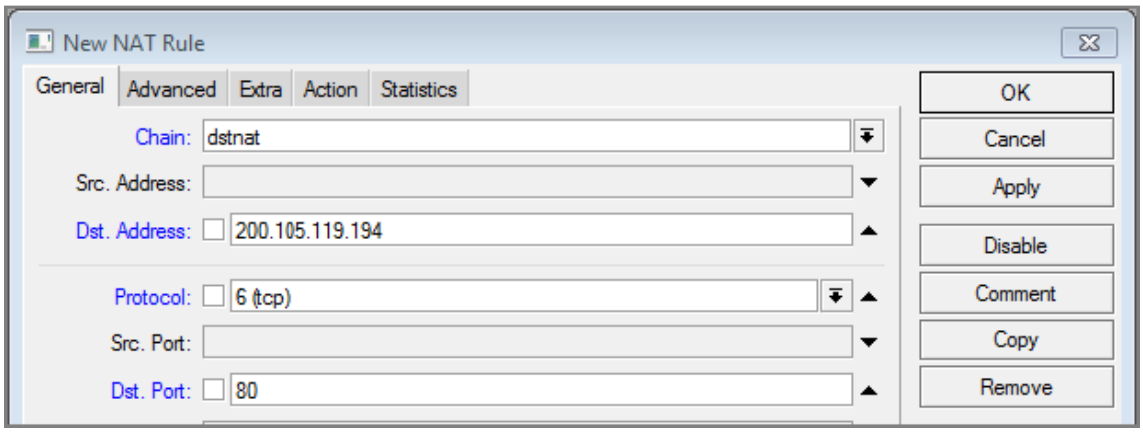


Figura 2.26 Redireccionamiento al servidor WEB

La regla indica que todo el tráfico de Internet destinado para la dirección IP 200.105.119.194 y que requiera el puerto TCP 80 sea direccionado a la dirección IP local 10.10.10.2 que es un servidor de página web

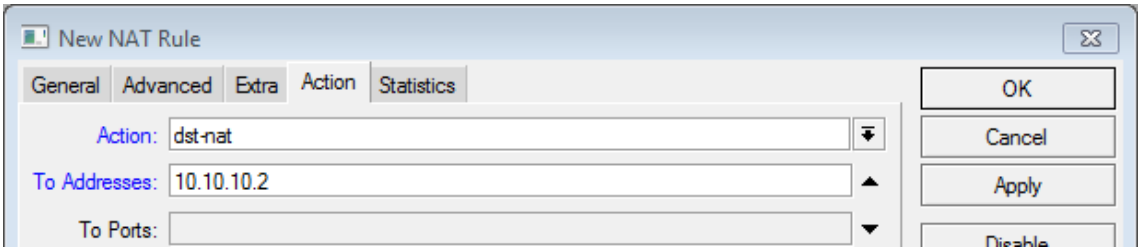


Figura 2.27 DST-NAT red LAN

2.4.3.2 Servidor Email

De forma similar al direccionamiento del servidor web se ingresa la regla de firewall que permitirían realizar el redireccionamiento de la IP pública hacia el servidor de correo usando los puertos TCP 25 y 110.

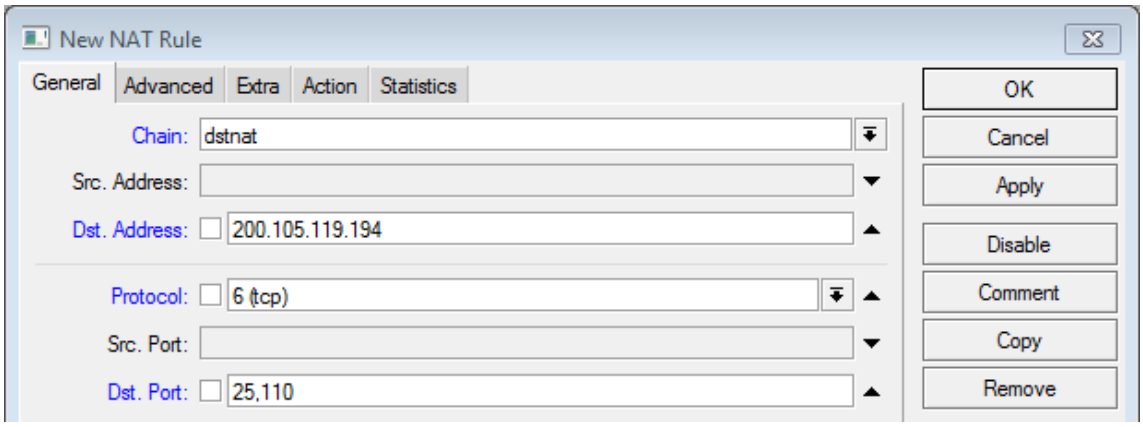


Figura 2.28 Redireccionamiento al servidor de correo

La regla indica que todo el tráfico que venga desde Internet destinado para la dirección IP 200.105.119.194 y requiera los puertos TCP 25 y 110 sea direccionado a la dirección IP local 10.10.10.3 que será el servidor de correo

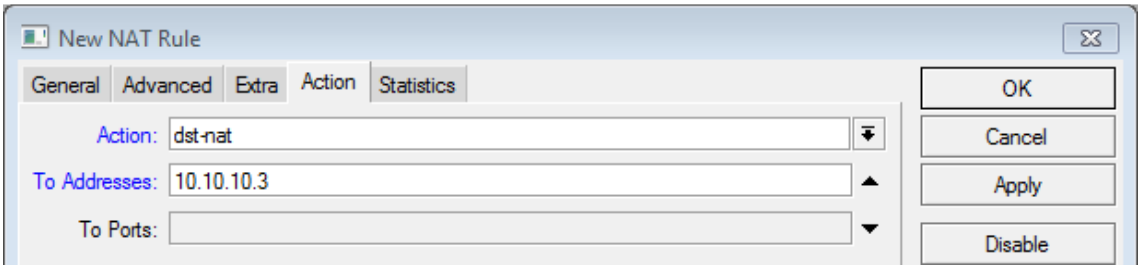


Figura 2.29 DST-NAT red LAN email

2.4.3.3 Servidor FTP

Finalmente se ingresa la regla que permitirá ingresar al servidor FTP a través de la IP pública usando el puerto TCP 21 usado para este fin.

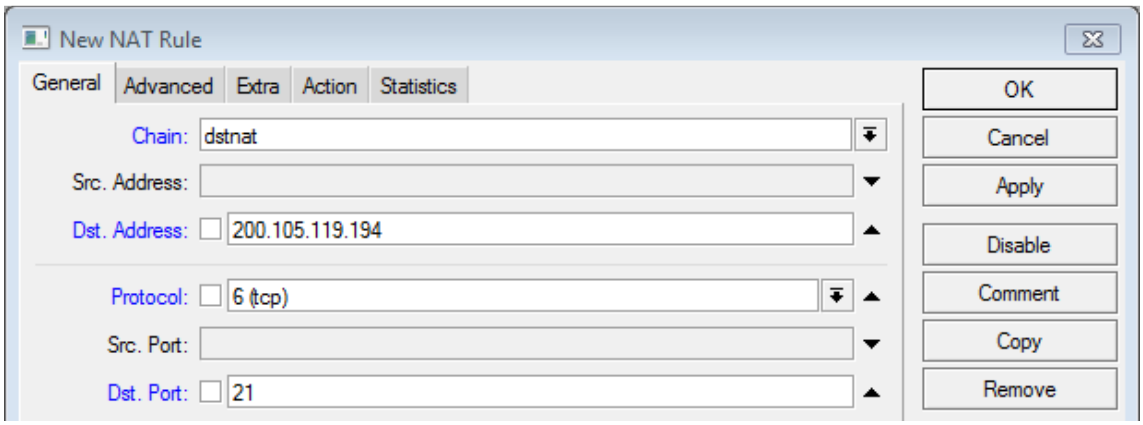


Figura 2.30 Redireccionamiento al servidor FTP

La regla indica que todo el tráfico que venga desde Internet destinado para la dirección IP 200.105.119.194 y requiera el puerto TCP 21 sea direccionado a la dirección IP local 10.10.10.4 que será el servidor de archivos FTP

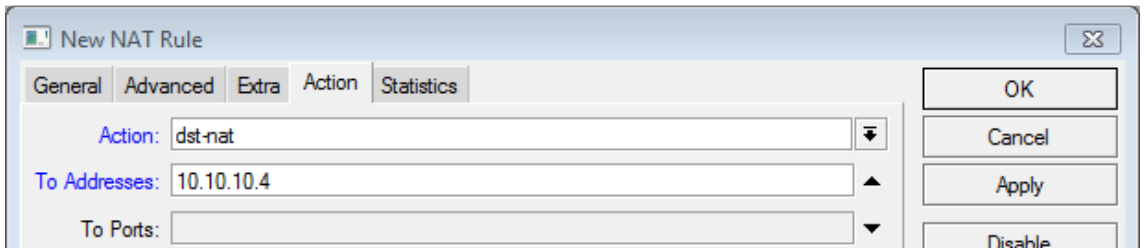


Figura 2.31 DST-NAT red LAN FTP

2.5 FIREWALL

2.5.1 SERVIDOR PROXY TRANSPARENTE, DENEGACIÓN DE SERVICIOS MEDIANTE PROXY

Un servidor PROXY es un equipo intermediario que mejora la calidad y el rendimiento del servicio a los usuarios conectados atrás de este, así como ayuda a mejorar la velocidad de conexión de los usuarios.

Al ser un equipo negociador entre la red interna y el Internet, permite incorporar reglas de seguridad a la red Interna, así como la restricción de servicios de forma individual o a un grupo de usuarios. Mediante el uso de memoria caché es posible el ahorro de tráfico.

Para configurar un servidor PROXY mediante RouterOS se trabaja en el menú principal se busca IP y en el submenú se busca Web Proxy

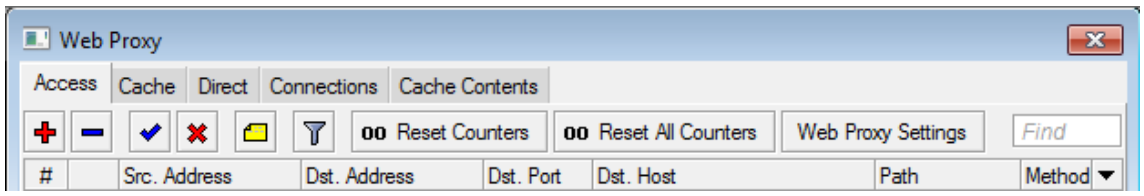


Figura 2.32 WEB proxy

Dentro de Web Proxy se da clic en Web Proxy *Settings*, de esta forma se ingresa a la ventana de configuración del servidor proxy, se llena los campos con la siguiente información:

- *Src. Address*: Si existe una sola red en la interface de LAN este campo puede quedar en blanco, caso contrario se identifica cual es la puerta de enlace *(Gateway)* de la red interna que debe filtrar mediante Proxy
- *Port: 8080*. Mediante este puerto se redirige el tráfico del puerto 80 al 8080 configurado como proxy se usa también el puerto 3128
- *Parent Proxy*: se deja vacío.
- *Parent Proxy Port*: se deja vacío.
- *Cache Administrator*: webmaster@stealthtelecom.net
- *Max. Cache Size: none*. Actualmente por la gran demanda de tráfico y la dinámica en las páginas de Internet no tiene mucho sentido el tener una memoria cache, por lo que se prefiere deshabilitar esta opción.
- *Cache on Disk*: no se escoge. Esta opción permite tener un disco duro extra para memoria cache.
- *Max. Client Connections*: 600. Este valor viene por defecto, y es el número de clientes conectados
- *Max. Server Connections*: 600. Este valor viene por defecto y son las conexiones administradas por el servidor.
- *Max. Fresh Time*: 3d 00:00:00. Indica el tiempo de refresco de cada enlace a usuario
- Cache Hit DSCP (TOS): 4 Indica si existe priorización de tráfico con Tipo de Servicio, el valor 4 es para tráfico normal (normal *Througthput*)

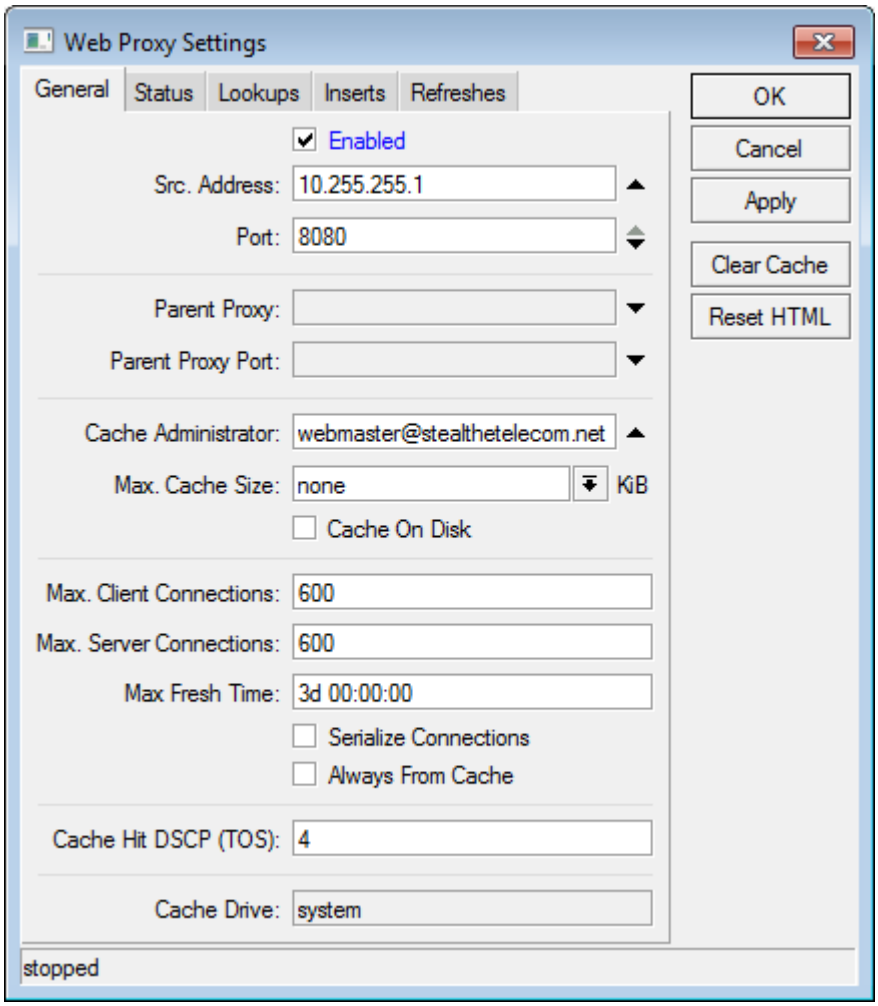


Figura 2.33 Configuración PROXY

Dentro del NAT del Firewall se debe incluir reglas para el direccionamiento del puerto 80 hacia el puerto 8080 del proxy configurado anteriormente. Para esto se ingresa en IP, Firewall / NAT, se da clic en el signo (+), y se configura la viñeta general con la siguiente información:

- *Chain: dstnat*. Indica que se realiza un NAT a la dirección destino
- *Src. Address*. 10.255.255.0/24. Indica la red interna que se desea filtrar
- *Protocol*: 6(tcp). Indica el tipo de protocolo que se quiere filtrar
- Dst. Port: 80. Indica el puerto de destino que se va a filtrar, en este caso se filtra el puerto 80 que está destinado para navegación.

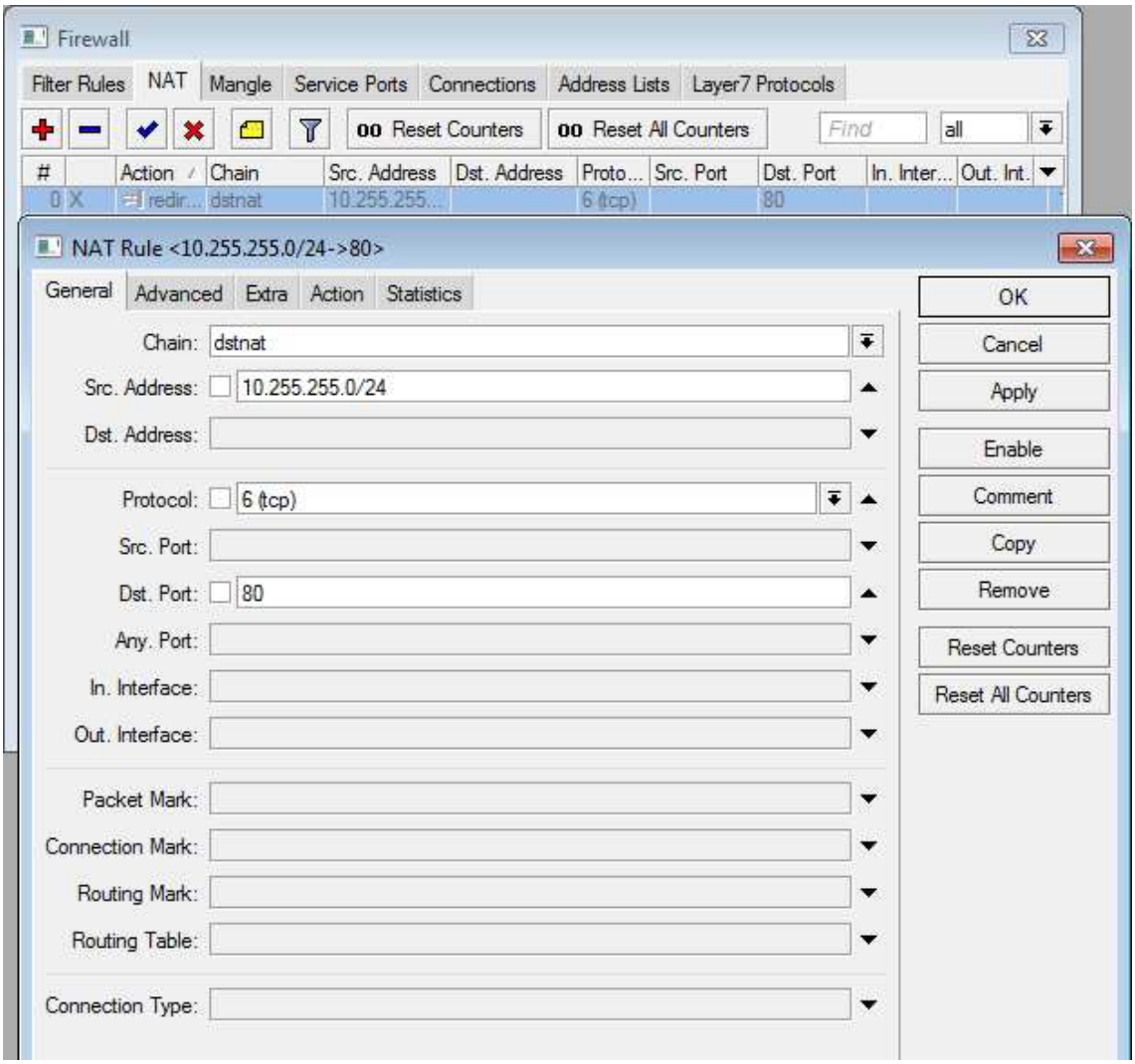


Figura 2.34 Configuración Proxy puertos

A continuación en la viñeta de *Action* se redirige el tráfico al puerto 8080, de la siguiente manera:

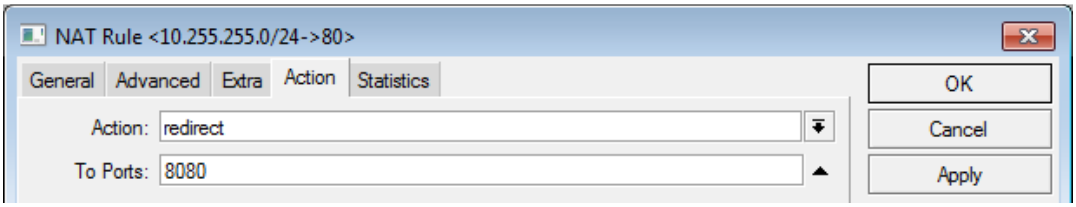


Figura 2.35 Redireccionamiento puerto 8080

Hasta ahora se ha realizado la configuración de proxy transparente y la redirección del puerto destino 80 al 8080, a continuación se crearán las reglas para denegar servicios, o especificar páginas autorizadas. Dentro del menú

principal se ingresa a IP/ Web Proxy, se da clic en signo (+), y se configura los siguientes campos:

- *Src. Address*: Se deja vacío si no existe otra red configurada en la misma interface interna, si existe dos o más redes internas se debe especificar cuál es la red que requiere filtrar
- *Dst. Address*: Este campo se utiliza para restringir una dirección IP o un grupo de direcciones específicas mediante la notación CIDR por ejemplo 207.46.0.0/16
- *Dst. Port*: Este campo restringe un puerto destino, por ejemplo; si se desea restringir el uso del Messenger uno de los pasos es bloquear el puerto 1863
- *Local Port*: Especifica el puerto a través del cual el paquete fue recibido, este valor deberá marcar uno de los puertos que el proxy utiliza
- *Dst. Host*: Este campo permite restringir un host en Internet, es decir bloquea el acceso a una determinada página como puede ser www.facebook.com, para esto no es necesario ingresar la dirección Ip de dicho host sino que se puede ingresar directamente la dirección URL
- *Path*: Este campo se utiliza en el caso que se requiera denegar ciertas aplicaciones vinculadas con páginas web como puede ser *.mp3, *.mp4, *.mpg, *.avi, *.wmv, etc.
- *Method*: Indica el modo de respuesta desde el Internet hacia el servidor Proxy.
- *Action*: Este campo indica que acción realizará el servidor proxy con el paquete solicitado y puede ser restringir *(deny)*, o permitir *(allow)*
- *Redirect To*: Este campo permite redireccionar el paquete hacia un host específico, como puede ser una página que indique que tal solicitud está restringida por el administrador de la red

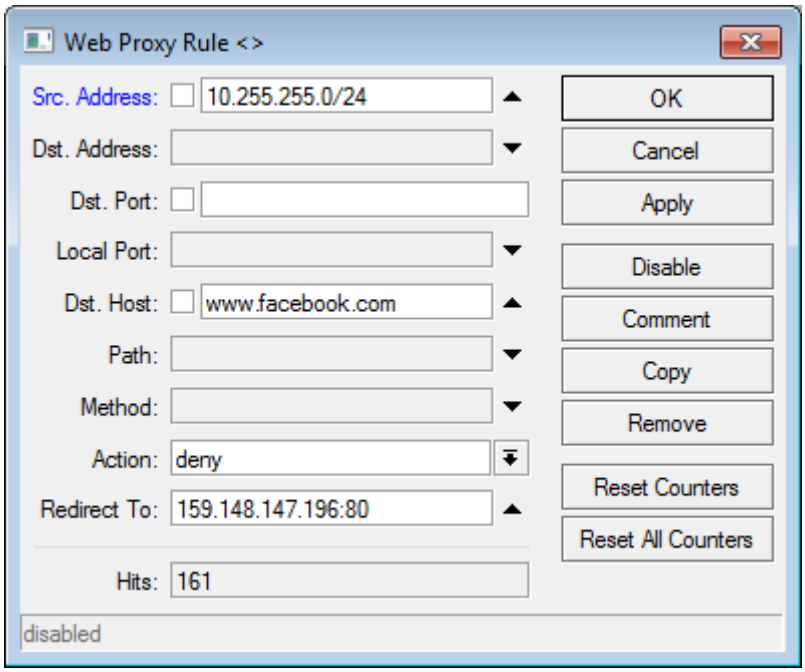


Figura 2.36 Regla WEB PROXY

En la ventana anterior la regla indicaría que el tráfico que provenga de la red 10.255.255.0/24 (red interna), y este dirigida al host de destino www.facebook.com sea denegada y redireccionada a la página 159.148.147.196:80 que es la página www.mikortik.com

Se debe tener en cuenta que las reglas que se agrega en el proxy serán ejecutadas de acuerdo al orden de ingreso de la regla, esto se puede modificar arrastrando de forma vertical las reglas que se necesita dar más o menos prioridad.

Por ejemplo si se desea bloquear al acceso de la red interna 10.255.255.0/24 a la página de descargas www.rapidshare.com se realizará lo siguiente:

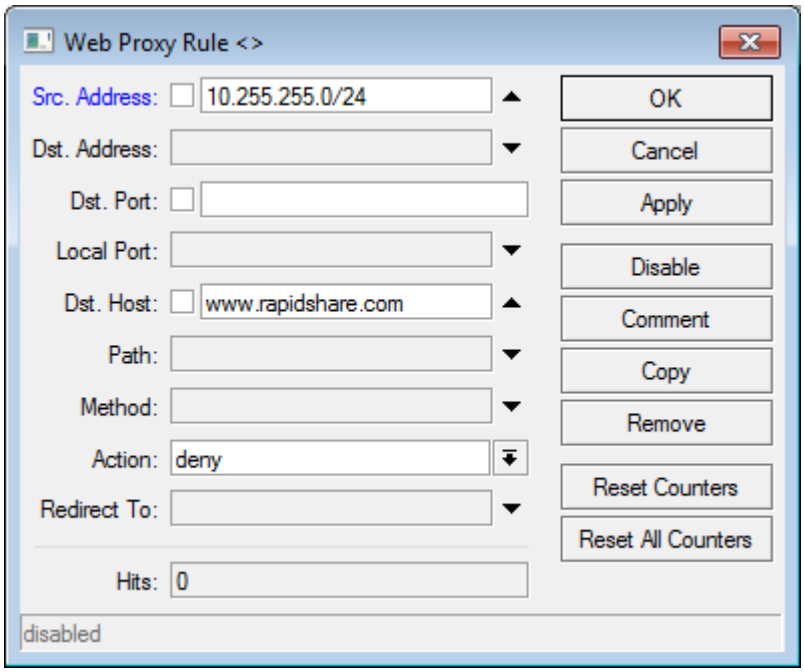


Figura 2.37 Denegación PROXY

Para denegar aplicaciones vinculadas con páginas web, como puede ser: radio on line, mp3, videos, etc. Se utiliza el campo *path*, por ejemplo, si se desea bloquear videos de la página www.youtube.com, los videos de la página youtube tienen una extensión propia llamada videoplayback, por lo que en el campo Path se colocará esta extensión de esta manera, Path: *.*videoplaback** y en el campo *Action* se denegará la petición, con esto se elimina los videos de los servidores de youtube así como los vínculos de otras páginas hacia estos servidores, la configuración se mostrará así:

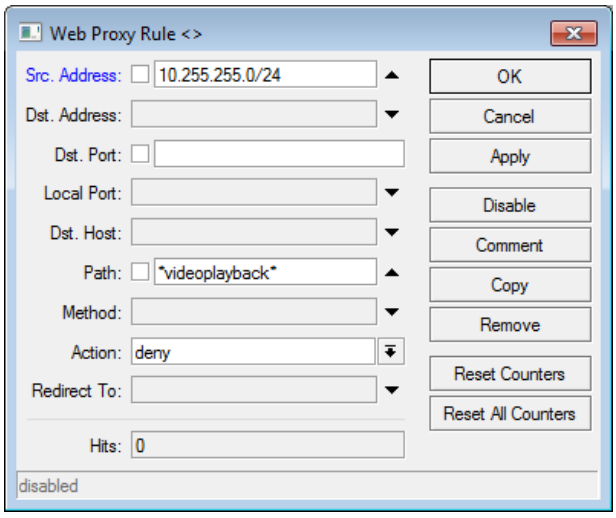


Figura 2.38 Denegación de videos con PROXY

2.5.2 DENEGACIÓN DE SERVICIOS MEDIANTE LAYER 7

Layer 7 o L7, es un paquete de software diseñado para Linux Netfilter que es usado como un subsistema para categorizar paquetes IP con el fin de identificar lo mejor posible programas *peer to peer* (P2P), esto se realiza mediante la identificación de paquetes en la capa de datos mediante el uso de expresiones regulares llamadas también patrones. Las ventajas de usar filtrado de paquetes mediante filtros L7 son que ayudan a optimizar el ancho de banda, y permite un mejor uso de QoS, además de crear filtros para aplicaciones no deseadas como puede ser el P2P.

Para configurar el filtrado de paquetes mediante L7 en RouterOS se ingresa en IP/Firewall, se busca la viñeta *Layer7 Protocols*, se ingresa una nueva regla con el signo (+),

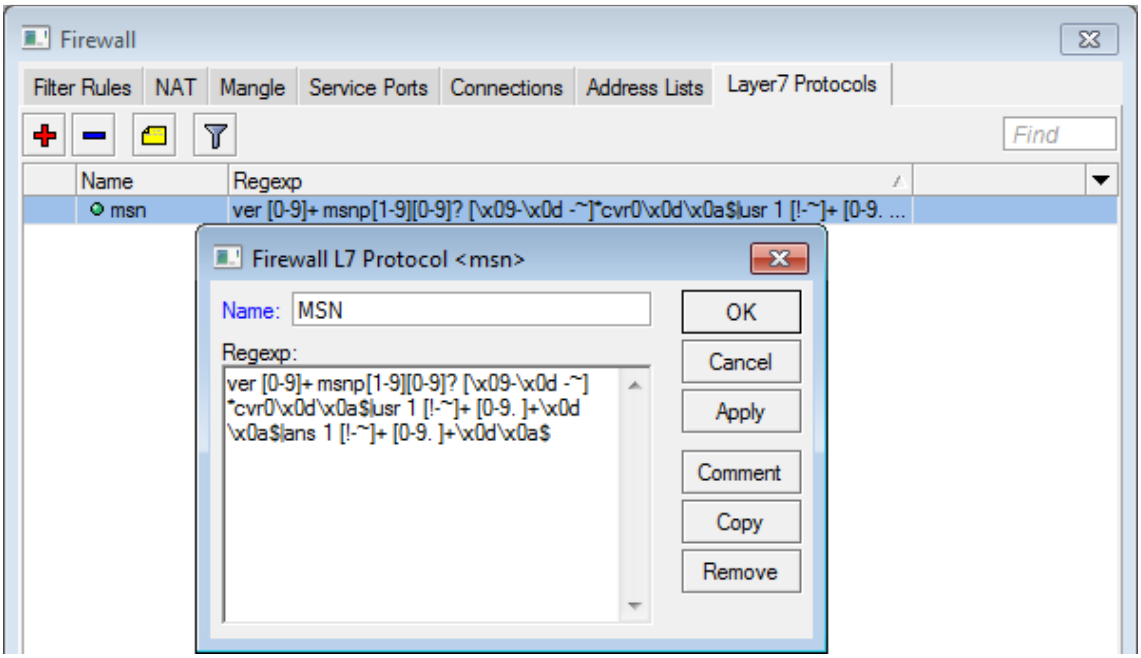


Figura 2.39 Configuración Layer 7

En el campo de *Name* se ingresa el nombre de filtro, y en el campo Regexp se ingresa la expresión regular. Se puede encontrar patrones con filtros para protocolo L7 en la página http://l7-filter.sourceforge.net/protocols.

Normalmente si se desea crear un filtro en un Firewall se identifica el tráfico que se desea filtrar mediante puerto, protocolo, o direcciones IP, etc. Sin embargo algunas aplicaciones usan puertos comunes que son usados por

otro tipo de aplicaciones. Por ejemplo algunas aplicaciones de mensajería instantánea como el *Messenger MSN* utiliza el puerto TCP 80 el cual es usado también para tráfico HTTP, con lo que es virtualmente imposible bloquear esta aplicación sin afectar la navegación.

Para definir el filtro L7 se busca el patrón relacionado con MSN el cual es: ver [0-9]+ msnp[1-9][0-9]? [\x09-\x0d -~]*cvr0\x0d\x0a$|usr 1 [!-~]+ [0-9.]+\x0d\x0a$|ans 1 [!-~]+ [0-9.]+\x0d\x0a$. Este valor es desarrollado por desarrolladores de sistema Linux, para la creación de filtros L7[16]

Una vez creada la regla en el protocolo L7 se crea una regla en el Firewall que indique que todo el tráfico que marcado con L7 MSN será rechazada mediante DROP, para esto se ingresa en IP/ Firewall, en la viñeta *General* se ingresa los siguientes datos:

- *Chain: Forward*. Cadena que reenvía el tráfico hacia el filtro L7
- *Src. Address*: 10.255.255.0/24. Red interna que se desea filtrar
- *Protocol: 6 tcp*. Tipo de protocolo que se quiere filtrar

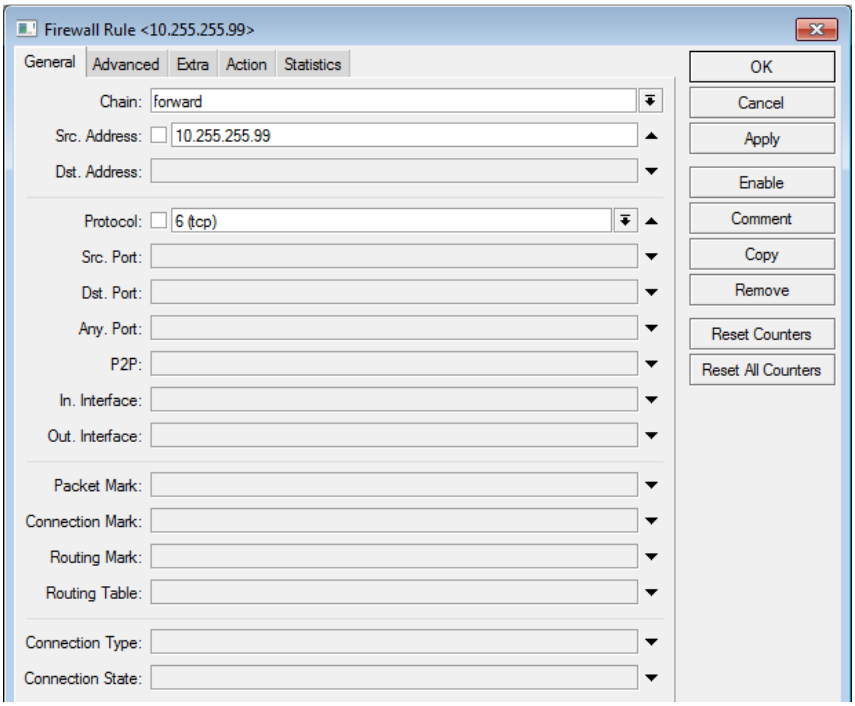


Figura 2.40 Bloqueo MSN

En la viñeta de *Advanced* dentro de la regla de Firewall que se está creando se habilita el protocolo *Layer7 Protocol* de la siguiente manera:

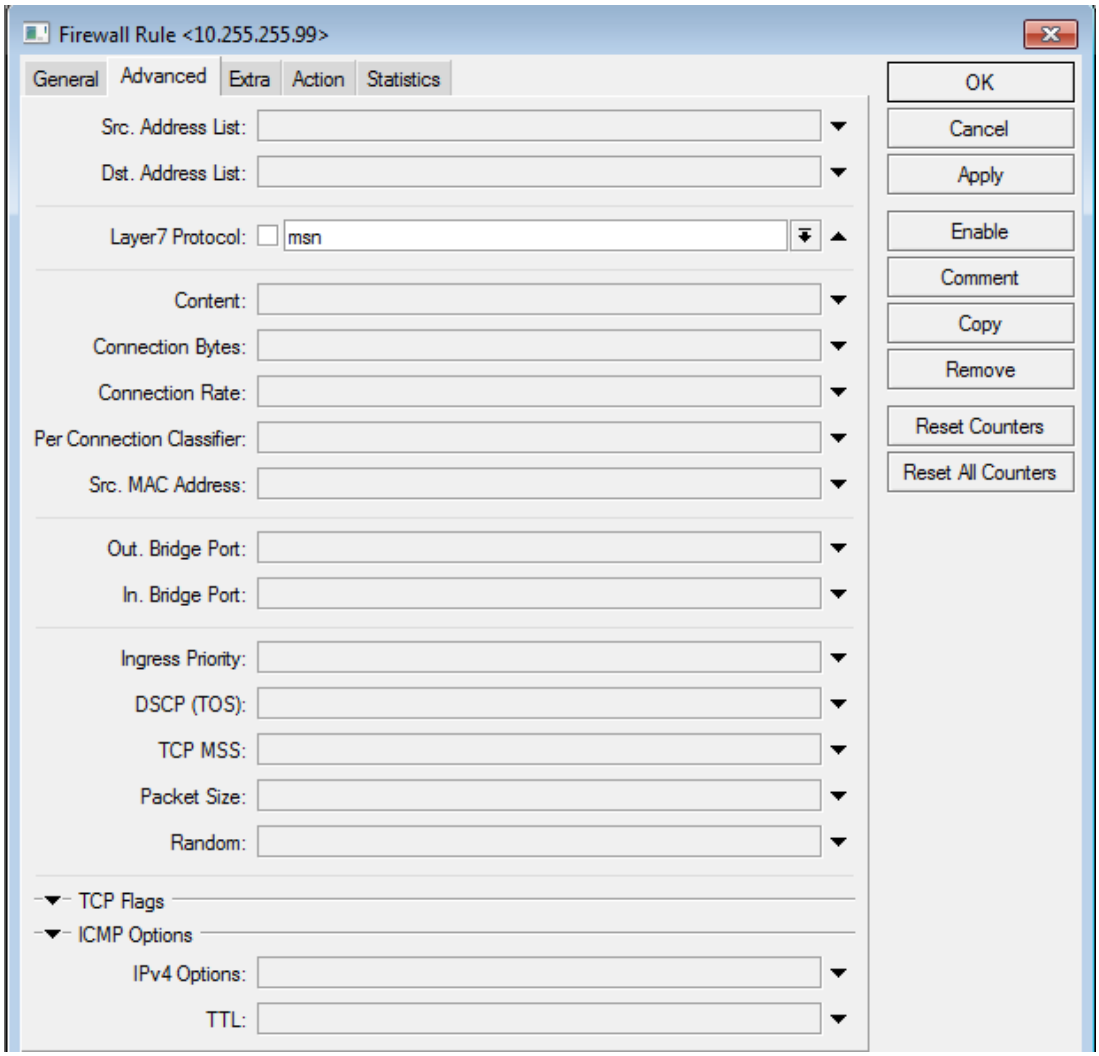


Figura 2.41 Firewall MSN

Como último paso se indica que acción realizará la regla, para esto se ingresa en la viñeta *Action* y se marca *drop*.

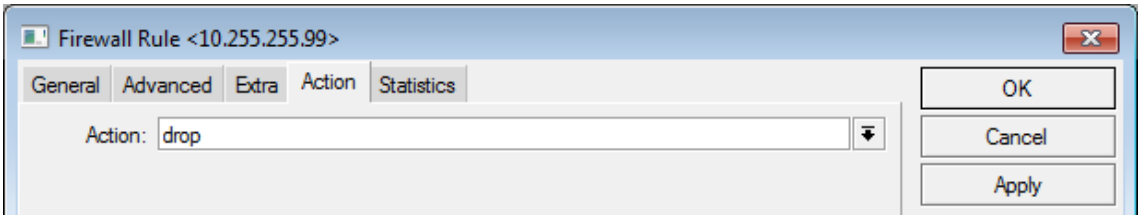


Figura 2.42 Drop Messenger MSN

De esta manera se bloquea el tráfico MSN desde la red interna 10.255.255.0/24 sin necesidad de generar marcado de paquetes, los cuales pueden requerir de muchas reglas y no siempre son efectivos ya que se puede realizar un cambio de puertos en la aplicación que administra en MSN.

2.6 TÚNELES.

Por la complejidad del tema y considerando que el análisis de los distintos protocolos destinados al tráfico de datos mediante túneles son muy amplios y requiere mucho tiempo, en este estudio se va a describir los más utilizados en las diversas aplicaciones.

2.6.1 VPN IPSEC (INTERNET PROTOCOL SECURITY)

Es un protocolo completo de estándar abierto es decir puede comunicarse entre varios fabricantes y es utilizado para asegurar las comunicaciones sobre IP autenticando y encriptado cada paquete IP de una sesión. IPsec utiliza protocolos para mutua autenticación entre hosts, mediante el uso de criptografía

Se va a crear una conexión IPsec que permita unir una red privada con direcciones 10.255.255.0/24 hacia una segunda red privada remota con dirección 10.10.10.0/24, mediante equipos con RouterOS los cuales tienen en su cara WAN las direcciones IP públicas, 200.105.112.194, y 200.105.119.194

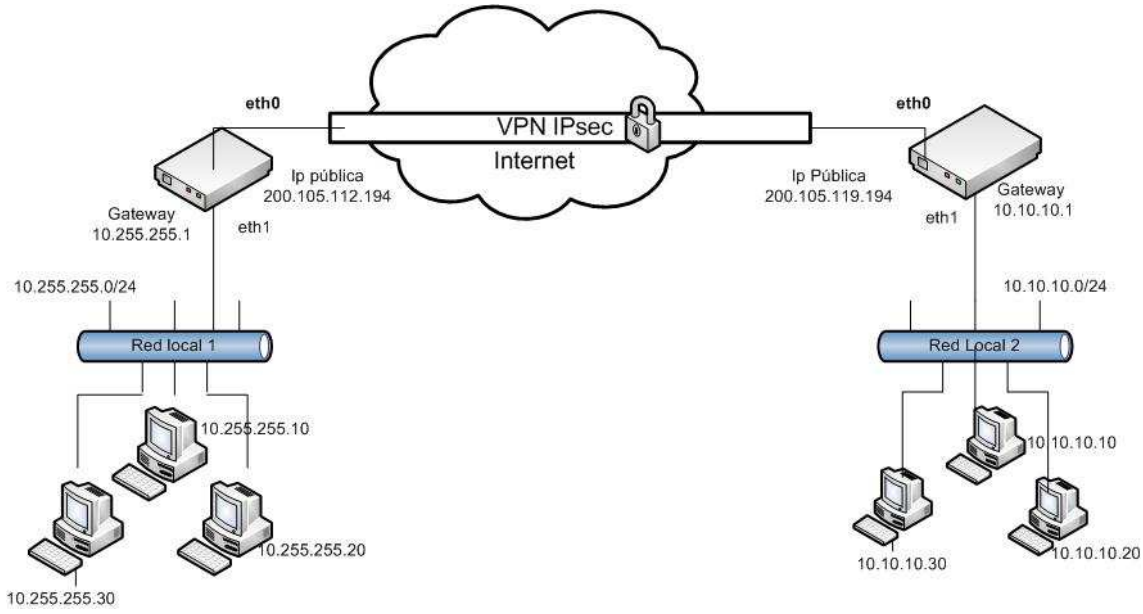


Figura 2.43 Esquema VPN IPsec

Se Ingresa en el menú principal IP/IPsec, y dentro de la viñeta *Policies* se da clic en el signo (+) en la ventana general permite marcar las redes que se necesita encriptar tanto la red fuente o red privada local y la red destino o red privada remota, estos campos se llena con la siguiente información:

- *Src. Address*: *10.255.255.0/24* Red Privada Local
- *Scr Port:* Puerto de origen que utilizará IPsec en el ruteador local
- *Dst. Address*: 10.10.10.0/24 Red Privada Local
- *Dst. Port*: Puerto de destino que utilizará IPsec en el ruteador remoto
- *Protocol*: all. Indica los tipos de protocolos que comunicará, es decir que por el túnel se puede enviar información específica, como puede ser TCP, UDP, ICMP (ping), etc.

En la ventana *action* se configura de la siguiente manera:

- *Action: encrypt*. Permite encriptar los datos que van a ser transmitidos, o descartar los datos a ser enviados.
- *Level*: Indica si se desea que los datos sean encriptados o enviados sin seguridad de encripción.
- *IPsec Protocols*: esp. Indica el tipo de encripción que se va a utilizar en los datos
- *Tunnel*: habilitado.
- *SA. Src. Address*: 200.105.112.194. Indica en Gateway o puerta de enlace del ruteador local
- *SA. Dst. Address*: 200.105.119.194. Indica en Gateway o puerta de enlace del ruteador remoto
- *Proposal: Default*. Este campo indica la propuesta de algoritmos que utilizarán los ruteadores el instante de establecer una comunicación par con par, este campo refleja el tipo de propuesta definida previamente en la viñeta *Proposals* de la configuración general del IPsec
- *Manual SA*: none.
- *Priority*: 0. Se puede clasificar entre diversos tipos de tuneles y asignar una prioridad de uso de canal, esto en la caso de necesitar priorizar tráfico.

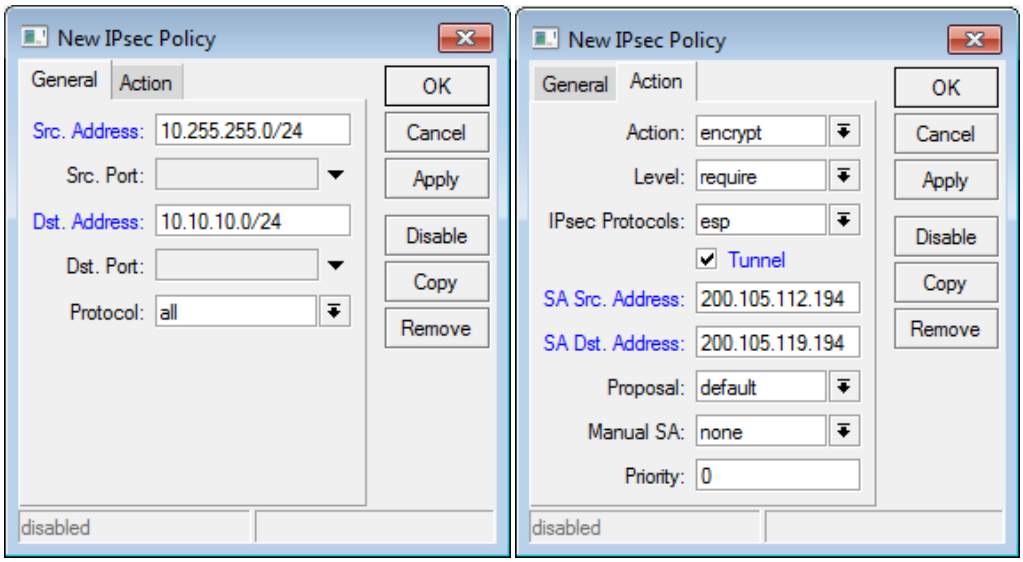


Figura 2.44 Políticas IPsec

Ahora es necesario la configuración de los pares *(IPsec peers),* con lo cual se realizará la negociación para establecer la comunicación entre los ruteadores, los campos contendrán la siguiente información.

- *Address*: 200.105.112.194. Dirección IP del router remoto con el cual se va a negociar la comunicación.
- *Port: 500*. Este es el puerto por defecto utilizado por IPsec para negociar las llaves de autenticación ISAKMP.
- *Auth. Method*: pre-shared key. Este campo indica el método de autenticación que se utilizará para la negociación, y puede ser *pre-shared key, ó rsa signature.*
- *Secret*: nevado. En este campo se configura las clave secreta para la autenticación
- *Exchange mode*: main. Este campo indica el modo de intercambio de la autenticación IKE *(Internet Key Exchange).*
- *NAT Traversal*. Habilitado. Este campo permite atravesar con el túnel el NAT que puede tener los ruteadores.
- *Proporsal Check: main*. Indica la forma del chequeo de la propuesta y pueden ser: *claim* (bajo demanda), *obey* (obediente), *exact* (exacto), *strict* (estricto)
- *Hash Algorithm*: sha. Indica el tipo de algoritmo Hash que se va a usar y puede ser sha, ó md5

- *Encryption Algorithm:* 3des Este campo indica el tipo de algoritmo de encripción que se utilizará, y puede ser: 3des, aes-128, aes-196, aes-256, des

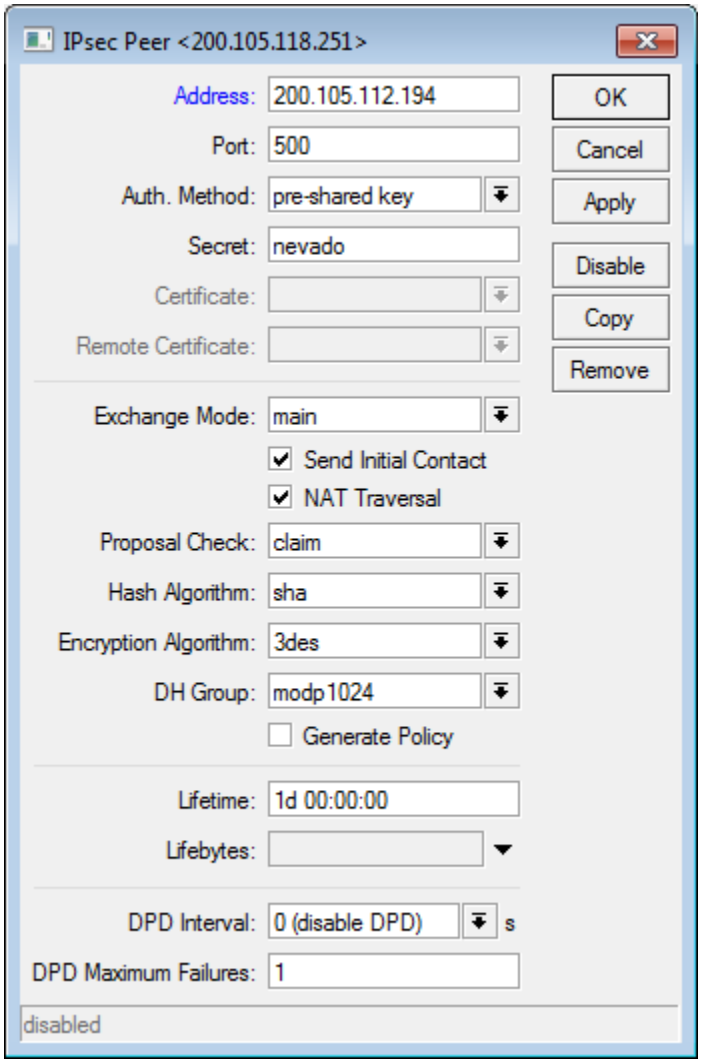


Figura 2.45 Configuración IPsec peers

Ahora es necesario configurar las propuestas IPsec, aquí se configurará el tipo de algoritmos de autenticación y algoritmos de encripción.

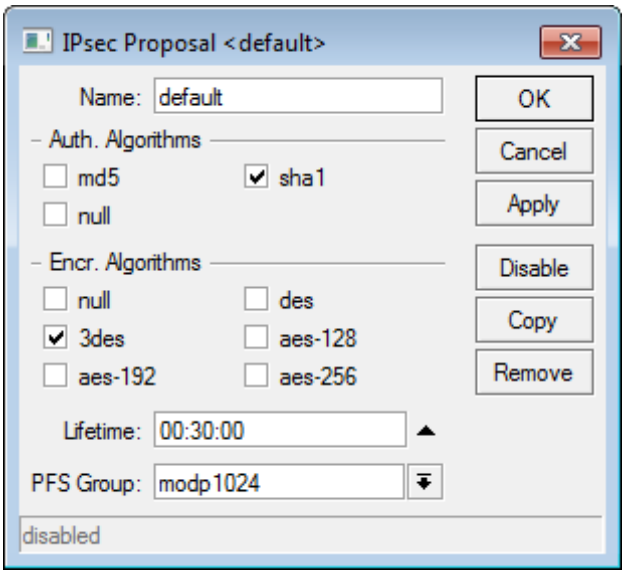


Figura 2.46 Propuesta IPsec

Para confirmar que el IPsec ha sido establecido, se puede ingresar en la ventana *IPsec remote peer* en la cual indicará que la conexión ha sido establecida.

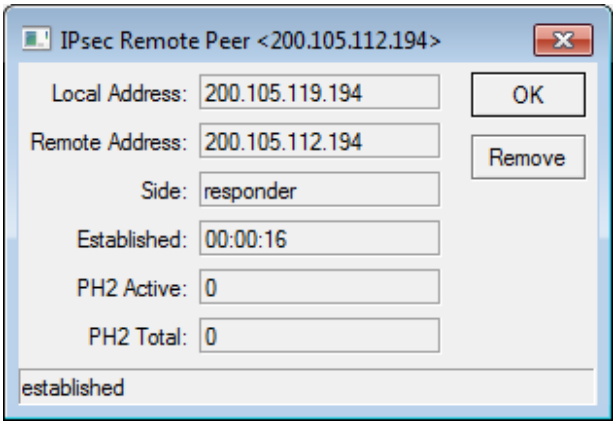


Figura 2.47 IPsec peer remoto

Como último paso se tendrá que añadir una regla en el firewall que indique que acepta las redes internas remotas en el caso que exista un NAT en los ruteadores, para esto se va a IP/ Firewall NAT, y se añade una regla de la siguiente manera:

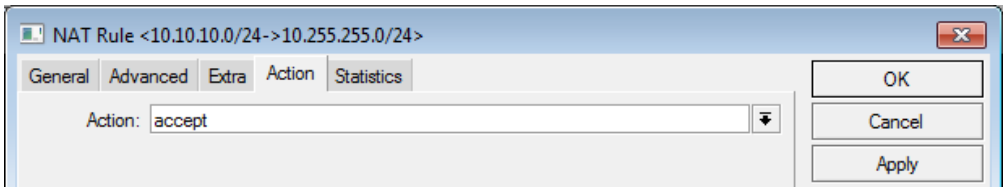


Figura 2.48 Action Firewall NAT IPsec

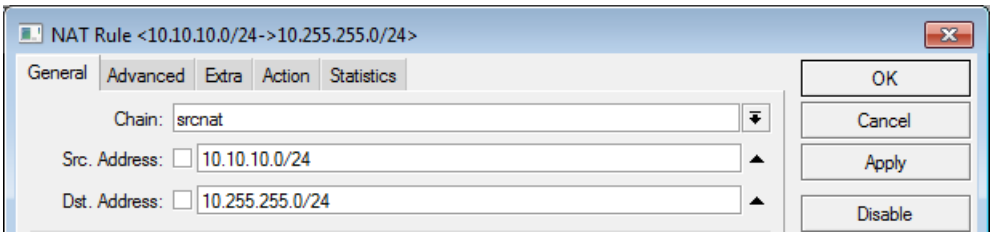


Figura 2.49 Aceptación redes NAT IPsec

2.6.2 TUNELES EOIP

EoIP, *Ethernet over IP*, es un tipo de túnel de propiedad de RouterOS MikroTik, el cual crea un túnel *Layer 2* entre 2 ruteadores con RouterOS usando el protocolo 47 usado para túneles tipo GRE, el cual crea una conexión no encriptada la cual puede correr sobre otros túneles. Par crear un túnel EoIP en los dos ruteadores se ingresa a Interface, se da clic sobre el signo (+), y se busca *EoIP Tunnel*, va a abrir la pantalla en la que se configurará el nombre del túnel, el valor MTU, la dirección IP del equipo remoto y el *Tunnel ID*, este último campo identifica el número del túnel que se va a crear, este valor debe ser el mismo en los dos equipos a configurar

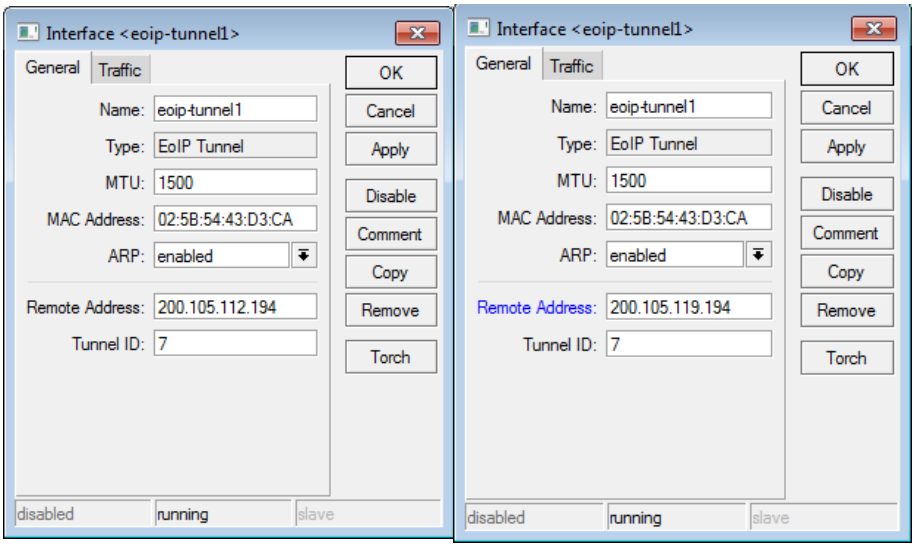


Figura 2.50 Configuración túnel IPSec

De esta manera se crea un túnel que no tendrá muchas seguridades, pero sobre el cual se puede crear un túnel con encripción o rutas estáticas las cuales se transportarán dentro del túnel, este túnel, tiene la posibilidad de comportarse como una interface adicional, y existe posibilidad de conectar redes remotas en la cual se pueda aplicar controles de ancho de banda, reglas de firewall o marcado de paquetes (mangle). Como ejemplo se va a unir dos redes remotas las cuales serán ruteadas de forma estática dentro del túnel EoIP, una red 10.255.255.0/24 y otra red 10.10.10.0/24.

Una vez creado el túnel EoIP, se agrega una IP de una subred /30 con una sola dirección IP habilitada la cual estará incluida dentro de la Interface EoIP por ejemplo en el ruteador 1 se incluirá la dirección 10.27.27.1/30, y en el ruteador 2 con dirección IP 10.27.27.2/30, las dos direcciones se agregarán a la nueva interface llamada *eoip-tunnel1*.

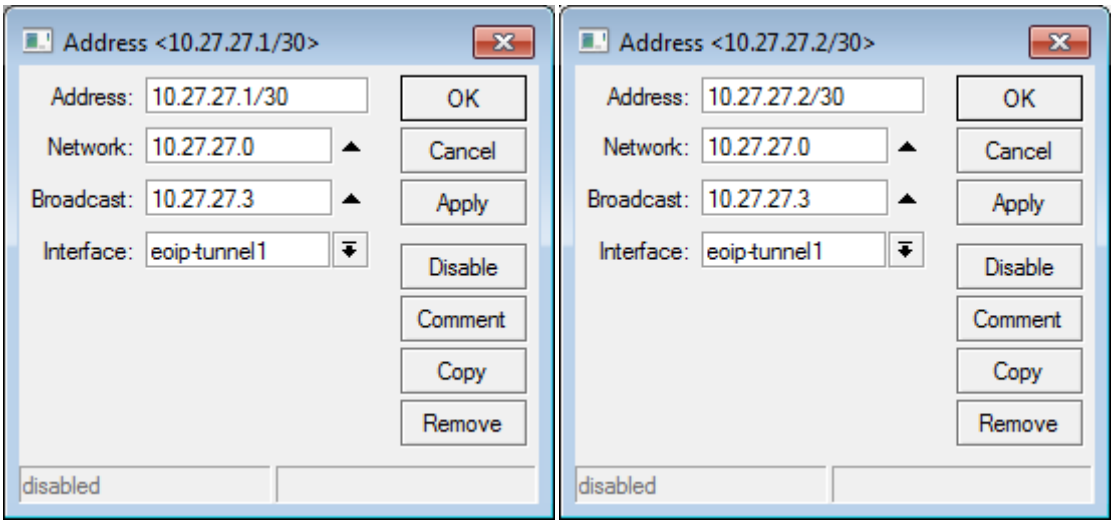


Figura 2.51 Direcciones IP EoIP

Ahora se incluirá rutas estáticas entre las redes internas remotas y se tendrá como Gateway las interfaces EoIP 10.27.27.0/30 de la siguiente manera:

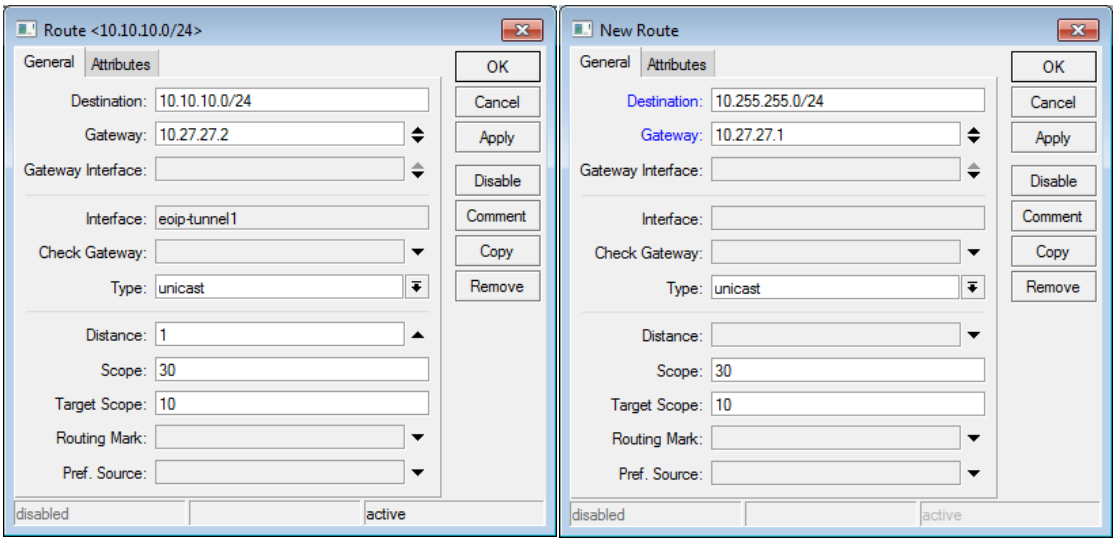


Figura 2.52 Rutas EoIP

Para probar la comunicación entre las dos redes, se utilizará el protocolo ICMP (ping), desde cada router hacia cada puerta de enlace remota de la red interna, esta herramienta está incluida en el RouterOS dentro de Tools /Ping

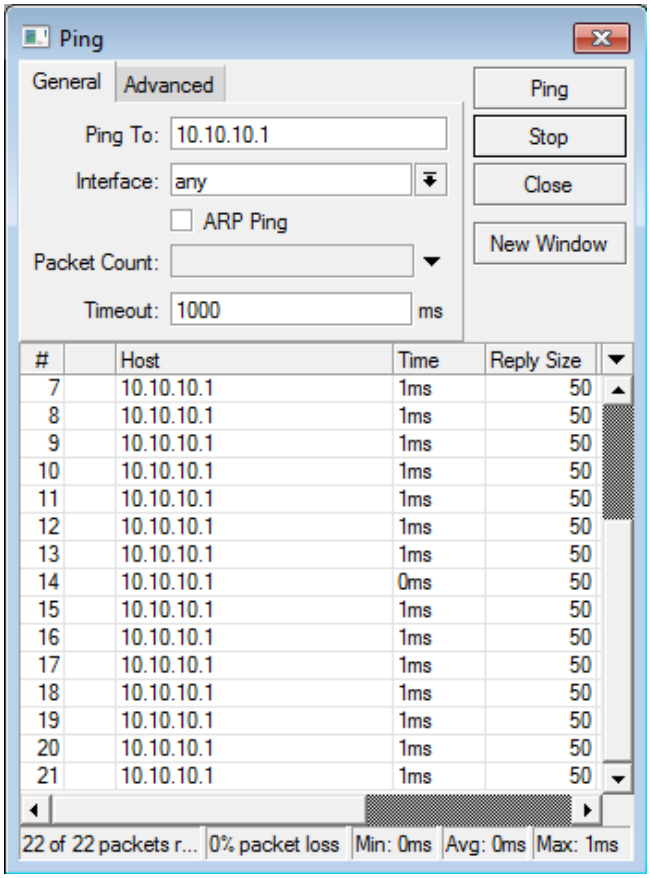


Figura 2.53 Pruebas ICMP EoIP

2.7 CONTROL DE ANCHO DE BANDA

RouterOS para el control de ancho de banda y QoS o calidad de servicio *(Quality of Service)*, utiliza HTB *(Hierarchical Token Bucket)*, este sistema se basa en un algoritmo el cual controla la cantidad de datos que es inyectado dentro de una red, permitiendo una ráfaga de datos en un tiempo determinado, además de crear una estructura jerárquica que determina relaciones de colas de datos entre padres e hijos, para una mejor distribución y priorización de los datos.

2.7.1 SISTEMA DE COLAS SIMPLES (SIMPLE QUEUES)

Basado en el sistema HTB, RouterOS ha diseñado un fácil sistema de control de datos mediante el uso de una cola simple para una o múltiples direcciones IP y subredes.

Para crear un cola que permita controlar un IP o una subred, en el menú principal se busca *Queues,* dentro de *Queues* se busca la viñeta *Simple Queues* y en el signo (+) se agrega una cola.

El método es bastante simple, se tiene el nombre de la cola, se selecciona la red que se necesita controlar este es el campo *Target Address*, se selecciona si el control requerido es en el *Upload* o tráfico de salida de la red interna al internet o *Download* o tráfico que ingresa del Internet a la red interna, esto mediante los campos *Target Upload* y *Target Download,* y finalmente se ingresa el valor máximo de ancho de banda que estará designado para esta red tanto para *upload* como para *download*, de la siguiente manera:

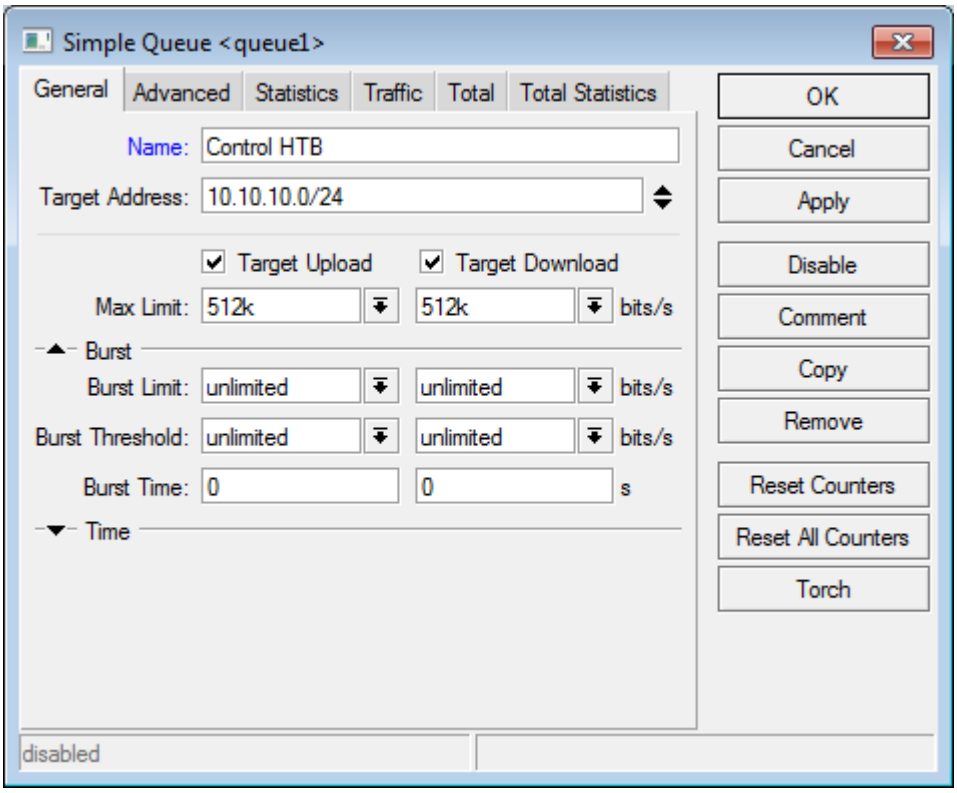


Figura 2.54 Configuración de control de ancho de banda

Este ejemplo permitirá controlar el tráfico generado en la red Interna 10.10.10.0/24 a un máximo de 512Kbps tanto en *upload* como en *download*.

2.7.2 BURST O RÁFAGAS DE DATOS

La mayor parte del tráfico de Internet se realiza en una vía, es decir *download*; un usuario solicita una página web, una vez cargada la página, estadísticamente el usuario utiliza una gran cantidad de tiempo en la lectura de la página, en estos momentos el tráfico de datos desde internet al usuario es mínimo.

El *burst* o ráfagas de datos, son utilizados en situaciones donde se requiere recibir una gran cantidad de tráfico por breves períodos de tiempo.

Por ejemplo: un usuario tiene asignado un ancho de banda de 1 Megabit, pero requiere una descarga inicial de 2 Megabits para acceso a páginas http durante un tiempo de 30 segundos, esto se configuraría de la siguiente forma:

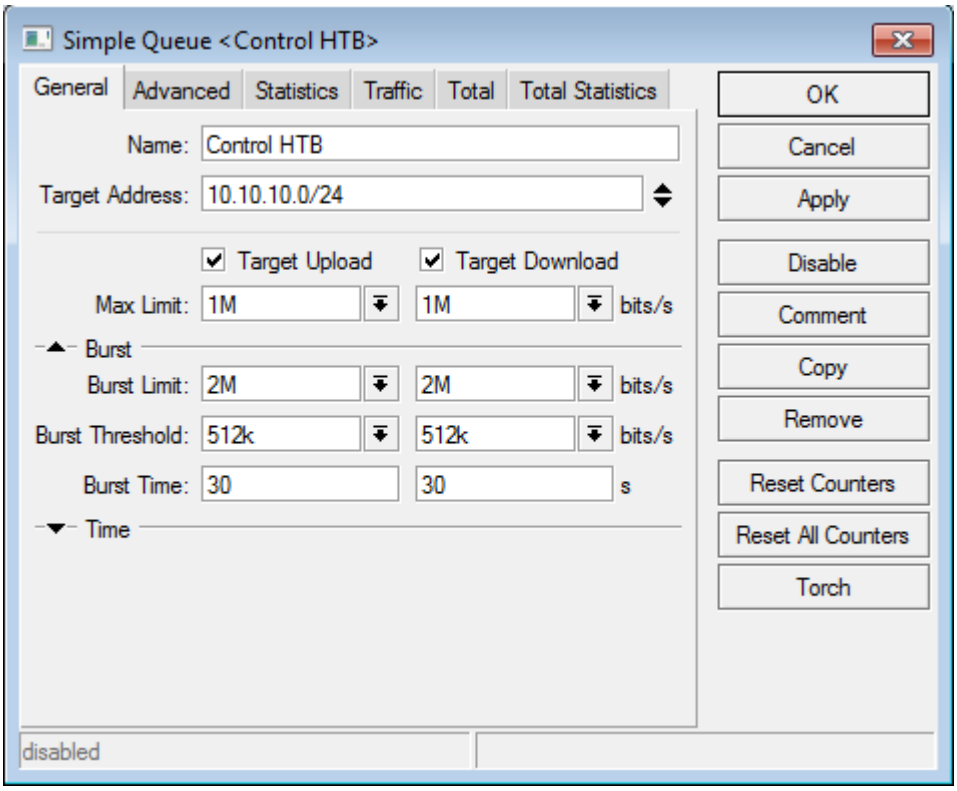


Figura 2.55 Configuración de ráfagas en el control de ancho de banda

2.7.3 COLAS PARA DISTRIBUCIÓN DE TRÁFICO UNIFORME.

La demanda de Internet de un usuario es muy dinámico, y con sistemas convencionales de control de ancho de banda basados en colas FIFO *(first in-first out)* o RED *(random early detection)*, no permiten la optimización del ancho de banda de forma dinámica, es decir; si el acceso a Internet de una empresa es de 1 Mbps controlado por colas tipo FIFO, y existe un usuario conectado a Internet, este usuario tiene la posibilidad de usar este Megabit, si se conecta un segundo usuario es posible que la distribución no se de de forma uniforme.

Para optimizar el ancho de banda de forma uniforme y dinámicamente se utilizan colas basadas en PCQ *(Per-Connection Queuing)*, estas permiten subdividir el ancho de banda general o total de forma equitativa y en función de la demanda y el número de usuarios.

Por ejemplo; si en la red 10.10.10.0/24 se tiene un ancho de banda general de 2 Mbps, para un número de cuatro usuarios, es posible configurar un control que permita de forma dinámica utilizar un máximo de 2 Mbps, si existe un solo usuario conectado a la red, o un mínimo real de 512 Kbps si se

encuentran conectados los cuatro usuarios de forma simultánea. Para esto primero se va a *Queue* se busca *Queue Type*, y se agrega dos nuevos tipos de cola, una para el *upload* que se nombrará “subida”, y otra para el *download* que se denominará “descarga”, esto mediante el signo (+), en *Type Name* se ingresará el nombre con el que se identificará esta nueva cola, en el campo Kind se selecciona pcq, los campos *Rates, Limit*, *Total limit*, se escoge los valores que vienen por defecto, y en el campo clasificador se escoge *Src. Address* para el *upload* y *Dst. Address* para el *download*.

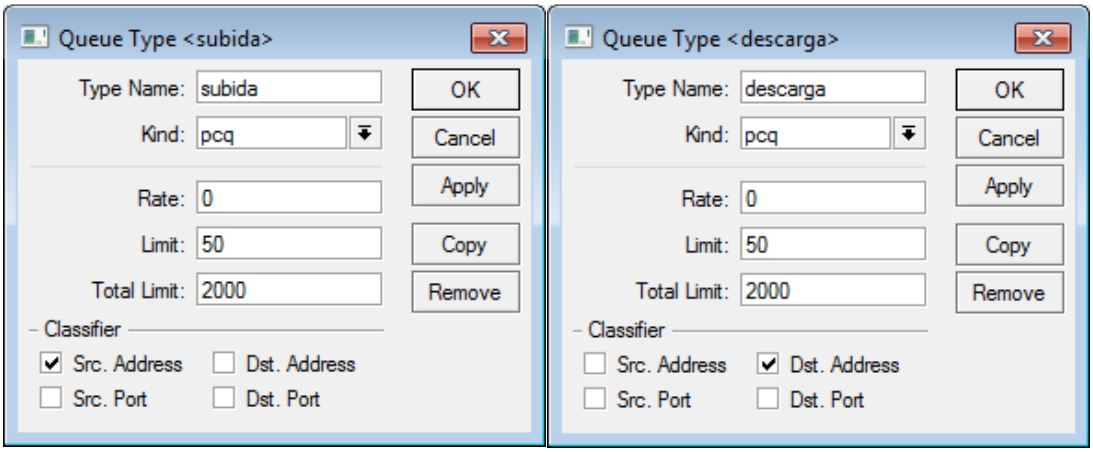


Figura 2.56 Control de ancho de banda upload y download

A continuación, se crea una cola simple, en la viñeta general se especificará la dirección de red objetivo o *target address*, y el límite máximo de ancho de banda de la red, y en la viñeta *Advanced* se especificará el tipo de cola que se usará, es decir las colas que se acaba de crear “subida” y “descarga”.

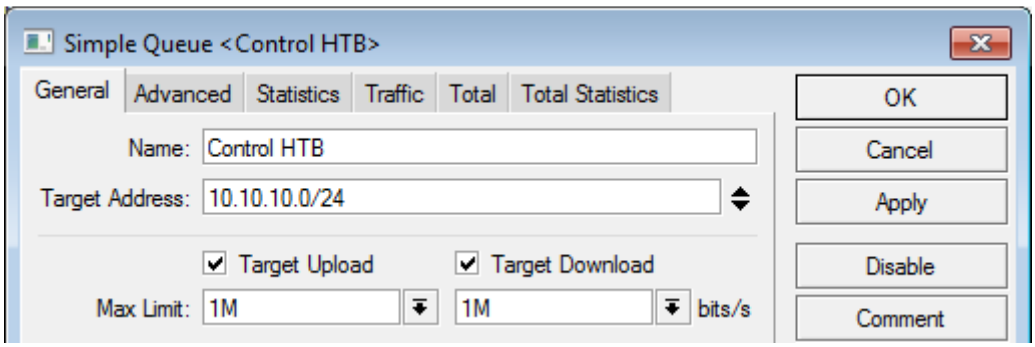


Figura 2.57 Cola para control de ancho de banda

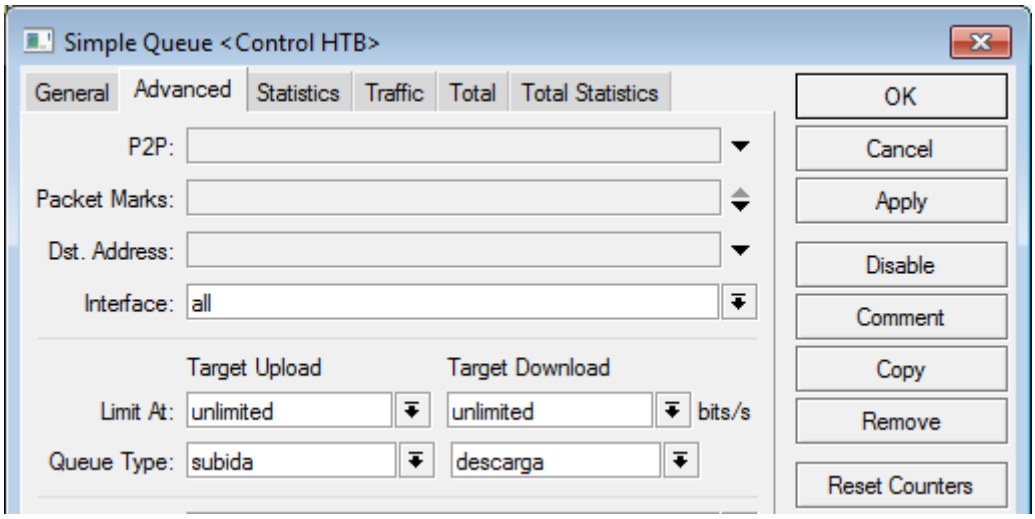


Figura 2.58 Control de ancho de banda por cola

2.8 MANEJO DE ARCHIVOS DE RESPALDO DEL SISTEMA (BACKUP) Y DE SCRIPT

2.8.1 RESPALDO DEL SISTEMA

RouterOS permite guardar las configuraciones o cambios realizados en su configuración, para guardar un respaldo, se ingresa a FILE, y se hace clic sobre el botón *Backup*, esto crea un archivo MikroTik-xxxxxxxx-0000.backup, mediante el botón copiar, o se puede arrastrar este archivo directamente a la carpeta del equipo que guardará la configuración.

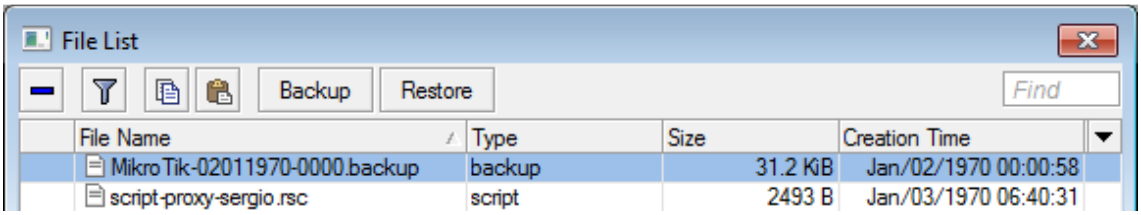


Figura 2.59 Respaldo de configuraciones

Para restaurar una configuración previamente guardada se copia el archivo guardado, y dentro del menú Files se da un clic en el botón pegar, una vez que se comprueba que el archivo fue copiado dentro del RouterOS, se da clic sobre Restore, inmediatamente indicará que es para que los cambios surtan efecto es necesario reiniciar el equipo, a lo que se responderá que si dando clic sobre el botón *yes.*

Figura 2.60 Confirmación de restauración de archivos

2.8.2 RESPALDO DE ARCHIVOS SCRIPT

En el caso de haber creado un programa ejecutable en RouterOS, o requerir guardar una configuración especial, se lo realiza mediante línea de comandos, dentro de RouterOS se ingresa mediante el menú principal opción New Terminal. Al abrir la pantalla de línea de comandos se ingresa a la raíz del menú principal de RouterOS, con ayuda de la tecla TAB se desplegará las opciones del menú principal. En la línea de comandos se indica que parte de la configuración se desea salvar; por ejemplo fue creado un servidor proxy, en el cual se incluyen restricciones de servicios o páginas y se necesita guardar la configuración para ser usada en otro equipo o ser modificada posteriormente para salvar la configuración del proxy se realizará de la siguiente forma:

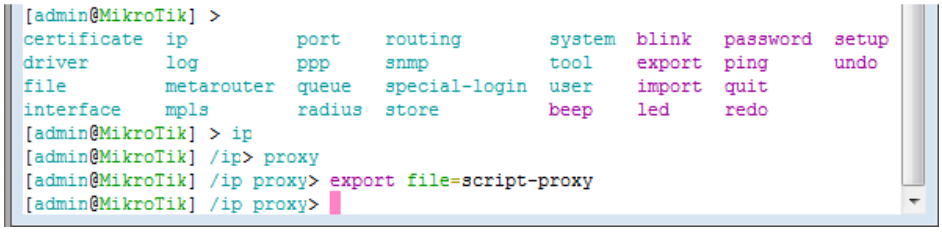


Figura 2.61 Respaldo de archivos por script

El archivo fue salvado mediante el comando export file= el nombre del archivo para este caso será *script-proxy*. Una vez ejecutado el comando se creará un archivo dentro del menú FILE llamado *script-proxy.rsc*. Este archivo al igual que en las configuraciones *backup* puede ser copiado y guardado en otro servidor.

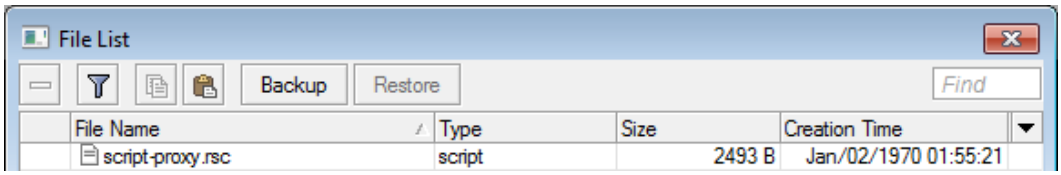


Figura 2.62 Archivo respaldado

2.8.3 REGISTROS

RouterOS tiene un sistema de registros que muestra cambios, errores del sistema, y ayuda a diagnosticar problemas que se generan en la configuración del router. Para acceder al registro, desde el menú principal se hace clic sobre la ficha Log, y abrirá una ventana que indica las fechas de cambios realizados, además indica diagnósticos generales del sistema

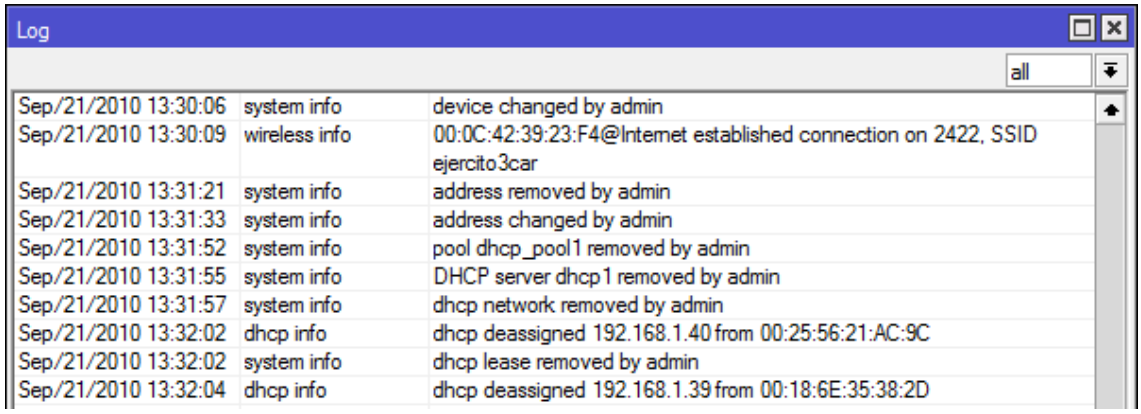


Figura 2.63 Registro del sistema

RouterOS permite llevar un registro de varios tipos de aplicaciones que corren sobre él y pueden ser activados de forma individual en función de su requerimiento. Para activar de forma individual estos registros se ingresa en el menú principal, se busca *System / Logging* se da un clic sobre el símbolo (+) y en *Topics* se busca la aplicación que se necesita llevar registro.

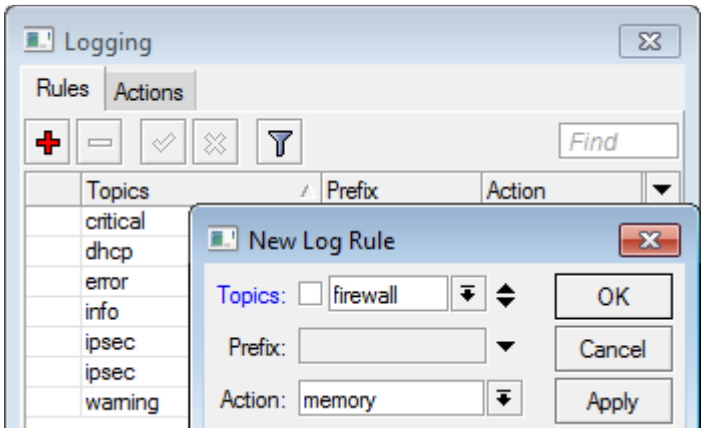


Figura 2.64 Temas del registro

2.8.4 CLIENTE Y SERVIDOR NTP (NETWORK TIME PROTOCOL)

Este es un protocolo utilizado para la sincronización de hora y fecha en servidores y equipos en general.

Para configurar RouterOS como cliente NTP, se ingresa al menú principal, se busca *System,* y se da clic en *NTP client*. A continuación se habilita el servicio agregando un visto en la opción *enable*. En este modo se escoge la opción *unicast*, ya que se recibirá la información desde un servidor a un solo equipo router y en los campos *Primary NTP Server*, y *Secondary NTP Server* se ingresará las direcciones IP de los servidores NTP que se usará. Estos pueden ser servidores locales, o servidores globales por ejemplo server 1: 129.6.15.28, server 2: 129.6.15.29 que es un servidor NTP del *National Institute of Standards and Technology* en EEUU.

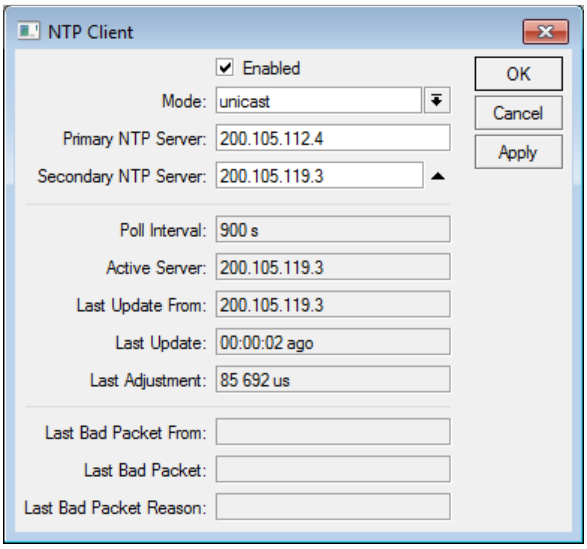


Figura 2.65 Configuración cliente NTP

Para habilitar como servidor NTP simplemente dentro del NTP server del menú System se habilita el modo en el que se desea que trabaje.

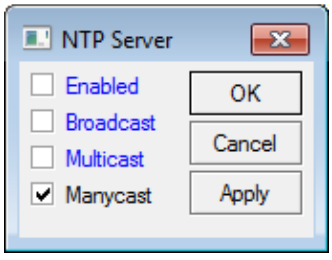


Figura 2.66 Configuración NTP servidor

2.8.5 SERVIDOR SNMP

El protocolo SNMP es utilizado para la administración de dispositivos de red basados en protocolos TCP/IP, mediante un conjunto de elementos básicos como son: Estaciones administradoras o administradores y agentes de red o gestores de red. Las estaciones administradoras son los servidores de administración y gestión de la red, son los equipos que monitorean a los agentes de red o equipos a ser gestionados, elemento pasivos ubicados en los nodos – hosts, routers, módems, multiplexores, etc.

Para habilitar el monitoreo SNMP desde RouterOS MikroTik, dependiendo de la versión se busca SNMP en el menú principal o en su defecto dentro del menú IP, con el símbolo (+) se agrega una nueva comunidad SNMP, para esto se llena los campos *name* con el nombre de la comunidad SNMP, y en *address* la dirección IP a la que se va a servir, por defecto se coloca la red 0.0.0.0/0 esto es para poder ser monitoreado desde cualquier red.

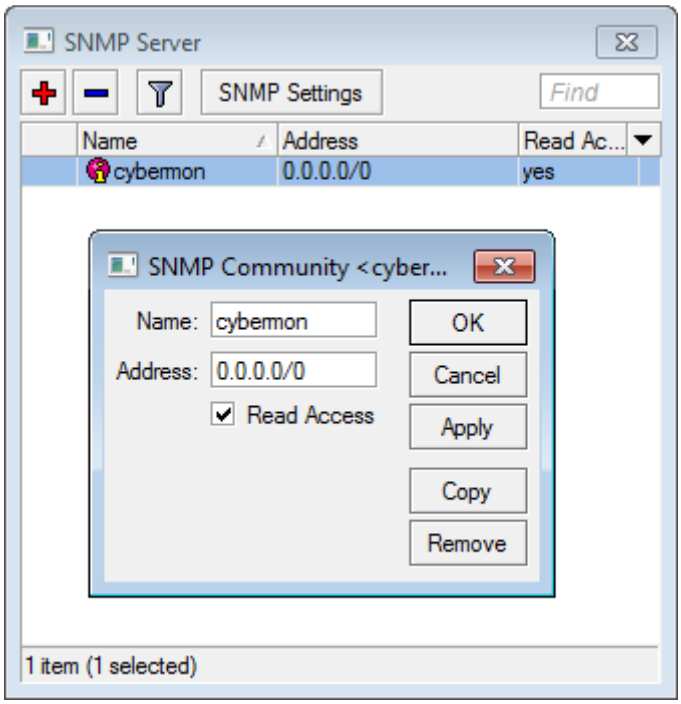


Figura 2.67 Configuración SNMP

Adicionalmente para habilitar el SNMP server es necesario habilitarlo, para esto se da clic en SNMP *settings* y se marca el cuadro *enable*, en el espacio de *contac* se coloca una dirección electrónica para recepción de mensajes, y en *location* se indica el lugar geográfico del equipo.

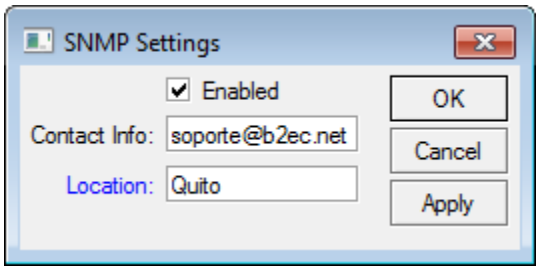


Figura 2.68 Habilitación SNMP

2.9 MIKROTIK ROUTEROS COMO EQUIPO DE FRONTERA

MikroTik presenta varias alternativas de equipamiento *RouterBoard*, los mismos que pueden alcanzar una gran gama de posibilidades, como por ejemplo: administración de ISP's; el RB1100 puede ser una solución para un ISP en el manejo de anchos de banda de clientes, servidor proxy, administración de túneles, manejo BGP, etc. Estos equipos pueden ser comparables en sus aplicaciones y rendimientos a equipos de la marca CISCO serie 3600 usados principalmente para manejo de VPN's y priorización de VoiP, pero con un notable diferencia de precio a favor de los equipos MikroTik.

Mikrotik ofrece también equipos de mediana gama como son el RB 450G, usados para la infraestructura de un ISP, estos equipos pueden prestar servicios como: MPLS, BGP, Bonding, Spannig Tree, VPN's, etc., prestaciones similares a las que puede ofrecer routers CISCO de la serie 1800.

Como equipos routers de frontera MikroTik presenta su equipo RB750, el cual puede funcionar como un CPE en el cliente, con prestaciones y características similares a routers usados como equipos terminales, es decir; túneles PPPOE, VPN's, Proxy, control de ancho de banda, etc.

La configuración de estas aplicaciones es la misma que hemos revisado en este capítulo.

CAPÍTULO 3

COMUNICACIONES INALÁMBRICAS

3.1 INTRODUCCIÓN A LAS COMUNICACIONES INALÁMBRICAS [17]

Las comunicaciones inalámbricas son un eje fundamental en las comunicaciones, permiten cubrir áreas que las comunicaciones cableadas por diversos factores no pueden alcanzar, además de ofrecer grandes ventajas como son:

Movilidad. La posibilidad de movimiento de un sistema, es uno de los grandes beneficios de las comunicaciones inalámbricas, el poder comunicarse desde cualquier lugar que se necesite y en cualquier momento, es uno de los objetivos de los sistemas de comunicación.

Flexibilidad. Las redes inalámbricas permiten con relativa facilidad la reorganización topográfica de una red, esto ayuda a mejorar la gestión y planificación de una red.

Escalabilidad. Una red inalámbrica permite fácilmente incorporar a su red nuevos equipos que permitan expandir o mejorar la cobertura de su red, o trabajar con otro tipo de sistemas que ayuden a mejorar su desempeño.

Costos. Los costos en equipamiento en comparación con sistemas cableados son mucho menores si se considera las distancias que se pueden cubrir.

Las desventajas que se pueden presentar en sistema inalámbrico son:

Menor velocidad. Los sistemas cableados dependiendo del tipo pueden alcanzar velocidades desde unos pocos Megabits por segundo hasta cientos de Gigabits por segundo, con la implementación de nuevas tecnologías inalámbricas como WiMAx y MIMO es posible alcanzar velocidades de 100 y hasta velocidades teóricas de 600 Mbps, pero estas velocidades se encuentran aún debajo de las que puede alcanzar una fibra óptica.

Seguridad. Al no requerir de un medio físico, los sistemas inalámbricos presentan una clara desventaja de seguridad ya que la señal se propaga al espacio quedando vulnerable al ataque de intrusos. Existen métodos para implementar seguridades en este tipo de sistemas, pero la comunicación será más segura si cuenta con un medio físico para su transporte.

Interferencias. Muchos de los sistemas inalámbricos trabajan en frecuencias no licenciadas, esto significa que cualquier operador puede coincidir con sistemas de comunicación en frecuencias similares, lo que eleva la posibilidad de sufrir interferencia.

Alcance. El alcance de un sistema inalámbrico será determinado por la potencia de salida de los equipos y la ganancia que puedan ofrecer las antenas, y en función de la frecuencia en la que trabaje un enlace, su alcance estará definido por factores como la geografía en que trabaje el enlace, la refractividad de la atmósfera, permitividad o constante dieléctrica de medio, clima, etc.

3.2 MODELO DE REFERENCIA ESTÁNDAR IEEE 802.11X[18]

La arquitectura de la norma IEEE 802.11x sigue el mismo modelo que el estándar IEEE 802, es decir se centra en definir los niveles más bajos del modelo OSI, la capa física y la subcapa de Control de Acceso al Medio (MAC).

3.2.1 CAPA FÍSICA.

Distingue dos subcapas. Una capa inferior llamada PMD *(Physical Media Dependent)*, especifica los sistemas de transmisión a nivel físico, es decir es la responsable de la transmisión de las tramas al medio, además de las técnicas de codificación y modulación que se entregará al medio de transmisión. La segunda capa denominada *PLCP (Physical Layer Convergence Procedure)*, esta cabecera contiene información acerca del paquete MAC transmitido, la duración, la velocidad de transmisión y se encarga de añadir una cabecera a la capa MAC para formar un *MPDU (MAC Protocol Data Unit)*.

La cabecera MPDU o PLCP se divide en tres campos los cuales son: el preámbulo, que sincroniza e inicia la trama, la cabecera PLCP, contiene la

información de la velocidad, iniciación y longitud de la trama, Datos, contiene la trama de la subcapa MAC

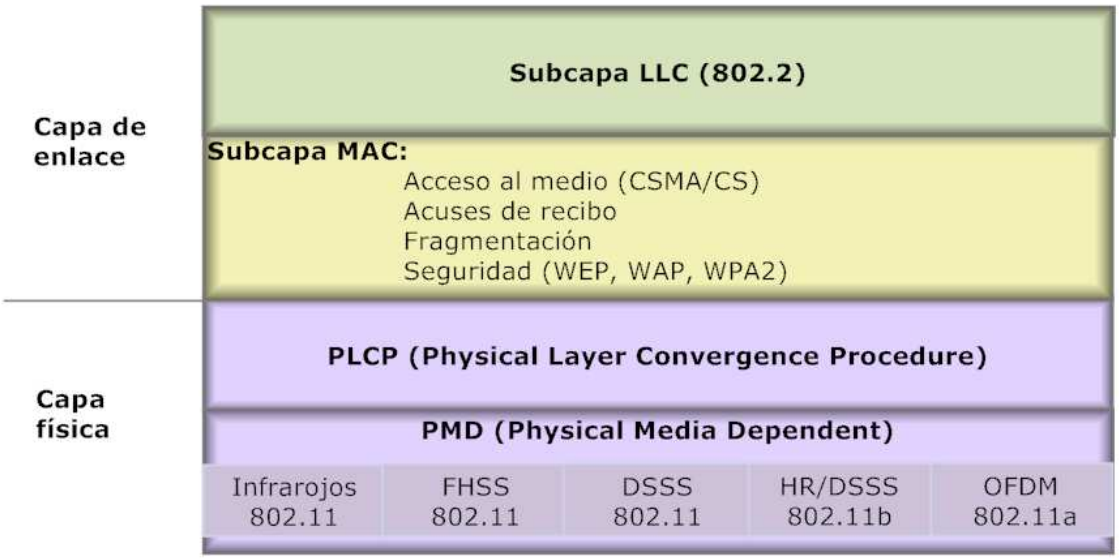


Figura 3.1 Capa física 802.11

La primera norma 802.11 aprobada por la IEEE en 1997 especifica tres capas físicas para velocidades de 1 y 2 Mbps en la frecuencia 2,4 GHz, usando técnicas de espectro expandido *(SS, Spread Spectrum)* como son: espectro expandido por saltos de frecuencia *(FHSS, Frecuency Hopping Spread Spectrum)*, y espectro expandido por secuencia directa *(DSSS, Direct Sequence Spread Spectrum).*

En 1999, la IEEE emite una segunda norma conocida como 802.11b, en la cual se alcanzan velocidades de transmisión de 1, 2, 5.5, 11 Mbps para la banda de 2,4 GHz, mediante la técnica de espectro expandido por secuencia directa de alta velocidad *(HR-DSSS High Rate – Direct Spread Spectrum).*

En este mismo año la IEEE define una tercera norma la 802.11a, la cual permite operar equipos en la banda de frecuencia de 5 GHz, y alcanza velocidades teóricas de hasta 54 Mbps mediante el uso de Multiplexación por División de Frecuencia Ortogonales *(OFDM Orthogonal Frecuency Division Multiplexing).*

En el año 2003 la IEEE especifica la norma 802.11g, que opera en frecuencia 2,4 GHz y permite alcanzar velocidades de 6, 9, 12, 18, 24, 36, 48, y 54 Mbps, y además es compatible con la norma 802.11b.

En noviembre del 2009 la IEEE emite el estándar 802.11n, en la cual los sistemas pueden alcanzar velocidades de hasta 300 Mbps con límites teóricos de hasta 600 Mbps, y trabajan en frecuencias 2,4 GHz y 5,4 GHz simultáneamente, siendo además compatible con los estándares 802.11b y 802.11g, este nuevo estándar utiliza una nueva tecnología denominada Multiples Entradas – Multiples Salidas *(MIMO- Multiple Input – Multiple Output)*, usando dos canales unidos *(Channel Bonding)* llamados también 40 MHz, debido a que usa 2 canales de 20 MHz antes usados en el estándar 802.11b.

Existen cinco tipos de técnicas de espectro ensanchado: sistemas de secuencia directa de espectro ensanchado (DSSS), sistemas de salto de frecuencia (FHSS), Sistemas de salto temporal, Sistemas de Frecuencia Modulada Pulsada y Sistemas Híbridos (OFDM, MIMO).

3.2.1.1 Espectro expandido por secuencia directa (DSSS)

Un sistema DSSS utiliza un código de pseudo ruido o “chip code”, generado localmente para codificar cada bit que compone la señal de información. El estándar 802.11 utiliza un código llamado secuencia de Barker, en el cual se sustituye un bit por una secuencia de once “chips”, que es el tiempo de duración de cada elemento.

Este código pseudo ruido es formado mediante un código de señales binarias periódicas y de cierta longitud, de tal forma que dentro de cada periodo la señal puede aproximarse a una señal aleatoria. Este código es generado a una velocidad mucho mayor que la velocidad de los datos y es multiplicada por la información mediante una operación EXOR.

Al multiplicar dos señales en el tiempo se realiza una convolución en frecuencia, lo que implica una nueva señal con espectro disperso. Al dispersar el espectro de una señal, la densidad espectral de potencia disminuye; así, esta nueva señal es más resistente a interferencias, además de que es posible multiplicar un canal logrando un canal multiusuario.

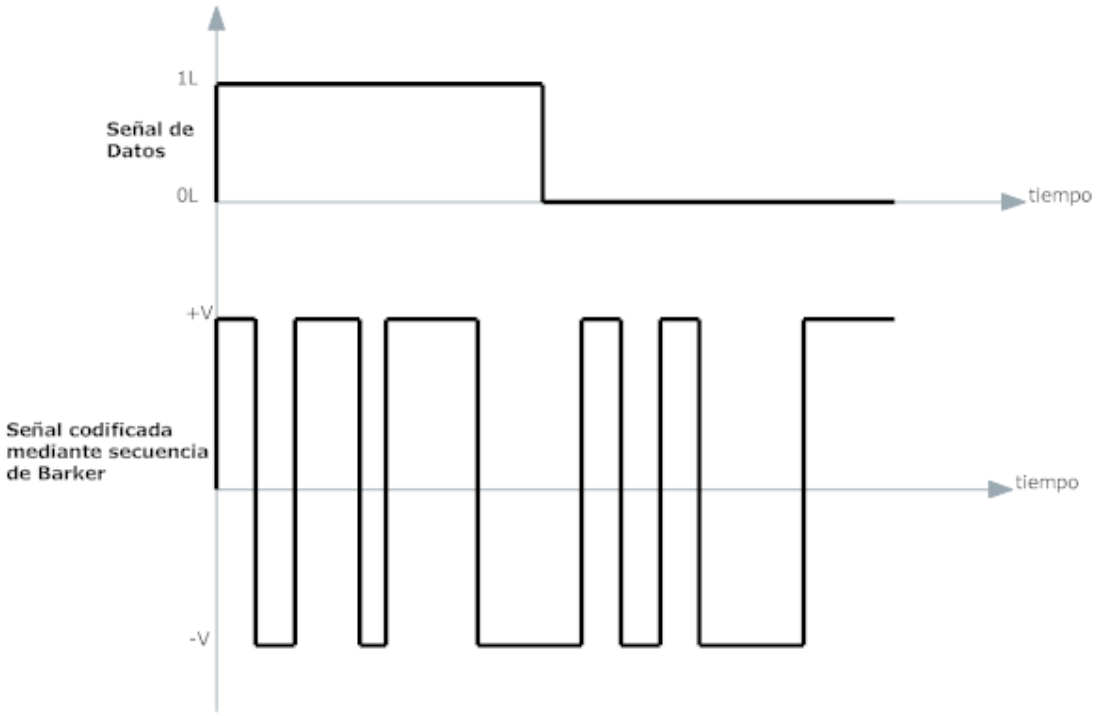


Figura 3.2 Codificación DSSS

La señal resultante de la multiplicación de la señal de información con la secuencia Barker es modulada mediante una modulación por desplazamiento diferencial de fase binario *(DBPSK – Differential Binary Phase Shift Keying),* para velocidades de transmisión de 1Mbps, y la modulación de fase diferencial en cuadratura *(DQPSK – Differential Quadrature Phase Shift Keying)*, para velocidades de hasta 2 Mbps.

3.2.1.1 Trama PLCP DSSS

La trama está formada de un campo usado para sincronización con el receptor de 128 bits. Un campo delimitador de inicio de trama, que indica el inicio de la trama de 16 bits. Un campo de señalización, que indica la velocidad de transmisión de los datos formado de 8 bits. Un campo de servicio, no asignado actualmente de 8 bits. Un campo llamado longitud, formado de 128 bits, indica el tiempo necesario para transmitir la trama MAC (Datos), este valor puede variar de 16 a 65535 microsegundos. Un campo CRC código de redundancia cíclica, el cual es el encargado del control de errores de la

cabecera PLCP. Y por último el campo de datos, el cual tiene una longitud variable y contiene la trama MAC.

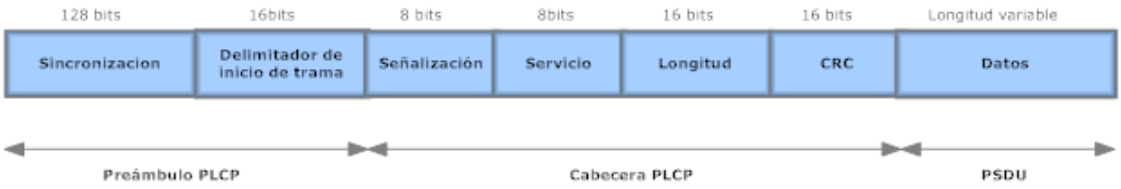


Figura 3.3 Trama PLCP DSSS[19]

3.2.1.2 Espectro expandido por salto de frecuencia (FHSS)

En este sistema la frecuencia portadora cambia en un tiempo llamado dwell time inferior a 400 ms, pasado este tiempo la frecuencia portadora es cambiada, y la transmisión se realiza en otra frecuencia durante el tiempo dwell. De esta manera la información se transmite en frecuencias diferentes en cortos intervalos de tiempo.

Los saltos son determinados mediante una secuencia pseudo aleatoria registrados por el transmisor y el receptor para mantener la sincronización que por momentos cambia de nivel físico, pero que mantiene un único canal lógico. Con esto se consigue un nivel de seguridad ya que solo el receptor conoce la secuencia en la que recibirá la información.

FHSS utiliza la frecuencia 2,4 GHz y se divide en 79 canales de 1 MHz, el número de saltos está definido por la legislación de cada país.

3.2.1.2.1.1 Trama PLCP FHSS

La trama para FHSS tiene los mismos campos que para DSSS excepto el campo de servicio que no es incluido en esta trama, además varía el tamaño de cada campo. El campo de sincronización contiene 80 bits, el campo delimitador de inicio de trama tiene 16 bits, el campo de longitud se forma de 12 bits, el campo de señalización contiene 4 bits, el campo designado para la detección de errores CRC contiene 16 bits, y los datos tienen una longitud

variable.

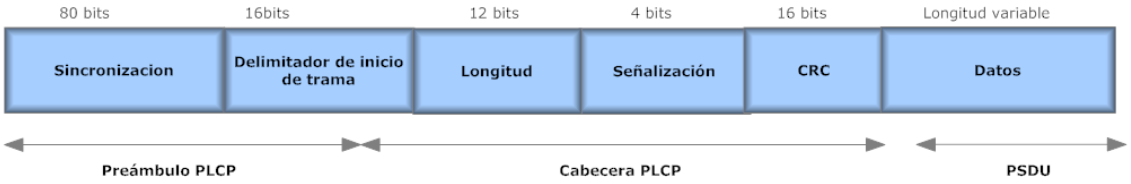


Figura 3.4 Trama Trama PLCP FHSS[20]

3.2.1.3 Multiplexación por división de frecuencia ortogonal (OFDM – Orthogonal Frecuency Division Multiplexing)

Esta técnica es utilizada por el protocolo 802.11a, y utiliza la banda de 5 GHz denominada U-NII *(Unlicenced National Information Infraestructure)*. Esta se encuentra dividida en tres sub-bandas de cuatro canales cada sub-banda, con lo cual se obtiene un total de 12 canales de 20 MHz de ancho de banda.

Las modulaciones que se utiliza para este sistema son, modulación de fase binaria BPSK, modulación de fase en cuadratura QPSK, modulación de amplitud en cuadratura 16 o 64 16 QAM / 64 QAM, y para la detección de errores se utiliza el FEC *(Forward Error Correction)* que utiliza códigos convolucionales para la detección de errores. La velocidad de los datos está determinada por la modulación y la velocidad de codificación.

La modulación OFDM envía la información en varias portadoras que están espaciadas en frecuencia, por lo que la información total es la suma de las portadoras individuales, esto hace que esta señal sea muy resistente a interferencia y a desvanecimientos por multitrayecto.

La modulación usada para estos sistemas es modulación de amplitud en cuadratura QAM y la modulación de fase PSK.

3.2.1.3.1 Trama PLCP OFDM

La trama se compone de tres áreas, el preámbulo PLCP, la señal, y los datos. Estos a su vez contienen campos que gestionan velocidad, paridad, longitud, servicio, cola, etc.

El preámbulo PLCP: Permite la sincronización con el receptor, y contiene campos como STF *(Short Training Field)* y el LTF *(Long Training Fiedl).*

La señal: Contiene 24 bits, en los cuales se incluye los siguientes campos:

- Velocidad *(Rate),* especifica la velocidad a la que se transmite el campo datos y está compuesta de 4 bits.
- Reservado, este campo es de un solo bit y está reservado para usos futuros.
- Longitud, indica el número de bytes que contiene la trama de datos MAC, y está formada de 12 bits.
- Paridad, este es un bit de paridad de los 17 bits de los campos velocidad, reservado y longitud.
- Cola *(Tail),* contiene seis ceros añadidos al campo señal.

Datos: Es de longitud variable y contiene a su vez subcampos como:

- Servicio, este campo es utilizado para sincronizar el proceso de aleatoriedad que deben sufrir los datos antes de ser transmitidos, esto para evitar colas de unos y ceros.
- PSDU, contiene los datos entregados por la capa MAC
- Cola, se utiliza para reiniciar el codificador convolucional, está formado de 6 bits
- PAD, este campo se utiliza como relleno cuando el campo dato no es múltiplo de 48, 96, 192, o 288 bits.

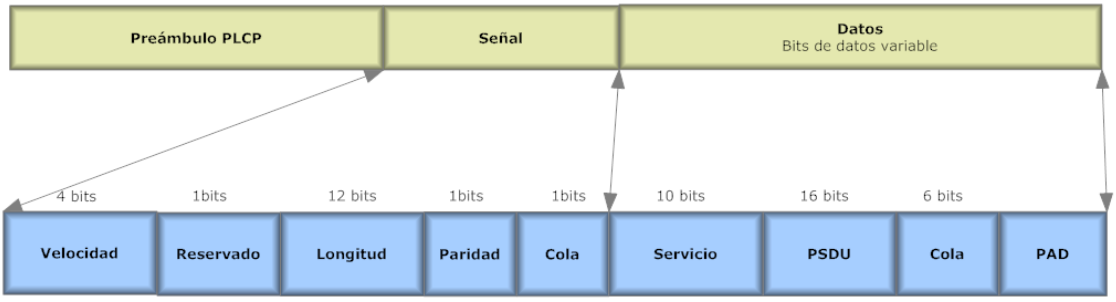


Figura 3.5 Trama PLCP OFDM[21]

3.2.2 CAPA ENLACE.

La capa enlace define el control de acceso al medio, y el protocolo 802.11 incorpora un algoritmo similar al 802.3[I] llamado CSMA/CA *(Carrier Sense Multiple Access / Collision Avoidance)*, el cual permite que el medio de transmisión sea utilizado por múltiples equipos.

3.2.2.1 Protocolo CSMA/CA

Un equipo para poder transmitir, debe primero escuchar si el medio de transmisión se encuentra libre, si el canal se encuentra libre, el equipo podrá anunciar su intención de transmitir, de esta forma se evita la colisiones entre paquetes de datos. Por el contrario si el medio de transmisión se encuentra ocupado, deberá esperar un tiempo aleatorio corto y esperar recibir un mensaje de acuse si recibe un ACK *(Acknowledgement)* y solamente si, tras ese corto periodo, el medio se encuentra libre, se procede con la transmisión esto reduce la probabilidad de colisiones en el canal.

Pueden producirse colisiones cuando dos estaciones coinciden en un mismo tiempo de espera aleatorio para transmitir, en ese caso reintentan utilizando un rango más amplio de tiempo aleatorio de espera en la cual se reduce la posibilidad de coincidencia en la transmisión de los dos equipos.

3.2.2.1.1 Fragmentación.

La fragmentación de paquetes es utilizada cuando el medio está expuesto a interferencia o ruidos, que podrían dificultar el envío y la recepción de paquetes, el transmisor fragmenta las tramas grandes y con esto aumenta la posibilidad de transmitir la información, pero esto deviene en un aumento en el tiempo de transmisión de la información.

Dependiendo de la potencia de transmisión de las estaciones y el alcance de transmisión de las mismas pueden presentarse inconvenientes como:

[I] 802.3 especifica el protocolo Ethernet que define las características de cableado y señalización de nivel físico y los formatos de tramas de datos del nivel de enlace de datos del modelo OSI.

3.2.2.2 Problema de nodos ocultos [22]

Se tiene tres estaciones A, B y C, en la cual A y C desean comunicarse con B, A y C envían una trama, pero estas estaciones por el rango de potencia de transmisión están ocultas entre ellas, por lo que las dos estaciones tienen la posibilidad de transmitir hacia B simultáneamente originando una colisión en la estación B que es difícil de detectar.

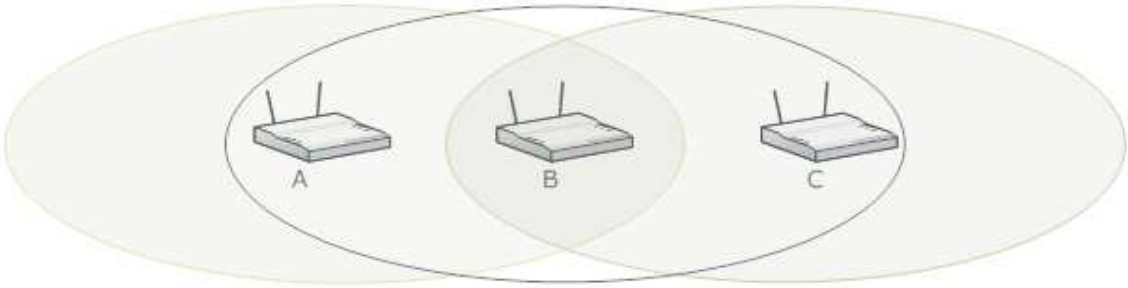


Figura 3.6 Nodos ocultos

3.2.2.3 Problema de nodos expuestos

Se tiene cuatro estaciones A, B, C y D. La estación C se encuentra fuera del rango de transmisión de A y advierte que B ha establecido comunicación con A por lo que no puede solicitar comunicación con B, por lo que busca una estación que pueda transmitir que puede ser D.

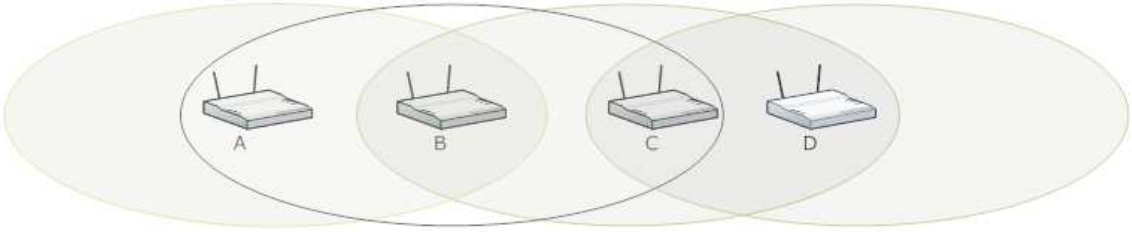


Figura 3.7 Nodos expuestos

Para solucionar estos problemas la estación donde colisionan los mensajes debe informar a las otras estaciones que el mensaje ha colisionado, para esto utiliza un algoritmo llamado MACA *(Multiple Access Colision Avoidance).* En el

cual la estación que transmite y el receptor intercambian tramas de control antes de que el transmisor envíe algún dato, el proceso se realiza de la siguiente forma:

- Cuando una estación anuncia su intención de transmitir envía una trama de solicitud de envío *(Request To Send, RTS)*, esta trama contiene un campo en el que indica el tiempo que la estación utilizará el medio de transmisión, o en su defecto indica la longitud de la trama de datos que desea transmitir. Las estaciones cercanas escuchan la trama y almacenan este valor en un vector de asignación de red *NAV (Network Allocation Vector)*, este vector indica el tiempo de utilización y funciona como un temporizador decreciente.
- El receptor que recibe el RTS, a su vez envía una trama libre de envío CTS *(Clear To Send)*, esta trama también contiene el tiempo de utilización del canal. De esta manera se soluciona el problema del nodo oculto, ya que cualquier nodo que recibe la trama CTS sabe que el receptor se encuentra ocupado y deberá esperar el tiempo solicitado por el NAV de la primera estación para luego del tiempo especificado poder transmitir.
- El equipo transmisor al recibir la trama CTS envía los datos, una vez concluido el envío de datos, el equipo receptor envía un ACK al equipo transmisor confirmando que los datos fueron recibidos exitosamente, de esta forma el resto de estaciones deben esperar este ACK antes de intentar transmitir. Si el equipo transmisor no recibe el ACK porque el ACK fue dañado o el mensaje no fue entregado en el tiempo establecido, se reenviará la trama por parte del equipo transmisor.

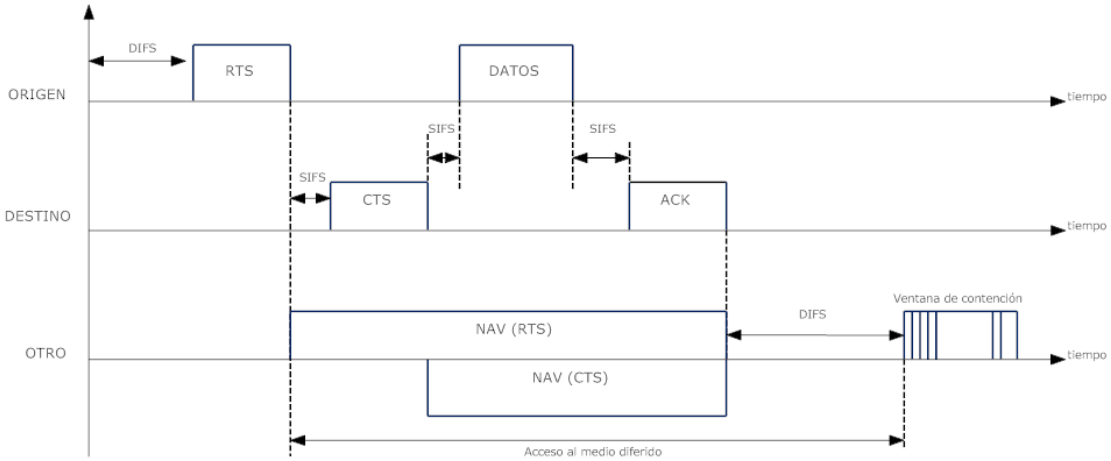


Figura 3.8 Proceso MACA[23]

3.3 PROTOCOLOS 802.11

3.3.1 PROTOCOLO 802.11 LEGACY[24]

También conocida como IEEE 802.11-1997, hace referencia a la original versión de la IEEE 802.11, estándar para redes inalámbricas que especifica dos velocidades de transmisión de 1 y 2 Mbps transmitidas por señales infrarojas (IR) o por FHSS y DSSS en la banda ISM[I] en la banda de frecuencias 2,4 GHz.

El estándar original también definía CSMA/CA como el método de acceso al medio. Un porcentaje significativo de la capacidad del canal disponible era sacrificado cubriendo las necesidades de la codificación para mejorar la calidad de la transmisión lo que produjo dificultades de interoperabilidad entre equipos.

La versión de 802.11 DSSS fue rápidamente reemplazada por el protocolo 802.11b en 1999, que aumentó la tasa de bits a 11 Mbps teóricos. La adopción generalizada de las redes 802.11 sólo se produjo después de la liberación de 802.11b que dio lugar a múltiples productos interoperables y a múltiples proveedores. Como consecuencia muy pocas redes implementaron el estándar 802.11-1997.

[I] ISM Industrial Scientific Medical

3.3.2 PROTOCOLO 802.11a

El protocolo utiliza tecnología OFDM con 52 subportadoras de las cuales 48 subportadores son usadas para transmitir datos y las cuatro restantes son utilizadas como portadoras piloto. Ofrece 12 canales sin traslape de 20 MHz, de los cuales 8 canales son usados para sistemas mutipunto y 4 canales para sistemas *backhaul* (punto – punto). Permite un ancho de banda teórico de hasta 54 Mbps, en la banda de 5 GHz U-NII. No es compatible con el protocolo 802.11b por trabajar en diferentes frecuencias.

Banda (GHz)	Número de canal	Frecuencia de transmisión
U-NII banda baja **(5,15 – 5,25)**	36	5,180 GHz
	40	5,200 GHz
	44	5,220 GHz
	48	5,240 GHz
U-NII banda media **(5,25 – 5,35)**	52	5,260 GHz
	56	5,280 GHz
	60	5,300 GHz
	64	5,320 GHz
U-NII banda alta **(5,35 – 5,835)**	149	5,745 GHz
	153	5,765 GHz
	157	5,785 GHz
	161	5,805 GHz

Tabla 3.1 Asignación de frecuencias 802.11ª

3.3.3 PROTOCOLO 802.11b

El estándar IEEE 802.11b fue anunciado en 1999, funciona en la banda de 2,4 GHz, la velocidad máxima teórica de transmisión es de 11 Mbps, utiliza el método de acceso al medio definido para el estándar original CSMA/CA, el máximo throughput[I] que alcanza este estándar es 5,9 Mbps sobre TCP[I], y 7,1 Mbps sobre UDP[II]

[I] **Throughput**, es el volumen de trabajo o de información que fluye a través de un sistema. Así también se le llama al volumen de información que fluye en las redes de datos.

Utiliza DSSS como método de modulación. Opera en la banda de frecuencias comprendida desde los 2412 y 2484 GHz dentro de la banda ISM[III], con un ancho de banda disponible de 73 MHz, del cual se dividen 14 canales.[IV]

Número de canal	Frecuencia (GHz)	Norteamérica	Europa	España	Francia	Japón
1	2,412	X	X			
2	2,417	X	X			
3	2,422	X	X			
4	2,427	X	X			
5	2,432	X	X			
6	2,437	X	X			
7	2,442	X	X			
8	2,447	X	X			
9	2,452	X	X			
10	2,457	X	X		X	
11	2,462	X	X	X	X	
12	2,467		X	X	X	
13	2,472		X		X	
14	2,483					X

Tabla 3.2 Asignación de canales 802.11b

Si se existen varias estaciones transmitiendo simultáneamente, para que puedan trabajar sin interferencia deben separarse 25 MHz es decir que la primera estación trabajará en el canal 1 con frecuencia 2,412 GHz, la segunda estación trabajará en el canal 6 frecuencia 2,437 GHz, y la tercera estación en el canal 11 es decir en la frecuencia 2,462 GHz

---

[I] **TCP**, es un protocolo de comunicación orientado a conexión y fiable del nivel de transporte

[II] **UDP**, es un protocolo del nivel de transporte basado en el intercambio de datagramas, sin control de flujo

[III] **ISM (Industrial, Scientific and Medical)** son bandas reservadas internacionalmente para uso no comercial de radiofrecuencia electromagnética en áreas industrial, científica y médica. Estas bandas se encuentran en las frecuencias 902 -928 MHz, 2,4 – 2,484 GHz, 5,725 – 5,850 GHz

[IV] Puede variar según la legislación de cada país

3.3.4 PROTOCOLO 802.11g[25]

Este estándar fue aprobado en 2003, utiliza la banda 2,4 GHz igual que el estándar 802.11b, utiliza DSSS y OFDM como métodos de modulación por lo que puede ser compatible con el estándar 802.11b, puede alcanzar velocidades teóricas de hasta 54 Mbps, o cerca de 24,7 Mbps de velocidad real de transferencia (throughput), similar al estándar 802.11a.

3.3.5 PROTOCOLO 802.11d[26]

Este estándar especifica comunicaciones inalámbricas en los países donde los sistemas que utilizan las normas 802.11 no se les permite operar.

La especificación 802.11d es similar en muchos aspectos a la 802.11b. La diferencia principal es que la configuración en el nivel del control de acceso al medio (Capa MAC) para cumplir con las normas del país o del distrito en el que la red se va a utilizar. Las normas incluyen frecuencias permitidas, niveles de potencia, ancho de banda permitido. La especificación elimina la necesidad de diseño y fabricación de decenas de soluciones de hardware diferente, cada una para su uso en una jurisdicción en particular. La especificación 802.11d es, incluye normas para sistemas que quieren ofrecer *roaming global*

3.3.6 PROTOCOLO 802.11e[27]

El estándar 802.11e introduce mecanismos a nivel de la capa MAC para soportar servicios que requieren Calidad de Servicio *(QoS – Quality of Service),* mediante el uso de un nuevo estándar llamado Hybrid Coordination Function (HCF)

- *(EDCA) Enhanced Distributed Channel Access*, equivalente a DCF.
- (*HCCA) HCF Controlled Access*, equivalente a PCF.

Este estándar define cuatro categorías de acceso al medio:

- *Background (AC_BK)*
- *Best Effort (AC_BE)*
- *Video (AC_VI)*
- *Voice (AC_VO)*

Para conseguir la diferenciación del tráfico se definen diferencies tiempos de acceso al medio y diferentes tamaños de la ventana de contención para cada una de las categorías.

3.3.7 PROTOCOLO 802.11f

El protocolo especifica la compatibilidad entre proveedores en el caso de sistemas multipunto, además especifica la posibilidad de uso de *roaming* entre redes[l] con el cual un usuario que está en movimiento puede cambiarse de un punto de acceso a otro punto de acceso mediante el protocolo IAPP *(Inter-Acess Point Protocol).*

3.3.8 PROTOCOLO 802.11h[28]

Estándar que sobrepasa al 802.11a al permitir la asignación dinámica de canales para permitir la coexistencia de éste con el *HyperLAN*. Además define el TPC *(Transmit Power Control)* según el cual la potencia de transmisión se adecúa a la distancia a la que se encuentra el destinatario de la comunicación.

3.3.9 PROTOCOLO 802.11i

Este estándar provee encripción para redes que utilizan el protocolo 802.11a, 802.11b y 802.11g. Utiliza los protocolos de encripción TKIP *(Temporal Key Integrity Protocol)* y el protocolo AES *(Advance Encryption Standard).*

Otra característica del protocolo 802.11i es el llamado *“Key caching”,* el cual facilita la rápida reconexión de los usuarios al servidor que se encontraban temporalmente suspendidos, o fuera del servicio, esto permite un rápido *roaming* ideal para usos con aplicaciones avanzadas como voz sobre IP (VoIP).

---

[l] **Roaming (Itinerancia)**, es un concepto utilizado en comunicaciones inalámbricas que está relacionado con la capacidad de un dispositivo para moverse de una zona de cobertura a otra

3.3.10 PROTOCOLO 802.11j

Estándar que permitirá la armonización entre el IEEE, el ETSI[I] HyperLAN2, ARIB[II] e HISWANa[III].

3.3.11 PROTOCOLO 802.11n

Este protocolo fue aprobado en enero del 2009, mejora de forma significativa el ancho de banda de sus protocolos antecesores 802.11b y 802.11g, con una velocidad máxima teórica de hasta 600 Mbps, utiliza multiplexación espacial llamada MIMO *(Multiple Input – Multiplo Output),* con canales de 40 MHz.

MIMO utiliza varias antenas tanto en transmisor como en el receptor, utiliza varias técnicas de transmisión basadas en codificación espacio temporal por bloques *(STBC – Space Time Block Coding)*, con la cual se transmiten múltiples copias de un flujo de datos

3.4 MULTIPLEXACIÓN POR DIVISIÓN ESPACIAL (SDM)[29]

Esta técnica utiliza varios canales independientes para enviar información de un transmisor a un receptor, es decir un equipo que transmite utiliza varias antenas para transmitir y recibir la información.

[I] **ETSI** European Telecommunications Standards Institute, Instituto Europeo de Normas de Telecomunicaciones

[II] **ARIB** Association of Radio Industries and Businesses, Asociacion de estandarizacion en Japón

[III] **HISWANa** High-Speed Wireless Access Network

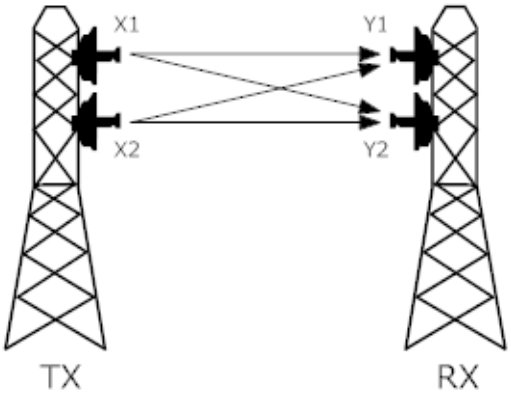


Figura 3.9 Multiplexación por división espacial

En el sistema TX tiene dos canales de comunicación hacia RX, X1 tiene la posibilidad de transmitir hacia Y1 y Y2, y X2 puede transmitir a Y1 y Y2, de esta forma se crea un sistema 2x2 MIMO/SDM, mediante esta tecnología es posible que la transmisión se la realice mediante un número N de antenas y un número M para la recepción, con lo cual se puede formar sistemas MIMO/SDM NxM. Este protocolo puede trabajar con canales de 40 MHz que son el resultado de unir dos canales de 20 MHz adyacentes, cada canal soporta 128 subportadoras[I], de las cuales 108 son usadas para datos.

CAPÍTULO 4

[I] El espaciamiento entre canal es de 312,5 KHz similar al canal de 20 MHz

DISEÑO E IMPLEMENTACIÓN DE ENLACES DE BACKBONE CON ROUTEROS.

4.1 CARACTERÍSTICAS DEL EQUIPAMIENTO[30]

El equipamiento escogido por su desempeño y características de procesamiento serán RouterBoards MikroTik 411AH (analizados en el segundo capítulo), y con radios mini PCI modelo R52Hn del mismo fabricante los cuales tiene las siguientes características:

Figura 4.1Radio R52Hn

- Soporta protocolo IEEE 802.11a/b/g/n banda dual
- Potencia de salida de hasta 25dBm en bandas a / g / n
- Soporte para hasta 2x2 MIMO con multiplexación espacial.
- Cuatro veces el rendimiento de 802.11a/g.

- Radio con chipset Atheros AR9220.
- 2x Conector de antena MMCX
- Modulaciones: OFDM: BPSK, QSPK, 16 QAM,
  DSSS: DBPSK, DQSPK, CCK
- Temperaturas de funcionamiento: -40 grados C a 70 grados C
- Consumo de energía en modo inactivo 0.4W
- Máximo consumo de energía 7w
- MiniPCI IIIA+ diseño (3mm más largo que el MiniPCI IIIA)

4.2 CONFIGURACIONES INALÁMBRICAS CON ROUTEROS

RouterOS permite diferentes modos de operación como enlaces punto – punto o enlaces multipunto. Se va a estudiar configuraciones inalámbricas básicas que permite RouterOS, para lo cual se utilizará diferentes modelos de RouterBoards y tarjetas de radios.

Dentro de la interface *wireless* existen varias viñetas de configuración entre las cuales se tiene:

General, indica información general de la interface como por ejemplo la dirección *MAC Address* de la tarjeta de radio.

Wireless, permite configurar los valores principales de la interface de radio como son: modo, la banda, la frecuencia, seguridad, etc.

Data Rates, permite configurar la velocidad de transmisión de la interface.

Advanced, permite configurar opciones avanzadas de la interface como son: ACK timeout, inmunidad al ruido, etc.

WDS, permite habilitar la opción WDS[I]

Nstreme, permite trabajar con la opción Nstream la cual es un tipo de protocolo propietario de MikroTik (no es compatible con otros equipos), el cual incrementa el rendimiento del enlace de forma significativa sin límite de distancia.

TX power, permite la configuración manual de la potencia de salida de la tarjeta de radio.

Status, indica el estado de funcionamiento de la interface wireless.

Tráfico, indica gráficamente la velocidad de transmisión de la interface y los paquetes que transmite la interface.

4.3 CONFIGURACIONES GENERALES DE RADIO[31]

Dependiendo del tipo de placa de radio que se disponga y el nivel de licencia soportado el equipo permitirá trabajar en diferentes modos, por ejemplo para configurar un equipo como CPE *(Customer Premises Equipment)* es posible realizarlo con un RouterBoard modelo 411AH con licencia nivel 3 y una tarjeta de radio modelo R52Hn, esto permitirá trabajar sistemas con los protocolos 802,11 a/b/g y n. Para configurar un Access Point con el sistema RouterOS es necesario que se disponga un equipo RouterOS con nivel 4, el cual permite habilitar la opción de Access Point y puede ser un RouterBoard MikroTik 433AH, con tarjeta de radio R52Hn, el cual tiene RouterOS nivel 4.

[I] **WDS Wireless Distribution System** permite que una red inalámbrica pueda ser ampliada mediante múltiples puntos de acceso sin la necesidad de un cable troncal que los conecte.

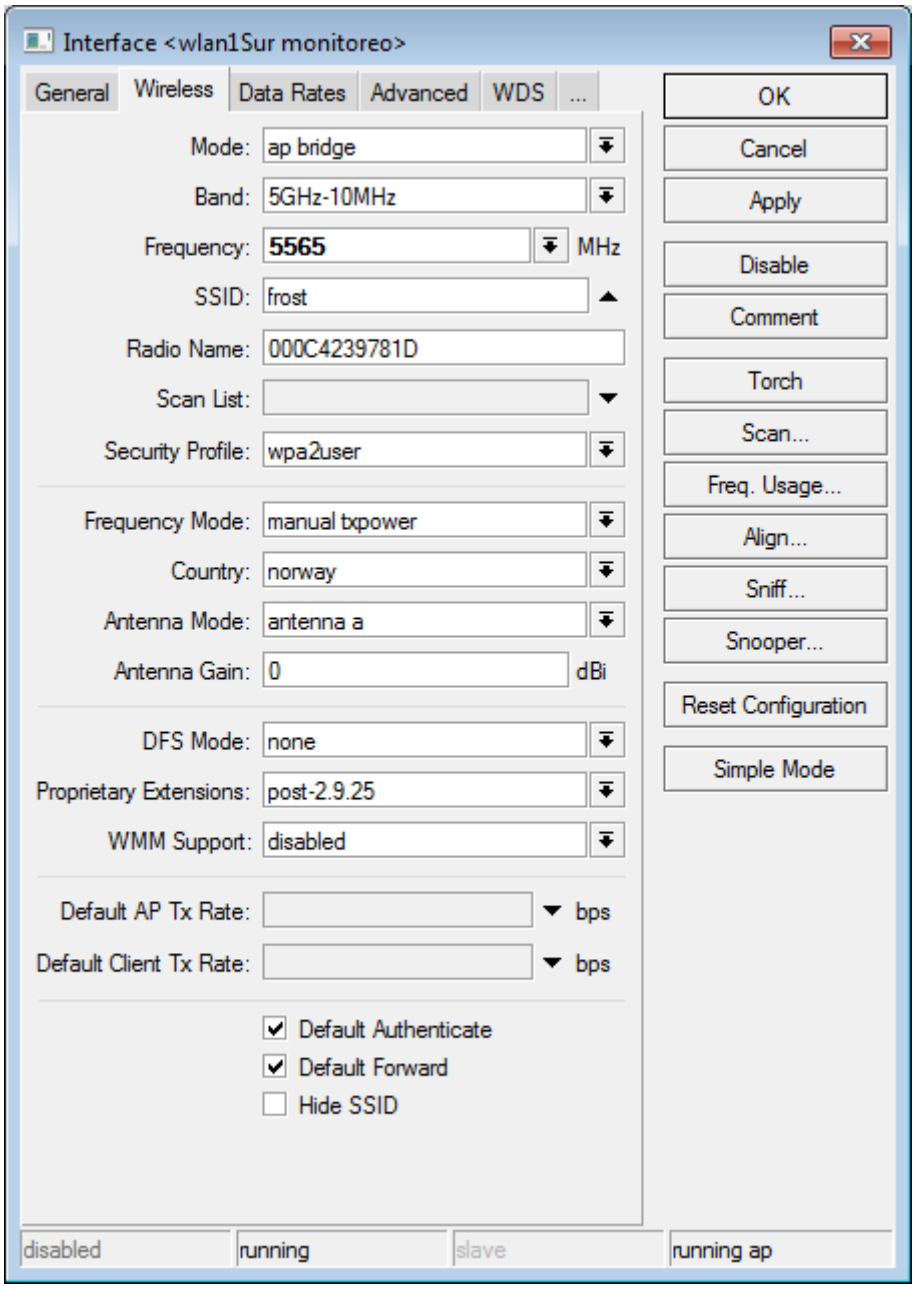


Figura 4.2 Configuración inalámbrica con RouterOS

Dentro de las opciones de la tarjeta se va a la interface Wireless y se considera los siguientes campos:

Mode: Indica en que diferentes modos puede trabajar el sistema

- *Aligment only*, permite la alineación de antenas de un sistema
- *AP Bridge*, este modo permite trabajar al equipo como Access Point configuraciones punto – multipunto. Esto da la posibilidad de conectar al

mismo tiempo varios clientes e ingresar esta interface a un bridge para trabajar en capa 2 entre una interface Ethernet y la interface Wireless.

- *Bridge,* este modo permite trabajar con configuraciones punto – punto, de este modo administra las configuraciones del enlace es decir trabaja como modo maestro (master), y también puede ser incluido en un bridge o usar el modo WDS.
- *Station,* este modo permite trabajar al equipo como un radio cliente CPE. Si se desea trabajar como un CPE es necesario hacer alguna forma de ruteo o un enmascaramiento ya que no permite trabajar con un bridge.
- *Station pseudobridge,* esta es una forma de realizar un bridge en el CPE para trabajar a nivel de capa 2, es decir permite añadir la interface wireless dentro de un bridge.

Band: permite escoger la banda de frecuencias en la que va a trabajar el equipo y considera el protocolo a usar:

- *2.4Ghz-b* - IEEE 802.11b.
- *2.4Ghz-b/g* - IEEE 802.11b/g.
- *2.4Ghz-g-turbo* – IEEE 802.11g usa un doble canal con lo cual provee una tasa de transferencia de 108 Mbps.
- *2.4Ghz-onlyg* - IEEE 802.11g.
- *5Ghz* - IEEE 802.11a hasta 54 Mbit.
- *5Ghz-turbo* - IEEE 802.11a usa un doble canal con lo cual provee una tasa de transferencia de 108 Mbps.
- *2Ghz-10Mhz* - Variación del protocolo IEEE 802.11g con media banda, y la mitad de la tasa de transferencia de hasta 27 Mbps.
- *2Ghz-5Mhz* – Variación del protocolo IEEE 802.11g con un cuarto de banda, con una tasa de transferencia cuatro veces más lento hasta 13,5 Mbps.
- *5Ghz-10Mhz* – variación del protocolo IEEE 802.11a con la mitad de la banda y la mitad de la tasa de transferencia de hasta 27 Mbps.
- *5Ghz-5Mhz* – Variación de protocolo IEEE 802.11a con un cuarto de banda, con una tasa velocidad de hasta 13,5 Mbps.

Frequency: indica la frecuencia en la que trabajará el equipo dependiendo de la banda escogida, es decir el protocolo escogido.

SSID: Service Set Identifier[32], es un nombre incluido en todos los paquetes de una red inalámbrica para identificarlos como parte de esa red. El código consiste en un máximo de 32 caracteres que la mayoría de las veces son alfanuméricos pero el estandar no lo especifica así que puede consistir en cualquier caracter. Todos los dispositivos inalámbricos que intentan comunicarse entre sí deben compartir el mismo SSID.

Radio Name: asigna un nombre a la interface.

Scan List: permite escoger el rango de frecuencias que un equipo cliente o estación puede escanear

Security Profile: configura el sistema de seguridad del sistema, WPA WPA2, Radius, etc.

Frecuency mode: define que canales son permitidos.

Country: configura las frecuencias permitidas en función de la legislación del país.

Antenna Mode: en el caso de diversidad de antena o trabajar con el protocolo 802.11n, permite identifica cual antena transmitirá la información y cual antena recibirá la información.

Antenna Gain: permite regular la ganancia de la antena en función de regulación del país.

4.4 DISEÑO DE ENLACES DE RADIO

4.4.1 FACTIBILIDAD DEL ENLACE

Para realizar un enlace sea este punto a punto o punto multipunto, se deben considerar factores técnicos, de infraestructura, y los relacionados con la logística como son: la geografía (topografía), accesibilidad, servicio público de electricidad, seguridad, estudios de la zona de Fresnel de los puntos a enlazar, interferencias, etc.

Actualmente se dispone de herramientas informáticas que ayudan a determinar la factibilidad de un enlace, para esto, en este proyecto se utilizará software libre Google Earth, y RADIO MOBILE, además de herramientas propias de RouterOS que ayudarán a analizar la topografía del enlace y determinar los parámetros de radioenlace del mismo

Después de un minucioso análisis considerando los puntos anteriormente expuestos, los sitios escogidos como nodos son:

Nodo	Latitud	Longitud	Altura msnm
Buenos Aires	00° 08` 47,10'' S	78° 27′ 35,00" O	2897 m
Cerro Blanco	00° 12` 31,00" N	78° 20` 19,30" O	3529 m

Tabla 4.1 Coordenadas de nodos

El nodo Buenos Aires se encuentra ubicado en la provincia de Pichincha en la ciudad de Quito, en el sector de Monteserrín al nororiente de la ciudad, cuenta con facilidad de acceso por estar ubicado dentro de la zona urbana de la ciudad y dispone de energía eléctrica pública, por su ubicación este nodo permitiría brindar servicio a clientes en las zonas de: Tumbaco, Puembo, Pifo, El Quinche, Yaruqui, Guayllabamba, Checa, además de la zona Nor-occidental de Quito.

El nodo Cerro Blanco se encuentra ubicado en la provincia de Imbabura a 15 Km aproximadamente de la ciudad de Otavalo, en este nodo por su ubicación geográfica, altitud y facilidad de acceso se encuentran nodos de otras empresas de comunicaciones que brindan servicio a la provincia de Imbabura y a otras provincias, este nodo permitiría brindar servicio a clientes en las zonas de Otavalo, San Pablo del Lago, Cotacachi.

La distancia entre los nodos a estudiar es de 41,42 Km. Mediante la herramienta Google Earth se puede analizar los puntos que se va a enlazar. De esto se obtiene la siguiente imagen:

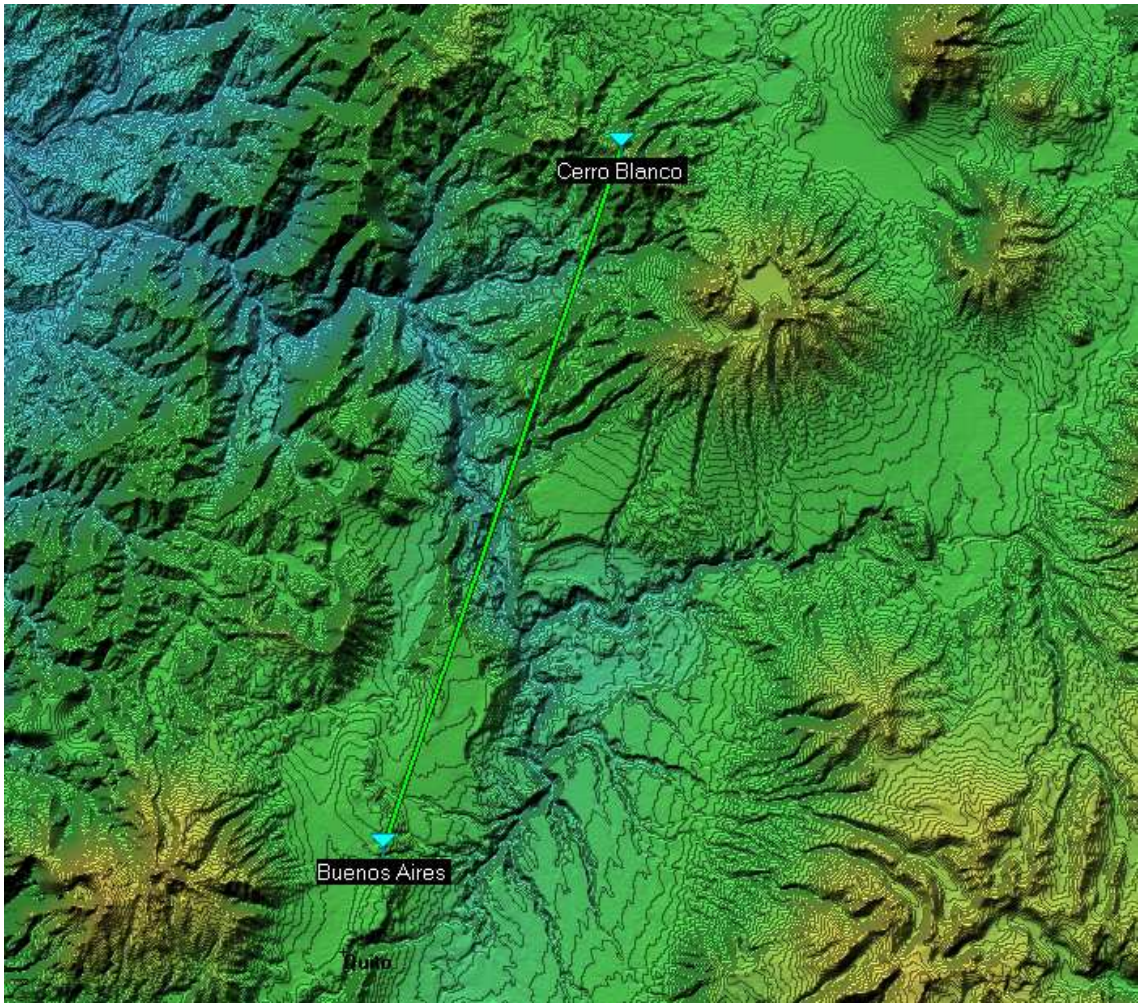


Figura 4.3 Ubicación de los nodos

Mediante el software Radio Mobile se examina el perfil topográfico del sistema el cual permitirá analizar la zona de Fresnel del enlace, este es muy importante en el desempeño de el enlace e incluso permitirá considerar la factibilidad del mismo.

4.4.2 ZONA DE FRESNEL[33]

Se llama zona de Fresnel al volumen de espacio entre el emisor de una onda electromagnética, acústica, radiación gravitacional, etc., y un receptor, de modo que el desfase de las ondas en dicho volumen no supere los 180º.

La difusión de ondas electromagnéticas en el espacio libre en función de la frecuencia en la que se está transmitiendo una señal y las obstrucciones que se puedan presentar en la línea de vista (*LoS – Line of Sight*), puede resultar en reflexiones y cambios de fase, esto puede significar un aumento o disminución del nivel de potencia de la señal en el receptor.

Así, la fase mínima se produce para el rayo que une en línea recta emisor y receptor. Tomando su valor de fase como cero, la primera zona de Fresnel abarca hasta que la fase llegue a 180º, adoptando la forma de un elipsoide de revolución. La segunda zona abarca hasta un desfase de 360º, y es un segundo elipsoide que contiene al primero. Del mismo modo se obtienen las zonas superiores.

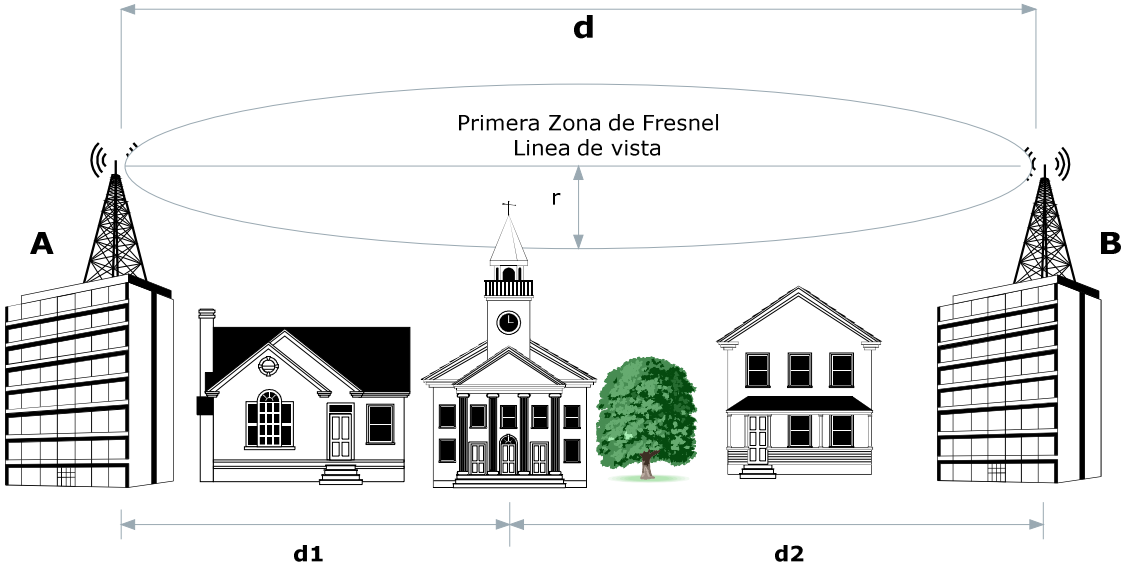


Figura 4.4 Zona de Fresnel

La obstrucción máxima permisible para considerar que no hay obstrucción es el 40% de la primera zona de Fresnel. La obstrucción máxima recomendada es el 20%. Para el caso de radiocomunicaciones depende del Factor K (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 se debe tener despejado el 60% de la primera zona de Fresnel.

Para establecer la zona de Fresnel, es necesario que exista línea de vista (LoS) entre los puntos, es decir que debe existir una la línea imaginaria entre el transmisor y el receptor.

4.4.2.1 Cálculo del radio de la primera zona del Fresnel.

La fórmula general para encontrar n-sima zona de Fresnel es:

$$r_n = 548\sqrt{\frac{n*d1*d2}{f*d}}$$

En la ecuación:

r_n: $radio\ en\ la\ nsima\ zona\ de\ Fresnel\ en\ metros$

548: $Constante\ de\ la\ curvatura\ de\ la\ tierra$

$d1$: $distancia\ desde\ el\ transmisor\ hasta\ la\ obstrucción\ \ Km$

$d2$: $distancia\ desde\ la\ obstrucción\ al\ receptor\ en\ Km$

f: $frecuencia\ del\ sistema\ en\ MHz$

Para determinar en el enlace Buenos Aires – Cerro Blanco la primera zona de Fresnel, se aplica la fórmula con la d1 = d2 y n igual a 1, por ser la primera zona de Fresnel.

$$r_1 = 548\sqrt{\frac{1 * 20{,}71 * 20{,}71}{5500 * 41{,}42}}$$

$$r_1 = 23{,}777\ m$$

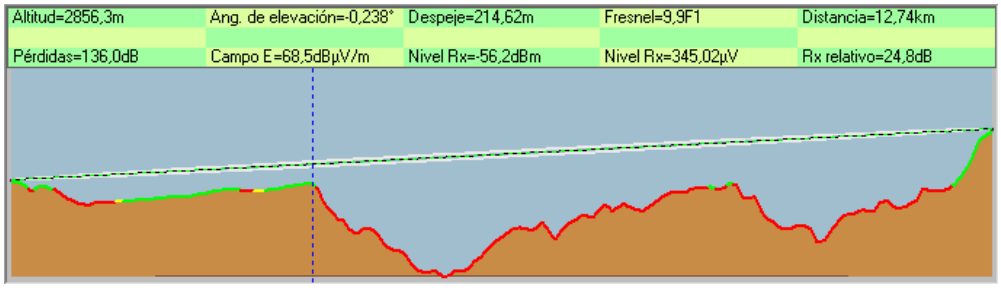


Figura 4.5 Análisis Fresnel Buenos Aires – Cerro Blanco

En el análisis topográfico entre los nodos Buenos Aires – Cerro Blanco se observa que existe una posible obstrucción de la primera zona de Fresnel a

12,74 Km desde Buenos Aires por lo que es necesario comprobar que en esa zona el radio de la primera zona de Fresnel está despejado.

Para comprobar que esta zona se encuentra libre se calcula la altura de despeje.

4.4.3 CÁLCULO DE LA ALTURA DE DESPEJE

La fórmula general para el cálculo del despeje es:

$$hdes = h1 + \frac{d1}{d}(h2 - h1) - \left(H + \frac{d1 * d2 * 1000}{2k * a}\right)$$

en la fórmula:

$hdes$: $altura\ de\ despeje\ desde\ el\ obstáculo\ hacia\ el\ eje\ de\ linea\ de\ vista$

$h1$: $altura\ del\ punto\ A$

$h2$: $altura\ del\ punto\ B$

H: $altura\ del\ obstáculo$

d: $distancia\ del\ eje\ de\ línea\ de\ vista$

$d1$: $distancia\ del\ transmisor\ hasta\ el\ obstáculo$

$d2$: $distancia\ del\ obstáculo\ hasta\ el\ receptor$

k: $coeficiente\ del\ radio\ efectivo\ de\ la\ tierra\ \frac{4}{3}\ para\ atmósfera\ estándar$

a: $radio\ promedio\ de\ la\ tierra\ igual\ a\ 6370\ Km.$

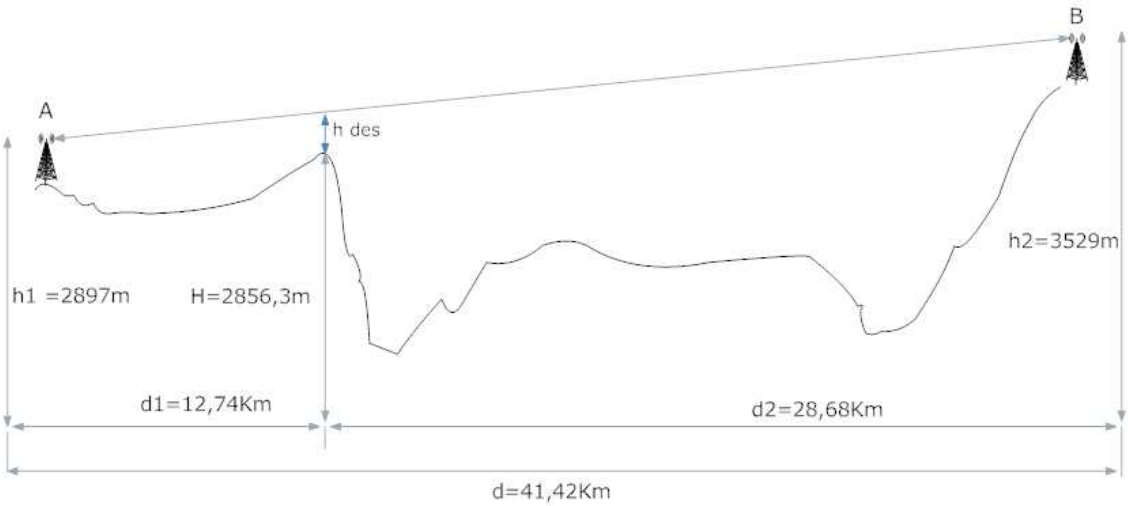


Figura 4.6 Análisis altura de despeje

Para el análisis se aplicará la fórmula:

$$hdes = 2897 + \frac{12{,}74}{41{,}42}(3529 - 2897) - \left(2856{,}3 + \frac{12{,}74 * 41{,}42 * 1000}{2 * \frac{4}{3} * 6370}\right)$$

$$hdes = 203{,}98\, m$$

En el análisis el valor de $hdes$ es mayor que el primer radio de la primera zona de Fresnel r_1, por lo tanto se asegura que no existe obstrucción en el trayecto del enlace.

$$hdes = 203{,}98\, m$$

$$r_1 = 23{,}777\, m$$

$$hdes > r_1$$

4.4.4 CÁLCULO DE DESEMPEÑO DEL ENLACE

A pesar de las buenas características técnicas del equipamiento escogido y del despeje en la línea de vista del enlace, es necesario calcular el presupuesto de potencia del enlace, esto permitirá coexistir con otros sistemas de similares características y mejorar en la implementación del sistema.

Este cálculo permite determinar la potencia en el receptor y con esto se determinará la factibilidad del mismo, esto tomando en cuenta el balance de

ganancias y pérdidas producidas por cables, antenas, conectores, espacio libre.

Se consideran tres partes para el análisis del desempeño del sistema:

1. El lado de transmisión con potencia efectiva de transmisión
2. Perdidas en la propagación (medio de transmisión)
3. El lado de recepción con efectiva sensibilidad receptiva (*efective receiving sensibility)*

4.4.5 PRESUPUESTO DE PÉRDIDAS Y GANANCIAS DEL ENLACE

El presupuesto del enlace se obtiene sumando algebraicamente de todos los aportes (ganancias) y pérdidas (en decibeles), que podría sufrir el enlace.

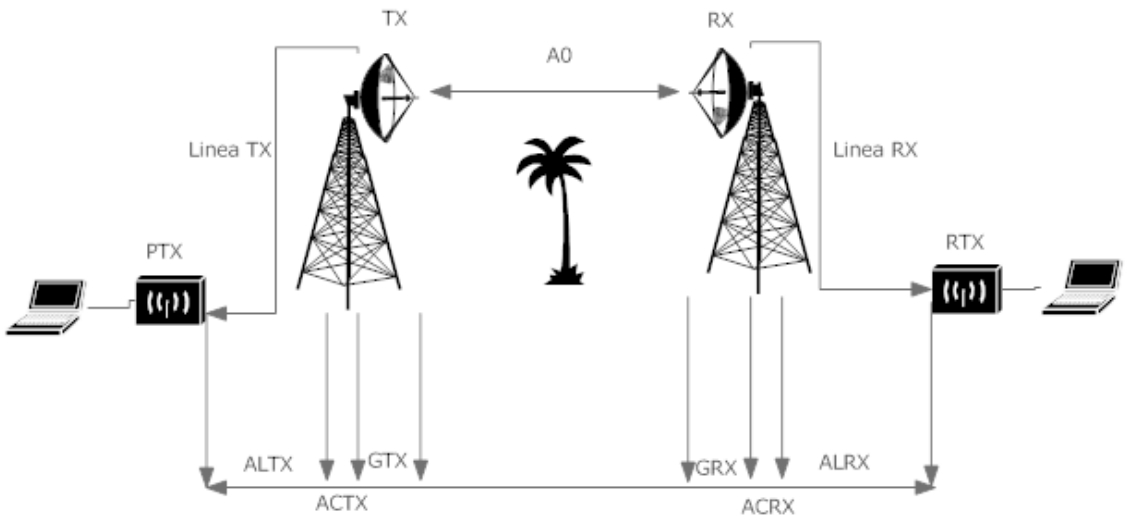


Figura 4.7 Análisis de pérdidas y ganancias

$$P_{RX} = P_{TX} - Ac_{TX} - Al_{TX} + G_{TX} - A_0 + G_{RX} - Al_{RX} - Ac_{RX}$$

En la fórmula:

P_{RX}: $Potencia\ del\ receptor\ [dBm]$

P_{TX}: $Potencia\ del\ transmisor\ [dBm]$

Ac_{TX}: Pérdid□□n c□n□ct□r TX $[dB]$

Al_{TX}: Pérdid□□n □l c□bl□ TX $[dB]$

G_{TX}: $Ganancia\ de\ antena\ TX$ $[dBi]$

A_0: Pérdidas en la trayectoria en el espacio libre [dB]

G_{RX}: $Ganancia\ de\ antena\ RX$ $[dBi]$

Al_{RX}: Pérdidas en el cable del RX [dB]

Ac_{RX}: Pérdidas en conector RX $[dB]$

Para calcular la confiabilidad real del enlace se debe entender y calcular parámetros como: pérdidas en el espacio libre, pérdidas en el cable, pérdidas en los conectores, ganancia de las antenas, etc.

4.4.5.1 Potencia de transmisión.

La potencia del transmisor es la potencia de salida del equipo emisor, este valor se encuentra en las especificaciones del vendedor, su límite superior depende de las regulaciones de cada país. La potencia típica para equipos IEEE 802.11 varían entre 16 – 27.7 dBm (300 – 600 mW).

Para el estudio las tarjetas de radio R52Hn radian una potencia típica de salida de 25 dBm (300 mW), para las bandas a/g/n.

4.4.5.2 Pérdidas en el cable

El cable y los conectores que une los equipos de transmisión/ recepción con las antenas agregan pérdidas al sistema. Las pérdidas dependen del tipo de cable y de la frecuencia de operación del sistema y normalmente se mide en dB/m.

Los valores típicos para pérdidas en cable van desde 0,1 dB/m hasta 1dB/m, se debe considerar que independientemente del tipo y material del cable usado este siempre presentará pérdidas, por lo que el cable que une la antena hacia el equipo debe ser lo más corto posible. En general mientras mayor sea el diámetro del cable que se está usando menor será la atenuación con una misma longitud.

La atenuación en el cable depende de la frecuencia de operación del enlace por lo que es necesario verificar los rangos de frecuencia que indica el

fabricante. Como regla general en frecuencia 5,4 Ghz un cable presenta el doble de pérdidas que en 2,4 GHz.

Tipo de cable	Pérdidas dB/m 2,4Ghz
LMR-100	1.3 dB por metro
LMR-195	0.62 dB por metro
LMR-200	0.542 dB por metro
LMR-240	0.415 dB por metro
LMR-300	0.34 dB por metro
LMR-400	0.217 dB por metro
LMR-500	0.18 dB por metro
LMR-600	0.142 dB por metro
LMR-900	0.096 dB por metro
LMR-1200	0.073 dB por metro
LMR-1700	0.055 dB por metro
RG-58	1.056 dB por metro
RG-8X	0.758 dB por metro
RG-213/214	0.499dB por metro
9913	0.253 dB por metro
3/8” LDF	0.194 dB por metro
1/2” LDF	0.128 dB por metro
7/8” LDF	0.075 dB por metro
1 1/4” LDF	0.056 dB por metro
1 5/8” LDF	0.46 por metro

Tabla 4.2 Pérdidas en los cables coaxiales

4.4.5.3 Pérdidas en los conectores

Los conectores en los cables coaxiales y los adaptadores (extensiones) incrementan las pérdidas de un sistema. Para cables coaxiales certificados se debe estimar 0.25 dB de pérdida por cada conector, este valor puede incrementar si los cables son fabricados por el usuario. Como regla general se considera un promedio de 0,3 a 0,5 dB por conector o adaptador.

4.4.5.4 Ganancia de Antenas[34]

Una antena es un transductor capaz de radiar y capturar ondas electromagnéticas y trasformar estas en energía eléctrica. Conectan las líneas

de transmisión de un transmisor con el espacio libre, el espacio libre a líneas de transmisión de un equipo receptor.

La ganancia de potencia se define como la dirección de máxima radiación. La ganancia directiva es la relación de la densidad de potencia irradiada en una dirección particular entre la densidad de potencia irradiada al mismo punto por una antena de referencia, suponiendo que ambas antenas estén radiando en la misma cantidad de potencia. La unidad de Ganancia (G) de una antena es el dB al ser una unidad de potencia.

$$G = 10 \log \frac{Pn}{Pref}$$

En donde:

$$Pn: potencia\ de\ la\ antena$$

$$Pref: potencia\ de\ referencia$$

Para el enlace se utilizará antenas tipo grilla marca *Hyperlink* modelo HG5426G con las siguientes características:

Frequency	5470-5725 MHz
Gain	26 dBi
Polarization	Horizontal or Vertical
Horizontal Beam Width	6°
Vertical Beam Width	9°
Front to Back Ratio	25 dB
Impedance	50 Ohm
Max. Input Power	100 Watts
VSWR	< 1.5:1 avg.
Weight	5.3 lbs. (2.4 kg)
Grid Dimensions	15.7 x 23.6 inches (400 x 600 mm)
Mounting	2 in. (50.8 mm) diameter mast max.
Operating Temperature	-40° C to 85° C (-40° F to 185° F)
Lighting Protection	DC Short
RoHS Compliant	Yes
Connector	N-Female

Tabla 4.3 Características de la antena Hyperlink HG5426G

Gráficos de radiación de la antena

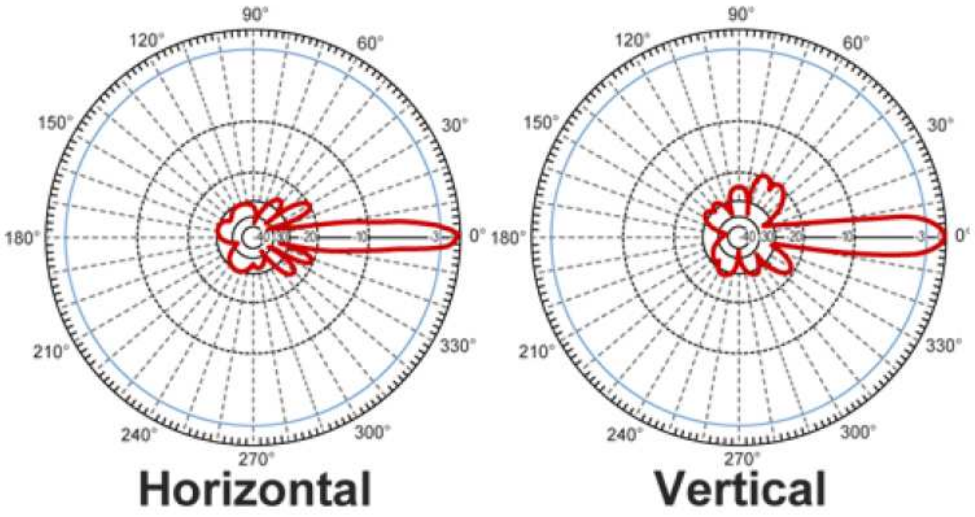


Figura 4.8 Gráficos de radiación de la antena

4.4.5.5 Pérdidas en el espacio libre

Gran parte de la potencia de la señal de radio se perderá en el espacio libre. Incluso en el vacío una señal pierde potencia (de acuerdo con los principios de Huygens). Esta pérdida mide la potencia que se pierde sin ningún tipo de obstáculo, esto incluye aire, lluvia, niebla, etc.

La fórmula general para pérdidas en el espacio libre:

$$PEA(dB) = 20log_{10}(d) + 20log_{10}(f) + K$$

En donde:

$$d = distancia$$

$$f = frecuencia$$

$$K = constante\ que\ dependen\ de\ f\ y\ d\ 92{,}45$$

Para el análisis del enlace se va a aplicar la fórmula:

$$PEA(dB) = 20log_{10}(41{,}42) + 20log_{10}(5{,}5GHz) + 92{,}45$$

$$PEA(dB) = 139{,}61\ dB$$

4.4.5.6 Margen de desvanecimiento

El desvanecimiento de la señal es un análisis de atenuación de un enlace en función del tipo de terreno y el factor climático en el que se va a desempeñar el sistema para esto se ha determinado la siguiente fórmula:

$$Fm\ (dB) = 30\ log\ D + 10\ log\ (6 * A * B * F) - 10\ log\ (1 - R) - 70$$

en donde:

$Fm\ (dB) = Atenuación\ por\ desvanecimiento\ en\ dB$

$D = distancia\ entre\ los\ nodos\ en\ Km$

$A = Factor\ de\ rugosidad\ del\ terreno,$

$B = Factor\ de\ análisis\ climático$

$F = frecuencia\ de\ la\ portadora\ en\ GHz$

$R = Objetivo\ de\ la\ confiabilidad\ de\ la\ transmisión\ \ 99{,}99\ \%$

El factor de rugosidad del terreno (*A)* se establece según la siguiente tabla:

Tipo de terreno	Factor de rugosidad del terreno
Espejos de agua, ríos anchos, etc.	4,00
Sembrados densos, pastizales, arenales	3,00
Bosques, la propagación va por arriba	2,00
Terreno normal	1,00
Terreno rocoso muy disparejo	0,25

Tabla 4.4 Factor de rugosidad del tipo de terreno

El factor de análisis climático (*B)* se establece según la siguiente tabla:

Clima	Factor climático
Área marina o condiciones de peor mes	1,00
Áreas calientes y húmedas	0,50
Áreas mediterráneas de clima normal	0,25
Áreas montañosas de clima seco y fresco	0,125

Tabla 4.5 Factor climático

Cálculo de margen de desvanecimiento para el enlace:

$$Fm\ (dB) = 30\ log\ 42{,}41 + 10\ log\ (6 * 2 * 0{,}5 * 5{,}5) - 10\ log\ (1 - 0.9) - 70$$

$$Fm\ (dB) = 14{,}009\ dB$$

4.4.5.7 Cálculo de potencia en el receptor

$$P_{RX} = P_{TX} - Ac_{TX} - Al_{TX} + G_{TX} - A_0 + G_{RX} - Al_{RX} - Ac_{RX}$$

$$P_{RX} = 25 - 1 - 1 + 28 - 139{,}61 + 28 - 1 - 1$$

$$P_{RX} = -62{,}61\ dB$$

La potencia de umbral de un equipo o sensibilidad del mismo está determinado por el fabricante y para este caso la sensibilidad del radio MikroTik R52Hn es de -84 dBm, con chipset Atheros AR9220.

R52Hn	Rx Sensibilidad dBm	Tx Power dBm
802.11ª		
6 Mbps	-97	25
54 Mbps	-80	21
802.11b		
1 Mbps	-93	24
11 Mbps	-93	24
802.11g		
6 Mbps	-94	25
54 Mbps	-81	22
802.11n 2,4GHz		
MCS0 20 MHz	-94	25
MCS0 40 MHz	-92	24
MCS7 20 MHz	-78	21
MCS7 40 MHz	-75	20
802.11n 5,4GHz		
MCS0 20 MHz	-97	24
MCS0 40 MHz	-92	22
MCS7 20 MHz	-77	18
MCS7 40 MHz	-74	17

Tabla 4.6 Sensibilidad radio Atheros AR9220

Para el análisis el umbral de potencia del radio es de -81dBm (P_u)

4.4.5.8 Cálculo de presupuesto total del enlace o potencia de umbral

El cálculo de presupuesto de enlace es para estar seguro de que el margen en el receptor es mayor que un cierto umbral. El margen de un presupuesto de enlace puede ser resumido de la siguiente manera:

$$Mu = P_{RX} - P_u$$

$$Mu = -62{,}61 - (-81)$$

$$Mu = 18{,}39\ dB$$

Para garantizar la eficiencia del enlace la potencia de umbral Mu debe ser igual o mayor que el margen de desvanecimiento Fm

$$Mu \geq Fm$$

$$18{,}39dB \geq 14{,}009dB$$

4.4.5.9 Resultados de la simulación con Radio Mobile

Figura 4.9 Resultado de análisis con Radio Mobile

4.5 CONFIGURACIÓN DE ENLACE PUNTO A PUNTO CON ROUTEROS

Una vez determinado la factibilidad del enlace se va a analizar las distintas maneras de configurar RouterOS para optimizar un enlace inalámbrico punto a punto, es decir el enlace debe permitir gestionar la mayor cantidad de ancho de banda.

En el enlace los equipos serán configurados con las direcciones IP's 10.1.7.175 en el nodo Buenos Aires y 10.1.7.174 en el nodo San José, la forma de configuración se la realizará como fue explicado en el capítulo 2.3.1

4.5.1 CONFIGURACIÓN DE LA INTERFACE INALÁMBRICA WLAN1 EN EL NODO BUENOS AIRES

Para la configuración el equipo en el nodo Buenos Aires trabajará como equipo Master, es decir este equipo administra la frecuencia portadora, la lista de escaneo de frecuencias, el SSID, etc.

Se va a configurar las viñetas y los campos importantes relacionados con la interface inalámbrica o wlan1. Dentro de *Interfaces, wlan1, wireless,* se llenará los campos con la siguiente información:

- Modo: Bridge
- Banda: 5GHz-turbo, es decir IEEE 802.11g modificada
- Frecuencia portadora: 5500 GHz
- SSID (Set Service IDentifier): ruidogris
- Nombre del radio: Buenos Aires
- Lista de escaneo: 5175 – 5840, para regular el sistema a normas ecuatorianas
- Perfil de seguridad: wpa2BH
- Modo de frecuencia: manual, permite modificar las frecuencias de forma manual
- Modo de la antena: antenna a, permite escoger la salida de antena del radio R52Hn

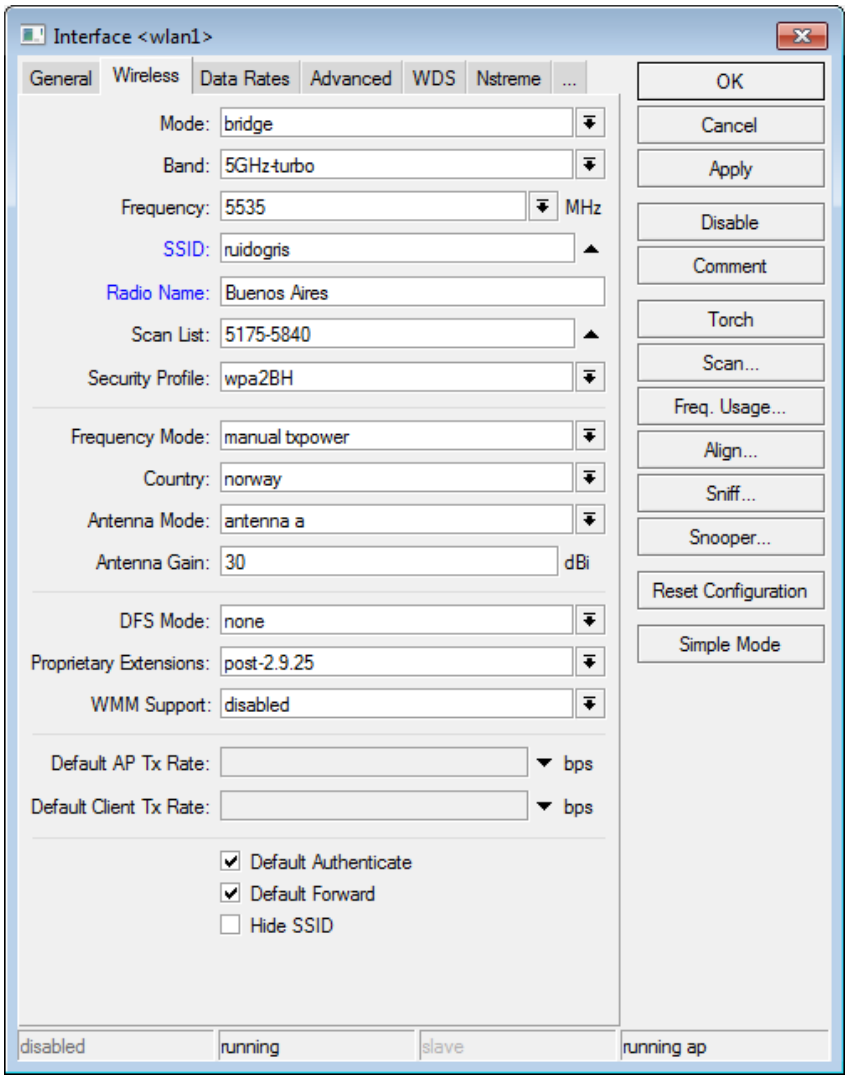


Figura 4.10 Configuración Interface inalámbrica master

La banda de frecuencias escogida es 5GHz-Turbo, que permite trabajar como el protocolo IEEE 802.11a pero usando canales de 40 MHz que incrementa significativamente el ancho de banda

En la configuración del equipo master es posible ocultar el SSID por seguridad, mediante la habilitación de la opción *Hide SSID*, esto hace que el equipo master no transmita el SSID en el paquete *beacon*[l]. Además, es posible habilitar un listado de equipos autorizados habilitando la opción *Default*

[l] **Beacon frame** en un paquete de administración de IEEE 802.11 para WLANs, el cual contiene información acerca de la red.

Authenticate, esto permite que los equipos registrados con sus direcciones MAC en la viñeta *Access List* puedan ser considerados seguros.

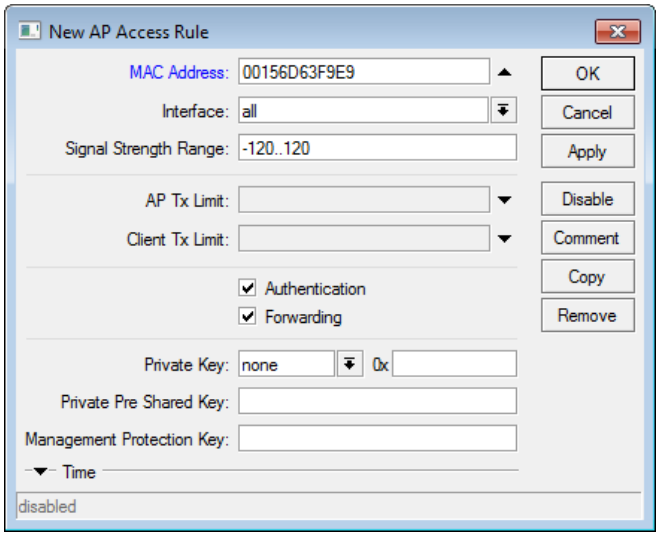


Figura 4.11 Autenticación del equipo

En la viñeta *Data Rates* se calibra el límite máximo de la velocidad de transmisión del enlace, se debe considerar que a mayor ancho de banda transmitido son mayores las posibilidades de errores ACK y esto significaría mayores errores en la transmisión. Para el enlace, según los valores obtenidos del estudio de factibilidad del enlace se puede usar la máxima capacidad del canal, por lo que se escogerá la opción *rates default*.

Dentro de la viñeta *Advanced* existe un parámetro importante que es el *Hardware Retries*, este parámetro permite regular las colisiones y evitar desconexiones del cliente hacia el equipo Master, para un óptimo funcionamiento en enlaces punto – punto este valor se sugiere configurarlo con valor 10[35], esto debido a que este parámetro permite controlar los intentos de comunicación entre estaciones y si el valor es bajo (0) el equipo no hará intentos de reconexión por lo tanto existe mayor posibilidad de perder la comunicación entre equipos, mientras que si el valor de *Hardware Retries* es alto (15) los intentos de reconexión son mucho mayores pero la velocidad de transmisión será más baja.

Adicionalmente, dentro de esta viñeta existen varios parámetros para estabilizar el enlace como son: *ACK Timeout, Noise Floor Threshold,*

Adaptative Noise Immunity, los cuales permiten calibrar parámetros como ruido de piso, inmunidad adaptativa al ruido en el caso de interferencia, etc, en tarjetas de radio que basan su chipset en Atheros AR5211[36].

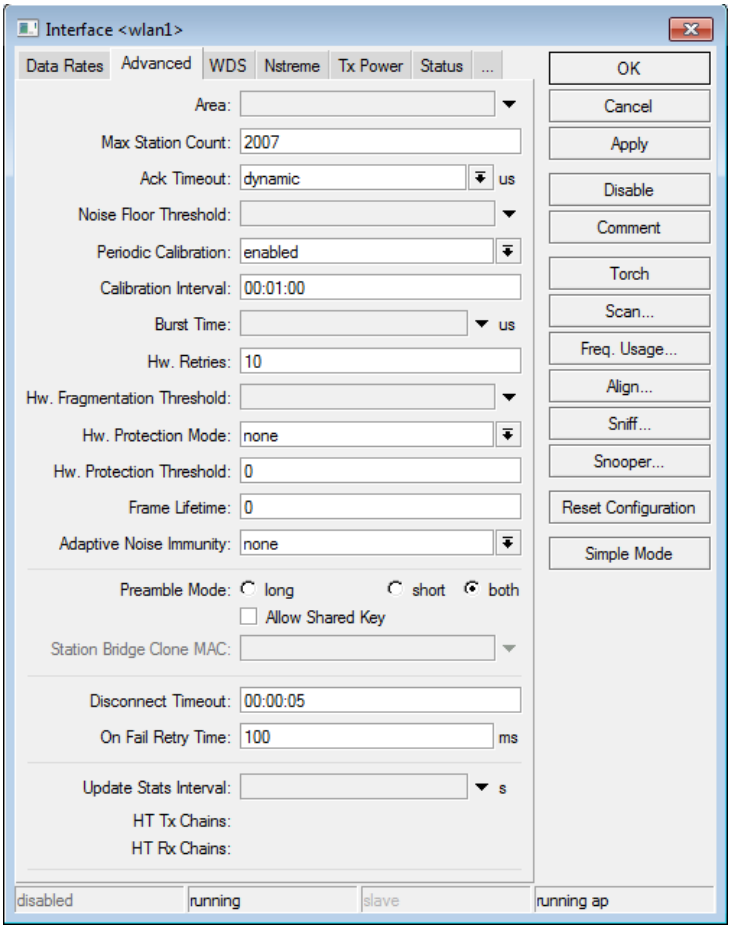


Figura 4.12 Configuración avanzada de la interface inalámbrica

En la viñeta *WDS* se habilita el *Wireless Distribution System*, esto permite que el enlace pueda funcionar con un bridge transparente, es decir puede permitir transitar tráfico encapsulado[l] como un equipo capa 2. Para el enlace se escogerá el modo *dynamic* y el default bridge hacia el bridge1, esto significa que el WDS está dirigido hacia un bridge que se creará posteriormente.

[l] **El encapsulamiento** es el proceso por el cual los datos que se deben enviar a través de una red se deben colocar en paquetes que se puedan administrar y rastrear

En la viñeta *Nstreme* se habilitará la opción *Nstreme,* este parámetro permite trabajar con una modulación inalámbrica propietaria MikroTik que mejora notoriamente el desempeño en los enlaces inalámbricos, habilitar esta opción es posible solo si se trabaja en todos los equipos con equipos RouterOS. Para el enlace se habilitará esta opción ya que los dos equipos que se dispone trabajan con RouterOS.

En la viñeta *TX Power* se escogerá la opción *TX Power Mode* en default, esto permite trabajar con la máxima potencia de salida de la tarjeta de radio que en este caso es 25 dB

4.5.2 CONFIGURACIÓN LA INTERFACE INALÁMBRICA WLAN1 EN EL NODO CERRO BLANCO

Este equipo tendrá una configuración similar al equipo de Buenos Aires, con la diferencia que este equipo al escoger el modo *station* trabajará como cliente o esclavo, esto significa que recibirá la información de funcionamiento del equipo master esto mediante paquetes *beacon* en los que se establecerá por ejemplo la frecuencia de la portadora, SSID, tipo de seguridad, etc.

La configuración de la interface inalámbrica será la siguiente:

En la viñeta *wireless*, dentro *de Interface/wlan1* se llenarán los campos con la siguiente información:

- Modo: Station WDS
- Banda: 5GHz-turbo, es decir IEEE 802.11g modificada
- Frecuencia portadora: 5500 GHz
- SSID (Set Service IDentifier): ruidogris
- Nombre del radio: Cerro Blanco
- Lista de escaneo: 5175 – 5840, para regular el sistema a normas ecuatorianas
- Perfil de seguridad: wpa2BH
- Modo de frecuencia: manual, permite modificar las frecuencias de forma manual
- Modo de la antena: *antenna* a, permite escoger la salida de antena del radio R52Hn

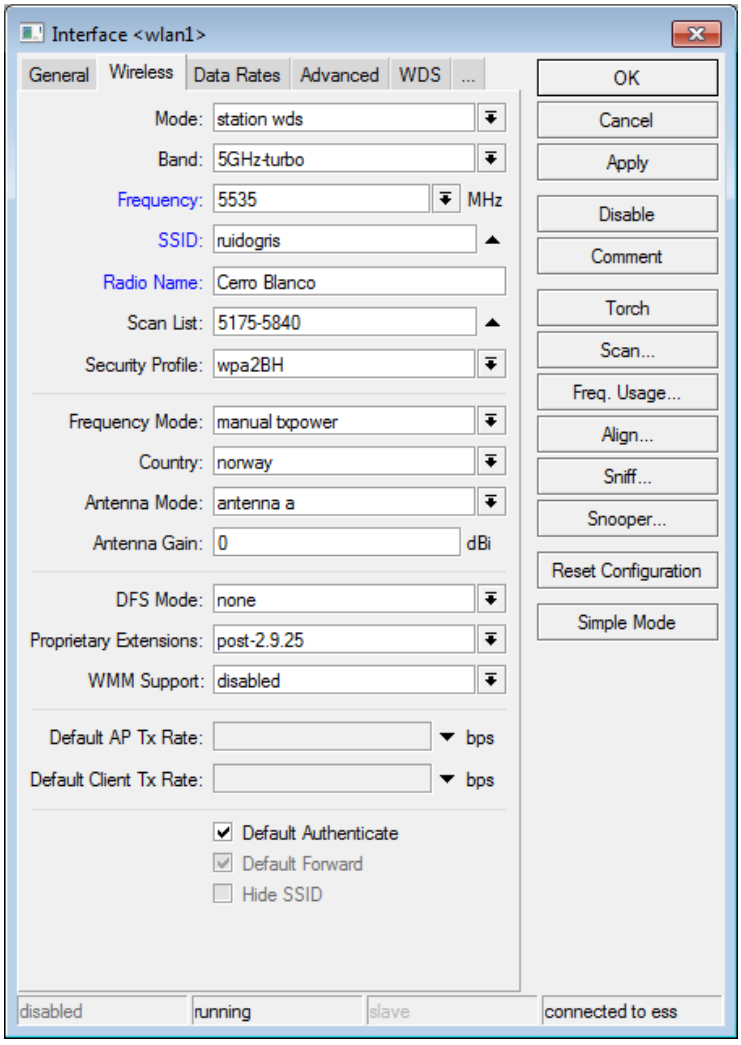


Figura 4.13 Configuración Interface inalámbrica cliente

En la viñeta *Data Rates* los valores escogidos no tendrán importancia ya que el equipo master administra estos valores, adicionalmente, en la viñeta *Advanced* se configurará el valor de *Hardware Retries* en 10, esto para evitar colisiones por ACK con el equipo Master. En la viñeta WDS al igual que el equipo master se escogerá la opción *WDS mode dynamic*, para permitir tráfico encapsulado. Por ultimo en la viñeta *Nstreme* se habilitará la opción Nstreme que permite trabajar con la modulación propietaria de MikroTik.

4.5.3 CREACIÓN DE PUENTES DE RED CAPA2

Finalmente se configurarán los dos equipos para que funcionen como puentes transparente *(transparent bridge).* Esto es necesario debido a que la

configuración por defecto de RouterOS asigna diferentes dominios de *broadcast* en sus interfaces (definición de ruteador). En este caso se requiere que el tráfico que maneja la interface inalámbrica del equipo sea la misma en la interface Ethernet, es decir que el equipo se maneje como un puente de red[I] que opera en capa 2.

Para crear un puente en RouterOS en el menú principal se escoge *Bridge,* dentro de la viñeta bridge se escoge el signo (+), y se configura los valores del bridge como el nombre, los valores de MTU (de ser necesario), y la habilitación ARP[II] *(Address Resolution Protocol).*

Adicionalmente dentro del Bridge es posible configurar el *STP (Spanning Tree),* el cual permite gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes, la configuración de la gestión de sistemas redundantes se analizará posteriormente.

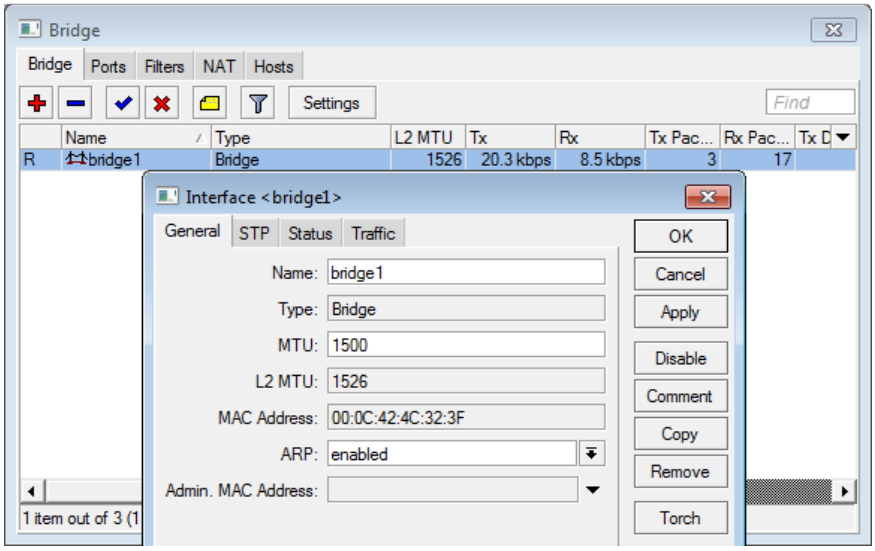


Figura 4.14 Configuración del Bridge

[I] **Puente** o **bridge** es un dispositivo de interconexión de redes de ordenadores que opera en la capa 2 (nivel de enlace de datos) del modelo OSI. Este interconecta dos segmentos de red (o divide una red en segmentos) haciendo el pasaje de datos de una red hacia otra, con base en la dirección física de destino de cada paquete.

[II] **ARP** Es un protocolo de nivel de red responsable de encontrar la dirección hardware (Ethernet MAC) que corresponde a una determinada dirección IP

Como paso final se asignarán los puertos que gestionará el bridge, para nuestro caso la interface inalámbrica y la interface Ethernet, para esto en la vinieta *Ports* se adicionará la interfaces *ether1* y *wlan1*.

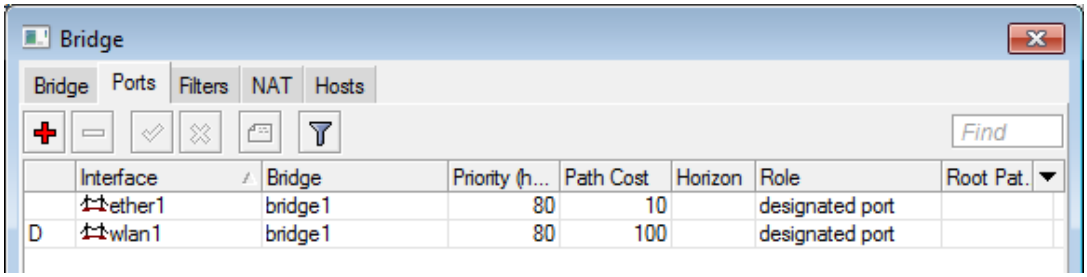


Figura 4.15 Asignación de puertos en el Bridge

4.5.4 PRUEBAS DE RADIO ENLACE

Dentro de RouterOS existen herramientas para verificación de un enlace inalámbrico o un host cercano a la interface Ethernet como son el Ping, *Traceroute, Torch, Bandwidth test*, entre otras que permiten la verificación de un óptimo funcionamiento de un equipo o un enlace.

Ping, es una herramienta de diagnóstico usado en networking que comprueba el estado de conexión de un host o varios equipos remotos mediante el envío de paquetes ICMP (*Internet Control Message Protocol)* de solicitud y respuesta. Mediante esta herramienta es posible determinar el estado de conexión de un equipo terminal, su velocidad y capacidad de tráfico hacia un host.

Traceroute, es una herramienta de diagnóstico de redes que permite seguir la pista de los paquetes que van desde un host (punto de red) a otro. Se obtiene además una estadística del RTT (Round-Trip delay Time), o latencia de red de esos paquetes, lo que viene a ser una estimación de la distancia a la que están los extremos de la comunicación.

Torch (Realtime Traffic Monitor), Es una herramienta de diagnóstico desarrollada por MikroTik, usada para el monitoreo de tráfico que va a través de una interface. Mediante esta herramienta es posible clasificar el tráfico por nombre de protocolo, dirección fuente, dirección destino, puerto.

Bandwidth Test, es una herramienta propia diseñada por MikroTik, que puede ser usada para monitorear el tráfico efectivo (throughput) hacia un ruteador remoto MikroTik.

4.6 CONFIGURACIÓN DE ENLACES REDUNDANTES MEDIANTE EL USO DEL PROTOCOLO *STP (SPANNING TREE).*

4.6.1 *SPANNING TREE*[37]

El *STP (Spanning Tree Protocol)* es un estándar utilizado en la administración de redes, basado en el algoritmo desarrollado por *Radia Perlman*, para describir como los puentes y conmutadores puedes comunicarse para evitar bucles en la red.

El protocolo STP automatiza la administración de la topología de la red con enlaces redundantes, la función principal del protocolo *spanning-tree* es permitir rutas conmutadas/puenteadas duplicadas sin considerar los efectos de latencia de los *loops*[l] en la red.

Al crear redes tolerantes a las fallas, una ruta libre de *loop* debe existir entre todos los nodos de la red. El algoritmo de *spanning tree* se utiliza para calcular una ruta libre de bucles Las tramas del *spanning tree*, denominadas unidades de datos del protocolo puente *(BPDU)*, son enviadas y recibidas por todos los switches de la red a intervalos regulares y se utilizan para determinar la topología del *spanning tree.*

4.6.1.1 Cómo funciona el protocolo STP:

El Protocolo *Spanning Tree* que trabaja a nivel de MAC, inicialmente construye un árbol de la topología de la red, comenzando desde la raíz (CORE). Uno de los dispositivos STP se convierte en la raíz después de haber ganado la selección, para ello cada dispositivo STP (router, switch, u otros)

[l] **Loop,** Un bucle o ciclo, en programación, es una sentencia que se realiza repetidas veces a un trozo aislado de código, hasta que la condición asignada a dicho bucle deje de cumplirse

desde el momento en que se enciende comienza a tratar,de convertirse en la raíz del árbol STP mediante el envío de paquetes de datos específicos denominados *BPDU (Bridge Protocol Data Unit)* a través de todos sus puertos. La dirección del receptor del paquete BPDU es una dirección de un grupo *multicast,* esto permite al paquete BPDU atravesar dispositivos no inteligentes como hubs y switches no STP.

Después de recibir el paquete BPDU desde otro dispositivo, el “puente” (Conmutador o switch) compara los parámetros recibidos con los propios y, dependiendo del resultado decide seguir o no intentando ser el nodo raíz. Una vez terminadas las elecciones el dispositivo con el Identificador de Puente con un valor más bajo será designado raíz. El Identificador de Puente es una combinación entre la dirección MAC del Puente y una prioridad del Puente predefinida. Si se identifica un solo dispositivo STP en la red, éste será la raíz.

La raíz Designada *(Designate Root Bridge)* no tiene ninguna responsabilidad adicional, tan solo es el punto de inicio desde el cual se comenzará a construir el árbol de la topología de la red. Para todos los demás Puentes en una red, STP define el Puerto raíz como el puerto más cercano al Puente raíz. Los demás puentes se diferencian con su Identificador (combinación de la MAC y la prioridad definida para ese puerto)

El Coste de la Ruta raíz *(Root Path Cost)* es también un valor significativo para las elecciones STP, comienza siendo una suma de los costes de las rutas: del puerto raíz del Puente dado y todos los costes de las rutas a los puertos raíz de los demás Puentes en la ruta hacia el Puente raíz

En adicción al Puente raíz principal STP define una entidad lógica denominada 'Puente Designado'. Este cargo también está sujeto a elección.

Una vez que se ha elegido el puente raíz *(root bridge)* el resto de switches deben elegir su puerto raíz *(*root port) en el cual solo debe haber uno por switch que es el puerto con menor coste hacia el puente raíz. El coste es un valor acumulativo de todos los enlaces hasta llegar al puente raíz. Cada enlace tiene un coste que se llama *path cost* y la suma de todos los costes de

todos los enlaces hasta llegar al puente raíz se llama *root path cost* y es el que se envía en el BPDU.

Ancho de banda	Costo STP
4 Mbps	250
10 Mbps	100
16 Mbps	62
45 Mbps	39
100 Mbps	19
155 Mbps	14
622 Mbps	6
1 Gbps	4
10 Gbps	2

Tabla 4.7 Valores de costos STP

El coste de *root path cost* se determina de la siguiente manera:

El bridge envía un BPDU con el root path cost a cero, ya que todos sus puertos están conectados directamente. Cuando el siguiente switch recibe esta BPDU, suma al *root path cost* el coste del puerto por donde ha recibido la BPDU. Este switch envía la BPDU con el nuevo valor del *root path cost*, y el proceso se repite según se reciba la BPDU a los switches, según cuan más alejados estén del *root bridge*

Es importante remarcar que el *root path cost* se incrementa cuando el switch recibe la BPDU y que si se calcula el *root path cost* manualmente en un esquema en necesario tenerlo presente al sumar el coste cuando entra en el switch nunca cuando sale. Cada switch almacena el mejor *root path cost* que ha recibido, por lo que si recibe uno mejor del que tiene almacenado guarda el nuevo y por tanto actualiza que su nuevo *root port* es el puerto por donde ha recibido el menor *root path cost*.

Una vez que se tiene el *root bridge* y el *root port* del resto de switches, estos deben elegir los *designated ports* (puerto designado). Si un un switch recibe una BPDU con menor *root path cost* asume que el

puerto del switch vecino es el *designated port*, por el contrario si la BPDU que recibe tiene un mayor *root path cost* asume que su puerto (por donde recibe la BPU) es el puerto designado.

Puede ocurrir que un switch reciba por varios puerto el mismo root cost path con lo cual hay un “empate” que hay que romper para ello STP tiene 4 condiciones para romper este empate:

1. El *root bridge* ID más bajo.
2. El *root path cost* más bajo hacia el root bridge.
3. El *bridge* ID más bajo del emisor.
4. El *port* ID más bajo del emisor.

4.6.1.2 Estados de STP

Cuando el STP está activo un puerto empieza en estado desactivado (*Disabled*) y pasa por ciertos estados hasta alcanzar el estado activo (*Forwarding*). Los estados son:

*Disabled**:*** Los puertos en administrativamente *shutdown* o por una condición de error están en estado *Disabled*. Este estado no forma parte de cambio de estados del STP.

*Blocking**:*** Cuando un puerto se inicializa comienza en estado *Blocking* para prevenir bucles. En este estado un puerto no puede ni recibir ni enviar nada ni aprende MACs solo recibe BPDUs para conocer el estado de otros switches. Además los puertos que se eliminan de la redundancia para evitar un bucle se ponen en este estado de *Blocking*.

Listening: Un puerto pasa del estado *Blocking* al estado *Listening* si el switch cree que este puerto puede ser un root o *designated port* y va camino de ser un puerto activo (*Forwarding*). En este estado (*Listening*) no puedo enviar o recibir tramas, pero ahora puede enviar y recibir BPDUs con lo que este switch participa activamente en el STP. Si el puerto pierde su estado de *root* o *designated* entonces vuelve al estado de *Blocking*.

*Learning**:*** Tras pasar en modo *Listening* durante un tiempo (llamado *Forward Delay*) el puerto puede pasar al estado *Learning*. Aún el puerto sigue sin poder

mandar o recibir tramas, sigue mandando BPDUs pero ahora el switch aprende MACs que añade a la tabla de MACs. Este estado da un poco de tiempo a que el switch se asiente.

Forwarding: Tras otro tiempo de *Forward Delay* el puerto pasa del estado *Learning* a *Forwarding*. En este estado el puerto es totalmente operativo, envía y recibe tramas, BPDUs y aprende MACs.

4.6.1.3 Temporizadores *(timers)* de STP

STP usa tres temporizadores *(timers)* para asegurarse que la red converge correctamente, estos son los siguientes:

Hello Time: Es el intervalo de tiempo entre cada BPDU de configuración que envía el *root bridge.* El *Hello Time* configurado en el *root bridge* determina el *Hello Time* de cada switch no *root* ya que estos reenvían las BPDUs que recibe del *root*. Aunque los switches no root tienen un *Hello Time* configurado localmente que se usa para temporizar los BPDUs TCN (cambio de topología). IEEE 802.1D especifica por defecto un *Hello Time* de 2 segundos.

Forward Delay: El intervalo de tiempo que un switch espera en los estados *Listening y Learning*. Por defecto son 15 segundos.

Max Age: El intervalo de tiempo máximo que un switch almacena una BPDU antes de descartarla. STP almacena la “mejor” copia de BPDU que ha recibido hasta que deja de recibir las BPDUs durante el periodo de tiempo especificado por *Max Age* en cuyo momento asume un cambio de topología y elimina el BPDU almacenado. Por defecto este valor es de 20 segundos.

4.6.1.4 Cambios de topología

Para anunciar un cambio en la topología actual de la red, los switches envían una BPDU TCN. Un cambio de topología ocurre cuando un switch pasa un puerto al estado *Forwarding* o cambia un puerto de los estados *Forwarding o Learning* al estado *Blocking* (o lo que es lo mismo un puerto cambia a UP o DOWN). El switch envía una BPDU TCN por su *root port* para que le llegue al *root bridge*. La BPDU TCN no lleva información sobre el cambio en sí solo que se ha producido un cambio. El switch no envía la BPDU TCN si el puerto ha sido configurado con el parámetro *PortFast.*

El switch continúa enviando BPDUs TCN cada intervalo *Hello Time*. Cuando el root bridge recibe el BPDU TCN envía la BPDU de configuración con el *flag* de TCN activo, lo cual hace que todos los switches acorten sus tiempos de memorización de MACs (que por defecto es 300 segundos) al tiempo de *Forward Delay* (que es por defecto 15 segundos).

4.6.1.5 Configuración de STP (Spanning Tree) con RouterOS

Para el análisis del protocolo RSTP (protocolo 802.1d), se usará el software libre de administración desarrollado por MikroTik llamado *The Dude*[38].

The Dude es un software libre utilizado para la gestión y administración de redes IT, permite analizar, visualizar, y gestionar a tiempo real por medio del monitoreo de servicios como: SMTP, POP3, HTTP, NNTP, PING, etc.

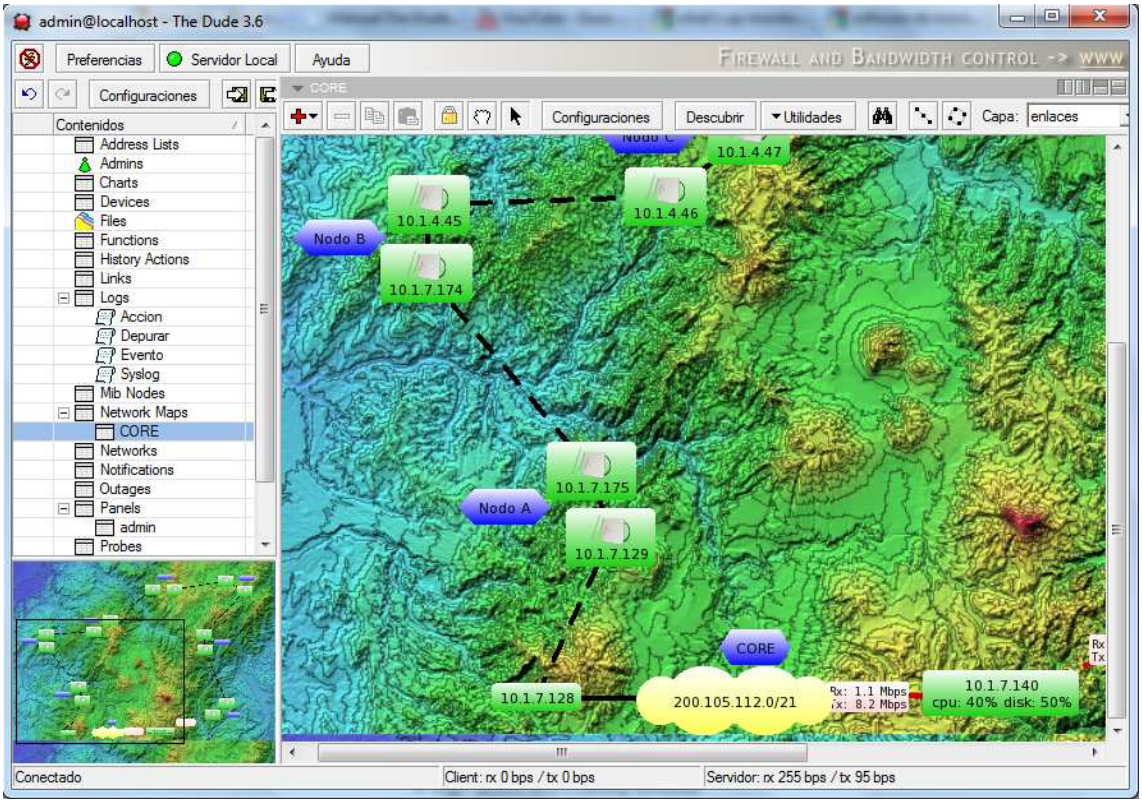


Figura 4.16 El Dude

Para el análisis del uso del protocolo RSTP con RouterOS se creará una red de *backbone* con siete nodos interconectados en topología en forma de anillos conectados de forma inalámbrica con equipos MikroTik y sistema operativo RouterOS. El *core* STP será un switch L7 marca D-Link el cual tiene

la capacidad de gestionar STP, y será el equipo más cercano al router BGP (*Border Gateway Protocol)* es decir, el segundo equipo de acceso a Internet de la empresa.

Se ha elegido que el equipo de administración del *spannig tree* sea un *switch* debido a que en los otros puertos se conectará el *backbone* de la red con STP y los routers de frontera BGP, esto para tener redundancia tanto en el *backbone* como en la salida a Internet a través de los equipos BGP que administrarán el sistema autónomo (AS).

Los equipos MikroTik configurados para la gestión del STP tendrán configurados direcciones IP privadas, esto ya que no es necesario que estos equipos sean vistos por Internet. A continuación se definen las direcciones IP de los equipos que gestionarán el STP.

NODO	Dirección IP
ROOT	10.1.7.169
CORE	10.1.7.128
CORE	10.1.7.140
Nodo A	10.1.7.129
Nodo A	10.1.7.175
Nodo B	10.1.7.174
Nodo B	10.1.4.45
Nodo C	10.1.4.46
Nodo C	10.1.4.47
Nodo D	10.1.4.48
Nodo D	10.1.4.50
Nodo E	10.1.4.51
Nodo E	10.1.7.59

Tabla 4.8 Nodos gestionados por STP

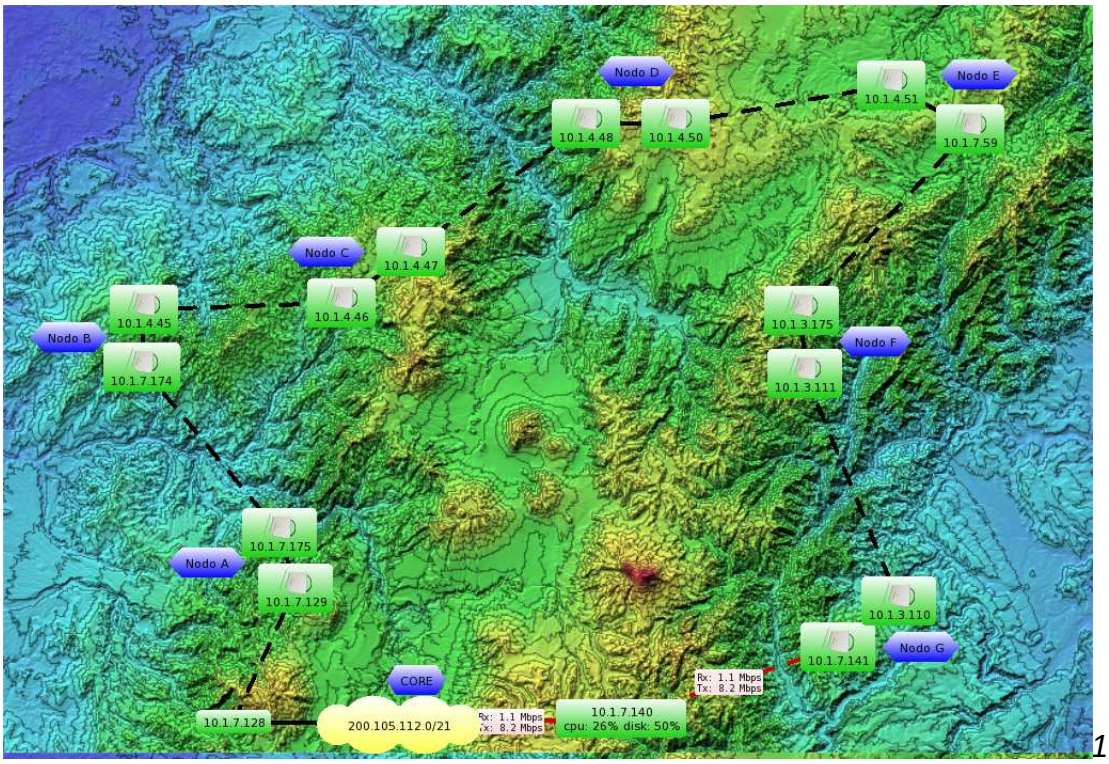


Figura 4.17 Ubicación geográfica de los nodos

El protocolo RSTP nos permitirá una gestión dinámica del tráfico que atraviesa cada nodo de *backbone* en el caso de averías en uno de los nodos.

4.6.1.5.1 Configuración del spannig tree en el switch D-Link equipo ROOT

El equipo utilizado es un D-Link modelo DES-3326SR, este equipo tiene la capacidad de gestionar varios parámetros como *Forwarding, QoS, Vlans*, 802.1x[39], etc.

La configuración del switch D-Link se la realiza mediante *browser,* es decir ingresando la dirección IP http://10.1.7.169:6222 en un navegador. Una vez que se ha ingresado en el equipo se busca la configuración *Spanning Tree.*

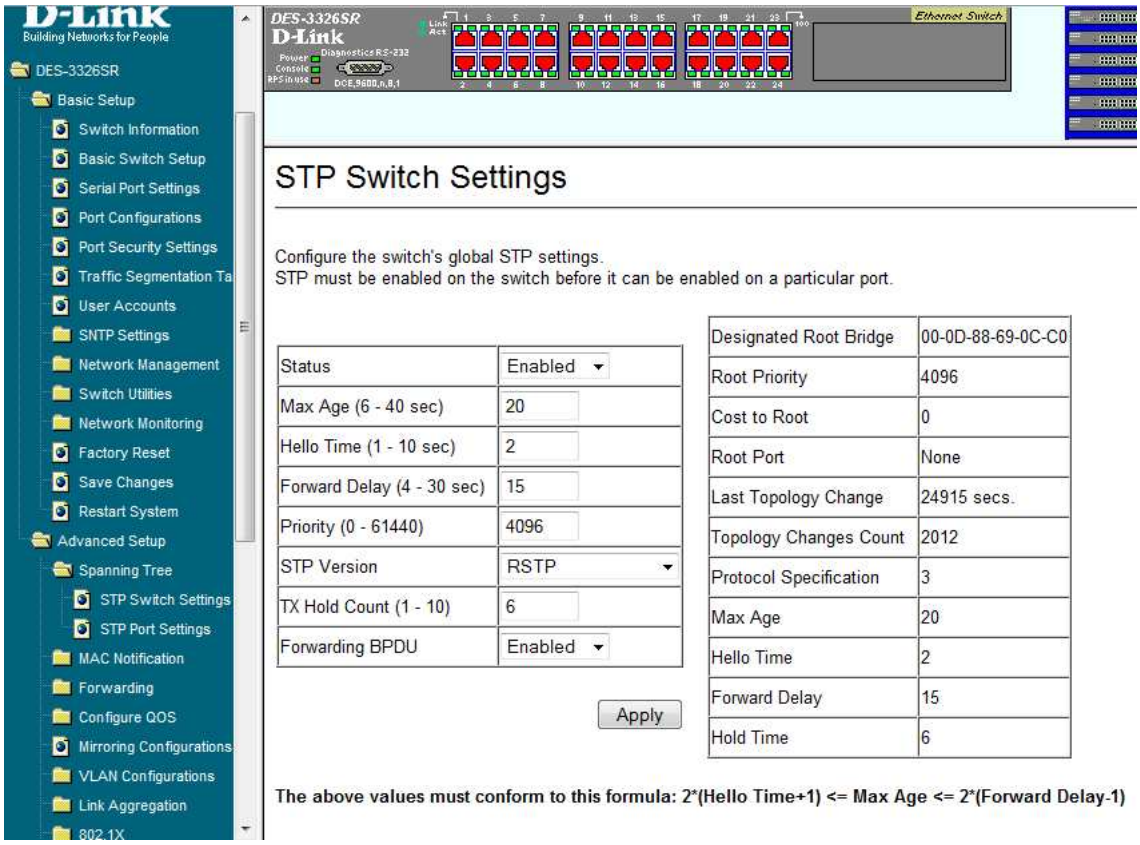


Figura 4.18 Configuración equipo root spanning tree.

Dentro del *STP Switch Settings* se configura varios parámetros:

- *max age,* este valor determina la máxima cantidad de tiempo (segundos) que el switch podría esperar a recibir un paquete BPDU antes de reconfigurar el STP, para este caso el tiempo utilizado es 20 segundos
- *Hello Time,* este parámetro gestiona el intervalo de tiempo de transmisión de mensajes por el equipo *root*, se usará 2 segundos.
- *Forward Delay,* este parámetro gestiona la máxima cantidad de tiempo en segundo que el equipo *root* puede esperar antes de cambiar de estado.
- *Priority,* este parámetro es un valor numérico entre 0 y 61440 y es usado para determinar el equipo root, el puerto root, y el puerto designado, equipo con la más alta prioridad será el equipo root. Para el ejemplo se usará 4096
- *TX Hold Count,* este parámetro gestiona el número máximo de paquetes *Hello* transmitidos por intervalo

Ahora es necesario configurar los puertos del switch que van a adminsitrar el STP.

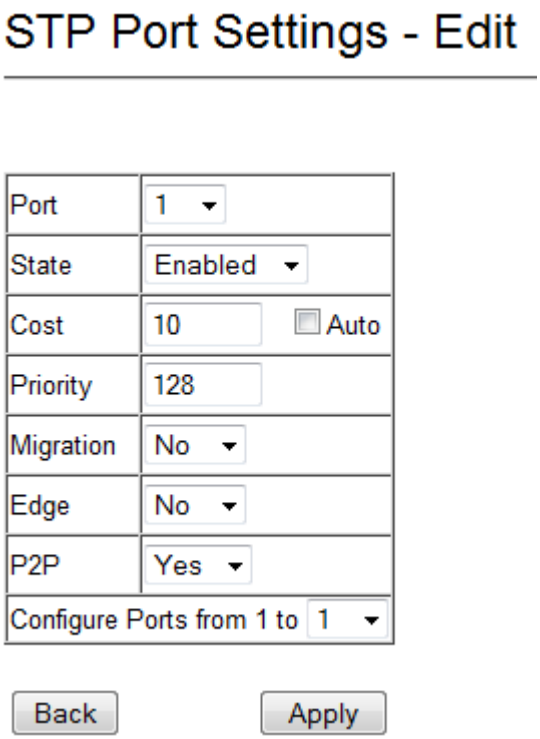


Figura 4.19 Configuración de puertos STP en el switch D-link

Los puertos del switch pueden ser configurados individualmente para administrar el STP. Los parámetros que se deben configurar son:

- *Port,* elige el puerto a configurar.
- *State,* Habilita o deshabilita que el puerto gestione el *spanning tree protocol.*
- *Cost,* este parámetro define una métrica[I] que indica el costo relativo de envió de paquetes al puerto especificado, los valores más bajos tienen

[I] **Métrica**. En el campo de la ingeniería del software una **métrica** es cualquier medida o conjunto de medidas destinadas a conocer o estimar el tamaño u otra característica de un software o un sistema de información, generalmente para realizar comparativas o para la planificación de proyectos de desarrollo. Un ejemplo ampliamente usado es la llamada métrica de punto función.

la mayor probabilidad de realizar en envío de paquetes. En la configuración del equipo este valor se configurará en 10 esto permitirá este puerto ser el root, será el equipo con el menor costo y administrará el *spanning tree.*

- *Priority,* el valor de priority puede ser 0 a 240. El número más bajo elige el puerto *root*. El valor escogido es de 128.

Ahora es necesaria la configuración del resto de equipos que serán parte del *backbone* y gestionarán el spanning tree.

El restante de los equipos que componen el *backbone* y gestionarán el *spanning tree* son RouterBoards MikroTik con sistema operativo RouterOS, por lo que la configuración del *spanning tree* será similar en todos los casos.

Para habilitar el *spannig tree* con RouterOS el router debe tener configurado un bridge, este bridge permitirá comunicarse a todos los equipos de la red en capa 2 por lo tanto todos tienen la misma jerarquía a nivel de rutas, además que de esta forma se facilita el redireccionamiento STP en el caso de que existan cambios en la topología de la red.

Para configurar el STP en un equipo con RouterOS se busca la viñeta *bridge* del menú principal, una vez creado el *bridge* se busca la viñeta STP dentro del *bridge* se escoge el modo del protocolo, en este caso se elegirá rstp (*rapid spanning tree protocol*)[40], y se configurará la prioridad, para este caso se elegirá 8000.

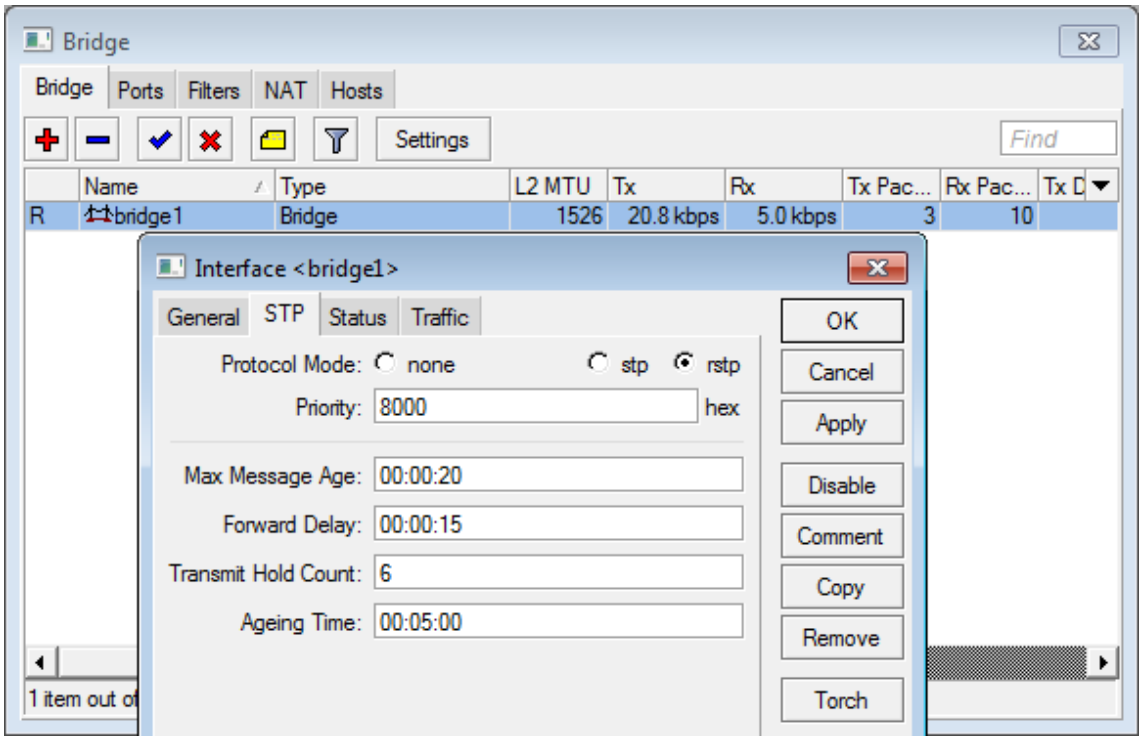


Figura 4.20 Configuración RouterOS spannig tree

El equipo raíz (*root*) D-Link 3326, tiene una prioridad de 4096 y el resto de equipos tendrá configurado el *spanning tree* con prioridad de 8000. En la sumatoria de prioridades de cada equipo revisará cual su prioridad y enviará un BPDU con su prioridad y comparará con la que el recibe, de esta forma cada equipo sabrá que el de mayor prioridad es el D-Link 3326, en el caso de existir una falla en el bucle cada equipo tiene el registro de cuál es el equipo root del STP.

Para verificar el funcionamiento del STP se puede verificar los registros de cambio de topología del switch D-link 3326 de esta manera:

Switch History

Displays the log of switch events with the newest event at the top.

Index	Time	Log Text
8333	2011/01/18 17:10:42	Successful login through Web (Username: d3326)
8332	2011/01/18 17:09:41	Successful login through Web (Username: d3326)
8331	2011/01/18 17:07:26	Successful login through Web (Username: d3326)
8330	2011/01/18 17:07:24	Login failed through Web (Username: Anonymous)
8329	2011/01/18 10:16:04	Topology changed
8328	2011/01/18 10:15:14	Topology changed
8327	2011/01/18 10:08:43	Topology changed
8326	2011/01/18 10:07:52	Topology changed
8325	2011/01/18 10:02:53	Port 24 link up, 100Mbps FULL duplex
8324	2011/01/18 10:02:52	Topology changed
8323	2011/01/18 10:02:51	Port 24 link down
8322	2011/01/18 07:39:59	Topology changed
8321	2011/01/18 07:39:29	Topology changed

Figura 4.21 Registro de cambios de topología STP

En este registro indica cuando existió un cambio de topología en la red, adicionalmente mediante la ayuda de programas de administración de red como *The Dude, Nagios*[41]*, What's Up*[42]*,* etc., que permita la configuración SNMP (*Simple Network Management Protocol*)[43] para conocer el funcionamiento de la red, un posible cambio de topología de la red y conocer un falla en la red.

4.7 CONFIGURACIÓN DE UN PUNTO DE ACCESO INALÁMBRICO Y UN ROUTER DE FRONTERA INALÁMBRICO CON ROUTEROS.

Los equipos RouterBoard modelo: RB433,RB 433AH,RB493, RB493AH, RB800, tienen licencia para trabajar como puntos de acceso inalámbrico. Estos equipos permiten la integración de tarjetas de radio miniPCI como interface inalámbrica, con los protocolos 802.11a/b/g/n

Para configurar un equipo como punto de acceso se ingresa al menú principal y se busca *Wireless*, dentro de *Wireless* se busca la interface y dentro de la interface se busca la viñeta *Wireless*, y el parámetro *mode* configura el equipo como: punto de acceso inalámbrico (*AP Bridge*), puente (*bridge*), *station* (estación inalámbrica), estación pseudobridge (*station pseudobridge*), estación WDS (station WDS). El resto de parámetros son configurados de forma similar a un bridge como fue revisado en el capítulo 4.4.2.

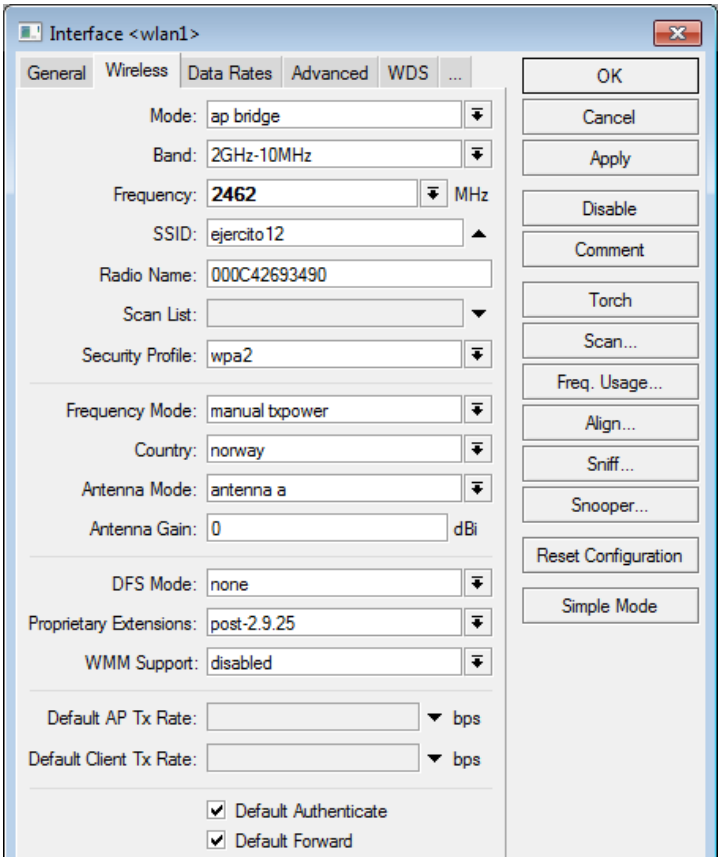


Figura 4.22 Configuración como AP

Para un mejor control del ancho de banda se configurará los valores de *Data Rates,* este parámetro permite configurar la negociación del ancho de banda que los CPE' (*Customer Premises Equipments*) se conectarán.

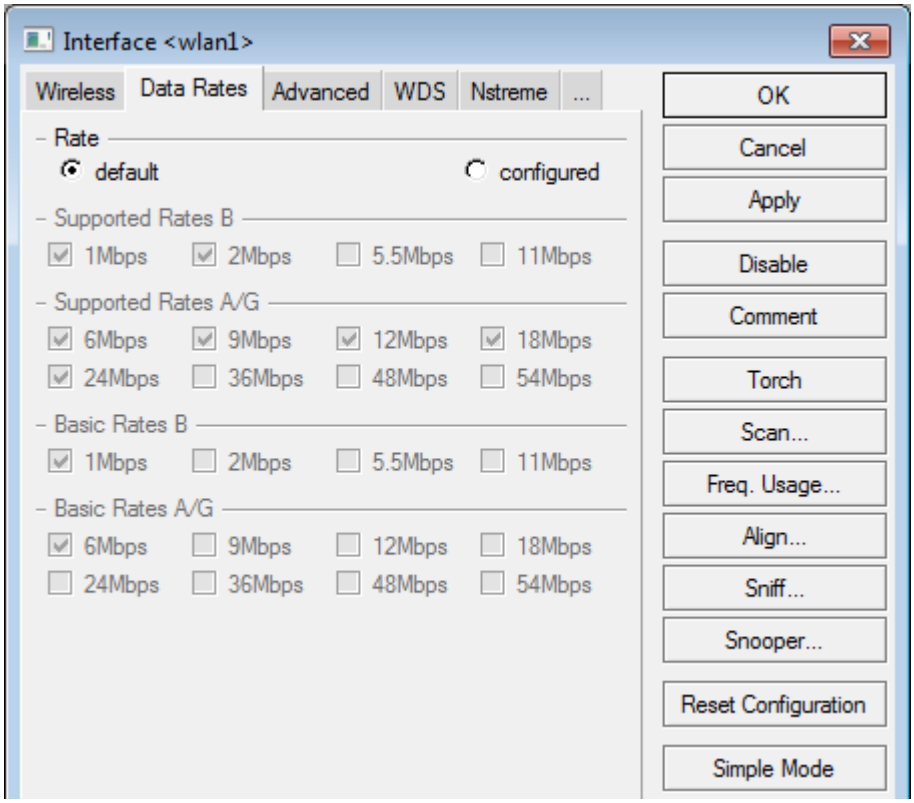
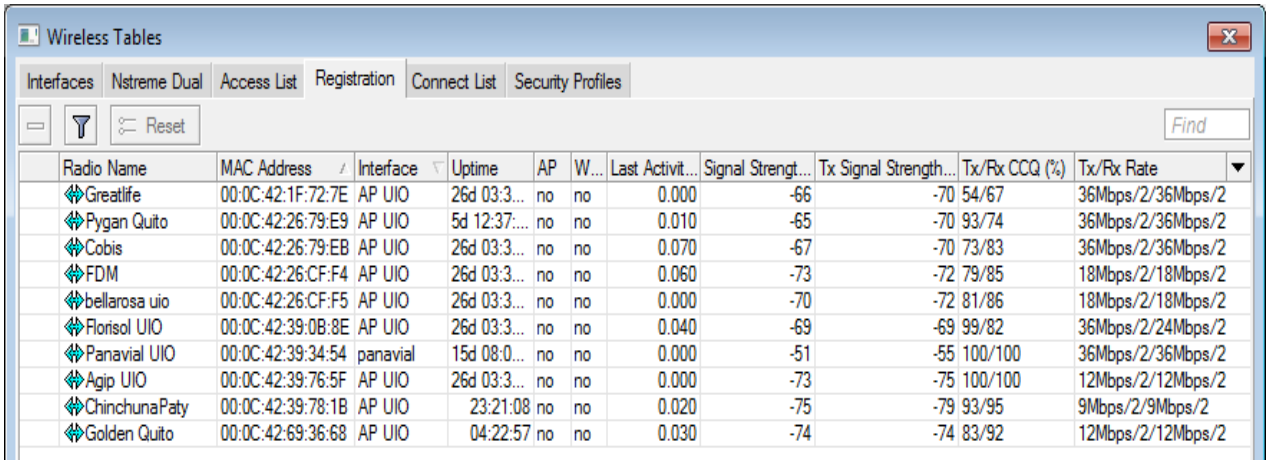


Figura 4.23 Configuración de Data Rates AP

Cuando se han conectado equipos CPE's al punto de acceso se puede verificar los valores de enlace de cada enlace en la viñeta *registration*



Radio Name	MAC Address	Interface	Uptime	AP	W...	Last Activit...	Signal Strengt...	Tx Signal Strength...	Tx/Rx CCQ (%)	Tx/Rx Rate
Greatlife	00:0C:42:1F:72:7E	AP UIO	26d 03:3...	no	no	0.000	-66	-70	54/67	36Mbps/2/36Mbps/2
Pygan Quito	00:0C:42:26:79:E9	AP UIO	5d 12:37:...	no	no	0.010	-65	-70	93/74	36Mbps/2/36Mbps/2
Cobis	00:0C:42:26:79:EB	AP UIO	26d 03:3...	no	no	0.070	-67	-70	73/83	36Mbps/2/36Mbps/2
FDM	00:0C:42:26:CF:F4	AP UIO	26d 03:3...	no	no	0.060	-73	-72	79/85	18Mbps/2/18Mbps/2
bellarosa uio	00:0C:42:26:CF:F5	AP UIO	26d 03:3...	no	no	0.000	-70	-72	81/86	18Mbps/2/18Mbps/2
Florisol UIO	00:0C:42:39:0B:8E	AP UIO	26d 03:3...	no	no	0.040	-69	-69	99/82	36Mbps/2/24Mbps/2
Panavial UIO	00:0C:42:39:34:54	panavial	15d 08:0...	no	no	0.000	-51	-55	100/100	36Mbps/2/36Mbps/2
Agip UIO	00:0C:42:39:76:5F	AP UIO	26d 03:3...	no	no	0.000	-73	-75	100/100	12Mbps/2/12Mbps/2
ChinchunaPaty	00:0C:42:39:78:1B	AP UIO	23:21:08	no	no	0.020	-75	-79	93/95	9Mbps/2/9Mbps/2
Golden Quito	00:0C:42:69:36:68	AP UIO	04:22:57	no	no	0.030	-74	-74	83/92	12Mbps/2/12Mbps/2

Figura 4.24 Tabla de clientes registrados

En el caso de un CPE (*Customer Premises Equipment*)[44], la configuración de la interface inalámbrica es bastante similar que el AP, es decir los parámetros son similares con excepción de *Mode* que se configurará como *station* para que funcione como CPE, es decir que el CPE administrará dos redes diferentes, a un lado WAN y al otro lado LAN cada interface con una dirección IP diferente.

Además es posible configurar el equipo de forma transparente es decir como un bridge, para esto se elige la opción de *station pseudobridge*, esta configuración permite al equipo trabajar de forma transparente es decir como un equipo capa 2.

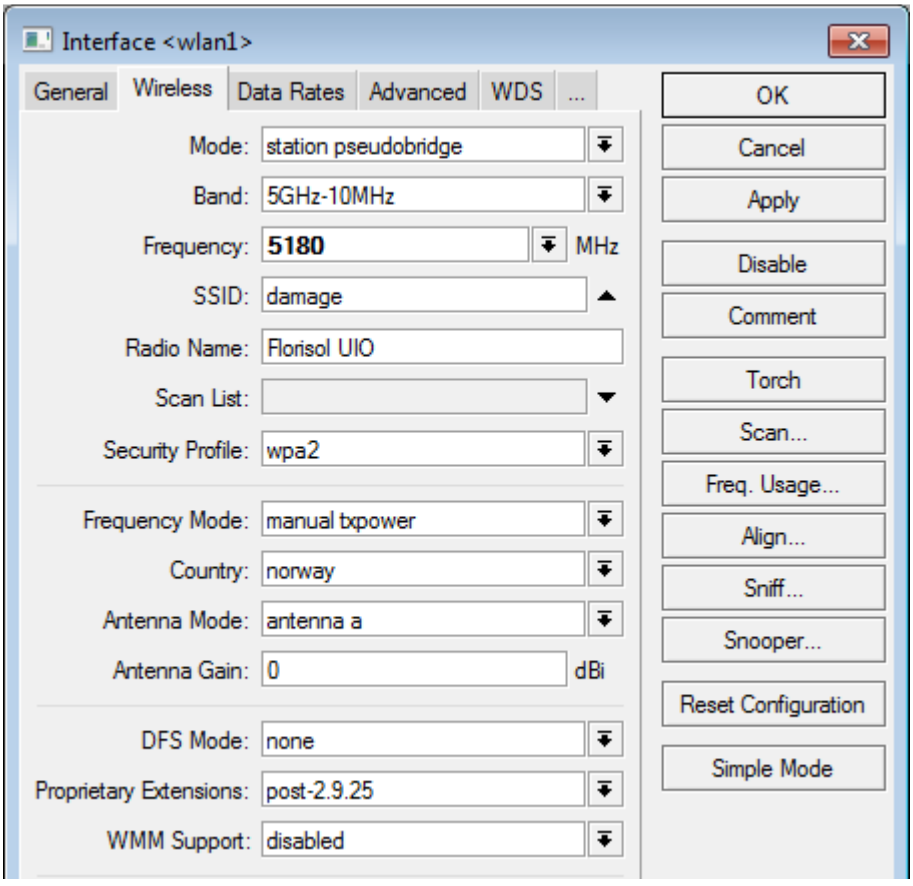


Figura 4.25 Configuración Wireless CPE

Existe una relación directamente proporcional entre la calidad de la señal de un enlace y el ancho de banda soportado, es decir si existe una buena calidad de señal de enlace el ancho de banda que puede soportar el enlace será mucho mayor, por el contrario, si la calidad de señal de un enlace no es muy buena y se exige del enlace un mayor ancho de banda este puede sufrir

pérdidas de paquetes y por tanto el deterioro de la comunicación. Para evitar estos problema es recomendable realizar un análisis de cuanto ancho de banda debe soportar el enlace y configurar el *data rates* en el máximo valor requerido.

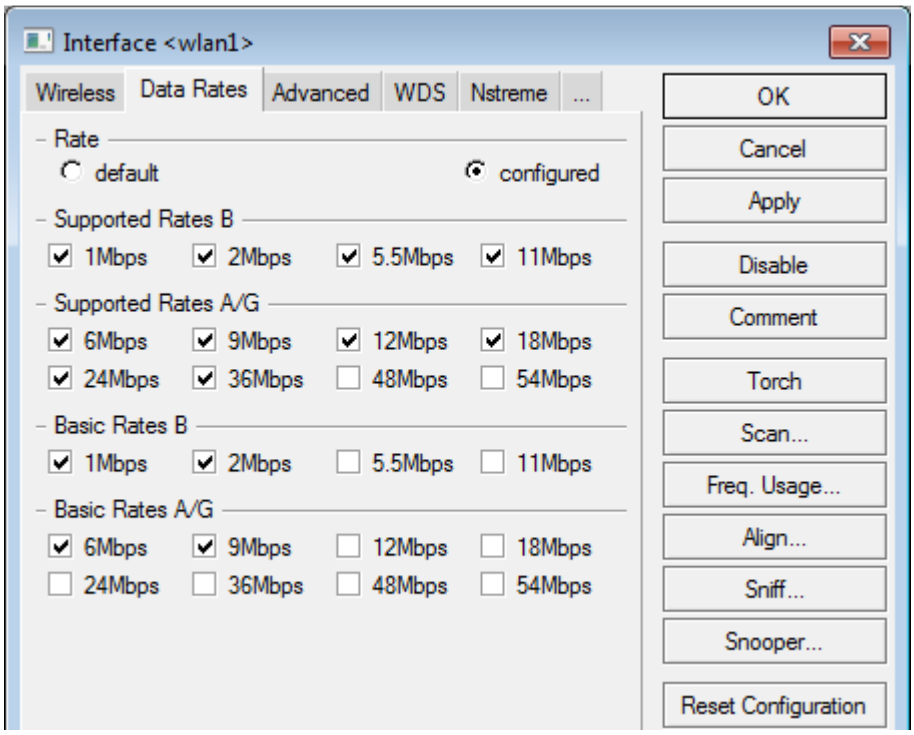


Figura 4.26 Data Rates CPE

Con esta configuración de *Data Rates*, el radiotransmisor usa la misma potencia de salida con un tráfico menor de paquetes, eso hace que existan menos pérdidas de paquetes, por lo tanto un mejor desempeño del enlace.

En la opción *Registration* de la interface *Wireless* del *Access Point* es posible verificar la calidad del enlace de cada CPE y su capacidad de ancho de banda, además de un parámetro CCQ propio de MikroTik que permite evaluar en porcentaje la calidad del enlace y al ancho de banda soportado.

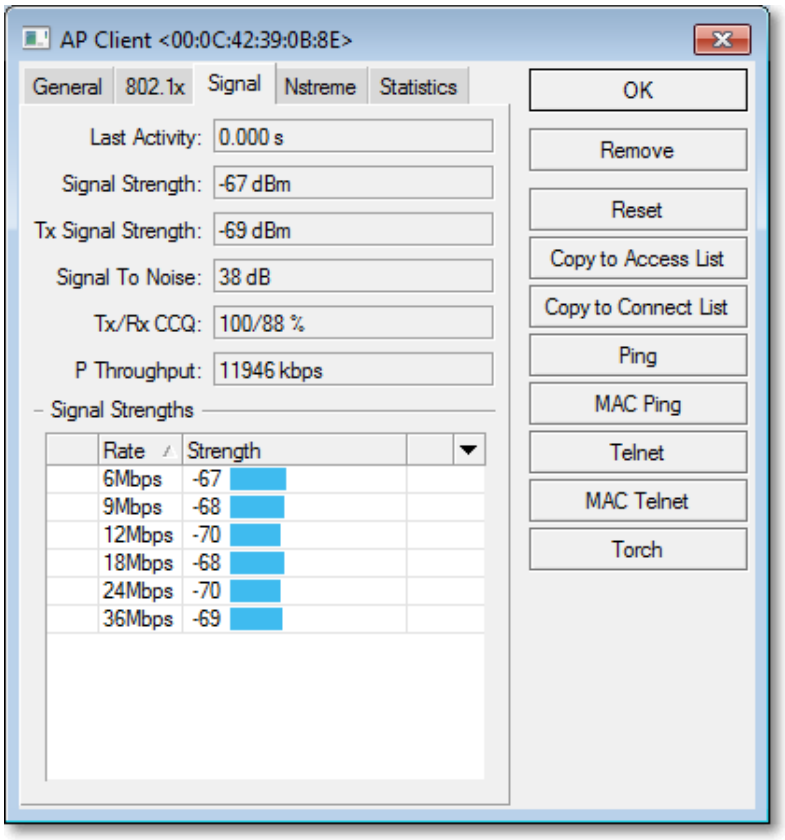


Figura 4.27 Valores de señal del CPE en el AP

Esta configuración puede ser la más utilizada en un WISP, y es el uso de un equipo como CPE y que además permita ser un router de frontera entre su red de *backbone* y la red interna del cliente. El equipo debe estar en capacidad de conectarse de forma inalámbrica al nodo y administrar la red nateada (NAT) del cliente con posibles: redireccionamientos de puertos, firewall, control de ancho de banda, configuración de VPN's, túneles etc., y su configuración se realizará como fue revisado en capítulos anteriores.

4.8 MONITOREO Y GESTIÓN DE LA RED MEDIANTE *THE DUDE*

Existen varios programas usadas para la administración, monitoreo y gestión de la una red, entre los principales se puede nombrar a *Nagios, What's Up*, *The Dude*, etc.

The Dude es una herramienta gratuita desarrollada por la empresa MikroTik para la administración de un entorno de red de telecomunicaciones.

Este software permite el escaneo de equipos IP conectados en la red, con la especificación de subredes, dibujando un mapa de la red, monitoreando servicios de cada equipo de la red y ejecutando acciones basadas en cambios de estados de los equipos.

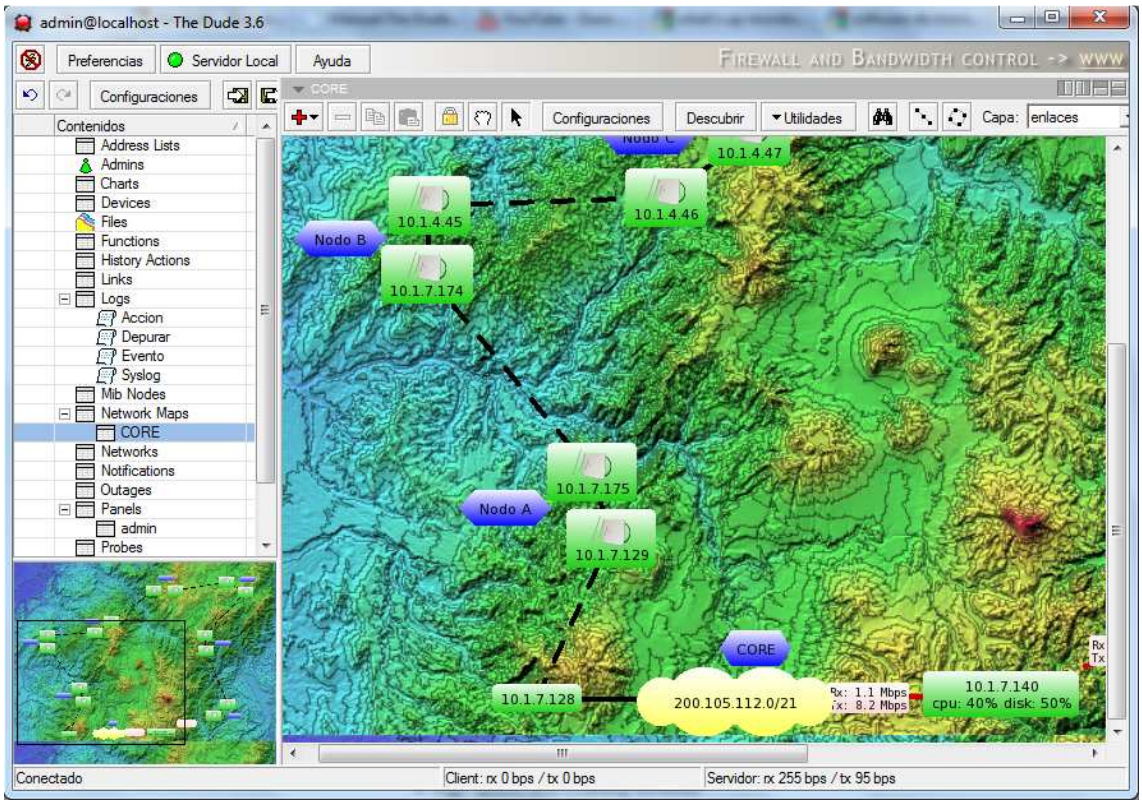


Figura 4.28 The Dude

4.8.1 REQUERIMIENTOS E INSTALACIÓN DEL SISTEMA PARA EL USO DE *THE DUDE*

Dude puede correr sobre cualquier sistemas a partir de *Windows 2000,* además puede correr sobre Linux Wine y MacOS

Para correr de forma óptima *The dude* requiere de un procesador de al menos un Pentium IV, capacidad de memoria RAM de 2 Gigabytes, y un disco duro de 20 Gigabytes, esto permitirá una rápida gestión y monitoreo de una red de al menos unos 2000 dispositivos.

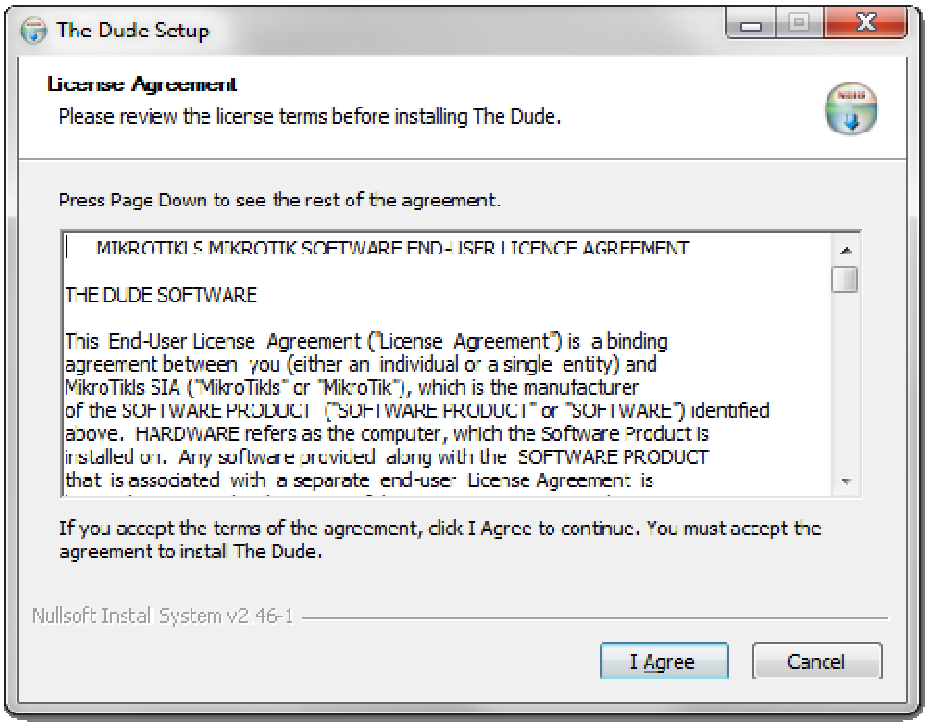


Figura 4.29 Instalación de The Dude

Una vez realizada la instalación, este se abrirá de forma automática, en el primer ingreso al programa se conectará al servicio *localhost* y presentará una pantalla que permite descubrir las redes conectadas a este equipo.

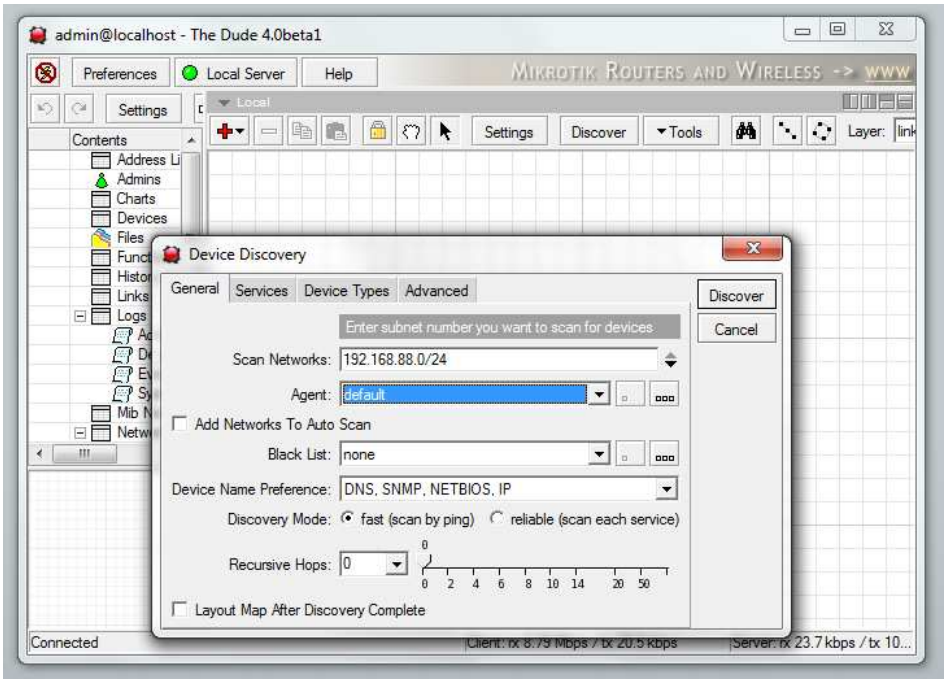


Figura 4.30 Discovery DUDE

La principal ventana del dude puede mostrar varias pantallas llamadas *Panes*, cada pantalla puede mostrar opciones diferentes como puede ser, un mapa de la red, propiedades de un dispositivo, historial de dispositivos caídos, etc.

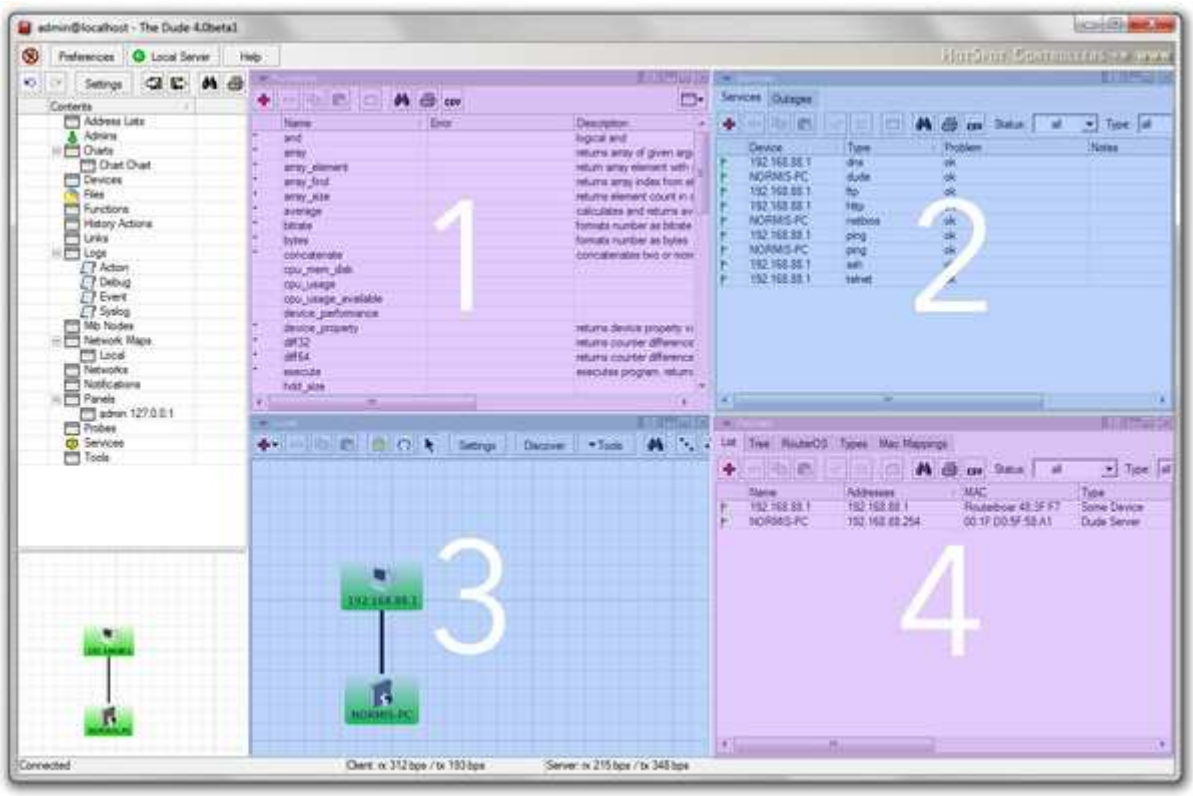


Figura 4.31 Pantalla principal del Dude

En el lado izquierdo de la pantalla existe un menú principal, este menú provee acceso a varias pantallas. Se puede dar clic sobre un ítem para abrir en la pantalla principal una pantalla relacionada con el ítem elegido, o abrir múltiples pantallas, también es posible arrastrar un ítem hacia el menú principal.

Los contenidos del menú principal son:

- *Address list* – Lista de direcciones IP para ser usado en la lista de bloqueo y otros lugares
- *Admins* – Lista de usuario que pueden acceder al servidor DUDE

- *Charts* – Configura gráficos basados sobre cualquier fuente de datos en el mapa por ejemplo gráficos obtenidos por SNMP de un dispositivo
- *Devices* – Lista de todos los equipos mostrados y mapas que contenga la red
- *Files* – Lista de archivos cargados al servidor como imágenes de fondo del mapa de red o sonidos
- *Functions* – Funciones que pueden ser incluida como scripts y configuraciones avanzadas
- *History Actions* – Historial de tareas realizadas por el administrador como añadir o remover equipos.
- Links – Lista de encadenamientos en todos los mapas
- *Logs* – Registro de estado de cada dispositivo. Dude incluye también un servidor de registro del sistema y puede recibir los registro de otros equipos.
- *MIB nodes* – Información acerca de MIB's *(Management Información Base)*[45]
- *Network maps*- Todos los mapas registrados en el sistema
- *Networks* – Lista de todos los segmentos de sobre un mapa
- *Notifications* – Diferentes formas de alerta del administrador
- *Panels* – Permite configurar ventanas separadas para usar con múltiples monitores.
- *Probes* – Son los responsables del tipo de respuesta del equipo a monitorear, como puede ser ICMP o SNMP.
- *Tools* – Configura las herramientas que pueden ser usadas sobre cada dispositivo como puede ser conectar un dispositivo mediante telnet, winbox, telnet, ftp, etc.

4.8.2 CONFIGURACIÓN DE PANTALLA PRINCIPAL DEL DUDE

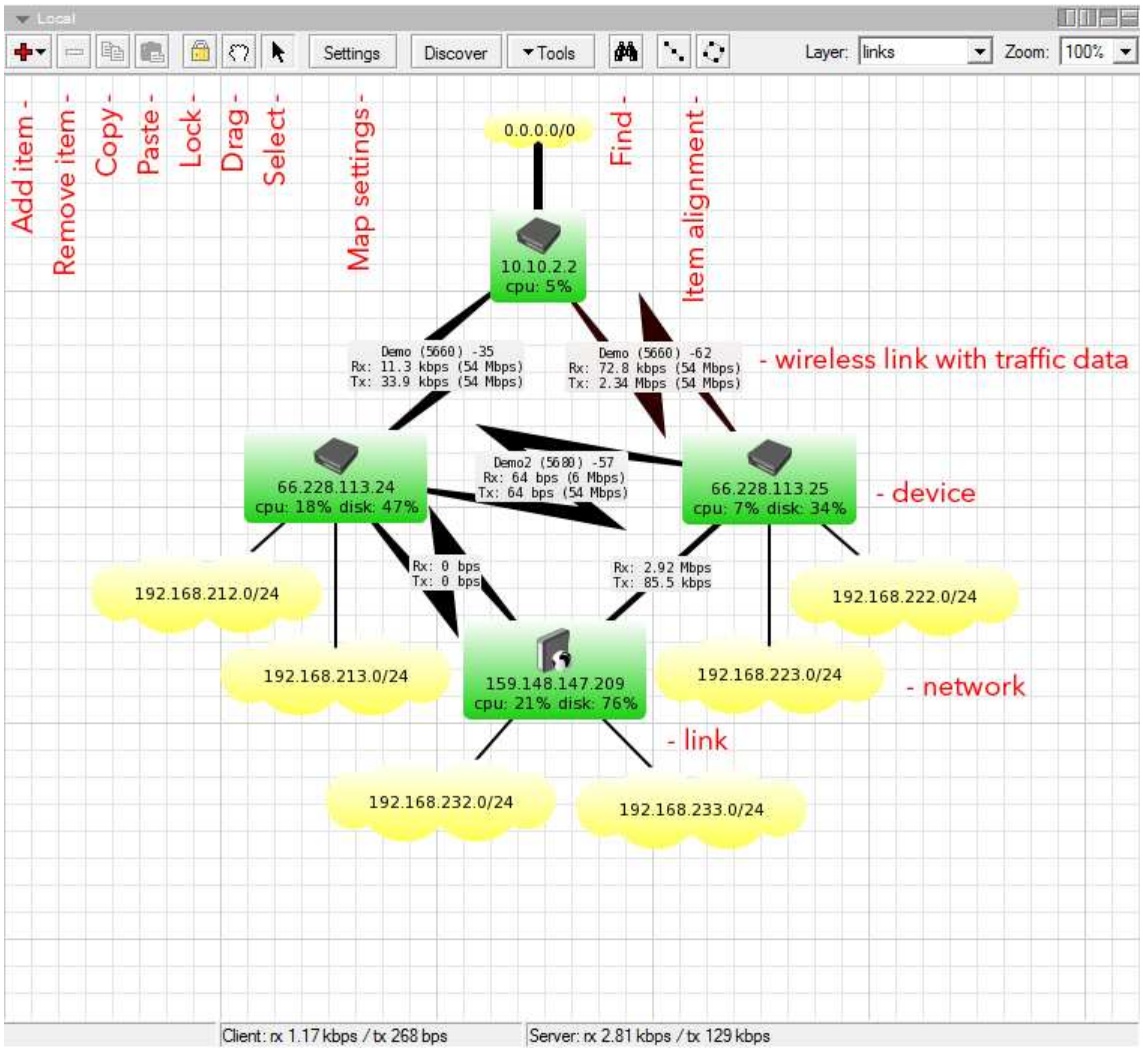


Figura 4.32 Configuración de pantalla principal del Dude.

Lista de los botones principales:

- *Add ítem* – Permite añadir manualmente un dispositivo al mapa, entre las opciones tenemos:
  - *Device* – Cualquier equipo que pueda responder mediante ICMP o SNMP.
  - *Network* – Un icono de una nube de red ayuda a visualizar de forma organizada diferentes mapas
  - *Submap* – Los submapas permite crear accesos rápidos a otros mapas para ayudar a expandir un mapa principal con jerarquías
  - *Static* – Un icono general que puede representar cualquier cosa.

- *Link* – Permite encadenar equipos que se encuentran juntos y están conectados

- *Remove Item* – Borra cualquier ítem del mapa
- *Copy and paste* – Habilita la copia de ítems a otros mapas
- *Lock* – Ayuda a asegurar movimientos accidentales de los ítems sobre el mapa
- *Drag* – Para mapas extensos el *drag* permite arrastrar ítems entre mapas.
- *Select* – Modo de selección, para ítems seleccionados en el mapa
- *Map settings* – Abre la configuración de mapas actuales
- *Tools* – permite la exportación de iconos de mapas
- *Find* – Abre la búsqueda de ítems en una pantalla
- *Item aligment* – selecciona múltiples ítem, y elige una forma de organización en hilera o en círculo.

4.8.3 CONFIGURACIÓN DE UN NUEVO DISPOSITIVO

Para agregar un nuevo dispositivo en la pantalla principal se busca el signo (+), y se busca dispositivo.

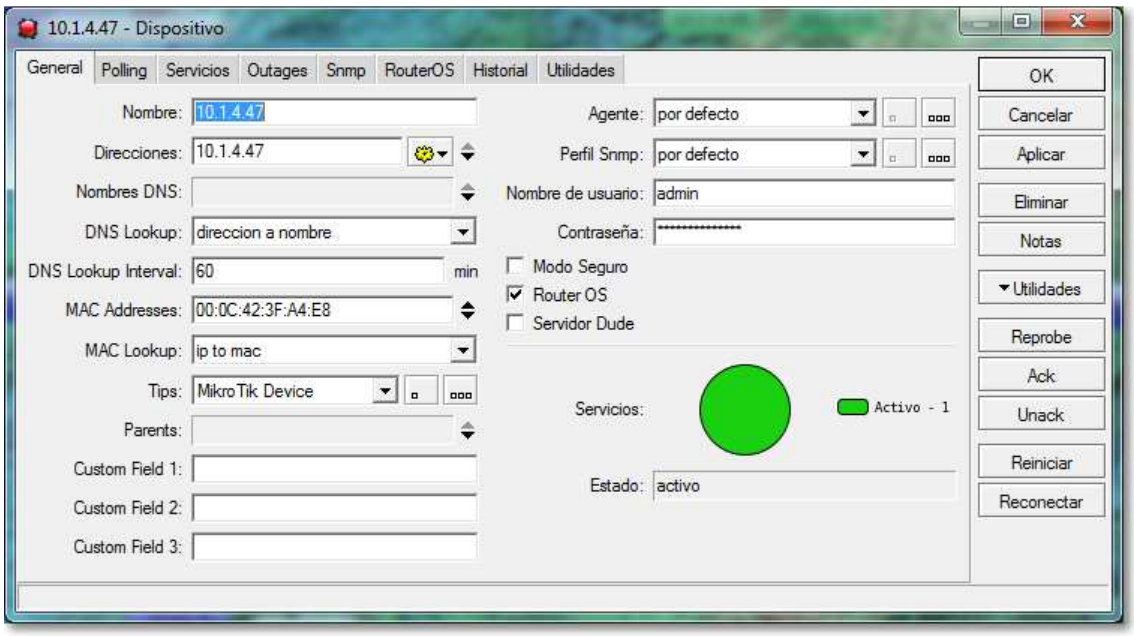


Figura 4.33 Propiedades del dispositivo.

En los campos se ingresa la información relacionada con el dispositivo, como es la dirección IP, nombre del dispositivo, Servidor DNS, tipo de

dispositivo, en el caso de tener un orden jerárquico es posible la configuración de sus parientes superiores. En la viñeta servicios se escoge el tipo de servicio que va a monitorear al dispositivo como puede ser Ping (ICMP), telnet, SNMP, http, etc.

En el caso de que el dispositivo a ser monitoreado tenga como sistema operativo RouterOS, el Dude puede monitorear a través del SNMP directamente las interfaces del dispositivo, y realizar modificaciones del mismo. Además crea un gráfico de las pruebas ICMP con los tiempos de latencia del dispositivo.

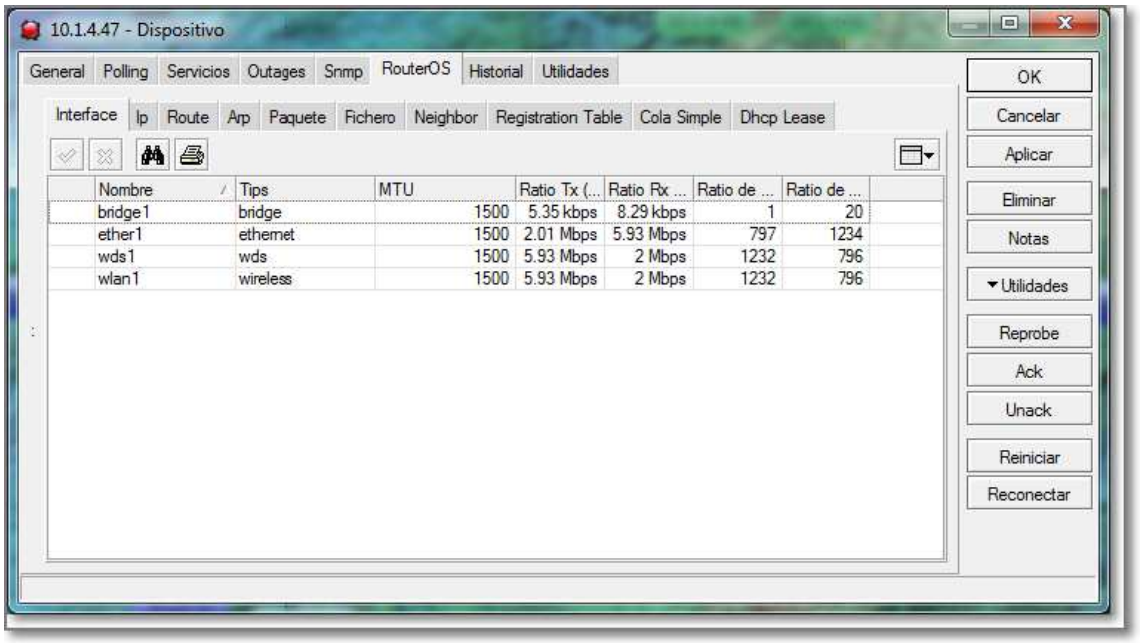


Figura 4.34 Administración de RouterOS con Dude

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

- La investigación de nuevas alternativas en equipamiento y tecnología para la infraestructura de una red de telecomunicaciones, considerando las prestaciones y su relación costo beneficio es un factor fundamental para el crecimiento o la implementación de una empresa de telecomunicaciones. Este proyecto abre la posibilidad a una nueva alternativa rentable en equipos de telecomunicaciones como es MikroTik.
- Una eficaz administración y la facilidad en la gestión de una red de telecomunicaciones dependen esencialmente de las herramientas administrativas que los dispositivos de la red incorporen, estas herramientas deben permitir detectar problemas a tiempo y su solución debe ser lo más rápida e intuitiva posible.
- El buen diseño de un enlace de *backbone* va permitir el crecimiento y una mejor planificación de la infraestructura de la red de una empresa de telecomunicaciones, además ayuda a mejorar la gestión de su tráfico y la evaluación de posibles alternativas a problemas de respaldos y redundancias.
- El mejoramiento de equipo tecnológico de una empresa de telecomunicaciones no debe significar necesariamente una gran inversión para la empresa, sino la oportunidad analizar nuevas alternativas para el mejoramiento de la administración de la red de la empresa.
- Una buena infraestructura para una empresa de telecomunicaciones garantiza la estabilidad de una empresa en el mercado, pues esta no dependerá del uso de última milla de otras empresas además de poder administrar su ancho de banda a su conveniencia.

5.2 RECOMENDACIONES

- Antes de iniciar una inversión en nuevo equipo tecnológico es recomendable estudiar las alternativas que ofrece el mercado, evaluando su disponibilidad y el alcance del soporte técnico que ofrece la empresa proveedora de equipos posterior a la implementación de los enlaces.
- Se debe analizar cuáles son los requerimientos de uso de ancho de banda de un enlace y su posible crecimiento, con el fin de formular respuestas a mediano y a largo plazo, a fin de no requerir nueva inversión en un plazo menor al evaluado.
- Es importante la capacitación continua del personal técnico de campo en aspectos relacionados con el manejo de nuevos equipos y nueva tecnología
- Se deben manejar programas constantes que permitan evaluar el desempaño de la red de telecomunicaciones a fin de evitar posibles saturamientos del ancho de banda que una red maneja
- Una red de telecomunicaciones con un buen sistema de redundancia permite al administrador gestionar problemas a tiempo real y con una mínima afectación para el usuario final.

BIBLIOGRAFÍA

#	TEMAS
[1]	*Clusters* http://es.wikipedia.org/wiki/Cluster_de_computadores
[2]	*Backhaul* http://en.wikipedia.org/wiki/Backhaul_%28telecommunications%29
[3]	*RouterOS* http://download.MikroTik.com/what_is_RouterOS.pdf
[4]	*RouterBoard* http://download.MikroTik.com/what_is_routerboard.pdf
[5]	*Hotspot* http://es.wikipedia.org/wiki/Hotspot
[6]	*Customers MikroTik* http://www.MikroTik.com/ourcustomers.php
[7]	*Características MikroTik* http://wiki.MikroTik.com/wiki/Manual:RouterOS_features
[8]	*Firewall* MikroTik Libro Learn RouterOS de Dennis Burgess, pág 137
[9]	*Routing Mikrotik* http://wiki.MikroTik.com/wiki/Manual:RouterOS_features
[10]	*Wireless MikroTik* Libro Learn RouterOS de Dennis Burgess, pág 214
[11]	*Nstreme* http://wiki.MikroTik.com/wiki/Enlaces_Inal%C3%A1mbricos_con_RouterOS#Mejorando_el_desempe.C3.B1o_del_enlace:_Nstreme
[12]	*Control de ancho de banda* Libro Learn RouterOS de Denniss Burgess, pag 246
[13]	*Licenciamiento MikroTik* http://wiki.MikroTik.com/wiki/New_Policy_Spanish
[14]	*Modelos RouterBoard* http://download.MikroTik.com/what_is_routerboard.pdf
[15]	*Manejo de Paquetes del sistema RouterOS* Libro Learn RouterOS de Dennis Burguess, pag 61
[16]	*Filtros Capa 7* http://l7filter.sourceforge.net/layer7protocols/protocols/msnmessenger.pat
[17]	*Comunicaciones Inalámbricas* Libro 802.11® Wireless Networks: The Definitive Guide, O'Reilly. Matthew Gast
[18]	http://standards.ieee.org/getieee802/download/802.11-2007.pdf
[19]	Libro 802.11® Wireless Networks: The Definitive Guide, O'Reilly. Matthew Gast, pág. 158

[20]	802.11 Libro 802.11® Wireless Networks: The Definitive Guide, O'Reilly. Matthew Gast pág. 165
[21]	802.11 Libro 802.11® Wireless Networks: The Definitive Guide, O'Reilly. Matthew Gast pág. 167
[22]	*Problema de nodos ocultos* 802.11 Wireless Networks The Definitive Guide Oreilly
[23]	802.11 Wireless Networks The Definitive Guide Oreilly cap 7, pág 124
[24]	*Protocolo 802.11 Legacy* http://standards.ieee.org/getieee80
[25]	*802.11g* Libro 802.11 Wireless Networks The Definitive Guide O'Reilly
[26]	*802.11d* http://searchmobilecomputing.techtarget.com/definition/80211e
[27]	*802.11e* http://en.wikipedia.org/wiki/IEEE_802.11e-2005
[28]	*802.11h* http://ieeestandards.galeon.com
[29]	*Multiplexación por división espacial* Libro 802.11 Wireless Networks The Definitive Guide O'Reilly, pag. 203
[30]	*Características RouterOS* http://www.routerboard.com/pricelist/download_file.php?file_id=202
[31]	*Configuraciones de radio* MikroTik RouterOS Refman 3.0 manual de usuario
[32]	*SSID* http://es.wikipedia.org/wiki/SSID
[33]	*Zona de Fresnel* http://es.wikipedia.org/wiki/Zona_de_Fresnel
[34]	*Ganancia de antenas* Sistemas de comunicaciones electrónicas Wayne Tomasi Cap 10
[35]	*Hardware Retries* http://forum.MikroTik.com/viewtopic.php?f=2&t=21231
[36]	*Atheros AR5211* http://wiki.MikroTik.com/wiki/Manual:Interface/Wireless
[37]	http://www.decom-uv.cl/~mferrand/cursos/redes/spanningtree.pdf
[38]	*The Dude* http://wiki.MikroTik.com/wiki/Manual:The_Dude
[39]	*802.1x* http://es.wikipedia.org/wiki/IEEE_802.1X

[40]	*RSTP* http://en.wikipedia.org/wiki/Rapid_Spanning_Tree_Protocol#Rapid_Spanning_Tree_Protocol_.28RSTP.29
[41]	*Nagios* http://www.nagios.org/
[42]	*What's Up* http://www.whatsupgold.com/
[43]	*SNMP* http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol
[44]	*CPE* http://es.wikipedia.org/wiki/Customer_Premises_Equipment
[45]	*MIB's* http://es.wikipedia.org/wiki/Management_Information_Base

Anexos

Anexo 1

MikroTik

RouterBOARDS

Anexo 2

MikroTik RADIOS

Anexo 3

MikroTik RouterOS

[1] http://es.wikipedia.org/wiki/Cluster_de_computadores
[2] http://en.wikipedia.org/wiki/Backhaul_%28telecommunications%29
[3] http://download.MikroTik.com/what_is_RouterOS.pdf
[4] http://download.MikroTik.com/what_is_routerboard.pdf
[5] http://es.wikipedia.org/wiki/Hotspot
[6] http://www.MikroTik.com/ourcustomers.php
[7] http://wiki.MikroTik.com/wiki/Manual:RouterOS_features
[8] Libro Learn RouterOS de Dennis Burgess, pag 137
[9] http://wiki.MikroTik.com/wiki/Manual:RouterOS_features
[10] Libro Learn RouterOS de Dennis Burgess, pág 214
[11]http://wiki.MikroTik.com/wiki/Enlaces_Inal%C3%A1mbricos_con_RouterOS#Mejorando_el_desempe.C3.B1o_del_enlace:_Nstreme
[12] Libro Learn RouterOS de Denniss Burgess, pag 246
[13] http://wiki.MikroTik.com/wiki/New_Policy_Spanish
[14] http://download.MikroTik.com/what_is_routerboard.pdf
[15] Libro Learn RouterOS de Dennis Burguess, pag 61
[16] http://l7-filter.sourceforge.net/layer7-protocols/protocols/msnmessenger.pat
[17] Libro 802.11® Wireless Networks: The Definitive Guide, O'Reilly. Matthew Gast
[18] http://standards.ieee.org/getieee802/download/802.11-2007.pdf
[19] Libro 802.11® Wireless Networks: The Definitive Guide, O'Reilly. Matthew Gast pág 158

[20] Libro 802.11® Wireless Networks: The Definitive Guide, O'Reilly. Matthew Gast pág 165

[21] Libro 802.11® Wireless Networks: The Definitive Guide, O'Reilly. Matthew Gast pág 167

[22] 802.11 Wireless Networks The Definitive Guide Oreilly
[23] 802.11 Wireless Networks The Definitive Guide Oreilly cap 7, pág 124
[24] http://standards.ieee.org/getieee80
[25] Libro 802.11 Wireless Networks The Definitive Guide O'Reilly
[26] http://searchmobilecomputing.techtarget.com/definition/80211e
[27] http://en.wikipedia.org/wiki/IEEE_802.11e-2005
[28] http://ieeestandards.galeon.com
[29] Libro 802.11 Wireless Networks The Definitive Guide O'Reilly, pág. 203
[30] http://www.routerboard.com/pricelist/download_file.php?file_id=202
[31] MikroTik RouterOS Refman 3.0 manual de usuario.
[32] http://es.wikipedia.org/wiki/SSID
[33] http://es.wikipedia.org/wiki/Zona_de_Fresnel
[34] Sistemas de comunicaciones electrónicas Wayne Tomasi Cap 10
[35] http://forum.MikroTik.com/viewtopic.php?f=2&t=21231
[36] http://wiki.MikroTik.com/wiki/Manual:Interface/Wireless
[37] http://www.decom-uv.cl/~mferrand/cursos/redes/spanningtree.pdf
[38] http://wiki.MikroTik.com/wiki/Manual:The_Dude
[39] http://es.wikipedia.org/wiki/IEEE_802.1X
[40]http://en.wikipedia.org/wiki/Rapid_Spanning_Tree_Protocol#Rapid_Spanning_Tree_Protocol_.28RSTP.29
[41] http://www.nagios.org/
[42] http://www.whatsupgold.com/
[43] http://es.wikipedia.org/wiki/Simple_Network_Management_Protocol
[44] http://es.wikipedia.org/wiki/Customer_Premises_Equipment
[45] http://es.wikipedia.org/wiki/Management_Information_Base