Índice

Introducción **3**
Metodología **6**
Resultado y discusión **8**
Estudio bibliográfico de Mikrotik RouterOS 8
Características principales 8
Características de ruteo 8
Características del RouterOS 9
Calidad de servicio (QoS) 9
Tipos de colas 9
Colas simples 9
Árboles de colas 9
Interfases del RouterOS 10
Herramientas de manejo de red 10
Estudio descriptivo de la empresa Royaltech 11
Router CBA 13
Sub-red Administración 15
Sub-red Ventas 17
Sub-red Producción 19
Sub-red Hotspot 20
Sub-red Servidores 21
Diseño de la implementación virtualizada de la red. 22
Instalación de Mikrotik RouterOS 22
Logueo al Mikrotik 26
Backup y Restore de Configuración 29
Backup de la configuración. 29
Restore de la configuración. 31
Definición y configuración de interfases. 32
Asignación de nombres a las interfases 32
Definición de Vlans 39
Asignación de Direcciones IP´s a las interfases 42
Definimos UPnP para las interfases: 47
Configuración Pools de Direcciones de IP 49
Definir DNS 51
Nat Masquerade para todas las redes 52
Configuración Servidor DHCP 53
Asignación de direcciones de ip fijas a partir de direcciones MAC. 58
Configuración Servidor - Cliente NTP: 60
Servidor NTP 60
Cliente NTP 60
Servidor y Cliente PPPoE 63
Configuración Servidor PPPoE 63
Configuración Cliente PPPoE: 65
Servidor – Cliente PPTP 68
Configuración Servidor PPTP: 68
Configuración Cliente PPTP 71

Servidor Web Proxy 79
Bloqueo Pornografía 86
Bloqueo paginas que brinden el servicio de Web Messenger 88
Bloqueo del Live Messenger A Través del Proxy 90
Bloqueo de páginas que brinden webmail 91
Bloqueo descarga directa de archivos MP3 y AVI 92
Bloqueo descarga directa de archivos RAR, ZIP, EXE 93
Bloqueo Archivos RAR 93
Bloqueo Archivos ZIP 94
Bloqueo Archivos EXE 94
Balanceo de carga 95
Control de ancho de banda 105
Asignación de ancho de banda por sub red 105
Traffic Shaping de (P2P) 108
Liberación del ancho de banda fuera del horario de trabajo 114
Firewall 118
Bloqueo de los P2P para redes de ventas y producción 118
Bloqueo del cliente MSN Live Messenger 120
Redireccionamiento de puertos 124
Puerto 80 WEB 124
Puerto 110 POP3 125
Puerto 25 SMTP 126
Puerto 1723 PPTP 127
Descartar conexiones inválidas 130
Aceptar conexiones establecidas 131
Acepta Trafico UDP 132
Acepta icmp Limitados 133
Descarta excesivos icmp 134
Descarta el resto de las conexiones externas 135
Configuración Hot Spot 137
Servidor de SNMP 157
Configuración Servidor SMNP 158
Servidor Radius 163
Configuración Servidor Radius 163
Configuración MySQL 166
Configuración dialup admin 167
Configuración servidor - cliente Jabber 174
Servidor Jabber 174
Cliente Jabber 175
Sniffing de Paquetes 182
Instalación Ntop 182
Instalación Wireshark 185
Conclusión 196
Bibliografía 197

Introducción

Hoy por hoy la realidad nos dice que las redes informáticas, se han vuelto indispensables, tanto para las personas como organizaciones. Les da oportunidad de interactuar con el resto del mundo, ya sea por motivos comerciales, personales o emergencias.

La optimización en el uso de los sistemas informáticos es uno de los elementos de interacción y desarrollo que rige los destinos de la ciencia informática. Es por ello que la aparición de las plataformas de interconexión de equipos de computación o redes informáticas. Las mismas resultan ser uno de los elementos tecnológicos más importantes al momento de definir un sistema informático en una organización.

Entre las principales las ventajas que le brinda a una empresa el uso de redes informáticas, podemos detallar algunas: compartir recursos especialmente información (datos), proveer la confiabilidad, permite la disponibilidad de programas y equipos para cualquier usuario de la red que así lo solicite sin importar la localización física del recurso y del usuario. Permite al usuario poder acceder a una misma información sin problemas llevándolo de un equipo a otro. También es una forma de reducir los costos operativos, compartiendo recursos de hardware y/o de software entre las diversas computadoras de su empresa.

La empresa ROYAL-TECH se encuentra ubicada en la ciudad de Córdoba, dicha empresa cuenta con tres áreas, administración, ventas y producción. Además cuenta con una oficina de ventas en la ciudad de Buenos Aires.

En los últimos dos años la empresa creció abruptamente, paso de tener 200 puestos de trabajo a 600 puestos de trabajo; lo cual acarreo una serie de problemas estructurales a nivel informático. Entonces se decidió diseñar una nueva red informática la cual pueda soportar la nueva estructura de la empresa. Por medio de esta nueva red la empresa podrá contar con dos proveedores de Internet simultáneos, los cuales se distribuirán balaceadamente en el área de ventas. Esto es debido a la gran utilización que se produce en esta sub-red del ancho de banda. Se utilizan dos proveedores distintos del servicio de Internet debiendo que en el caso que se caiga una de las conexiones, la empresa siempre posea conectividad con el exterior.

Dicha red informática deberá proveer servicio al total de la empresa con 600 puestos de trabajo distribuidos en sus tres áreas y se deberá crear una red virtual privada (VPN) para interconectar la oficina de ventas ubicada en la ciudad de Buenos Aires, con la oficina de ventas situada en la ciudad de Córdoba. Brindándole una conexión más rápida y segura, considerando aspectos económicos y tecnológicos.

En el presente trabajo se documenta la configuración y puesta a punto de una red así como la definición de las políticas de seguridad de la red para un funcionamiento flexible y óptimo.

Tras un análisis y estudio de las necesidades particulares de cada caso, se creara una red con cuatro sub-redes: LAN Administración, LAN Ventas, LAN Producción, LAN Servidores.

Se utilizará un servidor DHCP para cada una de las sub-redes, con lo cual logramos asignar automáticamente las direcciones IP a cada uno de los puestos de los usuarios dentro de cada sub-red. Para la sub-red de servidores se les asigna una dirección IP dependiendo del número de MAC que tenga el servidor.

Se creara servidor ntp y usuario ntp, para sincronizar la hora con todos los usuarios. También se creara un servidor PPTP; que es el servidor VPN con el cual se conecta la oficina de Ventas de Buenos Aires a nuestra red derivándola a la red del área de Ventas. Se configura un servidor SNMP. Dicho servidor nos muestra el estado de las interfases, y se utiliza para monitoreo del estado de las interfaces del Mikrotik

Se aplicara políticas de control de ancho de banda, por sub-redes o por puesto de trabajo. El control de ancho de banda de los P2P será aplicado a la red de administración por política de la empresa. También el filtrado total de los p2p será aplicado a las redes del las áreas de Ventas y Producción

Se bloqueara en los puesto de usuario el MSN Live Messenger y se creará un servidor llamado JABBER de mensajería privada de la empresa.

La instalación de un Web Proxy, se utilizará para la optimización del ancho de banda utilizado en Internet y filtrado de páginas no aptas. Su funcionamiento consiste en guardar en un disco fijo todas las páginas que se hayan visitado. A propósito para

que cuando un nuevo usuario desee visitar una de las paginas ya guardadas. Entonces el servidor automáticamente le envía la página guardada del disco fijo y no la descarga desde la Web. Haciendo este proceso mucho más rápido y eficiente.

Liberación del ancho de banda fuera del horario de trabajo: Debido a que la empresa no trabaja las 24hs al día, se dispuso la posibilidad de liberar el ancho de banda para la red de Administración, en un rango horario determinado. Para ello lo primero que debemos hacer es una nueva cola que la habilitaremos en los horarios de 20:00hs a 06:00hs.

Dicha red se implementara con Mikrotik Routeros, el mismo es un sistema operativo y software del router; el cual convierte a una PC Intel ó un Mikrotik RouterBOARD en un router dedicado. Se toma esta decisión ya que estos equipos brindan seguridad, flexibilidad y son muy económicos lo cual es un gran beneficio para la empresa, ya que la red es de un tamaño considerable.

En el presente trabajo se analizara la implementación de una red simulada con Mikrotik en la empresa virtual Royal Tech

Metodología

1. **Estudio Exploratorio bibliográfico sobre el manual de referencia de Mikrotik y normas internacionales.**

   Se busco información en el manual de referencia, se tuvo en cuenta las normativas y reglamentaciones internacionales.

2. **Estudio descriptivo de la empresa Royal Tech.**

   2.1. Unidad de Análisis del entorno organizacional de Royaltech

   Se re diseño la red teniendo en cuenta.

   2.2. Variables

   - Las nuevas áreas de la empresa
   - Cantidad de puestos de trabajos
   - Interfaces a utilizar.
   - Redes Virtuales Privadas
   - Servidor de monitoreo SNMP
   - Servidor de autenticación RADIUS
   - Servidor de mensajería privada JABBER
   - Seguridad.
   - Modelado de colas de tráfico.
   - Tráfico cursado.

3. **Diseño de la implementación virtualizada de la red, para la empresa Royal Tech utilizando mikrotik.**

   Los pasos y procedimientos para la implementación del Mikrotik fueron:

   · Instalación Mikrotik

   · Acceso al Mikrotik

- Declaración de interfaces
- Definición Vlan´s
- Asignación de dirección ip por interfaces
- Asignación de pools de direcciones ip´s
- Configuración servidor DHCP
- Instalación del servidor y cliente NTP.
- Servidor VPN
- Balanceo de carga
- Control de ancho de banda
- Instalación servidor SNMP
- Instalación servidor RADIUS
- Instalación servidor JABBER
- Instalación servidor PROXY
- Configuración Hotspot.

Resultado y discusión

Estudio bibliográfico de Mikrotik RouterOS

Dicha red se implementara con Mikrotik RouterOS que es el sistema operativo y software del router, el cual convierte a una PC Intel ó un Mikrotik RouterBOARD en un router dedicado.

Se toma esta decisión ya que estos equipos brindan seguridad, flexibilidad y son muy económicos, lo cual es un gran beneficio para la empresa ya que la red es de un tamaño considerable

El RouterOS es un sistema operativo y software que convierte a una PC en un ruteador dedicado, bridge, firewall, controlador de ancho de banda, punto de acceso inalámbrico, por lo tanto puede hacer casi cualquier cosa que tenga que ver con las necesidades de red, además de ciertas funcionalidad como servidor.

El software RourterOS puede ejecutarse desde un disco IDE memoria tipo FLASH. Este dispositivo se conecta como un disco rígido común y permite acceder a las avanzadas características de este sistema operativo.

Características principales

- El Sistema Operativo es basado en el Kernel de Linux y es muy estable.
- Puede ejecutarse desde discos IDE o módulos de memoria flash.
- Diseño modular
- Módulos actualizables
- Interfaz grafica amigable.

Características de ruteo

- Políticas de enrutamiento. Ruteo estático o dinámico.
- Bridging, protocolo spanning tree, interfaces multiples bridge, firewall en el bridge.

- Servidores y clientes: DHCP, PPPoE, PPTP, PPP, Relay de DHCP.
- Cache: web-proxy, DNS.
- Gateway de HotSpot.
- Lenguaje interno de scripts.

Características del RouterOS

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

Calidad de servicio (QoS)

Tipos de colas

- RED
- BFIFO
- PFIFO
- PCQ

Colas simples

- Por origen/destino de red.
- Dirección IP de cliente.
- Interfase

Árboles de colas

- Por protocolo.
- Por puerto.

- Por tipo de conexión.

Interfases del RouterOS

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

Herramientas de manejo de red

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

Estas son las principales características del sistema operativo y software Mikrotik RouterOS elegido para la implementación de la red virtualizada.

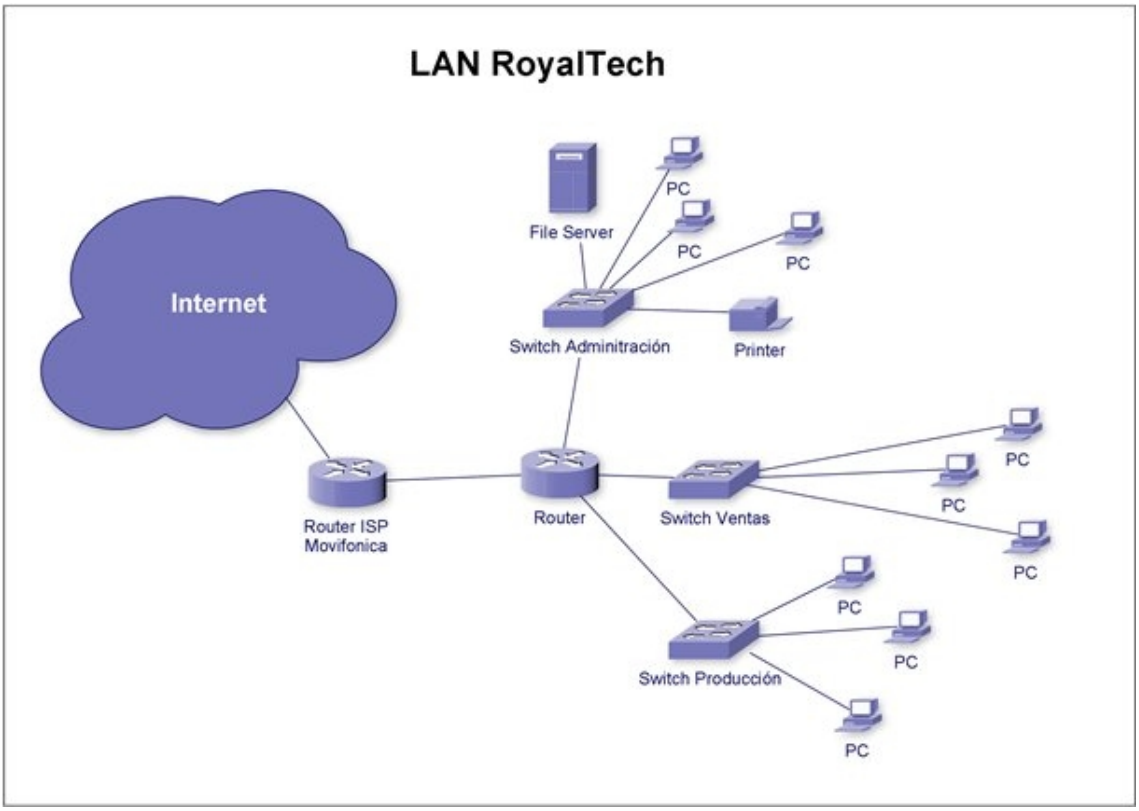
Estudio descriptivo de la empresa Royaltech

Después de haber hecho un análisis exhaustivo de la estructura de Royaltech, se pudo diagramar la estructura de cómo estaba conformada dicha empresa.

Tenemos una sub-red de administración, la cual, cuenta con un servidor de archivos que se utiliza para brindar dicho servicio a todas las otras redes. Esto acarrea el problema de que se genera demasiado tráfico de datos hacia la red de Administración, lo cual produce congestión y altas pedidas de paquetes. Por ende tenemos descontento del personal de la empresa al igual que ineficiencia de los mismos. Además posee una impresora en la red del tipo hogareña para que impriman todas las otras sub-redes.

Tener una sola impresora le trajo muchos inconvenientes a la empresa debido a que se generan colas interminables de documentos a imprimir. También, la impresora se rompe cotidianamente debido al exceso de carga. Otro inconveniente que se produce es el ingreso de personal ajeno al área de administración. Esto genera lentitud a la hora de trabajar y perdida de tiempo de los empleados para ir a buscar sus documentos a la impresora en otra área. Rotura de mobiliario en la zona en cuestión al igual que la falta injustificada de insumos.

Las sub-redes de Ventas y Producción simplemente poseen pc´s conectadas a través de un switch. Todo este grupo de computadoras acceden al servidor de archivos al igual que la impresora a través del router principal.

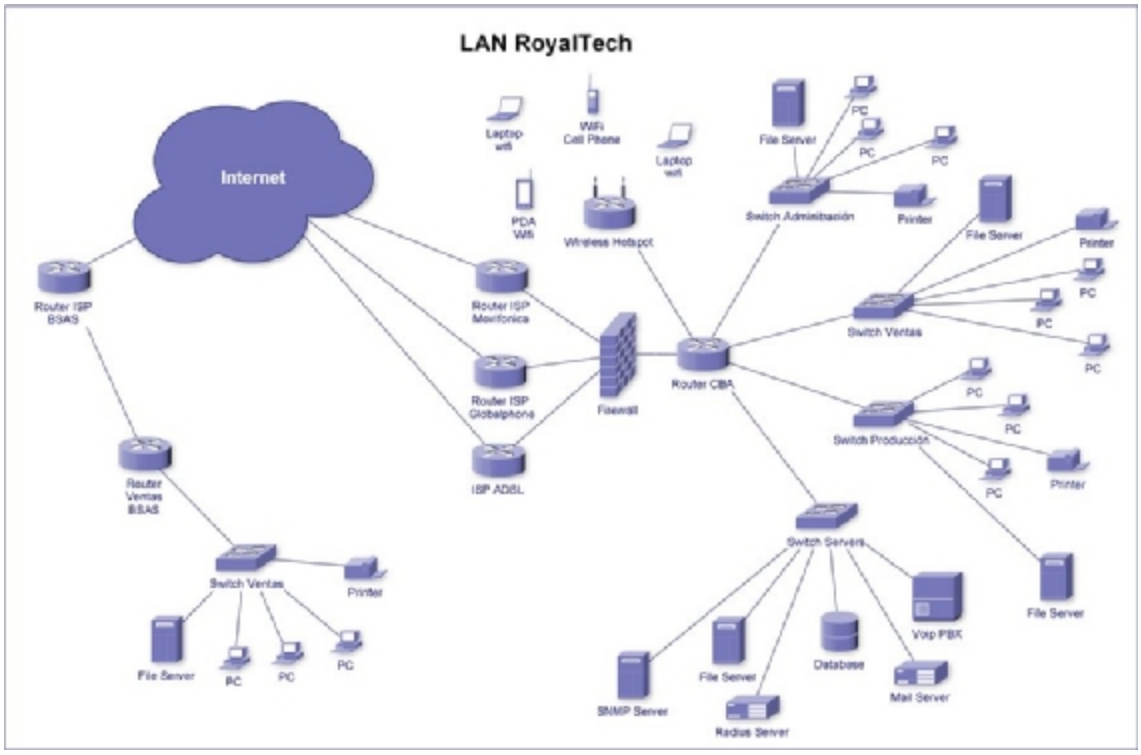


El router en cuestión, no es un router de alta productividad, con lo cual se generan grandes problemas de congestión, debido a que no puede administrar la gran cantidad y volumen de información que transita por la red.

Los switch en cada una de las áreas son idénticos. Ninguno posee la habilidad de poder administrar sus puertos, al igual que están imposibilitados de generar vlan o cualquier otro tipo de política que se pueda generar en otro tipo de switch.

Debido a esta disposición de red y los constantes problemas técnicos que posee, al igual que la pedida de tiempo de los recursos humanos de tener que desplazarse hasta otro piso para buscar sus impresiones. Por eso la empresa decidió la reestructuración de su red para optimizar y mejorar la producción de la misma y sus recursos humanos.

Luego de examinar dicha situación se decidió planificar toda una reestructuración de la red nueva. Lo cual solucionará los problemas de congestión al igual que proveerá mayor productividad. Lo cual traerá grandes beneficios.



La nueva red planeada posee dos nuevas sub-redes, una un hotspot y la otra una sub-red de servidores. También en esta nueva reestructuración se interconectara las oficinas de ventas que están ubicadas en la ciudad de Buenos Aires con las oficinas de ventas en la ciudad de Córdoba. Asimismo se opto por la utilización de dos proveedores de Internet distintos, debido a que constantemente poseían problemas de caída del servicio de ADSL. Se dejo a este ultimo como backup de las dos otras conexiones.

Router CBA

Nuestro router en las oficinas de Córdoba esta basado en la plataforma Intel con dos placas de red que poseen 4 puertos Gigabit Ethernet cada una. El sistema operativo para la implementación será Mikrotik RouterOs.

El router proveerá de varios servicios para la red. En los cuales podemos encontrar Servidor DHCP, Firewall, Servidor PPPoE, Cliente PPPoE, Servidor PPTP Server, Modelado de colas, Cliente NTP, Servidor NTP, Web Proxy, Hotspot.

El servidor DHCP, nos brindara las direccion de IP, Gateway, broadcast, dns para cada una de a las sub redes.

El Firewall se utilizará para las siguientes actividades:

- Bloqueo del cliente MSN Live Messenger.
- Bloqueo P2P para redes Producción y Ventas.
- Redireccionamiento de puertos.
    - Puerto 80 WEB.
    - Puerto 110 POP3.
    - Puerto 25 SMTP.
    - Puerto 1723 PPTP.
- Descartar conexiones inválidas.
- Aceptar conexiones establecidas.
- Acepta Trafico UDP.
- Acepta paquetes de icmp Limitados.
- Descarta excesivos paquetes de icmp
- Descarta el resto de las conexiones externas

El servidor PPTP, será utilizado para interconectar las oficinas de Buenos Aires y Córdoba.

El servidor PPPoE será utilizado para autenticar a los usuarios que se deseen loguear desde fuera de la red de producción.

El cliente PPPoE se utilizará en el caso improbable que las dos otras conexiones a Internet se caigan. Con lo cual se utilizará como ruta alternativa de backup.

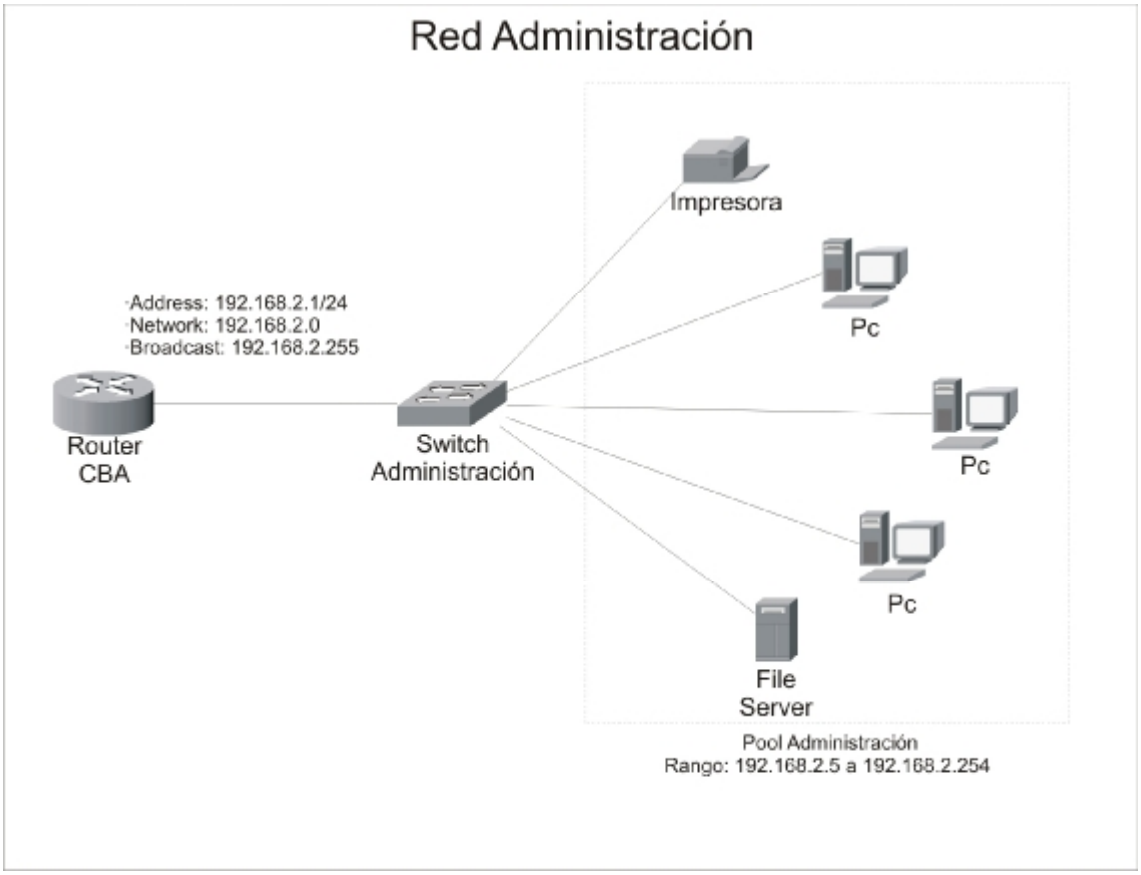
El modelado de colas se utilizará para asignarle un determinado ancho de banda a cada una de las sub redes. Al igual se utilizará el modelado de colas para el control de ancho de banda para los clientes P2P

El cliente NTP, se utilizará para sincronizar la hora de nuestro mikrotik. El servidor NTP se utilizará para que las computadoras de la red estén sincronizadas.

El Web Proxy se utilizará para filtrar el contenido que los usuarios realicen al navegar a través de Internet. Para ello se aplicaran las siguientes políticas:

- Bloqueo Pornografía
- Bloqueo paginas que brinden el servicio de Web Messenger
- Bloqueo del Live Messenger A Través del Proxy
- Bloqueo de páginas que brinden webmail
- Bloqueo descarga directa de archivos MP3 y AVI
- Bloqueo descarga directa de archivos RAR, ZIP, EXE

Sub-red Administración



La nueva restructuración de la sub-red de administración se dio debido al alto tráfico que tenían entre todas las otras redes. A esta sub-red se decidió cambiar el switch que poseía para utilizar un switch de alta productividad.

Nuestra sub-red poseerá un pool de impresoras de red para esta sola área. Esto disminuirá el tráfico de impresión al igual que el tráfico de personal ajeno a Administración.

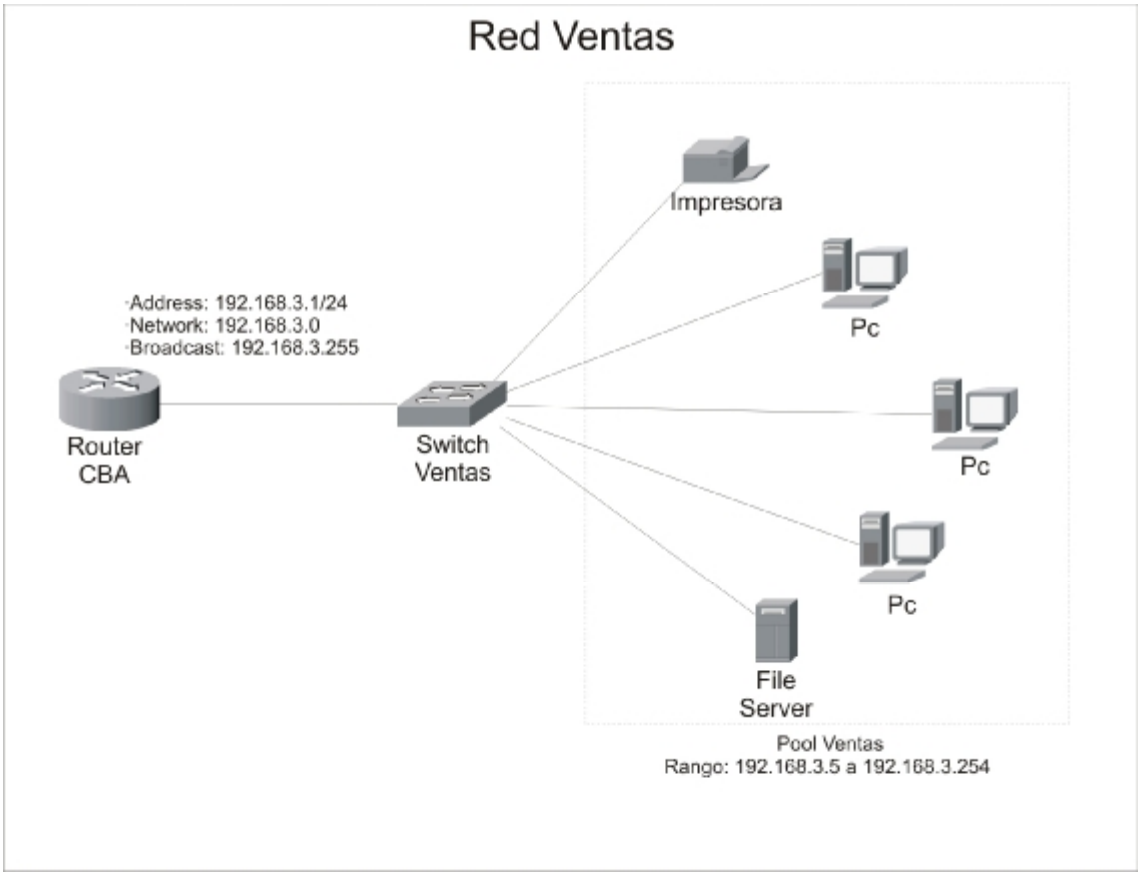
Asimismo se le instalará un servidor de archivos propio de administración en el cual se encontrará exclusivamente los archivos de dicha aréa.

Los números de ip, Gateway, Broadcast y dns, serán asignados por el router mikrotik mediante DHCP. El Rango de direcciones será desde 192.168.2.5/24 al 192.168.2.254/24. Se decidió dejar las direcciones desde el 192.168.2.2/24 al 192.168.2.4/24 fuera de este rango para el caso de que se quieran instalar algún otro tipo de servidores en dicha área en un futuro próximo. Los números de ip asignados a los servidores serán asignado mediante la dirección mac de cada uno.

La red de administración será conectada a través del switch al router mediante un backbone de 1Gbit Ethernet. El cual será limitado mediante teoría de colas simples a 250M/bits de subida y 300M/bits de bajada.

Debido a que dentro del área de administración se encuentra gerencia, la misma autorizó la utilización de los P2P para dicha área. El trafico P2P será modelado para que no ocupe gran cantidad de ancho de banda.

Sub-red Ventas



A esta sub-red se le decidió cambiar el switch que poseía para utilizar un switch de alta productividad.

Nuestra sub-red poseerá un pool de impresoras de red para esta sola área. Esto disminuirá el tráfico de impresión al igual que el tráfico de personal ajeno a Administración. Asimismo se le instalará un servidor de archivos propio de ventas en el cual se encontrará exclusivamente los archivos de dicha aréa.

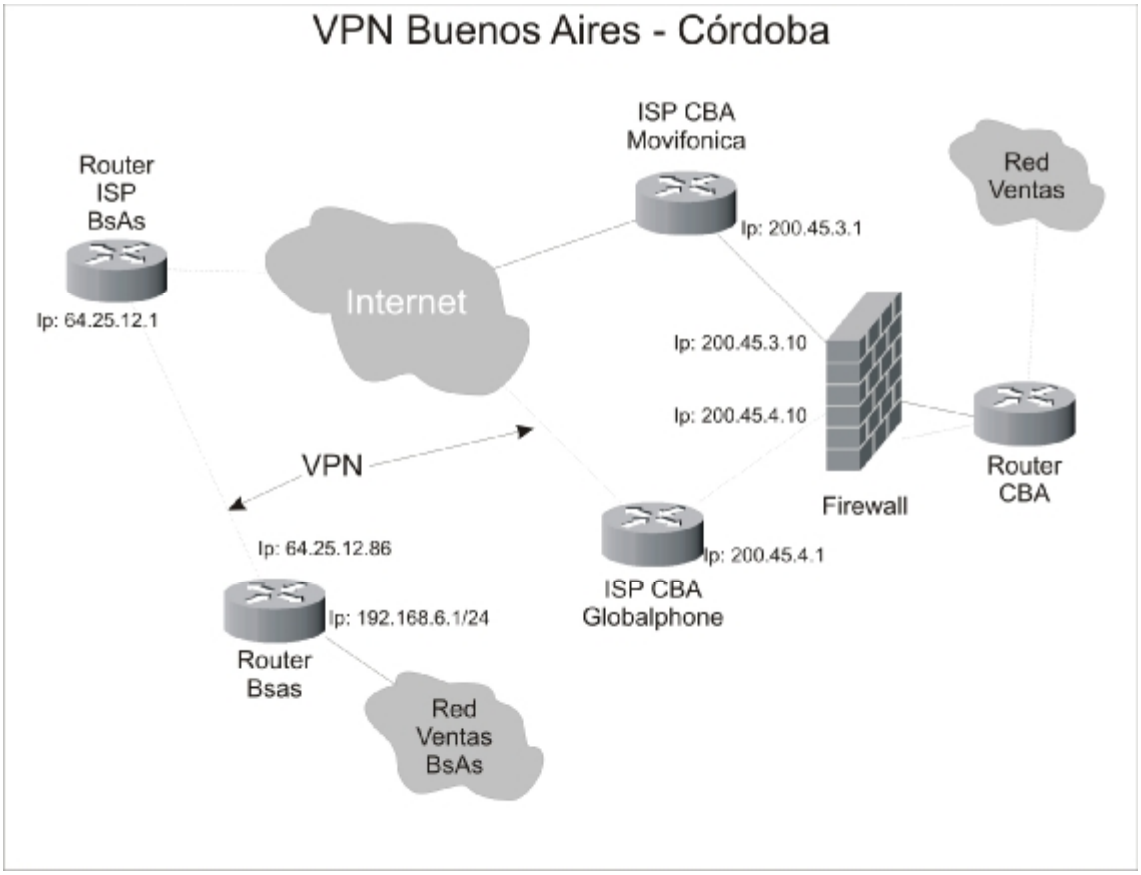
Los números de ip, Gateway, Broadcast y dns, serán asignados por el router mikrotik mediante DHCP. El Rango de direcciones será desde 192.168.3.5/24 al 192.168.3.254/24. Se decidió dejar las direcciones desde el 192.168.3.2/24 al 192.168.3.4/24 fuera de este rango para el caso de que se quieran instalar algún otro tipo

de servidores en dicha área en un futuro próximo. Los números de ip asignados a los servidores serán asignado mediante la dirección mac de cada uno.

La red de ventas será conectada a través del switch al router mediante un backbone de 1Gbit Ethernet. El cual será limitado mediante teoría de colas simples a 400M/bits de subida y 300M/bits de bajada.

Esta sub-red albergara también las pc´s de la oficina de Buenos Aires. Dicha oficina será conectada a las oficinas de Córdoba mediante una VPN. Se utilizará el protocolo PPTP para crear el túnel.

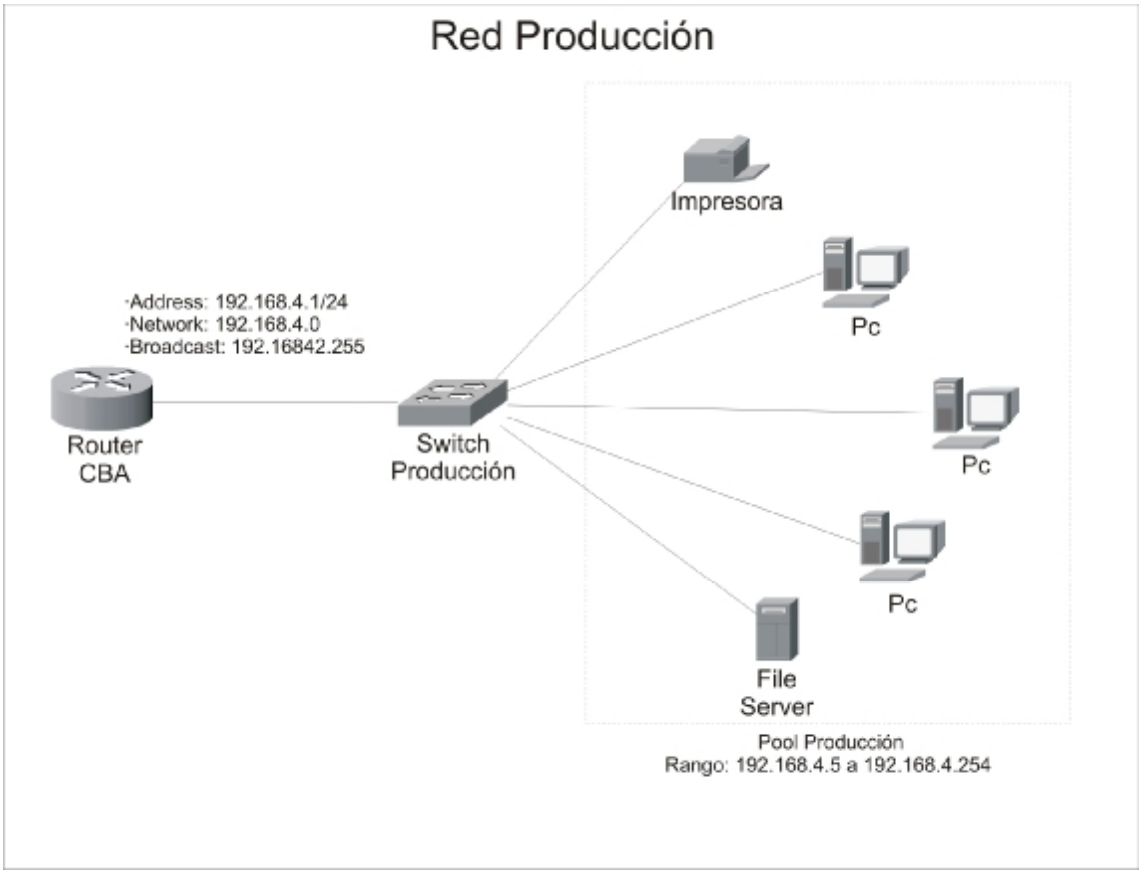
El tráfico de P2P quedará bloqueado absolutamente para esta sub-red. Ya que se prohibió el trafico p2p para esta área.



Para contra restar la carga hacia Internet desde esta red, se decidió realizar un balanceo de carga entre los dos proveedores de Internet. Lo cual traerá grandes

beneficio ya que no desbordara uno solo de los enlaces. Sino todo el tráfico generado será balanceado entre ambas conexiones.

Sub-red Producción



A la sub-red de producción se decidió cambiarle el switch que poseía para utilizar un switch de alta productividad, que nos brinde la posibilidad de administrar puertos.

Nuestra sub-red poseerá un pool de impresoras de red para esta sola área. Esto disminuirá el tráfico de impresión al igual que el tráfico de personal ajeno a Administración.

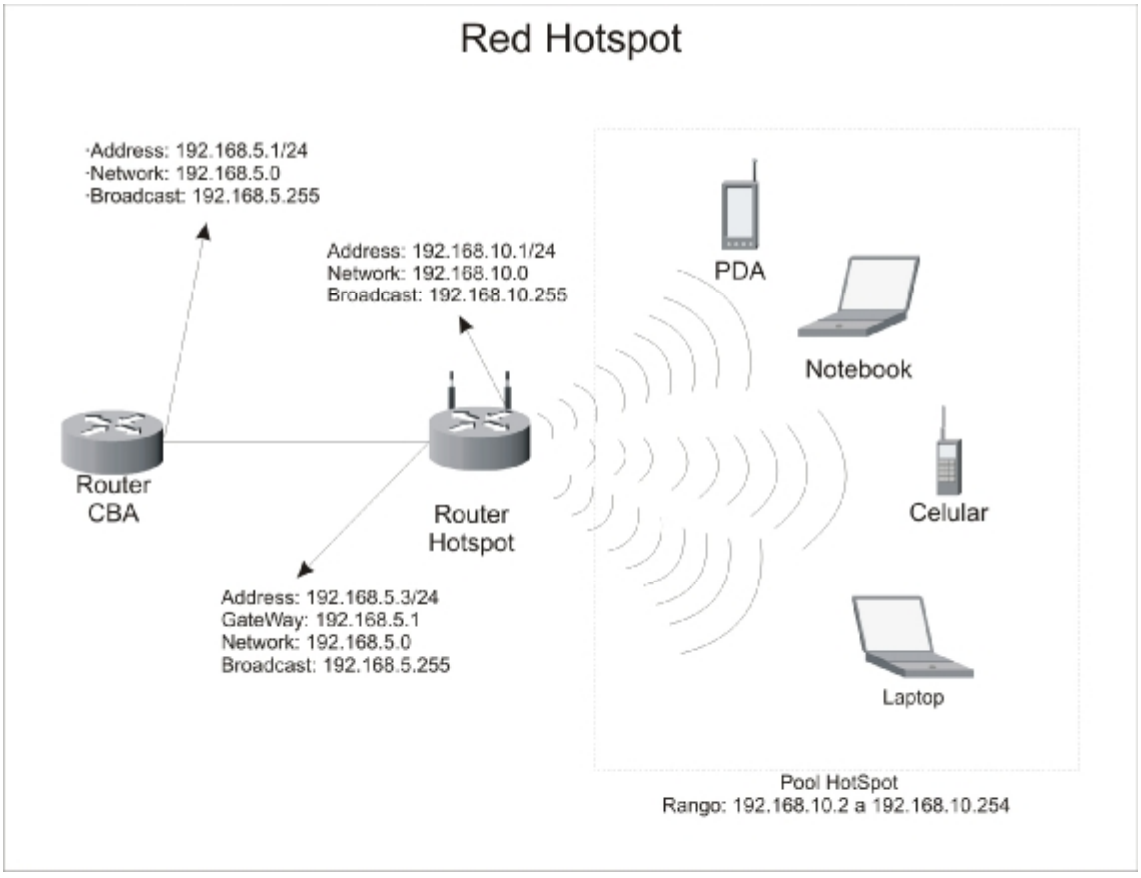
Asimismo se le instalará un servidor de archivos propio de producción en el cual se encontrará exclusivamente los archivos de dicha aréa.

Los números de ip, Gateway, Broadcast y dns, serán asignados por el router mikrotik mediante DHCP. El Rango de direcciones será desde 192.168.4.5/24 al 192.168.4.254/24. Se decidió dejar las direcciones desde el 192.168.4.2/24 al 192.168.4.4/24 fuera de este rango para el caso de que se quieran instalar algún otro tipo de servidores en dicha área en un futuro próximo. Los números de ip asignados a los servidores serán asignado mediante la dirección mac de cada uno.

La red de ventas será conectada a través del switch al router mediante un backbone de 1Gbit Ethernet. El cual será limitado mediante teoría de colas simples a 350M/bits de subida y 400M/bits de bajada.

Esta sub-red poseerá la posibilidad que usuarios que estén en otras áreas de la empresa, se puedan conectar a esta sub-red mediante PPPoE. El tráfico de P2P quedará bloqueado absolutamente para esta sub-red. Ya que se prohibió el trafico p2p para esta área.

Sub-red Hotspot

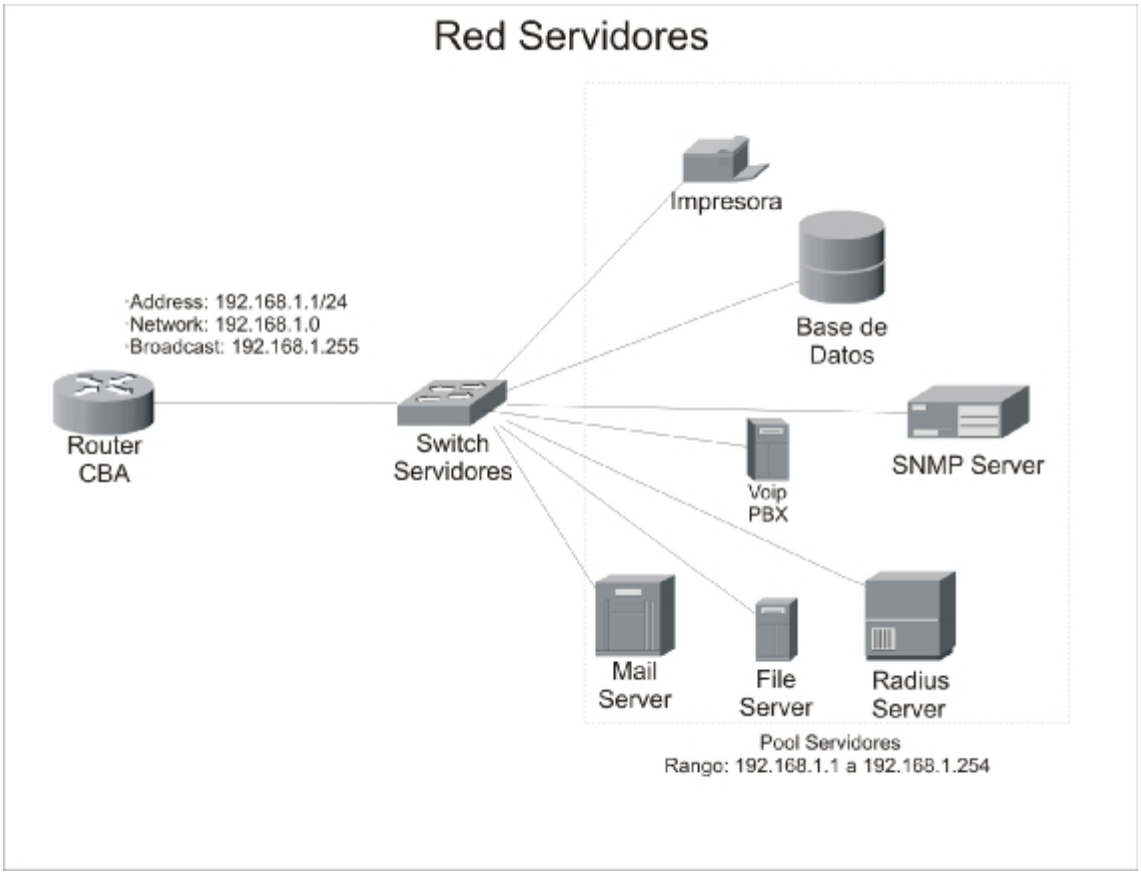


La red hot spot es una nueva red que se decidió implementar debido a que la empresa ahora posee un área de recreación. La misma red solo poseerá la capacidad de navegar a través de Internet.

Los números de ip, Gateway, Broadcast y dns, serán asignados por el router mikrotik mediante DHCP. El Rango de direcciones será desde 192.168.10.2/24 al 192.168.10.254/24.

Para la protección de los datos en la sección wireless se decidió asegurarlos mediante WPA PSK o WPA2 PSK. Esto nos dará fiabilidad y seguridad en los mismos. No obstante la seguridad WPAx que se desee implementar, todos los usuarios que se conecten al hotspot deberán ser autenticados mediante el servidor radius instalado en la granja de servidores.

Sub-red Servidores



A la sub-red de Servidores se decidió cambiarle el switch que poseía para utilizar un switch de alta productividad, que nos brinde la posibilidad de administrar puertos.

Nuestra sub-red poseerá un pool de impresoras de red para esta sola área. Esto disminuirá el tráfico de impresión al igual que el tráfico de personal ajeno a Administración.

Los números de ip, Gateway, Broadcast y dns, serán asignados por el router mikrotik mediante DHCP. El Rango de direcciones será desde 192.168.1.5/24 al 192.168.1.254/24. Los números de ip asignados a los servidores serán asignado mediante la dirección mac de cada uno.

Asimismo se le instalará un servidor de archivos propio de administración en el cual se encontrará exclusivamente los archivos de dicha aréa.

En esta sub-red se instalará un servidor radius para la autenticación de los usuarios que se conecten desde el hotspot.

El servidor de correo de la empresa se encontrará dentro de esta sub-red. Este servidor se utilizará tanto para correo interno al igual que correo externo.

El servidor de SNMP se utilizara para la monitorización de la red.

Diseño de la implementación virtualizada de la red.

Instalación de Mikrotik RouterOS

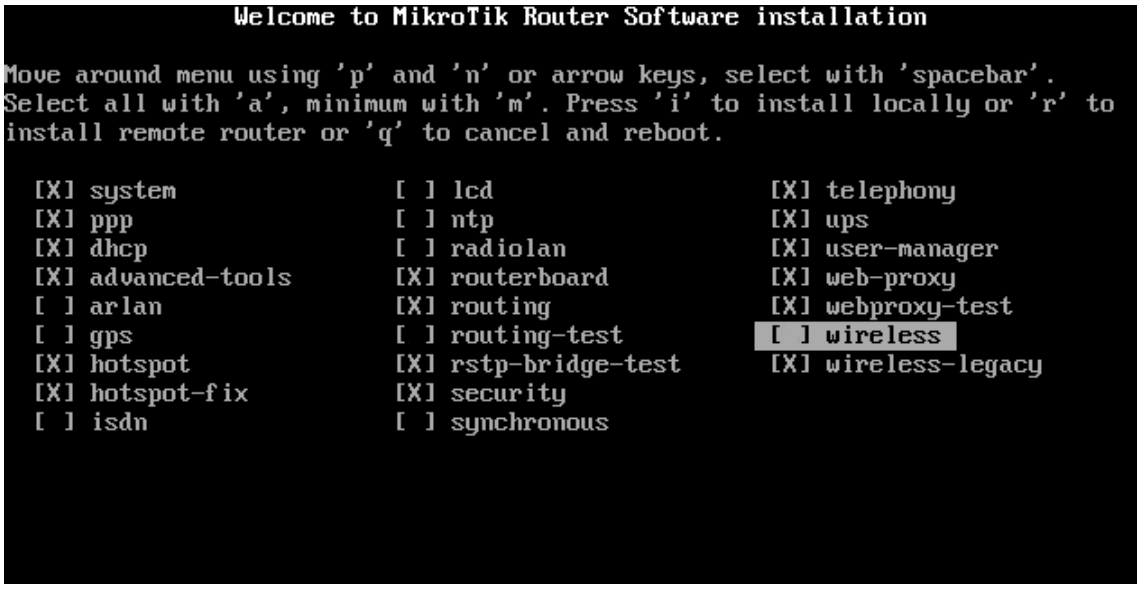
A continuación vamos a mostrar paso por paso como se realiza la instalación de Mikrotik sobre una plataforma x86. La plataforma cuenta con 2 placas de red pci que poseen 4 bocas de red gigabyte Ethernet. Utilizaremos 2 bocas para conectarnos a dos proveedores de Internet distintos y una tercera para conectarnos a un proveedor de

ADSL. El resto de las placas se utilizaran para la distribución de nuestra red interna. Utilizaremos la versión 2.9.27 Nivel 6 del software Mikrotik Router Os.

Booteamos con un CD que contenga la imagen del Mikrotik RouterOs ya quemada. Luego nos aparecerá el menú de instalación que nos preguntará que paquetes deseamos instalar.

Para desplazarnos por el menú utilizamos las tecla ´P´ o ´N´ o sino las flechas del teclado. Para seleccionar o deseleccionar los paquetes a instalar utilizamos la Barra Espaciadora. Luego presionamos la tecla ´I´ para comenzar la instalación local en nuestra plataforma.

Los paquetes seleccionados para nuestra configuración son los siguientes:

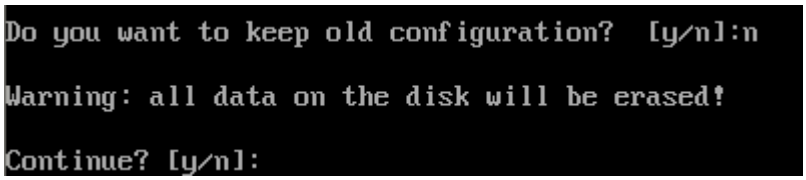


- System: Paquete principal que posee los servicios básicos al igual que los drivers básicos.
- Ppp: Provee de soporte para PPP, PPTP, L2TP, PPPoE e ISDN PPP.
- Dhcp: Servidor y cliente DHCP.
- Hotspot: provee de un hot spot.
- Hotspot-fix: Provee el parche para actualizar el modulo hot spot que tiene problemas en las versión 2.9.27.
- Ntp: Servidor y cliente NTP.

- Routerboard: provee de las utilidades para el routerboard.
- Routing: Provee soporte para RIP, OSPF y BGP4.
- Rstp-bridge-test: provee soporte para Rapid Spanning Tree Protocol.
- Security: Provee soporte para IPSEC, SSH y conectividad segura con Winbox.
- Telephony: Provee soporte para H.323.
- Ups: provee soporte para UPS APC.
- User-manager: Servicio de usuario del RouterOs
- Web-Proxy: Paquete para realizar un Web Proxy.
- wireless-legacy: Provee soporte para placas Cisco Aironet, PrismII, Atheros entre otras.

Luego la instalación nos pregunta si deseamos quedarnos con la configuración anterior, contestamos que no ´N´.

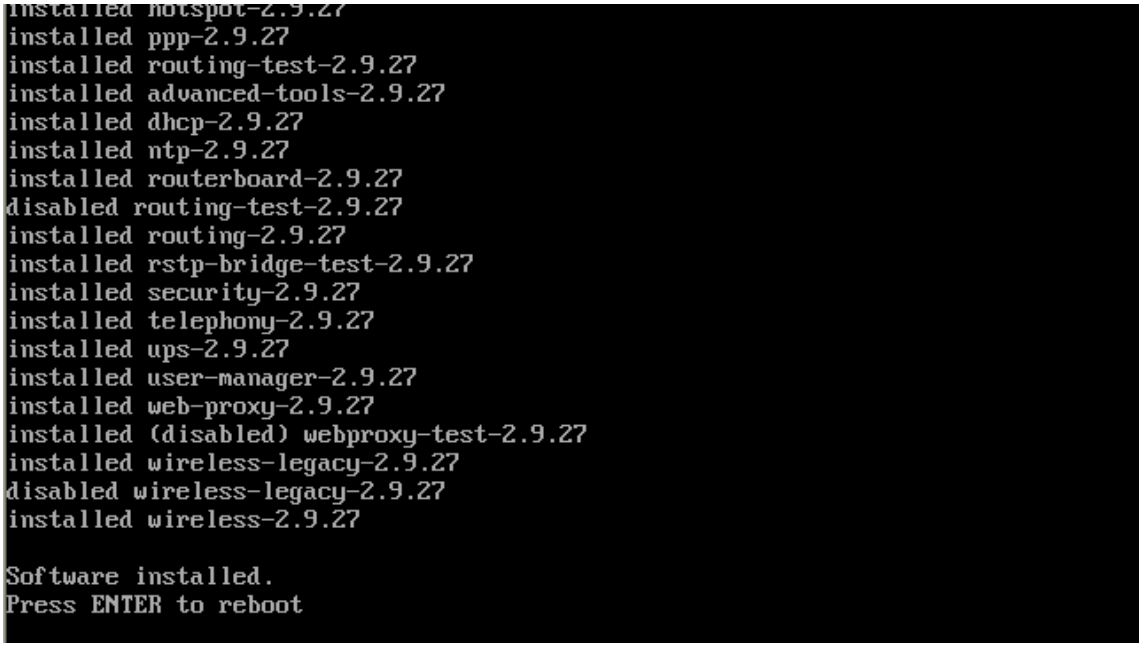
La siguiente pregunta hace referencia a que perderemos todos los datos que se encuentran en el disco fijo le contestamos que si ´Y´.



A continuación comienza el proceso de particionado y formateado del disco fijo que es automático y no nos hace ningún tipo de preguntas. Luego nos dice que presionemos ´Enter´ para que el sistema se reinicie.

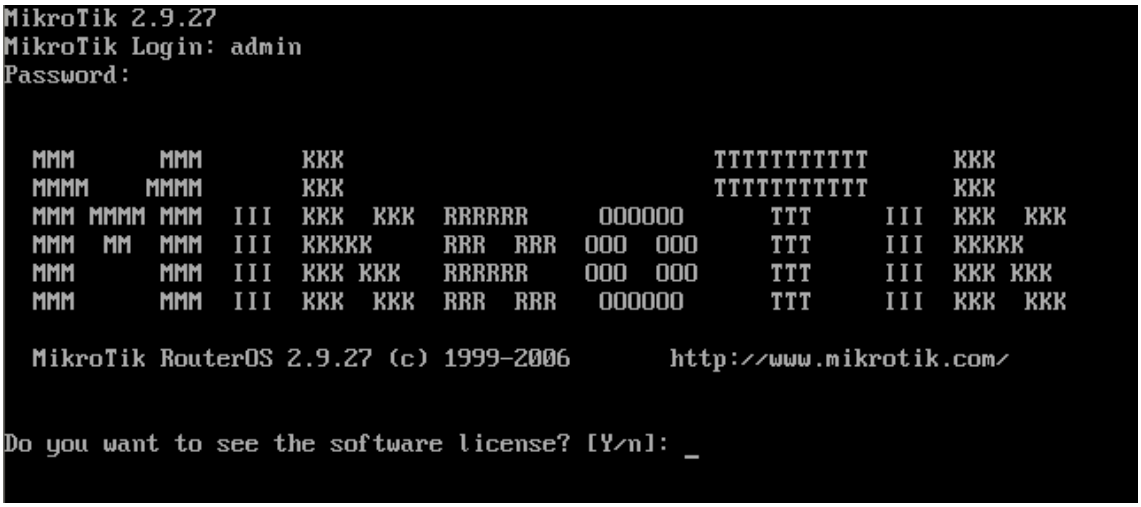
Seguidamente que se reinicia el sistema, nos pregunta si deseamos chequear la superficie del disco fijo le contestamos que si ´Y´.

Luego comienza la instalación de los paquetes seleccionados con anterioridad. Al finalizar dicho proceso nos pide que presionemos ´Enter´ nuevamente para reiniciar el sistema.

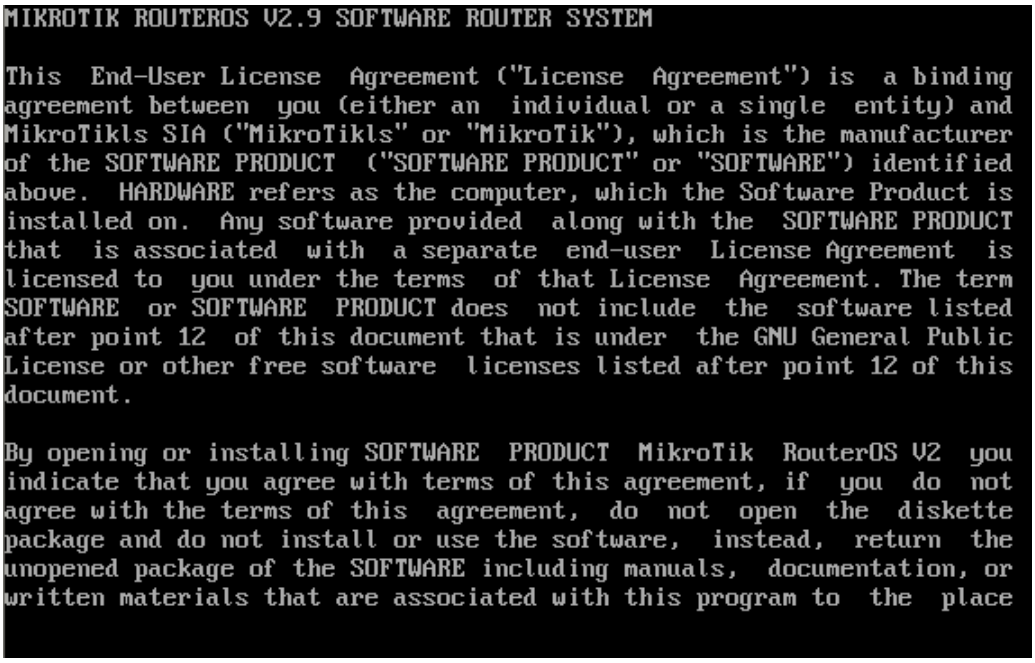


Con el sistema reiniciado e instalado, la consola nos pide el usuario y contraseña. Por defecto dicho nombre de usuario es: ***admin*** y para la contraseña se deja el casillero en blanco y se presiona enter.

A continuación nos da la bienvenida y nos pregunta si deseamos leer la licencia lo cual contestamos que si ´Y´.



Luego de haber leído la licencia ya nos queda la consola para comenzar a configurar nuestro Mikrotik.



Logueo al Mikrotik

Hay varias maneras para acceder a la administración del Mikrotik sin haber configurado nada en un principio.

La primera es directamente desde la consola finalizada la instalación, otro método es utilizando una consola Telnet a través del el puerto serie o Ethernet por mac o ip, sino mediante la utilización del software winbox, el cual lo brinda los desarrolladores de Mikrotik.

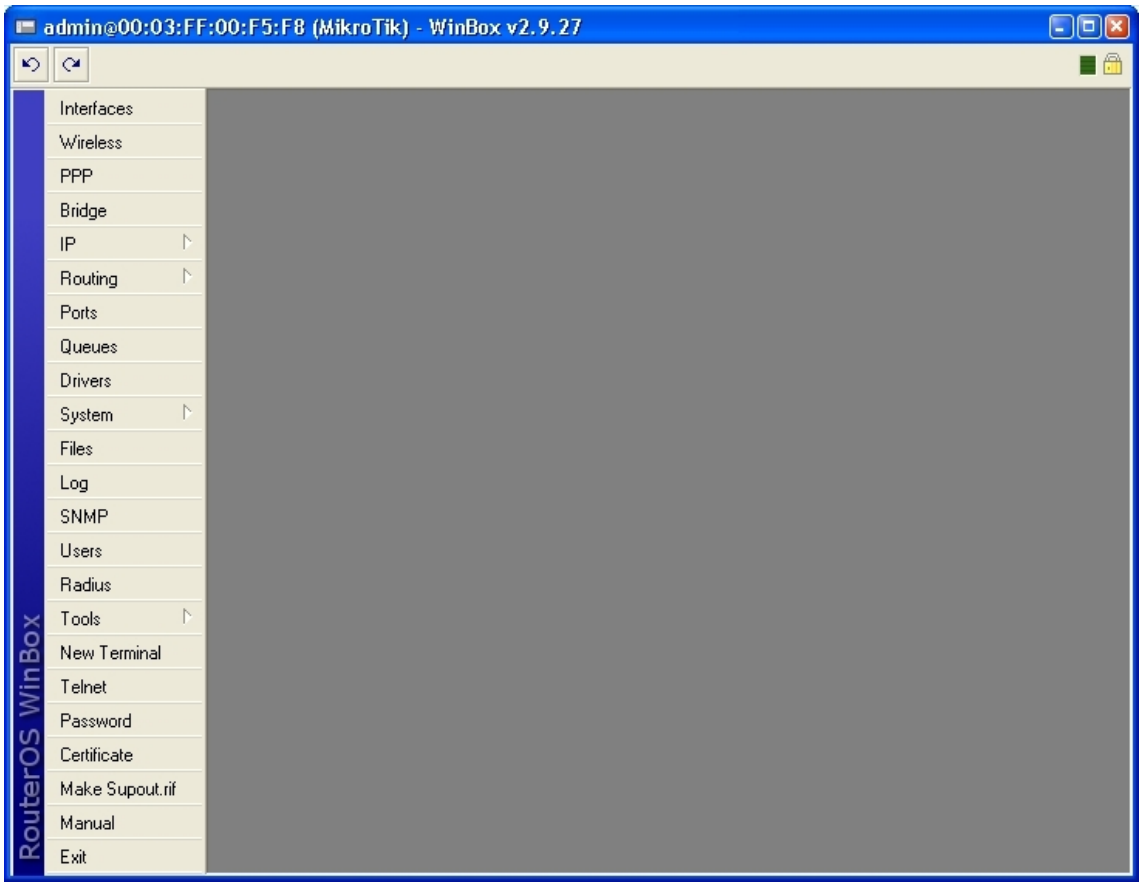
Debido a la flexibilidad, rapidez y ventajas que presenta la utilización de winbox respecto a los otros métodos, éste será la manera con la cual realizaremos la configuración de la red.

Desde una PC remota con Windows xp instalado. Conectados mediante un cable cruzado al Mikrotik al puerto Ethernet. Hacemos correr el soft Winbox, el cual nos brindara una ventana para loguearse al Mikrotik.

En esta ventana nos deja introducir las direcciones Mac o ip de la placa del Mikrotik a la cual estamos conectados. Debido a que no hemos configurado el Mikrotik desde la consola. Hacemos clic en (…) esto hará que el software nos devuelva las direcciones Mac de las interfases de red que posean un Mikrotik instalado y corriendo. Seleccionamos la interfase y luego utilizaremos de Login: admin y como Password: (nada). Al finalizar esta carga de datos hacemos clic en Connect.

Luego cuando el soft se conecta al Mikrotik automáticamente empieza a descargar los plugins instalados en el Mikrotik para poder administrarlos remotamente.

Al finalizar la descarga de los plugins nos aparece la pantalla de configuración del Mikrotik. En la cual a mano izquierda se encuentra el menú de configuración de cada uno de los módulos instalados.



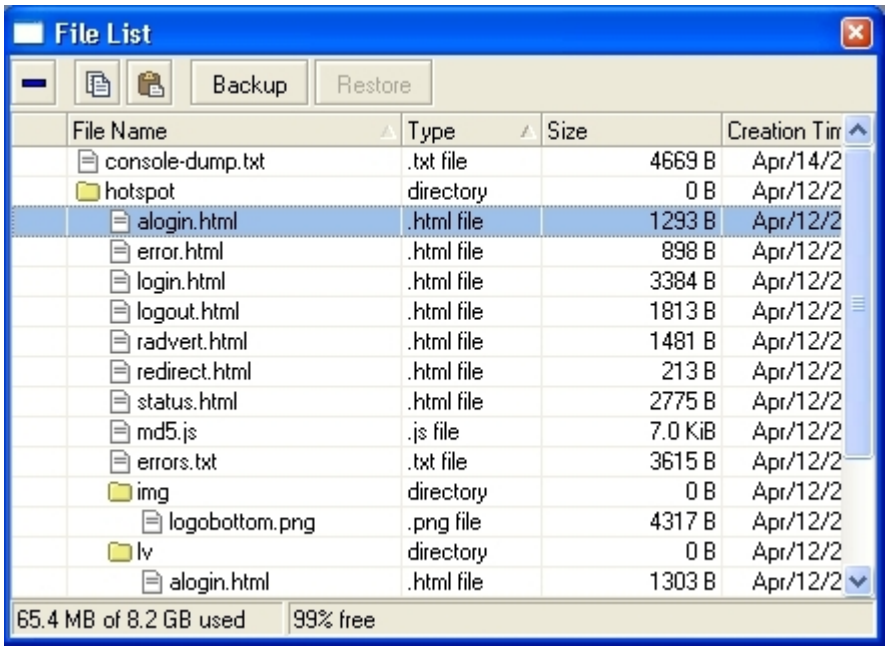
En la barra superior del software nos encontramos con la barra de herramienta. En la misma sobre mano izquierda posee las opciones de undo y redo. Sobre mano derecha podemos encontrar dos iconos, el primero muestra la utilización del Mikrotik y el segundo nos indica si la conexión que estamos realizando es segura o no.

Backup y Restore de Configuración

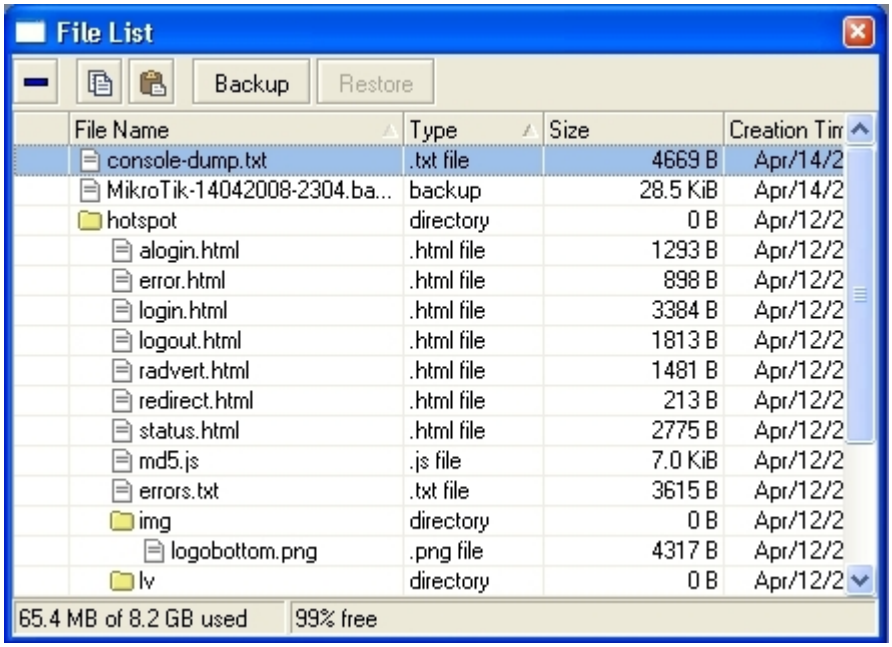
Debido a los problemas que pueden producirse en los equipamientos, siempre es buena política tener back up de todas las configuraciones de los sistemas. Ahora mostraremos como se realizar un backup de la configuración y como se recupera.

Backup de la configuración.

Primero nos Dirigimos al menú *FILES* allí se nos abrirá una ventana y nos mostrará los archivos que se encuentran almacenados. Debemos hacer clic sobre el botón de *BACKUP* para realizar nuestro backup.

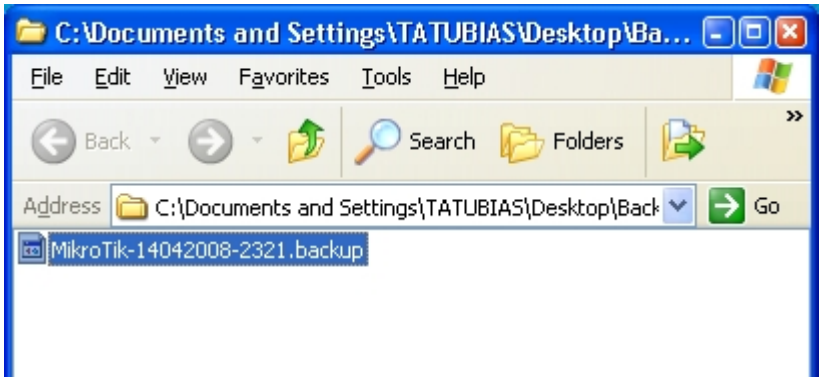


Luego de haber hecho clic nos aparece un nuevo archivo en la lista que poseíamos, que es nuestro backup de toda la configuración del Mikrotik.



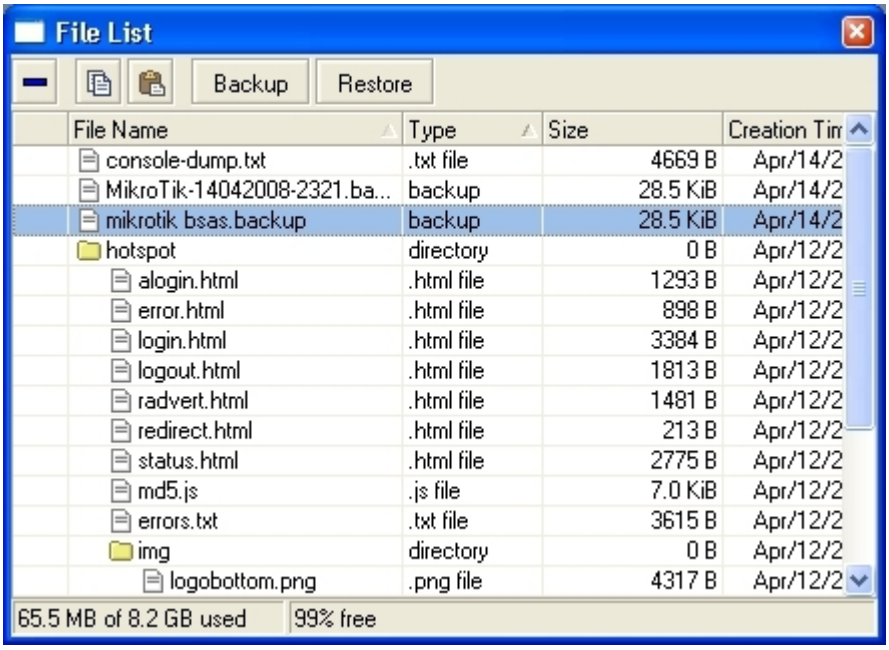
Sabiendo que el almacenamiento puede fallar, siempre es bueno tener una copia de resguardo en otro sitio. Para ello debemos hacer lo siguiente.

Seleccionamos el archivo de backup que deseamos y luego hacemos clic sobre el icono de *COPY*. Esto hará que nuestro archivo de configuración quede almacenado en el porta papeles de Windows. A continuación creamos una carpeta en el disco fijo de la PC y pegamos el archivo. Nos aparecerá y ya tendremos el backup de nuestro archivo de configuración en nuestra PC.

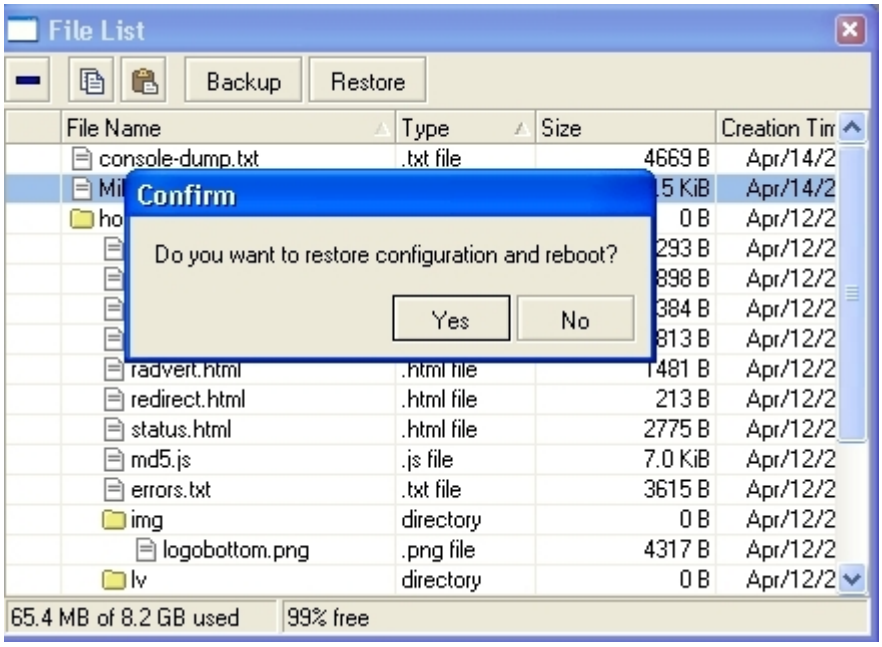


Restore de la configuración.

Si estamos recuperando el archivo de configuración que esta dentro del Mikrotik. Simplemente debemos ir al menú *FILES*. En la ventana que nos aparece debemos seleccionar la versión del backup que deseamos recuperar y hacer clic sobre el botón de *RESTORE*.



Para el caso que el archivo de back up se encuentre en nuestro disco fijo. Seleccionamos el archivo de backup, luego hacemos clic con el botón derecho del mouse y seleccionamos copiar. Luego en el winbox, simplemente debemos ir al menú *FILES*. En la ventana que nos aparece, debemos hacerle clic en el icono de pegar y nos aparecerá nuestra nueva configuración. A continuación seleccionamos nuestra nueva con figuración y apretamos el botón de restore. Se nos abrirá una nueva ventana que nos aplicara la nueva configuración y nos hará reiniciar nuestro Mikrotik.



Definición y configuración de interfases.

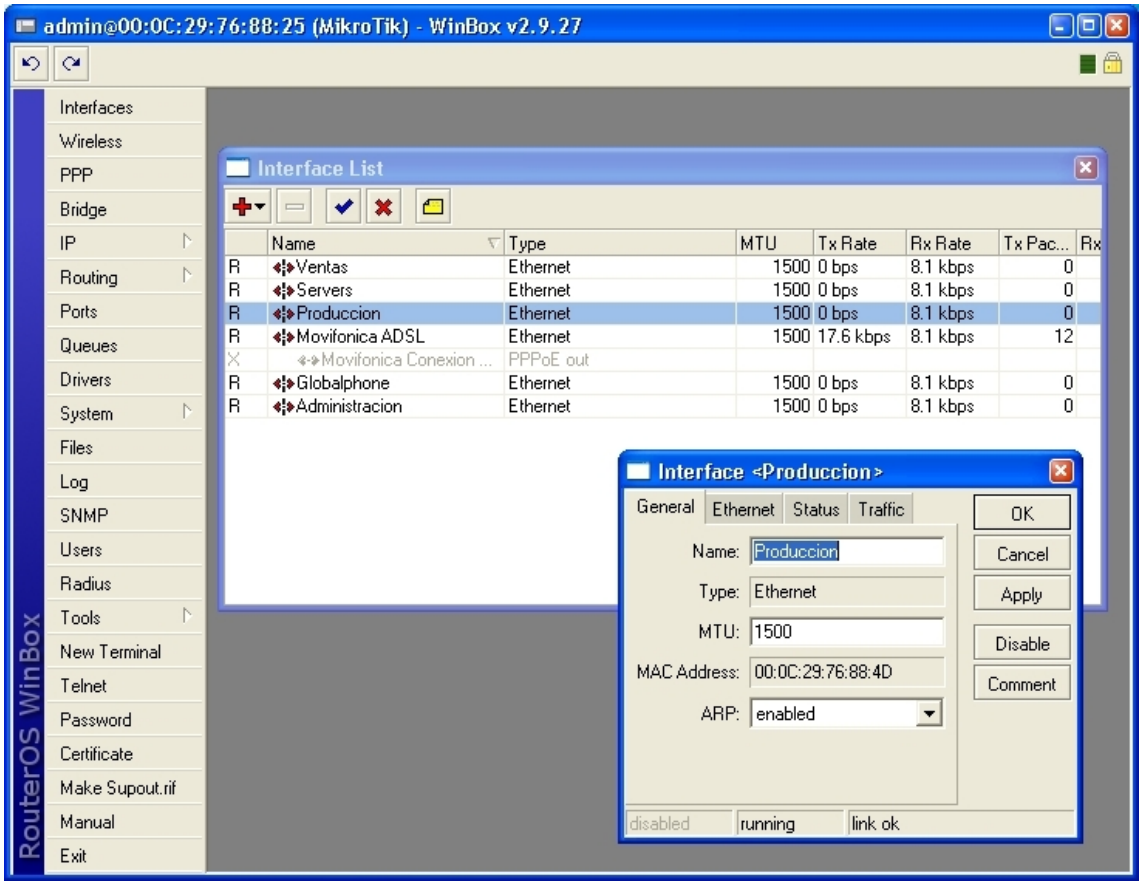
Actualmente las placas de red están funcionando pero les falta la configuración básica para que se pueda acceder a ellas. Para esto deberemos asignarles los IP a cada una de las interfases.

Asignación de nombres a las interfases.

Nos dirigimos al menú y elegimos *INTERFASES*. A continuación nos aparece la lista de interfases que posee nuestro sistema. Hacemos doble clicks sobre las interfases y les vamos cambiando el nombre asignándole los nombres correspondientes a cada una. En nuestro caso utilizaremos:

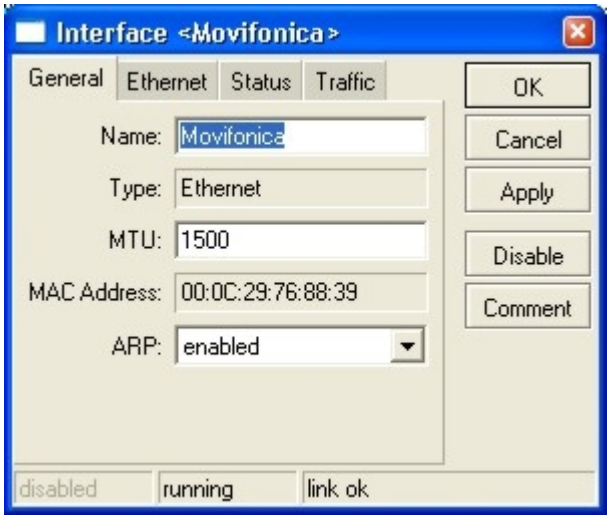
- *Globalphone*, para nuestra conexión dedicada con IP fijo.
- *Movifonica* para nuestra conexión dedicada con IP fijo con el otro proveedor.
- *Ventas:* Será la interfase exclusiva de ventas.
- *Administración*: Será la interfase exclusiva de Administración.
- *Producción*: Será la interfase exclusiva de Producción.
- *Servers*: Será la interfase para la granja de servidores.

- *ADSL*: Será la interfase para conectarse al ADSL de Backup
- *Hotspot*: será la interfase que proveerá acceso a la red mediante el hotspot



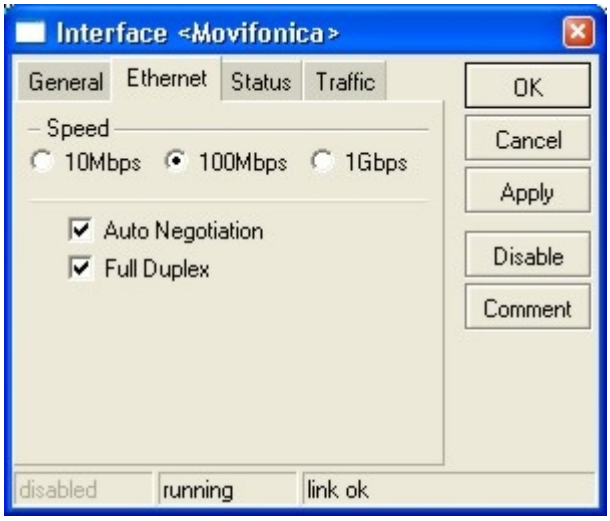
Interfase: Movifonica

- Pestaña *General*:
  - Name: Movifonica
  - MTU: 1500
  - ARP: Enable



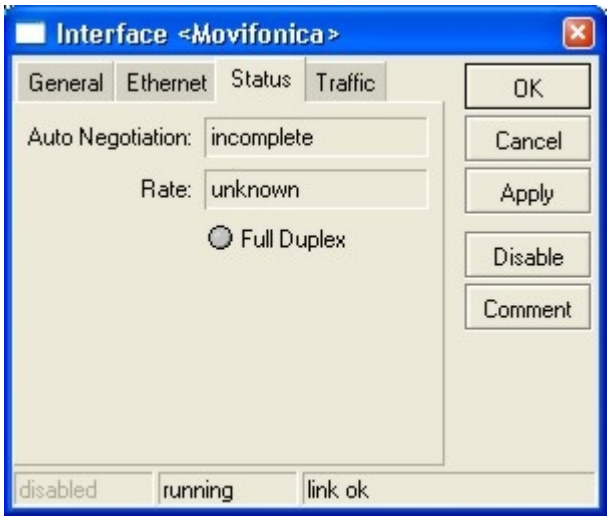
Pestaña *Ethernet*:

- 100Mbps: Seleccionado
- Auto negotiation: seleccionado
- Full duplex: seleccionado.



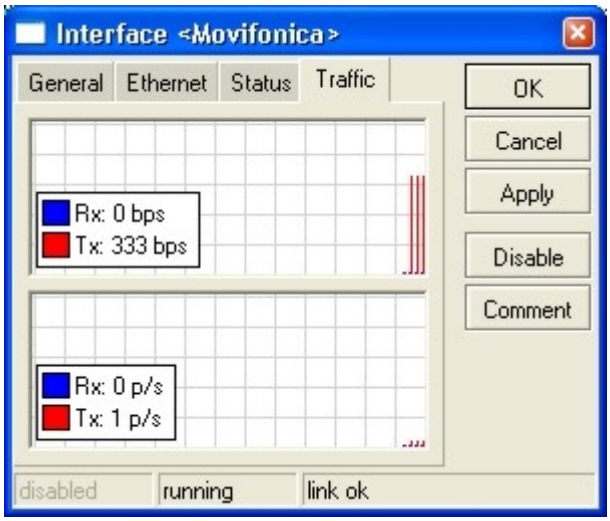
Pestaña *Status*:

En esta ventana podemos ver el estatus la interfase actual.



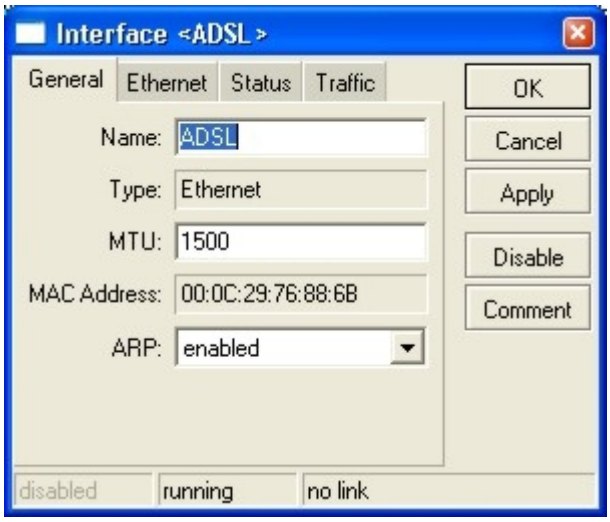
Pestaña *Traffic*:

1. Vemos la grafica de kbps enviados y recibidos por dicha interfase.
2. Vemos la grafica de p/s enviados y recibidos por la interfase.



Interfase: ADSL

- Pestaña *General*:
    - Name:ADSL
    - MTU: 1500
    - ARP: Enable



Interfase: Administracion

- Pestaña *General*:
    - Name: Adminitracion
    - MTU: 1500
    - ARP: Enable

Interfase: Globalphone

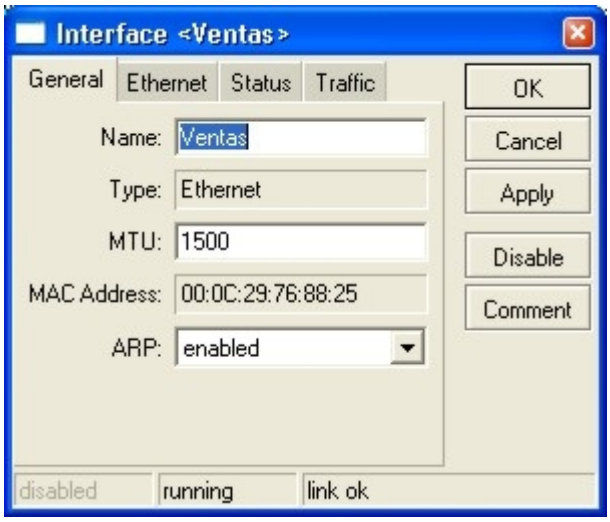
- Pestaña *General*:
    - Name: Globalphone
    - MTU: 1500
    - ARP: Enable

Interfase: Hotspot

- Pestaña *General*:
    - Name: Hotspot
    - MTU: 1500
    - ARP: Enable

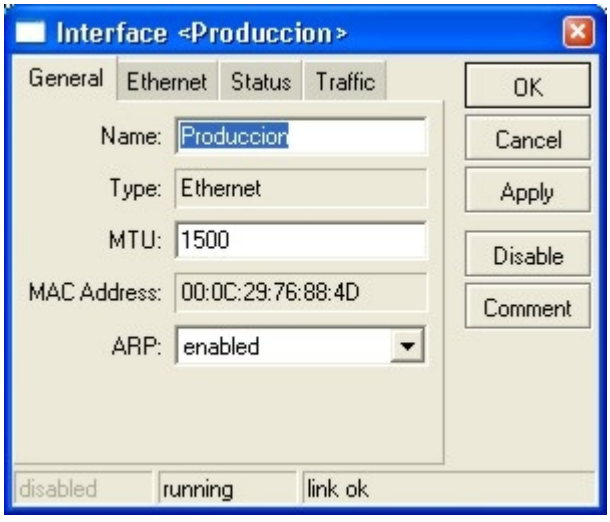
Interfase: Ventas

- Pestaña *General*:
    - Name: Ventas
    - MTU: 1500
    - ARP: Enable



Interfase: Produccion

- Pestaña *General*:
    - Name: Produccion
    - MTU: 1500
    - ARP: Enable



Definición de Vlans

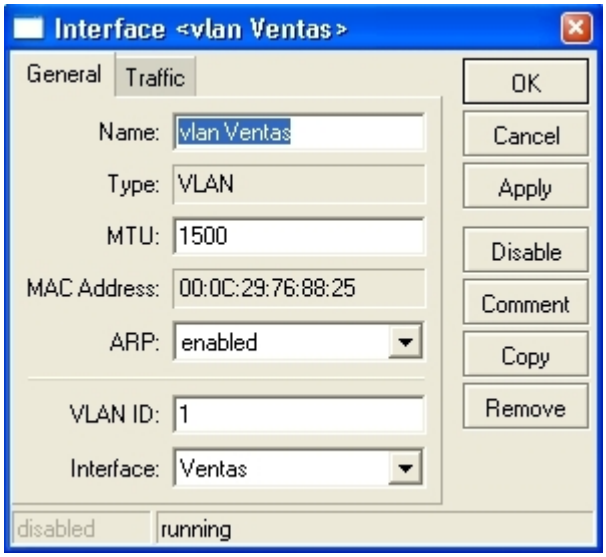
Debido a las características departamentales de la empresa debemos realizar 3 vlans para separar las áreas de:

- Administración
- Ventas
- Producción

Para configurar las vlans debemos ir al menú *Interfases,* se nos abrirá la ventana de configuración de interfases. Hacemos clic sobre el icono (+) y se nos desplegará un menú, elegimos la opción Vlan y entramos a la ventana de configuración de las mismas.

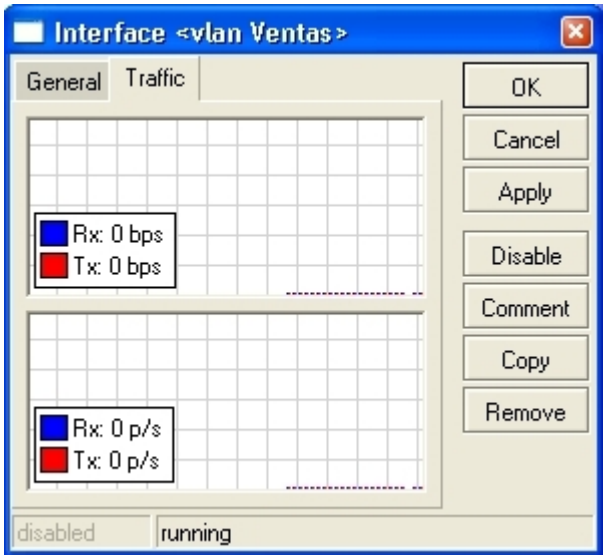
Vlan Ventas

- Pestaña *General*:
    - Name: Vlan_Ventas
    - Type: Vlan
    - MTU: 1500
    - MAC:00:0C29:76:88:25
    - ARP: Enable
    - Vlan ID:1
    - Interfase: Ventas



Pestaña *Traffic:*

- Ver la grafica de kbps enviados y recibidos por dicha vlan
- Ver la grafica de p/s enviados y recibidos por la vlan

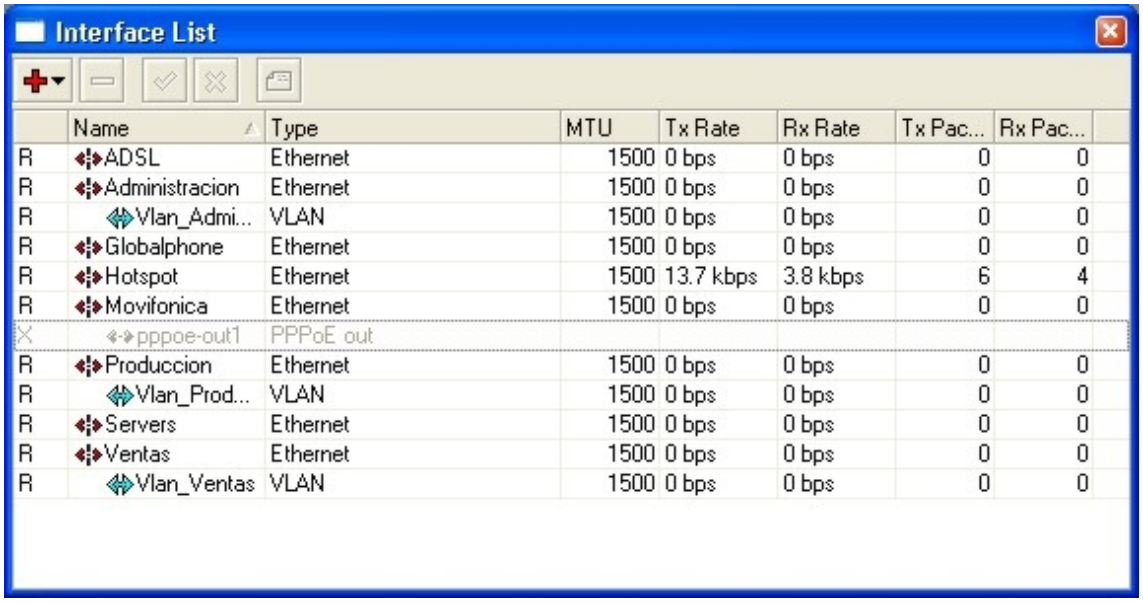


Vlan Administración

- Pestaña *General*:
    - Name: Vlan_Administracion
    - Type: Vlan
    - MTU: 1500
    - MAC:00:0C29:76:88:25
    - ARP: Enable
    - Vlan ID:1
    - Interfase: Adminitracion

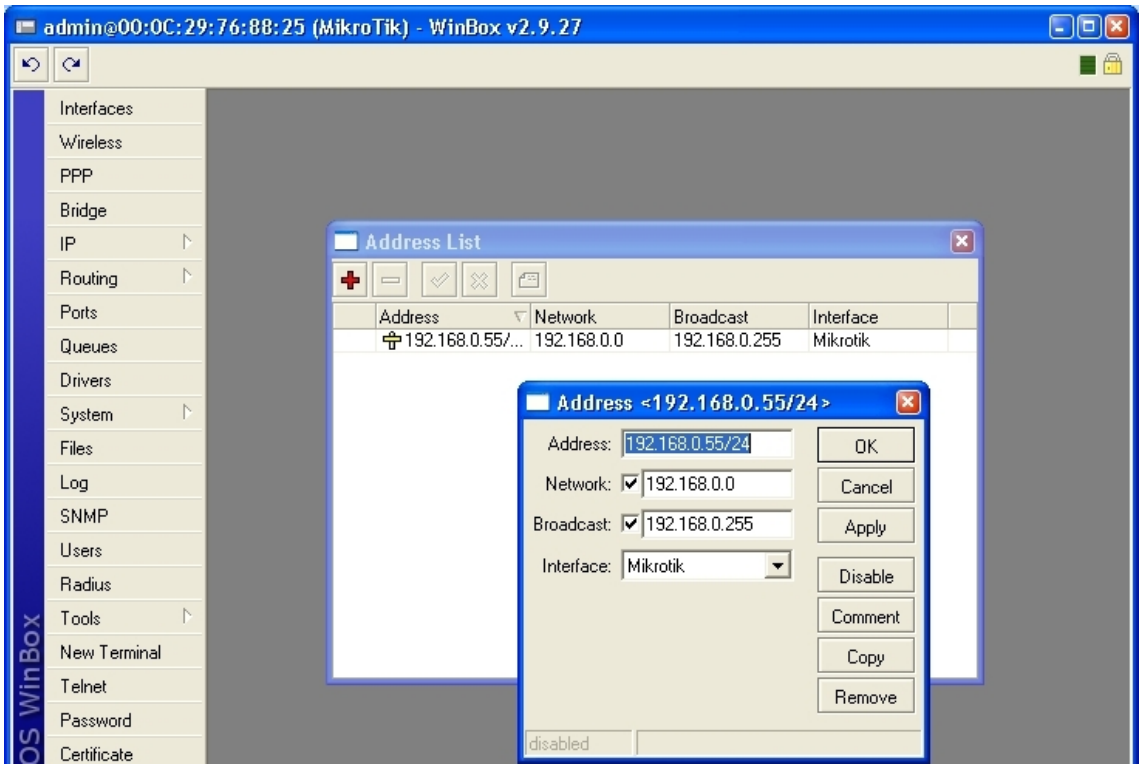
Vlan Produccion

- Pestaña *General*:
    - Name: Vlan_Produccion
    - Type: Vlan
    - MTU: 1500
    - MAC:00:0C29:76:88:25
    - ARP: Enable
    - Vlan ID:1
    - Interfase: Produccion



Asignación de Direcciones IP´s a las interfases

Con los nombres asignados a las interfases, debemos asignarle el IP a las mismas. Para ello debemos ir al menú *IP / Addresses.*



Haciendo clic sobre el icono (+) nos abre una ventana que nos deja introducir los datos necesarios para nuestras interfases.

Interfase *Globalphone:*

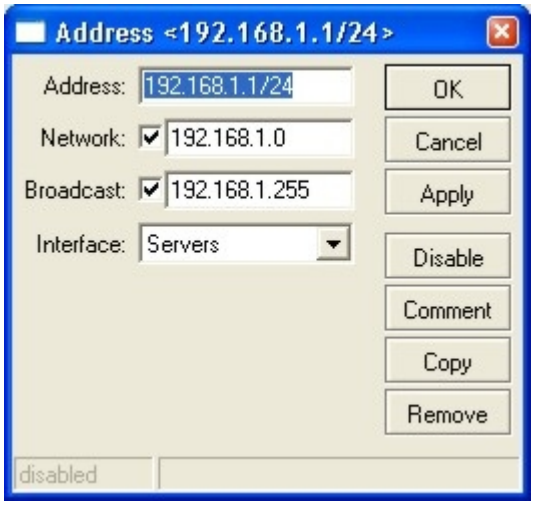
- Address: 200.45.3.10/30
- Network 200.45.3.0
- Broadcast: 200.45.3.255
- Interfase: Globalphone

Interfase *Movofonica*:

- Address: 200.45.4.10/30
- Network: 200.45.4.0
- Broadcast: 200.45.4.255
- Interfase: Movifonica

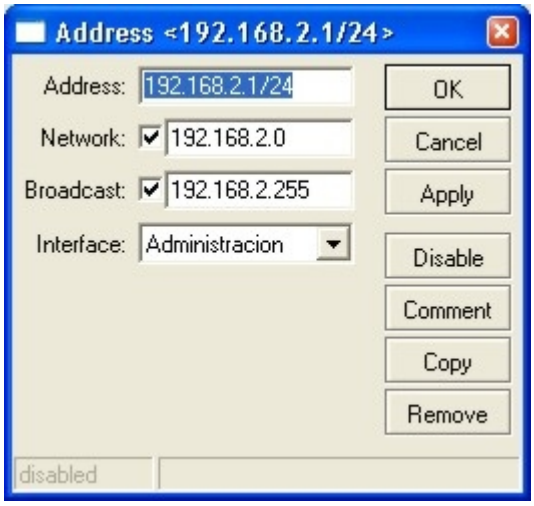
Interfase *Servers:*

- Address: 192.168.4.10/24
- Network: 192.168.4.0
- Broadcast: 192.168.4.255
- Interfase: Servers



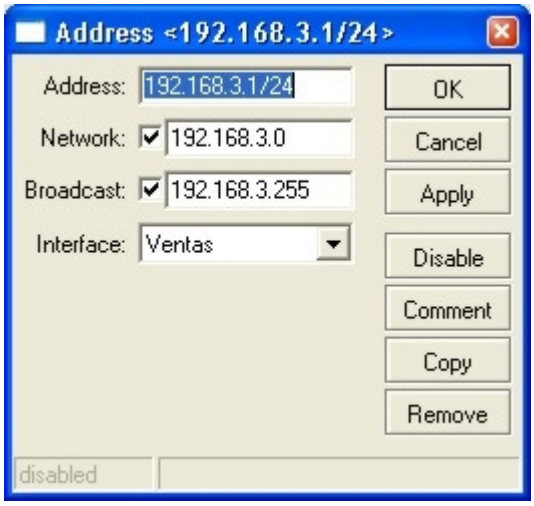
Interfase *Administración:*

- Address: 192.168.2.1/24
- Network: 192.168.2.0
- Broadcast: 192.168.2.255
- Interfase: Administración



Interfase *Ventas:*

- Address: 192.168.3.1/24
- Network: 192.168.3.0
- Broadcast: 192.168.3.255
- Interfase: Ventas

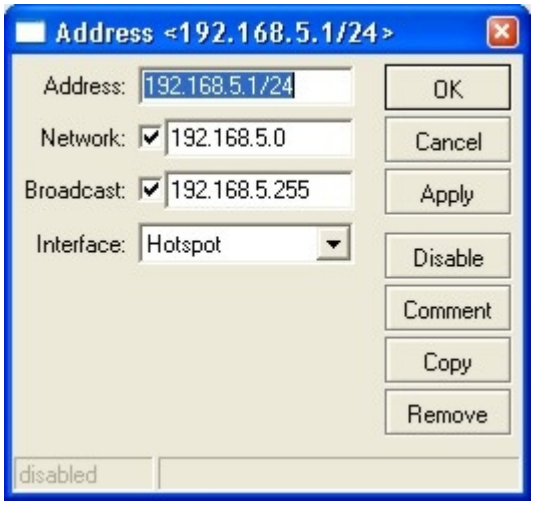


Interfase *Producción:*

- Address: 192.168.4.1/24
- Network: 192.168.4.0
- Broadcast: 192.168.4.255
- Interfase: Producción

Interfase *Hot spot:*

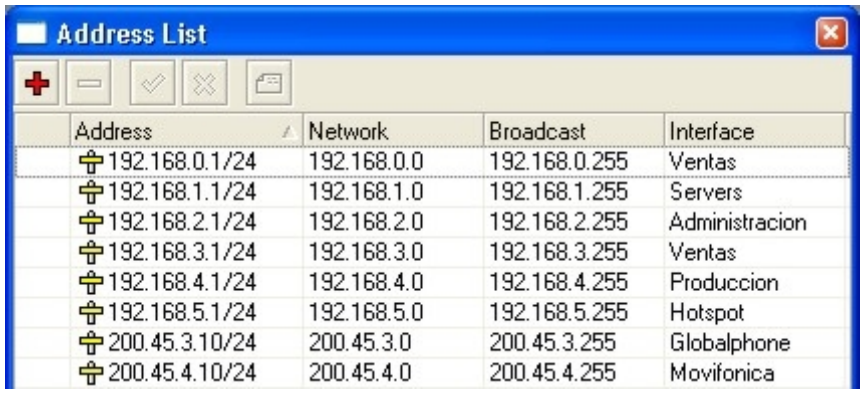
- Address: 192.168.5.1/24
- Network: 192.168.5.0
- Broadcast: 192.168.5.255
- Interfase: Hot spot



Interfase *ADSL*

- Address: 192.168.0.1/24
- Network: 192.168.0.0
- Broadcast: 192.168.0.255
- Interfase: ADSL

La configuración final se ve de la siguiente manera:



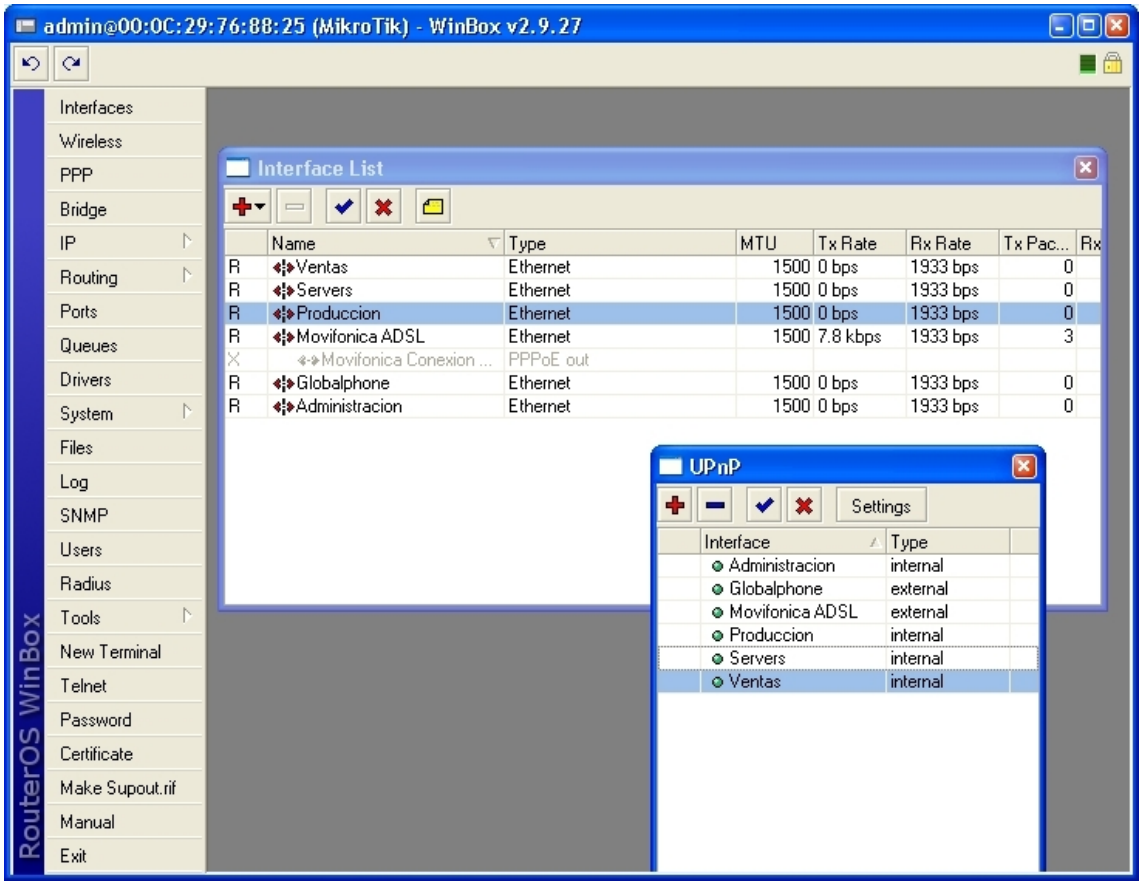
Address	Network	Broadcast	Interface
192.168.0.1/24	192.168.0.0	192.168.0.255	Ventas
192.168.1.1/24	192.168.1.0	192.168.1.255	Servers
192.168.2.1/24	192.168.2.0	192.168.2.255	Administracion
192.168.3.1/24	192.168.3.0	192.168.3.255	Ventas
192.168.4.1/24	192.168.4.0	192.168.4.255	Produccion
192.168.5.1/24	192.168.5.0	192.168.5.255	Hotspot
200.45.3.10/24	200.45.3.0	200.45.3.255	Globalphone
200.45.4.10/24	200.45.4.0	200.45.4.255	Movifonica

Definimos UPnP para las interfases:

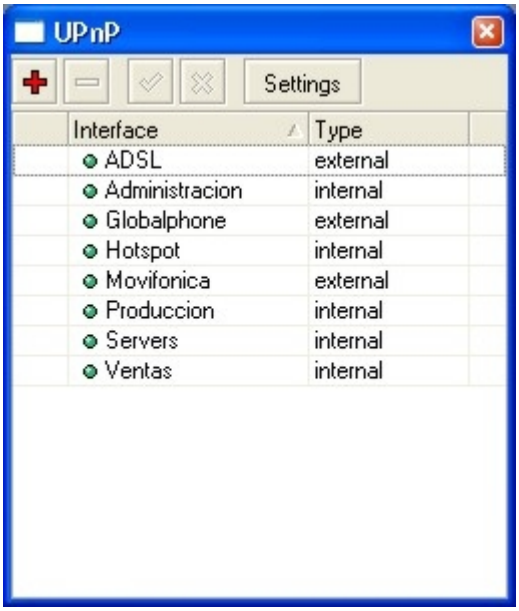
En este segmento simplemente tenemos que definir cuales de nuestras interfases van a “mirar hacia Internet” y cuales van a estar dentro de nuestra red. Nosotros configuraremos a las conexiones como:

- *Ventas:* Interna.
- *Administración:* Interna
- *Producción:* Interna
- *Servers:* Interna
- *Hotspot:* Interna
- *Movifoncia:* Externa.
- *Globalphone:* Externa.
- *ADSL:* Externa

Para realizar dicha configuración debemos ir en el menú a: *IP / UNPnP*. Hacemos clic sobre el icono (+) y asignamos a cada una de las interfases si es interna o externa.



Luego de haber asignado los tipos de interfase debemos configurar un último detalle en settings. Le deseleccionamos la opción “allow to disable External Interfase”

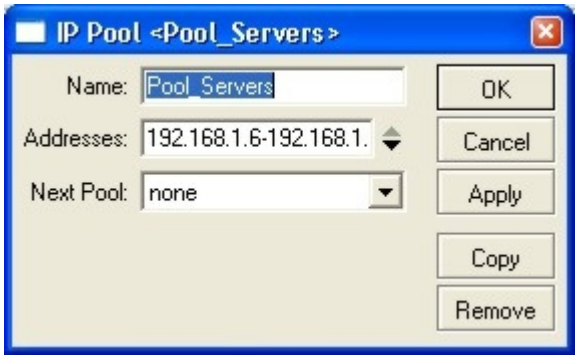


Configuración Pools de Direcciones de IP

En una primera instancia hay que crear los pool's de ip´s que van a poseer los grupos de administración, ventas y producción y servers.

Para ello Vamos al menú *IP / POOL*. Se nos abre la ventana de configuración de pool y hacemos clic en el icono (+). En la nueva ventana creamos cada pool para cada una de los grupos. La configuración de los mismos es:

- Nombre: *Pool Servers*
- Rango de ip: 192.168.1.5 a 192.168.1.254

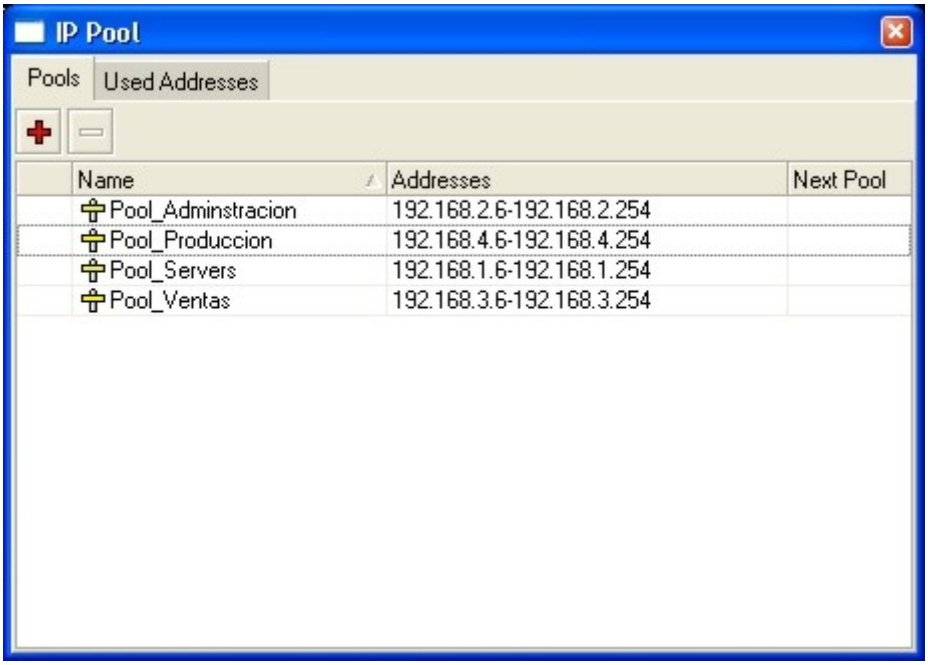


- Nombre: *Pool Ventas*
- Rango de ip: 192.168.2.5 a 192.168.2.254

- Nombre: *Pool Producción*
- Rango de ip: 192.168.4.5 a 192.168.4.254

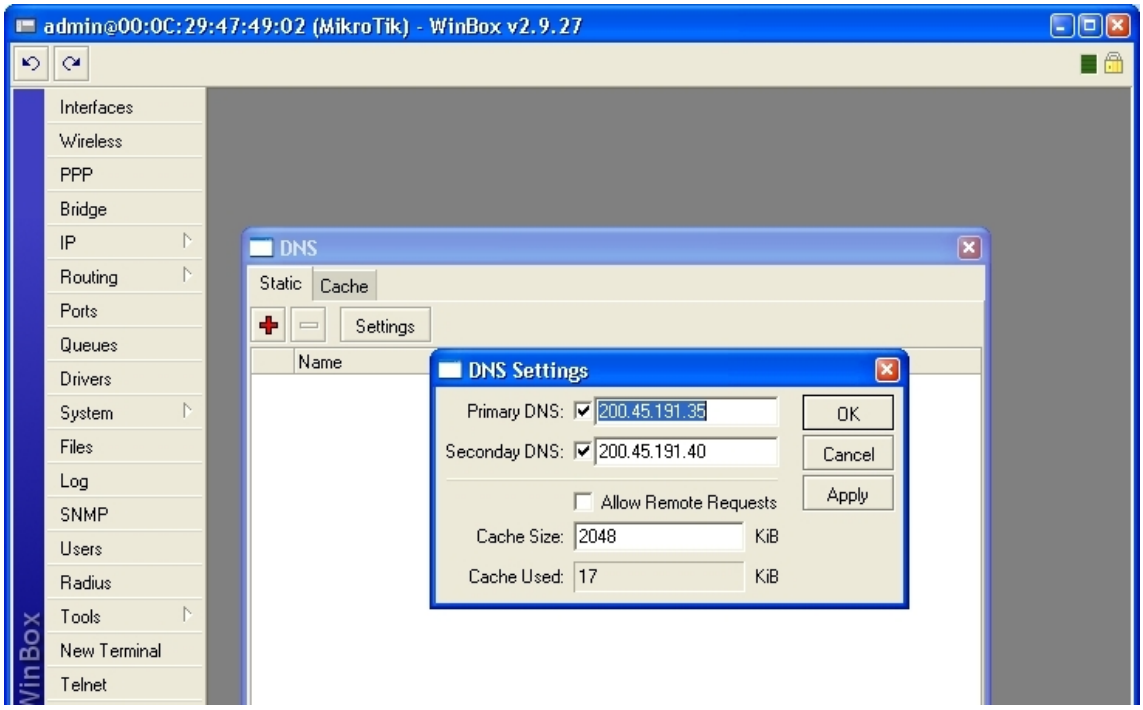
- Nombre: *Pool Administración*
- Rango de ip: 192.168.2.5 a 192.168.2.254

Se ha elegido comenzar todos los rangos a partir del ip x.x.x.5 para reservar números de ip en el caso que se necesite instalar algún tipo de servidor en cada grupo.



Definir DNS

Para definir los DNS simplemente hay que ir al menú *IP / DNS*. Se nos abre una ventana de configuración. Hacemos clic en *Settings* y escribimos los dns del proveedor de Internet.



Los datos que ingresamos son:

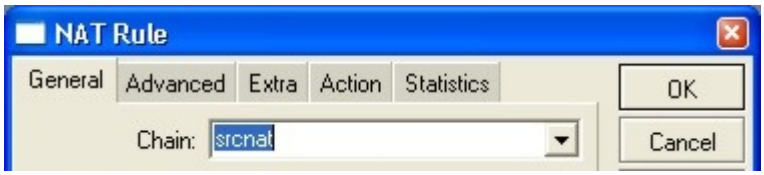
Primary DNS: 200.45.191.35
Secondary DNS: 200.45.191.40

Nat Masquerade para todas las redes

Par realizar el nat transparente entre todas las redes debemos ir al menú *IP/FIREWALL*. Ahí en la nueva ventana nos dirigimos a la pestaña *NAT* y hacemos clic sobre el icono (+). A continuación aparece una ventana nueva de configuración para políticas de *NAT* y la configuramos de la siguiente manera:

Pestaña General:

- Chan: srcnat



Pestaña Action:

- Action: masquerade

Configuración Servidor DHCP

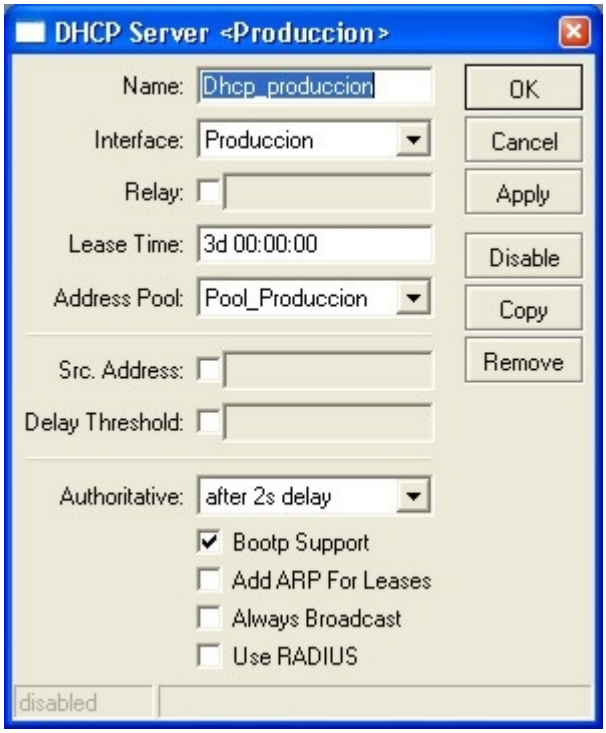
A continuación daremos de alta el servidor de DHCP en si. Para ello debemos ir al menú *IP / DHCP Server.* Se nos abrirá una ventana de configuración de servidores dhcp. Hacemos clic en el icono (+) y creamos nuestros servidores de dhcp para cada una de las áreas ya mencionadas.

Ventana de configuración DHCP:

En esta ventana iremos introduciendo todos los requisitos necesario para ir levantado los servidores de dhcp. La configuración para cada uno de los servidores dhcp fue la siguiente:

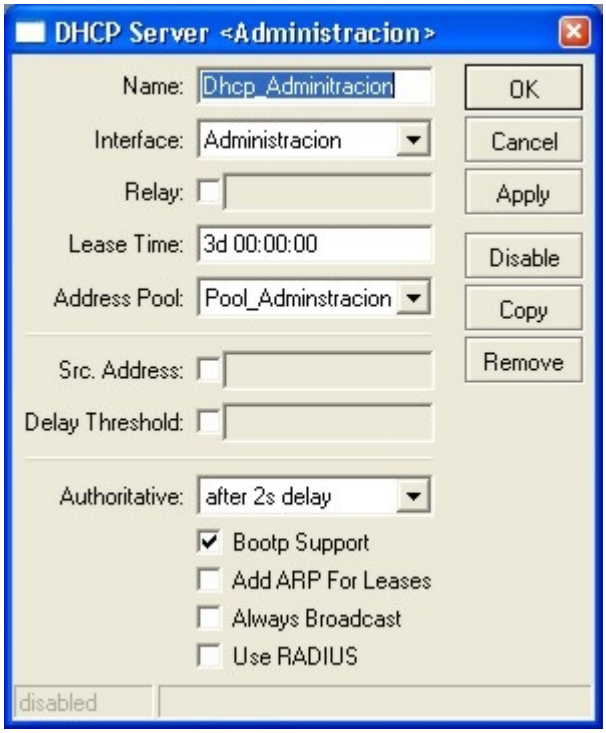
DHCP Producción:

- Nombre: DHCP Producción
- Interfase: Producción
- Address Pool: Pool Producción



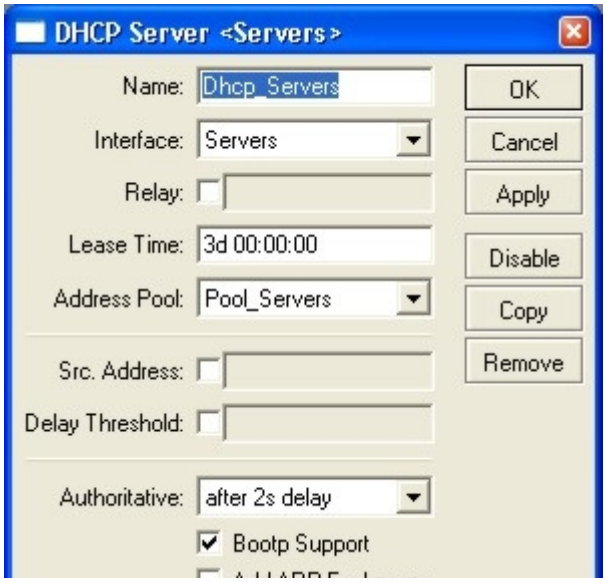
DHCP Administración:

- Nombre: DHCP Administración
- Interfase: Administración
- Address Pool: Pool Administración



DHCP Servers:

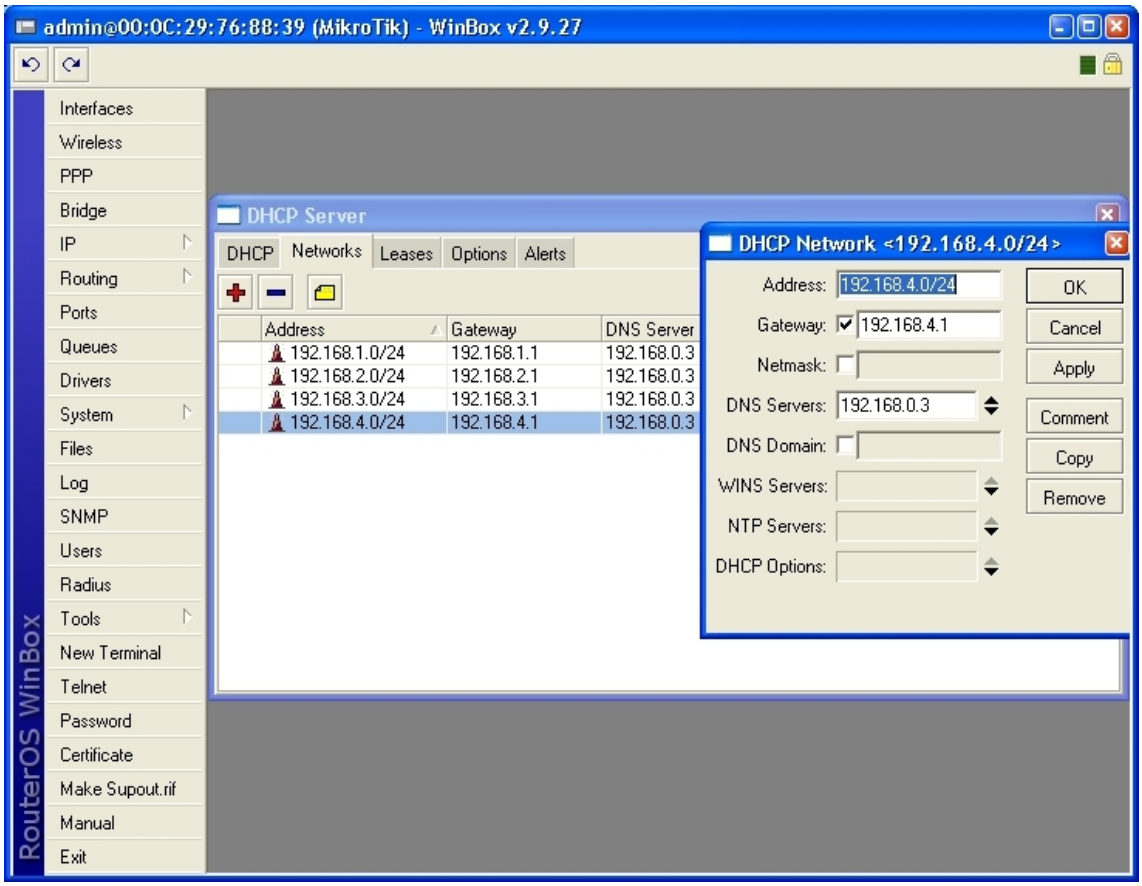
- Nombre: DHCP Servers
- Interfase: Servers
- Address Pool: Pool Servers



DHCP Ventas:

- Nombre: DHCP Ventas.
- Interfase: Ventas.
- Address Pool: Pool Ventas.

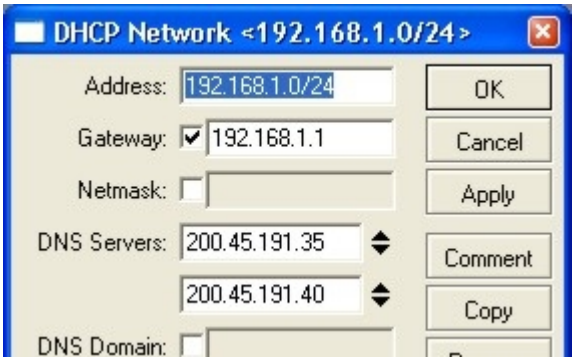
No obstante los servidores de dhcp están configurados, necesitamos configurar las *´redes´*. Para ello en la ventana de DHCP Server hacemos clic en la pestaña *Network.* Luego hacemos clic en el icono (+) y cargamos los datos de la red.



Configuración:

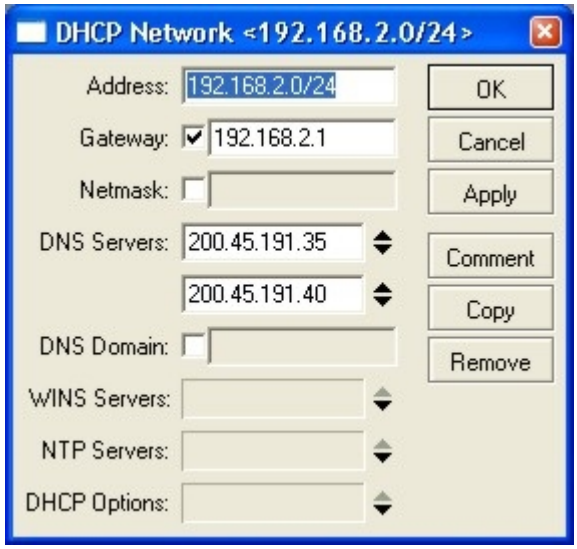
Red *Servers:*

- Address: 192.168.1.0/24
- Gateway: 192.168.1.1
- Dns Server: 192.168.0.3



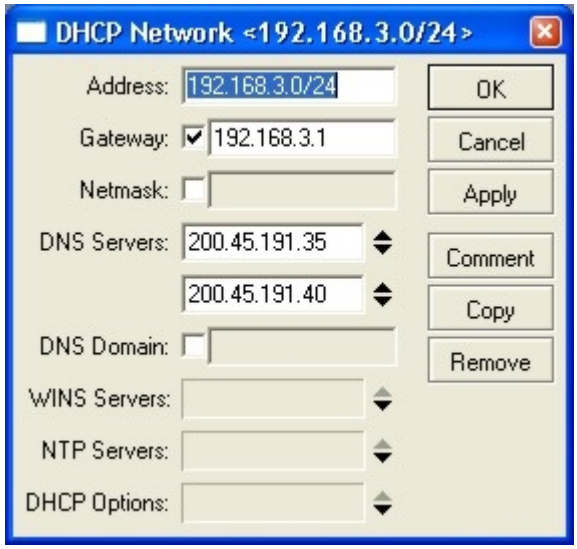
Red *Administración:*

- Address: 192.168.2.0/24
- Gateway: 192.168.2.1
- Dns Server: 192.168.0.3



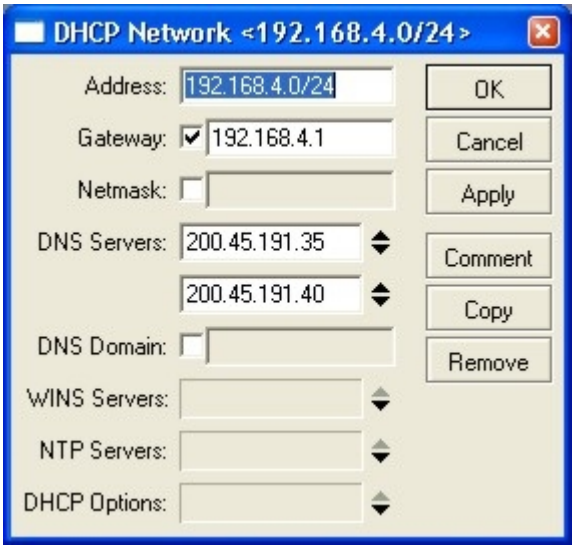
Red *Ventas:*

- Address: 192.168.3.0/24
- Gateway: 192.168.3.1
- Dns Server: 192.168.0.3



Red *Producción:*

- Address: 192.168.4.0/24
- Gateway: 192.168.4.1
- Dns Server: 192.168.0.3

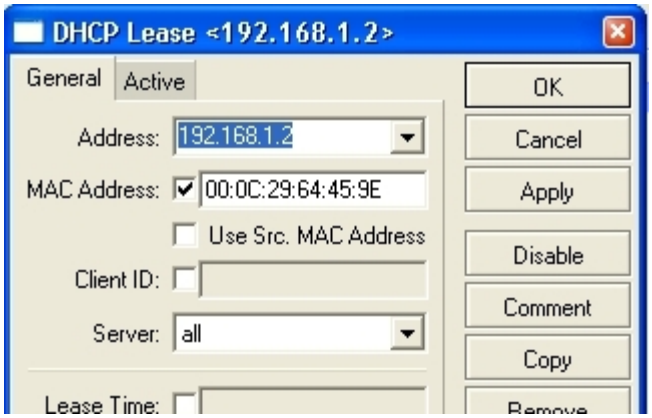


Asignación de direcciones de ip fijas a partir de direcciones MAC.

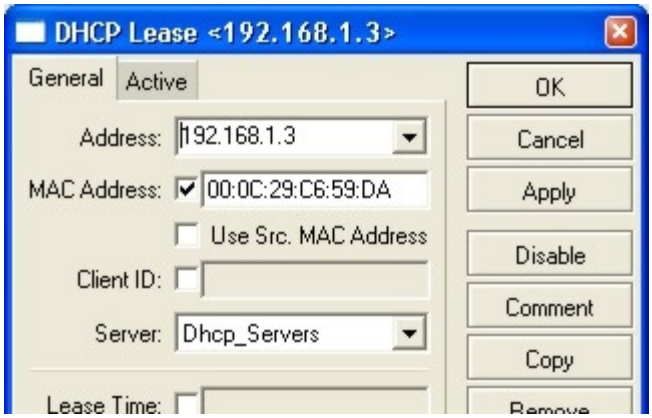
Debemos asignarle ip fijo a nuestros servidores para que sea mas simple nuestra configuración del sistema. Para ello la asignación de ip fijo la hacemos mediante el servidor de dhcp, asignando una dirección de ip fija a una Mac.

Los pasos de configuración son los siguientes. Nos dirigimos al menú *IP / DHCP Server*. En la ventana que nos aparece hacemos clic en la pestaña *LEASES*. En mencionada pestaña hacemos clic en el icono (+). La configuración de la ventanuela es:

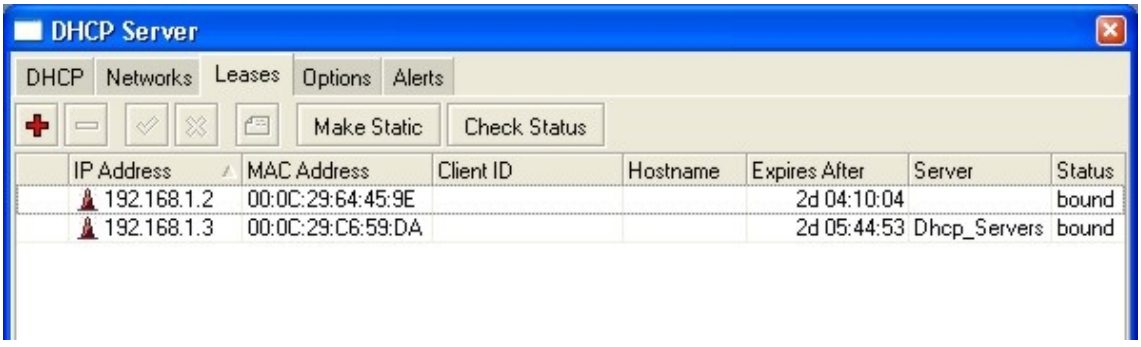
- Server de snmp, jabber:
    - Address: 192.168.1.2
    - MAC Address: 00:0C:29:64:45:9E (MAC del servidor snmp, jabber)
    - Servers: all



- Server RADIUS:
    - Address: 192.168.1.3
    - MAC Address: 00:0C:29:C6:59:DA (MAC del servidor)
    - Servers: all



Luego para que esta asignación quede estática debemos hacer clic en el botón de *MAKE STATIC.* De la pestaña *LEASES.*



Configuración Servidor - Cliente NTP:

Debido a que utilizaremos políticas referenciadas a tiempo debemos ser precisos con el mismo. Para ello debemos instalar un cliente en nuestro Mikrotik para tener la hora precisa y un servidor para brindarles dicha hora a los clientes. Consecuentemente debemos seguir los siguientes pasos.

Servidor NTP

Para el servidor nos dirigimos al menú *SYSTEM / NTP SERVER*. En la nueva ventana Seleccionamos solamente la opción *MANYCAST* y hacemos clic en el botón de *ENABLE*

Ahora Con esta configuración del servidor podemos hacer que todas las computadoras de la red estén sincronizadas con nuestro servidor de tiempo.

Cliente NTP

Para configurar nuestro cliente NTP, para que nos sincronice nuestra hora del Mikrotik conjuntamente con la de un reloj nuclear. Debemos ir al menú *SYSTEM / NTP CLIENT*. Se nos abrirá la ventana de configuración del cliente NTP y le asignamos los calores siguientes:

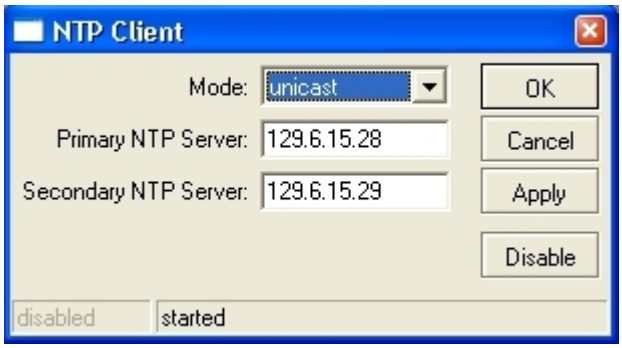
- Mode: Unicast
- Primary NTP Server: 129.6.15.28
- Secondary NTP Server: 129.6.15.29

Luego hacemos clic en *ENABLE*.

Dichos servidores son:

- time-a.nist.gov
  129.6.15.28
  NIST, Gaithersburg, Maryland

- time-b.nist.gov
  129.6.15.29
  NIST, Gaithersburg, Maryland



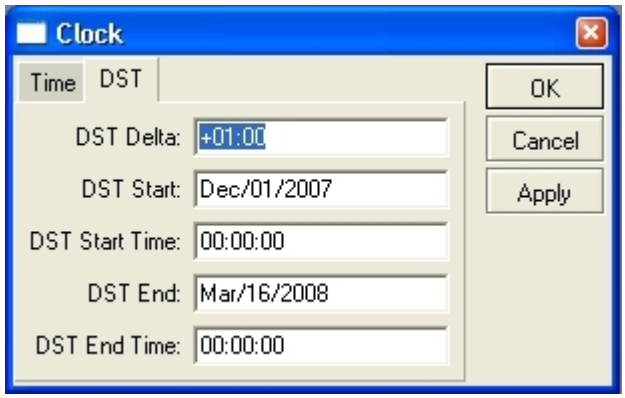
A continuación nos dirigimos al menú *SYSTEM / CLOCK*. En la nueva ventana le cargamos los datos de fecha, hora, y uso horario. Para nuestro caso los mismos son:

- Date: Apr/04/2008
- Time: 16:17:00
- Time Zone: -03:00

Utilizamos -03:00 para la Time Zone ya que nosotros en Cordoba tenemos ese uso horario que es el mismo de Buenos Aires respecto a Greenwich.

En la pestaña DST, configuraremos cambios del uso horario por ejemplo: en el horario de verano que tenemos 1 hora de diferencia. Par ello hacemos clic en DST. Los datos que utilizaremos como ejemplo son los siguientes:

- DST Delta: +:01:00
- DST Start: Dec/01/2007
- DST Start Time: 00:00:00
- DST End: Mar/16/2008
- DST End Time:00:00:00



Habilitando esta opción nos ahorramos todos los inconvenientes de cambiar los horarios de todas las políticas que se hayan generado.

Servidor y Cliente PPPoE

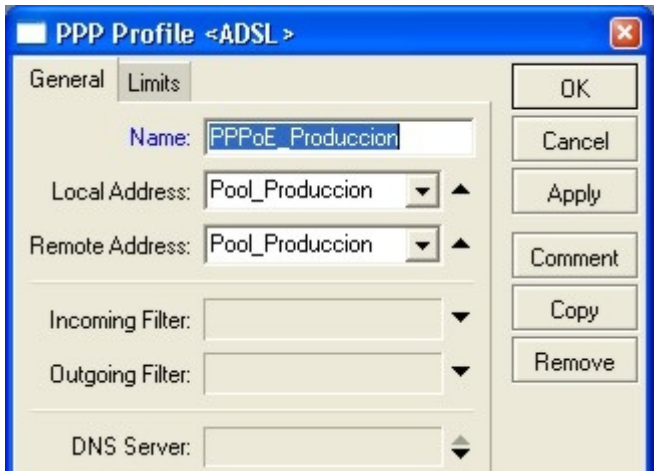
Configuración Servidor PPPoE

Debido a que la sub red de producción se podrá acceder desde otras subredes de la empresa se decidió por cuestiones de seguridad acceder mediante una conexión PPPoE. Debemos habilitarle el servidor de PPPoE. Para ello nos dirigimos al menú *PPP*. Se nos abre la ventana de configuración de PPP.

Luego nos dirigimos a la pestaña *Profiles*. Ahí hacemos clic en el icono (+) para generar el perfil de usuario que necesitamos. A continuación se nos abre una ventana y la llenamos con los siguientes datos:

- Name: PPPoE_Produccion
- Local Address: Pool_Produccion
- Remote Address: Pool_Produccion

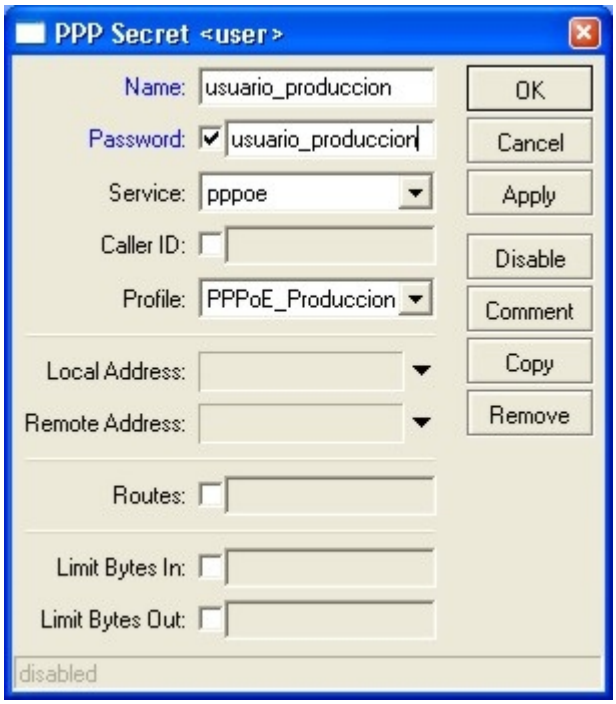
Luego toda la otra información la dejamos por defecto.



A Continuación nos dirigimos nuevamente al menú *PPP* y en la ventana que se abrió nos dirigimos a la pestaña *Secrets*. Ahí hacemos clic en el icono (+) y

generaremos nuestro usuario. Para ello llenaremos la ventana con la siguiente información:

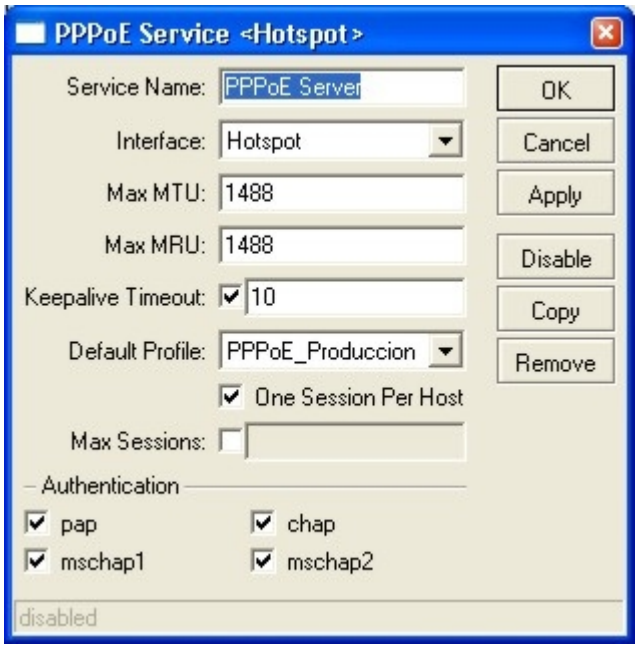
- Name: Usuario_Produccion
- Password: Usuario_Produccion
- Service: pppoe
- Profile PPPoE_Produccion



Nos dirigimos nuevamente al menú ***PPP***. En la ventana nueva hacemos clic sobre el botón PPPoE Server. En la nueva ventana que se nos abre configuraremos el nuevo servidor de PPPoE. Para ello debemos hacer clic en el botón (+). La configuración del mismo será:

- Service Name: PPPoE Server
- Interfase: Hotspot
- Max MUT: 1488
- Min MUT: 1488
- Keep Alive time out: 10

- Default Profile: PPPoE_Produccion
- Autenticaciones: PAP, chap mschap1 y mschap2

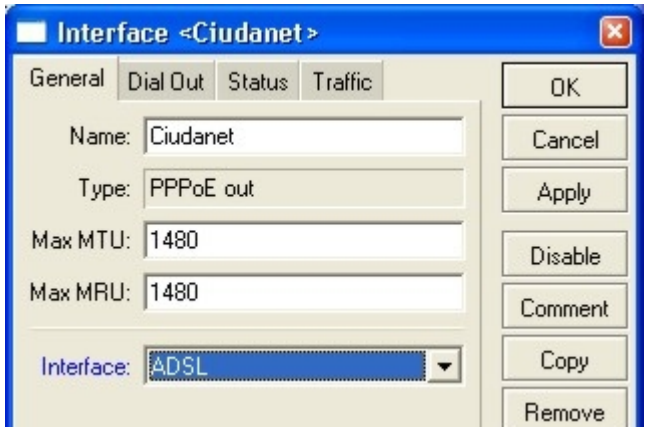


Configuración Cliente PPPoE:

Para configurar la conexión a Internet mediante el ADSL debemos generar la conexión con el proveedor, para ello debemos ir al menú y seleccionar *PPP*. Se nos abre una ventana y debemos presionar en el (+) y elegir PPPoE Client. Para configurar la conexión de ADSL seguimos los siguientes pasos.

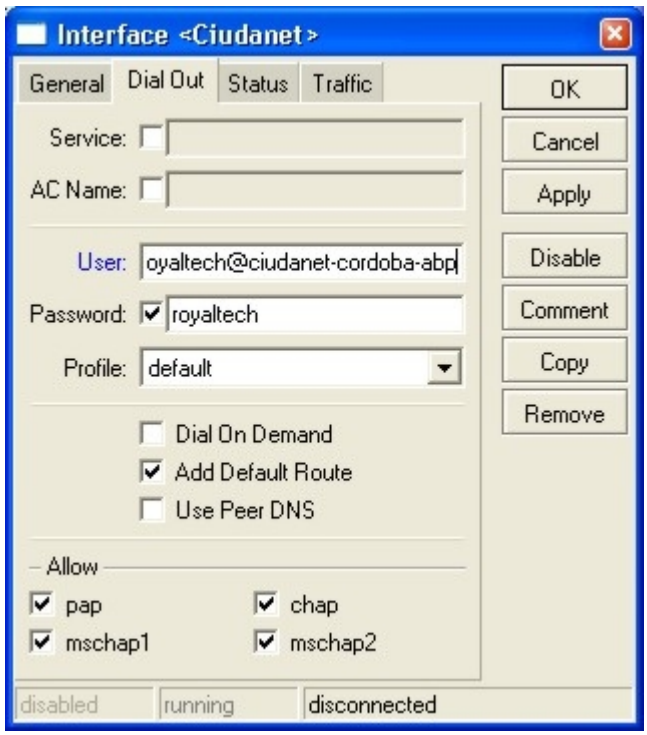
En la pestaña *General*:

- Introducimos el nombre de la conexión “Ciudanet”
- Max MTU:1480
- Max MRU: 1480
- Seleccionamos la interfase por donde queremos realizar la conexión de Adel “ADSL”.



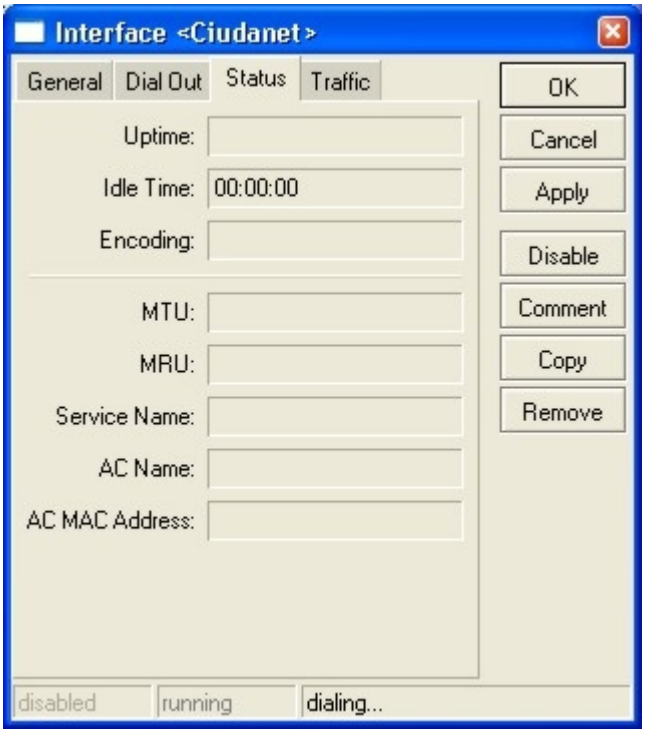
En la pestaña D*ial Out:*

- User: royaltech@ciudanet-cordoba-apb
- Password: royaltech
- Profile: Default
- Add default Route
- PAP, chap, Mschap, mschap2: (seleccionados)



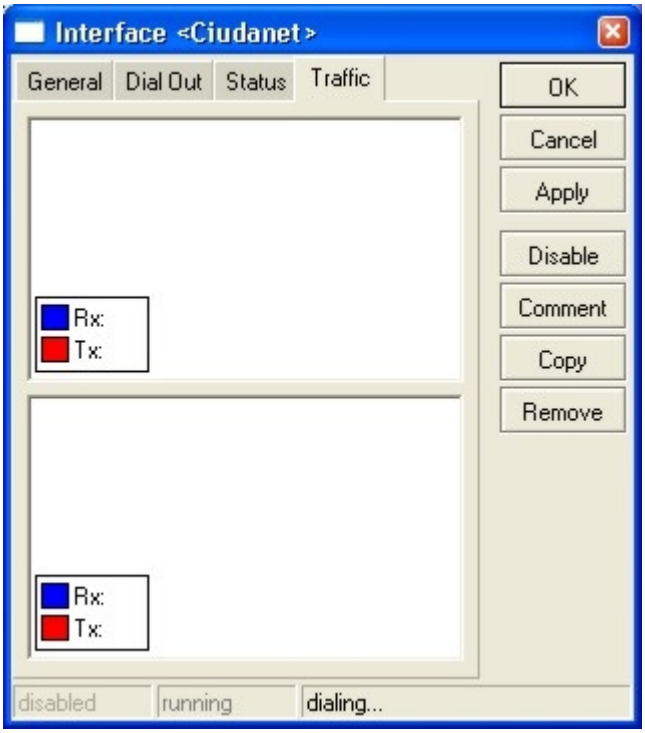
En la pestaña *Status* Podemos:

- Ver el tiempo activo de la conexión
- Ver el tiempo que estuvo inactivo la conexión
- El tipo de codificación
- Tamaño MTU
- Tamaño MRU
- El nombre del servicio
- El AC Name
- AC MAC Address



En la pestaña *Traffic* podemos:

- Ver la grafica que los bps enviados y recibidos.
- Ver la grafica de p/s enviados y recibidos.



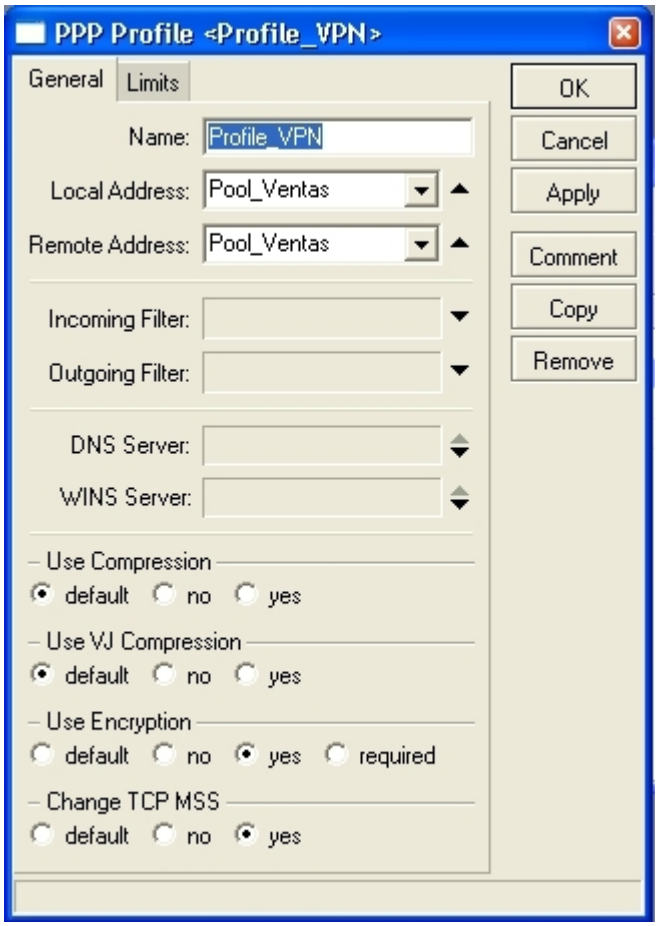
Servidor – Cliente PPTP

Configuración Servidor PPTP:

Debido a que tenemos oficinas de ventas fuera de córdoba, surgió la necesidad de realizar una VPN entre Buenos Aires y Córdoba. Para ello se necesita configurar el servidor de PPTP en la ciudad de Córdoba. Los pasos para dicha con figuración son:

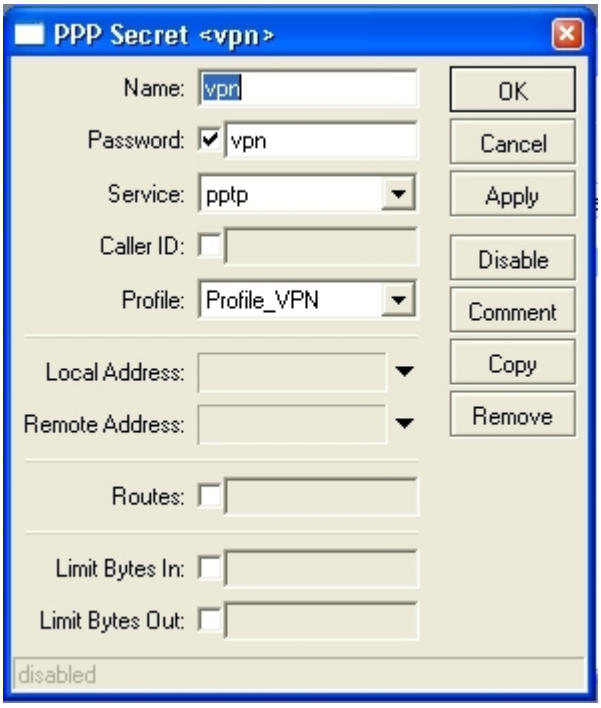
Debemos ir al menú *PPP*, se nos abrirá la ventana de configuración de conexiones PPPx. Luego hacemos clic en la pestaña *PROFILES*. A continuación hacemos clic en icono (+). Con la nueva ventana de profiles abierta la configuramos de la siguiente manera:

- Name: Profile_VPN
- Local Address: Pool_Ventas
- Remote Address: Pool_Ventas
- Use compresión: Default
- Use Vj Compression: Default
- User Encryption: Yes
- Change TCP MMS: Yes



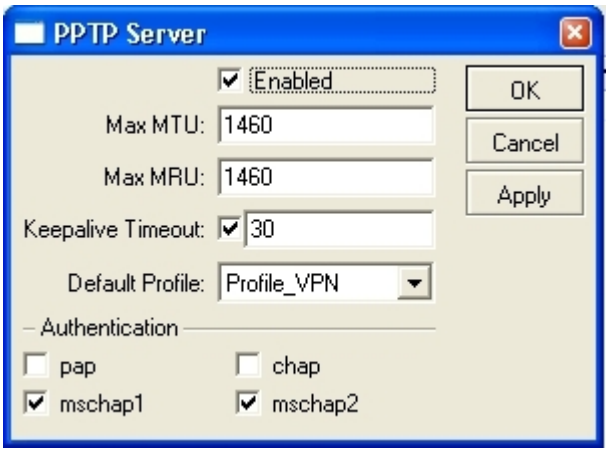
Con el profile ya generado para VPN debemos crear el usuario que utilizara dicho profile. Para ello vamos al menú *PPP*, hacemos clic en la pestaña *SECRESTS*. Hacemos clic sobre el icono (+) y en la nueva ventana la configuramos de la siguiente manera:

- Name: vpn
- Password: vpn
- Service: pptp
- Profile: Profile_VPN



Finalmente debemos dar de alta el servidor de PPTP. Para ello nos dirigimos al menú ***PPP***, en la pestaña Interfases hacemos clic sobre el botón PPTP Server. En la nueva ventana la configuramos de la manera siguiente:

- Enable (seleccionado)
- Max MTU: 1460
- Max MRU: 1460
- Keepalive Timeout:30
- Default Profile: Profile_VPN
- Mschap1 y mschap2 (seleccionados)

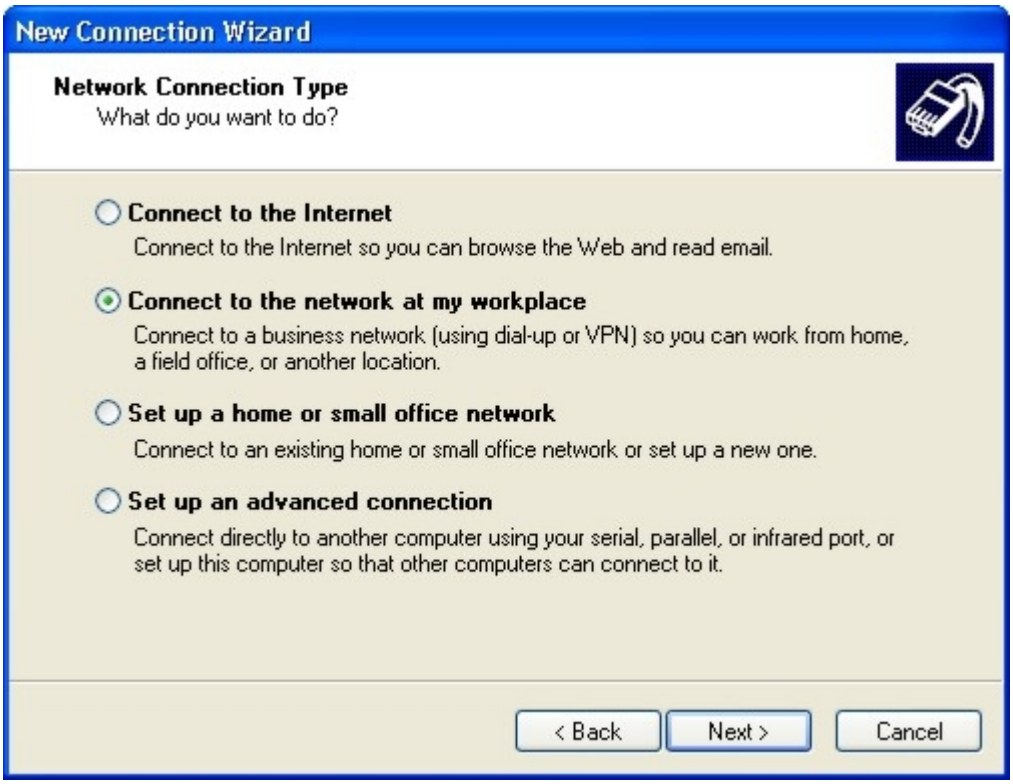


Configuración Cliente PPTP

Utilizaremos la conexión de vpn de Windows Xp para el ejemplo. En el escritorio de Windows nos dirigimos a *INICIO / PANEL DE CONTROL / CONEXIONES DE RED*. Creamos una conexión nueva siguiendo los próximos pasos.

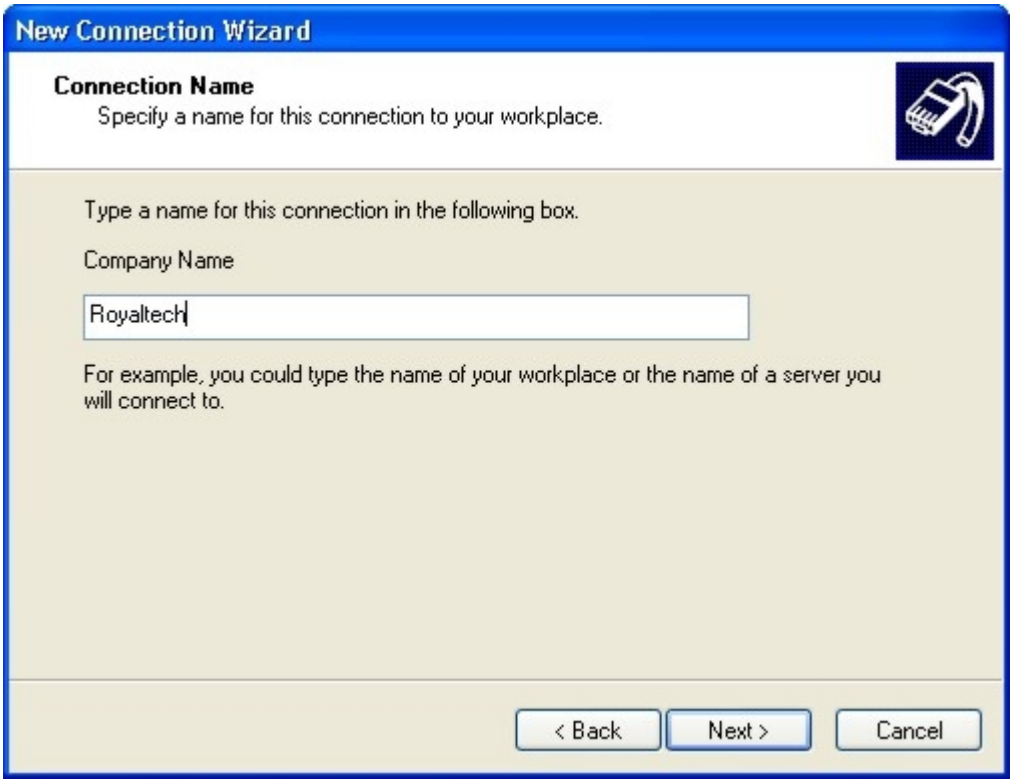
Hacemos clic en siguiente

Seleccionamos Connect to the network at my place

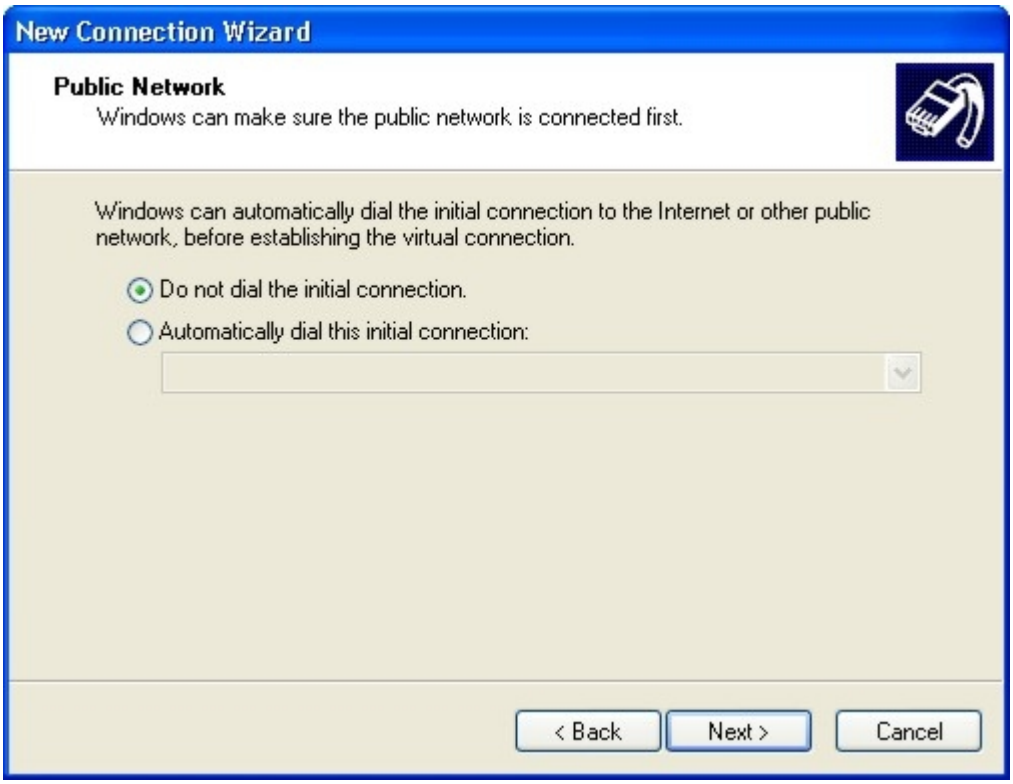


Seleccionamos Virtual Private Network Connection

Escribimos el nombre de la conexión: Royaltech

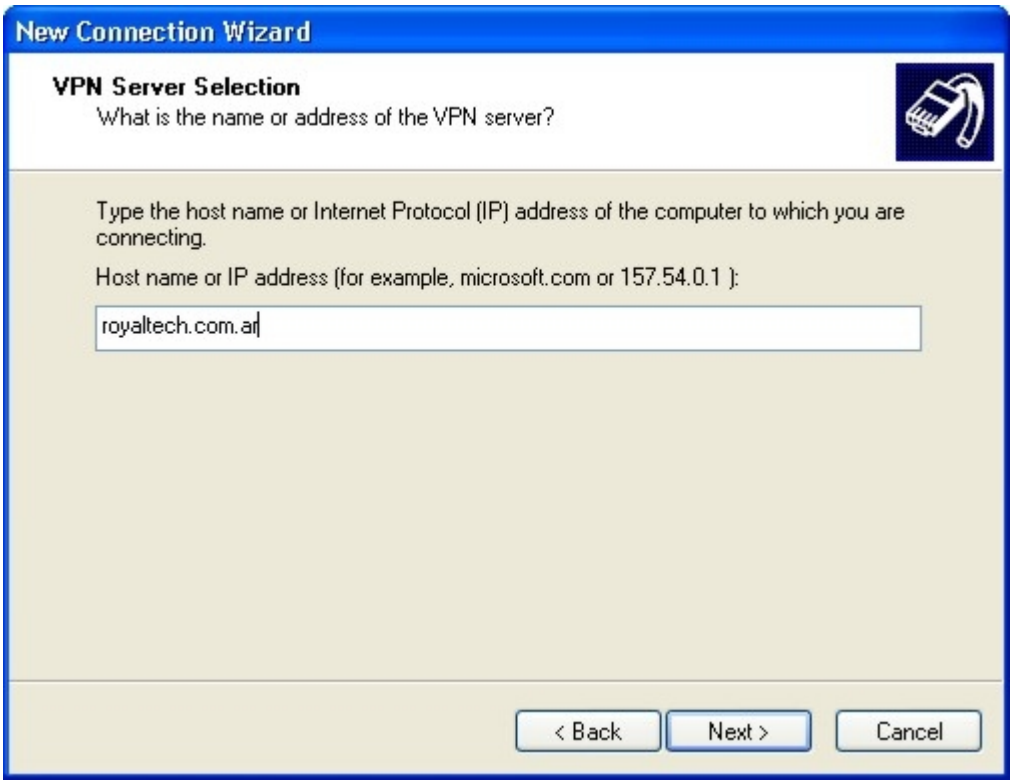


Seleccionamos que no nos disque una conexión inicial. Para el caso de que utilicemos el ip fijo en nuestras oficinas en Buenos Aires. Luego clic en Siguiente



Finalmente escribimos la dirección web de nuestro servidor.

- Address: royaltech.com.ar

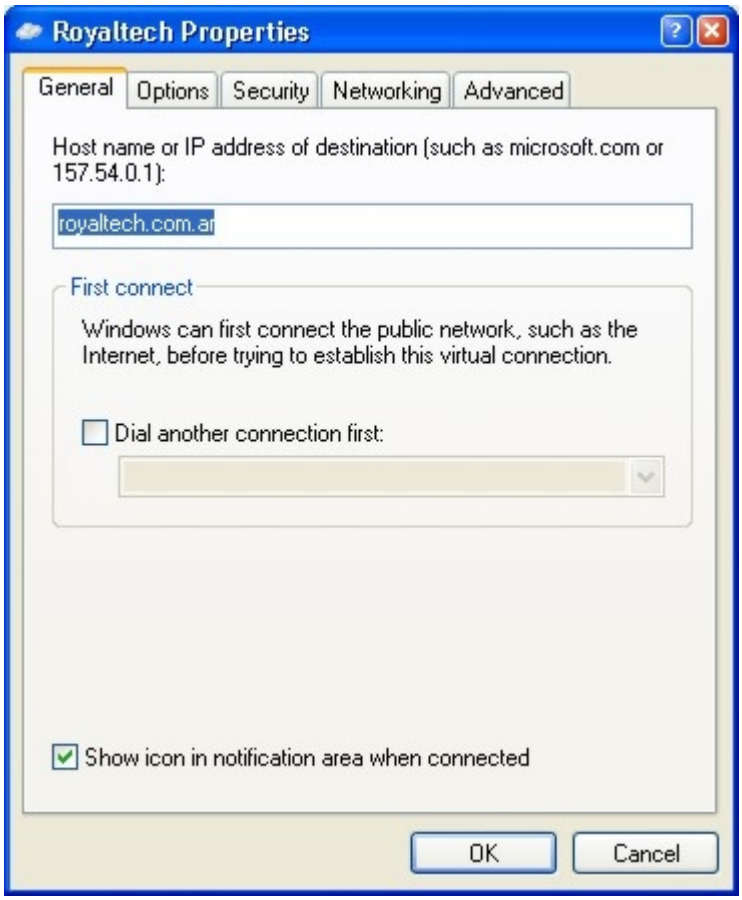


A continuación hay que configurar el tipo de autenticación que vamos a utilizar para ello nos paramos sobre la conexión Royaltech, la abrimos.

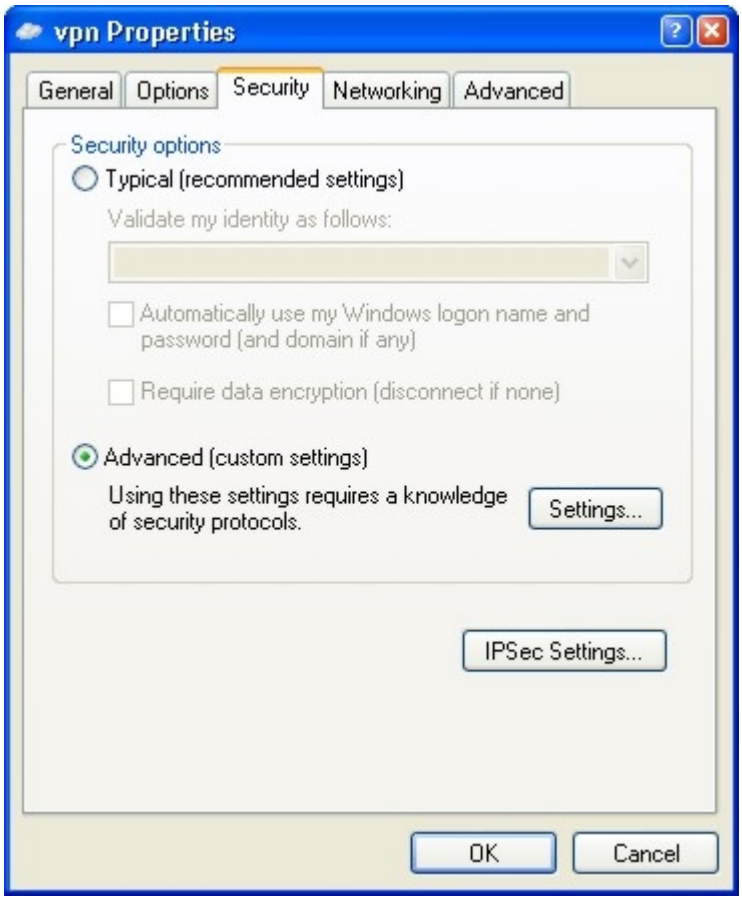
A la ventana la configuramos de la siguiente manera:

- Nombre de usuario: victor
- Contraseña: victor
- Guardar nombre de usuario y contraseña (seleccionado)

Luego hacemos clic en propiedades.



Hacemos clic en la pestaña Seguridad.

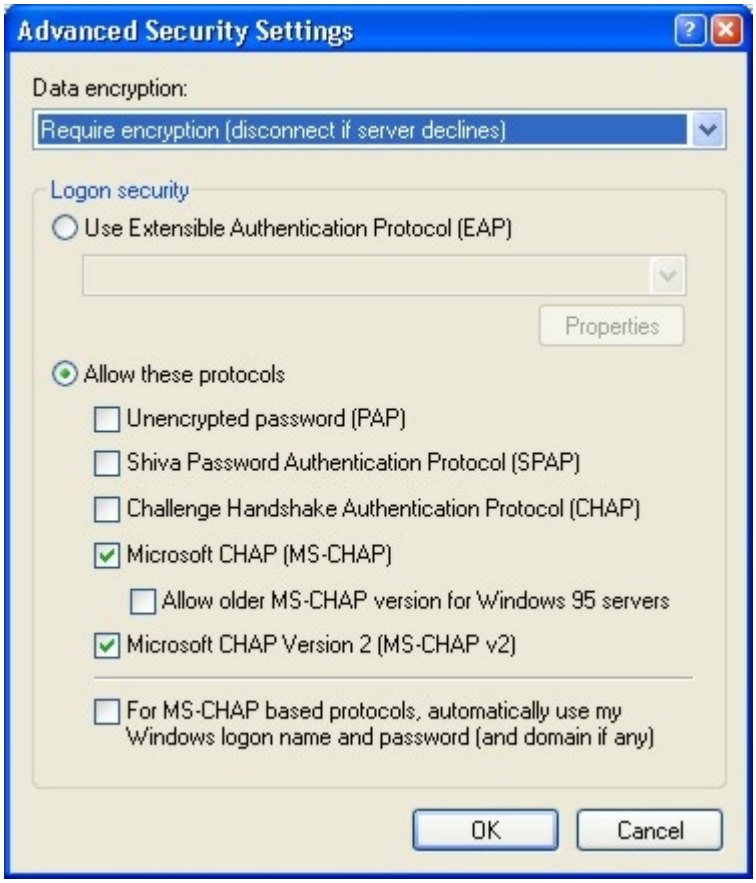


Seleccionamos Avanzado y luego clic en Settings.

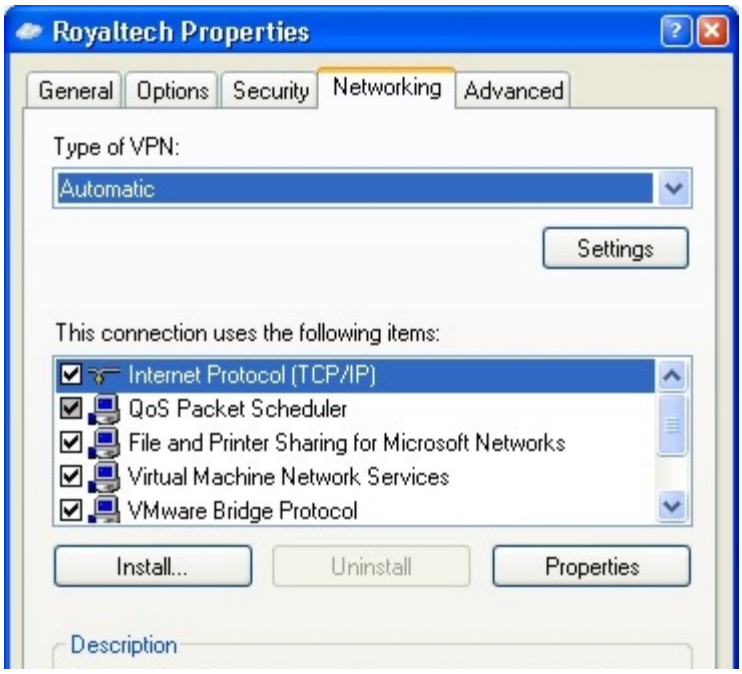
En nuestra ventana de configuración avanzada de seguridad la seteamos de la siguiente manera:

- Allow this Protocols: Seleccionado
- Uncrypted Password: Deseleccionado
- Shiva Autenticación Password Protocol : Deseleccionado
- Chalenge handshake authentication protocol: Deseleccionado
- Microsoft CHAP : Seleccionado
- Microsoft CHAP Versión 2 : Seleccionado

Luego hacemos clic en OK



Luego hacemos clic en la pestaña Networking y Editamos las propiedades de *Internet Protocol (TCP/IP)*



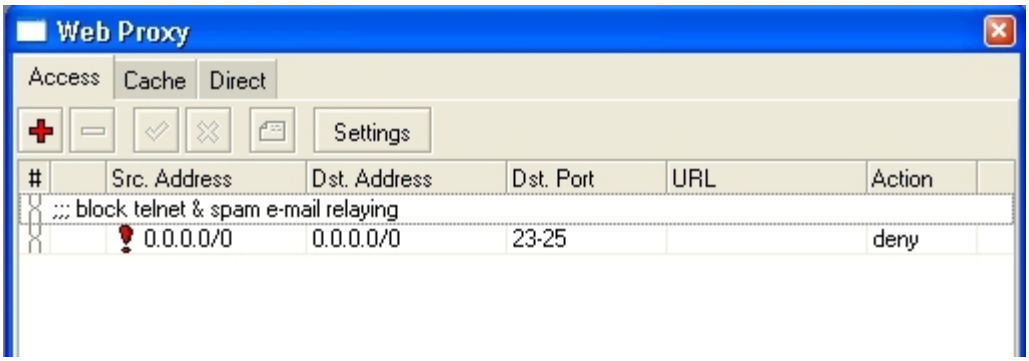
En dicha ventana hacemos clic en Avanzado.

En la ventana de avanzado la configuramos así:

- User default Gateway on remote network: Deseleccionado.

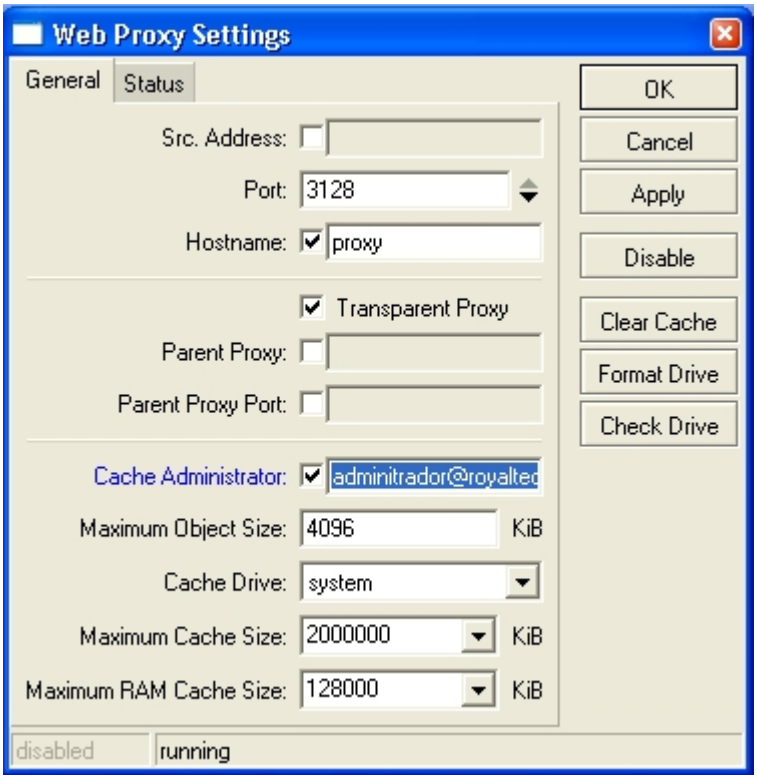
Servidor Web Proxy

Se decidió utilizar un servidor Web Proxy para ahorrar ancho de banda utilizado por los usuarios en Internet. Para ello nos dirigimos al menú *IP / WEB-PROXY.*



En nuestra ventana de configuración hacemos clic en *SETTINGS*. Se esta manera entramos a la ventana de configuración del servidor Proxy. Dicha ventana la configuraremos de la siguiente manera.

- Src. Address: La dejamos en blanco
- Port: 3128
- Hostname: Proxy
- Transparent Proxy: Seleccionado.
- Parent Proxy: lo dejamos en blanco
- Parent Proxy Port: lo dejamos en blanco
- Cache Administrator: adminitrador@royaltech.com.ar
- Maximum Object size: 4096
- Cache Drive: system
- Maximum cache Size : 2000000
- Maximum Ram Cache Size 128000

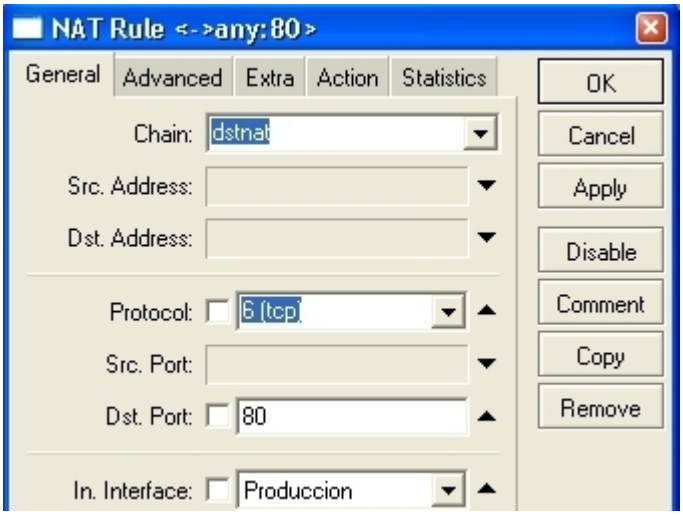


A continuación hacemos clic en *ENABLE*. Se nos abre una ventanita y le hacemos clic en ok.

Como segundo paso debemos generar un una regla en el firewall para que haga un redireccionamiento al servidor Proxy. Para ello nos dirigimos al menú *IP / FIREWALL* en nuestra ventana de configuración hacemos clic en la pestaña *NAT*, luego clic en el botón (+). La ventana la configuramos de la siguiente manera.

Interfase Producción:

- Chain: dstnat
- Protocol: 6 (tcp)
- Interfase producción.



Luego hacemos clic sobre la pestaña *ACTION* y la configuramos de la siguiente manera:

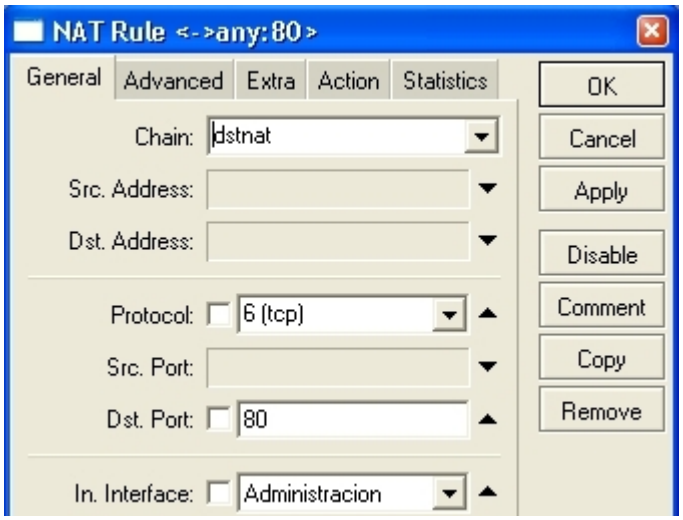
- Action: Redirect
- To ports: 3128

Realizamos esta misma configuración para cada una de las interfases de nuestra red. La configuración de las mismas es:

Interfase Administración:

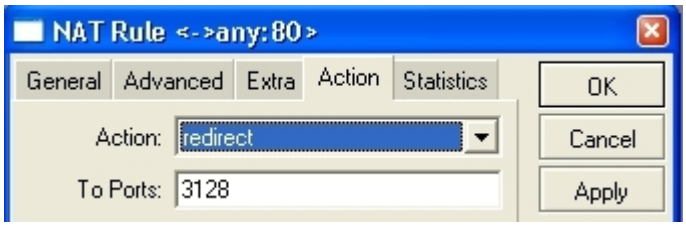
Pestaña *General:*

- Chain: dstnat
- Protocol: 6 (tcp)
- Interfase: administración



Pestaña Action:

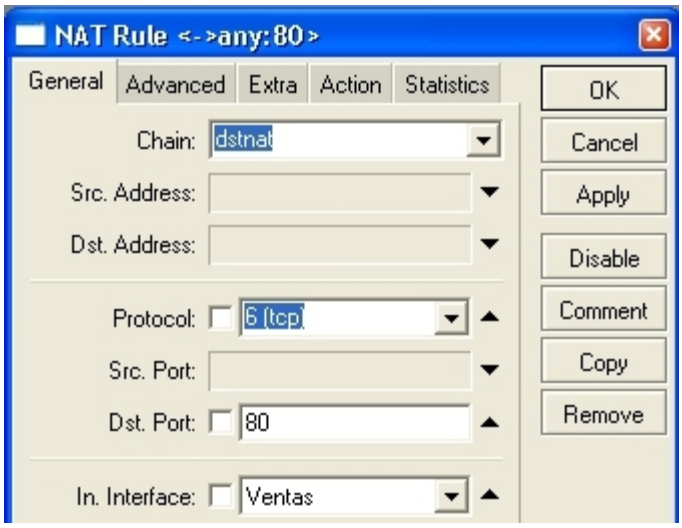
- Action: Redirect
- To ports: 3128



Interfase Ventas:

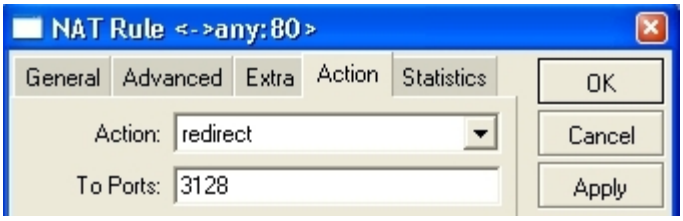
Pestaña *General:*

- Chain: dstnat
- Protocol: 6 (tcp)
- Interfase: ventas



Pestaña Action:

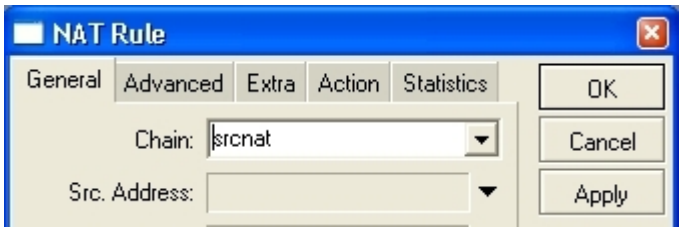
- Action: Redirect
- To ports: 3128



Por ultimo configuraremos el NAT para el ruteo entre todas las subredes de la empresa .Para ello nos dirigimos al menú *IP / FIREWALL* en nuestra ventana de configuración hacemos clic en la pestaña *NAT*, luego clic en el botón (+). La ventana la configuramos de la siguiente manera.

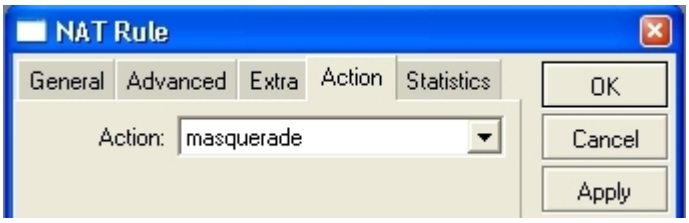
Pestaña General:

- Chain: srcnat

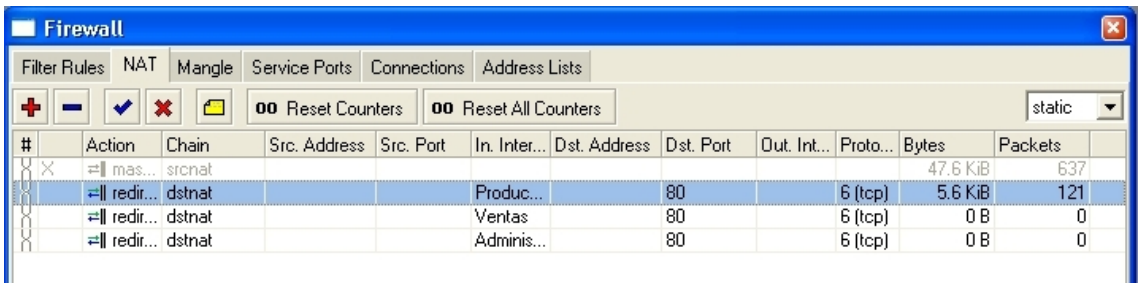


Pestaña Action:

- Action: Masquerade



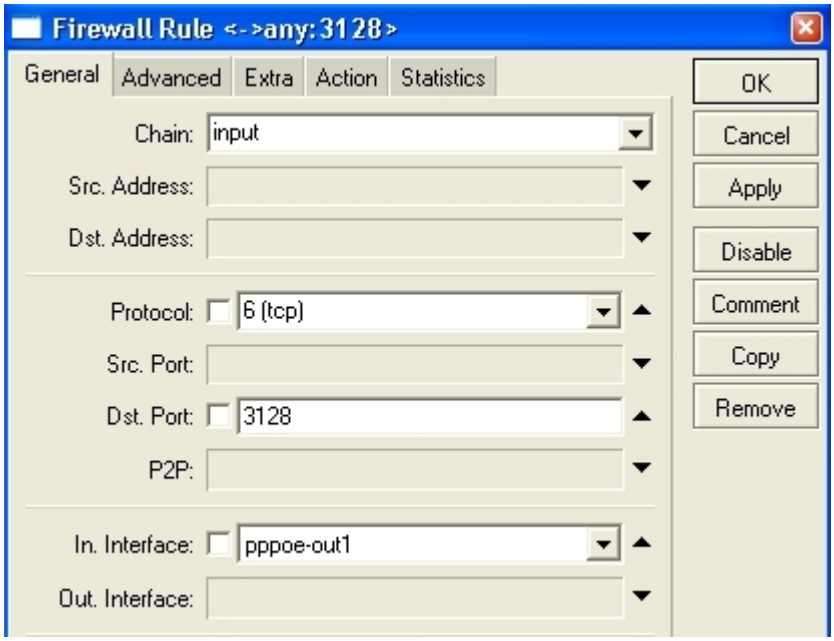
Nuestra configuración de políticas de NAT se ven de la siguiente manera:



A continuación debemos proteger nuestro servidor de cualquier utilización desde el exterior de la red. Para ello nos dirigimos al menú *IP / FIREWALL*. En la ventana nueva hacemos clic en la pestaña *FILTER RULES*, a continuación hacemos clic en el icono (+). Nuestra nueva política de filtrado de paquetes la configuramos así:

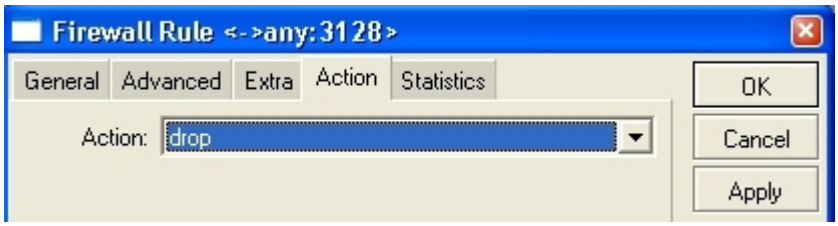
Pestaña: General:

- Chain: input
- Protocol: 6 (tcp)
- Dst. Port.: 3128
- In. Interfase: Ciudanet

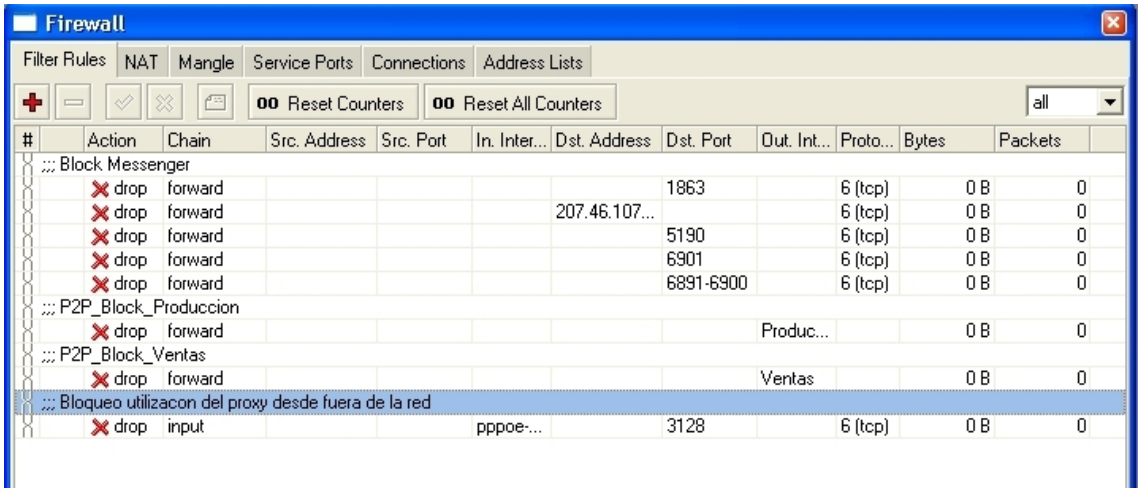


Pestaña Action:

- Action: Drop



Nuestras políticas de filtrado se ven de la siguiente manera:



Bloquearemos algunas páginas con la utilización del Web Proxy. Para ello se definió que no se podrá ingresar a sitios pornográficos desde la red ni la utilización de páginas que tengan el servicio de Web Messenger al igual que Yahoo u otros.

Bloqueo Pornografía

Nos dirigimos al menú *IP / Web Proxy*. En la nueva ventana dentro de la pestaña *Access* hacemos clic en el icono (+). Las nuevas políticas se configuran de la siguiente manera:

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *porn*
- Method: any
- Action: deny

Este filtro nos bloqueara cualquier site que posea la palabra *porn* en su nombre. También nos sirve debido a que si el usuario busca algo con la palabra porn en Google o cualquier otro buscador también nos bloquee la búsqueda.

Política 2

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *sex*
- Method: any
- Action: deny

Política 3

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *xxx*
- Method: any
- Action: deny

Bloqueo paginas que brinden el servicio de Web Messenger

El Bloqueo de las páginas que brindan el servicio de Web Messenger también será bloqueado. Para dicha configuración realizamos los siguientes pasos. Nos dirigimos al menú *IP / Web Proxy*. En la nueva ventana dentro de la pestaña *Access* hacemos clic en el icono (+). Las nuevas políticas se configuran de la siguiente manera:

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *webmessenger.yahoo.com*
- Method: any
- Action: deny

La configuración se repite para los siguientes sites:

Site: webmessenger.msn.com

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *webmessenger.msn.com*
- Method: any
- Action: deny

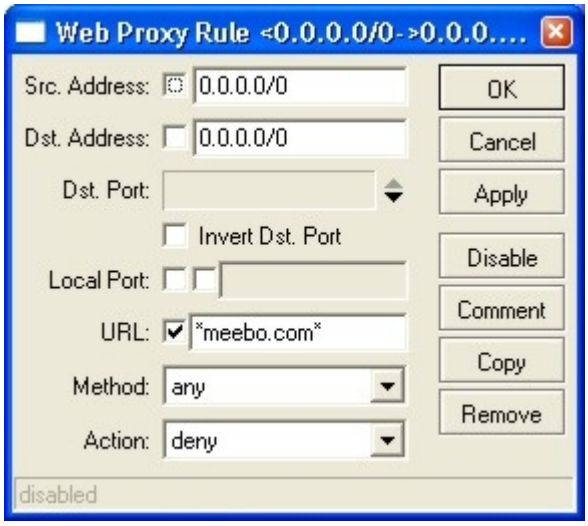
Sitio: www.ebuddy.com

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: * ebuddy.com*
- Method: any
- Action: deny

Site: meebo.com

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *meebo.com*

- Method: any
- Action: deny



Bloqueo del Live Messenger A Través del Proxy

Para e bloqueo del Messenger utilizamos la siguiente política en el Web Proxy para bloquearlo. Para ello realizamos los siguientes pasos. Nos dirigimos al menú *IP / Web Proxy*. En la nueva ventana dentro de la pestaña *Access* hacemos clic en el icono (+). Las nuevas políticas se configuran de la siguiente manera:

- Bloqueo Messenger
  - Src. Address: 0.0.0.0/0
  - Dst. Address: 0.0.0.0/0
  - URL: *Gateway.messenger.*
  - Method: any
  - Action: deny

Bloqueo de páginas que brinden webmail

Para e bloqueo de páginas que brinden webmail como mail.yahoo.com, Hotmail.com, etc. debemos utilizamos la siguiente política en el Web Proxy para bloquearlo. Para ello realizamos los siguientes pasos. Nos dirigimos al menú *IP / Web Proxy*. En la nueva ventana dentro de la pestaña *Access* hacemos clic en el icono (+). Las nuevas políticas se configuran de la siguiente manera:

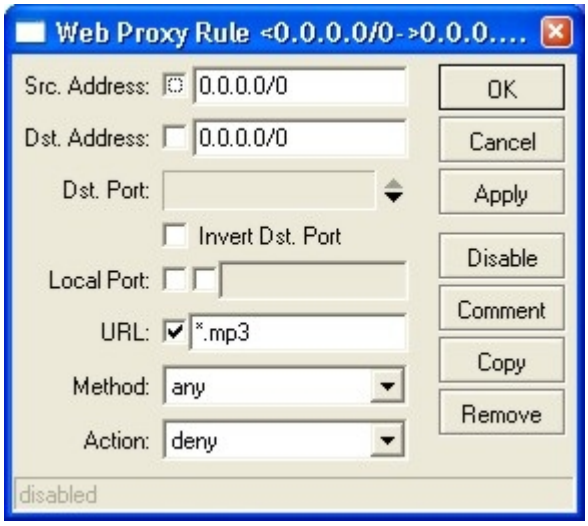
- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *mail*
- Method: any
- Action: deny

Bloqueo descarga directa de archivos MP3 y AVI

Para e bloqueo de descarga directa de archivos MP3 y avi debemos utilizamos la siguiente política en el Web Proxy para bloquearlo. Para ello realizamos los siguientes pasos. Nos dirigimos al menú *IP / Web Proxy*. En la nueva ventana dentro de la pestaña *Access* hacemos clic en el icono (+). Las nuevas políticas se configuran de la siguiente manera:

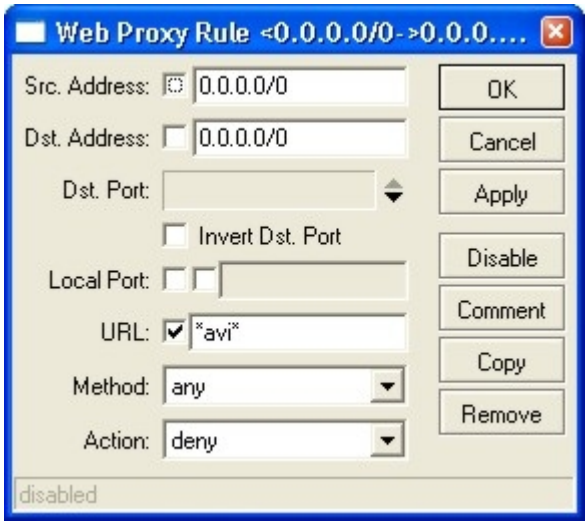
Bloqueo archivos Mp3

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *.mp3
- Method: any
- Action: deny



Bloqueo Archivos Avi

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *.avi*
- Method: any
- Action: deny



Bloqueo descarga directa de archivos RAR, ZIP, EXE

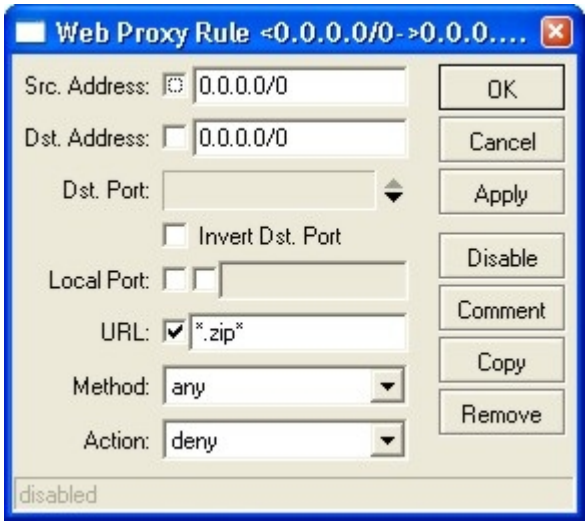
Para e bloqueo de descarga directa de archivos MP3 y avi debemos utilizamos la siguiente política en el Web Proxy para bloquearlo. Para ello realizamos los siguientes pasos. Nos dirigimos al menú *IP / Web Proxy*. En la nueva ventana dentro de la pestaña *Access* hacemos clic en el icono (+). Las nuevas políticas se configuran de la siguiente manera:

Bloqueo Archivos RAR

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *.rar*
- Method: any
- Action: deny

Bloqueo Archivos ZIP

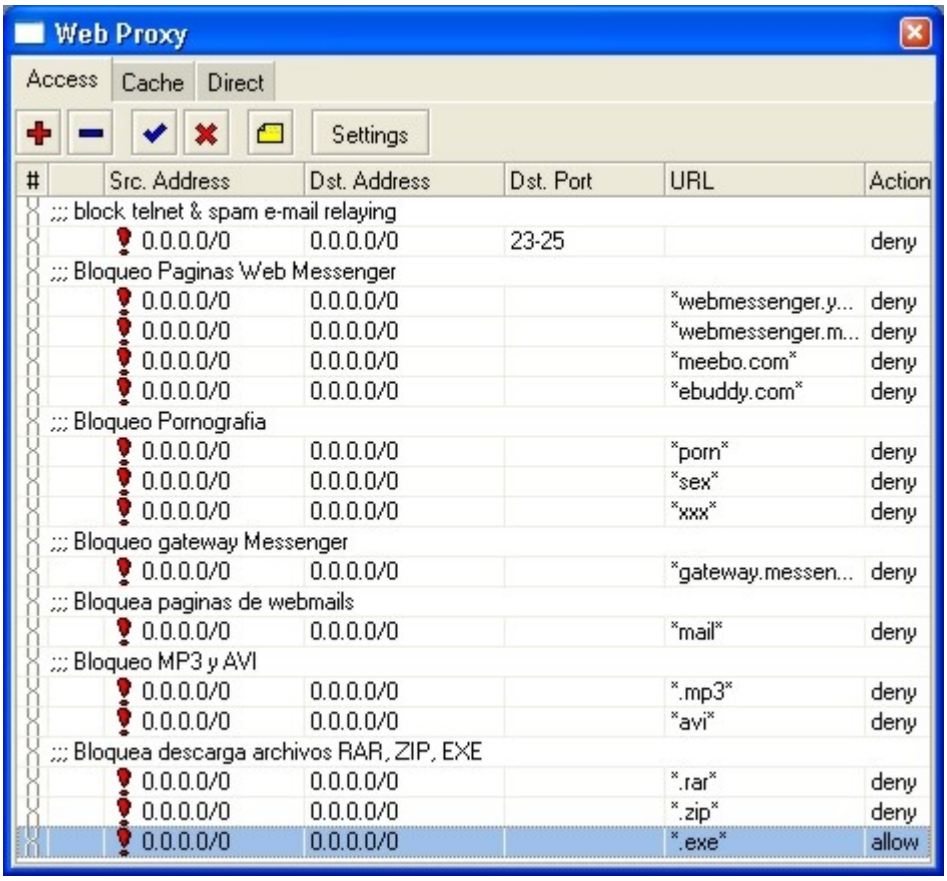
- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *.zip*
- Method: any
- Action: deny



Bloqueo Archivos EXE

- Src. Address: 0.0.0.0/0
- Dst. Address: 0.0.0.0/0
- URL: *.exe*
- Method: any
- Action: deny

Las politicas del servidor web Proxy se ven de la siguiente manera.



#		Src. Address	Dst. Address	Dst. Port	URL	Action
;;; block telnet & spam e-mail relaying						
		0.0.0.0/0	0.0.0.0/0	23-25		deny
;;; Bloqueo Paginas Web Messenger						
		0.0.0.0/0	0.0.0.0/0		*webmessenger.y...	deny
		0.0.0.0/0	0.0.0.0/0		*webmessenger.m...	deny
		0.0.0.0/0	0.0.0.0/0		*meebo.com*	deny
		0.0.0.0/0	0.0.0.0/0		*ebuddy.com*	deny
;;; Bloqueo Pornografia						
		0.0.0.0/0	0.0.0.0/0		*porn*	deny
		0.0.0.0/0	0.0.0.0/0		*sex*	deny
		0.0.0.0/0	0.0.0.0/0		*xxx*	deny
;;; Bloqueo gateway Messenger						
		0.0.0.0/0	0.0.0.0/0		*gateway.messen...	deny
;;; Bloquea paginas de webmails						
		0.0.0.0/0	0.0.0.0/0		*mail*	deny
;;; Bloqueo MP3 y AVI						
		0.0.0.0/0	0.0.0.0/0		*.mp3*	deny
		0.0.0.0/0	0.0.0.0/0		*avi*	deny
;;; Bloquea descarga archivos RAR, ZIP, EXE						
		0.0.0.0/0	0.0.0.0/0		*.rar*	deny
		0.0.0.0/0	0.0.0.0/0		*.zip*	deny
		0.0.0.0/0	0.0.0.0/0		*.exe*	allow

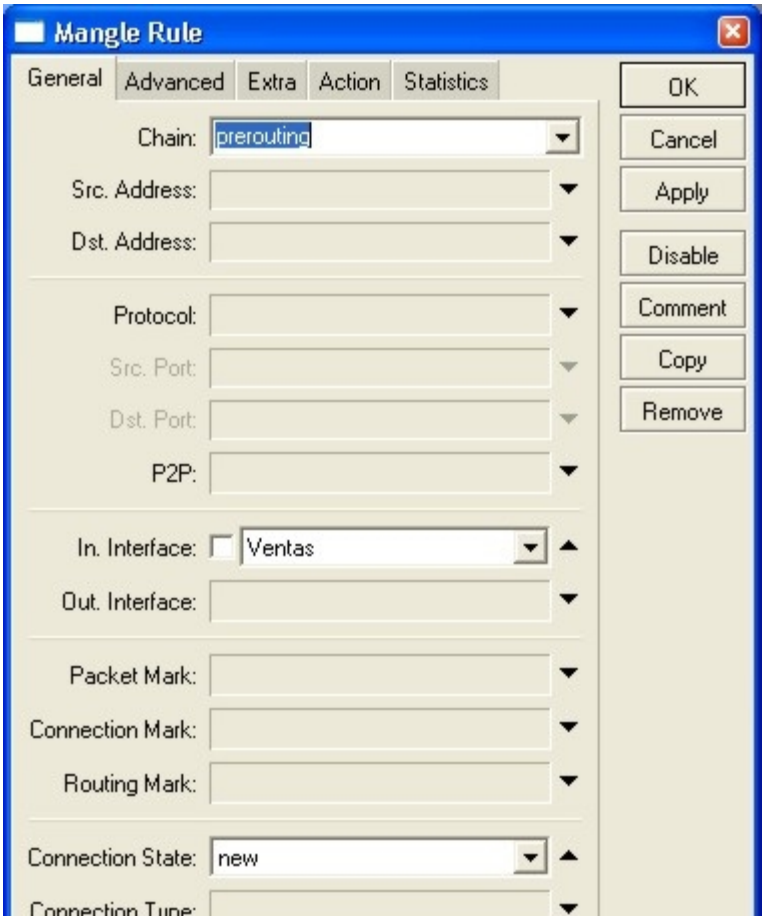
Balanceo de carga

Debido a que poseemos dos conexiones a los proveedores de Internet utilizaremos el balanceo de carga para optimizar el tráfico en la red. Debido a que la sub red ventas genera grandes volúmenes de trafico hacia Internet el balanceo de carga Será aplicado a ella.

Para configurar nuestro balanceo debemos realizar los siguientes pasos. No s dirigimos al menú *IP / FIREWALL*. De ahí vamos a la pestaña *Mangle*. Hacemos clic en el icono (+) y comenzamos nuestra configuración de las políticas para el balaceo de cargas. A la nueva ventana la configuramos de la siguiente manera.

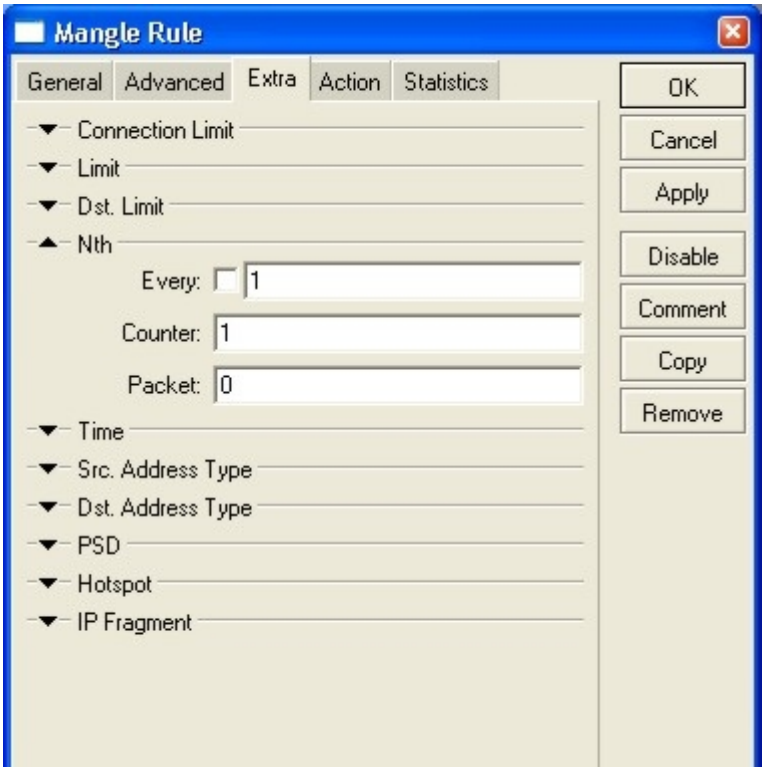
Pestaña General:

- Chain: prerouting
- In. Interfase Ventas
- Connection State: new



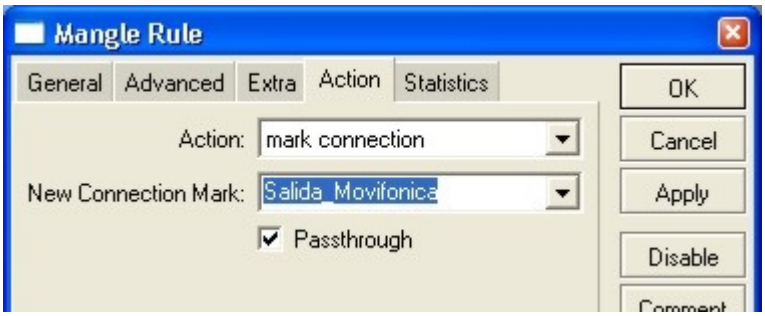
Pestaña Extra:

- Every: 1
- Counter: 1
- Packet:0



Pestaña Action:

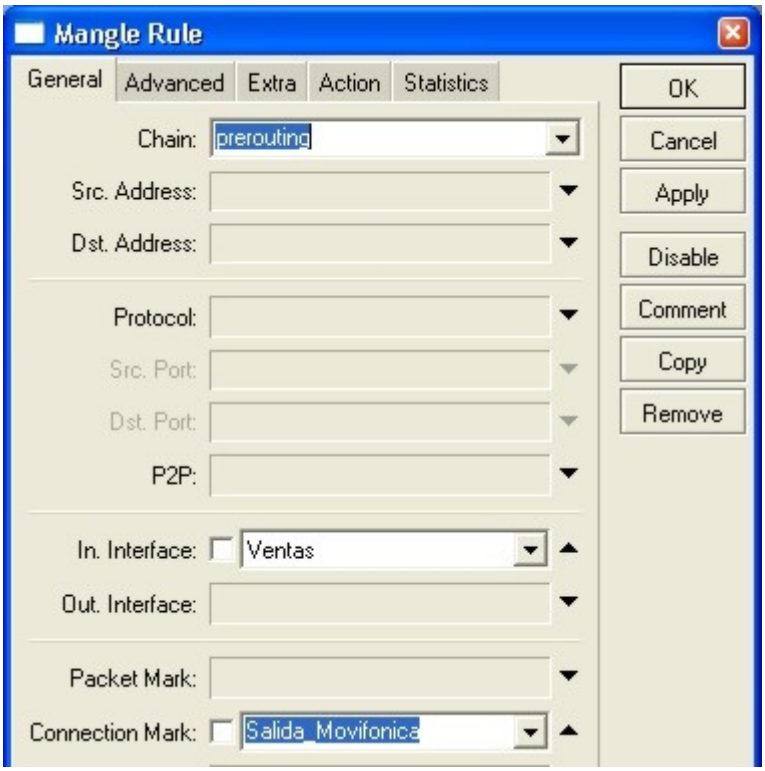
- Action: mark connection
- New Connection Mark: Salida_Movifonica
- Pass thought: seleccionado



Creamos una segunda política y la configuramos así:

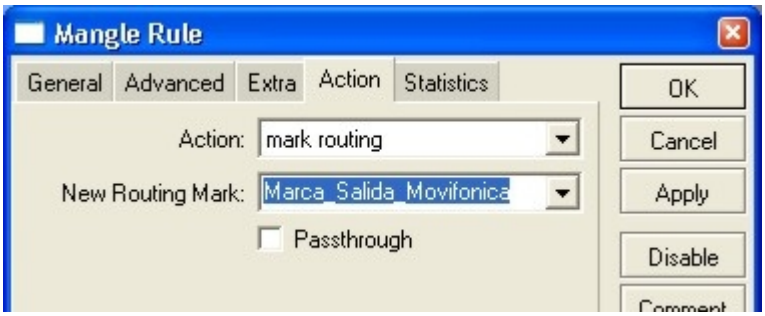
Pestaña General:

- Chain: prerouting
- In. Interfase: Ventas
- Connection mark: Salida_Movifonica



Pestaña Action:

- Action: mark routing
- New Routing Mark: Marca_Salida_Movifonica

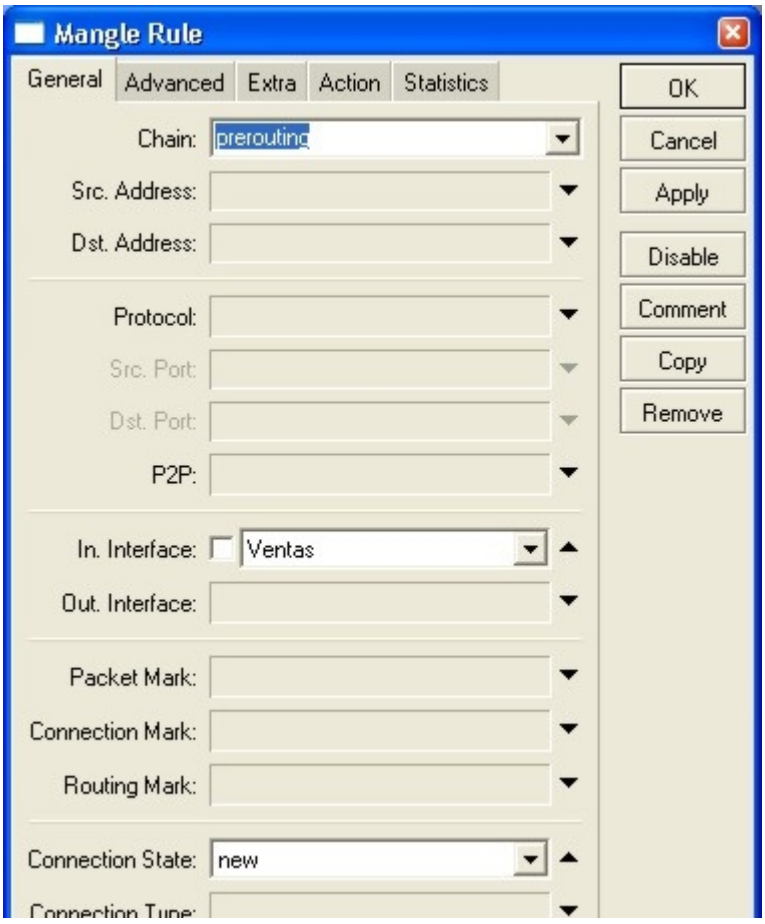


Tercera política de mangle. Se configura así:

Pestaña General:

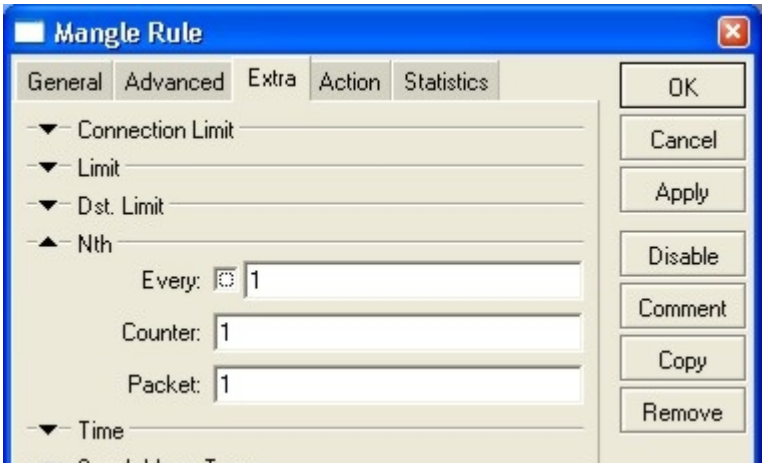
- Chain: prerouting
- In. Interfase

- Connection State: New



Pestaña Extra:

- Every: 1
- Counter:1
- Packet:1



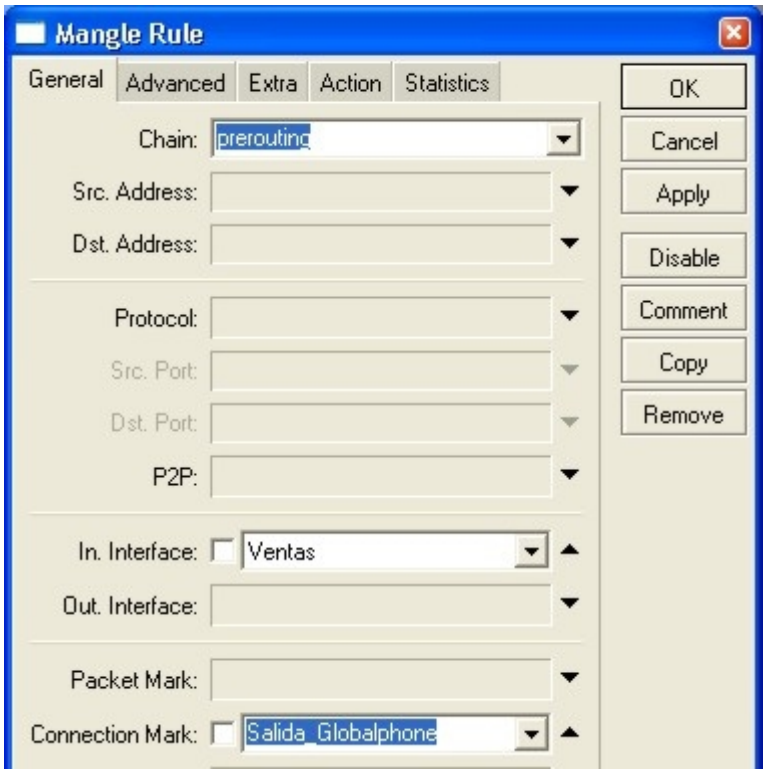
Pestaña Action:

- Action: mark connection
- New Connection Mark: Salida_globalphone
- Pass thought (seleccionado)

Cuarta política de mangle se configura así:

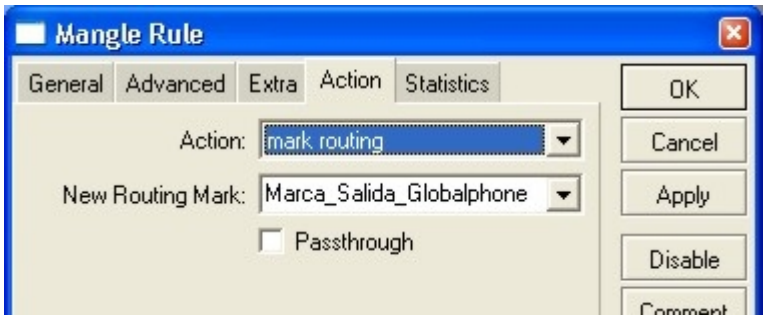
Pestaña general:

- Chain: prerouting
- In. Interfase: Ventas
- Connection mark: Salida Globalphone

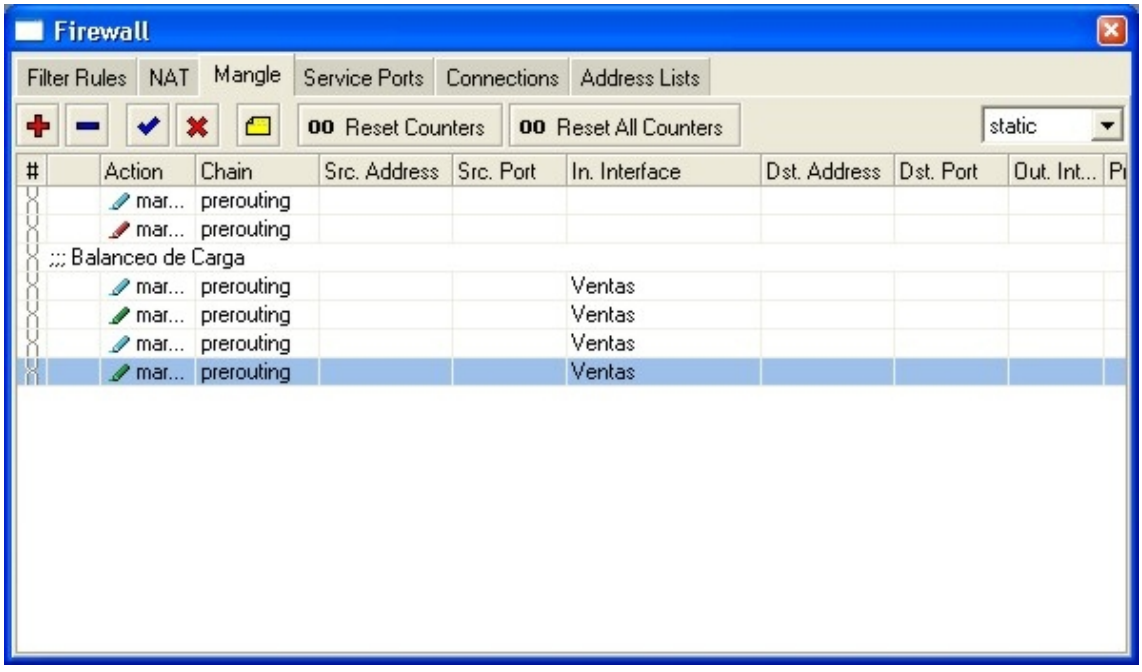


Pestaña Action:

- Action: mark routing
- New routing Mark: Marca_Salida_Globalphone
- Pass Thought: (No Seleccionado)



Nuestras políticas de Mangle se ven así:

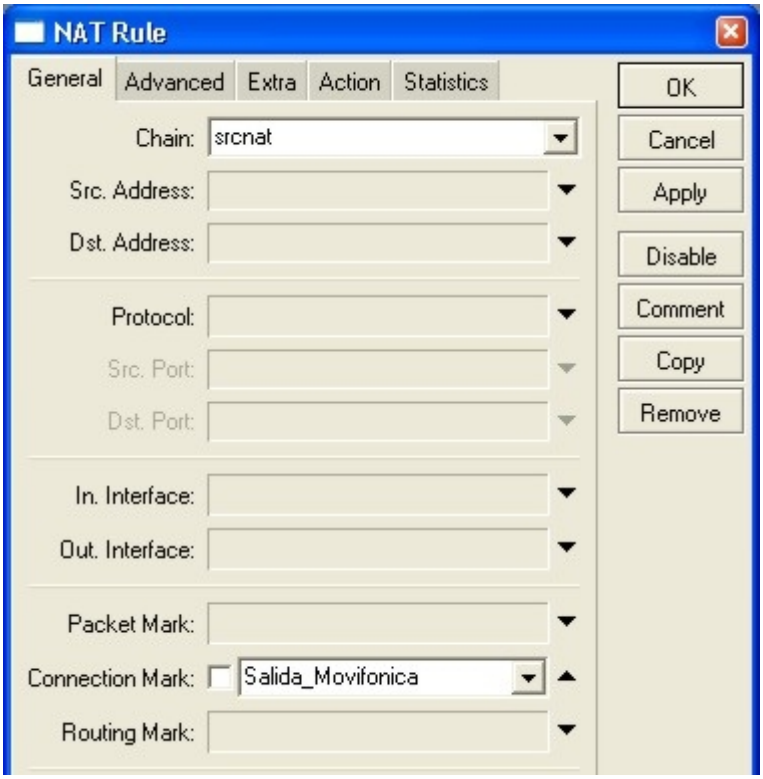


A continuación debemos crear dos políticas de NAT para continuar con la configuración. Para ello nos dirigimos al menú *IP / FIREWALL*. Hacemos clic en la pestaña NAT, luego clic en el icono (+).

La primera política de NAT se configura así:

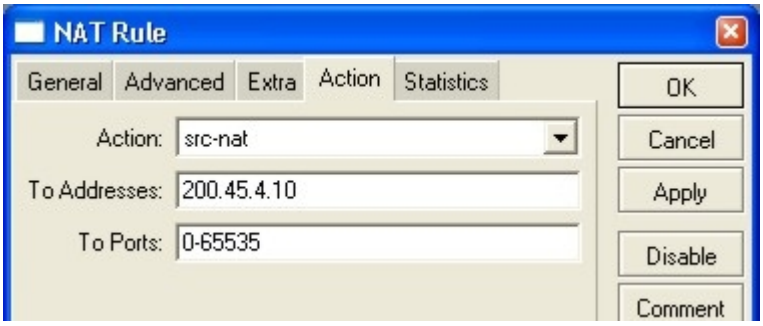
Pestaña General:

- Chain: srcnat
- Connection Mark: Salida_Movifonica



Pestaña Action:

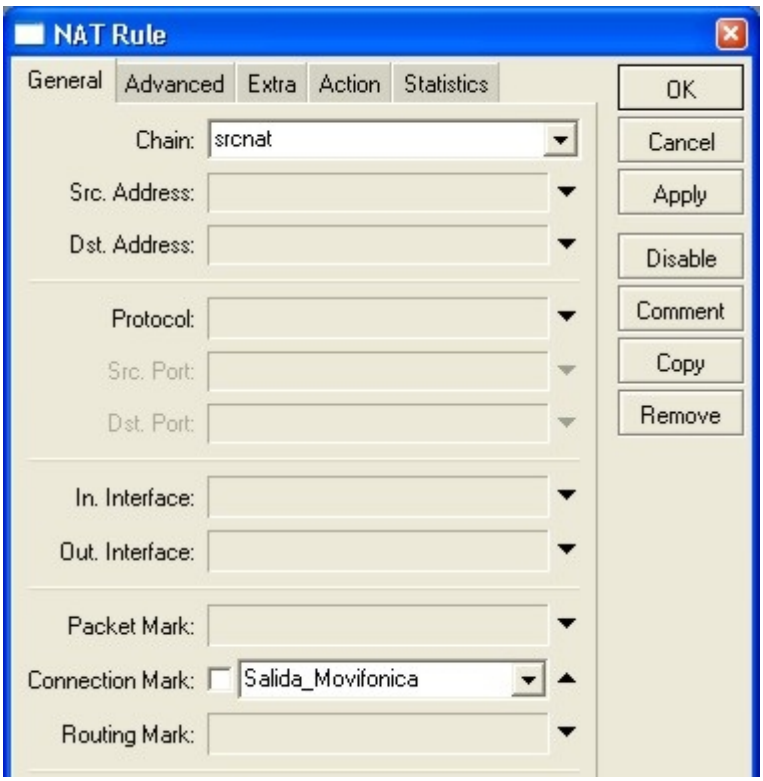
- Action: src-nat
- To addresses: 200.45.4.10
- To Ports: 0-65535



La segunda política de NAT se configura así:

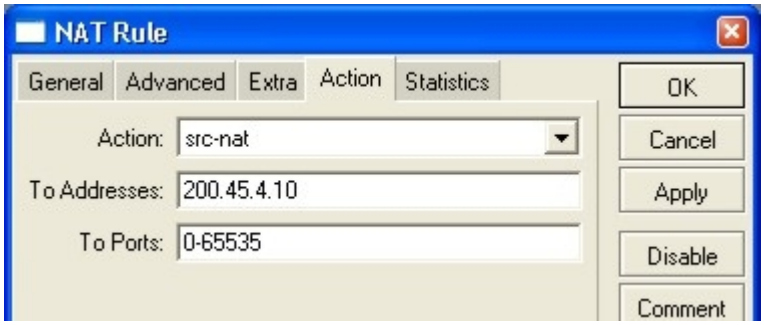
Pestaña General:

- Chain: srcnat
- Connection Mark: Salida_Movifonica

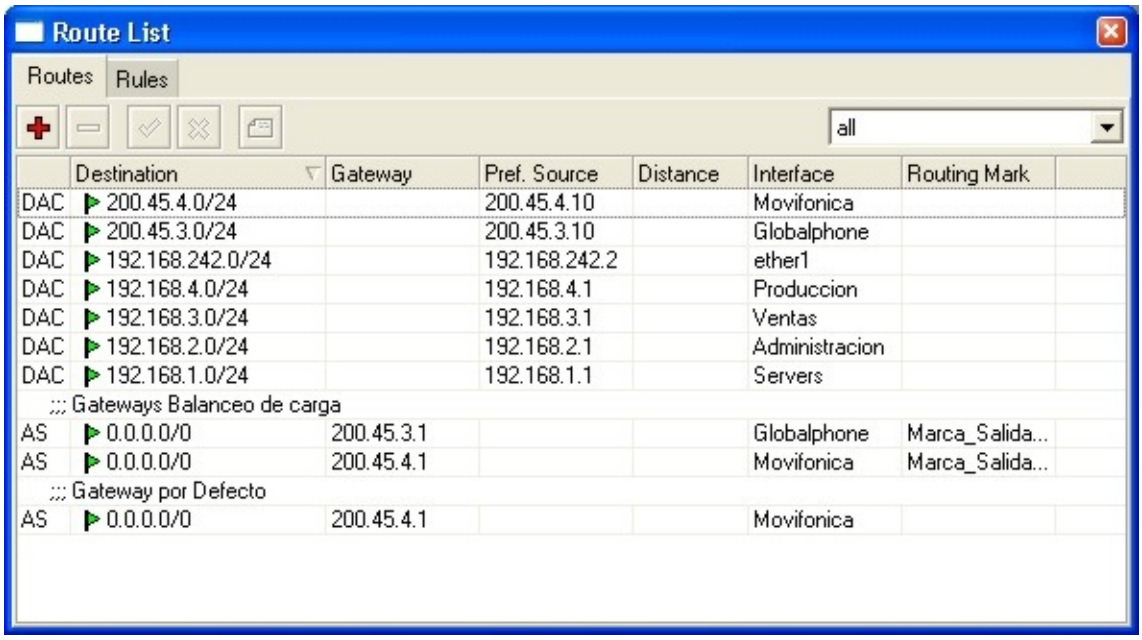


Pestaña Action:

- Action: src-nat
- To Addresses: 200.45.4.10
- 0-65535



Nuestras políticas de NAT se verán asi:



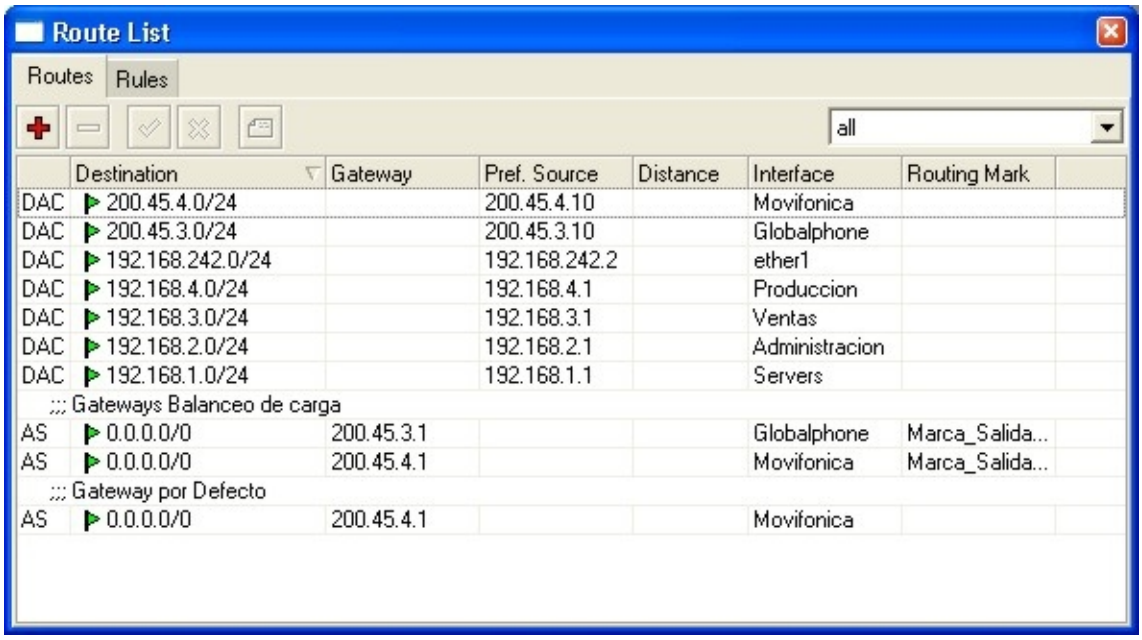
Por ultimo para finalizar la configuración debemos realizar unas últimas políticas de ruteo. Para ello entramos en el menú *NEW TERMINAL*. En la terminal que nos aparece tipeamos lo siguiente:

```
/ip route add dst-address=0.0.0.0/0 gateway=200.45.3.1 scope=255 t
arget-scope=10 routing-mark=Marca_Salida_Globalphone comment=""
disabled=no

/ip route add dst-address=0.0.0.0/0 gateway=200.45.4.1 scope=255 t
arget-scope=10 routing-mark=Marca_Salida_Movifonica  comment=""
disabled=no

/ip route add dst-address=0.0.0.0/0 gateway=200.45.4.1 scope=255 t
arget-scope=10 comment="Gateway por Defecto" disabled=no
```

Nuestras políticas de Ruteo se ven de la siguiente manera:



	Destination	Gateway	Pref. Source	Distance	Interface	Routing Mark
DAC	200.45.4.0/24		200.45.4.10		Movifonica	
DAC	200.45.3.0/24		200.45.3.10		Globalphone	
DAC	192.168.242.0/24		192.168.242.2		ether1	
DAC	192.168.4.0/24		192.168.4.1		Produccion	
DAC	192.168.3.0/24		192.168.3.1		Ventas	
DAC	192.168.2.0/24		192.168.2.1		Administracion	
DAC	192.168.1.0/24		192.168.1.1		Servers	
;;; Gateways Balanceo de carga						
AS	0.0.0.0/0	200.45.3.1			Globalphone	Marca_Salida...
AS	0.0.0.0/0	200.45.4.1			Movifonica	Marca_Salida...
;;; Gateway por Defecto						
AS	0.0.0.0/0	200.45.4.1			Movifonica	

Control de ancho de banda

Asignación de ancho de banda por sub red

Debido a que muchas veces los usuarios realizan malos usos de los anchos de banda, hemos decidido agregarle políticas al router para poder controlar dicho problema.

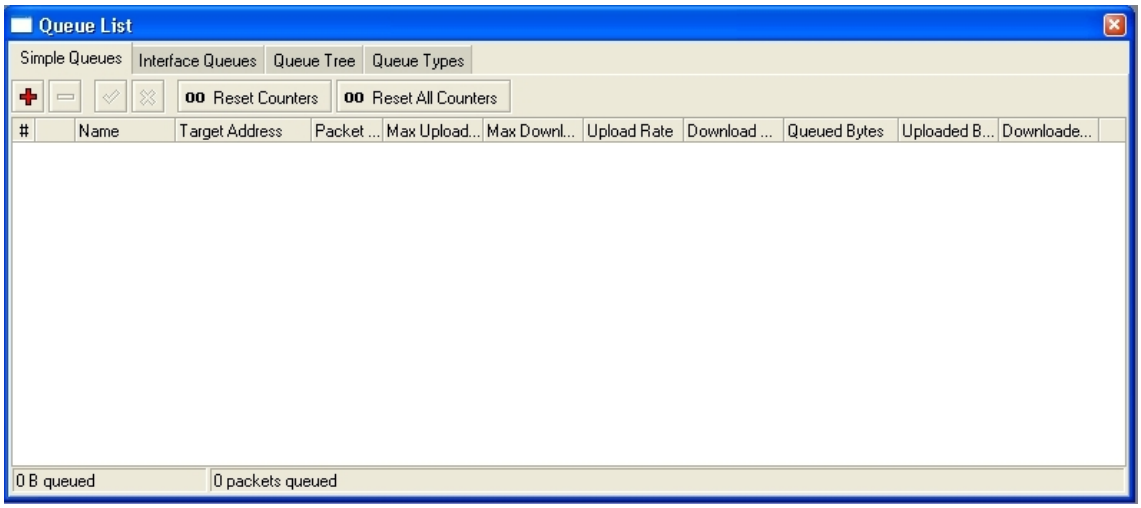
Para los distintos grupos de usuarios les asignaremos distinto ancho de banda:

- Administración :
    - Subida 250 M/Bits
    - Bajada 300 M/Bits

- Producción:
    - Subida 400 M/bits
    - Bajada 300 M/bits

- Ventas:
    - Subida 350 M/bits
    - Bajada 400 M/bits

Para el control del ancho de banda debemos ir al menú *QUEUES*. Allí se nos abrirá una ventana de configuración.

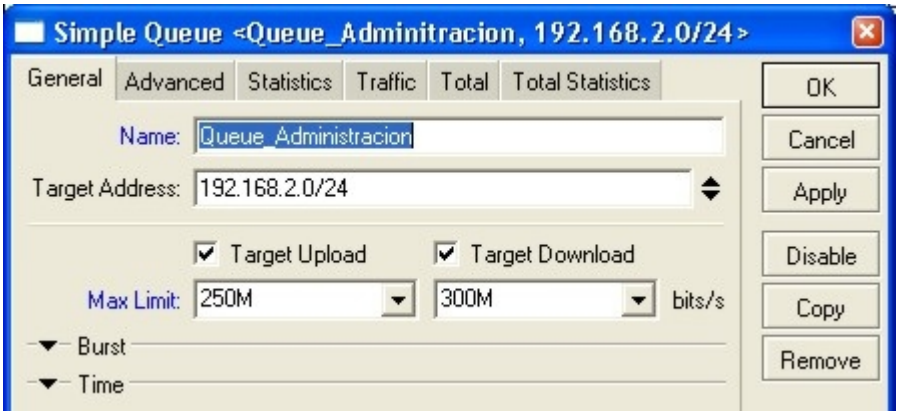


Hacemos clic en el icono (+) de la pestaña Simple *Queues*. Se nos abre la nueva para configurar la nueva cola.

Cola Administración:

Pestaña General:

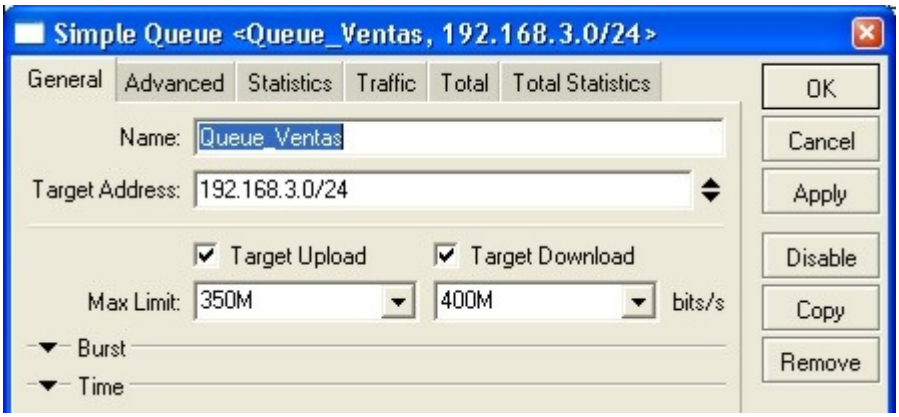
- Name: Queue_Administracion
- Target Address: 192.168.2.0/24
- Max Limit: 250M (upload) , 300M (download)



Cola Ventas:

Pestaña General:

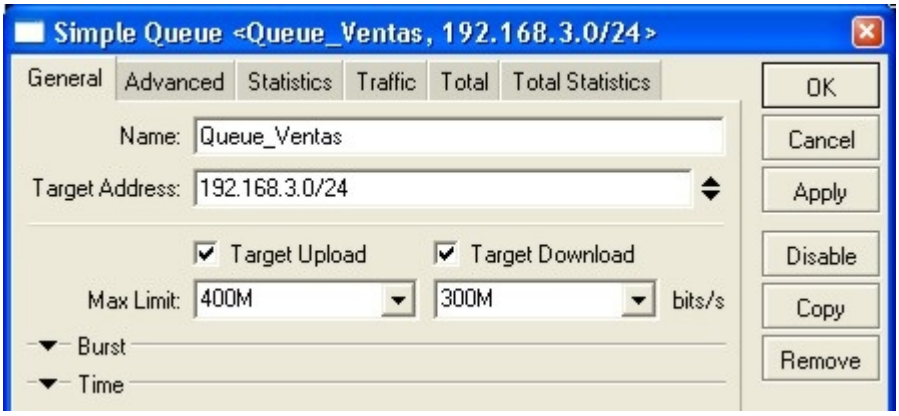
- Name: Queue_Ventas
- Target Address: 192.168.3.0/24
- Max Limit: 350M (upload) , 400M (download)



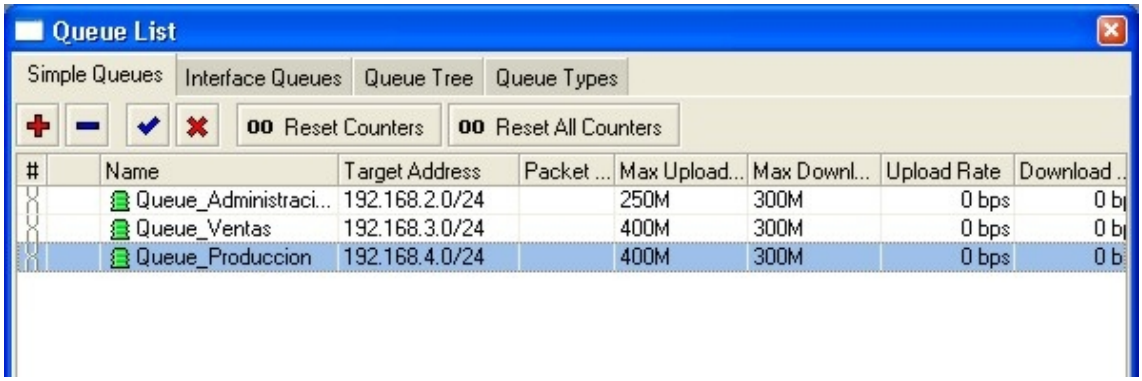
Cola Producción:

Pestaña General:

- Name: Queue_Produccion
- Target Address: 192.168.4.0/24
- Max Limit: 400M (upload) , 300M (download)



Las colas configuradas se verán de la siguiente manera:



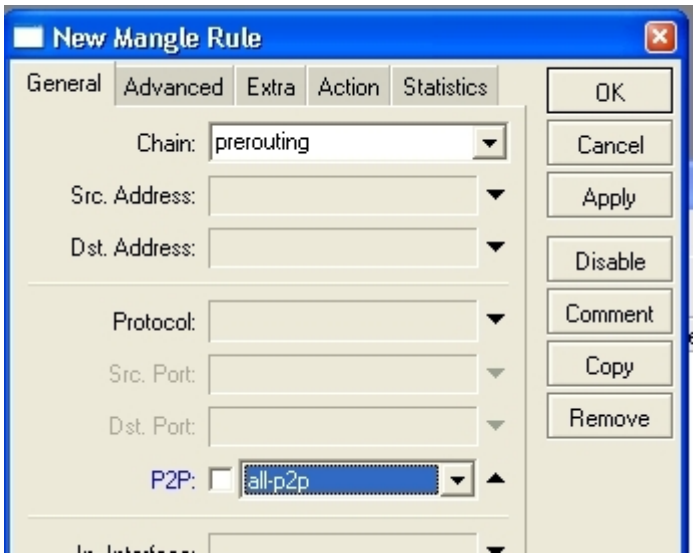
Traffic Shaping de (P2P)

Políticas internas de la empresa plantearon que solamente en el área de administración se pueda utilizar los p2p. Anteriormente habíamos asignado un cierto ancho de banda para administración ahora deberemos modelar las colas del trafico para que los p2p no se consuman todo el trafico.

Debemos ir al menú *IP / FIREWALL*. Ahí se nos abrirá nuestra ventana de configuración de políticas del firewall. Hacemos clic sobre la pestaña *Mangle*, a continuación hacemos clic sobre el botón (+).

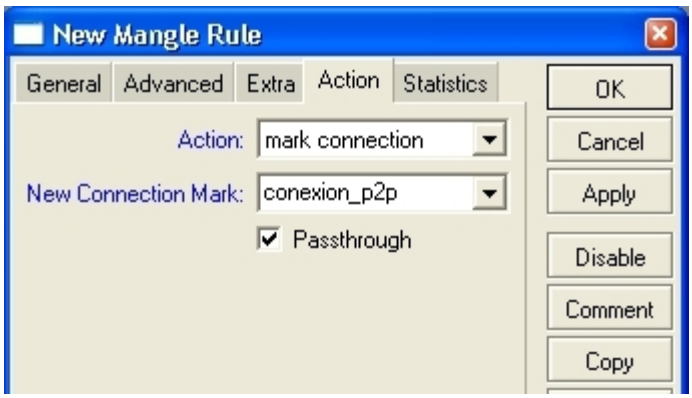
En la ventana de mangle con figuramos lo siguiente:

- Chain: prerouting
- P2P: all-p2p



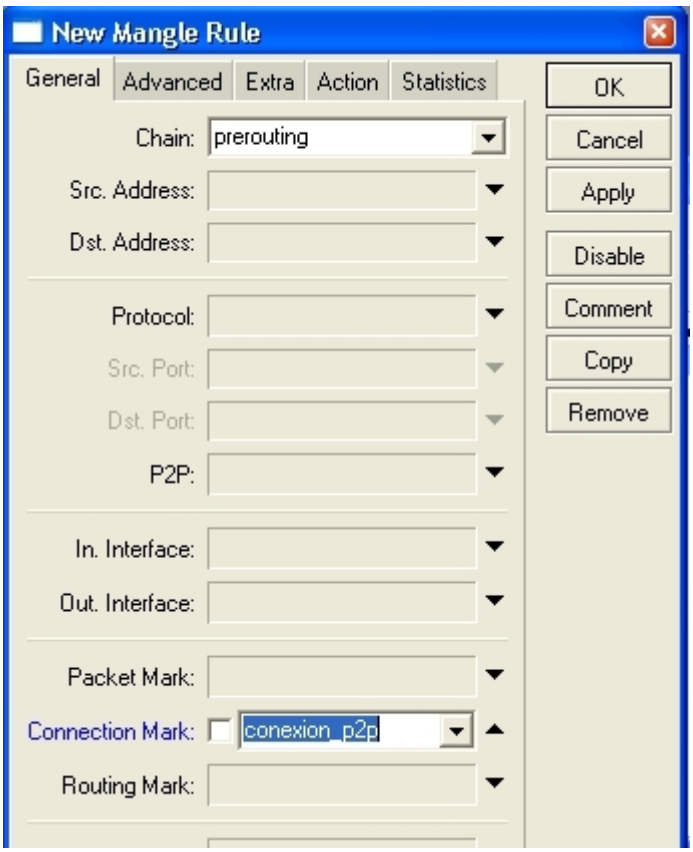
A continuación hacemos clic en la pestaña *Action*. Allí la configuración es la siguiente:

- Action: mark_connection
- New Connection Mark: (tipeamos) connexion_p2p
- Passthough (seleccionado).



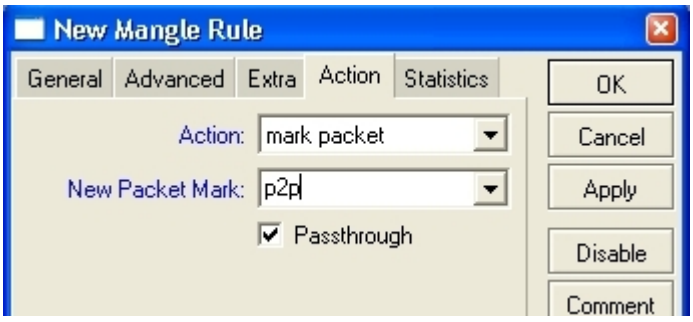
A continuación dentro de la pestaña *mangle* hacemos clic nuevamente en el botón (+) para crear una nueva regla. La configuración para la ventana es:

- Chan: prerouting
- Connection Mark: conexión_p2p (la que habíamos creado anterior mente)



Luego nos dirigimos a la pestaña *Action*, en la misma la configuramos de la siguiente manera:

- Action: Mark Packet
- New Packet Mark: (tipeamos) p2p

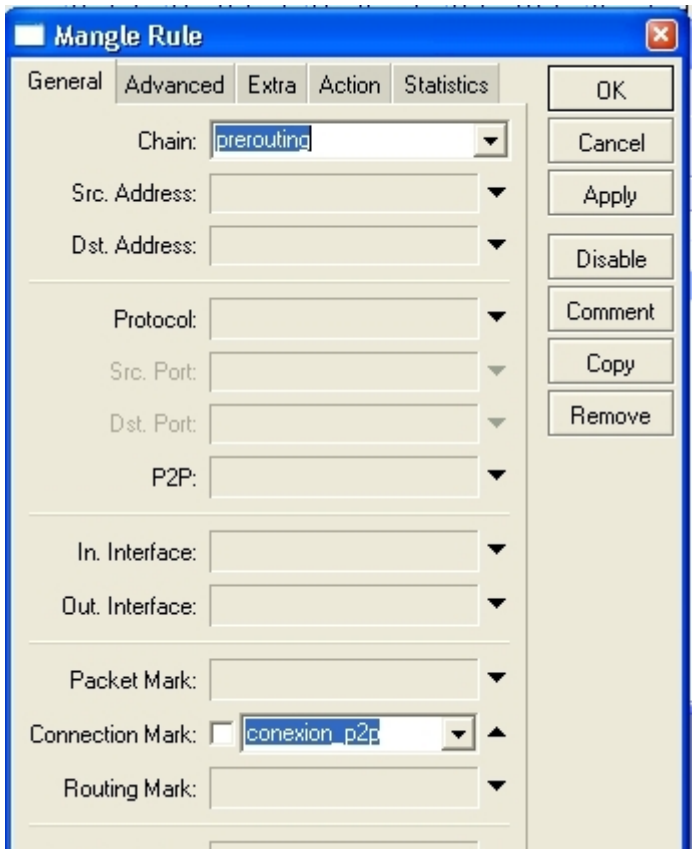


Ahora deberemos configurar las políticas para que nos marque los paquetes p2p para poder bloquearlos en las otras redes.

Para ello debemos ir al menú *IP /FIREWALL*. Hacemos clic en la pestaña *mangle* y luego clic en el icono (+).

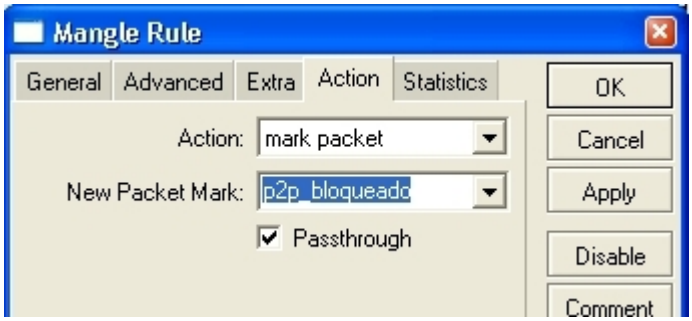
En la pestaña *General* de la nueva ventana la configuramos de la siguiente manera:

- Chain: prerouting
- Connection Mark: conexión_p2p

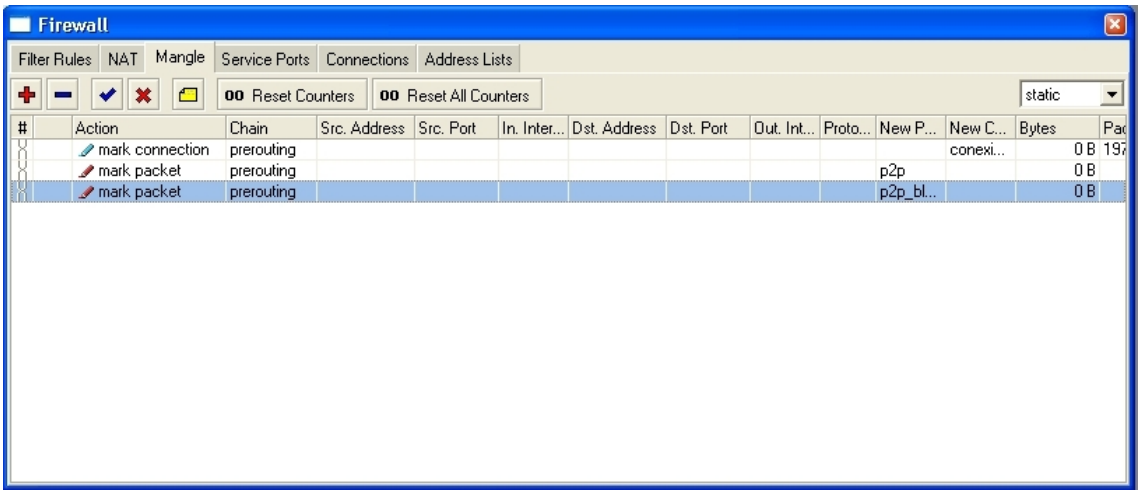


Luego nos dirigimos a la pestaña *Action* y la configuramos de la siguiente manera:

- Action: mark packet
- Packet mark: (tipeamos) p2p_bloqueado
- Pass though: (seleccionado)



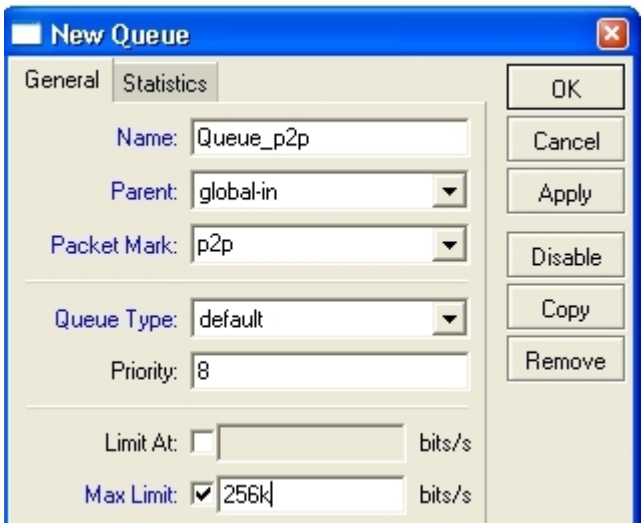
Las reglas creadas se verán de la siguiente manera.



Nos dirigiremos al menú *QUEUES*. En la ventana que nos aparece, crearemos cuatro nuevas colas para la política de los p2p. Hacemos clic sobre la pestaña *Queue Tree*. Y luego clic sobre el botón (+).

La configuración de la cola de entrada será la siguiente:

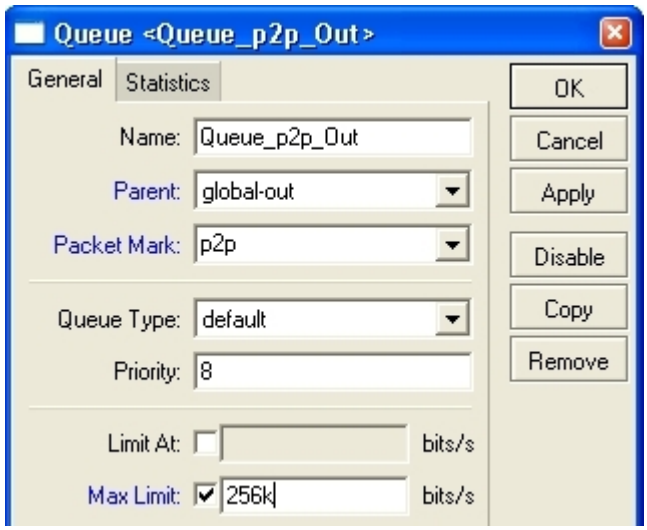
- Name: Queue_p2p_in
- Parent: Global-in
- Packet Mark: p2p
- Queue Type: default
- Priority: 8
- Max Limit: 256k



Hacemos clic en el botón (+) y generamos una nueva cola

La configuración de la cola de salida será:

- Name: Queue_p2p_out
- Parent: global-out
- Packet Mark: p2p
- Queue type: default
- Priority: 8
- Max Limit: 256k

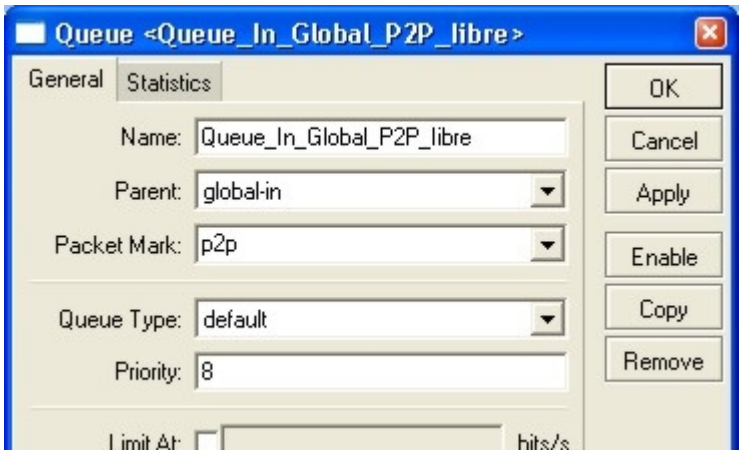


Liberación del ancho de banda fuera del horario de trabajo

Debido a que la empresa no trabaja las 24hs al día, se dispuso la posibilidad de liberar el ancho de banda para la red de Administración, en un rango horario determinado.

Para ello lo primero que debemos hacer es una nueva cola que la habilitaremos en los horarios de 20:00hs a 06:00hs. Ir al menú *QUEUES* en la pestaña Q*ueues Tree,* hacemos clic en el icono (+). Se nos abre la ventana de configuración. La configuración de la misma es:

- Name: Queue_in_Global_P2P_libre
- Parent: global-in
- Packet Mark: p2p
- Queue Type: Default
- Priority: 8

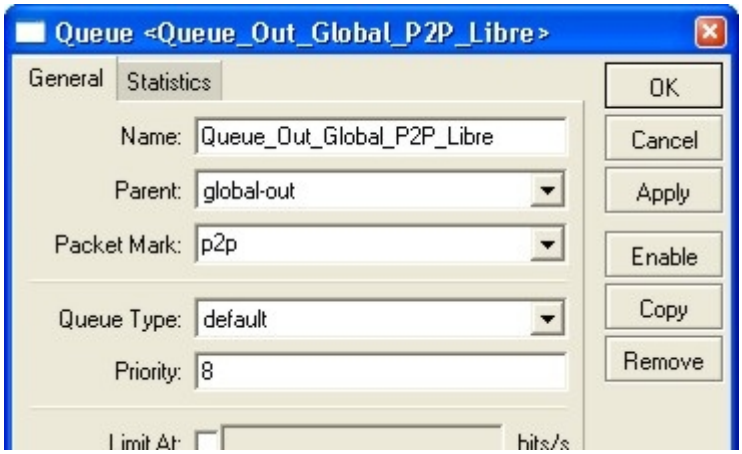


Antes de hacer clic sobre aceptar, hacemos clic en DISABLE y luego hacemos clic en aceptar.

La segunda cola que debemos realizar es de la siguiente manera:

- Name: Queue_out_Global_P2P_Libre

- Parent: global-out
- Packet Mark: p2p
- Queue Type: Default
- Priority: 8



Antes de hacer clic sobre aceptar hacemos clic en DISABLE y luego hacemos clic en aceptar.

Vamos al menú *SYSTEM / SCRIPTS.* Se nos abre la ventana de administración de scripts. Hacemos clic en el icono (+) y configuramos la ventana nueva con los siguientes datos:

- Name: Bloquea_Bw
- Policy: Write y Read
- Source:

```
/queue tree enable Queue_In_Global_P2P_Limitado
/queue tree disable  Queue_In_Global_P2P_Libre
/queue tree enable Queue_Out_Global_P2P_Limitado
/queue tree disable  Queue_Out_Global_P2P_Libre
```

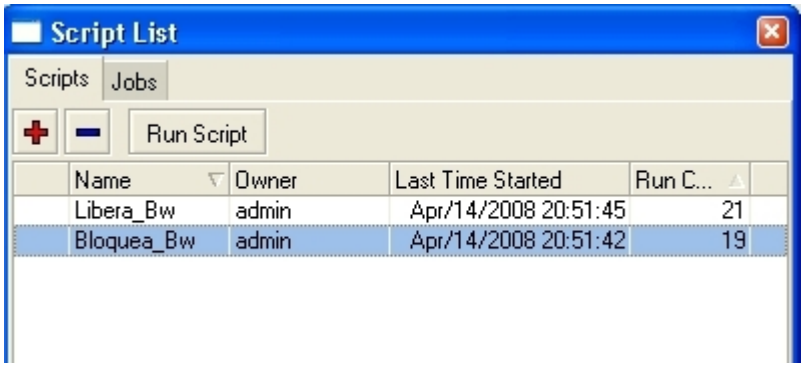
Ahora con nuestro segundo script. Vamos al menú *SYSTEM / SCRIPTS.* Se nos abre la ventana de administración de scripts. Hacemos clic en el icono (+) y configuramos la ventana nueva con los siguientes datos:

- Name: Libera_Bw

- Policy: Write y Read
- Source:

```
/queue tree disable Queue_In_Global_P2P_Limitado
/queue tree enable  Queue_In_Global_P2P_Libre
/queue tree disable Queue_Out_Global_P2P_Limitado
/queue tree enable  Queue_Out_Global_P2P_Libre
```

De la siguiente manera se ve como queda configurada nuestra lista de scripts:



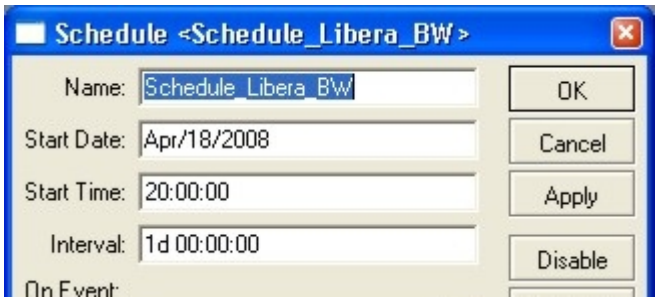
Siguiendo con la configuración vamos al menú *SYSTEM / SCHEDULER*. En la ventana nueva que se nos abre, comenzaremos con la configuración de nuestros eventos.

Hacemos clic sobre el botón (+). La configuración del primer evento es:

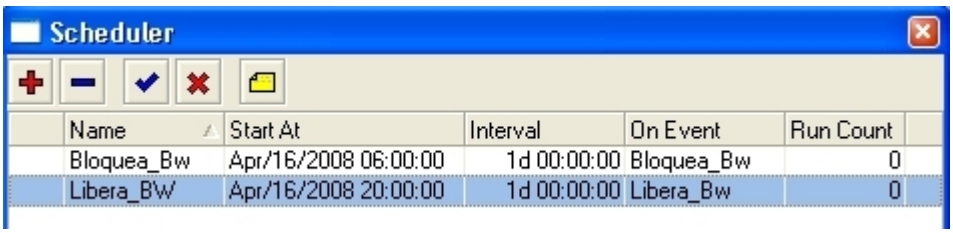
- Name: Bloquea_Bw
- State Date: Apr/16/2008
- Start Time: 06:00:00
- Interval: 1d 00:00:00
- On Event: Bloquea_Bw

Luego hacemos clic nuevamente en el icono (+) y creamos nuestro segundo evento, cuya configuración es:

- Name: Libera_Bw
- State Date: Apr/16/2008
- Start Time: 20:00:00
- Interval: 1d 00:00:00
- On Event: Libera_Bw



Así es como se ve configurada nuestra lista de scripts:



Firewall

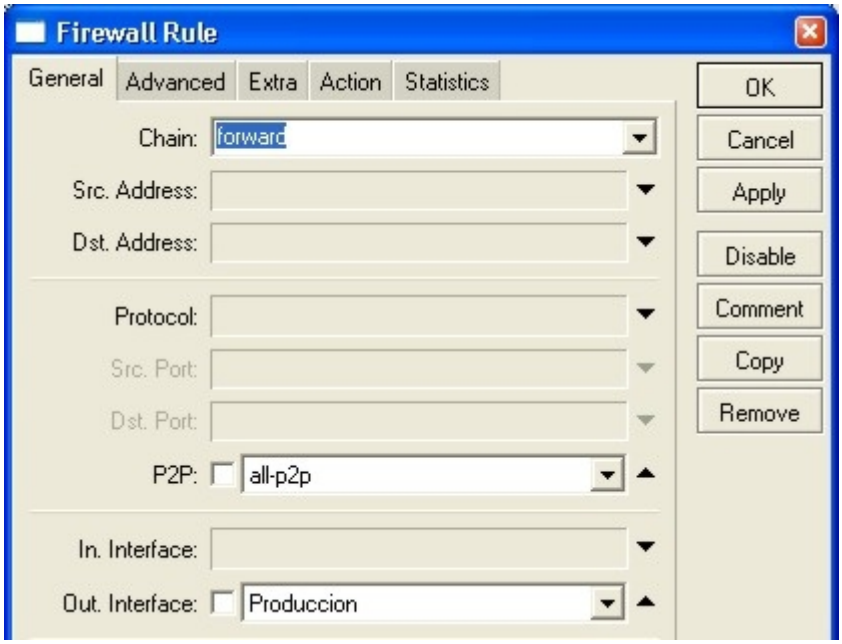
Bloqueo de los P2P para redes de ventas y producción

Debido alas políticas implementadas por gerencia solamente en el área de administración se podrá utilizar los P2P. para ello la configuración para bloquear dicho trafico es la siguiente.

Nos dirigimos a *IP / FIREWALL*. En la ventana que se nos abre hacemos clic en el icono (+). A continuación configuramos de la siguiente manera:

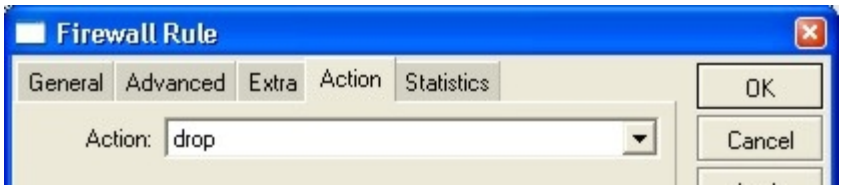
Pestaña general:

- Chain: forward
- P2P: all-p2p
- Out. Interface: Producción



Pestaña Action:

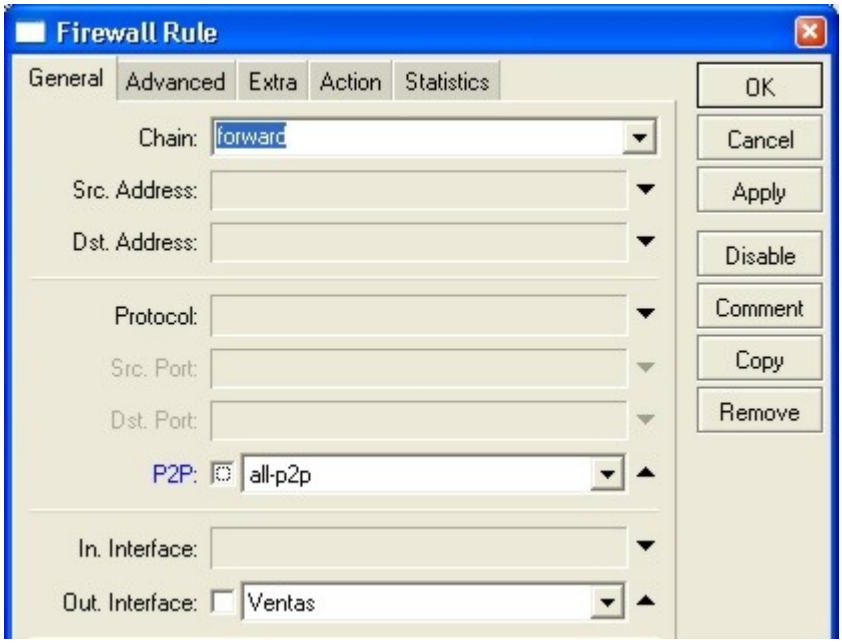
- Action: drop



Nos dirigimos a *IP / FIREWALL*. En la ventana que se nos abre hacemos clic en el icono (+). A continuación configuramos de la siguiente manera:

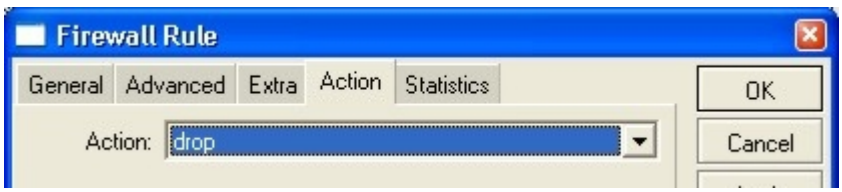
Pestaña general:

- Chain: forward
- P2P: all-p2p
- Out. Interface: Ventas



Pestaña Action:

- Action: drop



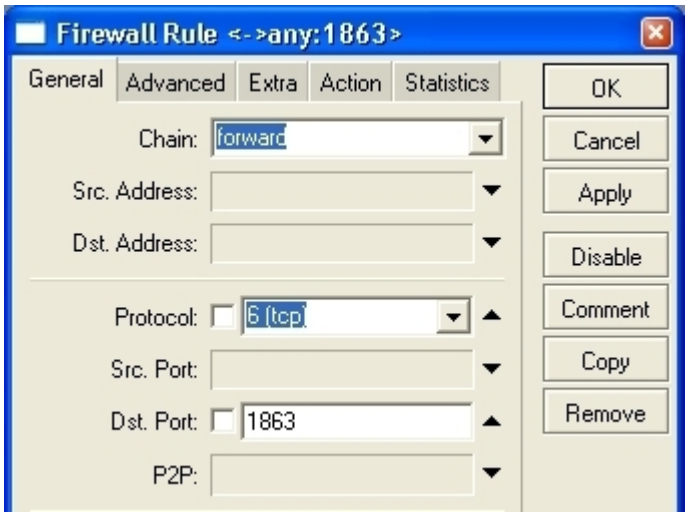
Bloqueo del cliente MSN Live Messenger

Debido a que los empleados de la empresa suelen perder demasiado tiempo utilizando el MSN Live Messenger, la empresa decidió bloquear dicho programa. Para ello se establecieron las siguientes políticas de firewall.

Nos dirigimos a *IP / FIREWALL*. En la ventana que se nos abre hacemos clic en el icono (+). A continuación configuramos de la siguiente manera:

Primera política de firewall:

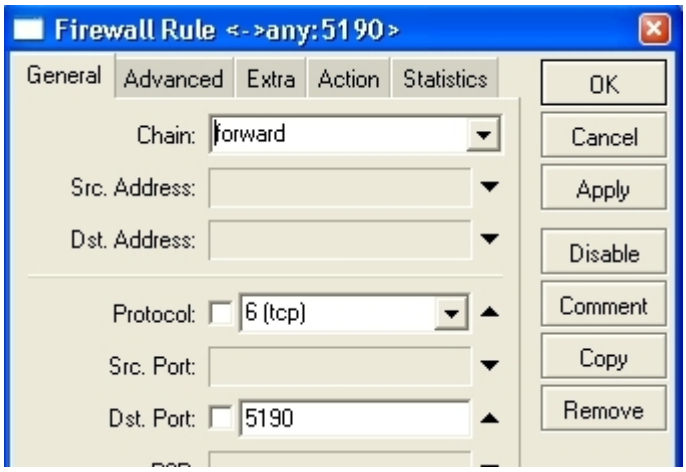
- Pestaña General:
  - Chain: Forward
  - Protocol: Tcp (6)
  - Dst. Port: 1863



- Pestaña General:
  - Action: Drop

Segunda política de Firewall:

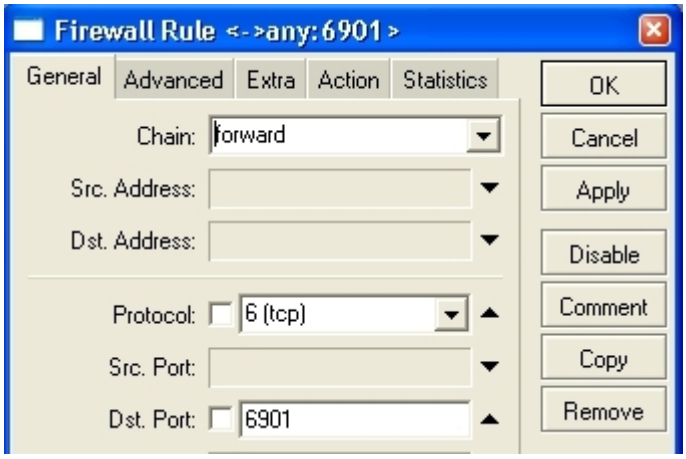
- Pestaña General:
  - Chain: Forward
  - Protocol: Tcp (6)
  - Dst. Port: 5190



- Pestaña Action
  - Action: Drop

Tercera política de Firewall:

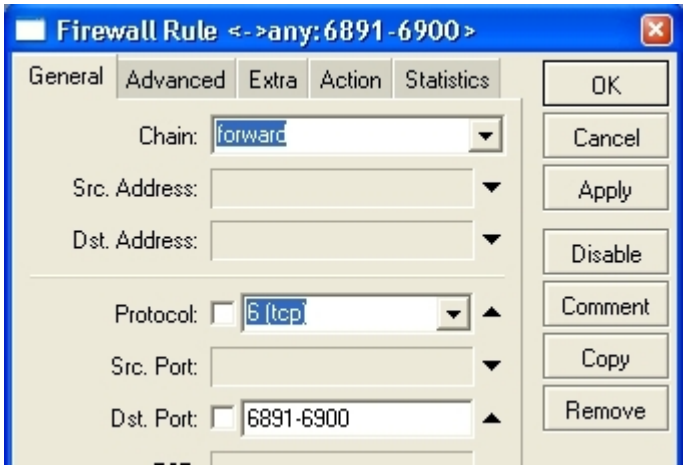
- Pestaña General:
  - Chain: Forward
  - Protocol: Tcp (6)
  - Dst. Port: 6901



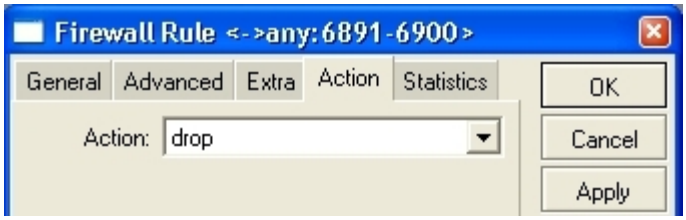
- Pestaña Action:
  - Action: Drop

Cuarta política de Firewall:

- Pestaña General:
  - Chain: Forward
  - Protocol: Tcp (6)
  - Dst. Port: 6891-6900

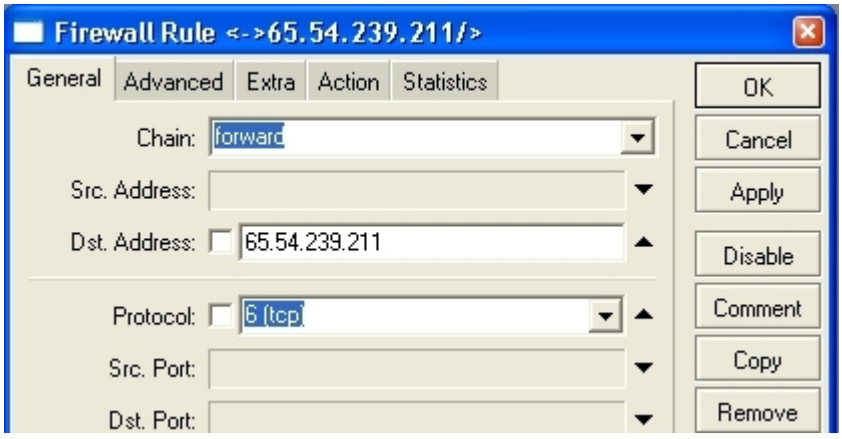


- Pestaña Action:
    - Action: Drop

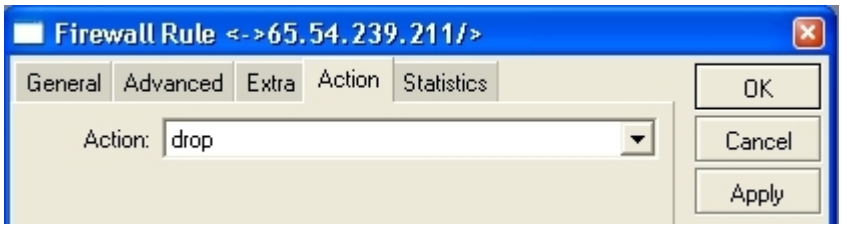


Quinta política de firewall:

- Pestaña General:
    - Chain: Forward
    - Protocol: Tcp (6)
    - Dst. Address: 65.54.239.211



- Pestaña Action:
    - Action: Drop



Finalizada dicha configuración ningún usuario podrá conectarse al MSN Live Messenger. Para que el bloqueo sea completo debemos utilizar una política en el Web-Proxy que instalaremos mas adelante.

Redireccionamiento de puertos

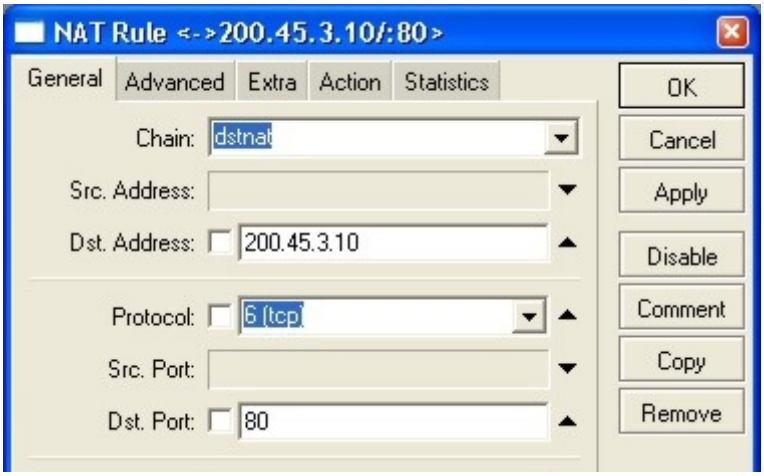
A continuación debemos redireccionar puertos para que el tráfico que se genere hacia adentro de la red obtengan las respuesta deseada. Por ejemplo que nuestro servidor web muestre las páginas correspondientes, que el servidor de SMTP y POP3 puedan enviar y recibir mails etc.

Puerto 80 WEB

Para redireccionar el puerto 80 desde el exterior a nuestro servidor web ip: 192.168.1.2 debemos realizar los siguientes pasos. Ir al menú *IP / FIREWALL*. Hacer clic en la pestaña *NAT*. Luego hacer clic en el icono (+). A la nueva ventana la configuramos de la siguiente manera.

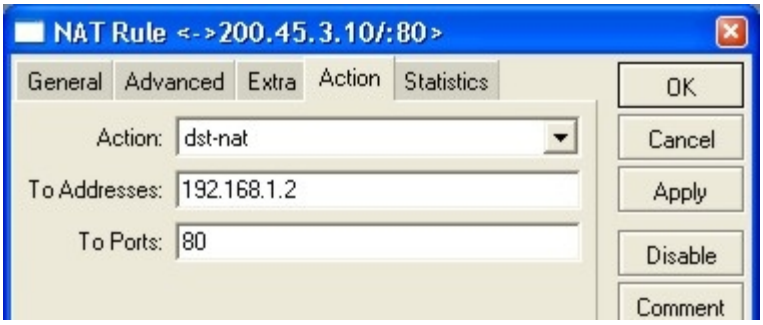
Pestaña General:

- Chain:dstnat
- Dst. Address: 200.45.3.10
- Protocol: 6 (tcp)
- Dst. Port: 80



Pestaña Action:

- Action: dst-nat
- To Addresses: 192.168.1.2
- To Port: 80

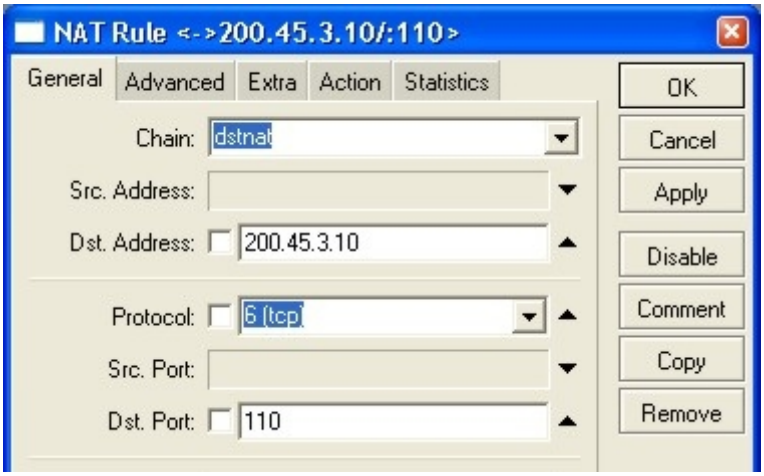


Puerto 110 POP3

Para redireccionar el puerto 110 desde el exterior a nuestro servidor pop3 ip: 192.168.1.2 debemos realizar los siguientes pasos. Ir al menú *IP / FIREWALL*. Hacer clic en la pestaña *NAT*. Luego hacer clic en el icono (+). A la nueva ventana la configuramos de la siguiente manera.

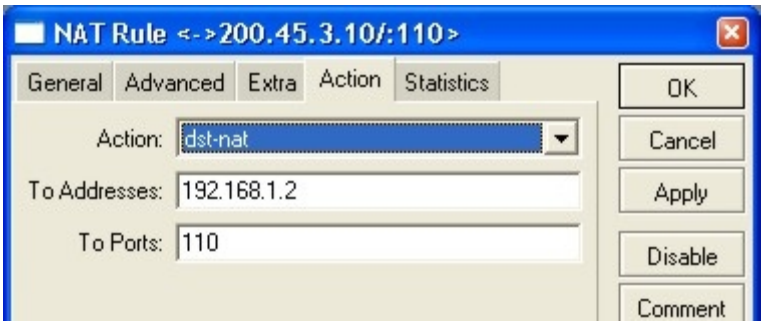
Pestaña General:

- Chain: dstnat
- Dst. Address: 200.45.3.10
- Protocol: 6 (tcp)
- Dst. Port: 110



Pestaña Action:

- Action: dst-nat
- To Addresses: 192.168.1.2
- To Port: 110

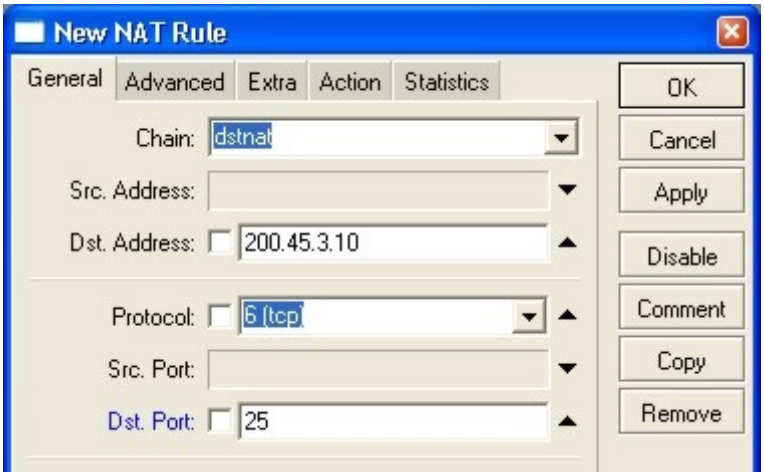


Puerto 25 SMTP

Para redireccionar el puerto 25 desde el exterior a nuestro servidor pop3 ip: 192.168.1.2 debemos realizar los siguientes pasos. Ir al menú *IP / FIREWALL*. Hacer clic en la pestaña *NAT*. Luego hacer clic en el icono (+). A la nueva ventana la configuramos de la siguiente manera.

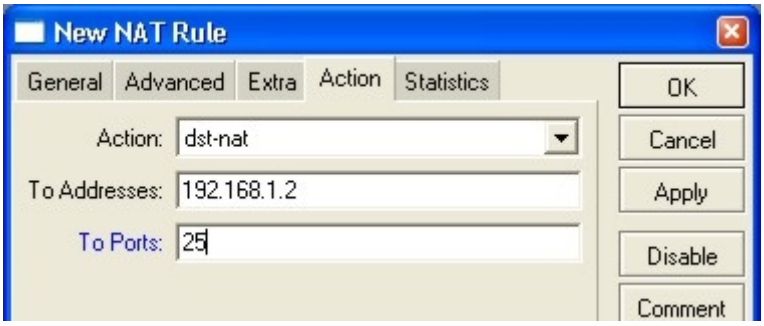
Pestaña General:

- Chain:dstnat
- Dst. Address: 200.45.3.10
- Protocol: 6 (tcp)
- Dst. Port: 25



Pestaña Action:

- Action: dst-nat
- To Addresses: 192.168.1.2
- To Port: 25



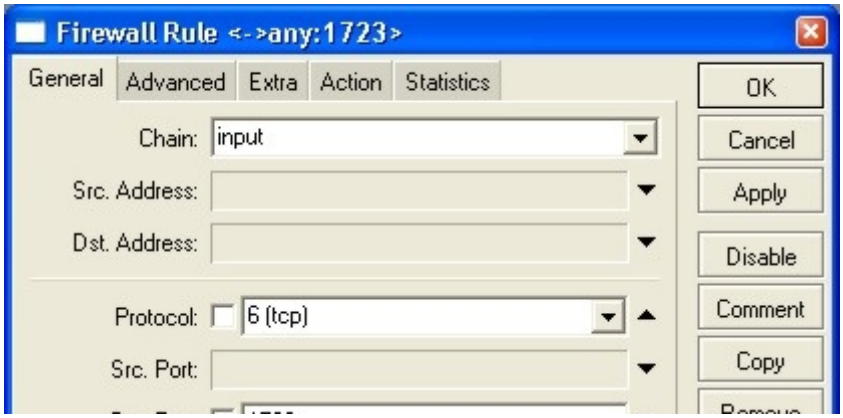
Puerto 1723 PPTP

Para aceptar conexiones al puerto 1723 desde el exterior debemos realizar los siguientes pasos. Ir al menú *IP / FIREWALL*. Hacer clic en la pestaña *FILTER RULES*. Luego hacer clic en el icono (+). A la nueva ventana la configuramos de la siguiente manera.

La primer politica es para aceptar el trafico al puerto 1723 tcp

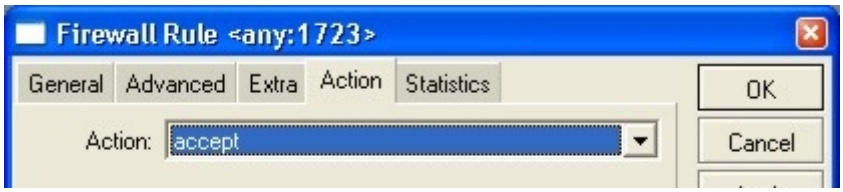
Pestaña General:

- Chain: input
- Protocol 6 (tcp)
- Dst. Port: 1723



Pestaña Action:

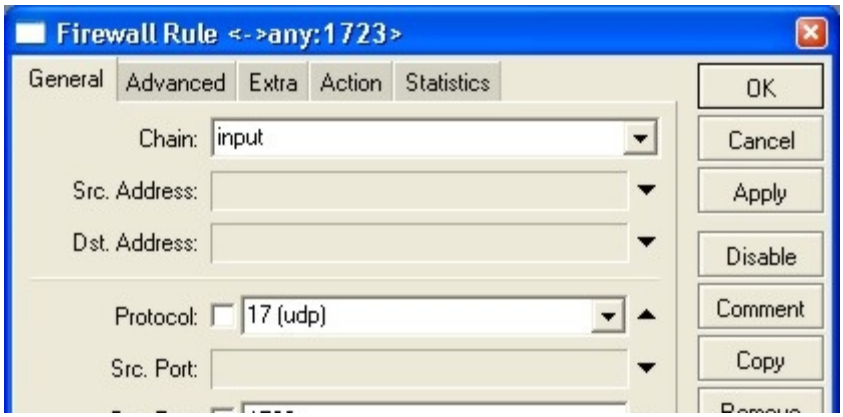
- Action: accept



La segunda politica es para aceptar todo el trafico al puerto 1723 UDP

Pestaña General:

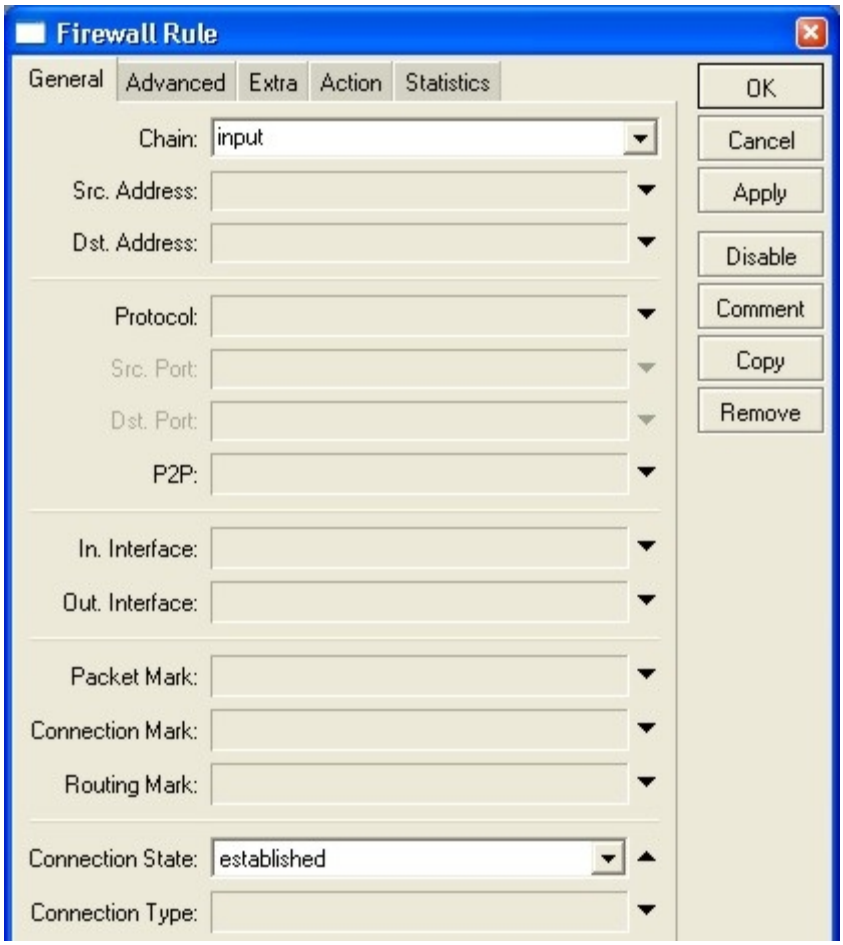
- Chain: input
- Protocol 17 (udp)
- Dst. Port: 1723



Por ultimo aceptaremos todas las comunicaciones que estén establecidas.

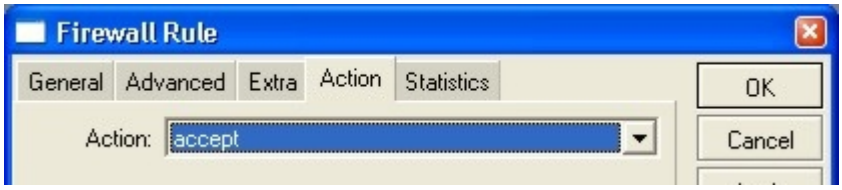
Pestaña General:

- Chain: input
- Connection State: established



Pestaña Action:

- Action: accept

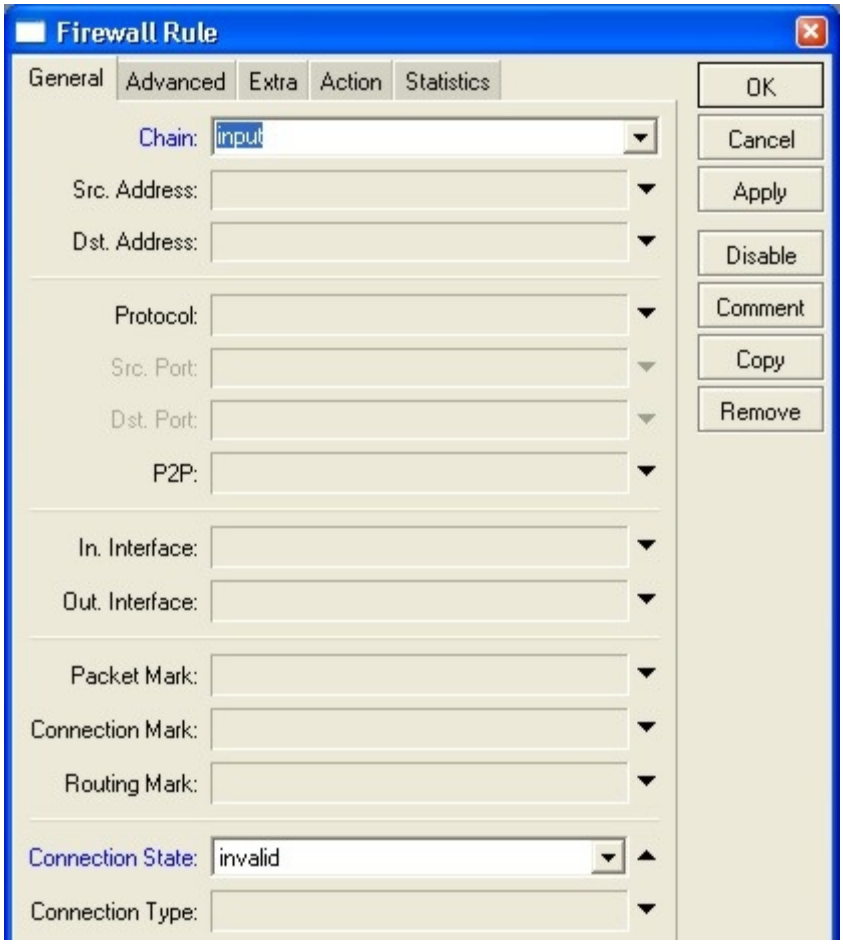


Descartar conexiones inválidas

Para descartar las conexiones inválidas desde el exterior debemos realizar los siguientes pasos. Ir al menú *IP / FIREWALL*. Hacer clic en la pestaña *FILTER RULES*. Luego hacer clic en el icono (+). A la nueva ventana la configuramos de la siguiente manera

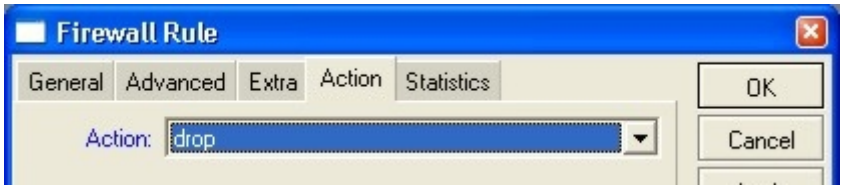
Pestaña General:

- Chain: input
- Connection State: Invalid



Pestaña Action:

- Action: drop

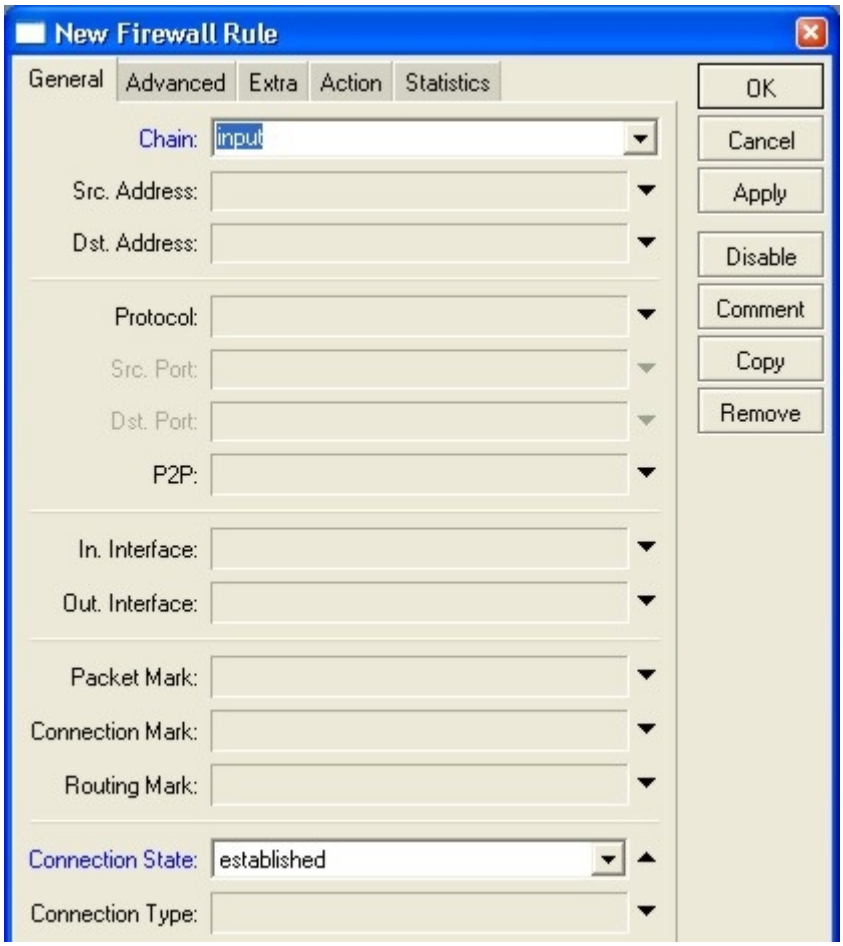


Aceptar conexiones establecidas

Para aceptar las conexiones establecidas desde el exterior debemos realizar los siguientes pasos. Ir al menú *IP / FIREWALL*. Hacer clic en la pestaña *FILTER RULES*. Luego hacer clic en el icono (+). A la nueva ventana la configuramos de la siguiente manera

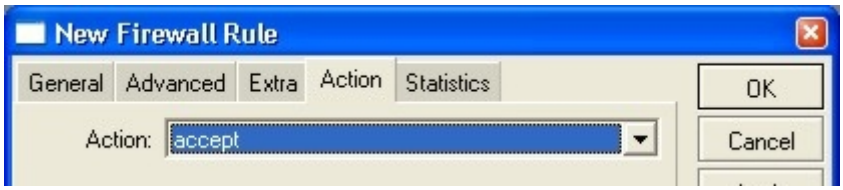
Pestaña General:

- Chain: input
- Connection State: established



Pestaña Action:

- Action: accept

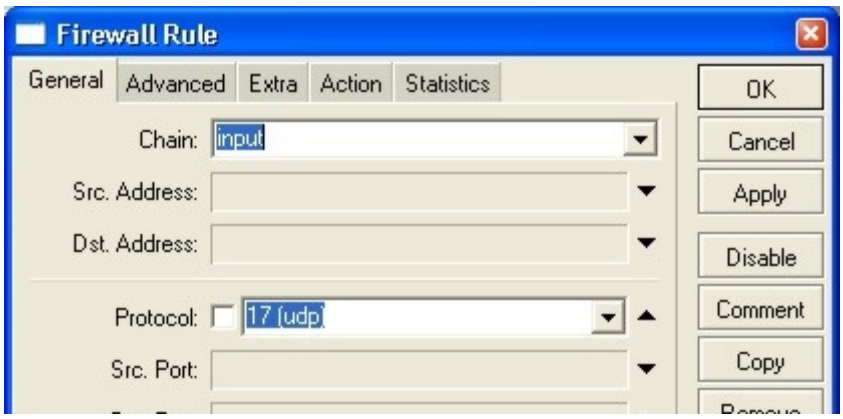


Acepta Trafico UDP

Para aceptar las conexiones UDP establecidas desde el exterior debemos realizar los siguientes pasos. Ir al menú *IP / FIREWALL*. Hacer clic en la pestaña *FILTER RULES*. Luego hacer clic en el icono (+). A la nueva ventana la configuramos de la siguiente manera

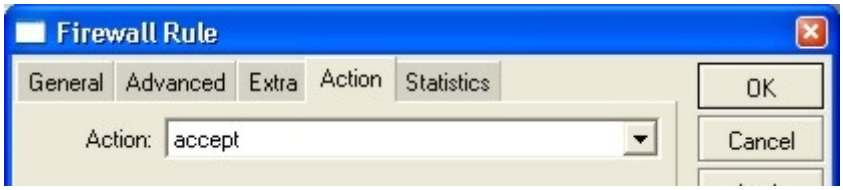
Pestaña General:

- Chain: input
- Protocol: 17 (udp)



Pestaña Action:

- Action: Accept

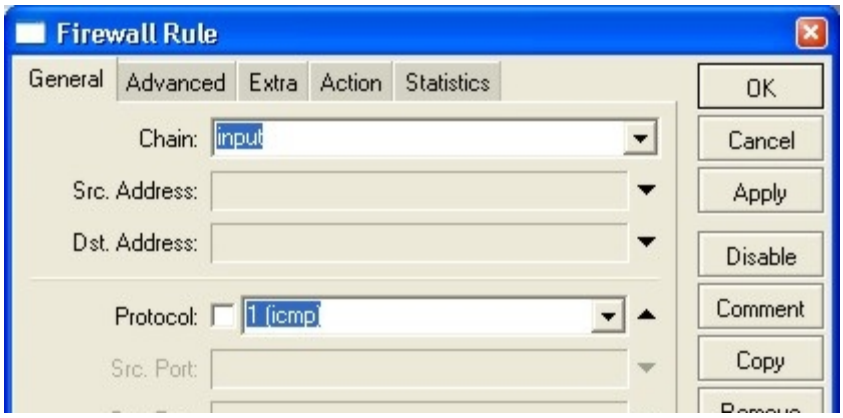


Acepta icmp Limitados

Para aceptar icmp limitados desde el exterior debemos realizar los siguientes pasos. Ir al menú *IP / FIREWALL*. Hacer clic en la pestaña *FILTER RULES*. Luego hacer clic en el icono (+). A la nueva ventana la configuramos de la siguiente manera

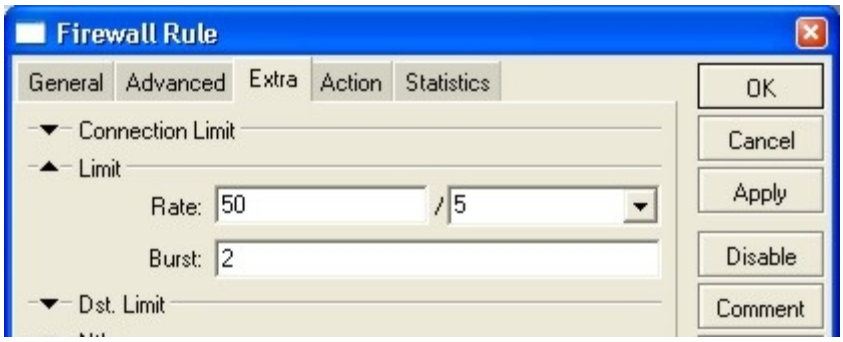
Pestaña General:

- Chain: input
- Protocol: 1 (icmp)



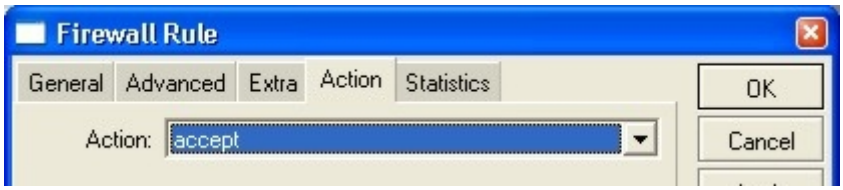
Pestaña Extra:

- Rate: 50 / 5
- Burst: 2



Pestaña Action:

- Action: accept

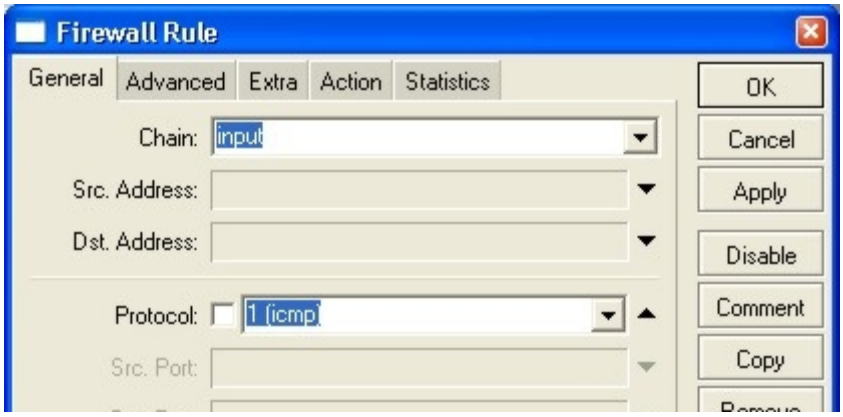


Descarta excesivos icmp

Para descartar excesivos icmp desde el exterior debemos realizar los siguientes pasos. Ir al menú *IP / FIREWALL*. Hacer clic en la pestaña *FILTER RULES*. Luego hacer clic en el icono (+). A la nueva ventana la configuramos de la siguiente manera

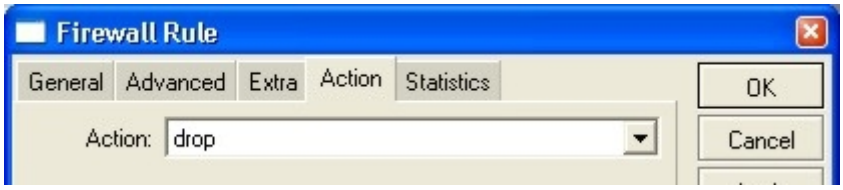
Pestaña General:

- Chain: input
- Protocol: 1 (icmp)



Pestaña Action:

- Action: Drop

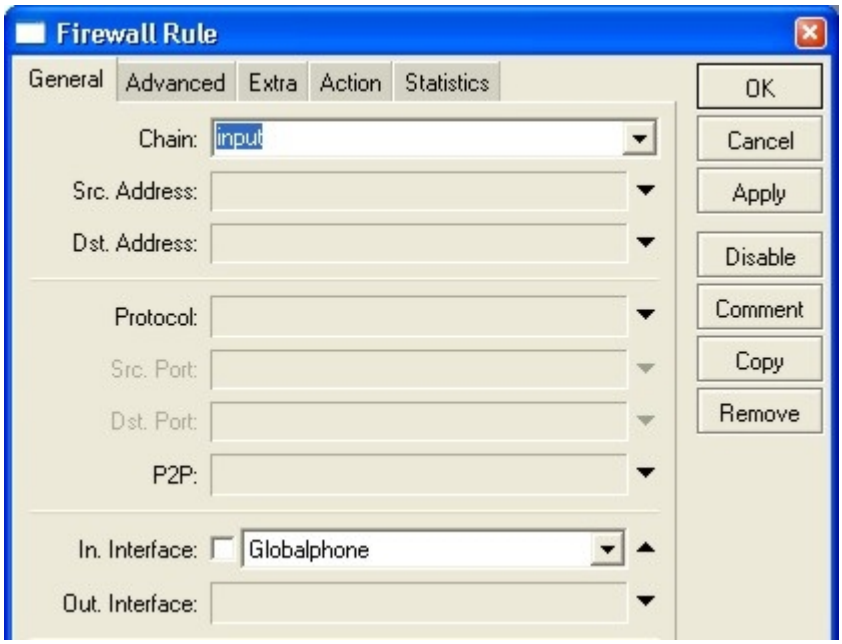


Descarta el resto de las conexiones externas

Para descartar el resto de las conexiones desde el exterior debemos realizar los siguientes pasos. Ir al menú *IP / FIREWALL*. Hacer clic en la pestaña *FILTER RULES*. Luego hacer clic en el icono (+). A la nueva ventana la configuramos de la siguiente manera

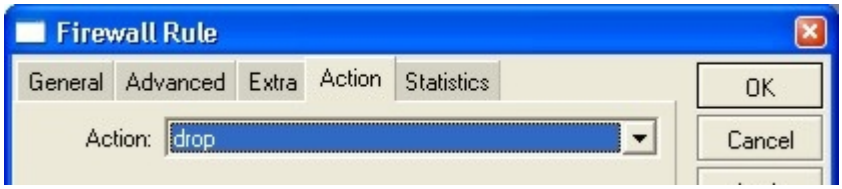
Pestaña General:

- Chain: input
- In. Interface: Globalphone



Pestaña Action:

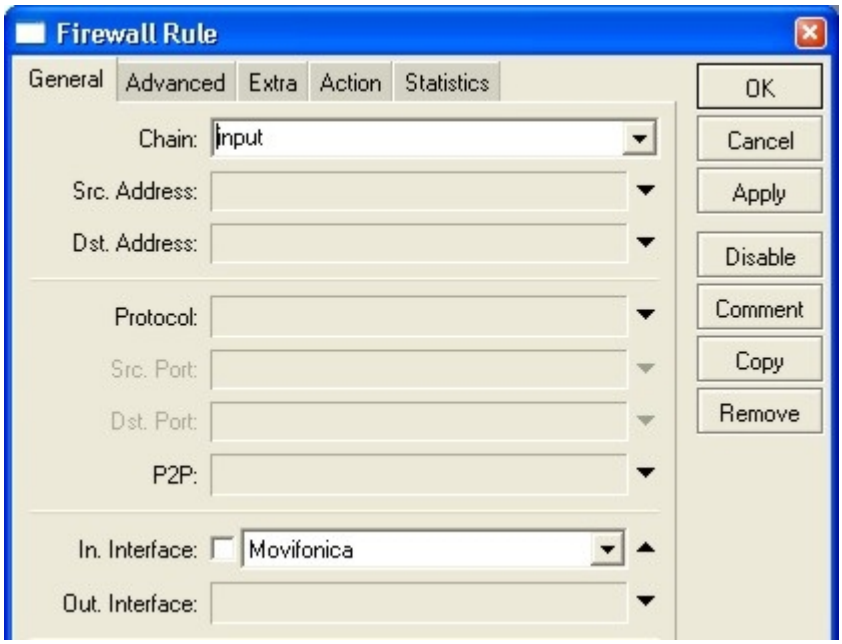
- Action: drop



Agregamos una política nueva para bloquear el acceso externo desde la internase Movifonica de esta manera:

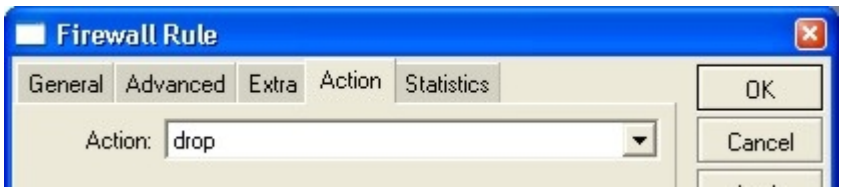
Pestaña General:

- Chain: input
- In. Interface: Movifonica.

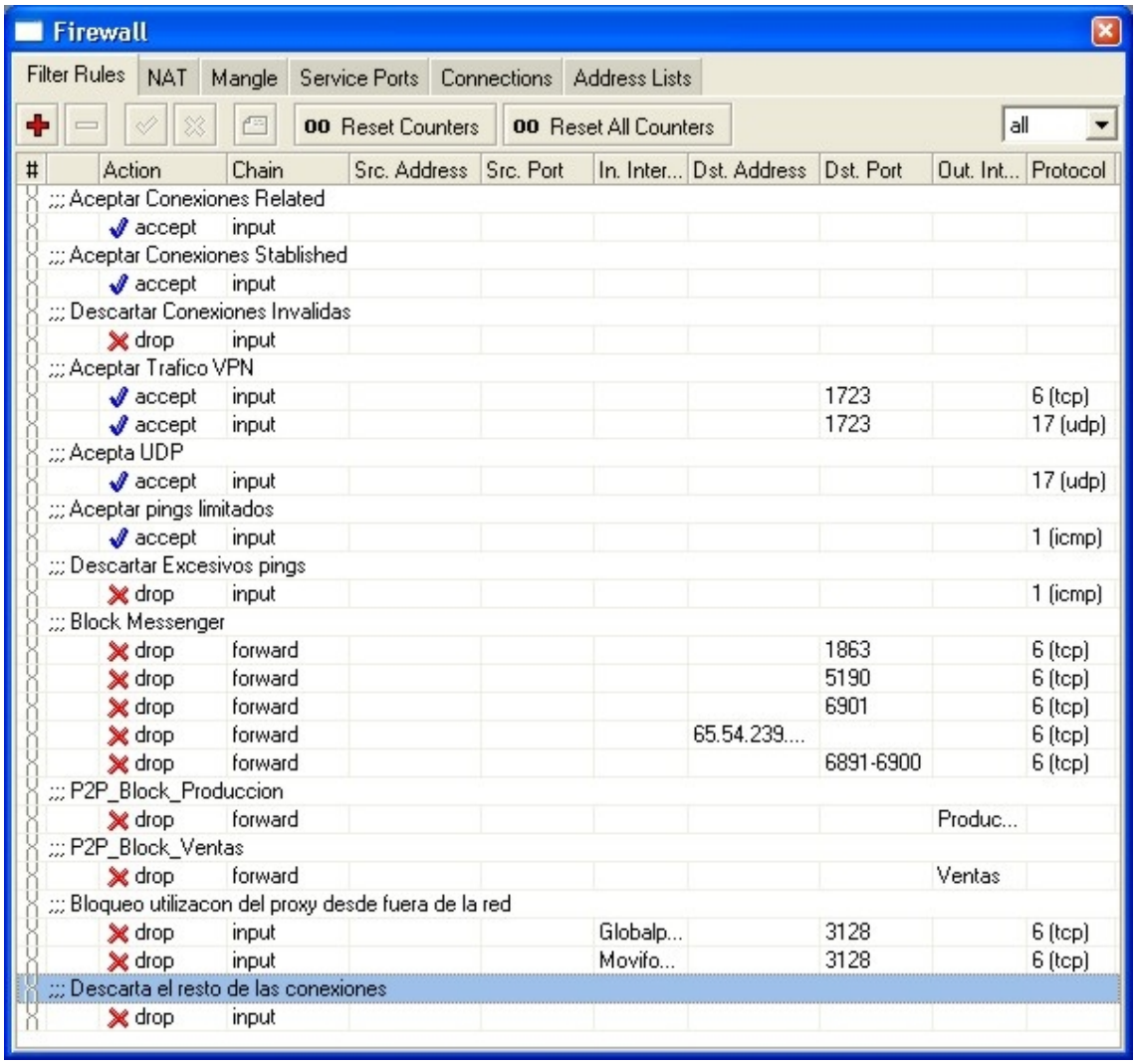


Pestaña Action:

- Action: drop



El orden de las políticas se ven en la siguiente grafica.

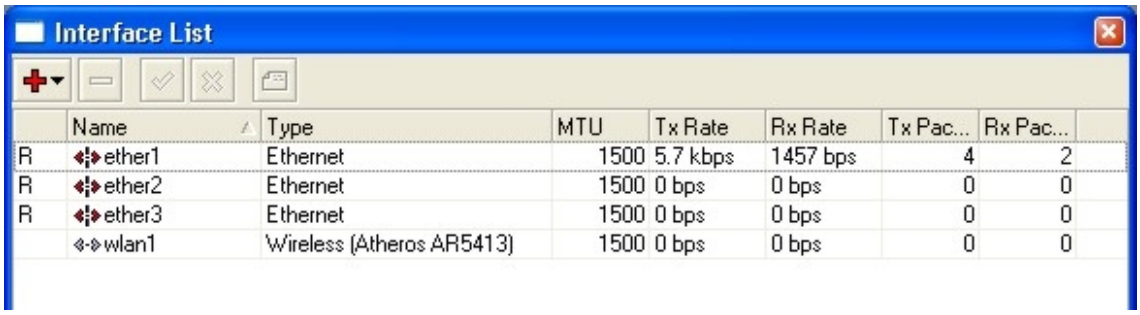


#	Action	Chain	Src. Address	Src. Port	In. Inter...	Dst. Address	Dst. Port	Out. Int...	Protocol
;;; Aceptar Conexiones Related									
	accept	input							
;;; Aceptar Conexiones Stablished									
	accept	input							
;;; Descartar Conexiones Invalidas									
	drop	input							
;;; Aceptar Trafico VPN									
	accept	input					1723		6 (tcp)
	accept	input					1723		17 (udp)
;;; Acepta UDP									
	accept	input							17 (udp)
;;; Aceptar pings limitados									
	accept	input							1 (icmp)
;;; Descartar Excesivos pings									
	drop	input							1 (icmp)
;;; Block Messenger									
	drop	forward					1863		6 (tcp)
	drop	forward					5190		6 (tcp)
	drop	forward					6901		6 (tcp)
	drop	forward				65.54.239....			6 (tcp)
	drop	forward					6891-6900		6 (tcp)
;;; P2P_Block_Produccion									
	drop	forward						Produc...	
;;; P2P_Block_Ventas									
	drop	forward						Ventas	
;;; Bloqueo utilizacon del proxy desde fuera de la red									
	drop	input			Globalp...		3128		6 (tcp)
	drop	input			Movifo...		3128		6 (tcp)
;;; Descarta el resto de las conexiones									
	drop	input							

Configuración Hot Spot

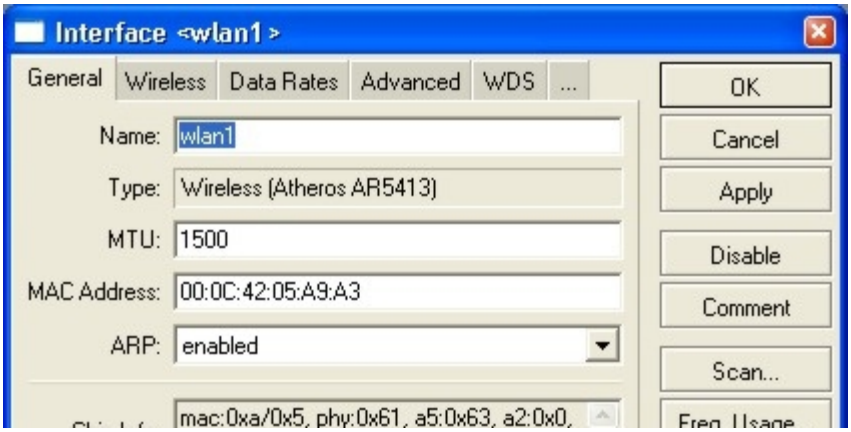
Debido a que nuestra área de esparcimiento no esta cercana al router principal. Se ha decido instalar una red wireless. Para ello se utilizara un router AP Mikrotik RB600.

Logueados al Mikrotik mediante Winbox. Nos dirigimos al menú *INTERFASES*. En la ventana que nos aparece hacemos clic sobre la interfase *wlan1* y la habilitamos apretando el botón derecho del Mouse y elegimos la opción *Enable*



A continuación le hacemos doble clic a la interfase y comenzamos la configuración de la misma. La pestaña General se configura de la siguiente manera.

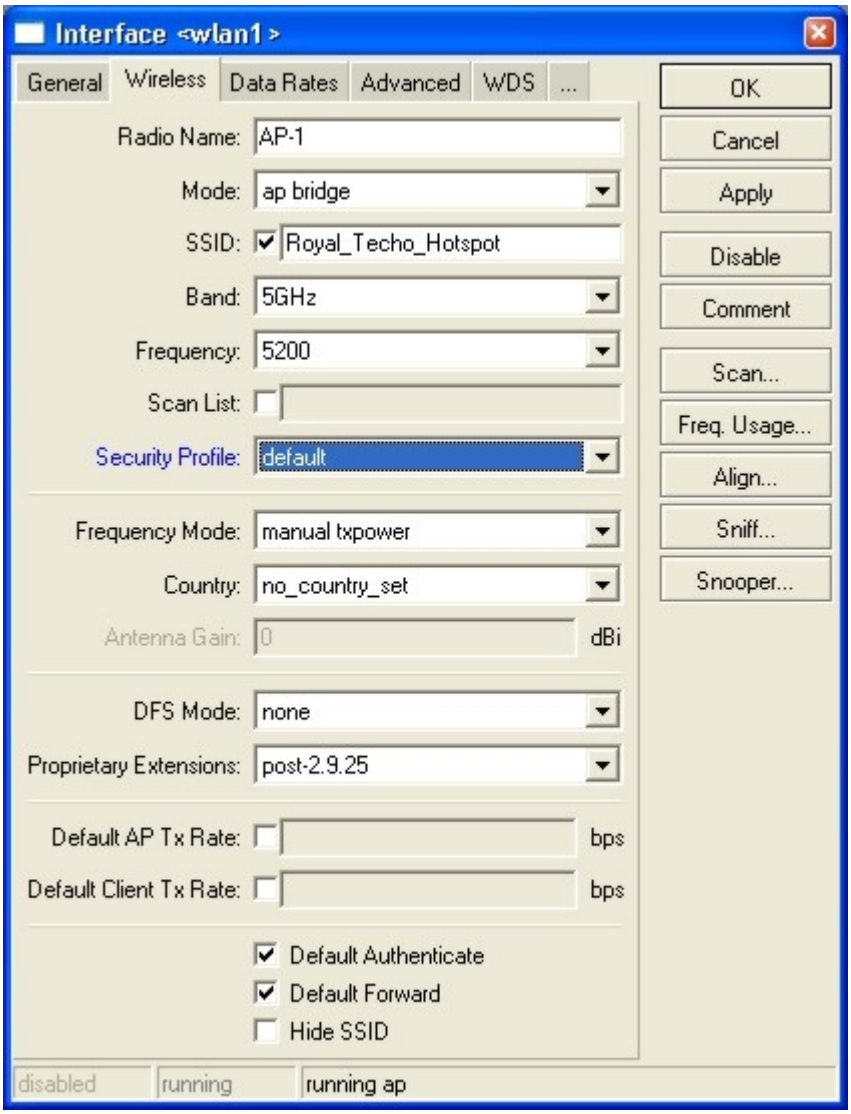
- Name: wlan1
- MTU: 1500
- MAC Address: 00:0C:42:05:A9:A3
- Arp: enabled



Pestaña Wireless:

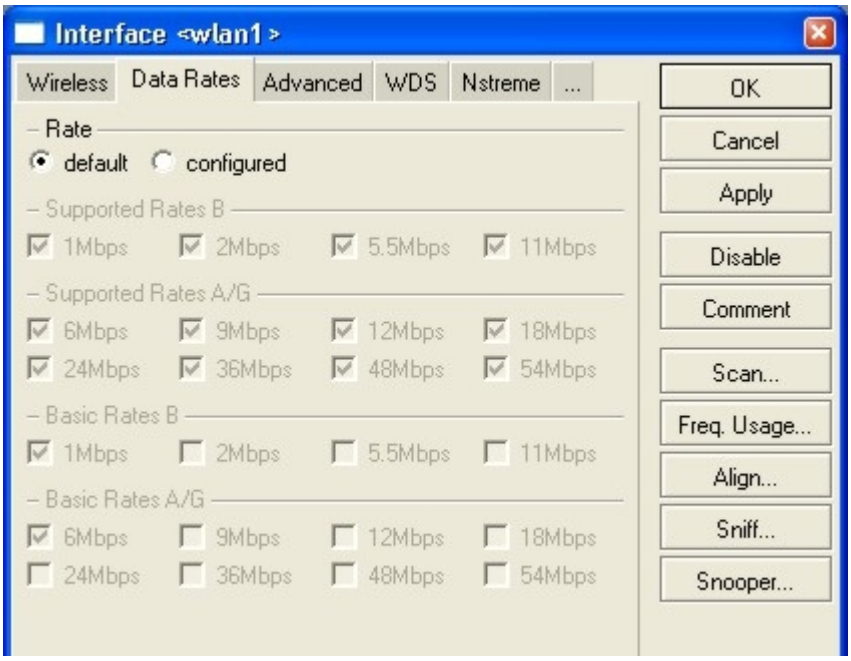
- Radio Name: AP-1
- Mode: AP bridge
- SSID: Royal_Tech_Hotspot
- Band: 5Ghz
- Frequency: 5200
- Security Profile: default

- Frequency Mode: manual Txpower
- County: no_country_set
- DFS Mode: none
- Proprietary Extensions: post-2.9.25
- Default Authenticate: Seleccionado
- Default forward: Seleccionado



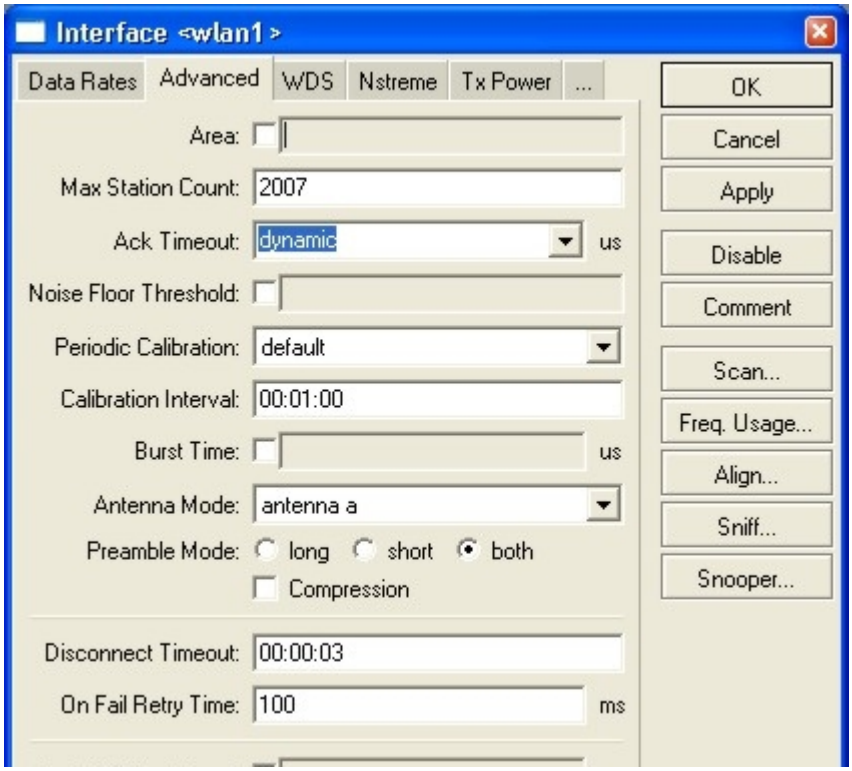
Pestaña Data Rates:

No se le modificara la configuración Standard.



Pestaña Advanced:

- Max Station Count: 2007
- Act Timeout: dynamic
- Periodic Calibration : Default
- Calibration level: 00:01:00
- Antenna mode: antenna a
- Preamble mode: both
- Disconnect time out: 00:00:03
- On Fail Retry Time:100

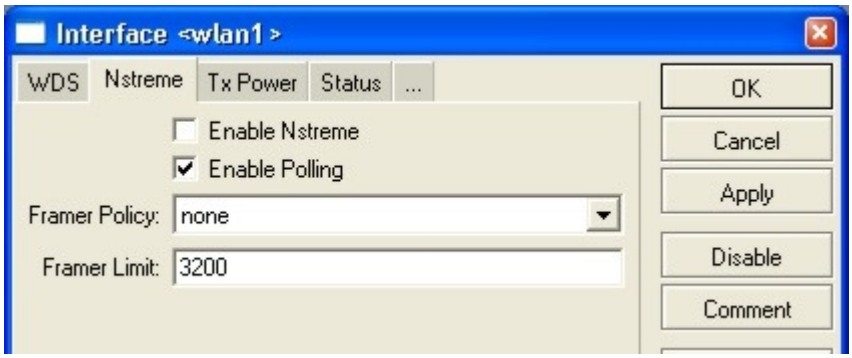


Pestaña WDS:

- WDS Mode: Disable
- WDS default Bridge: none
- WDS Default Cost: 100
- WDS Cost Range: 50-100

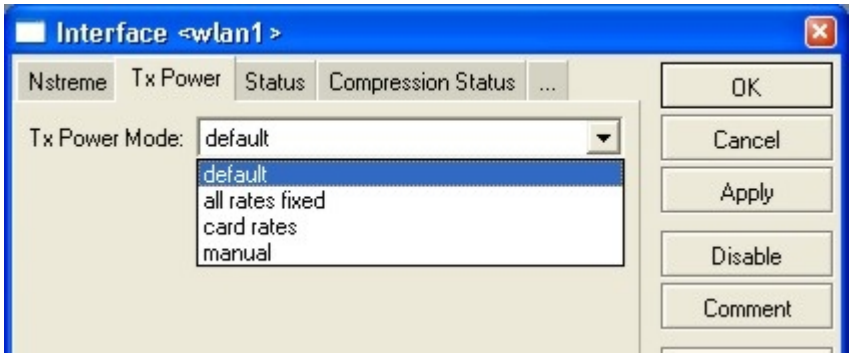
Pestaña Nstreme:

- Enable Ntreme: Deseleccionado
- Enable Polling: Seleccionado
- Framer Policy: none
- Framer Limit: 3200



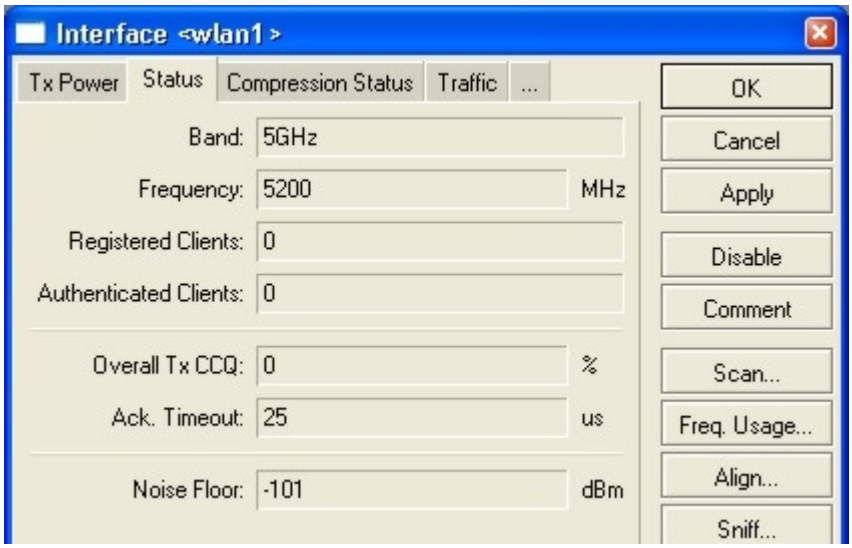
Pestaña Tx Power:

- Tx Power Mode: default



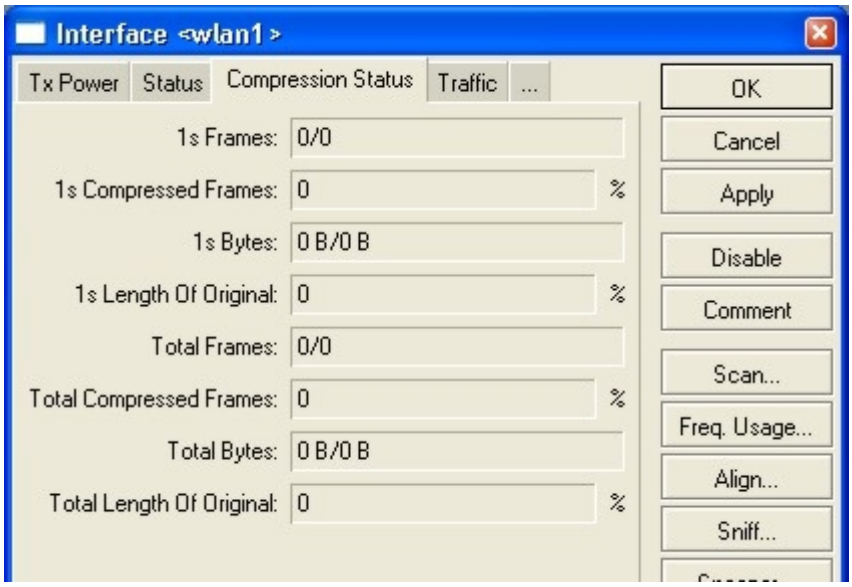
Pestaña Status:

Esta pestaña nos muestra el Status de la interfase Wireless.



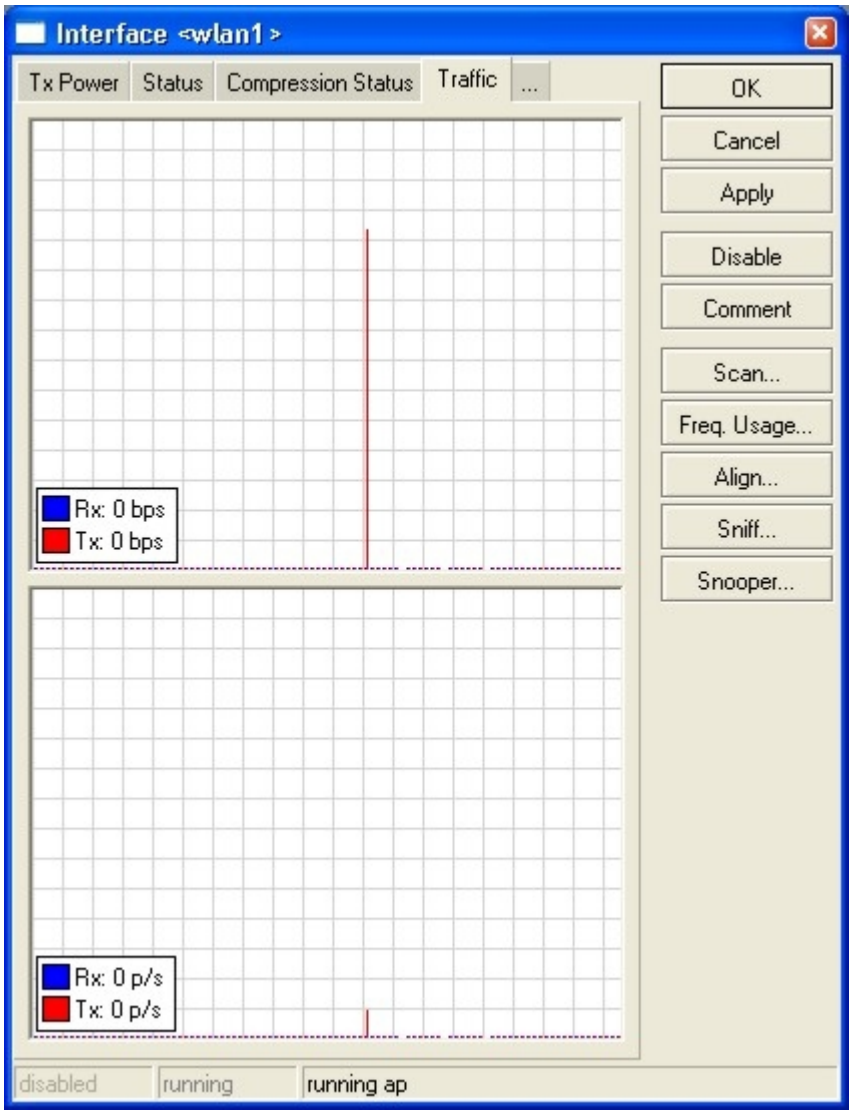
Pestaña compression Status:

Esta pestaña nos muestra el estado de la compresión de datos.



Pestaña Traffic:

Nos muestra el tráfico actual de la interfase en paquetes enviados y recibidos al igual que bits por segundo.



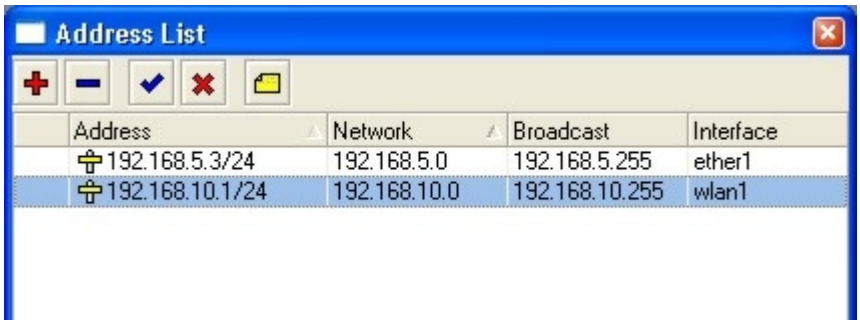
Luego nos dirigimos al menú *IP / ADDRESS*. En la nueva ventana hacemos clic sobre el icono (+) y configuramos una nueva ip, para la interfase ether1. La configuración de la misma es:

- Address: 192.168.5.3/24
- Network: 192.168.5.0
- Broadcast: 192.168.5.255
- Interfase: ether1

A continuación configuraremos la interfase wlan1. Para ello nos dirigimos al menú *IP / ADDRESSES* y hacemos clic sobre el icono (+)

- Address: 192.168.10.1/24
- Network: 192.168.10.0
- Broadcast: 192.168.10.255
- Interfase: wlan

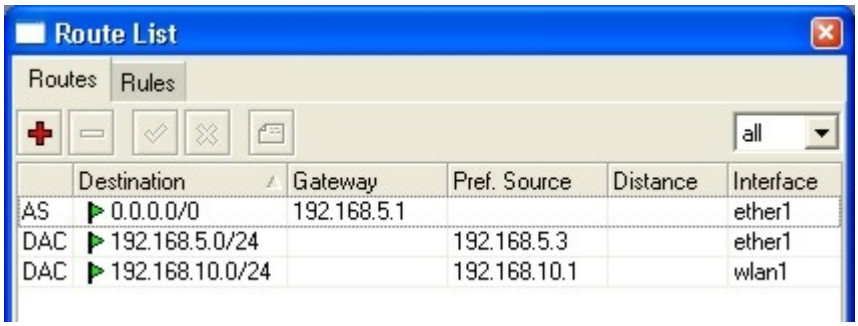
Las interfases configuradas se ven de la siguiente manera.



A continuación debemos asignarle al hotspot el default Gateway para ello, nos dirigimos al menú *IP / ROUTES*. En la nueva ventana le hacemos clic al icono (+) y configuramos la nueva ventana de la siguiente manera.

- Destination: 0.0.0.0/0
- Gateway: 192.168.5.1

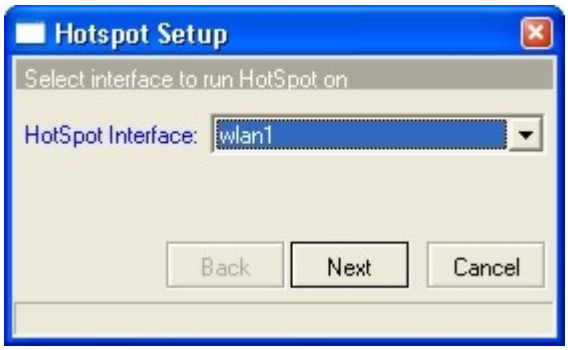
Las rutas se ven configuradas de la siguiente manera:



A continuación deberemos configurar nuestro HotSpot. Para ello nos dirigimos al menú *IP / Hotspot*. En la nueva ventana dentro de la pestaña Servers, hacemos clic sobre el botón *SETUP*.

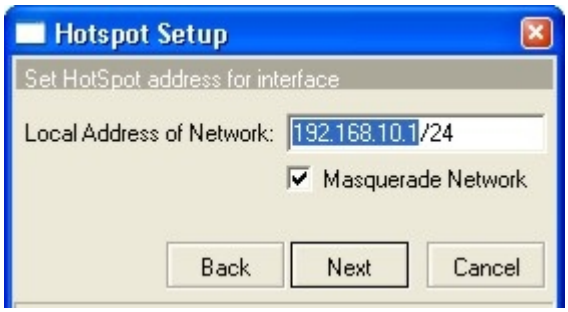
En la ventana que nos aparece la configuramos de la siguiente manera.

- HotSpot interfase: wlan1



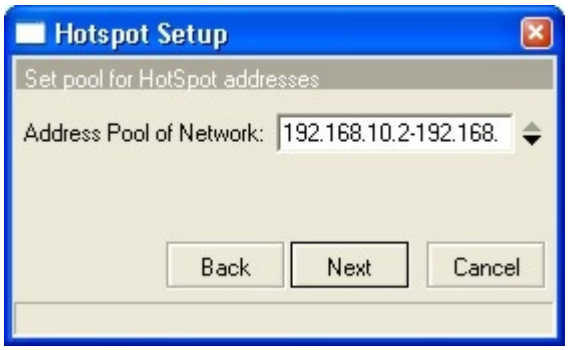
En la ventana siguiente elegimos la dirección de ip para la interfase de hotspot. La configuración es:

- Local Address of Network 192.168.10.1/24
- Masquerade Network: Seleccionado

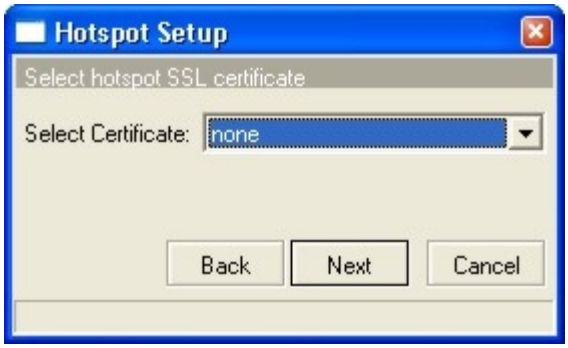


A continuación le asignamos el pool de ip que nos interesa que dicha interfase nos brinde a los clientes. La configuración es:

- Address Pool of Network: 192.168.10.2-192.168.10.254

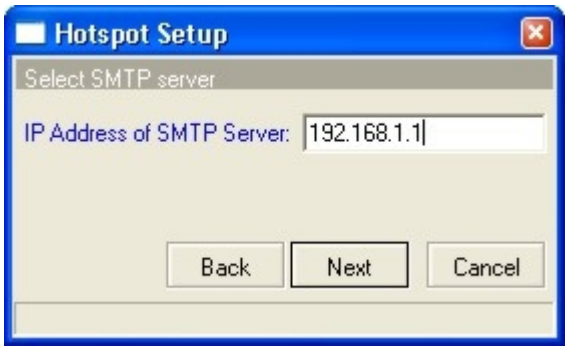


Luego no le seleccionamos ningún certificado SSL



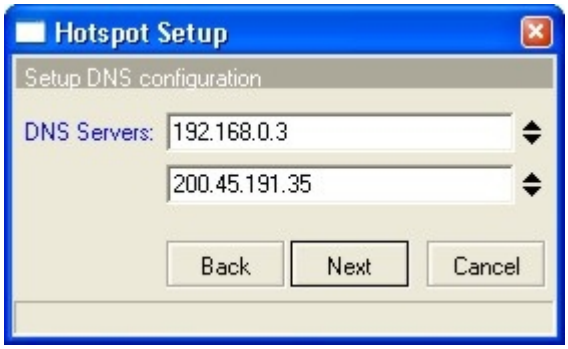
Siguiendo nos pide la dirección del servidor STMP de nuestra red local es:

IP Address of SMTP Server: 192.168.1.1



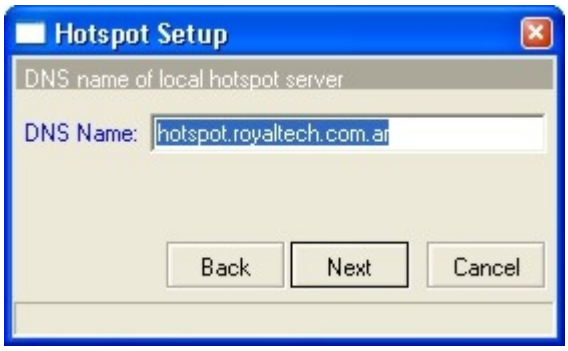
Luego le asignamos los dns correspondientes.

DNS Servers: 192.168.0.3
200.45.191.35

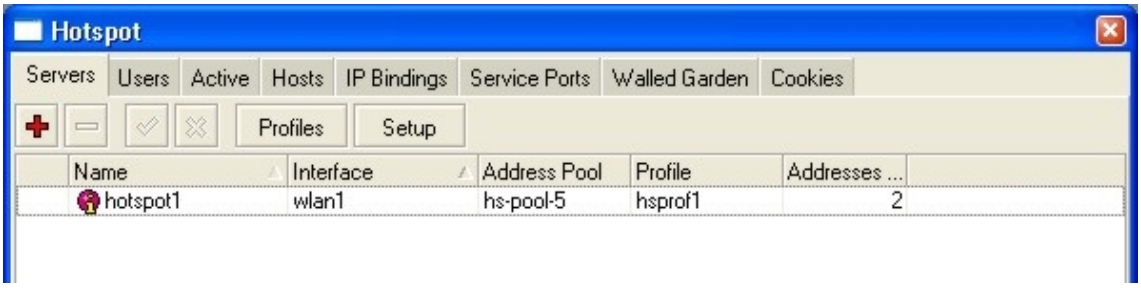


Seguimos con el nombre de nuestro servidor dns el cual es:

- DNS Name: hotspot.royaltech.com.ar



Finalizando creamos nuestro usuario administrador. Nuestro hotspot configurado se ve de la siguiente manera.



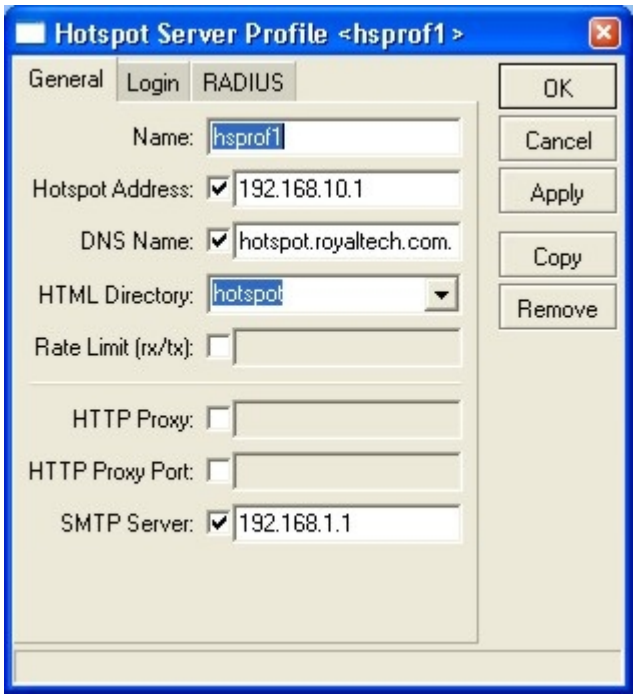
Le hacemos doble clic al hotspot1 para configurar sus parámetros. La configuración de los mismos son:

- Name: hotspot
- Interfase: wlan1
- Hs-pool-5
- Profile hsprofile1
- Idel Timeout: 00:05:00
- Addresses per Mac: 2

Luego dentro de la pestaña Servers hacemos clic en profiles. Y luego editamos la configuración del profile *hsprof1*. La configuración del mismo es:

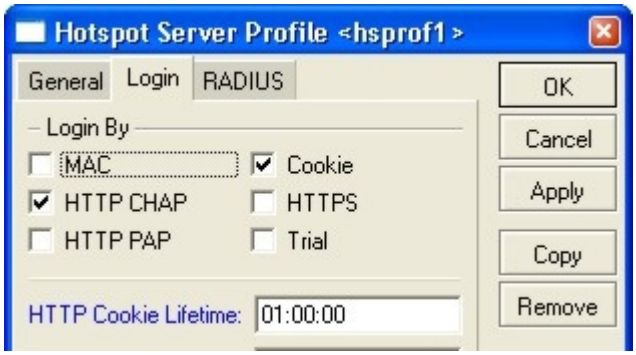
Pestaña General:

- Name: hsprof1
- Hotspot Address: 192.168.10.1
- DNS Name: Hotspot.royaltech.com.ar
- HTML Directory: hotspot
- SMTP: 192.168.1.1



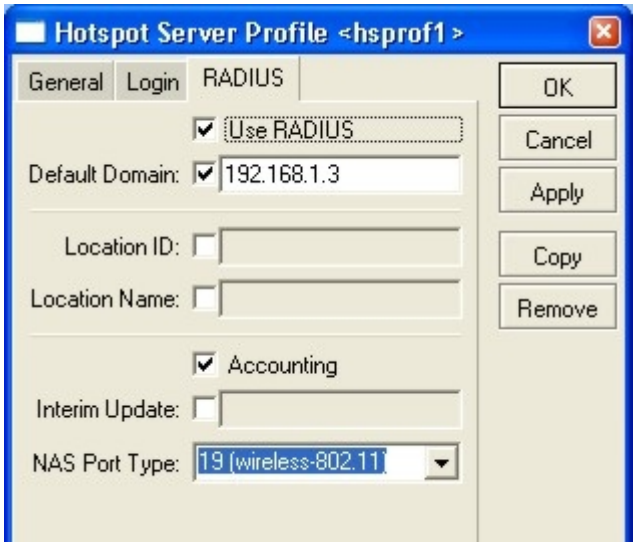
Pestaña Login:

- HTTP CHAP y Cookie: Seleccionado
- MAC, HTTP PAP, HTTPS y Trial: deseleccionado.
- HTTP Cookie Lifetime: 01:00:00



Pestaña RADIUS:

- Use RADIUS: (seleccionado)
- Default Domain: 192.168.1.3
- NAS PORT Type 19 (Wireless-802.11)



Luego hacemos clic sobre la pestaña Users hacemos clic en el botón Profile y generamos uno. La configuración del mismo es:

- Name Profile_Hotspot
- Address Pool: hs-pool-5
- Idle Timeout. None
- Keekalive Timeout: 00:02:00
- Shared Users: 1
- Rate limit: 128k/256k

Pestaña Advertise:

- Advertise: deseleccionado

Pestaña Script:

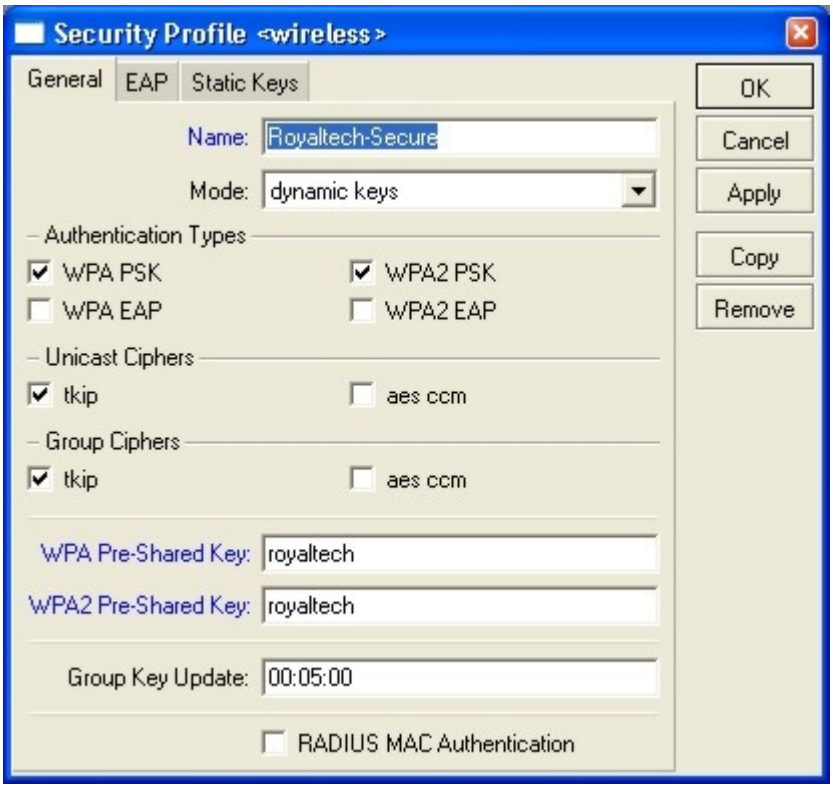
No se genera ningún script y queda configurada por default.

Finalmente generaremos un perfil de seguridad para las conexiones Wireless. Para ello debemos ir al menú *WIRELESS*, luego hacemos clic en al pestaña *Security Profiles*. Y creamos un profile nuevo haciendo clic en el icono (+).

Pestaña General:

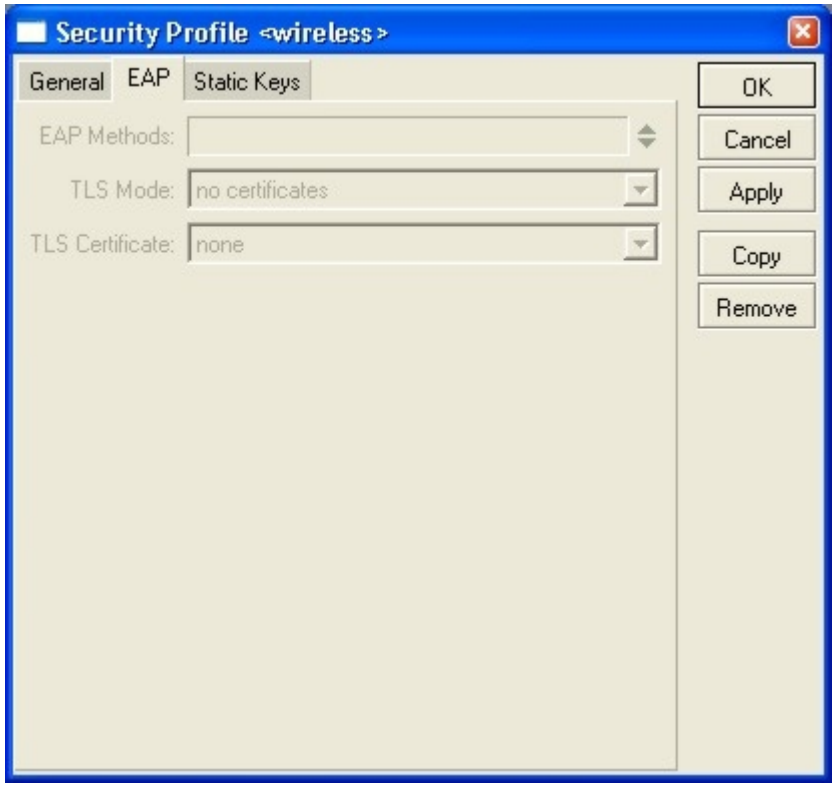
- Name: Royaltech-Secure
- Mode: dynamic keys
- WPA PSK, WPA2 PSK: Seleccionados
- Unicast ciphers
    - Tkip: Seleccionado
    - Aes ccm: Seleccionado
- Group Ciphers
    - Tkip: Seleccionado
    - Aes ccm: Seleccionado

- WPA Pre-Shared Key: royaltech
- WPA2 Preshared Key:royaltech
- RADIUS MAC Authentication (deseleccionado)



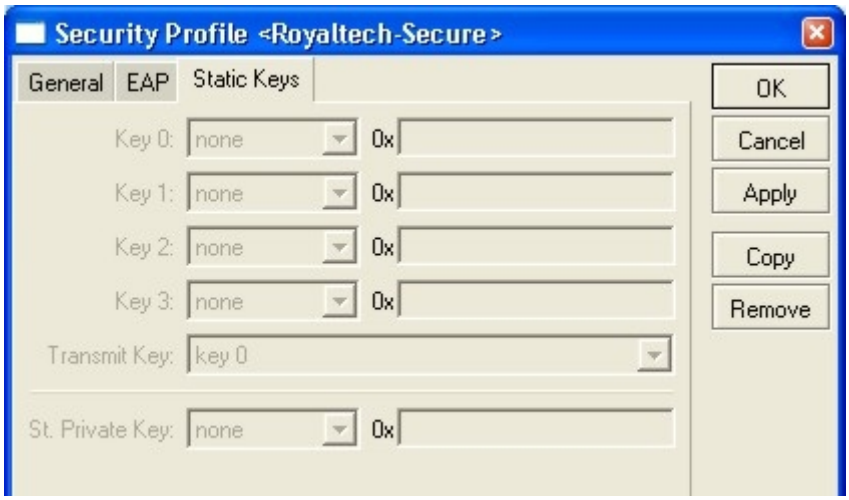
Pestaña EAP:

- EAP Methods:
- TLS Mode: no certifícate
- TLS certifícate: none



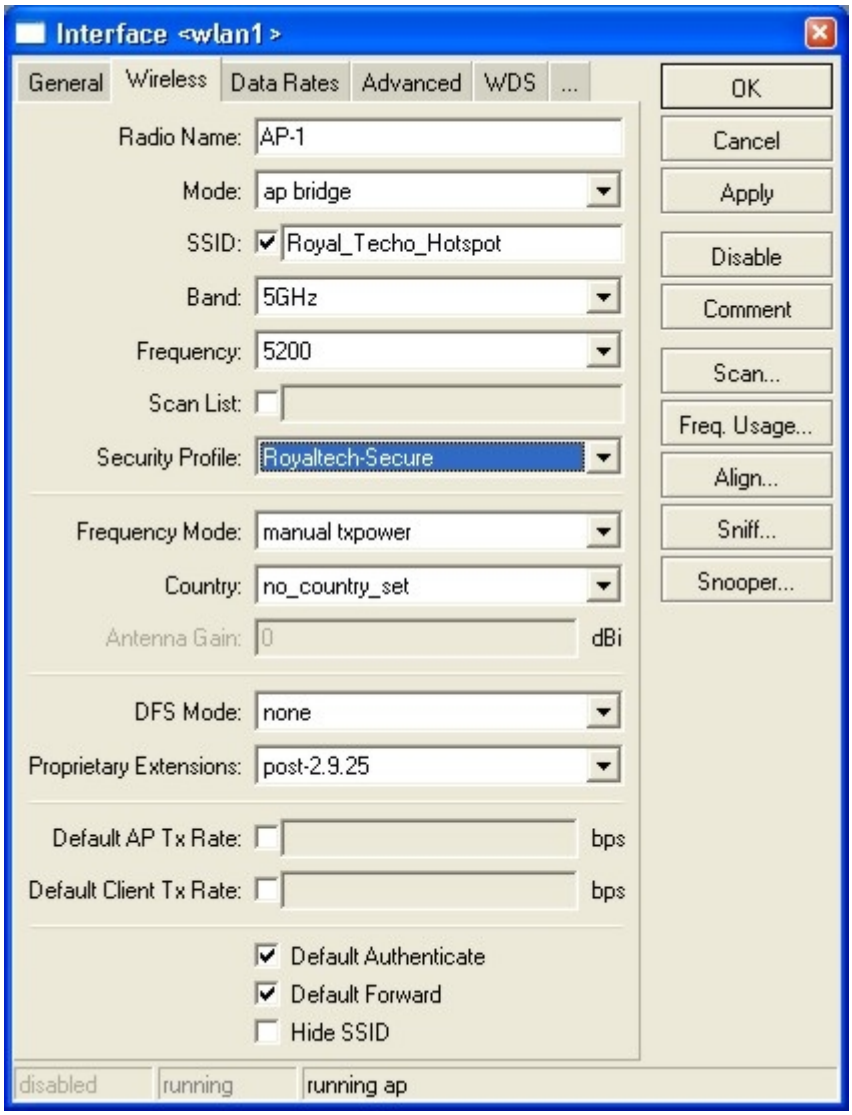
Pestaña Static Keys:

No utilizaremos llaves estáticas.



A continuación debemos asígnale este perfil de seguridad a nuestra interfase wlan1. Para ello nos dirigimos al menú *WIRELESS*. Dentro de la pestaña *Interfases*. Le hacemos doble clic a nuestra interfase wlan1 y modificamos el siguiente valor.

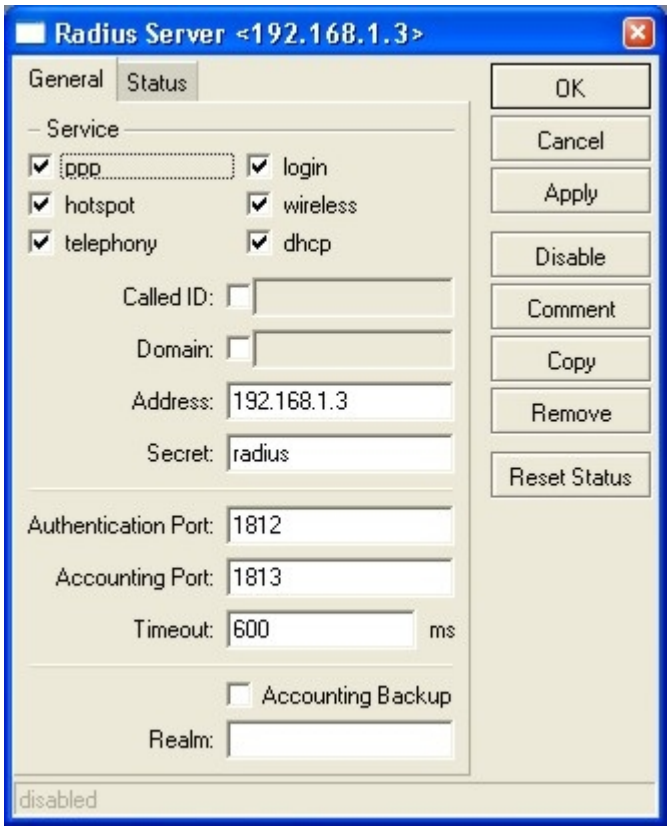
- Security Profile: royaltech-Secure.



Finalmente Vamos al menú *RADIUS*. En la ventana nueva que se nos abre la hacemos clic en el icono (+). La nueva ventana la configuramos de la siguiente manera:

- Ppp, hotspot, login, wireless, telephony, dhcp: Seleccionados
- Address: 192.168.0.3

- Secret: Radius
- Authentication port:1812
- Accounting:1813
- Time out : 600



Servidor de SNMP

Debido a los beneficios que brinda el monitoreo remoto de los servicios de una red. Hemos decidido implementar y habilitarle el servidor de snmp de un router Mikrotik.

Para poder realizar dicha implementación la dividiremos en dos partes. Primero la habilitación o activación del snmp en el router de CBA para la red 192.168.1.0. Luego utilizando la aplicación mrtg instalada en el servidor de la dirección de ip 192.168.1.2 graficaremos algunos datos obtenidos.

Configuración Servidor SMNP

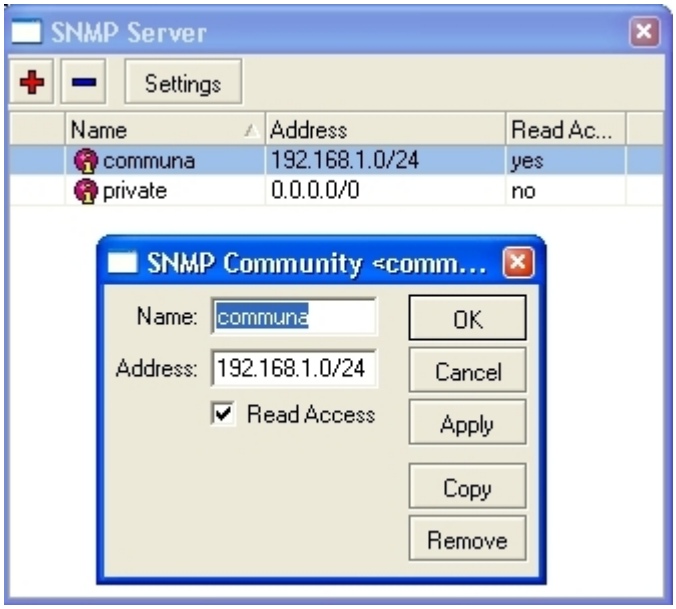
Dentro del winbox, nos dirigimos al menú *SNMP*, se nos abre la ventana de configuración, hacemos clic en el botón *Settings* y le cargamos los siguientes datos.

- Enabled (marcado)
- Contact info: tatubias@server
- Location: cba

Llenando esos casilleros ya tendremos habilitado el servidor de snmp del mikrotik. Luego hay que crear la comunidad snmp, la cual la llamaremos servers. Para ello hacemos clic en el icono (+) y se nos abre la ventana de configuración de comunidad y le cargamos los siguientes datos:

- Name: communa
- Address: 192.168.1.0/24
- Read Access (marcado)

Para una configuración básica esto nos alcanza para poder obtener cierta información del Mikrotik.



Dentro de winbox ir al menú *New Terminal* se nos abre una ventana de terminal. Ahí dentro debemos escribir lo siguiente para obtener las oid del sistema

```
# /interfase print oid
```

Dicho comando nos mostrara la salida de pantalla con los datos de oid requeridos.

```
[admin@MikroTik]interfase print oid

0  R name=.1.3.6.1.2.1.2.2.1.2.1 mtu=.1.3.6.1.2.1.2.2.1.4.1
      mac-address=.1.3.6.1.2.1.2.2.1.6.1 admin-status=.1.3.6.1.2.1.2.2.1.7.1
      oper-status=.1.3.6.1.2.1.2.2.1.8.1 bytes-in=.1.3.6.1.2.1.2.2.1.10.1
      packets-in=.1.3.6.1.2.1.2.2.1.11.1 discards-in=.1.3.6.1.2.1.2.2.1.13.1
      errors-in=.1.3.6.1.2.1.2.2.1.14.1 bytes-out=.1.3.6.1.2.1.2.2.1.16.1
      packets-out=.1.3.6.1.2.1.2.2.1.17.1 discards-out=.1.3.6.1.2.1.2.2.1.19.1
      errors-out=.1.3.6.1.2.1.2.2.1.20.1

 1  R name=.1.3.6.1.2.1.2.2.1.2.2 mtu=.1.3.6.1.2.1.2.2.1.4.2
      mac-address=.1.3.6.1.2.1.2.2.1.6.2 admin-status=.1.3.6.1.2.1.2.2.1.7.2
      oper-status=.1.3.6.1.2.1.2.2.1.8.2 bytes-in=.1.3.6.1.2.1.2.2.1.10.2
      packets-in=.1.3.6.1.2.1.2.2.1.11.2 discards-in=.1.3.6.1.2.1.2.2.1.13.2
      errors-in=.1.3.6.1.2.1.2.2.1.14.2 bytes-out=.1.3.6.1.2.1.2.2.1.16.2
      packets-out=.1.3.6.1.2.1.2.2.1.17.2 discards-out=.1.3.6.1.2.1.2.2.1.19.2
      errors-out=.1.3.6.1.2.1.2.2.1.20.2

 2  R name=.1.3.6.1.2.1.2.2.1.2.3 mtu=.1.3.6.1.2.1.2.2.1.4.3
      mac-address=.1.3.6.1.2.1.2.2.1.6.3 admin-status=.1.3.6.1.2.1.2.2.1.7.3
      oper-status=.1.3.6.1.2.1.2.2.1.8.3 bytes-in=.1.3.6.1.2.1.2.2.1.10.3
```

```
     packets-in=.1.3.6.1.2.1.2.2.1.11.3 discards-in=.1.3.6.1.2.1.2.2.1.13.3
     errors-in=.1.3.6.1.2.1.2.2.1.14.3 bytes-out=.1.3.6.1.2.1.2.2.1.16.3
     packets-out=.1.3.6.1.2.1.2.2.1.17.3 discards-out=.1.3.6.1.2.1.2.2.1.19.3
     errors-out=.1.3.6.1.2.1.2.2.1.20.3

3  R name=.1.3.6.1.2.1.2.2.1.2.7 mtu=.1.3.6.1.2.1.2.2.1.4.7
     mac-address=.1.3.6.1.2.1.2.2.1.6.7 admin-status=.1.3.6.1.2.1.2.2.1.7.7
     oper-status=.1.3.6.1.2.1.2.2.1.8.7 bytes-in=.1.3.6.1.2.1.2.2.1.10.7
     packets-in=.1.3.6.1.2.1.2.2.1.11.7 discards-in=.1.3.6.1.2.1.2.2.1.13.7
     errors-in=.1.3.6.1.2.1.2.2.1.14.7 bytes-out=.1.3.6.1.2.1.2.2.1.16.7
     packets-out=.1.3.6.1.2.1.2.2.1.17.7 discards-out=.1.3.6.1.2.1.2.2.1.19.7
     errors-out=.1.3.6.1.2.1.2.2.1.20.7

4  R name=.1.3.6.1.2.1.2.2.1.2.10 mtu=.1.3.6.1.2.1.2.2.1.4.10
     mac-address=.1.3.6.1.2.1.2.2.1.6.10 admin-status=.1.3.6.1.2.1.2.2.1.7.10
     oper-status=.1.3.6.1.2.1.2.2.1.8.10 bytes-in=.1.3.6.1.2.1.2.2.1.10.10
     packets-in=.1.3.6.1.2.1.2.2.1.11.10 discards-in=.1.3.6.1.2.1.2.2.1.13.10
     errors-in=.1.3.6.1.2.1.2.2.1.14.10 bytes-out=.1.3.6.1.2.1.2.2.1.16.10
     packets-out=.1.3.6.1.2.1.2.2.1.17.10 discards-out=.1.3.6.1.2.1.2.2.1.19.10
     errors-out=.1.3.6.1.2.1.2.2.1.20.10
```

Observemos los valores obtenidos:

- *packets-in=.1.3.6.1.2.1.2.2.1.11.10*
- *packets-out=.1.3.6.1.2.1.2.2.1.17.10*
- *packets-in=.1.3.6.1.2.1.2.2.1.11.7*
- *packets-out=.1.3.6.1.2.1.2.2.1.17.7*
- *packets-in=.1.3.6.1.2.1.2.2.1.11.3*
- *packets-out=.1.3.6.1.2.1.2.2.1.17.3*
- *packets-in=.1.3.6.1.2.1.2.2.1.11.2*
- *packets-out=.1.3.6.1.2.1.2.2.1.17.2*

Dichos valores los utilizaremos mas adelante en la configuración del mrtg

Concluida la primera parte de la configuración, deberemos instalar el software mrtg en el servidor de debian que tenemos en la red. Damos por entendido que el servidor apache ya esta instalado y corriendo.

Para la instalación seguiremos los siguientes pasos.

```
# apt-get install mrtg
```

Con el software ya instalado editamos el archivo de configuración que se encuentra en /etc/mrtg.cfg.

```
EnableIPv6: no
WorkDir: /var/www/mrtg

######################################################################
# System: 192.168.1.1
# Description: router
# Contact: tatubias@server
# Location: cba
######################################################################



Target[192.168.1.1_cpu]:
1.3.6.1.2.1.25.3.3.1.2.1&1.3.6.1.2.1.25.3.3.1.2.1:communa@192.168.1.1:
AbsMax[192.168.1.1_cpu]: 100
MaxBytes[192.168.1.1_cpu]: 100
Title[192.168.1.1_cpu]: 192.168.1.1 CPU load
PageTop[192.168.1.1_cpu]: <H1>192.168.1.1 CPU load</H1>
Options[192.168.1.1_cpu]: gauge,growright,nopercent, noo
YLegend[192.168.1.1_cpu]: CPU load
ShortLegend[192.168.1.1_cpu]: %
LegendI[192.168.1.1_cpu]: CPU load (percentage)

### Paquetes in out ###

Target[192.168.1.1_2]:
1.3.6.1.2.1.2.2.1.11.2&1.3.6.1.2.1.2.2.1.17.2:communa@192.168.1.1:
MaxBytes[192.168.1.1_2]: 64000
Title[192.168.1.1_2]: Paquetes in / out interfase 1
PageTop[192.168.1.1_2]: <H1>Paquetes in / out</H1>
 <TABLE>
   <TR><TD>System:</TD>     <TD>PMI 192.168.1.1 </TD></TR>
   <TR><TD>Description:</TD><TD> Paquetes in / out </TD></TR>
```

```
 </TABLE>


### Paquetes in out ###

Target[192.168.1.1_2]:
1.3.6.1.2.1.2.2.1.11.3&1.3.6.1.2.1.2.2.1.17.3:communa@192.168.1.1:
MaxBytes[192.168.1.1_2]: 64000
Title[192.168.1.1_2]: Paquetes in / out interfase 2
PageTop[192.168.1.1_2]: <H1>Paquetes in / out</H1>
 <TABLE>
   <TR><TD>System:</TD>     <TD>PMI 192.168.1.1 </TD></TR>
   <TR><TD>Description:</TD><TD> Paquetes in / out </TD></TR>
 </TABLE>



### Paquetes in out ###

Target[192.168.1.1_2]:
1.3.6.1.2.1.2.2.1.11.7&1.3.6.1.2.1.2.2.1.17.7:communa@192.168.1.1:
MaxBytes[192.168.1.1_2]: 64000
Title[192.168.1.1_2]: Paquetes in / out interfase 3
PageTop[192.168.1.1_2]: <H1>Paquetes in / out</H1>
 <TABLE>
   <TR><TD>System:</TD>     <TD>PMI 192.168.1.1 </TD></TR>
   <TR><TD>Description:</TD><TD> Paquetes in / out </TD></TR>
 </TABLE>



### Paquetes in out ###

Target[192.168.1.1_2]:
1.3.6.1.2.1.2.2.1.11.10&1.3.6.1.2.1.2.2.1.17.10:communa@192.168.1.1:
MaxBytes[192.168.1.1_2]: 64000
Title[192.168.1.1_2]: Paquetes in / out interfase 4
PageTop[192.168.1.1_2]: <H1>Paquetes in / out</H1>
 <TABLE>
   <TR><TD>System:</TD>     <TD>PMI 192.168.1.1 </TD></TR>
   <TR><TD>Description:</TD><TD> Paquetes in / out </TD></TR>
 </TABLE>
```

Esta configuración nos mostrara la carga del CPU y los paquetes enviados y recibidos por 4 interfases. A continuación deberá crear el archivo index.html para que sea visualizada la información en forma de gráficos en una pagina Web.

```
# indexmaker /etc/mrtg.cfg --columns=1 --output \
/var/www/mrtg/index.html
```

Finalmente debe correr 3 veces el comando *mrtg* para que se generen los archivos de base de datos necesarios.

```
#mrtg
```

Esta configuración será ejecutada cada 5 minutos mediante el cron

Redireccionando nuestro navegador a la dirección http://192.168.1.2/mrtg nos dará las graficas obtenidas.

Servidor Radius

Debido a la gran inseguridad que presentan las redes se ha decidido implementar un servidor radius para autenticar algunos de los usuarios. Para ello se necesitará instalar software adicional al Mikrotik. Partimos de la base de tener nuestro servidor con debian instalado. Los pasos a seguir son los siguientes:

Configuración Servidor Radius

Debemos instalar el servidor de base de datos MySQL y el servidor Web Apache.

```
#apt-get install apache2 mysql-server mysql-common
```

Para confirmar que estén funcionando utilizamos el cliente Web que poseamos y lo redirigimos a la dirección ip del servidor. Ahí nos aparecerá una venta que nos informa que el servidor Web esta funcionando.

Para verificar que el servidor MySQL este funcionando simplemente desde la consola del servidor tipeamos:

```
#mysql
```

Esto nos mostrara que se pudo conectar al servidor de base de datos. Para salir de cliente de MySQL escribimos:

```
#exit
```

A continuación debemos instalar el servidor radius en si y algunos otros componentes.

```
# apt-get install freeradius freeradius-mysql freeradius-dialupadmin
```

Seguido de la instalación de servidor nos toca la configuración del mismo. Para ello editamos el archivo /etc/freeradius/clients.conf

```
#nano /etc/freeradius/clients.conf
```

En dicho archivo agregaremos el ip del Mikrotik y el secreto o contraseña que se eligió “radius”.

```
# Client Name Key
#---------------- ----------
192.168.1.1 radius
```

A continuación debemos configurar el archive /etc/freeradius/naslist.

```
#nano /etc/freeradius/naslist
```

Al mismo le agregamos la siguiente línea, que nos dice el numero de ip de nuestro Mikrotik el un nombre corto para identificarlo y el tipo.

```
# NAS Name      Short Name      Type
#----------     ------------    ----
192.168.1.1     mikrotik        mikrotik
```

Editamos el archivo /etc/freeradius/radiusd.conf.

```
#vi /etc/freeradius/radiusd.conf
```

En el mismo buscamos las siguientes líneas dentro de la sección Unix, si están comentadas las descomentamos como esta a continuación. De lo contrario las agregamos.

```
passwd = /etc/passwd
shadow = /etc/shadow
group = /etc/group
```

Buscamos en el archivo freeradius.conf dentro de la sección “Authorize”. La secuencia “# sql”. La descomentamos y también buscamos dentro de la misma sección “suffix” y “files” a los mismos los comentamos

Buscamos luego la sección “accounting” la secuencia “# sql” y la descomentamos.

Buscamos dentro de la sección “modules” dentro de pap la siguiente secuencia encryption_scheme= cryp la cambiamos por encryption_scheme = clear. Esto hará que cuando el freeradius nos lea la contraseña de la base de dato, la lea sin ningún tipo de encriptación como md5 u otra.

Dentro de la sección “modules” nos dirigimos a la sub sección de *mschap* ahí descomentamos las siguientes líneas.

```
Require_encryption = yes
Require_strong = yes
```

Finalizada la configuración del archivo /etc/freeradius/radiusd.conf. Ahora debemos configurar el archivo /etc/freeradius/sql.conf.

```
#nano /etc/freeradius/sql.conf
```

En el mismo buscamos la sección connect info y la dejamos de la siguiente manera.

```
#connect info
server = "localhost"
login = "radius"
password = "radius"
```

Configuración MySQL

Para configurar la base de datos donde tendremos toda la información que utilizaremos para la autenticación del servidor radius. Debemos realizar los siguientes pasos.

```
#mysql –u root –p root
```

Recordamos que nuestro usuario y contraseña de root es simplemente root.

Ahora nos encontramos dentro del Shell del MySQL, debemos crear la base de datos para luego generar las tablas.

```
CREATE DATABASE radius;
```

Esto nos creo la base de datos radius vacía escribimos *exit* y salimos del Shell de MySQL.

Por suerte el servidor freeradius tiene el archivo SQL que nos genera las tablas necesarias. Para agregar dichas tablas solo debemos hacer lo siguiente.

```
# zcat /usr/share/doc/freeradius/examples/db_mysql.sql.gz | mysql -u root radius –p root

mysql –uroot –proot
USE radius;
SHOW TABLES;
```

A continuación debemos darle los privilegios al usuario radius para que pueda administrar la base de datos radius.

```
# mysql -u root –p

mysql> GRANT ALL PRIVILEGES ON radius.* TO 'radius'@'localhost'
IDENTIFIED BY 'radius';
mysql> FLUSH PRIVILEGES;
mysql> quit;
```

Configuración dialup admin

Utilizamos dicho software para simplificar la administración de los usuarios del servidor radius. Para la configuración realizamos los siguientes pasos.

Realizamos un link simbólico del directorio donde se encuentran la interfase Web del dialup admin freeradius a nuestro directorio raíz del servidor Web

```
#ln –s /usr/share/freeradius-diaupadmin/htdocs /var/www/radconfig
```

A continuación debemos agregarle algunas otras tablas a nuestra base de datos radius para la utilización del soft dialup admin. Para ellos realizamos l o siguiente:

```
  # mysql –uradius –pradius radius < /usr/share/freeradius-
dialupdamin/sql/baduser.sql
    # mysql -uradius –radius radius < /usr/share/freeradius-
dialupdamin/sql mtotacct.sql
    # mysql -uradius –pradius radius < /usr/share/freeradius-
dialupdamin/sql totacct.sql
    # mysql –uradius –pradius radius <  /usr/share/freeradius-
dialupdamin/sql userinfo.sql
```

Finalmente realizamos la ultima configuración del archive /etc/freeradius-dialupadmin/admin.conf

```
#nano /etc/freeradius-dialupadmin/admin.conf
```

Buscamos General_encryption_mode y lo cambiamos a clear

```
#antes
general_encryption_method = md5

# Después
general_encryption_method = clear
```

Buscamos sql_username, sql_password, sql_debug. Y los modificamos de la siguiente manera.

```
sql_username:  radius
sql_password: radius
sql_debug = false
```

Para finalizar reiniciamos nuestro radius server.

```
#/etc/init.d/freeradius restart
```

A continuación debemos crear algún nuevo usuario para que nuestro servidor radius nos autentique. Para ello en nuestro navegador Web redirigimos a la dirección del servidor radius de la siguiente manera:

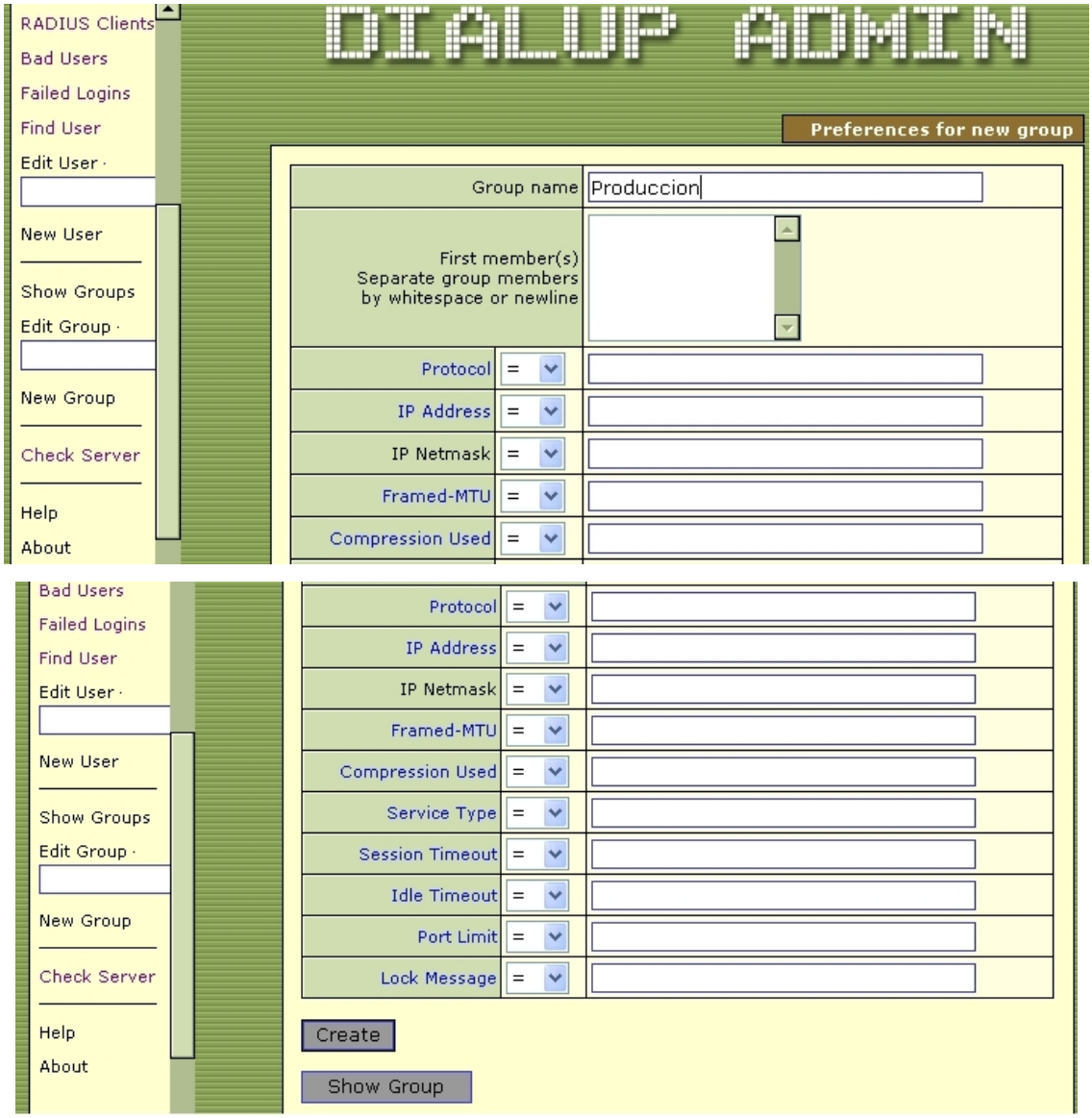
http://192.168.1.3/rad_config

Esto nos muestra la página de administración de usuarios.

En nuestra ventana de configuración de usuarios debemos hacer clic en nuestro menú en la opción *New Gorup*

En dicha ventana la configuramos de la siguiente manera:

Group Name: Producción

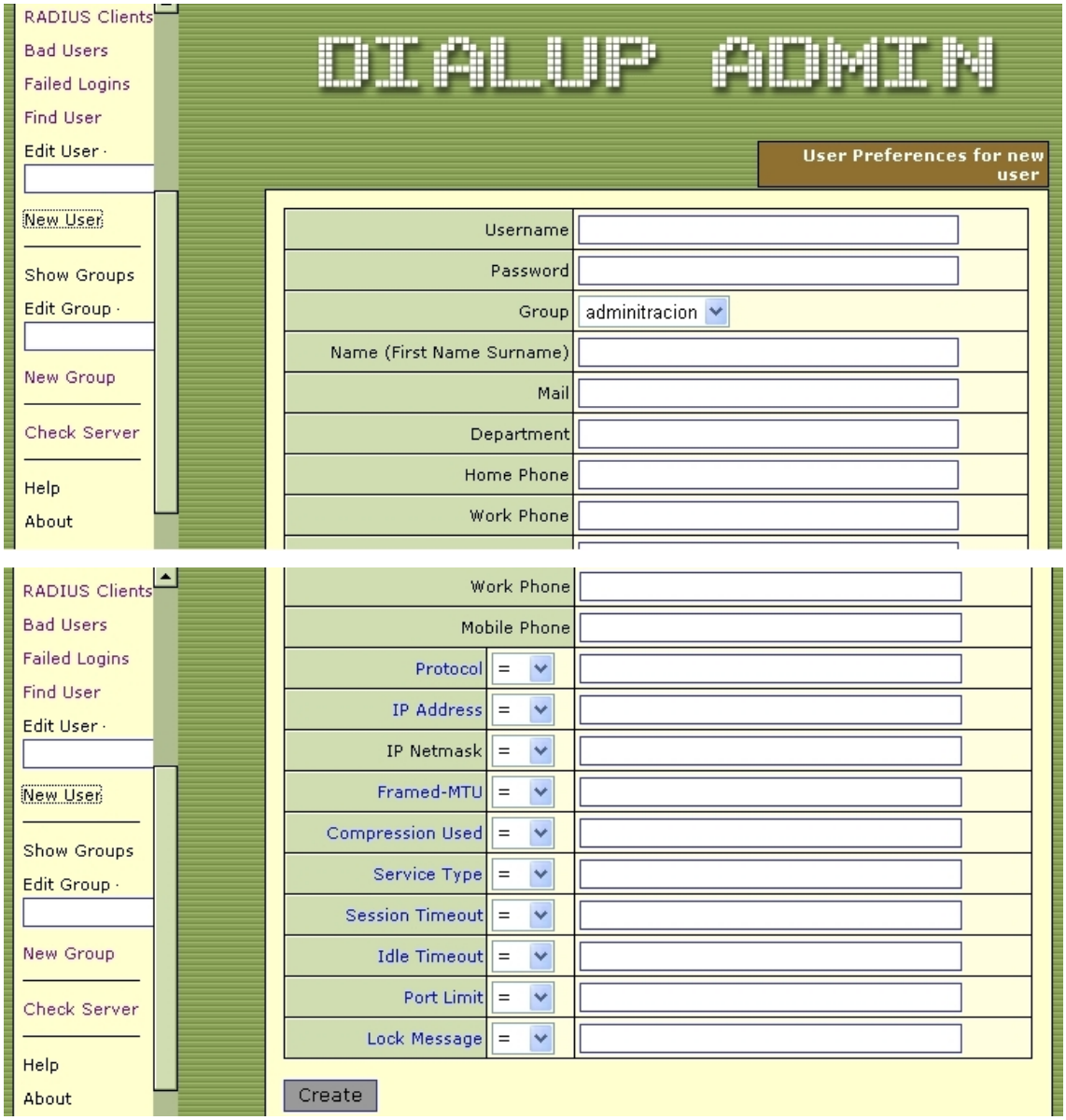


A continuación nos dirigimos a la menú a la opción *New User* allí la configuramos de la siguiente manera.

Username: gustavo

Password: gustavo

Group: Production



Final mente ya tenemos nuestro grupo y usuario creado. A continuación debemos configurar el Mikrotik para que nos autentique los usuarios PPPoE contra el servidor radius.

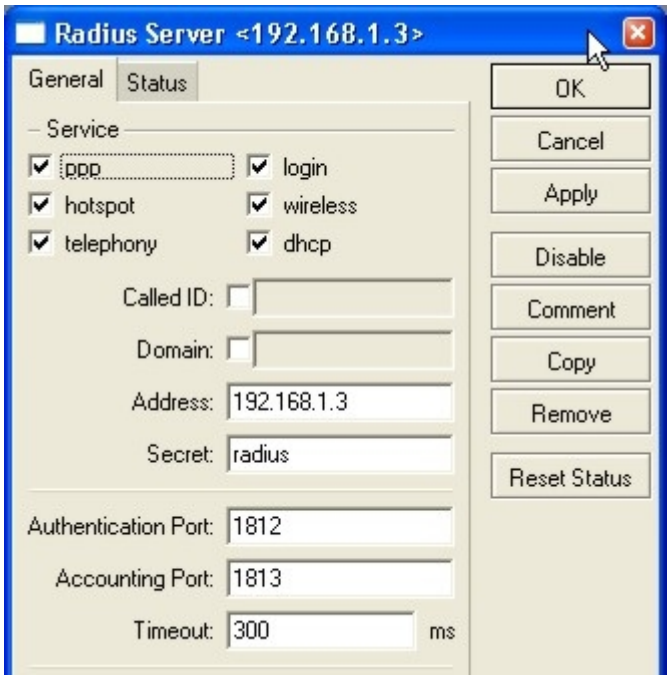
Logueados con winbox al Mikrotik nos dirigimos al menú *RADIUS*. En la nueva ventana hacemos clic en el icono (+). Configuramos a nuestro servidor radius de la siguiente manera:

Pestaña General:

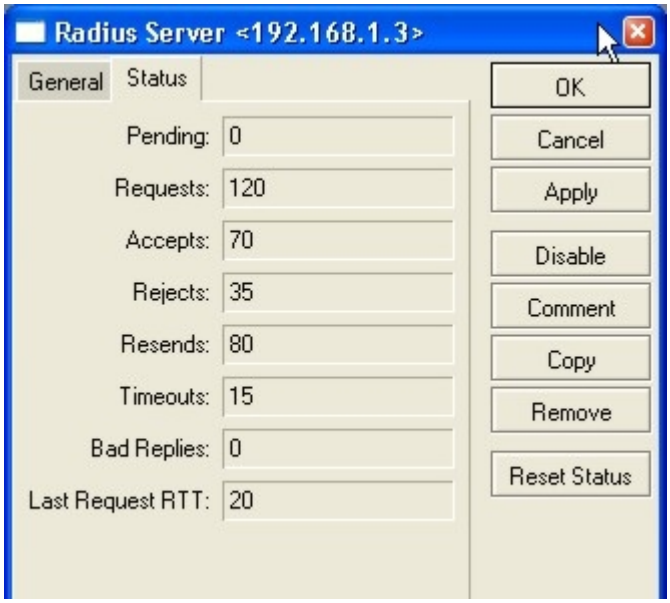
- Ppp, login, wireless, hotspot, telephony, dhcp (seleccionados)
- Address: 192.168.1.3

- Secret: radius
- Authentication port :1812
- Accounting Port: 1813
- Time out : 300

Antes de hacer clic en *Ok* debemos hacer clic en *ENABLE*



En la pestaña Status podemos ver mucha información valiosa acerca de los intentos de logueo respecto a pendientes, pedidos, aceptados, rechazados, etc.



Luego vamos al menú *PPP*. En la nueva ventana hacemos clic sobre la pestaña Secret. Luego clic en el botón *AAA*. Allí la configuramos:

- Use radius: Seleccionado
- Accounting: Seleccionado

Finalmente ya hemos terminado de configura nuestro servidor radius, ahora simplemente queda configurar la conexión del cliente que se realiza de la siguiente manera.

Configuración servidor - cliente Jabber

Servidor Jabber

Debido a que constantemente los empleados pierden tiempo valioso de trabajo por utilizar el servicio de mensajería MSN Messenger o Yahoo Messenger entre otros. La empresa tomo la decisión de bloquear dichos servicio e instalar un servidor de mensajería privada para los empleados de la empresa y clientes.

La instalación del servidor Jabber la hacemos en el servidor nuestro de la empresa que esta en la dirección de ip 192.168.1.2. Para instalarlo y configurarlos debemos realizar los siguientes pasos.

Desde la consola del servidor logueado como root escribimos el siguiente comando.

```
#apt-get install jabber
```

Automáticamente se baja los paquetes necesarios para la instalación. Con el servidor funcionando. Debemos detenerlo para comenzar la simple configuración.

```
# /etc/init.d/jabber stop
```

Con la confirmación de que el servidor esta detenido. Editamos el archivo de configuración del servidor */etc/jabber/jabber.cfg*. Al mencionado archivo le agregamos la siguiente línea.

```
JABBER_HOSTNAME=royaltech.com.ar
```

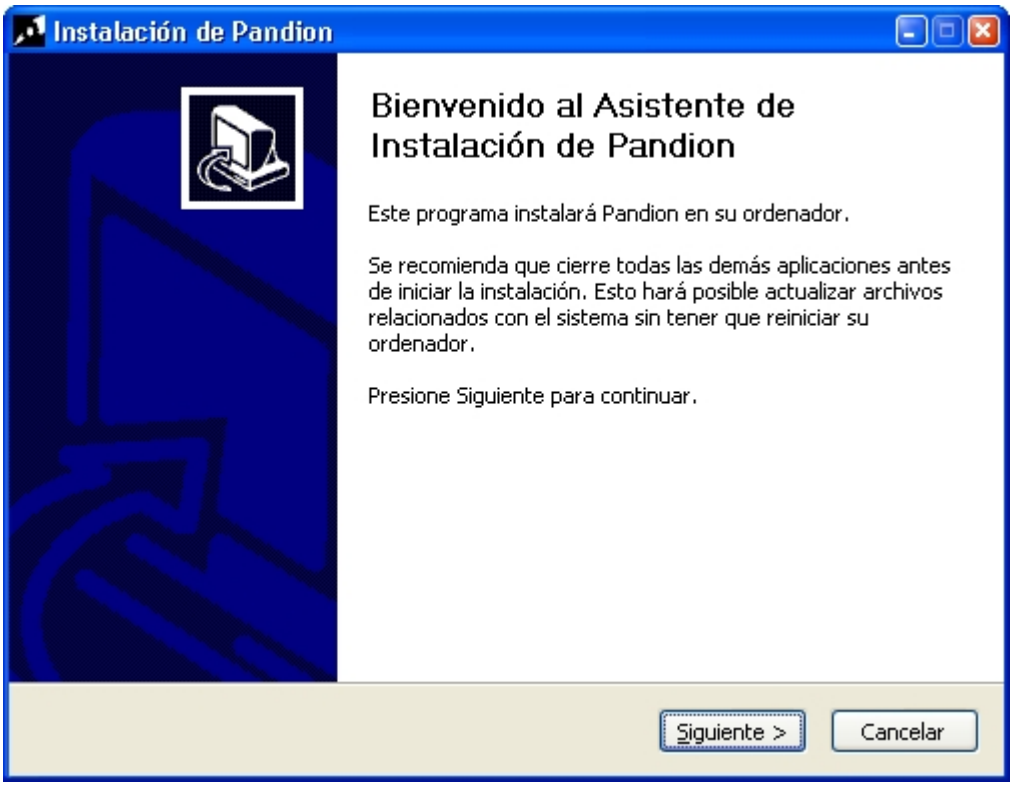
Con nuestro servidor Jabber instalado y configurado, lo que nos resta de la instalación simplemente es reiniciar el servidor de mensajería. Para ello desde la consola:

```
# /etc/init.d/jabber start
```

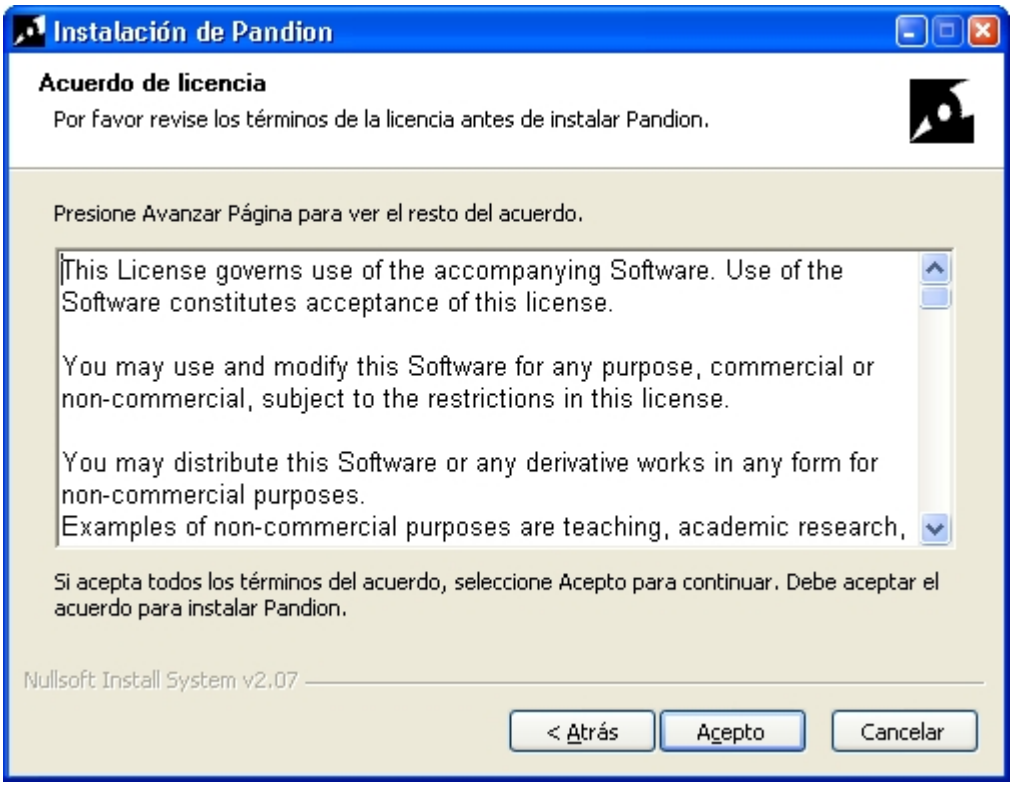
Cliente Jabber

Para la instalación del cliente Jabber se ah elegido el cliente Pandion. Esto es debido a la facilidad de utilización que posee y la versatilidad del mismo. Para la instalación seguimos los siguientes pasos:

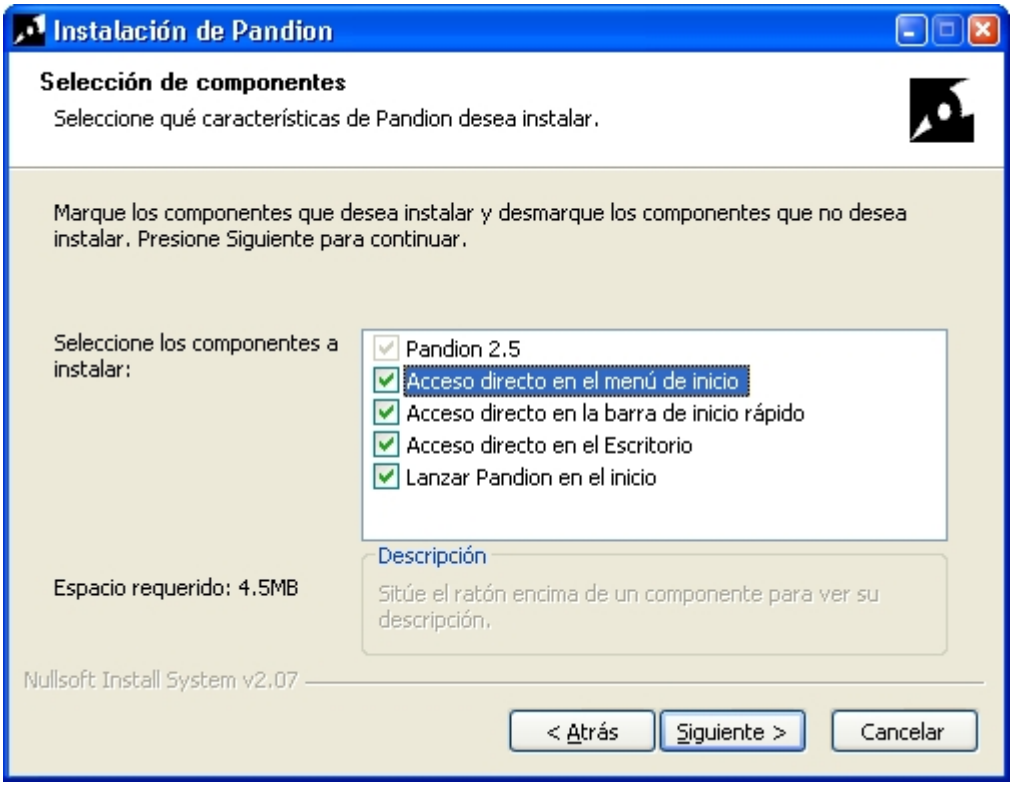
- Nos dirigimos al site http://www.pandion.be/download/ y descargamos el producto.
- Ejecutamos el instalador Pandion-2.5.exe
- Hacemos Clic En siguiente



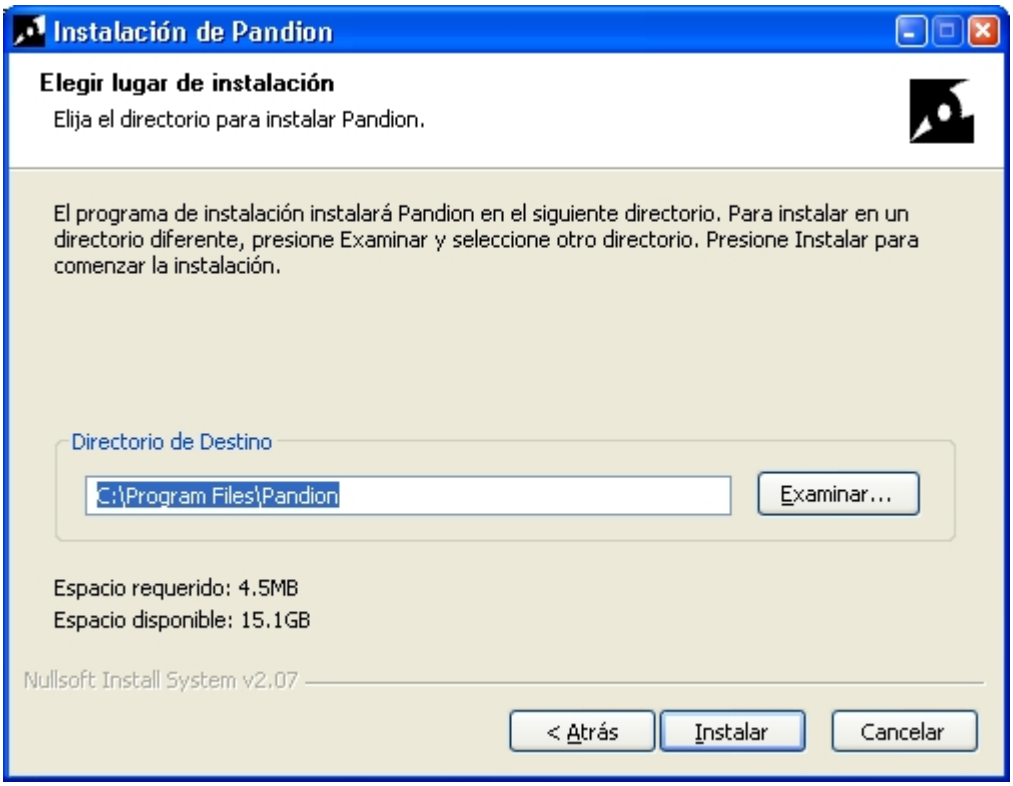
Aceptamos la licencia de pandion



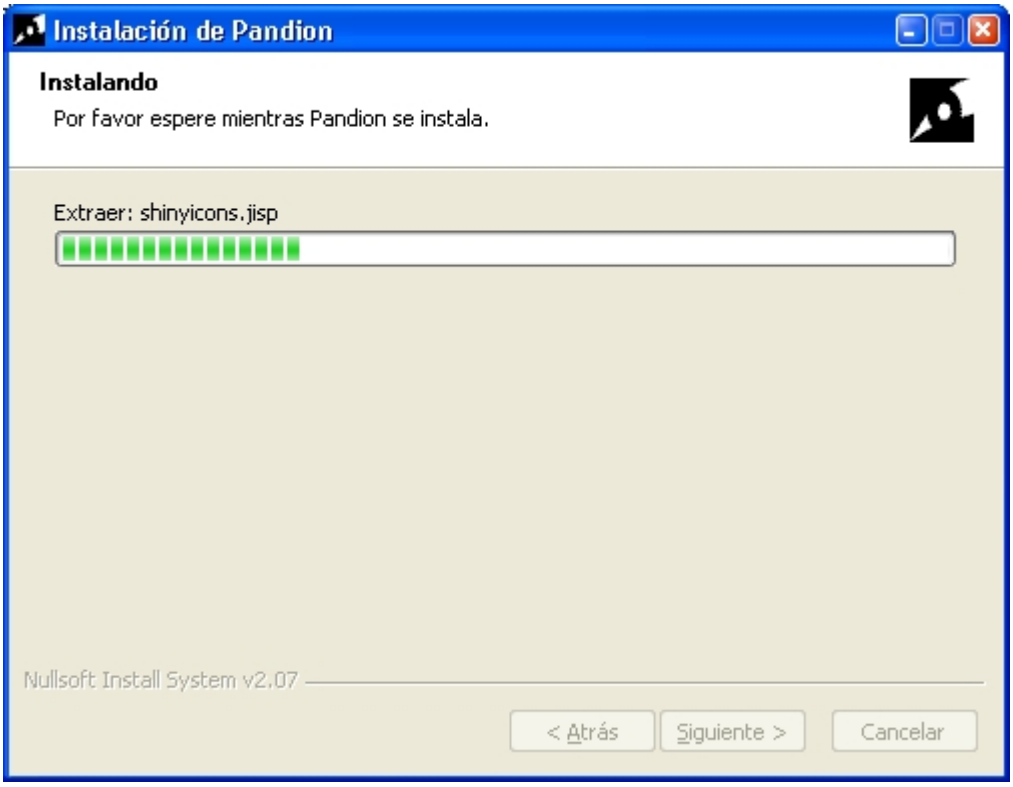
Dejamos Seleccionados todos los componentes y hacemos clic en Siguiente



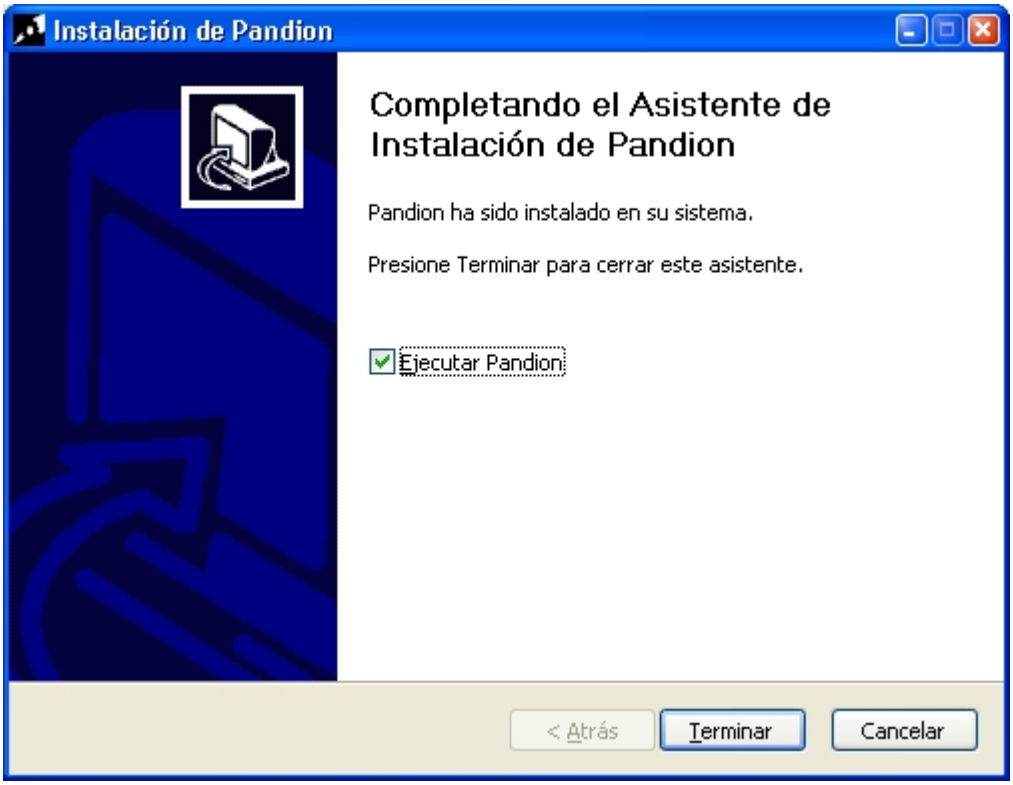
Dejamos el lugar de instalación tal cual como nos lo propone el software y hacemos clic en siguiente.



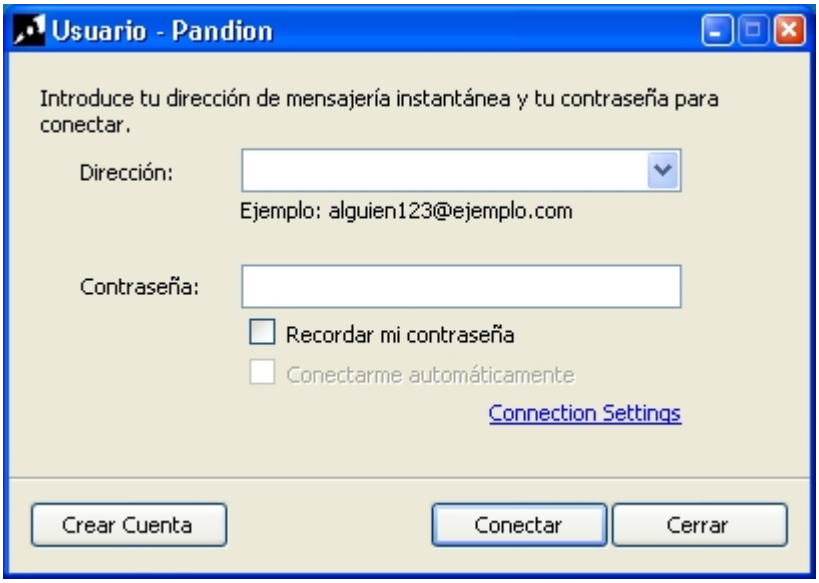
Automáticamente comenzara la instalación, solo hay que aguardar algunos segundos para que finalice la misma.



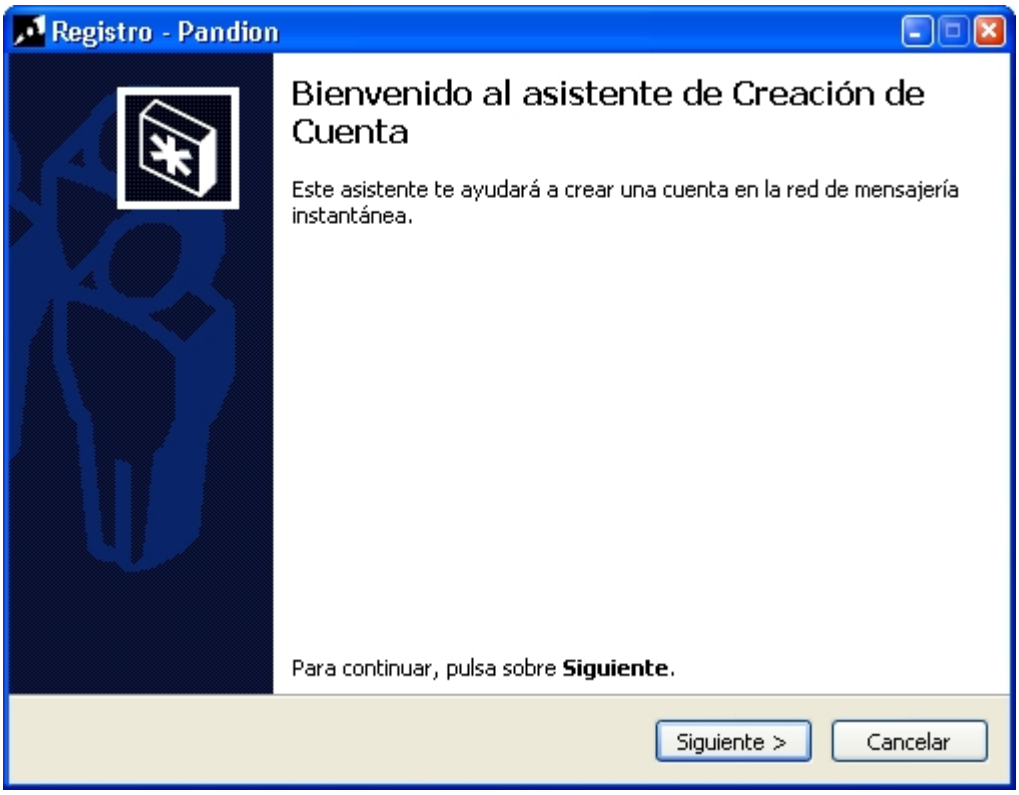
Dejamos seleccionado la opción Ejecutar Pandion y hacemos Clic en Terminar. Esto hará que el software se ejecute automáticamente después de finalizar la instalación.



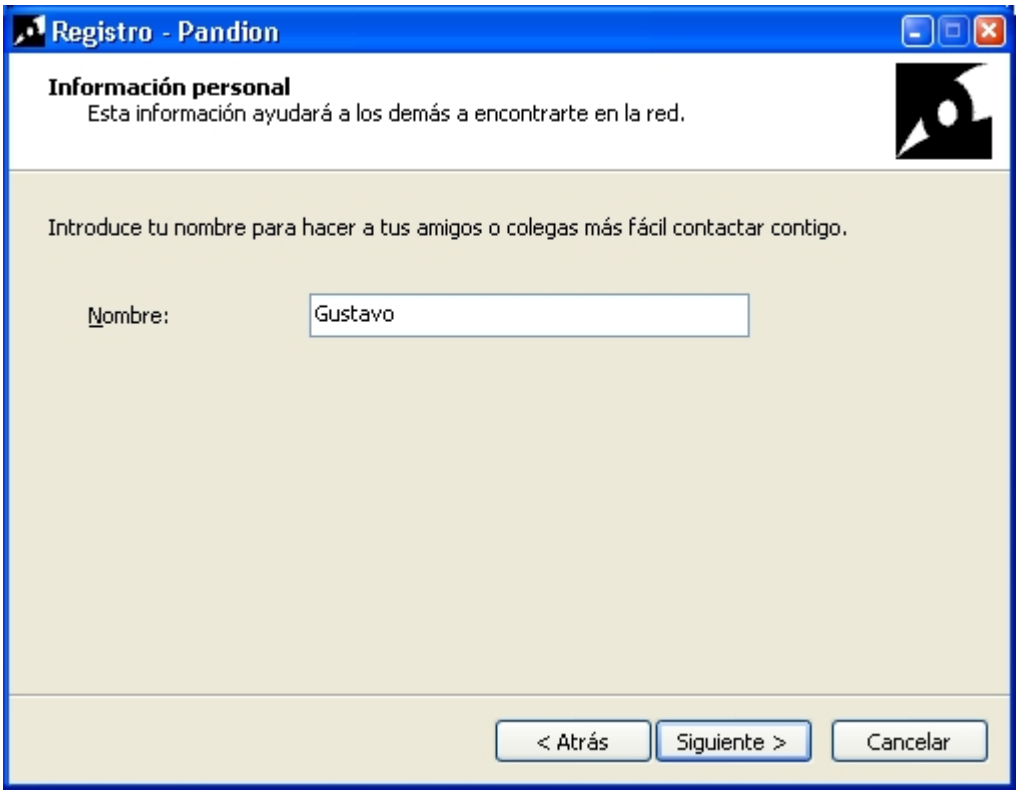
Se nos abre la ventana de configuración de conexión. En la misma Hacemos clic en el botón *CREAR CUENTA.*



Se nos abre una ventana de asistente de cuentas. Hacemos clic en siguiente.

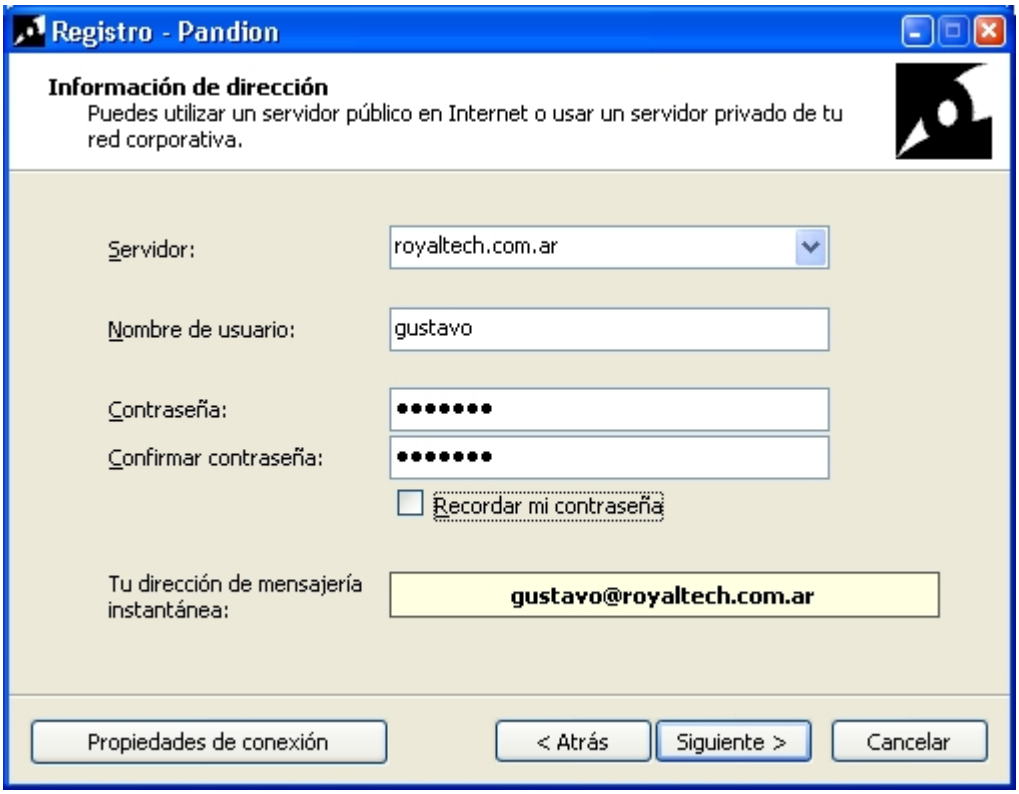


Ingresamos el nombre con el que queremos que nos reconozcan nuestros colegas. Para nuestro caso Gustavo. Luego hacemos clic en siguiente.

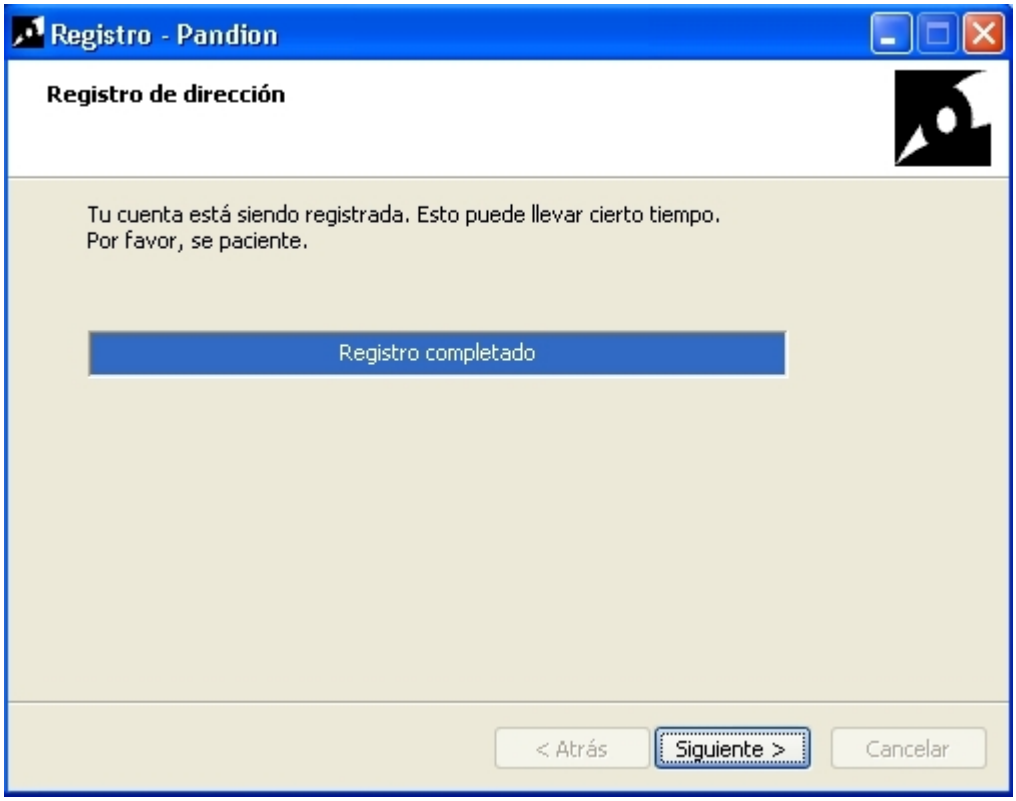


En la ventana de dirección la configuramos de la siguiente manera.

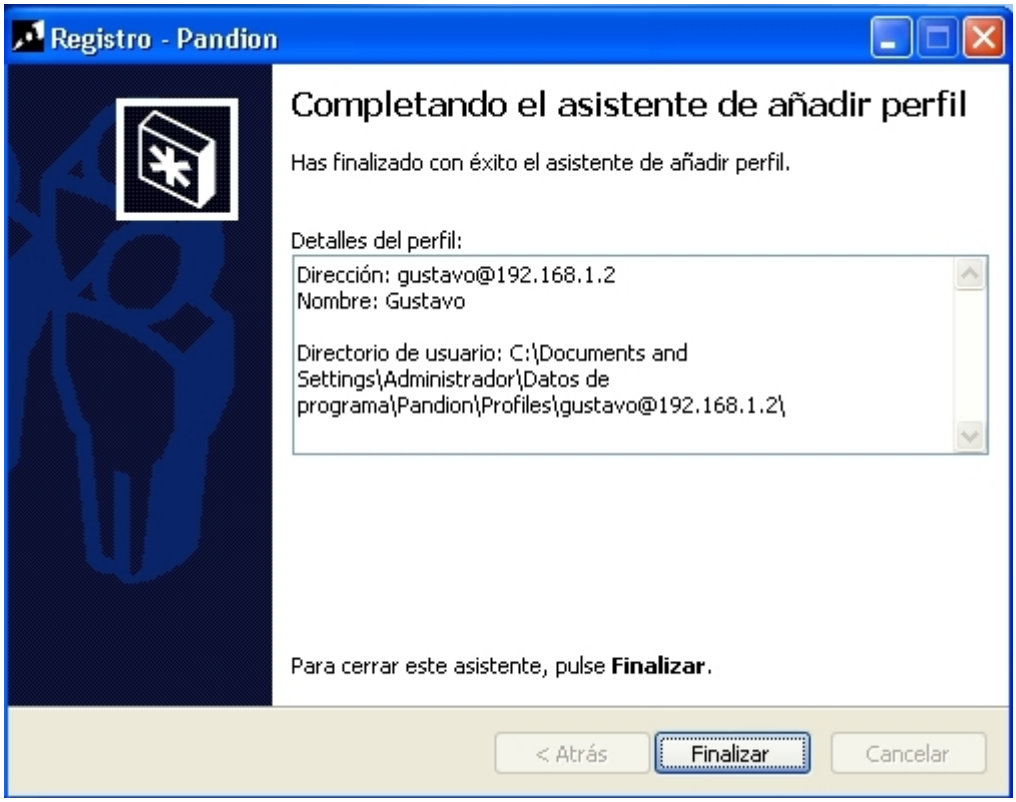
- Servidor: royaltech.com.ar
- Nombre de usuario: Gustavo
- Contraseña: Gustavo
- Confirmar Contraseña: Gustavo
- Recodar contraseña= Deseleccionar



A continuaón comienza la registración de nuestro nuevo usuario en nuestro servidor. Luego hacemos clic en siguiente.



Hacemos clic en finalizar



El Cliente ya estará corriendo y conectado al servidor, solo falta agregar contactos. Para ello Haga clic en Añadir contacto.-

Sniffing de Paquetes

Siempre es bueno tener una herramienta de análisis de paquetes para saber que es lo que esta ocurriendo en nuestra red. Para ello utilizaremos la aplicación ntop y Wireshark conjuntamente con la utilidad de sniffing de paquetes que posee el mikrotik.

Instalación Ntop

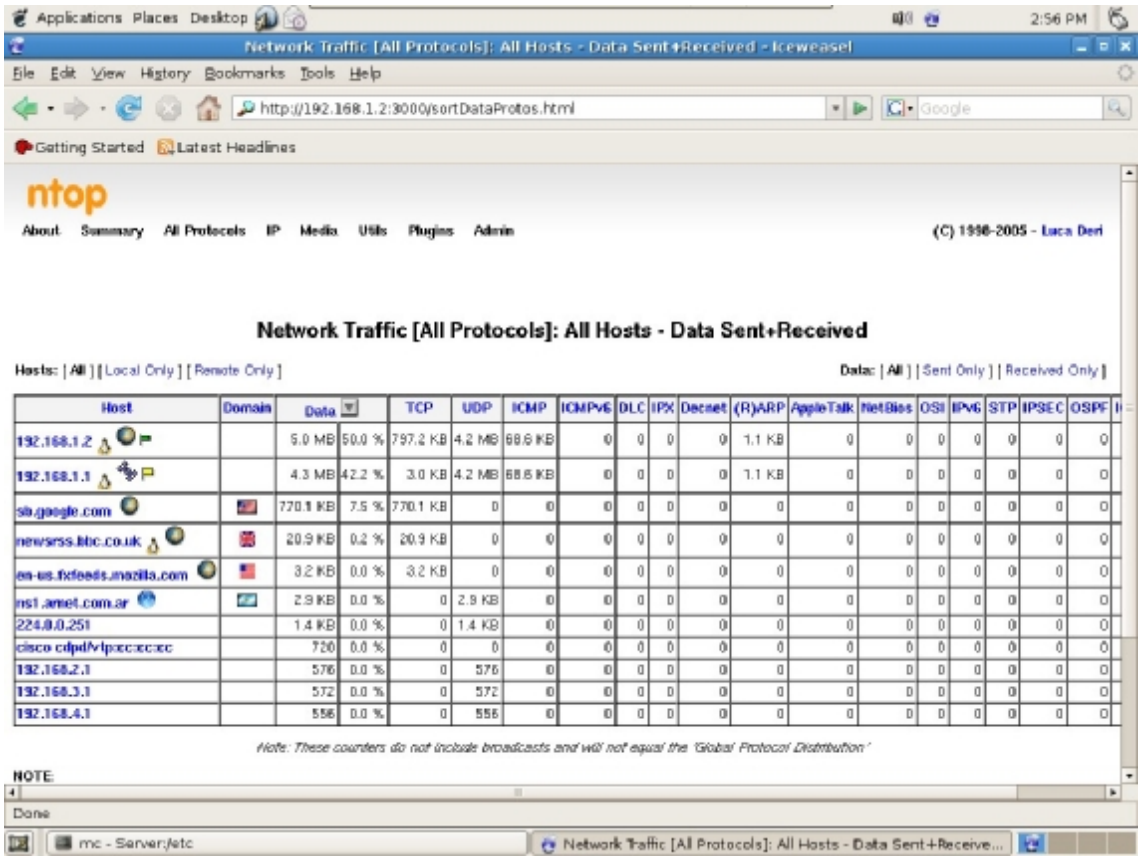
La insolación simplemente consta de estar logueado como root en nuestra consola de debian y tipeamos el siguiente comando

```
#apt-get install ntop
```

Este comando ya nos habrá instalado el ntop en nuestro servidor. Para acceder a la página web para ver el análisis de paquetes realizado por ntop, simplemente debemos redireccionar a nuestro explorador de Internet a la dirección de ip:

http://192.168.1.2:3000

El programa stop nos mostrará con gran cantidad de detalles toda la información que esta circulando por nuestra red. Una de las clásicas vistas del ntop puede ser la siguiente.

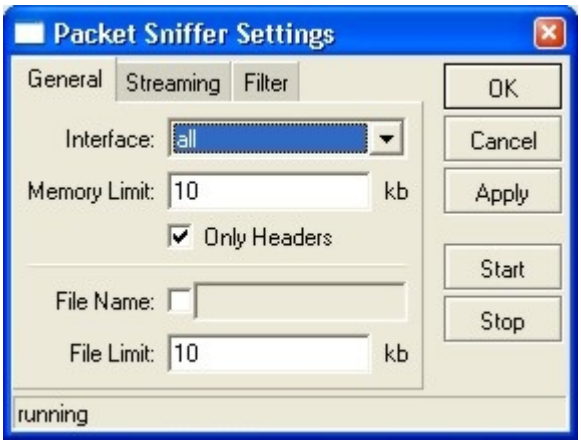


A continuación hay que configurar el mikrotik para que nos espeje todo el tráfico a nuestro ntop, para ello vamos al menú *TOOLS / PACKET SNIFFER*. En la nueva ventana hacemos clic en el botón *SETTINGS* y comienza nuestra configuración.

Pestaña General:

- Interface: all
- Memory Limit 10kb

- Only Headers: (seleccionado)
- File Limit: 10

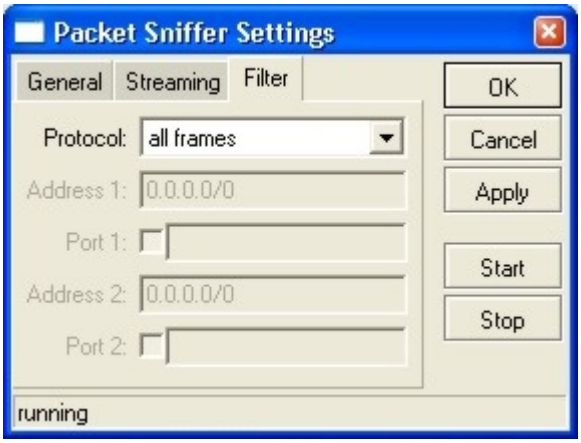


Pestaña Streaming:

- Streaming Enable: (Seleccionado)
- Server: 192.168.1.2
- Filter Stream: (Seleccionado)

Pestaña Filter:

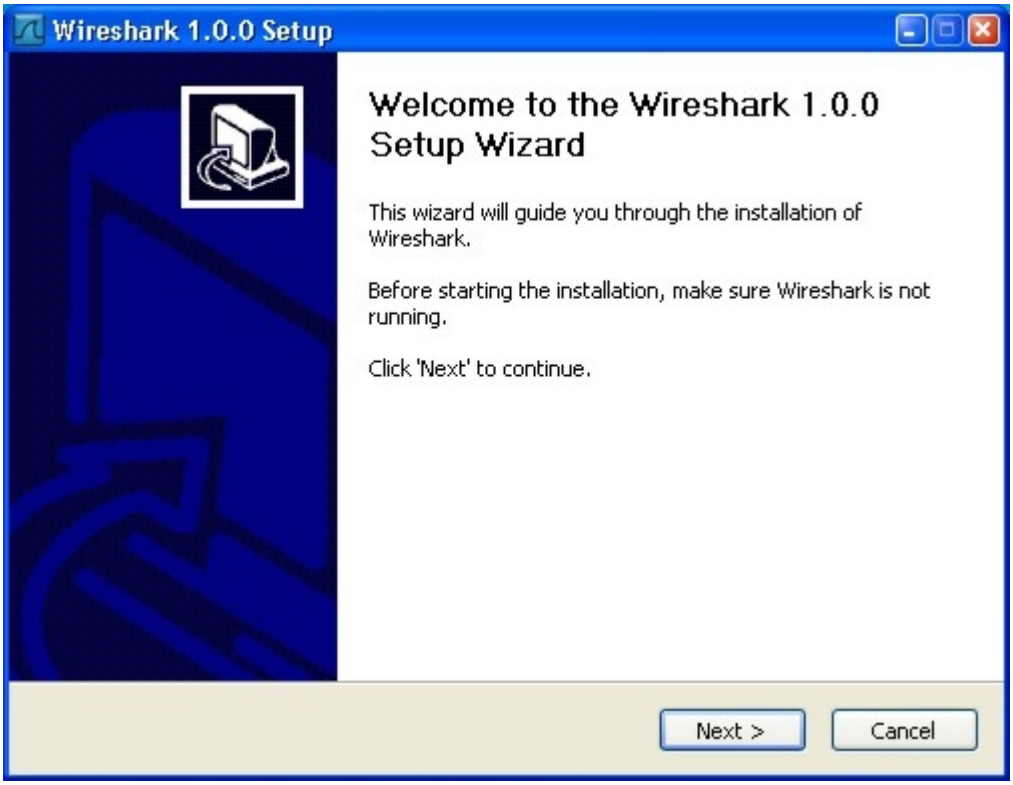
- Protocol: all frames.



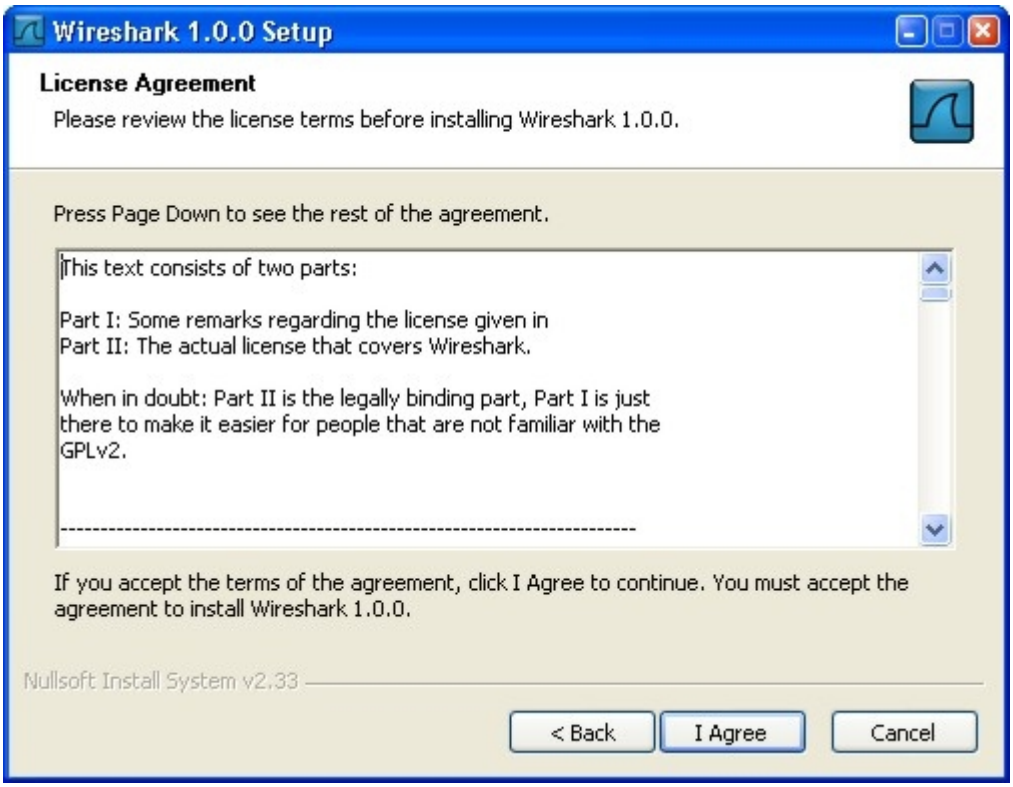
Instalación Wireshark

Para el análisis mas fino de los paquetes se utilizará la aplicación Wireshark la misma tiene muchas funcionalidades que el ntop no posee. Para instalar la misma aplicación en un cliente Windows debemos Sergui los siguientes pasos.

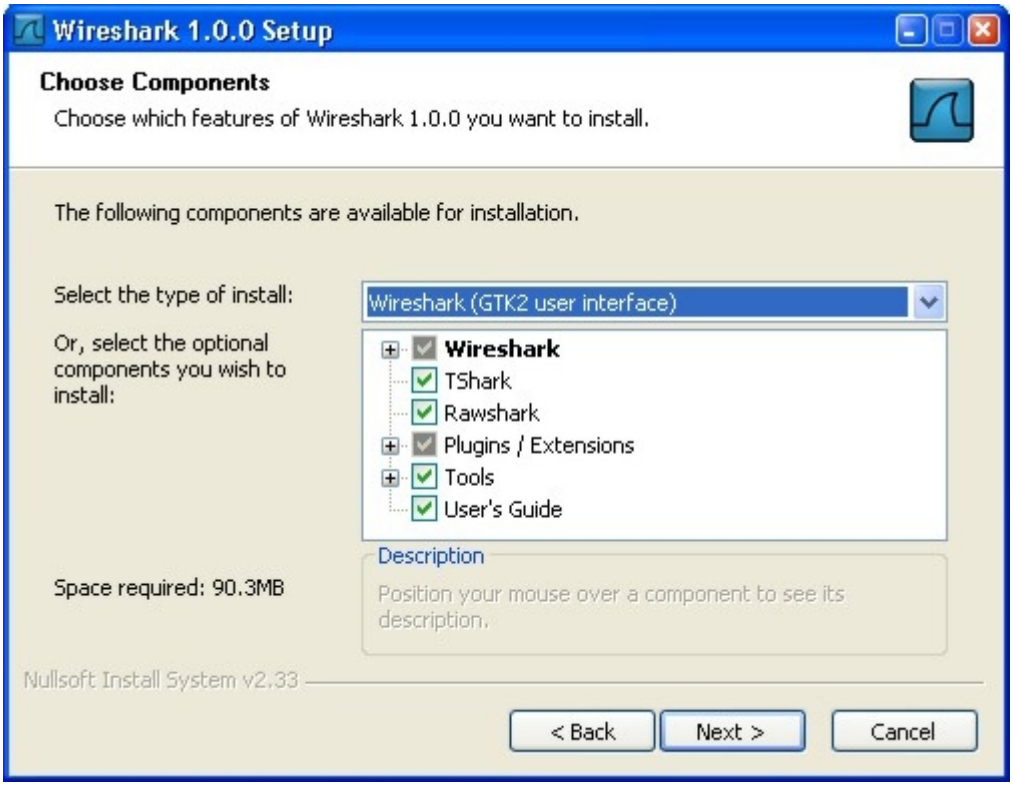
Ejecutamos el instalador y en la ventana de bienvenida hacemos clic en siguiente.



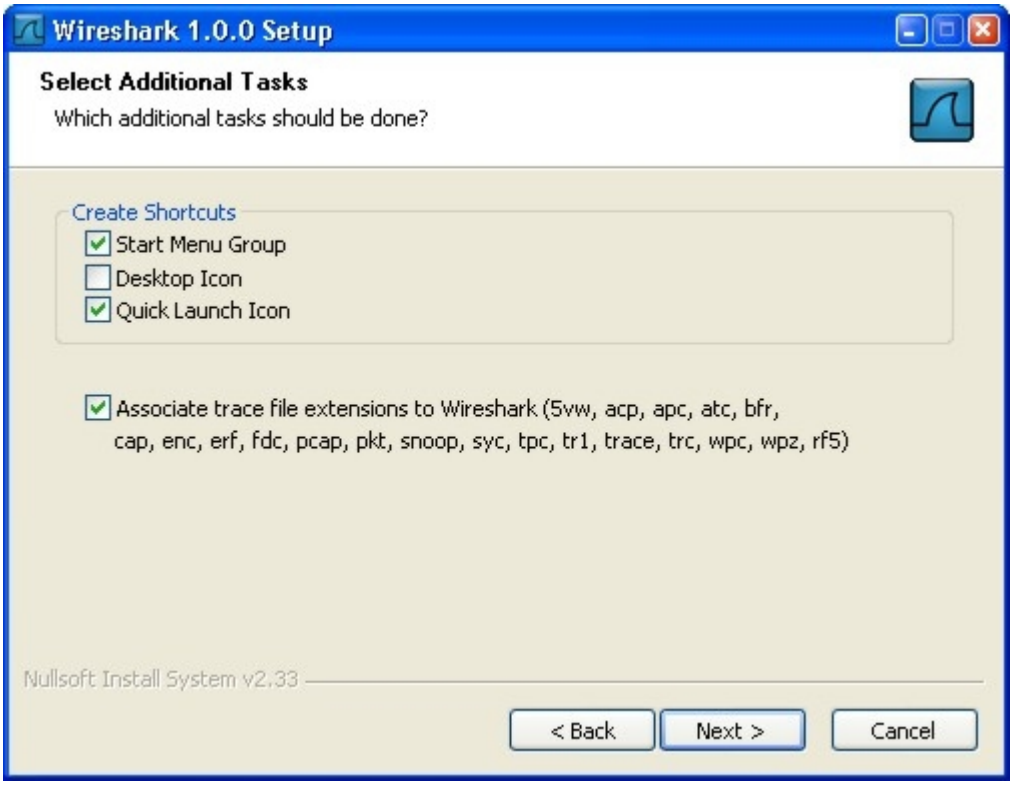
Aceptamos las condiciones del licenciamiento



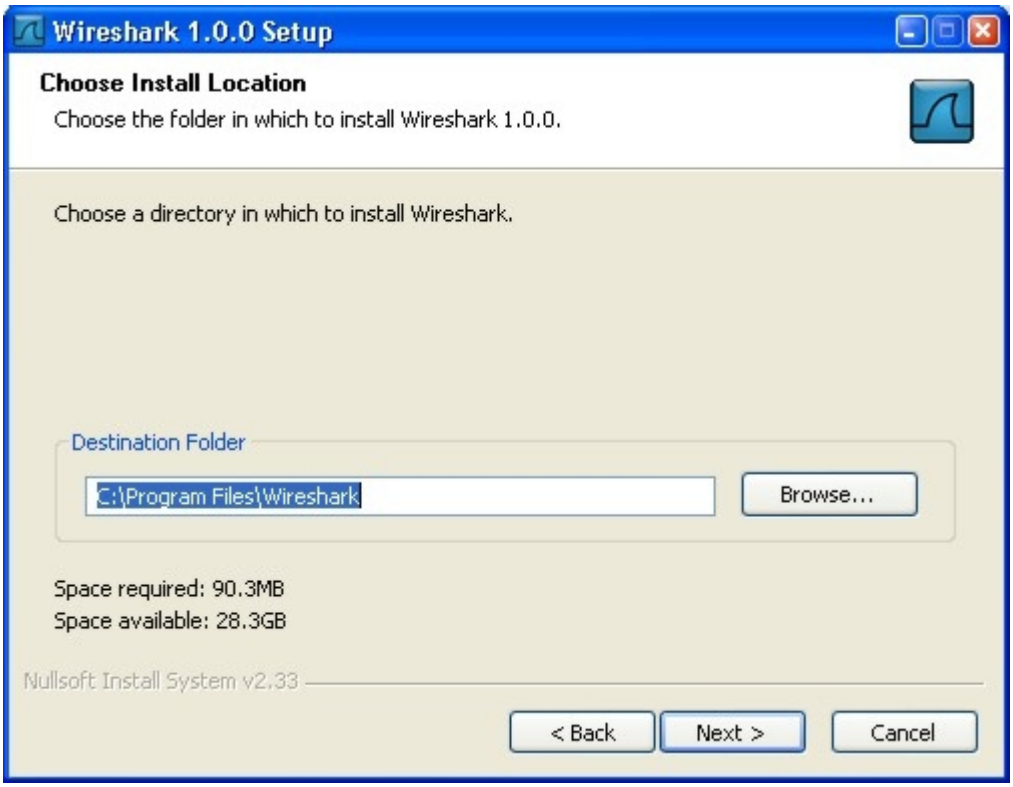
Dejamos los componentes por default que viene con la instalación y hacemos clic en siguiente.



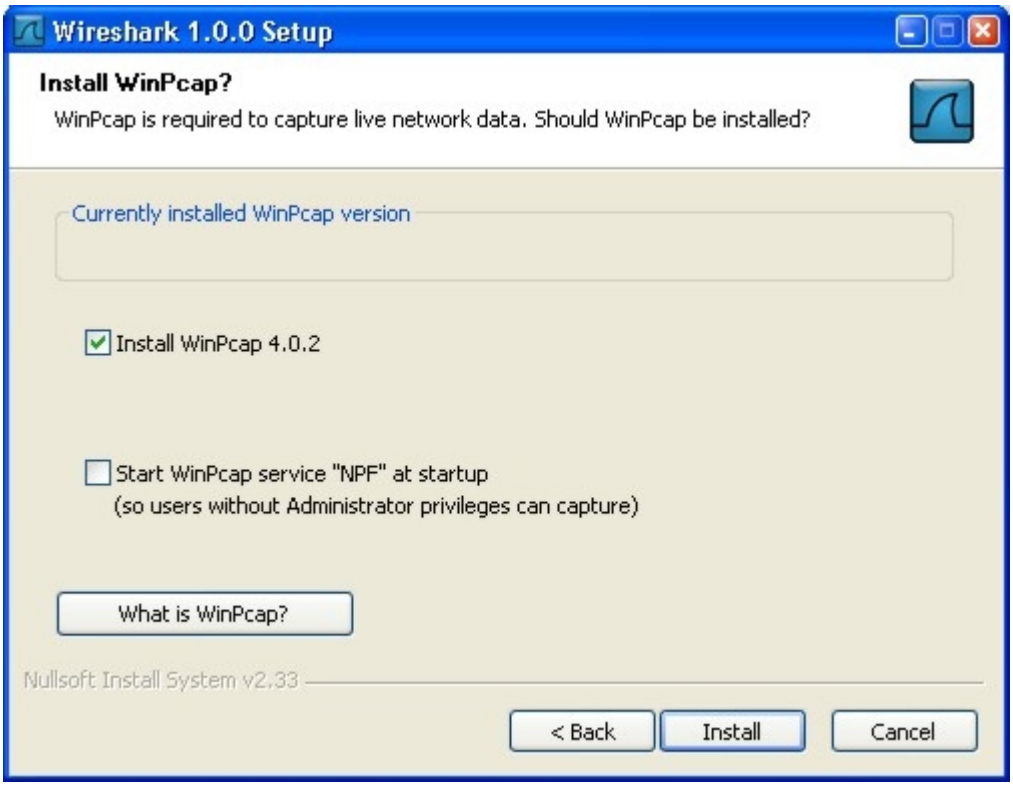
Hacemos clic en siguiente dejando toda la configuración por default.



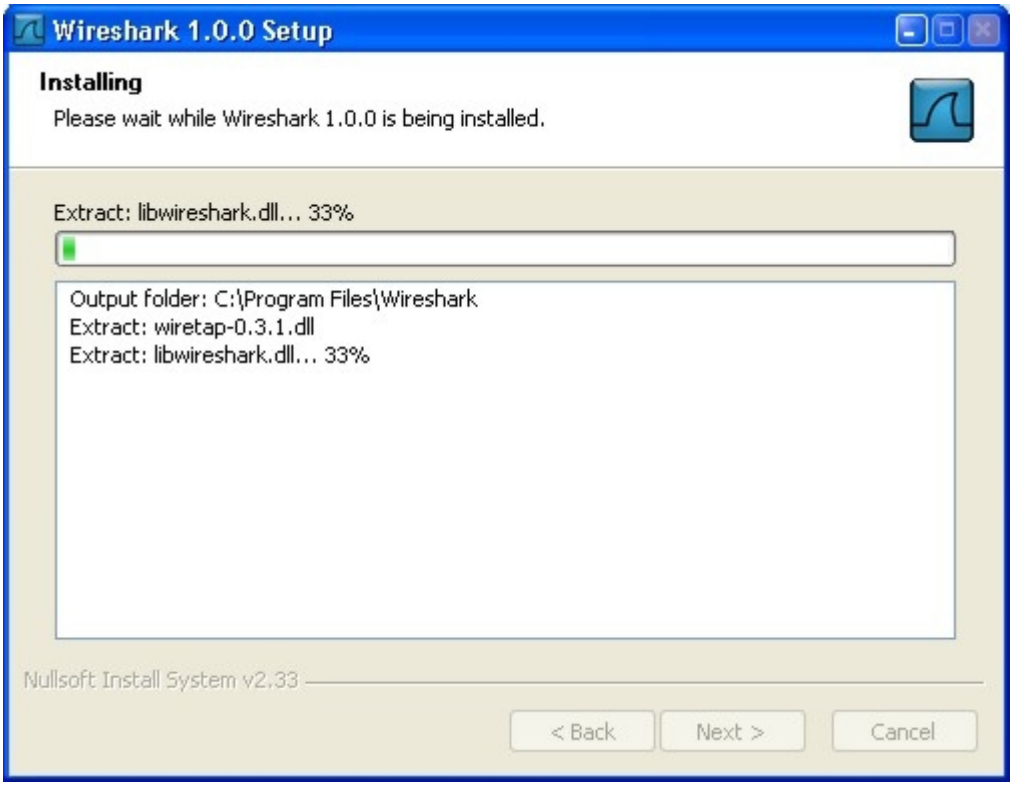
Hacemos clic en siguiente.



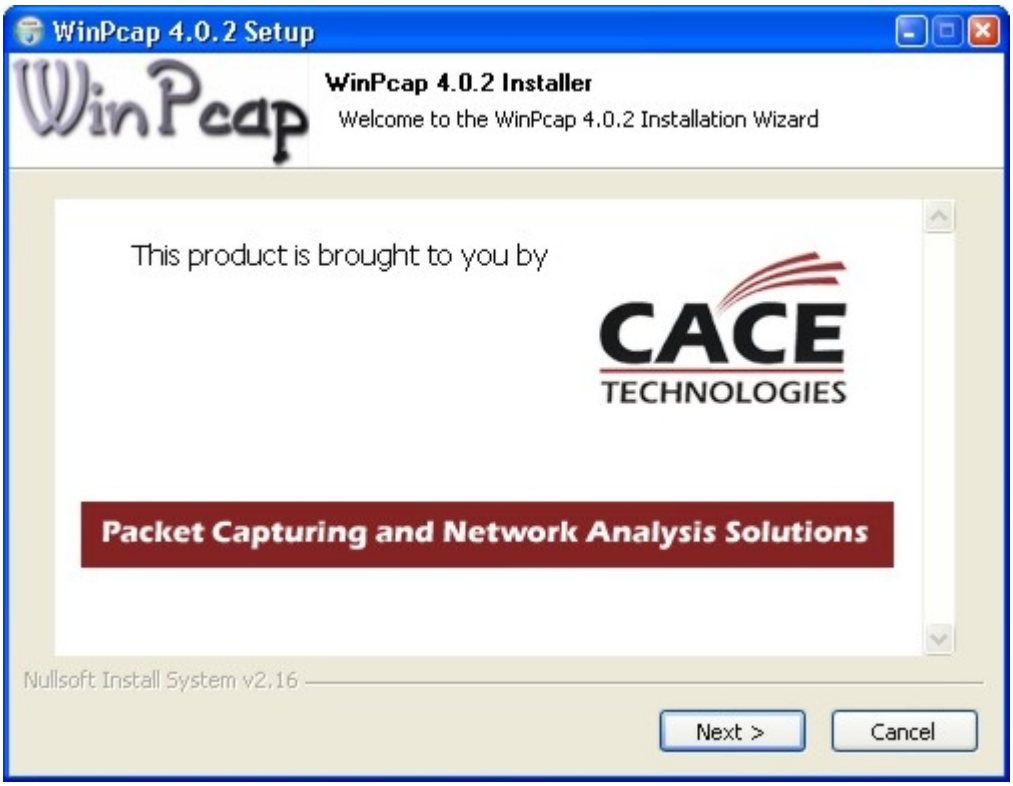
Clic en siguiente seleccionando install wincap



Comienza la instalación del software.

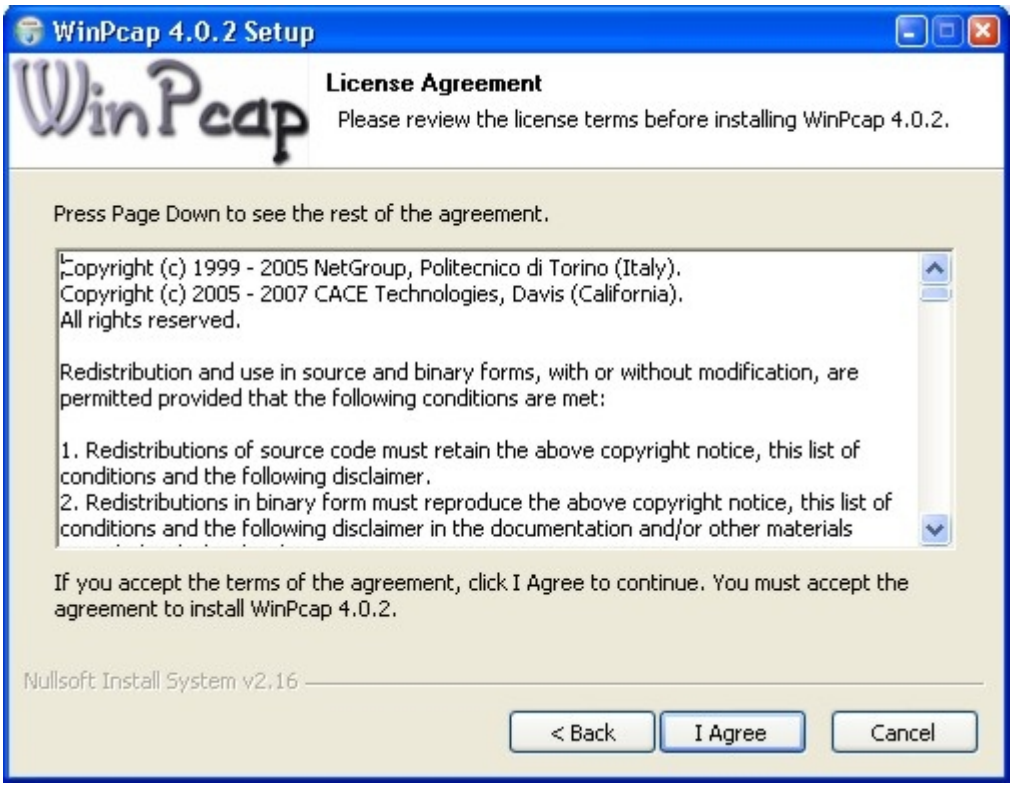


Luego nos aparece la ventana de instalación del wincap. Hacemos clic en siguiente.

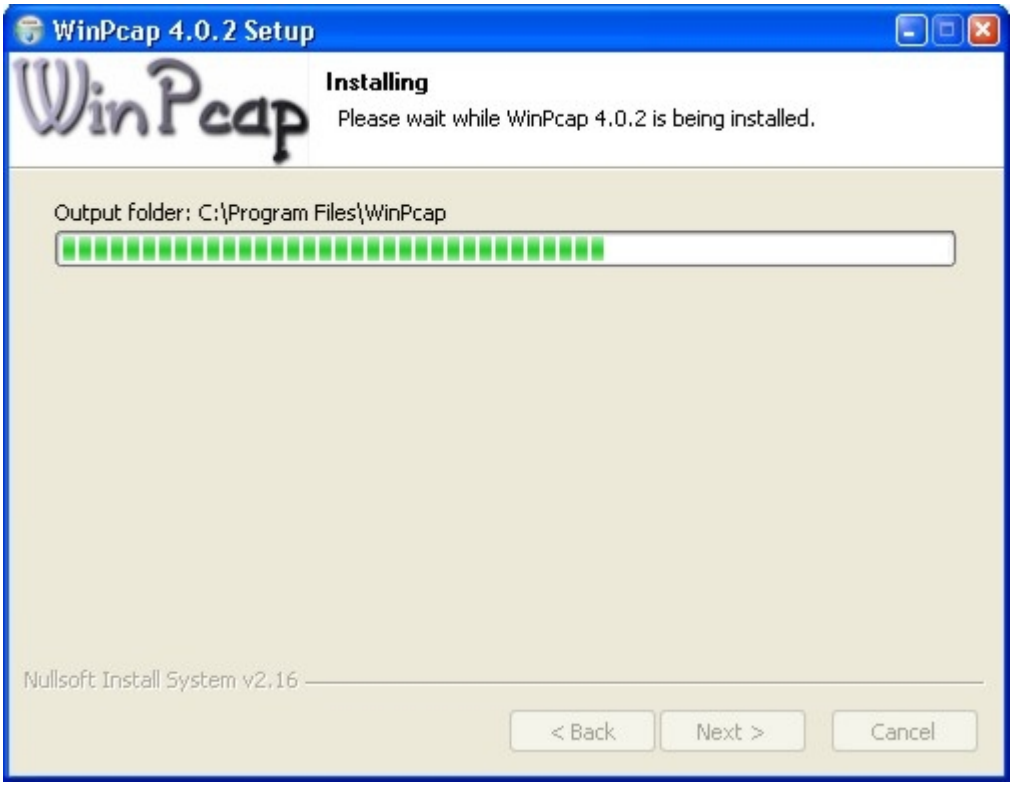


Clic en siguiente.

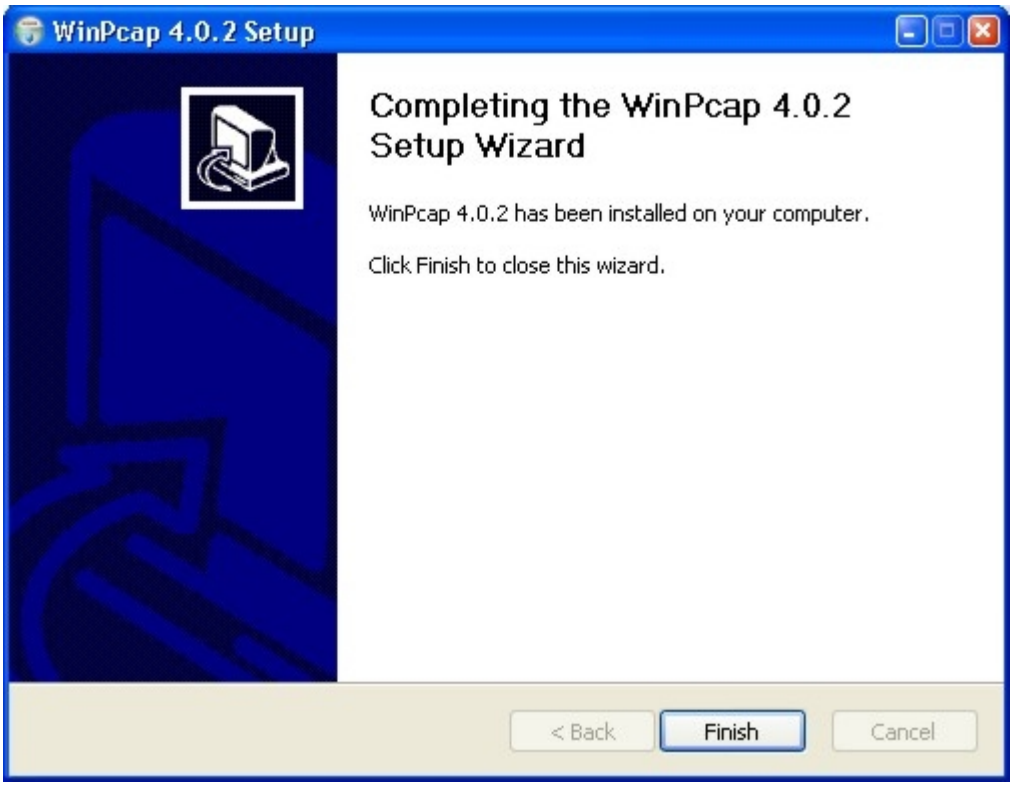
Aceptamos el contrato



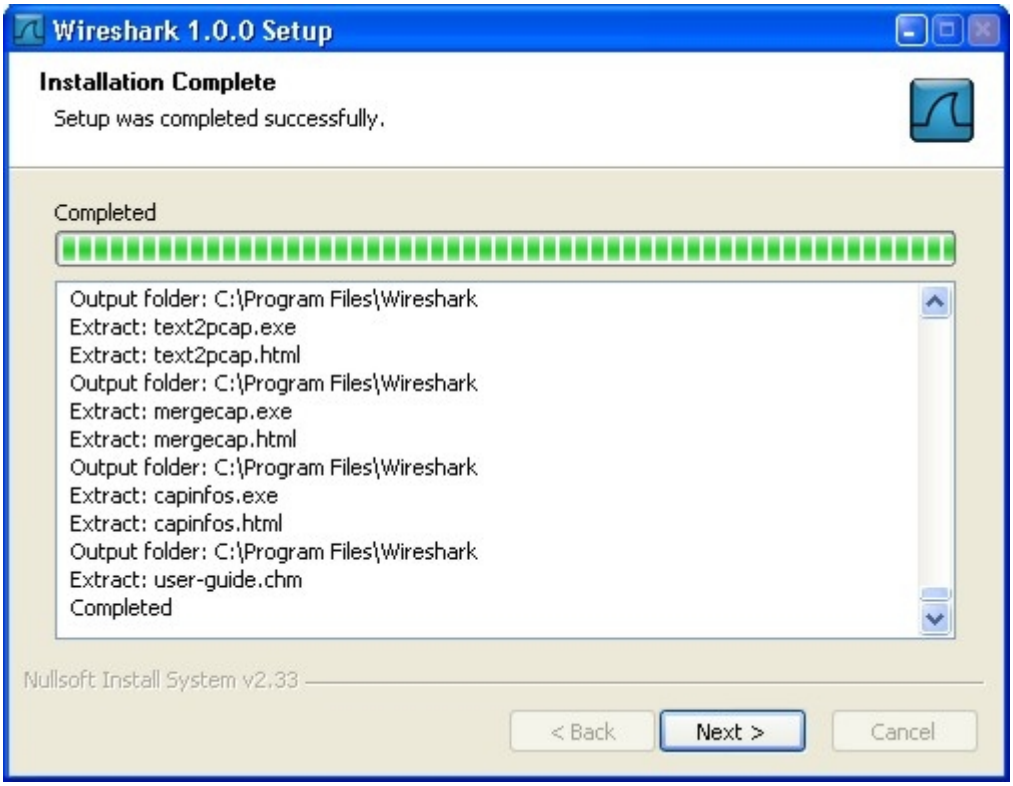
Comienza la instalación del wincap.



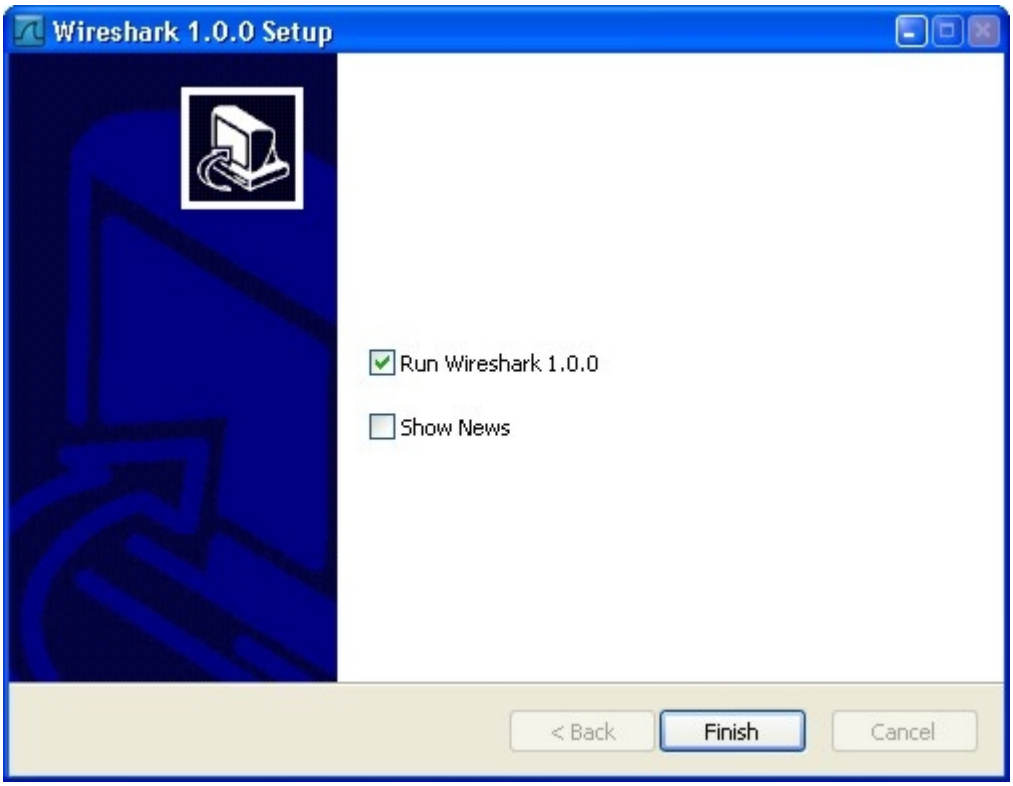
En la última ventana hacemos clic en finalizar.



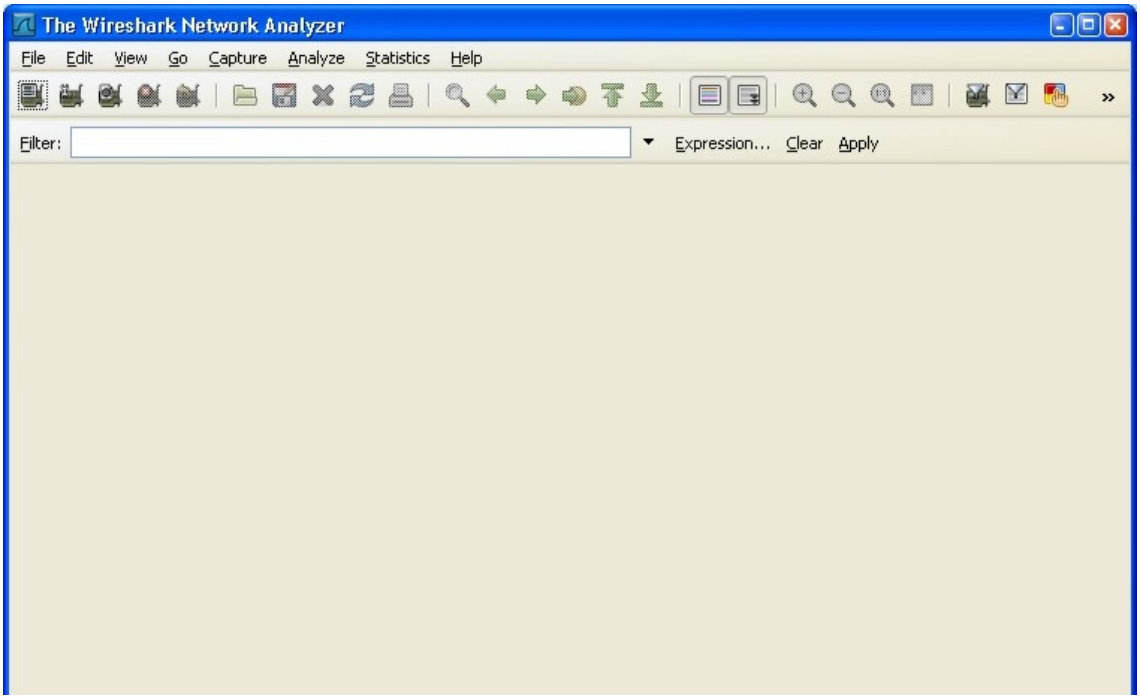
Finalizada la instalación del wireshark hacemos clic en siguiente.



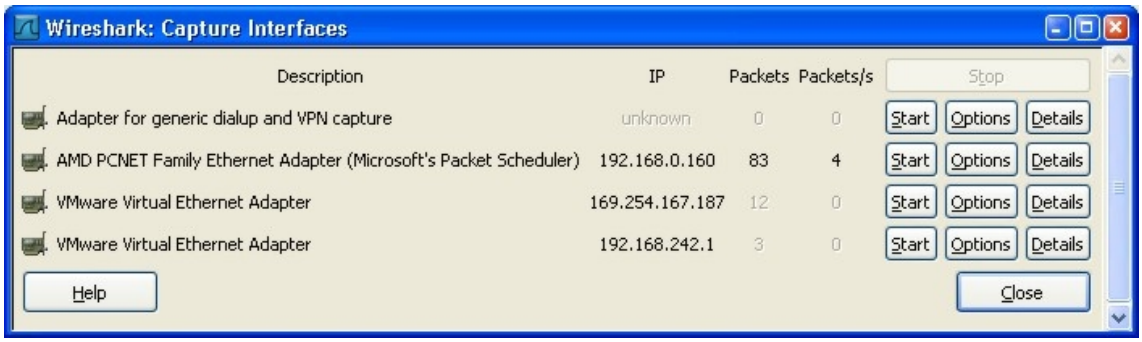
En la última ventana de instalación de wireshark seleccionamos run wireshark y hacemos clic en finalizar.



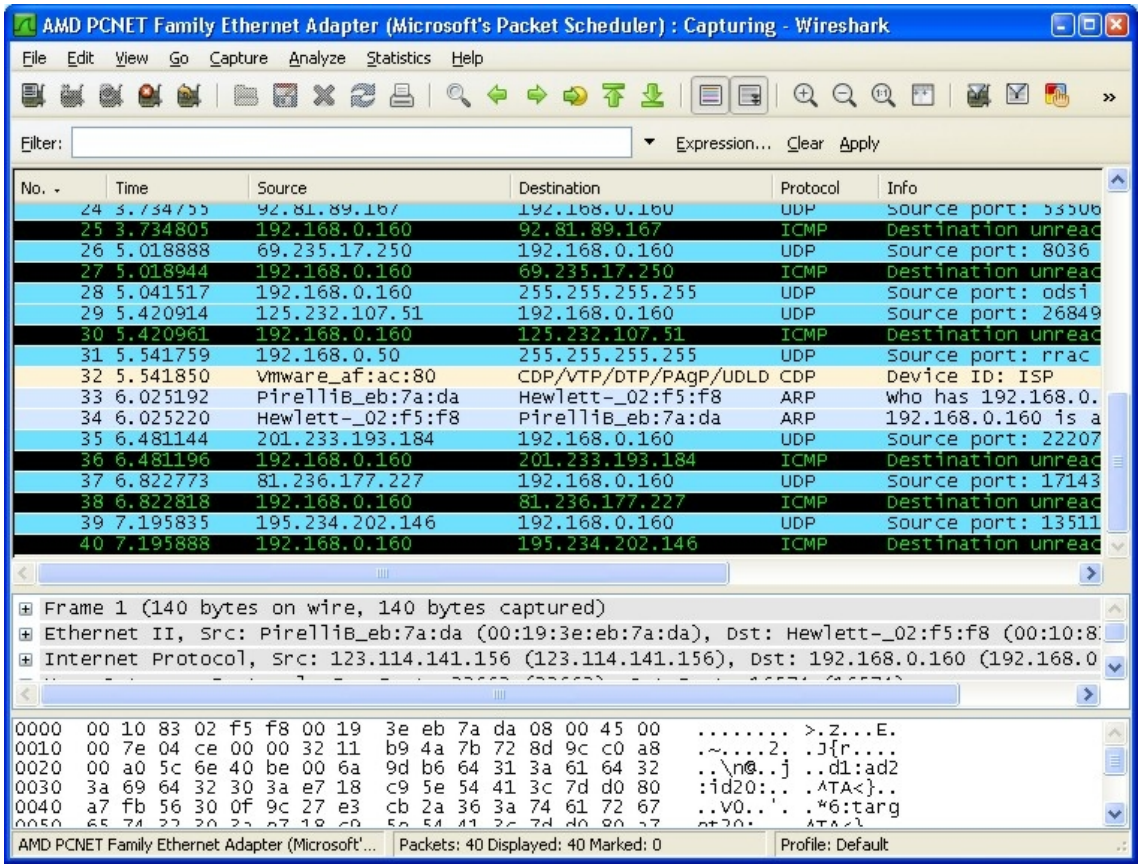
Con el programa corriendo ahora consta simplemente de configurarlo para que nos capture los paquetes enviados por el mikrotik.



Hacemos clic en nuestro primer icono comenzando de mano izquierda. Que nos abre una ventana la cual nos muestra todas las interfaces de red que poseemos en el equipo.



Hacemos clic en la interfase que deseamos capturar la información y comenzamos la captura del mismo.

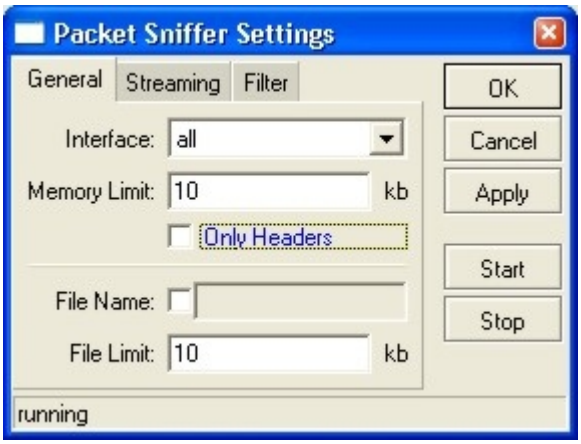


Para capturar tráfico de toda la red desde otro cliente que no sea el 192.168.1.2 debemos reconfigurar el mikrotik de la siguiente manera. Vamos al menú *TOOLS /*

PACKET SNIFFER. En la nueva ventana hacemos clic en el botón *SETTINGS* y comienza nuestra configuración.

Pestaña General:

- Interface: all
- Memory Limit 10kb
- Only Headers: (deseleccionado)
- File Limit: 10

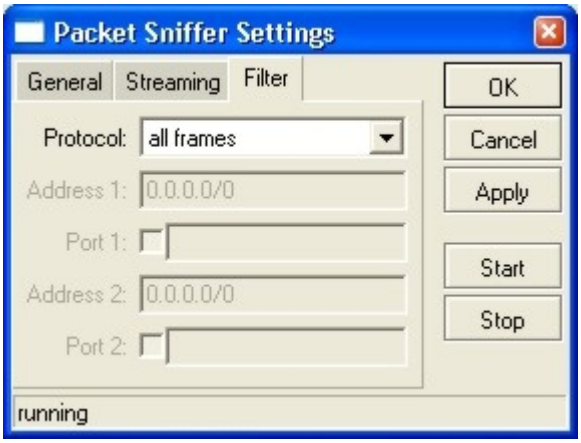


Pestaña Streaming:

- Streaming Enable: (Seleccionado)
- Server: 192.168.2.253
- Filter Stream: (Seleccionado)

Pestaña Filter:

- Protocol: all frames.



Conclusión

Del análisis de los resultados se concluye que Royal Tech debería re estructurar su red informática. Debido al ineficiencia de la misma, ya que estaba siendo desbordada por los nuevos requerimientos de la empresa en pleno crecimiento.

- Para la implementación de la red se utilizó el sistema operativo Mikrotik RouterOS basado en Linux. El mismo convierte una pc Standard en un router de dedicado de alto rendimiento.

- Se definió la configuración de las interfaces. Asignando nombres, direcciones de IP a las mismas y definición de las Vlan.

- Se configuró el servidor de DHCP para cada una de las sub redes. En el cual se definieron los pools de ip para cada una. También la asignación direcciones de IP fijas a partir de direcciones MAC de los servidores.

- Se configuró un servidor NTP para sincronizar la hora en dentro de toda la red. También se configuro un cliente NTP para sincronizar la hora de la red con otros servidores de tiempo.

- Se configuro un servidor PPPoE para autenticar usuarios que se deseen loguear al área de producción. El cliente de PPPoE se configuró para que la red tenga un tercer acceso a Internet mediante Adsl de backup.

- Se configuró un servidor de VPN para comunicar las oficinas de ventas de córdoba con las de ventas de Buenos Aires.

- Se configuró un servidor de Web Proxy para optimizar la utilización de los recursos hacia Internet. En el mismo se configuro politicas de bloqueo de tráfico hacia ciertas páginas al igual que el bloqueo de descarga de ciertos archivos.

- Se realizó un balanceo de carga entre los dos proveedores de Internet seleccionados. Para la optimización del recurso.

- Se realizaron políticas de control de ancho de banda para los clientes P2P.

- Se implemento políticas de firewall como bloqueo de p2p, bloqueo del Msn Messenger, redireccionamiento de puertos y bloqueo de paquetes no deseados.

- Se configuró un Hot Spot para el área de recreamiento de la empresa en la cual los usuarios se autentican mediante un servidor Radius.

- Se configuro un servidor de mensajería jabber para que los usuarios no mal dispongan su tiempo.

Bibliografía

- Chris Hurley, Russ Rogers, Frank Thornton, and Daniel Connelly. (2006).”Wardriving & Wireless Penetration Testing”. 1ra Edidcion. Estados Unidos: Syngress (431 Pag.)

- Freeraduis 2008. “Wiki site” < http://wiki.freeradius.org/Main_Page> [04/2008]

- Mallery, John; Zann, Jason; Kelly, Patrick. ”Blindaje de Redes”. 1ra Edicion. España. Anaya Multimedia. (720 pag)

- Mikrotik. (2006) “MikroTik RouterOS™ v2.9 Reference Manual”, 1ra Edicion, Estados unidos: Mikrotik SIA. (695 pag)

- Mikrotik 2007. “Manual de referencia”. < http://www.mikrotik.com/testdocs/ros/2.9/> [04/2008]

- Mikrotik 2008. “Mikrotik Forum”.< http://forum.mikrotik.com> [04/2008]

- Mikrotik. 2008. “Wiki Site”.<http://wiki.mikrotik.com> . [04/2008]

- Mrtg 2008. “Documentation Site” <http://oss.oetiker.ch/mrtg/doc/index.en.html> [04/2008]

- Scrimger, Rob (Wiley John + Sons).”Tcp/Ip Bible”.2da Edición. Estados Unidos: Hungry Minds. (626 pag)