

TRABAJO ESPECIAL DE GRADO

EVALUACIÓN DEL SERVICIO DE INTERNET PÚBLICO “MIRANDA WIFI” DE LA GOBERNACIÓN DEL ESTADO MIRANDA

Presentado ante la Ilustre
Universidad Central de Venezuela
por el Br. Gil A., Edgar A.
para optar al título de
Ingeniero Electricista

Caracas, 2013

TRABAJO ESPECIAL DE GRADO

EVALUACIÓN DEL SERVICIO DE INTERNET PÚBLICO “MIRANDA WIFI” DE LA GOBERNACIÓN DEL ESTADO MIRANDA

Profesor guía: PhD. Carlos Moreno
Tutor Industrial: Ing. Gustavo Otto

Presentado ante la Ilustre
Universidad Central de Venezuela
por el Br. Gil A., Edgar A.
para optar al título de
Ingeniero Electricista

Caracas, 2013

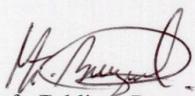
CONSTANCIA DE APROBACIÓN

Caracas, 07 de noviembre de 2013

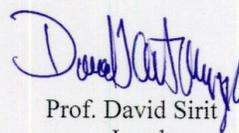
Los abajo firmantes, miembros del Jurado designado por el Consejo de Escuela de Ingeniería Eléctrica, para evaluar el Trabajo Especial de Grado presentado por el Bachiller Edgar Gil, titulado:

“EVALUACIÓN DEL SERVICIO DE INTERNET PUBLICO “MIRANDA WIFI” DE LA GOBERNACION DE MIRANDA”

Consideran que el mismo cumple con los requisitos exigidos por el plan de estudios conducente al Título de Ingeniero Electricista en la mención de Comunicaciones, y sin que ello signifique que se hacen solidarios con las ideas expuestas por el autor, lo declaran APROBADO.



Prof. Zeldívar Bruzual
Jurado



Prof. David Sirit
Jurado



Prof. Carlos Moreno
Prof. Guía

DEDICATORIA

A mi madre, en la búsqueda de tu felicidad y como una mínima retribución a todo tu apoyo incondicional, esfuerzo y sacrificio.

RECONOCIMIENTOS Y AGRADECIMIENTOS

Creo que me sería imposible agradecer y reconocer a quienes de una u otra manera han participado en este proceso, no solo en la elaboración de este trabajo especial de grado, sino en la formación de mi carrera y de mi vida personal, a ustedes estas palabras de agradecimiento:

En primera instancia a mis padres, a la Choli, Tía Adela, Milena, Tacha, en fin, mi familia, quienes debo confesar que a pesar de muchas veces no tener idea de lo que hacía y estudiaba, si tenían muy claro que palabra de aliento decir en qué momento, y cual muestra de alegría darme por mis avances, y de esta forma motivarme a seguir adelante, son pilares de mi persona.

A mis amigos, Víctor, Jerry, Jorge, Mariela quienes quizás en realidad en oportunidades entorpecimos (porque soy cómplice) mis estudios con esas Pilsen, pero despejamos la mente y refrescamos las neuronas, ustedes me han apoyado mucho, en este y en otros aspectos de mi vida, imposible no nombrarlos.

A mis compañeros, Katerin, Chuti, Felipe, El Bish, Astrid, Monic, Juan, William, el señor Bonet, con quienes compartimos horas estudio (a veces de güachafita) y de alguna forma las hacíamos amenas (claro... con la güachafita) y a pesar de muchas veces no terminar claros como el agua, terminábamos con una sonrisa en la cara (adivinen porque...), muchachos sin ustedes, ésta última etapa no hubiera sido tan grata, les agradezco enormemente por haber participado en mis últimos semestres y brindarme su amistad incondicional, dudo haber llegado hasta aquí sin ustedes.

A todos quienes creyeron en mí, porque estaban seguros de que estaría aquí, y a quienes no creyeron, por tener la oportunidad de demostrarles con el ejemplo de que estaban equivocados, y debo confesar que en oportunidades, me encontré a mi mismo entre éstos últimos.

A Leo, por las Voll-Damm que nos vamos a tomar.

A María Auxiliadora, cualquier palabra que escriba como agradecimiento sería una retribución insignificante para la entrega y compromiso que adquieres para con cada uno de nosotros los estudiantes, ojalá en mi carrera llegue a ser tan profesional y eficiente como lo eres tú en la tuya.

Al profesor Carlos Moreno, al Ing. Gustavo Otto y al Licenciado Joel Monroe por su apoyo incondicional en el desarrollo del trabajo, espero haber cumplido sus expectativas.

Y por último, aunque no por eso menos importante, a Dios, por de alguna forma haber engranado todas las situaciones y puesto los protagonistas, cuyo resultado es traerme hasta este grato momento de mi vida, en el que puedo decirle a todos los que recordé de plasmar en este breve reseña, y a los que olvidé mencionar pero igual merecen estar aquí, “lo logramos”, mi logro también les pertenece a ustedes.

Gil A., Edgar A.

**EVALUACION DEL SERVICIO DE INTERNET PÚBLICO
“MIRANDA WIFI” DE LA GOBERNACION DEL ESTADO
MIRANDA**

**Tutor académico: PhD. Carlos Moreno. Tutor industrial: Ing. Gustavo Otto.
Tesis. Caracas. U.C.V. Facultad de Ingeniería. Escuela de Ingeniería Eléctrica.
Ingeniero Electricista. Opción: Comunicaciones 52 h + anexos**

Palabras Clave: Internet público; QoS; Evaluación de radio bases servicio “Miranda WiFi”; configuración equipos Mikrotik.

Resumen. En el presente trabajo, se hace una evaluación técnica de diversas radio bases del proyecto “Miranda WiFi” de la Gobernación del estado Miranda, empezando con una breve investigación documental de las redes en general y calidad de servicio, así como las características de los equipos instalados. Se revisan los informes de ingeniería de las radio bases y se establece la configuración y disposición original de los equipos, en conjunto con el personal de la Gobernación se formula una propuesta de configuración para brindar calidad de servicio a los usuarios. En las visitas se ejecuta un análisis de fallas de red ascendente, diagnosticando las fallas en sitio, planteando soluciones viables al momento, recuperando de esta forma la operatividad del servicio. Adicionalmente se cumple con un requerimiento adicional por parte de la Gobernación, elaborando un manual de referencia para la configuración de los equipos Mikrotik, dirigido a su personal de soporte técnico.

INDICE GENERAL

CONSTANCIA DE APROBACION	iii
DEDICATORIA	iv
RECONOCIMIENTOS Y AGRADECIMIENTOS	v
RESUMEN	vii
INDICE GENERAL	viii
LISTA DE FIGURAS	xi
LISTA DE TABLAS	xii
LISTA DE ACRÓNIMOS	xiii
INTRODUCCIÓN	1
CAPÍTULO I	3
1.- DEFINICIÓN DEL PROBLEMA	3
1.1 Objetivo general	3
1.2 Objetivos Específicos	3
1.3 Metodología	4
1.3.1 Fase 1 Análisis preliminar	5
1.3.2 Fase 2 Estudio documental	5
1.3.3 Fase 3 Configuración de equipos:	6
1.3.4 Fase 4 Trabajo de campo	6
1.3.5 Fase 5 Documentación	7
CAPÍTULO II	9
2.- MARCO TEÓRICO	9
2.1 Introducción a las redes WLAN	9
2.2 Ventajas e inconvenientes de una red inalámbrica	9
2.3 Elementos de una red	11
2.3.1 Concentrador o hub	11
2.3.2 Conmutador o switch	12
2.3.3 Enrutador o router	12
2.4 Topologías de red inalámbrica	12

2.4.1 Conexión punto a punto	12
2.4.2 Punto de acceso.....	13
2.4.3 Interconexión de redes	13
2.5 Hotspot:	13
2.6 Portal Captivo.....	14
2.7 Diagnóstico de fallas en redes	14
2.8 Calidad de servicio (QoS)	15
2.8.1 Mejor esfuerzo (Best Effort).....	16
2.8.2 Servicios integrados (IntServ)	16
2.8.3 Servicios Diferenciados (DiffServ)	17
CAPÍTULO III	19
3.- EQUIPOS Y FUNCIONAMIENTO	19
3.1 Lanpro LP 2416 (Antena).....	19
3.2 Lanpro LP 1522 (Enrutador inalámbrico)	20
3.3 Lanpro LP-PA2410 (Amplificador de 1W).....	20
3.4 Lanpro SPL324 (Splitter 1–3)	21
3.5 Lanpro LB404 (Balanceador de carga)	21
3.6 Lanpro NC-1 (Balanceador de carga - portal captivo)	22
3.7 Mikrotik RB493A.....	23
3.7.1 “Mangle”.....	23
3.7.2 “Queue Tree”o “árbol de colas”	24
3.7.3 “Dual Limitation” o “Limitacion Dual”	24
3.7.4 Web Proxy	26
3.7.5 NAT	26
CAPÍTULO IV	27
4.- CONFIGURACIÓN Y MANUAL	27
4.1 Detalle del esquema de configuración:	27
4.1.1 Identificación y renombramiento de interfaces:	27
4.1.2 Asignación de direcciones y configuración de red:	27
4.1.3 Configuración de servidor DHCP en red local:	28
4.1.4 Configuración de hotspot para acceso inalámbrico:	28

4.1.5 Identificación de flujos y marcado de paquetes:.....	28
4.1.6 Establecimiento de velocidades de acceso y prioridades de colas de paquetes.	29
4.1.7 Configuración de webproxy.....	29
4.1.8 Configuración de reglas de traslación de direcciones.....	29
4.2 Manual de configuración.....	30
4.2.1 Público al que está dirigido.....	30
4.2.2 Utilidad y alcance del manual.....	30
CAPÍTULO V	31
5.- CASOS DE ESTUDIO.....	31
5.1 Caso de estudio, UNEFA Extensión Charallave.....	31
5.1.1 Análisis preliminar.....	31
5.1.2 Análisis en el sitio.....	32
5.2 Caso de estudio, Biblioteca Pública Cúpira.....	35
5.2.1 Análisis preliminar.....	35
5.2.2 Análisis en el sitio.....	37
5.3 Otros casos de estudio.....	45
CONCLUSIONES	48
RECOMENDACIONES	48
REFERENCIAS BIBLIOGRÁFICAS	52
BIBLIOGRAFÍA	54
ANEXO	¡Error! Marcador no definido.

LISTA DE FIGURAS

Figura 1 Esquema para determinar el análisis de falla de red a aplicar	15
Figura 2 Lanpro LP 2416 [11]	19
Figura 3 Lanpro LP-1522 [12].....	20
Figura 4 Lanpro LP-PA2410 [13].....	20
Figura 5 Ilustración del esquema de conexión Lanpro LP-PA2410 [13].....	21
Figura 6 Lanpro LP-SPLT243 [14].....	21
Figura 7 Lanpro LB404 [15].....	22
Figura 8 Lanpro LP-NC1 [16]	22
Figura 9 Mikrotik RB493A [17]	23
Figura 11 Disposición de los equipos de la Tabla 1 [18].....	32
Figura 12 Aspecto de la instalación de las antenas en la UNEFA, extensión Charallave	34
Figura 13 Detalle del tablero de protecciones para el circuito del rack en las instalaciones de la UNEFA, extensión Charallave.	35
Figura 14 Disposición de los equipos en la Tabla 2 [19].....	37
Figura 15 Detalle de caja de intemperie con equipos inoperativos.....	38
Figura 16 Detalle de los equipos inoperativos, sustituidos en la radio base de Cúpira.	39
Figura 17 Detalle del cableado sustituido desde el cajetín de distribución hasta la caja de intemperie.....	39
Figura 18 Detalle del cajetín de distribución e interruptor de energía hacia la caja de intemperie.....	40
Figura 19 Detalle del interruptor inoperativo.....	41
Figura 20 Tablero del circuito de los equipos de la radio base.....	45
Figura 21 Aspecto de la instalación externa en la radio base de la biblioteca pública en Curiepe	47

LISTA DE TABLAS

Tabla 1 Diferencias entre "proyecto de investigación" y "proyecto factible" [2].....	4
Tabla 2 Equipos instalados en la radio base de la UNEFA – Extensión Charallave [18].....	31
Tabla 3 Equipos instalados en la radio base de Cúpira [19].....	36
Tabla 4 Valores de prioridad de marcas de paquetes en árbol de colas, CIR y MIR en % del enlace disponible.....	44
Tabla 5 Listado de fechas de las visitas e instituciones visitadas	46

LISTA DE ACRÓNIMOS

CPE	Customer Premises Equipment
CPU	Central processor unit
DHCP	Dynamic host configuration protocol
DNS	Domain name server
LAN	Local area network
Led	Light emmitter diode
OSI	Open System Interconnection
QoS	Quality of service
TIC	Tecnología de Informacion y Comunicación
WAN	Wide Area network
WiFi	Wireless Fidelity
WLAN	Wireless Local Area Network

INTRODUCCIÓN

En los últimos cinco años, el mundo se ha vuelto cada vez más móvil. Como resultado, las formas tradicionales de la interconexión de los ciudadanos han resultado insuficientes para afrontar los retos planteados por el nuevo estilo de vida colectivo. Si los usuarios deben estar conectados a una red por cables físicos, su movimiento se reduce drásticamente. La conectividad inalámbrica, sin embargo, no posee tal restricción y permite una gran libertad de movimiento por parte del usuario de la red. Como resultado, las tecnologías inalámbricas están invadiendo el ámbito tradicional de redes "fijas" o "por cable".

Internet se ha convertido en una herramienta multidisciplinaria, con una cantidad de usos realmente impresionante, desde aplicaciones de juegos en línea para la recreación hasta el manejo de cuentas bancarias a nivel internacional para la transferencias de dinero, y por supuesto, no podían pasar por alto los propósitos académicos, llegando incluso a conseguirse portales influyentes gratuitos, sin fines de lucro ni publicidad, dedicados exclusivamente a la propagación del conocimiento en la nube, un ejemplo de ello lo conseguimos en la Organización Wikimedia, quien administra www.wikipedia.org disponible en 284 idiomas con más de 37 millones de artículos[1].

Motivado a la facilidad con la que se puede conseguir información en la Internet, se considera una herramienta de un potencial incalculable, en el proceso de instrucción y capacitación, no sólo académica, sino de cualquier área del saber, de allí la importancia que refleja el hecho que la Gobernación pueda brindar un servicio de acceso a Internet público de calidad, para las comunidades en donde se encuentran desplegados los nodos, sobre todo, en aquellas donde el despliegue tecnológico se limita a las bibliotecas y centros educativos, donde se encuentran instalados los nodos, es decir, el ciudadano promedio únicamente tiene acceso a Internet por estos enlaces.

Se visualiza una escalabilidad importante y muy significativa para este proyecto, en función de que abriría una ventana hacia el uso de tecnologías de información y comunicación (TIC's) en la educación e igualmente a la educación a distancia, adicionalmente como la implementación de herramientas administrativas para uso interno de la Gobernación y su personal en estas localidades remotas.

CAPÍTULO I

DEFINICIÓN DEL PROBLEMA

Actualmente la Gobernación del estado Miranda cuenta con la instalación de 18 nodos de conexión inalámbrica WiFi, pero muchos de ellos no se encuentran operativos, la Gobernación no cuenta con un departamento de soporte especializado en el área que pueda solventar las irregularidades que puedan presentarse, así como tampoco cuentan con un protocolo o manual de procedimientos a seguir para solventar alguna irregularidad.

Es importante resaltar que existen sólo dos tipos de radio base instalada, cuya única diferencia radica en que unas están implementadas con equipo Lanpro NC-1 y otras con Mikrotik RB493A, teniendo en común el resto de los equipos.

1.1 Objetivo general

Evaluar el servicio de Internet inalámbrico externo “Miranda WiFi” del Gobierno del estado Miranda

1.2 Objetivos Específicos

- a. Elaborar un estudio bibliográfico referente al funcionamiento de redes inalámbricas y calidad de servicio.

- b. Realizar un levantamiento de información sobre la arquitectura de las radio bases, con la finalidad de alcanzar la familiarización necesaria para elaborar una evaluación técnica y proponer los cambios que se consideren prudentes en la radio base de la Biblioteca Pública de Cúpira y la UNEXPO - Extensión Charallave

- c. Diagnosticar las fallas y plantear soluciones para retomar la operatividad de los nodos en evaluación.

d. Establecer la configuración más adecuada de los equipos (según sus características) para la aplicación del proyecto, en función de brindar el servicio a la mayor cantidad de usuarios simultáneamente.

1.3 Metodología

El tipo de investigación aplicado fue el de investigación proyectiva, la cual intenta proponer soluciones a una situación determinada. En ésta categoría entran los proyectos factibles y todas las investigaciones que conllevan al diseño o creación de algo. Establece el enfoque de la investigación y, en consecuencia, la forma de presentar los objetivos y resultados finales del trabajo.

Tabla 1 Diferencias entre "proyecto de investigación" y "proyecto factible" [2]

Proyecto de Investigación	Proyecto Factible
Plantea un problema de conocimiento (algo que se desconoce)	Plantea un problema de tipo práctico, generalmente determinado por una necesidad
Se plantea objetivos de investigación, lo que refleja aspectos a conocer.	Se traza objetivo de acción: tareas, actividades, procesos.
Requiere un marco teórico que fundamente la investigación a realizar	No necesariamente requiere de postura teórica. Hace mucho énfasis en la justificación del proyecto.
Puede formular hipótesis	Formula propuestas de acción y/o modelos operativos como alternativa de solución.
La metodología utiliza técnicas, instrumentos y procedimientos propios de la investigación científica	La metodología varía según la fase y naturaleza del proyecto.
Los elementos básicos que se incluyen en un proyecto de investigación son: <ul style="list-style-type: none"> • Planteamiento del problema • Objetivos • Justificación • Marco Teórico • Metodología. 	Los elementos básicos que se incluyen en un proyecto factible son: <ul style="list-style-type: none"> • Objetivos • Justificación • Diagnóstico de necesidades • Formulación del modelo o propuesta, • Análisis de su factibilidad.
En un proyecto de este tipo se investiga.	En un proyecto de este estilo se planifica.

El presente trabajo se desarrolló bajo las premisas de proyecto factible, se dividió en distintas fases, descritas a continuación:

1.3.1 Fase 1 Análisis preliminar

En esta fase se efectuó una revisión de los informes de ingeniería, determinando de esta forma el tipo de equipos instalados, disposición y configuración, así como de la infraestructura operativa de los sitios donde se encuentran instalados, definiendo la existencia en ambas instalaciones de una sala de computadores, de uso público para acceso a internet. Esta sala hace uso del enlace disponible para el servicio de internet inalámbrico, por medio de una red cableada.

1.3.2 Fase 2 Estudio documental

En esta fase se realizó una investigación bibliográfica acerca del funcionamiento de las redes en general, tanto cableadas como inalámbricas, así como de los manuales de los equipos para determinar sus características y posteriormente determinar la forma de usarlas para la aplicación del proyecto.

Es importante destacar que no se hizo mayor énfasis en investigar acerca de la seguridad en redes inalámbricas, en función de que los fines del proyecto son netamente académicos o culturales, y no se considera necesario tener un alto nivel de seguridad para proteger este tipo de información, de hecho, previamente a las visitas, en ninguna radio base había configurada ninguna medida de seguridad a nivel inalámbrico.

Igualmente no se hizo mayor énfasis en el funcionamiento a nivel de la capa física de la interfaz inalámbrica, en virtud de que no se disponía de equipos de medición para verificar valores de potencia recibida entre otros.

1.3.3 Fase 3 Configuración de equipos:

Una vez determinadas las características de los equipos, en conjunto con el personal de la Gobernación se establecieron los diferentes parámetros de configuración de los equipos, una vez dispuesta la configuración completa se procedió a configurar un equipo y hacer las pruebas de la configuración.

Éstos criterios se establecen como propuesta para lograr brindarle acceso al mayor número de usuarios simultáneos, por ello a las conexiones de menor tráfico, se le brinda prioridad, garantizando un acceso a páginas compuestas en su mayoría por texto, en virtud de que el servicio tiene como fin principal brindar un apoyo con fines académicos o de instrucción.

El trabajo de configuración de los equipos se realizó exclusivamente en las oficinas de la Dirección de Tecnología de la Información, en el km 23 de la carretera Panamericana, sector Los Cerritos, en este sitio se encuentra controlado el acceso a internet, no está permitido el acceso a contenido no apto para el desempeño de las funciones en la Gobernación, pero se dispuso de un acceso sin bloqueo hacia internet, con el cual se pudieron hacer pruebas acerca de la marcación de paquetes y bloqueo de páginas.

1.3.4 Fase 4 Trabajo de campo

Posteriormente a la configuración de los equipos y sus pruebas, se procedió a realizar las visitas a las radio bases. La logística para el traslado y viáticos fueron proporcionados por la Gobernación, adicionalmente se tenía a disposición varios de los equipos desplegados en las radio bases (3 amplificadores e inyectores, 1 Lanpro NC-1, 1 Lanpro Lp-1522, 1 Mikrotik RB493A, y sus respectivas fuentes, 1 Splitter) para hacer el reemplazo de los equipos que se encuentren inoperativos, en pro de recuperar el funcionamiento regular del nodo.

En esta etapa se hizo diagnóstico y análisis de las fallas presentes en campo. Para este proyecto se considera falla cualquier irregularidad que afectara la

operatividad del servicio de acceso a internet en el tramo desde el equipo Lanpro NC1 o Mikrotik RB493, según sea el caso, hasta la interfaz aire de la radio base. El punto de medición inalámbrico se ubicó en la sala de tecnología instalada en los sitios. El estudio de operatividad de la radio base no considera el tramo desde el equipo CPE del proveedor ISP hacia internet.

Es importante destacar que en esta etapa, luego de efectuar el diagnóstico de fallas se hacen propuestas factibles de ejecutar al momento, de acuerdo a los equipos disponibles, para recuperar la operatividad de los nodos.

Por la sencillez de la red desplegada en los nodos, en el caso de estudio de la radio base desplegada en la UNEXPO Extensión Charallave y en la Biblioteca Pública de Cúpira, se efectuó un enfoque ascendente para el diagnóstico de las fallas en la red.

El estudio de cobertura de las estaciones radio bases no forma parte del alcance del presente trabajo, en tal sentido se considera que la interfaz aire está operativa debido a que las pruebas realizadas garantizaron el correcto acceso a capas superiores del protocolo de internet conectado de forma inalámbrica a una distancia máxima de 20 metros.

Igualmente, durante las visitas de inspección, se revisaron los criterios básicos de ingeniería en cuanto a: instalación físicas de equipos, conexiones eléctricas (notando inexistencia de sistemas de puesta a tierra), también se hizo una revisión cualitativa de temperatura de operación de equipos, etc. Estas revisiones realizadas son factores que aumentan la probabilidad de falla de cualquier equipamiento electrónico, por lo que posteriormente se proponen recomendaciones para su mejora.

1.3.5 Fase 5 Documentación

En esta fase se realizó la documentación de un manual de configuración de los equipos Mikrotik. No se realiza manual de otro equipo, motivado a que el equipo Lanpro NC-1 cuenta con una configuración de respaldo que puede ser cargada a los

equipos. En los Mikrotik no se goza de esta ventaja y por ello fue requerido adicionalmente a los objetivos planteados, la elaboración de un manual para hacer la configuración desde un inicio. Por último se efectuó la redacción del informe final del Trabajo Especial de Grado.

CAPÍTULO II

MARCO TEÓRICO

2.1 Introducción a las redes WLAN

Antes de hablar de las redes WLAN es necesario definir las redes LAN, siendo éstas últimas, un conjunto de ordenadores o dispositivos interconectados entre sí, mediante un medio cableado, en un espacio físico pequeño (menos de 100 mts de radio) [3].

Partiendo de esta idea, podemos definir las WLAN's , como un conjunto de ordenadores o dispositivos interconectados entre sí mediante el espacio libre (aire) por medio de ondas electromagnéticas.

En particular, las redes inalámbricas, ofrecen una alternativa de despliegue de una red a corto plazo (son pocos los equipos que hay que instalar), bajo costo (no es necesario hacer cableado individual para todos los dispositivos que se requieren conectar), así como ofrecen una gran flexibilidad en cuanto a la instalación. En sitios donde el despliegue de una red cableada sea poco viable, la red inalámbrica ofrece estas ventajas así como adicionalmente brinda movilidad a los terminales dentro de su área de cobertura, ideal para la aplicación de terminales móviles en un área determinada (como por ejemplo en un almacén para un control de inventario).

2.2 Ventajas e inconvenientes de una red inalámbrica

Las principales ventajas de una red inalámbrica es la libertad de movimientos, sencillez en la reubicación de terminales, el despliegue a corto plazo, el bajo impacto a nivel de infraestructura, resultando ideal para proveer una red en edificios históricos o en aquellos donde el despliegue de una red cableada no sea viable, como por ejemplo grandes naves industriales, en donde exista una rutina de trabajo, en la cual, implementar una red cableada puede entorpecer otras funciones, como por ejemplo la instalación de canaletas o tuberías puede limitar el paso de transportes.

Todo esto resulta en una clara reducción de costes de explotación, en virtud de que en un entorno con cambios frecuentes o altamente dinámico, el costo de implementación de una red inalámbrica es significativamente más bajo, resultando mejor inversión incluso en el caso que los equipos representen un costo mayor a los de una red cableada, en función de que trasladar una red inalámbrica es relativamente sencillo, mientras que una red cableada necesariamente hay que desplegarla en el sitio y no se puede reutilizar el cableado, siendo éste en particular, un factor determinante al momento de la evaluación del costo, es común que en una instalación de red, el costo del cable instalado supere el costo de los equipos de la red.

Adicionalmente, la capacidad de la red inalámbrica estará determinada por el equipo que sirva de interfaz entre el medio cableado e inalámbrico, dando la ventaja en la necesidad de una expansión, únicamente sustituyendo éste equipo por uno de mayor capacidad, se aumenta la cantidad de equipos y conexiones simultáneas que se pueden manejar en la interfaz de aire.

En resumen, las ventajas de una red inalámbrica las podemos enumerar en:

- Movilidad.
- Corto tiempo de implementación.
- Bajo impacto estético y estructural en la instalación.
- Facilidad de escalamiento.
- Reciclaje de la red en caso de reubicación.

De igual forma, entre los inconvenientes de la implementación de esta tecnología, podemos citar los siguientes:

- Susceptibilidad en la banda de frecuencias en la que opera, todo dispositivo que funcione bajo el principio de propagación de ondas electromagnéticas en el espacio libre, está expuesto a sufrir interferencias por ondas electromagnéticas que se encuentren en la

misma banda de frecuencia, sin importar su naturaleza (teléfonos inalámbricos, hornos de microondas, etc...) [4]

- Seguridad o privacidad, al tener como canal el aire o espacio libre, cualquier equipo que se encuentre cerca de la estación base o terminal puede capturar paquetes de datos, o lograr un acceso no permitido a la red, cumpliendo únicamente el requisito de encontrarse bajo la sombra de irradiación del punto de acceso a la red. [4]
- La velocidad de transmisión por el medio inalámbrico no se puede garantizar de igual manera que en el medio cableado, a medida que se encuentra a mayor distancia de la radio base o bajo la influencia de interferencias, se experimenta una baja de velocidad de transmisión, en consecuencia del aumento de errores, sumado a esto la limitante que presenta la interfaz aire de los puntos de acceso, mientras más usuarios simultáneos se manejen, no se podrá garantizar la máxima velocidad de acceso para todos. [4]

2.3 Elementos de una red

2.3.1 Concentrador o hub

Es el dispositivo más básico para interconectar más de 2 equipos en el mismo segmento lógico de red, funciona a nivel de la capa 1 del modelo OSI, brinda únicamente un enlace físico, lo que recibe por uno de sus puertos lo replica a todos los puertos restantes, son los equipos terminales los encargados de discriminar si los paquetes que reciben están dirigidos hacia ellos o hacia otro terminal, y de esta forma descartarlo. La desventaja de estos dispositivos es que al momento de tener una conexión entre 2 dispositivos, todos los puertos con equipo conectado tienen tráfico, aumentando las probabilidades de colisiones en el caso que se inicie otra transmisión, simultánea, entre otros 2 dispositivos, mientras más conexiones simultáneas, más probabilidad de colisión, y pérdida de paquetes, requiriendo retransmisión y

representando un retraso en la comunicación, situación que afecta la calidad de servicio (QoS) [5].

“Todas las estaciones en los segmentos de medios conectados a los puertos del repetidor determinado, participan en un solo dominio de colisión. Un paquete transmitido por cualquiera de estas estaciones es visto por todas estas estaciones.” [6]

2.3.2 Conmutador o switch

Dispositivo que desempeña sus funciones en la capa 2 del modelo OSI, reconoce físicamente los equipos conectados en sus puertos, de allí que al momento de iniciar una conexión entre 2 equipos, éste dispositivo establece un puente entre los puertos que intervienen en esta conexión, este reconocimiento y aislamiento en la transmisión de datos exclusiva entre puertos, es la principal ventaja frente al concentrador, motivado a que los demás puertos no reciben tráfico inesperado o innecesario [5].

2.3.3 Enrutador o router

Dispositivo que desempeña sus funciones a nivel de la capa 3 del modelo OSI, es capaz de enlazar 2 o más segmentos de red lógicamente diferentes o distantes, brindando conectividad o acceso desde una red hasta la otra y/o viceversa [5].

2.4 Topologías de red inalámbrica

La versatilidad y flexibilidad de las redes inalámbricas, es el motivo por el cual una LAN implementada con esta tecnología, sea extremadamente variable, esta variedad de configuraciones y sus combinaciones, son las causas por las cuales este tipo de redes puede adaptarse a casi cualquier necesidad

2.4.1 Conexión punto a punto

También conocidas como redes ad-hoc, es la configuración más sencilla, únicamente intervienen los equipos terminales (no existe otro elemento activo en la

red para establecer el enlace), el requerimiento indispensable es que ambos equipos estén equipados con el hardware necesario, para comunicaciones inalámbricas, al ser un enlace directo entre transmisor y receptor, requiere de poca o ninguna gestión administrativa.

2.4.2 Punto de acceso

Estas configuraciones usan el concepto de celda, los clientes inalámbricos deben estar bajo la “sombra” de la emisión del dispositivo para acceder a la red, regularmente son colocados en alto, pero solo es necesario que esté dispuesto estratégicamente para dar cobertura necesaria a los clientes inalámbricos que soportan.

Los puntos de acceso inalámbricos son una extensión de la red cableada, por el medio inalámbrico, a pesar de ser dos medios totalmente diferentes, estos dispositivos permiten tener equipos en el mismo segmento lógico de red, limitado únicamente por la diferencia de velocidades de acceso que puede tener cada medio.

2.4.3 Interconexión de redes

Otra aplicación de las redes inalámbricas es lograr interconectar dos o más redes cableadas por medio inalámbrico, extendiendo así un segmento de red lógico en sitios remotos (o donde no es viable o no existe un enlace cableado) regularmente con línea de vista.

2.5 Hotspot:

O punto caliente, es llamado de esta forma el lugar en el que se ofrece un acceso a Internet al público, de forma gratuita o representando un costo para los usuarios, de acuerdo a la política del proveedor del servicio.

Regularmente los hotspot's son sitios donde existe alta demanda de tráfico hacia Internet, así como es común también conseguirlos en sitios con alta rotación de usuarios, como por ejemplo, aeropuertos, bibliotecas públicas, centros de

convenciones. Son puntos concebidos para brindar conexión al usuario casual, aunque también pueden brindar conexión a usuarios regulares, dependiendo igualmente de la política del proveedor del servicio.

2.6 Portal Captivo

Es un portal que regularmente se usa para manejar los hotspot, para obligar que los clientes se autentiquen en un página web local y de esta forma identificar cada usuario y brindarle su perfil determinado, es común la práctica de tener un acceso inalámbrico sin ningún tipo de seguridad para la conexión, pero al momento de hacer una solicitud hacia Internet, se solicitan credenciales para brindar acceso, al identificar al usuario se puede controlar tanto las velocidades a la que navega, el tráfico que consume, tiempo continuo de conexión, es decir, regularmente ofrecen una flexibilidad y un control bastante amplio.

2.7 Diagnóstico de fallas en redes

Existen estrategias esquematizadas para realizar el diagnóstico de fallas en una red, teniendo como principio el Modelo OSI, se puede hacer un análisis ascendente, análisis descendente o un análisis “divide y vencerás”. [7]

El análisis ascendente, consiste en hacer pruebas desde las capas más bajas hacia las más altas, detectando en la capa donde se presenta la irregularidad. [7]

El análisis descendente, consiste en hacer pruebas desde la capa más alta hasta la más baja hasta conseguir la capa que pasa la prueba y detectar en donde se presenta la irregularidad, se recomienda el uso de esta técnica cuando se tenga la sospecha de que la falla ocurre a nivel de software, verificando las aplicaciones del sistema final antes de abordar elementos de red más específicos y en capas inferiores. [7]

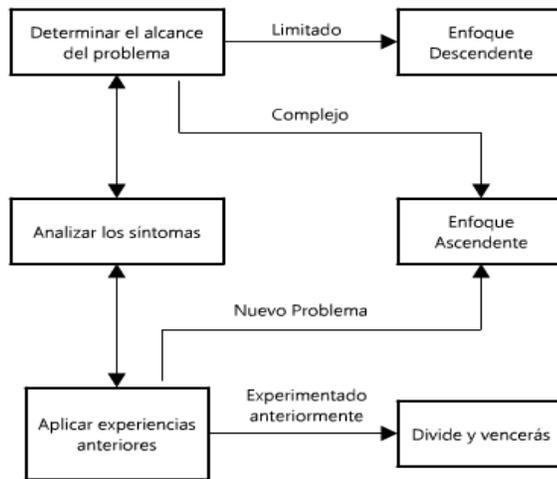


Figura 1 Esquema para determinar el análisis de falla de red a aplicar

La técnica de “divide y vencerás” empieza por recopilar o hacer uso de la experiencia de quien diagnostica la falla y el usuario, consiste en empezar el análisis desde una capa intermedia, en la que se supone se encuentra la irregularidad y hacer pruebas en la capa inferior siguiente, para verificar la operatividad de capas inferiores, o desplazarse hacia abajo en el caso que no se verifique operatividad en la capa inferior inmediata. Una vez que se verifica la correcta operatividad de una capa, se supone que las inferiores a ésta funcionan sin irregularidad, y se hace el diagnóstico hacia las capas superiores, ésta técnica es empleada con frecuencia por quienes poseen experiencia con fallas recurrentes. [7]

2.8 Calidad de servicio (QoS)

Si los recursos de una red fueran infinitos, no sería necesario aplicar técnicas para garantizar el buen funcionamiento de los servicios críticos que demandan un tráfico mínimo, como esto no es la realidad, y regularmente la demanda de tráfico es mucho mayor a la oferta que se tiene, se necesitan mecanismos para administrar los recursos finitos de la red y garantizar el correcto funcionamiento de los servicios críticos, como por ejemplo la comunicación de voz sobre ip (VoIP).

En la actualidad se pueden encontrar 3 modelos de aplicación de calidad de servicio:

- Mejor esfuerzo (best effort)
- Servicios integrados (IntServ)
- Servicios diferenciados (DiffServ)

2.8.1 *Mejor esfuerzo (Best Effort)*

Es el modelo aplicado en toda red en donde no está existe ninguna regla o política explícitamente definida. No garantiza ningún tratamiento especial para los flujos que lo requieran, todos los paquetes son tratados de igual forma, no existe ningún tipo de diferencia de prioridad o preferencia.

Como características principales podemos mencionar las siguientes:

- Altamente escalable.
- No requiere mecanismos o configuraciones especiales.
- No garantiza recursos ni diferencia ningún tipo de servicio.

2.8.2 *Servicios integrados (IntServ)*

Este modelo se aplica bajo demanda, antes de establecer la comunicación, los terminales señalizan y reservan recursos en la red para garantizar su disponibilidad a lo largo de la ruta específica.

“Los parámetros de control son utilizados por las aplicaciones, para proporcionar información a la red, en relación a las solicitudes de control de QoS. Un ejemplo es la especificación de tráfico (TSpec) generado por las aplicaciones de remitentes y receptores” [8].

“El comportamiento de extremo a extremo proporcionado a una aplicación, por una serie de elementos de red que prestan servicio de trafico controlado herméticamente, se aproxima el comportamiento visible para las aplicaciones que reciben servicio de mejor esfuerzo * bajo condiciones sin tráfico * de la misma serie de elementos de red” [9]

Antes de iniciarse propiamente la transmisión de datos, la sesión de la aplicación señala la ruta, para verificar la disponibilidad de recursos a lo largo de la misma. Posteriormente a la señalización, los recursos se mantienen reservados, aún cuando no se estén utilizando, hasta que se levante la reserva, este método permite garantizar la operación de aplicaciones críticas.

Entre sus características principales tenemos:

- Negocia las condiciones específicas de calidad de servicio, antes que se produzca la transmisión propiamente dicha.
- Una vez reservados los recursos, se cuenta con ellos indiferentemente del tráfico de la red.
- Puede adecuarse a demandas específicas y diferentes de cada tipo de tráfico y aplicación.
- La reserva de recursos se hace para cada flujo específicamente, no para aplicaciones en general.
- No es escalable en grandes redes, o en implementaciones complejas.

2.8.3 Servicios Diferenciados (DiffServ)

“La arquitectura de servicios diferenciados se basa en un modelo simple, donde el tráfico entrante en una red es clasificado y, posiblemente, condicionado en los límites de la red, y asignado a diferentes agregados de comportamiento” [10]

Modelo de recursos garantizados en forma genérica y no por flujos específicos. Permite garantizar diferentes condiciones de servicio para diferentes tipos de tráficos, de modo escalable a través de toda la red.

Como características principales podemos mencionar

- No requiere señalización previa.
- No garantiza condiciones de tráfico de extremo a extremo.
- Es muy flexible y escalable.

- Divide el tráfico en clases en función de los requerimientos de la organización.
- Cada paquete recibe el tratamiento definido para la clase a la que pertenece.
- A cada clase se le pueden asignar distintos recursos.
- La asignación de recursos se hace salto por salto, en cada dispositivo de la red, no a lo largo de una ruta específica.
- El mecanismo de implementación es relativamente complejo.

CAPÍTULO III

EQUIPOS Y FUNCIONAMIENTO

Se investigó en la documentación de los equipos, específicamente en los equipos de red en la búsqueda de sus capacidades de ofrecer Calidad de Servicio, en función de evaluar si se puede formular una configuración apropiada para la aplicación del proyecto, en los equipos de la etapa de radio frecuencia se determinaron sus características para verificar que estén diseñados para funcionar correctamente en la banda de frecuencia de WiFi.

3.1 Lanpro LP 2416 (Antena)



Figura 2 Lanpro LP 2416 [11]

Se revisó la documentación de la antena, verificando que efectivamente está diseñada para operar en la banda de 2.4GHz así como se verifica que el fabricante manifiesta que el dispositivo cuenta con una cobertura sectorial de 120°. [11]

3.2 Lanpro LP 1522 (Enrutador inalámbrico)



Figura 3 Lanpro LP-1522 [12]

Una vez revisada la documentación del dispositivo se puede establecer que es un enrutador inalámbrico, y puede ser configurado como punto de acceso y extender una red cableada a la interfaz aire sin la necesidad de realizar un NAT entre ambas interfaces, adicionalmente cuenta con antena removible, el rango de temperatura de operación de éste dispositivo se encuentra entre 0°C y 50°C. [12]

3.3 Lanpro LP-PA2410 (Amplificador de 1W)



Figura 4 Lanpro LP-PA2410 [13]

Se revisó la documentación en línea del fabricante del dispositivo, encontrando que el rango de frecuencias en la que trabaja se encuentra entre los 2400MHz y los 2500MHz, posee una impedancia de entrada de 50Ω, está diseñado para recibir hasta un máximo de 20dBm de potencia y entrega hasta un máximo de 30dBm de potencia, el modo de operación es bilateral. El rango de operación de temperatura de este equipo oscila entre los -20°C y los 70°C. [13]

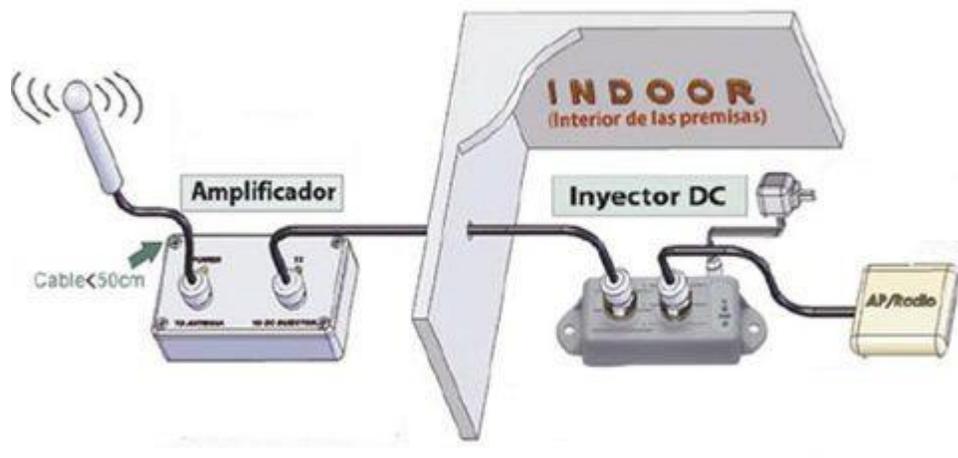


Figura 5 Ilustración del esquema de conexión Lanpro LP-PA2410 [13]

3.4 Lanpro SPL324 (Splitter 1–3)



Figura 6 Lanpro LP-SPLT243 [14]

Se revisó la documentación en línea de este dispositivo, observando que en la misma aparece reflejado explícitamente el rango de operación del dispositivo, entre los 800MHz y los 2500MHz [14]

3.5 Lanpro LB404 (Balanceador de carga)

Se revisó la documentación de éste dispositivo, verificando que su característica principal es la de hacer un balance de tasa de transferencia hasta un máximo de 4 enlaces hacia internet y una red local, adicionalmente se determinó que tiene la capacidad de ofrecer calidad de servicio basada en dirección IP, control de tasa de transferencia por puertos, control de sesiones IP, control de tasa de

transferencia por dirección IP y lista de sesiones conectadas, no es útil para la aplicación del proyecto Miranda WIFI este tipo de control de calidad de servicio. [15]



Figura 7 Lanpro LB404 [15]

3.6 Lanpro NC-1 (Balanceador de carga - portal captivo)



Figura 8 Lanpro LP-NC1 [16]

Se revisó la documentación de este dispositivo, verificando que posee igualmente la característica de balanceo de carga entre 2 accesos a internet y una red local, igualmente se determinó que una de sus características singulares es la de poder hacer control de usuarios mediante un portal captivo, se verifica las reglas de calidad de servicio que se pueden aplicar pero al igual que el equipo Lanpro LB404, ofrece la posibilidad de hacer control de tasa de transferencia por IP, por usuario de portal captivo y por puerto de origen y/o destino, de igual forma no es útil para este proyecto el control ofrecido por este equipo. [16]

3.7 Mikrotik RB493A

Al revisar la documentación del equipo Mikrotik RB493A se logra determinar que los equipos de este fabricante se basan en el sistema operativo RouterOS, se investiga acerca de este sistema operativo y se determina que cuenta con características bastante interesantes que pueden ser muy provechosas para cumplir con una apropiada aplicación del proyecto. A continuación se hace descripción de las características de este sistema operativo usadas en el proyecto.



Figura 9 Mikrotik RB493A [17]

3.7.1 “Mangle”

Mangle es una especie de "marcador" que establece una marca los paquetes para su posterior procesamiento. Otras características de RouterOS hacen uso de estas marcas, por ejemplo, árboles de colas, NAT, enrutamiento. Son capaces de identificar un paquete basándose, en su marca, y procesarlo en consecuencia. Las marcas de mangle sólo existen dentro del enrutador, por lo que no se transmiten a través de la red.

De esta función se usaron las siguientes características para la aplicación de la configuración

- Contenido.
- Destino y origen de tráfico.

- Tráfico de conexiones.

3.7.2 “Queue Tree” o “árbol de colas”

El “árbol de colas” es una característica del sistema operativo RouterOS, que permite organizar distintas colas de paquetes marcados en el “mangle”.

Para definir el árbol de colas, es necesario conocer HTB

HTB (Hierarchical Token Bucket o Cubo Jerárquico Simbólico) Es un método de gestión de colas con clases que es útil para el manejo de diferentes tipos de tráfico. Tenemos que seguir tres pasos básicos para crear HTB:

Detectar y marcar el tráfico - clasificar el tráfico para su uso posterior. Consiste en conseguir uno o más parámetros coincidentes para seleccionar paquetes para la clase específica.

Crear reglas (políticas) para marcar el tráfico – Colocar la clase específica de tráfico en su determinada cola y definir las acciones que se toman para cada clase.

Vincular la política para la interfaz específica– Añadir la política para todas las interfaces (global-in, global-out o global-total), para alguna interfaz específica o para la cola padre específica.

HTB permite crear una estructura jerárquica de colas, y determinar las relaciones entre las colas, como " padre-hijo" o "hijo- hijo".

Tan pronto como una cola tiene al menos un hijo se convierte en una cola interna, todas las colas sin hijos son ramas de cola. Las ramas de cola hacen el consumo real de tráfico, colas internas son responsables únicamente de distribución del tráfico.

3.7.3 “Dual Limitation” o “Limitacion Dual”

Cada cola HTB tiene dos límites de tasa:

CIR (Committed Information Rate o tasa de información comprometida) - (limit-in en RouterOS) peor de los casos, el flujo de datos va a conseguir esta velocidad de tráfico no importa lo que suceda (suponiendo que realmente podemos enviar el total de la suma de estas tasas de transferencia de datos)

MIR (Maximal Information Rate o tasa de información máxima) - (max-limit en RouterOS) mejor de los casos, la tasa de tráfico hasta la que se puede llegar, si la cola padre tiene la tasa de transferencia disponible.

En otras palabras, en un primer momento - el límite (CIR) de las todas las colas se cumple, sólo entonces las colas de hijo tratarán de pedir la velocidad de datos necesaria de sus padres con el fin de alcanzar su máximo límite (MIR).

Nota: CIR se asigna a la cola correspondiente, no importa lo que pase. (Incluso si se excede el límite máximo - de la cola padre)

Por eso, para asegurar (como fue diseñado) el uso óptimo de la función de doble limitación, es sugerido atenerse a las siguientes reglas:

La suma de las tasas de tráfico comprometido de todas las colas hijo, debe ser menor o igual a la tasa de tráfico que está disponible para la cola padre.

$$CIR_p \geq CIR_{h1} + CIR_{h2} + \dots + CIR_{hn} \quad (1)$$

Donde:

CIR_p : Tasa de información comprometida para la cola padre

$CIR_{h1}, CIR_{h2}, \dots, CIR_{hn}$: Tasa de información comprometida para cada una de las enésimas colas hijo.

En caso de que la cola padre es la principal cola padre

$$CIR_p = MIR_p \quad (2)$$

Donde:

CIR_p : Tasa de información comprometida para la cola padre.

MIR_p : Tasa de información máxima para la cola padre.

Tasa máxima de cualquier cola hijo debe ser menor o igual a la tasa máxima de la cola padre.

$$MIR_p \geq MIR_{h1} \text{ y } MIR_p \geq MIR_{h2} \text{ y } \dots \text{ y } MIR_p \geq MIR_{hn} \quad (3)$$

Donde:

MIR_p : Tasa de información máxima para la cola padre.

$MIR_{h1}, MIR_{h2}, \dots, MIR_{hn}$: Tasa de información máxima para cada una de las enésimas colas hijo.

Una vez satisfecha todos los límites CIR el HTB ofrecerá el tráfico disponible adicional a la cola con más prioridad.

3.7.4 Web Proxy

Esta es una característica que ofrece el equipo de funcionar como servidor proxy para las conexiones http, incluso es posible instalar un servidor de cache o proxy externo y configurar el dispositivo para que lo gestione mediante alguna de sus interfaces Ethernet.

3.7.5 NAT

Por ser un enrutador ofrece el traslado de direcciones de red (NAT) por naturaleza, pero adicionalmente es posible crear reglas específicas de forma manual.

CAPÍTULO IV

CONFIGURACIÓN Y MANUAL

Para efectuar la configuración del equipo Mikrotik, se aplican criterios recomendados por el fabricante, formulados en pro de lograr el mejor desempeño del equipo, así como se hacen configuraciones de características generales y específicas, se sigue el esquema descrito a continuación:

- Identificación y renombramiento de interfaces.
- Asignación de direcciones y configuración de red.
- Configuración de servidor DHCP en red local.
- Configuración de hotspot para acceso inalámbrico.
- Identificación de flujos y marcado de paquetes.
- Establecimiento de velocidades de acceso y prioridades de colas de paquetes.
- Configuración de webproxy.
- Configuración de reglas de traslación de direcciones.

4.1 Detalle del esquema de configuración:

4.1.1 Identificación y renombramiento de interfaces:

Como primer paso se identifican físicamente las interfaces del dispositivo, posteriormente, se asocia un nuevo nombre en el programa de configuración a cada una de las interfaces identificadas, de acuerdo a la función que van a cumplir, ya sea tener el acceso a internet (WAN), controlar la red local (LAN), o manejar el acceso a través de la interfaz aire (Hotspot).

4.1.2 Asignación de direcciones y configuración de red:

Una vez nombradas las interfaces se realiza la configuración determinada para cada una, asignando una dirección IP fija a las interfaces LAN y Hotspot, y configurando la interfaz WAN según sea el caso (cliente DHCP o IP manual).

4.1.3 Configuración de servidor DHCP en red local:

Una vez establecida la dirección IP de la red local, se procede a configurar el servidor DHCP para ésta interfaz.

4.1.4 Configuración de hotspot para acceso inalámbrico:

Una vez establecida la dirección de red para el hotspot, se procede a configurar el servidor de portal captivo, en la configuración, por defecto, tiene la posibilidad de configurar un servidor DHCP para esta interfaz, se configuran los parámetros necesarios y posteriormente se hace un cambio en la plantilla que se usa para la identificación de los usuarios, haciendo uso de una página que se encontraba en uso en las radio bases, en ella se hace el envío de las credenciales necesarias para el inicio de sesión, por ello el usuario no necesita identificarse colocando un nombre de usuario y contraseña.

4.1.5 Identificación de flujos y marcado de paquetes:

En esta etapa se catalogan los flujos por varias características particulares.

La primera de ellas es por el contenido de las conexiones, el equipo tiene la capacidad de identificar en su contenido cadenas de caracteres, al momento de identificar, es posible marcar esta conexión para diferenciarla.

Una vez identificada la conexión se hace el marcado de paquetes de esa conexión para su posterior uso en el árbol de colas y brindar de esta forma un nivel de calidad de servicio.

Es importante destacar que el fabricante recomienda emplear esta estrategia (identificar conexiones y marcar paquetes), en vez de identificar paquetes individualmente y marcarlos, en virtud de que realizarlo de esta forma exigiría mayor cantidad de recursos en el CPU del dispositivo.

Otra característica usada para el marcado de paquetes, es la identificación de la cantidad de información de las conexiones, el equipo tiene la capacidad de identificar la cantidad de información que ha transmitido una conexión y catalogarla de acuerdo a ello.

Igualmente se identifican las conexiones y posteriormente se marcan los paquetes de estas conexiones.

Como último paso es necesario marcar todos los paquetes que no hayan sido marcados anteriormente, para evitar congestión no prevista en el árbol de colas, es necesario que todo el tráfico pase por éste.

4.1.6 Establecimiento de velocidades de acceso y prioridades de colas de paquetes.

Una vez identificados los diferentes flujos, se generan las colas de paquetes, y se le asigna una velocidad garantizada y máxima de transferencia para cada cola, así como un nivel de prioridad.

4.1.7 Configuración de webproxy

Se hace uso de la característica de webproxy del dispositivo para denegar el acceso a páginas, cuya dirección tengan cadenas de caracteres particulares, que puedan considerarse que manejan contenido sensible o no apto para el servicio, por ejemplo, páginas para adultos.

4.1.8 Configuración de reglas de traslación de direcciones

Una vez realizada la configuración y activación del servidor webproxy, el equipo deja de atender solicitudes HTTP en el puerto 80, por ello, se configura una regla de traslación de puertos desde el puerto 80 hacia el puerto configurado en el webproxy para que atienda solicitudes, logrando de esta forma un proxy transparente, adicionalmente hay que generar una regla para que el equipo no atienda las peticiones que se le hacen a través del puerto 80 por la interfaz de WAN, en virtud de

que estaría funcionando como un proxy público (al activar la opción de webproxy, aplica para todas las interfaces).

4.2 Manual de configuración

Para la creación del manual se toma en cuenta los siguientes aspectos:

- Público al que está dirigido
- Utilidad y alcance del manual

4.2.1 Público al que está dirigido

Se establece como público al que está dirigido el manual, el personal técnico de la Gobernación, suponiendo de esta forma que es un personal con avanzados conocimientos en la interacción con equipos de escritorio (PC), portátiles (laptops) operando bajo sistema operativo Microsoft Windows, y conocimientos básicos de redes.

4.2.2 Utilidad y alcance del manual

El manual está diseñado para únicamente efectuar la configuración completa del equipo, no está diseñado para realizar diagnóstico de fallas, así como tampoco cuenta con descripción de métodos o herramientas para el monitoreo y diagnóstico de la red.

CAPÍTULO V

CASOS DE ESTUDIO

A continuación se hace una descripción general de la experiencia vivida en las visitas técnicas a los nodos. Para hacer el diagnóstico de la red se usó el enfoque ascendente, verificando en primera instancia la operatividad de las capas inferiores y posteriormente haciendo pruebas hacia las capas superiores.

5.1 Caso de estudio, UNEFA Extensión Charallave

5.1.1 *Análisis preliminar*

Para efectuar un análisis preliminar de la radio base y tener una visión concreta de la configuración y disposición de los equipos instalados en el sitio, se revisó el informe de ingeniería proporcionado por la empresa para esta locación.

Al verificar el informe de ingeniería proporcionado por la empresa, se obtienen los siguientes datos

Tabla 2 Equipos instalados en la radio base de la UNEFA – Extensión Charallave [18]

ITEM	DESCRIPCIÓN	CANTIDAD
1	Lanpro LP-1522 802.11 b/g High Power 800mW External Antenna AP w/PoE	1
2	Lanpro LP-LB404 High Performance Quad WAN Load Balancer	1
3	Lanpro LP-NC1 Network Access Controller	1
4	Lanpro LP-G10 3GHz High Power Surge Arrester N-N Female Type Connector	3
5	Lanpro LP-SPL324 2.4GHz Indoor Splitter 3:1 N Female Type Connector	1
6	Lanpro LP-Panel2416 2.4GHz Outdoor Panel Antenna 120H 90A	3
7	Lanpro LP-PA2410 Outdoor Power Amplifier 1W 802.11 b/g 2.4GHz	3
8	Outdoor NEMA Box w/internal electricity	1
9	Lanpro 12U Rack	1

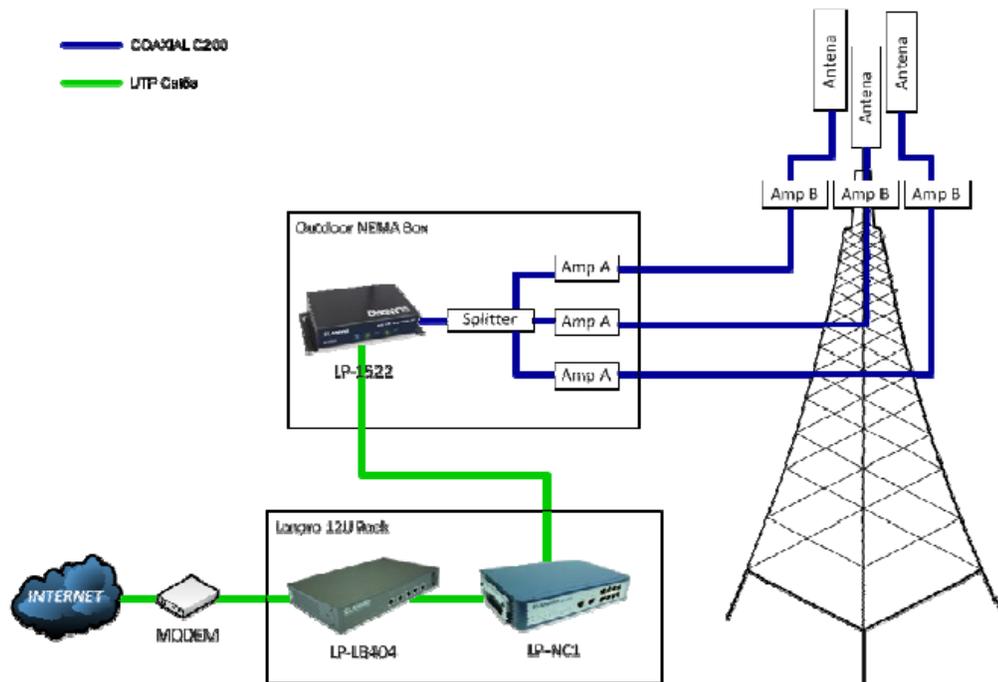


Figura 10 Disposición de los equipos de la Tabla 1 [18]

Una vez revisado el informe, se verifica con el personal de la Gobernación acerca del acceso a Internet en el sitio, determinando la existencia de un único acceso sin proyecciones a adquirir un segundo enlace. En función de eso, se recomendó la desinstalación del equipo Lanpro LP-LB404, en virtud de que su función principal es la de efectuar el balanceo de carga hasta un máximo de 4 enlaces hacia Internet, en estas condiciones no está desempeñando ninguna labor, únicamente una función de traslación de direcciones de red (NAT) innecesaria.

5.1.2 Análisis en el sitio

En el sitio haciendo uso del equipo portátil (laptop), se verifica la conectividad inalámbrica, logrando conexión con la red, se verifica la navegación, teniendo acceso al portal captivo de la radio base, se autentica para navegar y no se

tiene acceso hacia internet, se verifica la dirección IP que captura el equipo, encontrándose en el rango 192.168.2.0/24, se hace uso del comando “ping” a la puerta de enlace 192.168.2.254 y se tiene respuesta, se hace uso del comando “tracert” hacia la página de la Gobernación (www.miranda.gob.ve) y se observa que sólo se tiene respuesta en el primer salto.

Con este diagnóstico inicial se puede determinar que la interfaz aire de la radio base (punto de acceso, splitter, amplificadores, antenas) se encuentra operativa. El siguiente dispositivo en la ruta hacia Internet, según el diagrama de conexión, es el Lanpro LP-NC1, es el equipo que está cumpliendo la función de servidor DHCP, así como la de servidor de portal captivo.

Posteriormente al verificar el estado de los equipos en la instalación interna (rack), se pudo determinar que el equipo Lanpro LP-LB404 no se encontraba operativo, presentaba un funcionamiento errático en los leds del equipo (todos los leds indicadores de enlace físico de los puertos ethernet parpadean simultáneamente bajo un único patrón aleatorio).

Se efectúa la remoción del equipo Lanpro LP-LB404 y configuración del Lanpro LP-NC1 en la interface WAN para obtener dirección IP dinámica por DHCP, obteniendo dirección IP del proveedor y logrando tener acceso a Internet.

Posteriormente al hacer pruebas de navegación, se determinó que el equipo sufre una intermitencia de las mismas características a la diagnosticada en la radio base de la Biblioteca Pública en Curiepe (visitada previamente, documentado en el apartado “Otros casos de estudio”). La intermitencia se detecta con el equipo portátil, en principio, se logra conexión, pero al poco tiempo se desconecta y no se detecta la red, pasado un lapso de unos 5 segundos a 10 segundos se detecta de nuevo, se intenta conexión de nuevo y se logra, pero al cabo de unos 30 segundos (aproximadamente) se pierde la conexión y se repite el ciclo, no se logra verificar las condiciones de la instalación motivado a que la caja de intemperie y las antenas, se encuentran instaladas en una torre de aproximadamente 20 metros y no se disponía de

una escalera de esa altura ni con equipos de seguridad para subir improvisadamente por la estructura de la torre. Se presume que los equipos se encuentran afectados por la temperatura. El rango de temperatura de operación del equipo Lanpro LP 1522 se encuentra entre 0°C y 50°C, por ello se estima que existan altas probabilidades que la temperatura interna de la caja alcance y supere el valor máximo, producto de la incidencia directa de los rayos del sol, sumado a la temperatura disipada por el equipo, generada por su funcionamiento.

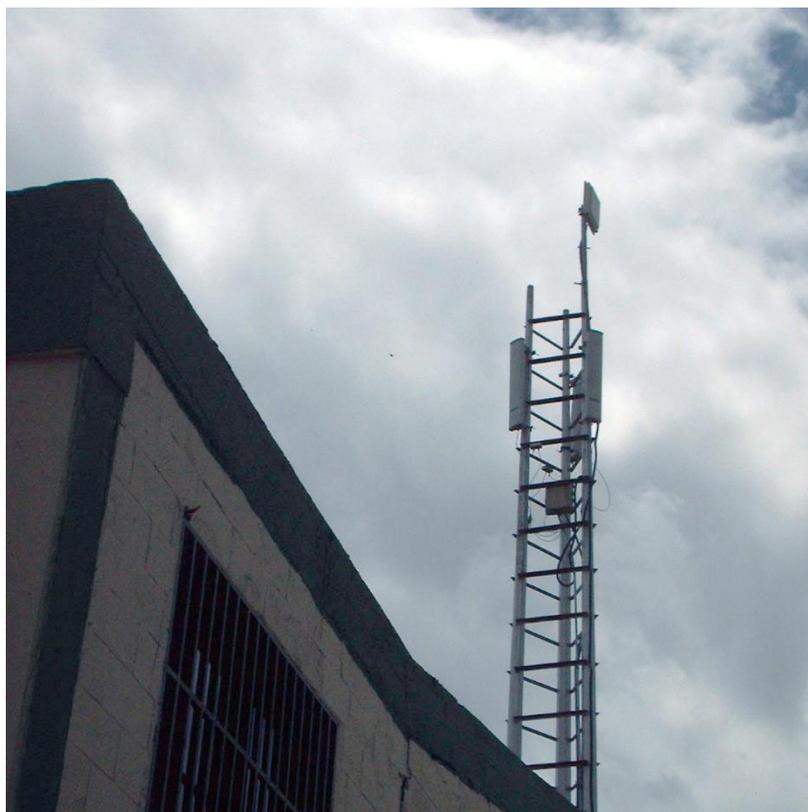


Figura 11 Aspecto de la instalación de las antenas en la UNEFA, extensión Charallave

Instalación eléctrica

Una vez verificada la operatividad del servicio se procede a chequear la instalación eléctrica, en función de determinar la existencia o ausencia de un sistema de puesta a tierra en la instalación. Al examinar el tablero de distribución de la sala en donde se encuentran instalados los equipos se pudo determinar la ausencia de una barra de tierra según lo establecido en el apartado 250 del Código Eléctrico Nacional.

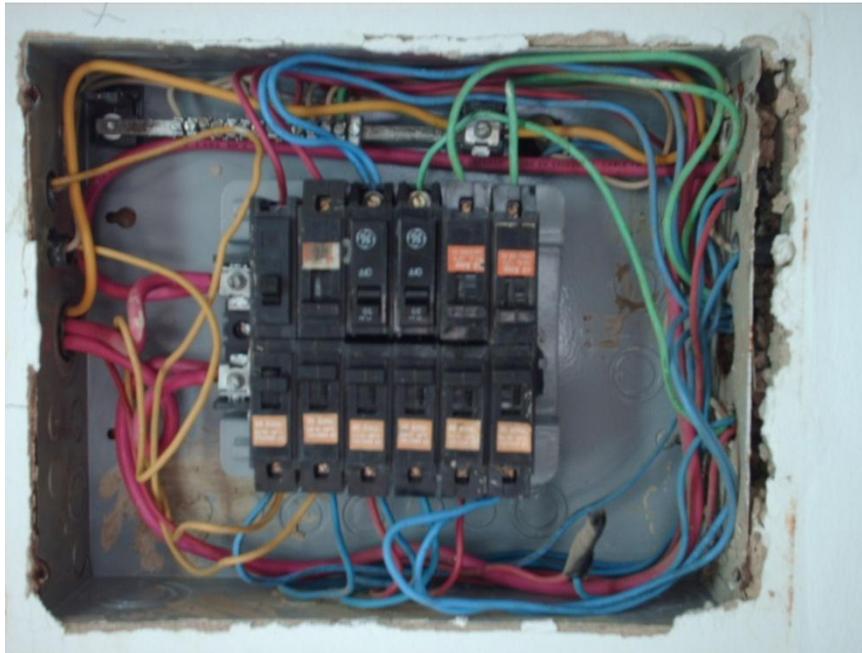


Figura 12 Detalle del tablero de protecciones para el circuito del rack en las instalaciones de la UNEFA, extensión Charallave.

Igualmente en la instalación de las antenas, se observa que tienen un dispositivo para conexión a tierra de la antena, igualmente se puede verificar que se encuentran conectados a la tubería EMT de la instalación eléctrica del edificio, no se logró determinar si ésta tubería se encuentra con una conexión apropiada a tierra

5.2 Caso de estudio, Biblioteca Pública Cúpira

5.2.1 Análisis preliminar

El análisis preliminar de esta radio base se apoyó en la revisión del informe de ingeniería proporcionado por la empresa que instaló los equipos, para tener clara la disposición de los equipos, así como su configuración.

Documentado en el informe de ingeniería aparecen los siguientes equipos como instalados en el sitio.

Tabla 3 Equipos instalados en la radio base de Cúpira [19]

ITEM	DESCRIPCIÓN	CANTIDAD
1	Lanpro LP-1522 802.11 b/g High Power 800mW External Antenna AP w/PoE	1
2	Lanpro LP-LB404 High Performance Quad WAN Load Balancer	1
3	Lanpro LP-NC1 Network Access Controller	1
4	Lanpro LP-G10 3GHz High Power Surge Arrester N- N Female Type Connector	3
5	Lanpro LP-SPL324 2.4GHz Indoor Splitter 3:1 N Female Type Connector	1
6	Lanpro LP-Panel2416 2.4GHz Outdoor Panel Antenna 120H 90A	3
7	Lanpro LP-PA2410 Outdoor Power Amplifier 1W 802.11 b/g 2.4GHz	3
8	Outdoor NEMA Box w/internal electricity	1
9	Lanpro 12U Rack	1

Igualmente, se verificó con el personal de la Gobernación qué tipo de servicios de conectividad particular es requerido en esta radio base, (como por ejemplo VPN, VoIP, FTP, etc.), determinando que no es requerido ningún servicio de conectividad especial para el uso de su personal, únicamente acceso a internet para la sala de tecnología y para el servicio de internet público.

Al revisar la información de la radio base documentada en el informe de ingeniería proporcionado por la empresa que realizó la instalación se puede observar la presencia de un equipo Lanpro LP-LB404. De la misma manera se indaga con el personal de la Gobernación, determinando que únicamente se cuenta con un enlace y no existen proyecciones de adquirir un segundo enlace. Se hace igualmente la recomendación de retirar el equipo en función de que no es necesario tenerlo allí operativo bajo estas condiciones.

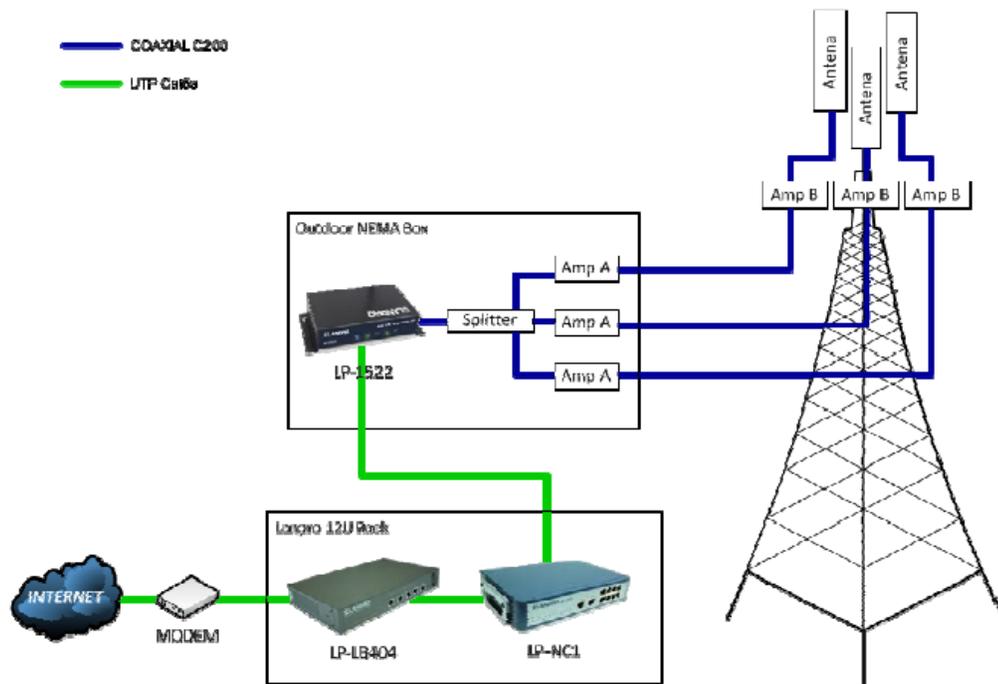


Figura 13 Disposición de los equipos en la Tabla 2 [19]

Es importante destacar que por información proporcionada por el personal de la Gobernación, ésta radio base sufrió una modificación en su instalación, en la cual se sustituyó el equipo Lanpro LP-NC1 por un Mikrotik RB493A.

5.2.2 Análisis en el sitio

Haciendo uso del equipo portátil (laptop), se verifican las redes inalámbricas en el entorno próximo a la biblioteca pública, determinando que no se está propagando el SSID de la red inalámbrica de la radio base. En primera instancia se verifica la caja de intemperie instalada en el mástil de la antena y se determina que los equipos se encuentran inoperativos por graves daños físicos. Se presume que sufrieron una sobretensión con un nivel de energía lo suficientemente alto para quemar y causar la fractura total de la cubierta de la fuente del Lanpro LP1522, y también quemar los inyectores de los amplificadores, tal como aparece reflejado en la figuras 15 y 16.



Figura 14 Detalle de caja de intemperie con equipos inoperativos.

Igualmente, la instalación eléctrica sufrió daños, como aparece reflejado en la figura 17, inutilizando el tramo de conductor desde el cajetín de distribución hasta la caja de intemperie, un tramo de aproximadamente 4,5 metros de longitud. Se sustituyó con cable calibre TWH AWG12 (el mismo calibre del cable instalado) y se recomendó la remoción del interruptor de suministro de energía hacia la caja de intemperie por la condición en la que se encuentra, como se puede observar en la figura 18 y 19.



Figura 15 Detalle de los equipos inoperativos, sustituidos en la radio base de Cúpira.

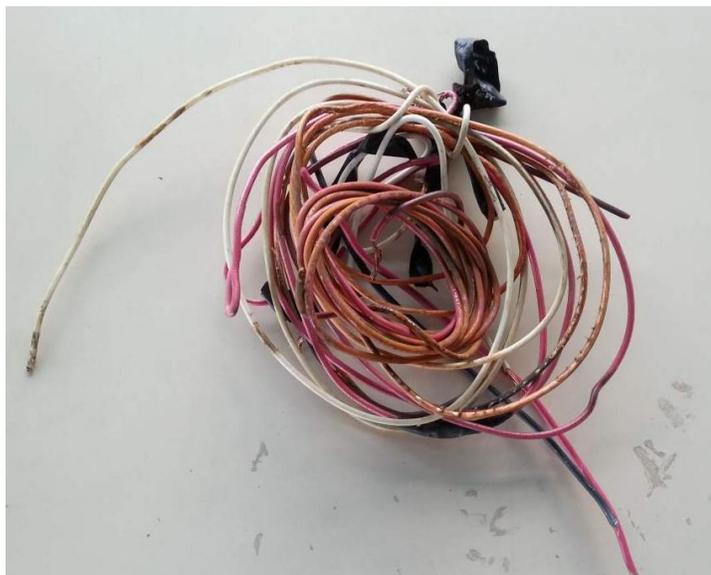


Figura 16 Detalle del cableado sustituido desde el cajetín de distribución hasta la caja de intemperie

En la Gobernación se contó con un conjunto de todos los equipos que se tienen instalados en las radio bases para hacer pruebas. En este sitio, para determinar la operatividad de los equipos, se sustituyeron la fuente de los amplificadores, los inyectores de los amplificadores y la fuente del LP1522. El Lanpro LP1522 no sufrió

daño aparente, se probó con una fuente de otro equipo similar y se verificó que estaba operativo, realizando la función de punto de acceso sin ninguna irregularidad.

Una vez sustituidos los equipos, se recuperó la operatividad de la interfaz aire de la radio base, detectando la red inalámbrica en el equipo portátil, en este sitio por estar desplegado un equipo Mikrotik no se realizaron más pruebas de conexión, directamente se procedió a realizar la configuración del equipo Mikrotik haciendo uso de sus características para brindar una calidad de servicio a los usuarios.



Figura 17 Detalle del cajetín de distribución e interruptor de energía hacia la caja de intemperie



Figura 18 Detalle del interruptor inoperativo.

El marcador de paquetes “mangle” se configuró para detectar distintos tipos de tráfico y hacer el correspondiente marcado de paquetes, para posteriormente realizar un árbol de colas y garantizar una calidad de servicio.

El criterio que se usó para la configuración se determinó en conjunto con el personal de la Gobernación, se explicaron las características y capacidades del equipo y una vez teniendo claro esto, se establecieron las siguientes reglas:

El marcado de los paquetes se puede hacer identificando una conexión, estableciendo su marca de conexión, y posteriormente marcando todos los paquetes de esa conexión, incluso se pueden crear varias reglas para detectar distintas conexiones, para posteriormente marcar a los todos los paquetes de un grupo de conexiones.

Es importante destacar que las marcas que se apliquen a conexiones son totalmente independientes de las marcas que se le apliquen a los paquetes, pudiendo tener el mismo nombre (ser la misma marca), pero al ser de elementos distintos, son marcas totalmente distintas.

Las reglas para el marcado fueron aplicadas en el mismo orden en el que se presentan a continuación.

Aplicar la marca “DNS” a los paquetes cuyo puerto de origen o destino sea el 53 en la interfaz WAN, para al momento de realizar el árbol de colas, resolver las consultas hacia los DNS sin tenerlas en cola con el resto del tráfico.

Aplicar la marca “DNS” a los paquetes cuyo puerto de origen o destino sea el 8291 en cualquier interfaz, para al momento de realizar el árbol de colas, darle prioridad al tráfico generado por motivo de configuración del equipo, en función de tener en un futuro, la necesidad de realizar alguna configuración con el servicio funcionando en el peor de los casos (todas las colas consumiendo su tasa de información comprometida), no se vea afectado el acceso a configurar el equipo.

Aplicar la marca “videos en línea” a los paquetes pertenecientes al tráfico proveniente de las páginas más populares de videos en línea, se crearon reglas para que el equipo detectara las conexiones cuyo contenido tuviera alguna de las siguientes cadenas de caracteres (sin distinción de mayúsculas o minúsculas):

- Youtube
- Vimeo
- Dailymotion
- Metacafe

Una vez detectada la conexión, efectuar el marcado de paquetes de esa conexión con la marca “videos en línea”.

Aplicar la marca “redes sociales” al tráfico proveniente desde las páginas de redes sociales más populares, se crearon reglas para que el equipo detectara las conexiones cuyo contenido tuviera alguna de las siguientes cadenas de caracteres (sin distinción de mayúsculas o minúsculas):

- Facebook

- Twitter
- Instagram
- Plus.google
- Pinterest
- Tumblr

Una vez detectada la conexión, efectuar el marcado de paquetes de esa conexión con la marca “redes sociales”.

Aplicar la marca “100k” a las conexiones en la interfaz WAN, con origen puerto 80 (tráfico http), cuya cantidad de información transferida se encuentre en el rango de 0Kb hasta 100Kb de tráfico, y posteriormente aplicar la marca “100K” a los paquetes de esas conexiones.

Aplicar la marca “100k-500k” a las conexiones en la interfaz WAN, con origen puerto 80 (tráfico http), cuya cantidad de información transferida se encuentre en el rango de 100Kb hasta 500Kb de tráfico, y posteriormente aplicar la marca “100k-500K” a los paquetes de esas conexiones.

Aplicar la marca “500k-1M” a las conexiones en la interfaz WAN, con origen puerto 80 (tráfico http), cuya cantidad de información transferida se encuentre en el rango de 500Kb hasta 1Mb, y posteriormente aplicar la marca “500-1M” a los paquetes de esas conexiones.

Aplicar la marca “>1M” a las conexiones en la interfaz WAN, con origen puerto 80 (tráfico http), cuya cantidad de información transferida se encuentre en el rango de 500Kb hasta 1Mb, y posteriormente aplicar la marca “>1M” a los paquetes de esas conexiones.

Aplicar la marca “otras conexiones” a las conexiones que no hayan sido marcadas por ninguna de las reglas anteriores, y posteriormente aplicar la marca “otras conexiones” a los paquetes de esas conexiones, esta configuración es necesaria

para encolar el tráfico restante, de no estar marcado y asignado en el árbol de colas, se tendría este flujo de tráfico en paralelo con el árbol de colas.

Una vez efectuado el marcado de paquetes, se procede a realizar el árbol de colas para brindar calidad de servicio, se realizó de la siguiente forma:

Tabla 4 Valores de prioridad de marcas de paquetes en árbol de colas, CIR y MIR en % del enlace disponible

Prioridad	Marca de paquetes	CIR	MIR
1	DNS	10%	90%
2	100k	15%	90%
3	Redes Sociales	10%	90%
4	100k-500k	15%	90%
5	Videos en línea	10%	90%
6	500k-1M	10%	90%
7	>1M	10%	90%
8	Otras conexiones	20%	90%

Posteriormente se efectuó la configuración del webproxy del equipo mikrotik, para filtrar las páginas cuya dirección tengan las siguientes cadenas de caracteres (sin distinción de mayúsculas o minúsculas):

- Porn
- Sex
- XXX
- Naked
- Gay

Las solicitudes detectadas con este filtro, son direccionadas a la página oficial de la Gobernación (www.miranda.gob.ve).

Instalación eléctrica

Una vez recuperada la operatividad del servicio, se chequea la instalación eléctrica para determinar la instalación de puesta a tierra en el sitio, según lo

establecido en el Código Eléctrico Nacional, verificando en el tablero principal la ausencia de una barra de conexión a tierra, como se puede apreciar en la figura 20.



Figura 19 Tablero del circuito de los equipos de la radio base

Una vez activo el webproxy, el equipo deja de atender solicitudes de los clientes en el puerto 80, por lo que es necesario crear una regla en el NAT del equipo para redirigir todas las solicitudes que recibe en el puerto 80, hacia el puerto 8080, puerto de escucha del webproxy.

5.3 Otros casos de estudio

Adicionalmente a las visitas de las radio bases objeto de estudio del presente proyecto, por disposición de tiempo se logró visitar un total de 10 radio bases adicionales, todas implementadas bajo el mismo esquema de las radio bases estudiadas anteriormente, (8 implementadas con equipos Mikrotik y 2 implementadas con equipos Lanpro), no se hace una documentación detallada de cada visita por estar fuera del alcance del presente trabajo, únicamente se documentan las situaciones

particulares que se consideran necesarias y, adicionalmente, son objeto de formulación de recomendaciones.

A continuación se presenta el cronograma del total de visitas realizadas.

Tabla 5 Listado de fechas de las visitas e instituciones visitadas

Fecha	Institución	Ubicación
13-jun	BP Juan del Rosario Blanco	Curiepe
13-jun	BP Don Luis Correa	Higuerote
18-jun	BP Lino Gallardo	Ocumare del Tuy
18-jun	U.E.E. Carmen Ruiz	Charallave
18-jun	UNEXPO - Extensión Charallave	Charallave
25-jun	BP Cecilio Acosta	Los Teques
16-jul	BP Cúpira	Cúpira
18-jul	BP Francisco de Miranda	Río Chico
25-jul	BP Las Minas	San Antonio de los Altos
06-ago	BP Tacarigua	Tacarigua
07-ago	BP Don Luis y Misia Virginia	Guatire
07-ago	BP Misia Ana de Infante	Petare

Es importante destacar que en todas las visitas, el equipo Lanpro LB404 se encontraba inoperativo, siendo en algunos casos, la única falla que se presentaba en el sitio, realizando el retiro y configurando el equipo siguiente aguas abajo para tener acceso desde el proveedor de internet, se recuperaba la operatividad del nodo.

Una situación particular sucedió en la radio base ubicada en Curiepe, en el que nos informo el personal operativo de la biblioteca que de día el servicio inalámbrico no funcionaba, pero de noche sí, se verifica con el equipo portátil y se logra conexión, pero al poco tiempo se desconecta y no se detecta la red, pasado un lapso de unos 5 segundos se detecta de nuevo, se intenta conexión de nuevo y se logra, pero al cabo de unos 30 segundos se cae la conexión y se repite el ciclo. Al tener clara la situación que está sucediendo, se procedió a verificar la interfaz aire, se abre la caja de intemperie y se percibe que los equipos están a una temperatura elevada, por no disponer del equipo adecuado, no se logra determinar la temperatura interna de la caja, el equipo con mayor susceptibilidad a alta temperatura es el Lanpro LP 1522, teniendo una temperatura máxima de operación de 50°C. Se presumen altas

probabilidades de que la caja alcance y supere este valor de temperatura, como consecuencia de no estar provista con aperturas de ventilación, sumado el calor propio de los equipos por su operación y como factor de mayor influencia la incidencia directa de los rayos del sol, se supone que por ésta situación es que tiene funcionamiento errático en el día y durante la noche si funciona con normalidad, al no tener la influencia del sol y bajar la temperatura interna de la caja.

Es importante destacar que los equipos no están diseñados para trabajar a la intemperie, por ello se resguardan en una caja hermética que les brinde la protección necesaria para poder desplegarlos en el mástil del arreglo de antenas.

Igualmente se considera prudente mencionar que no se cuenta con un registro de incidencias que indique la fecha desde la cual se genera esta irregularidad.



Figura 20 Aspecto de la instalación externa en la radio base de la biblioteca pública en Curiepe

CONCLUSIONES

El desarrollo del presente trabajo permitió asistir a la Gobernación del Estado Miranda en el diagnóstico de la situación operativa de 12 radio bases en las que se implementó el servicio de internet inalámbrico público “Miranda WIFI”, logrando recuperar la operatividad de las que se encontraban inoperativas e implementando un mecanismo de calidad de servicio en las que se encontraban desplegadas con equipos Mikrotik.

Como aporte más relevante se tiene la recuperación de la operatividad del servicio, el cual en sitios remotos del estado Miranda, es el único enlace en donde se brinda acceso a internet al público en general y sobre todo a las salas de tecnologías de las bibliotecas, sitios en los cuales dentro de sus funciones, tienen programado la ejecución de cursos y talleres de formación e instrucción para el público en general.

Igualmente se considera aporte importante la transferencia tecnológica que se hace hacia la Gobernación, con el manual de configuración de los equipos Mikrotik, desarrollado en el presente trabajo, motivado a que permite la independencia de la Gobernación al momento de tener la necesidad de reconfigurar completamente algún equipo. Así como la experiencia del personal de la Gobernación que asistió en las visitas, en virtud de que se llevan consigo los criterios para el diagnóstico y resolución de las fallas que afectaban los nodos que se encontraban inoperativos, así como conocimientos adicionales de las dudas y situaciones particulares que fueron aclaradas y resueltas en el sitio.

Por último se considera un aporte significativo las recomendaciones, generadas en función de lograr la operatividad ininterrumpida del servicio, mejorar el control a nivel de contenido y garantizar las condiciones de protección eléctrica, para prolongar la vida útil de los equipos, así como brindar el servicio al mayor número de usuarios simultáneos, sin hacer desperdicio de los recursos.

RECOMENDACIONES

Una vez finalizado el trabajo, se considera apropiado realizar las siguientes recomendaciones en función de lograr una operatividad ininterrumpida del servicio, así como una prolongada vida útil de los equipos:

La sustitución de las cajas de intemperie por unas más apropiadas, (más grandes) para evitar que la manipulación y disposición de los equipos no sea crítica y los cables portadores de señal de radio frecuencia, no sufran daños por curvaturas pronunciadas.

La determinación de la temperatura de operación en horas del día en las que se presente intermitencia en el servicio, y de ser necesario una protección a las cajas expuestas a la intemperie, con un techo que les brinde sombra, para evitar la incidencia directa del sol y evitar altas temperaturas dentro de la caja generada por ésta situación.

Un estudio de los medios de transmisión, en específico de las guías de ondas, para verificar su actual estado, para verificar la operatividad de todos los sectores de las radio bases, motivado a que, por condiciones de las dimensiones de las cajas, y su manipulación, hayan podido sufrir daños que afecten sus propiedades y características, y en consecuencia, pérdidas en la interfaz de aire y posible daño a largo plazo de los equipos de radio frecuencia.

La instalación de un sistema de puesta a tierra según lo establecido en el Código Eléctrico Nacional en su apartado 250, bajo las recomendaciones de la norma IEEE 81 para la medición y de la norma IEEE 142 para el diseño.

Diseño e instalación de un sistema de protección contra descargas atmosféricas, tanto en las antenas como en la acometida y alimentación de los equipos.

La sustitución de los equipos Lanpro NC-1 por dispositivos basados en RouterOS de Mikrotik, por la gran flexibilidad que ofrecen en el control de calidad de servicio.

Realizar un estudio del grado de utilización de los equipos Lanpro LP1522, para determinar la cantidad máxima de usuarios y de tráfico que logran manejar simultáneamente, y de ser necesario, implementar en las radio bases un punto de acceso por cada antena, en función de evitar la aparición de un cuello de botella que puede presentarse a nivel de la interfaz aire de la radio bases.

Hacer un estudio y evaluación de las de políticas de calidad de servicio implementadas, y de ser necesario, formular nuevas propuestas y ponerlas en producción.

La implementación de un servidor de cache en las radio bases implementadas con equipos Mikrotik (como por ejemplo Thundercache o Squid), en función de que los equipos toleran esta configuración y esto reduciría el tráfico hacia internet proporcionando mejora en la velocidad de navegación, tanto para los usuarios que navegan en el caché como en los usuarios que acceden hacia internet.

Disposición de personal calificado en la Gobernación, en el área de telecomunicaciones y redes, o en su defecto, la capacitación del personal de soporte técnico actual para el diagnóstico y resolución de fallas en las radio bases instaladas, así como llevar un registro de incidencias y fallas, en el que se refleje fechas, diagnósticos y acciones tomadas, para recuperar la operatividad del servicio, y por último se documente estado en el que se encuentran las radio bases al final de la jornada del personal técnico.

El uso de un servicio de DNS seguro como OpenDNS, en función de que el control de contenido inapropiado, mediante el filtrado de cadenas de caracteres en la dirección del servidor solicitado, es poco fiable, en virtud de que pueden existir enlaces o páginas con contenido sensible o no apto para el servicio, que no necesariamente tengan alguna de estas cadenas en su dirección, mientras que el

control de contenido mediante el uso de DNS seguros, es mucho más fiable, adicionalmente a la implementación de estos servidores, es necesario bloquear tráfico hacia cualquier otro servidor de DNS, para garantizar que todos los usuarios del servicio, necesariamente hagan uso de los servidores DNS configurados.

REFERENCIAS BIBLIOGRÁFICAS

- [1] Wikipedia “Wikipedia” <<http://es.wikipedia.org/wiki/Wikipedia>> Consultado [2013].
- [2] Arias, Fidas G. *Mitos y errores en la elaboración de Tesis y proyectos de investigación*, (Libro).—Caracas: Venezuela: Ed. Episteme C.A. p35-36.
- [3] *Sistemas de telecomunicación II*. Ligia Silombria. Apuntes de clases: [2011].
- [4] *Sistemas de Telecomunicacion III*. Jorge Fernández. Apuntes de clases: [2012].
- [5] *Redes de datos basadas en TCP-IP*. Carlos Moreno. Apuntes de clases: [2012].
- [6] McMaster, Donna. McCloghrie, Keith. *Definitions of Managed Objects for IEEE 802.3 Repeater Devices*. IETF RFC1368: Octubre 1992.
- [7] Cisco Networking Academy *CCNA Exploration 4.0 Acceso a la WAN*, Cisco Systems, 2007-2008.
- [8] Shenker, S. Wroclawski, J *General Characterization Parameters for Integrated Service Network Elements* IETF RFC2215: Septiembre 1997.
- [9] Wroclawski, J. *Specification of the Controlled-Load Network Element Service* IETF RFC2211: Septiembre 1997.
- [10] Blake, S. Black, D. Carlson, M. Davies, E. Wang, Z. Weiss, W. *An Architecture for Differentiated Services* IETF RFC2215: Diciembre 1998.
- [11] Lanpro *Antenas Sectoriales de 2.4 GHz* Manual del fabricante.
- [12] Lanpro *LP-1522 Punto de Acceso/Router con tecnología POE* Manual del fabricante.
- [13] Lanpro *Amplificadores RF 2.4 GHz, Manual 123*. Manual del fabricante

- [14] Lanpro *Splitter LP-SPL324* Manual del fabricante.
- [15] Lanpro *Balanceador de Cargas LP-LB404 de LanPro*. Manual del fabricante.
- [16] Lanpro *LP-NC1 Manual 123*. Manual del fabricante.
- [17] Mikrotik *RouterBOARD 493 Quick Setup Guide and Warranty Information*. Manual del fabricante.
- [18] Dávila, Dimas. Aldamiz, Jean P. *Ingeniería de detalle, instalación y comisionamiento* (Informe instalación UNEXPO) MCL Smart Solutions: 2011.
- [19] Dávila, Dimas. Aldamiz, Jean P. *Ingeniería de detalle, instalación y comisionamiento* (Informe instalación BP Cúpira) MCL Smart Solutions: 2011.

BIBLIOGRAFÍA

Tanembaun, Andrew S. Redes de computadoras. 4ta. Ed. México: Pearson Education, 2003.

Mikrotik WIKI <http://wiki.mikrotik.com/wiki/Main_Page> [Consultado 2013]

FONDONORMA (NTF 200:2009) Código Eléctrico Nacional—Caracas: Comité de Electricidad. 998p

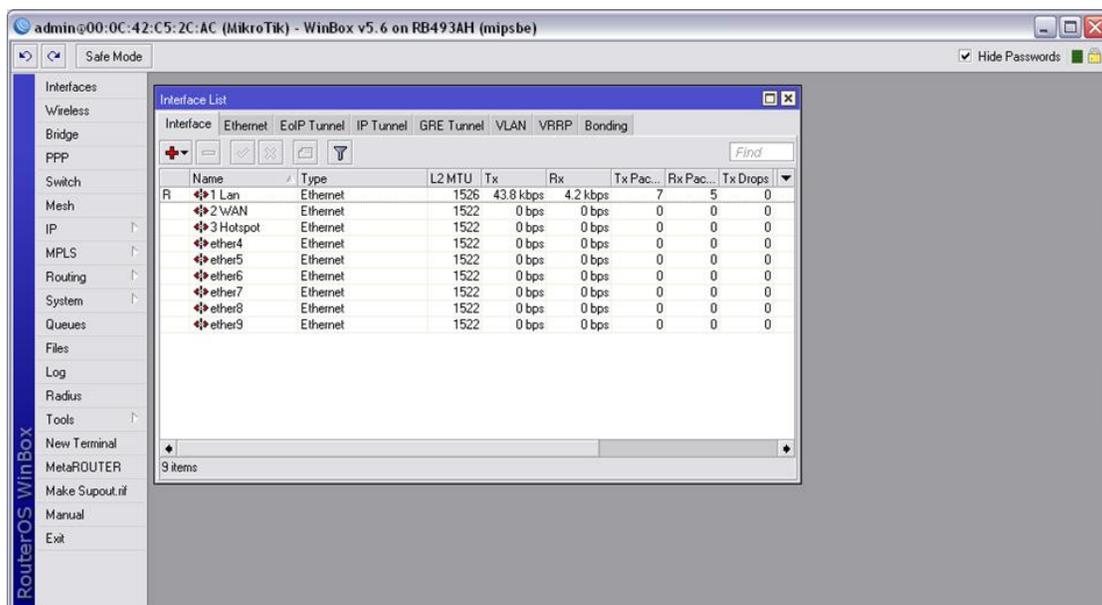
IEEE 81 (STD IEEE 81-1983) IEEE Guide for Measuring Earth Resistivity, Ground Impedance, and Earth Surface Potentials of a Ground System. Nueva York: The Institute of Electrical and Electronics Engineers.

IEEE 142 (STD IEEE 142-2007) IEEE Grounding of Industrial and Commercial Power Systems. Nueva York: The Institute of Electrical and Electronics Engineers.

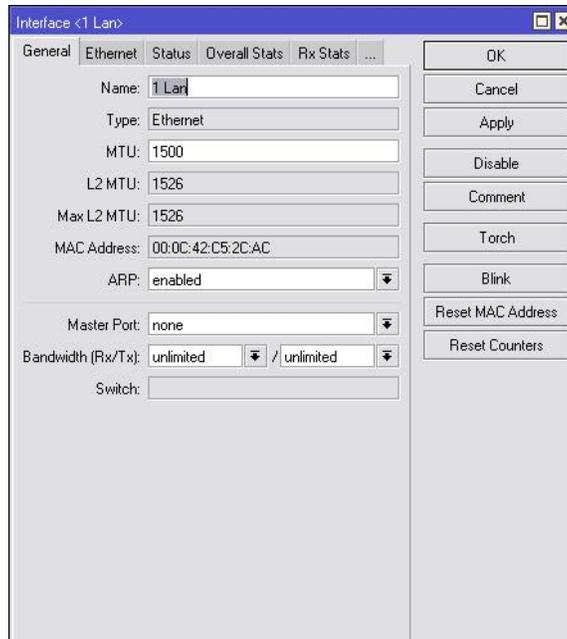
Manual de configuración para equipos basado en Sistema Operativo RouterOS

Para acceder a configurar algún equipo provisto del sistema operativo RouterOS, es necesario hacerlo desde un terminal mediante el programa Winbox (se puede descargar desde la página del fabricante www.mikrotik.com), el cual tiene una apariencia como la siguiente, provisto con un barra de menú de opciones ubicada a la derecha, incluso algunas opciones desplegables referentes a algunos apartados.

1. Como primer paso se establecen los nombres de las interfaces, para evitar confusiones y tener mejor manejo del equipo posteriormente en las demás opciones, se puede acceder al apartado de interfaces en el menú directamente

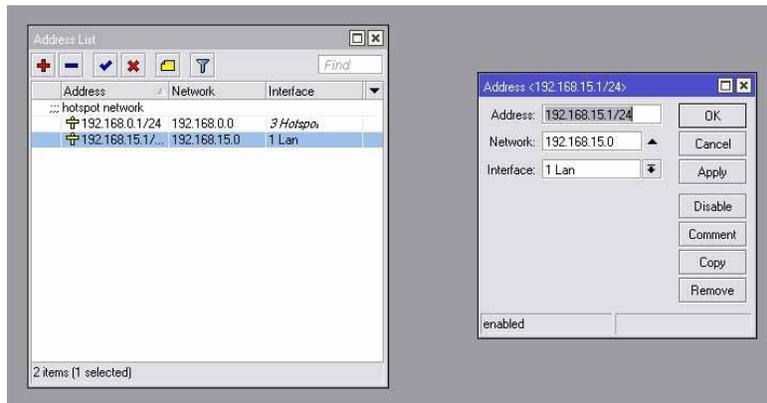


2. Se determinan cuales son las interfaces Ethernet que vamos a usar y su función, una vez decidido esto, al hacer doble click en una de ellas, se observa una ventana como la siguiente:



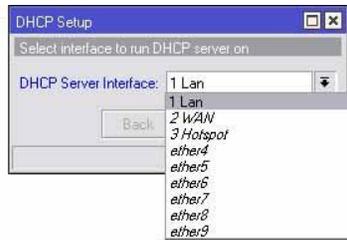
3. Se asigna el nombre determinado para cada interface y se acepta, se repite para las demás interfaces que se van a usar (Wan para la interfaz Ethernet 1, Lan para Ethernet 2 y HotSpot para el Ethernet 9).

4. Una vez nombrada las interfaces se asignan las direcciones ip correspondientes, en el menú IP>Address List, se hace click en el símbolo "+" ubicado en la parte superior y en la ventana que se despliega la siguiente ventana, se coloca la dirección ip del equipo con la máscara de subred en decimal para la red local 192.168.88.1/24, la dirección de la red 192.168.88.0 y se selecciona en el menú desplegable la interface "Lan"

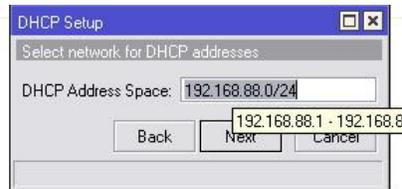


5. Se acepta en esta ventana y cerramos la anterior.

6. A continuación se configura el servidor DHCP para la interfaz LAN, se dirige a la opción IP>DHCP Server, se hace click en la opción "DHCP Setup" en la ventana que se abre, se observa una ventana como la siguiente, se selecciona la interfaz "Lan"

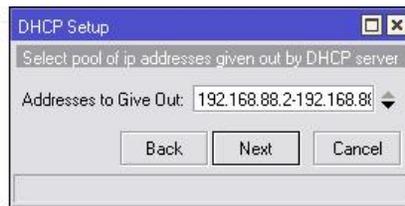


7. Posteriormente se hace click en siguiente, en la ventana a continuación se configura el espacio de direcciones IP 192.168.88.0/24



8. Se hace click en siguiente y se configura la puerta de enlace que otorgará el servidor DHCP, le asignamos 192.168.88.1

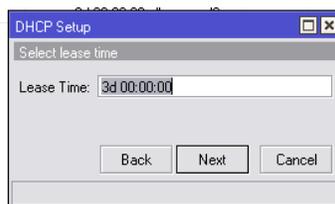
9. En la ventana siguiente se coloca el rango de direcciones en el que va a otorgar direcciones el servidor a los clientes



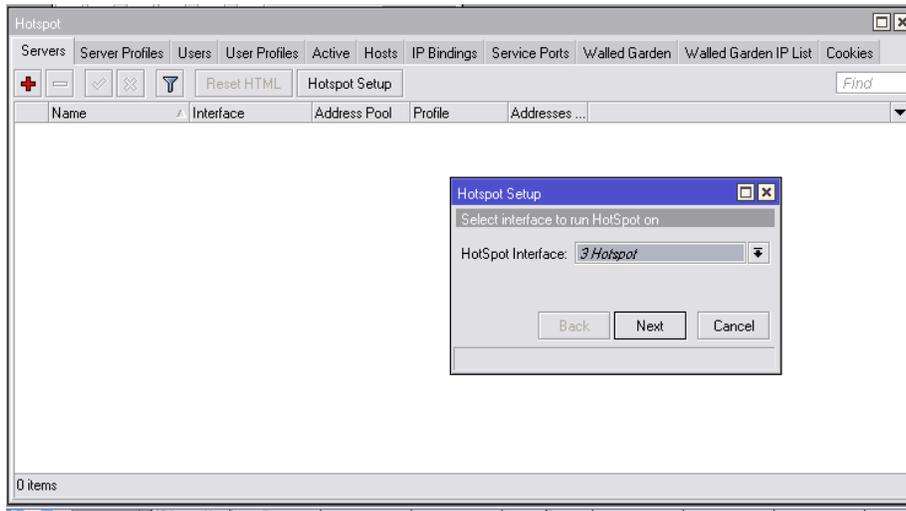
10. Se hace click en siguiente y se configuran las direcciones de servidores DNS que otorgara el servidor DHCP:



11. Se configura la duración de la concesión de dirección IP en 30 minutos

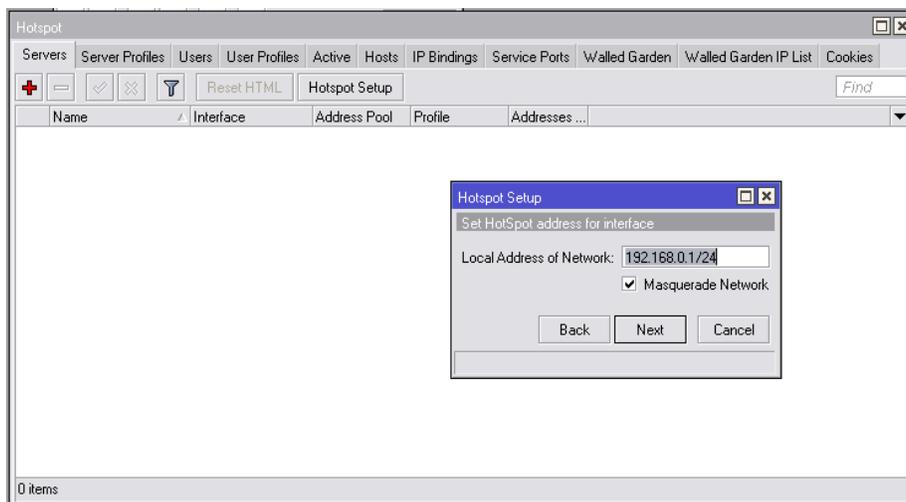


12. Se accede al apartado Hotspot en el menú IP, en la ventana que se despliega, se hace click en “Hotspot Setup”

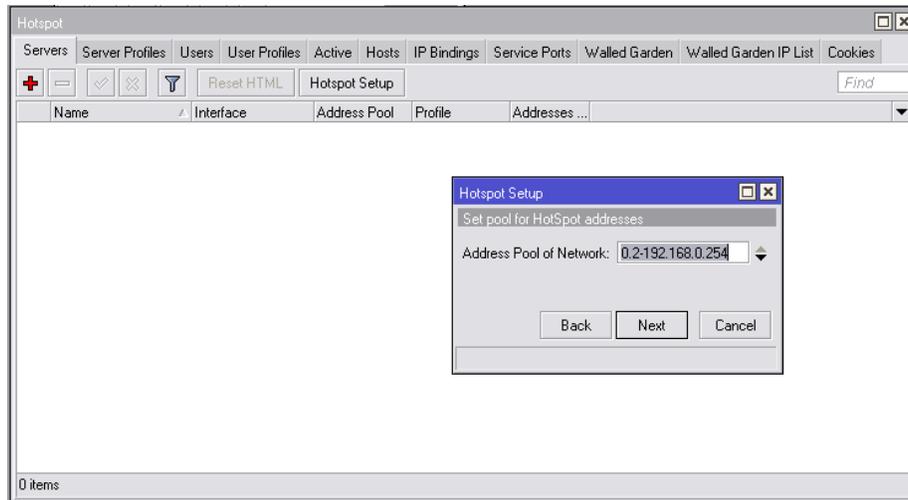


13. Se selecciona la interfaz en donde va a funcionar el portal captivo “Hotspot” (previamente nombrada en el paso 1) y se hace click en siguiente.

14. En la siguiente ventana se asigna la dirección ip y mascara de subred del servidor hotspot, se hace click en siguiente una vez establecida:

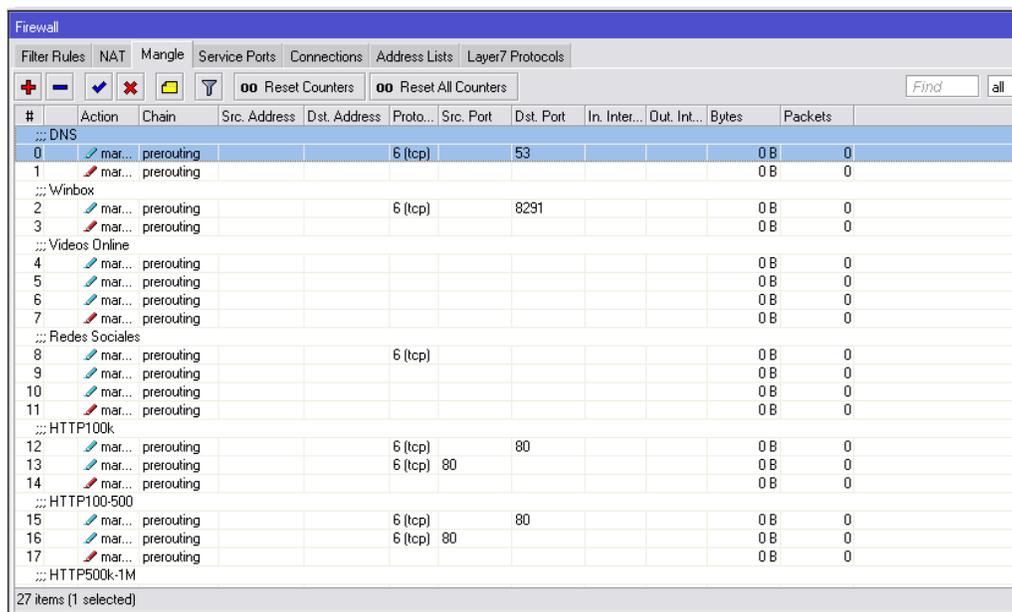


15. En la siguiente ventana se asigna el rango de direcciones IP a entregar por el servidor DHCP en la interfaz del Hotspot, una vez configurada, se hace click en siguiente:

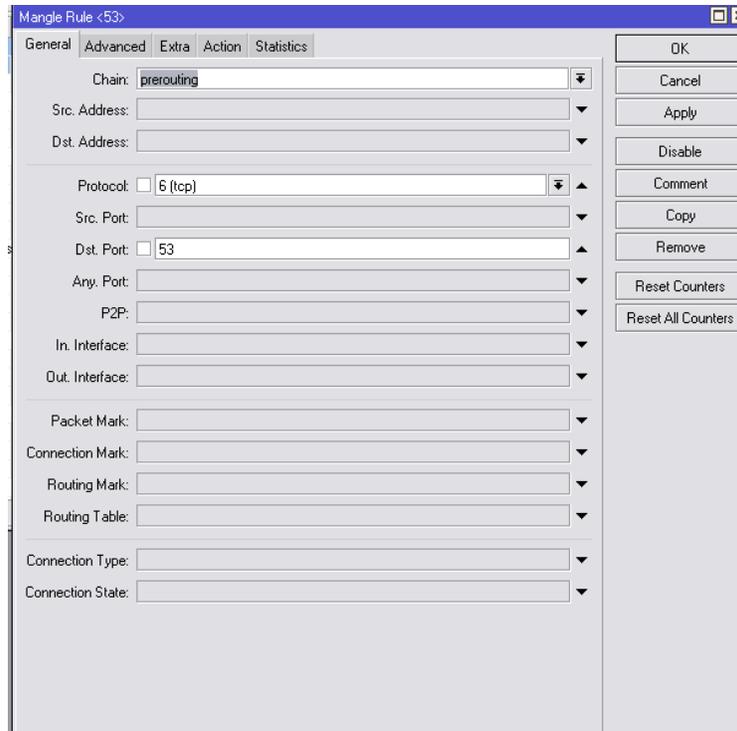


16. Se hace click en siguiente y de esta manera se finaliza la configuración del hotspot.

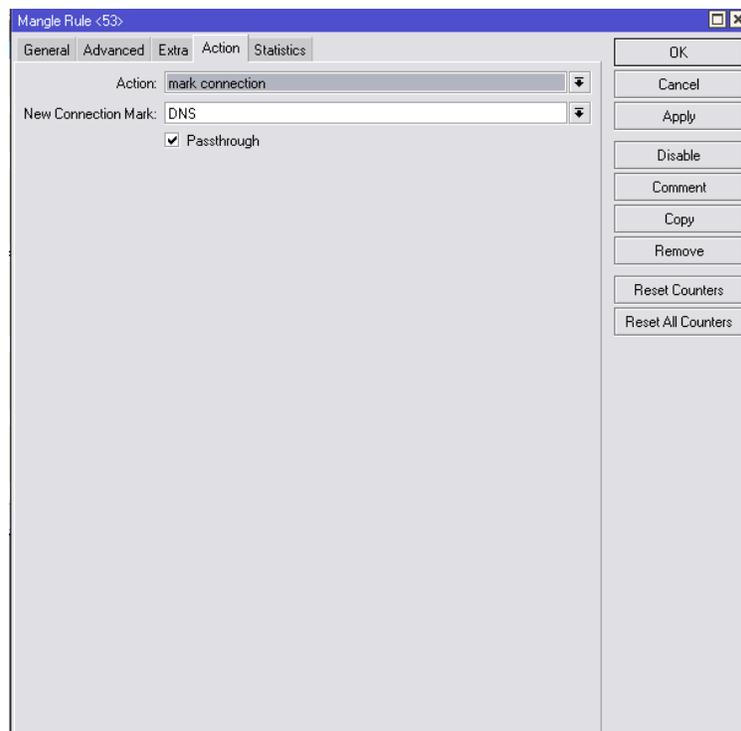
17. Se dirige al apartado "Firewall" en el menú "IP", posteriormente a la pestaña "Mangle":



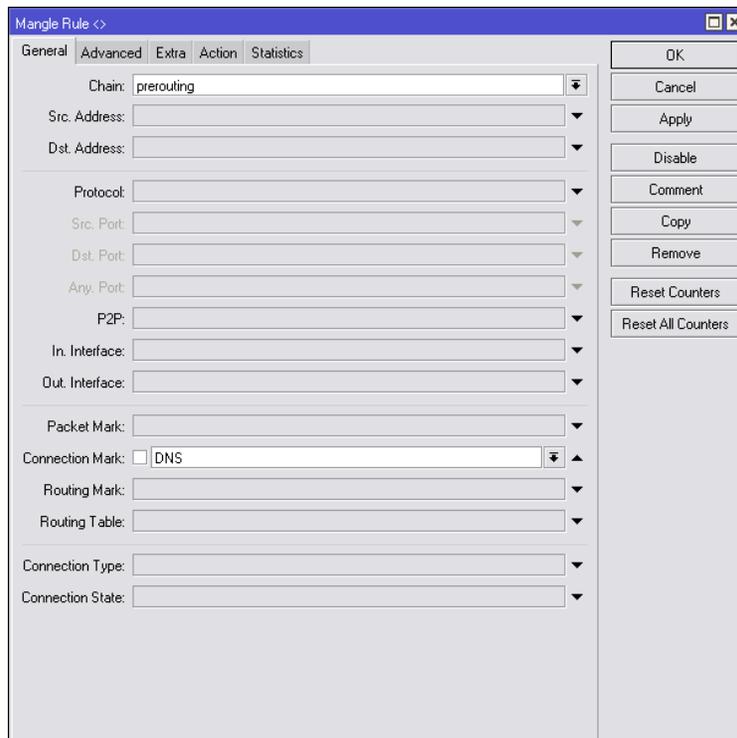
18. Se hace click en el símbolo "+" ubicado en la parte superior izquierda, se desplegara una ventana como la siguiente



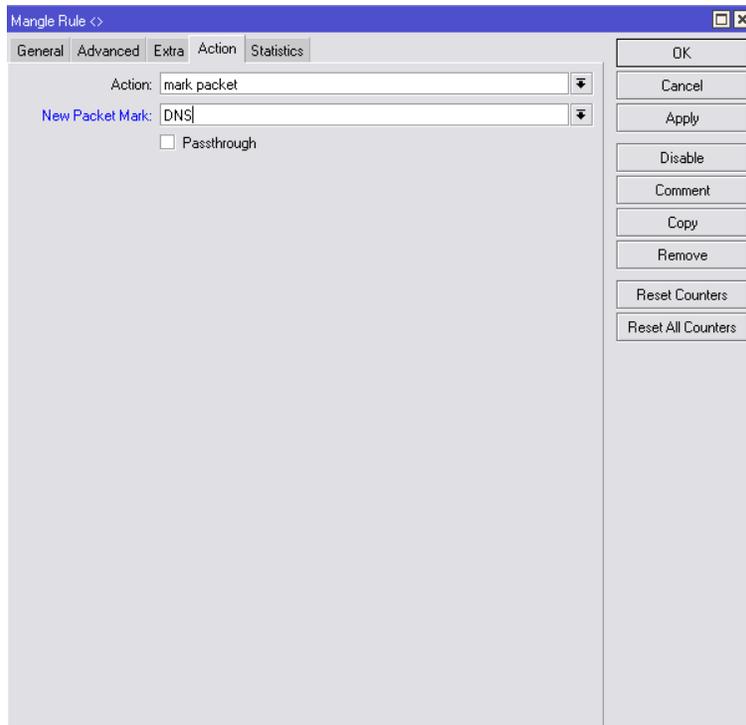
19. Se selecciona en el campo “Chain” la opción “prerouting”, en el campo “Protocol” la opción “6(tcp)”, en el campo “Dst Port” se escribe “53” y se dirige a la pestaña “action”, se observa una ventana como la siguiente



20. En acción se selecciona “Mark connection” y aparecerá el campo “New connection mark”, en este nuevo campo se coloca “DNS” y se deja la opción “passthrough” habilitada, se hace click en “Ok”.
21. Se repite el paso 18 y 19 pero en el campo “Dst Port” se escribe el numero 8291.
22. Se hace click en “+” para generar una nueva regla:

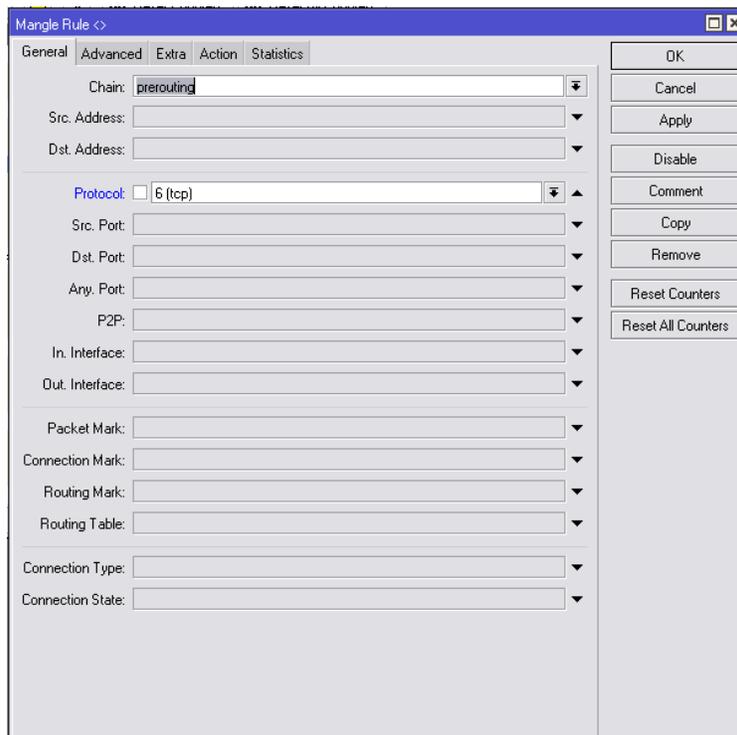


23. Se selecciona en el campo “chain” la opción “prerouting” y en “Connection Mark” se selecciona “DNS” y se dirige a la pestaña “Action”

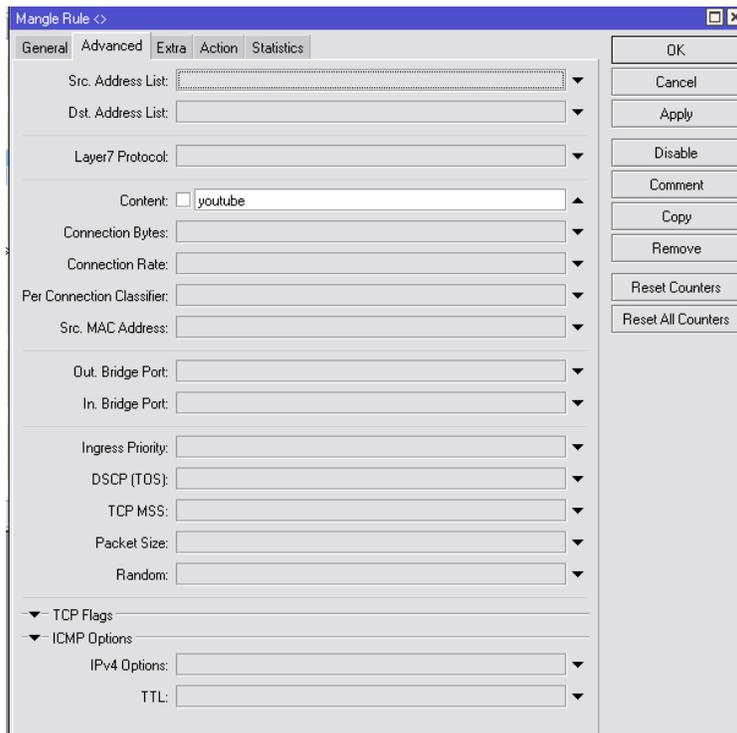


24. En esta pestaña en el campo "Action" se selecciona la opción "Mark Packet" y en el campo "New Packet Mark" se escribe "DNS", la opción "Passthrough" se deshabilita.

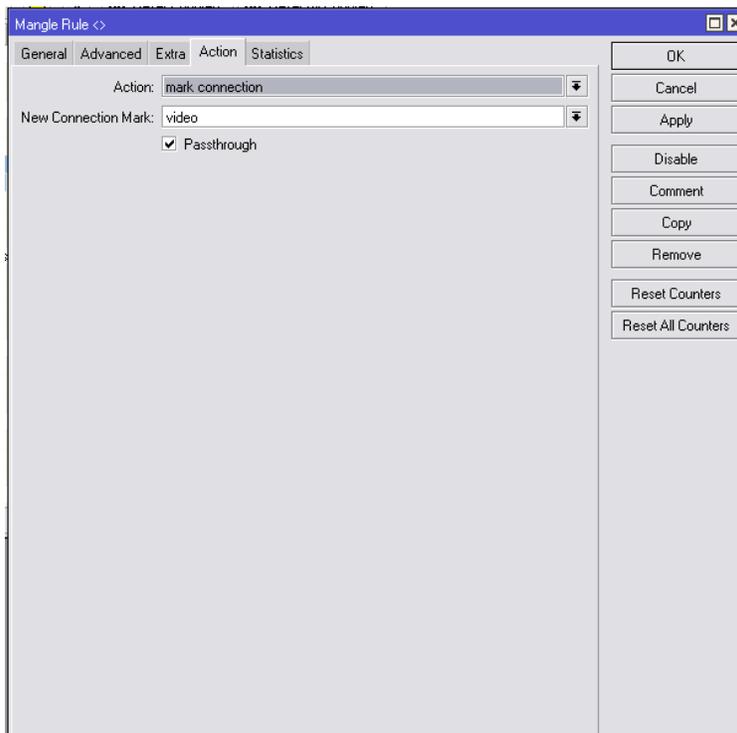
25. Se hace click en "+" para generar una nueva regla, en el campo "Chain" se selecciona la opción "prerouting", en el campo "Protocol" se selecciona "6 (tcp)" y se dirige a la pestaña "Advanced"



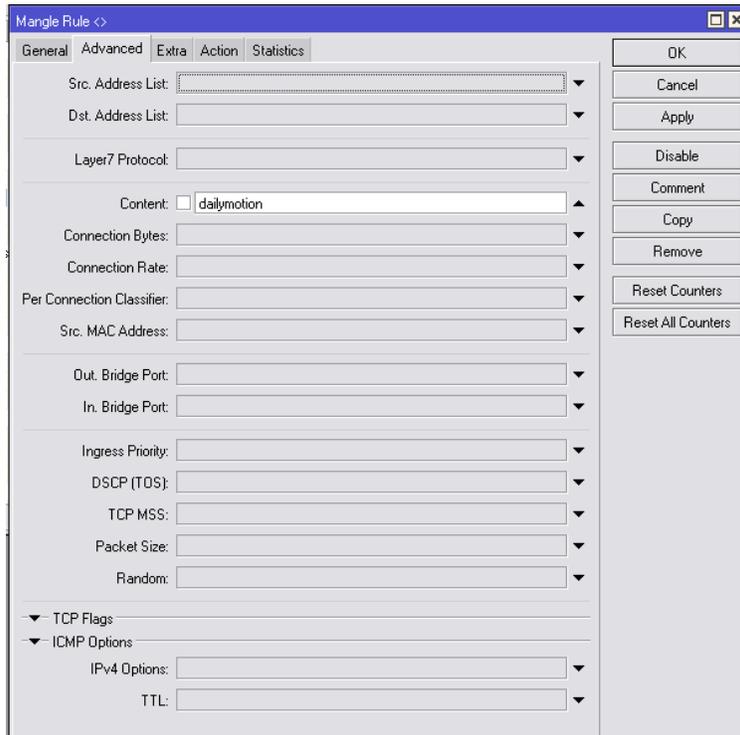
26. En la pestaña “Advanced” en el campo “Content” se escribe “youtube”



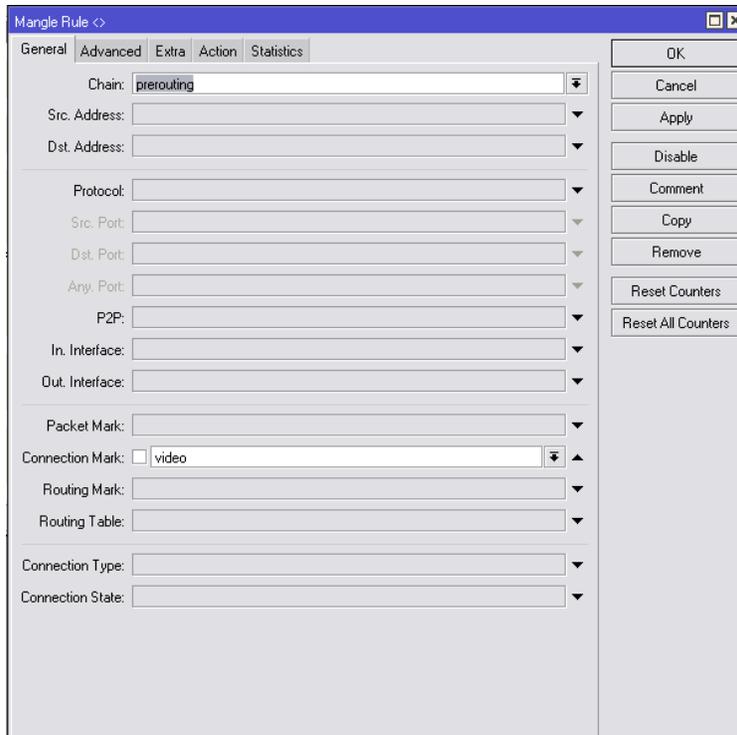
27. Posteriormente se dirige a la pestaña “Action”, en el menú “Action” se selecciona “Mark Connection” y en el campo “New Connection Mark” se escribe “video”, se deja habilitada la opción “Passthrough”, se hace click en “OK”.



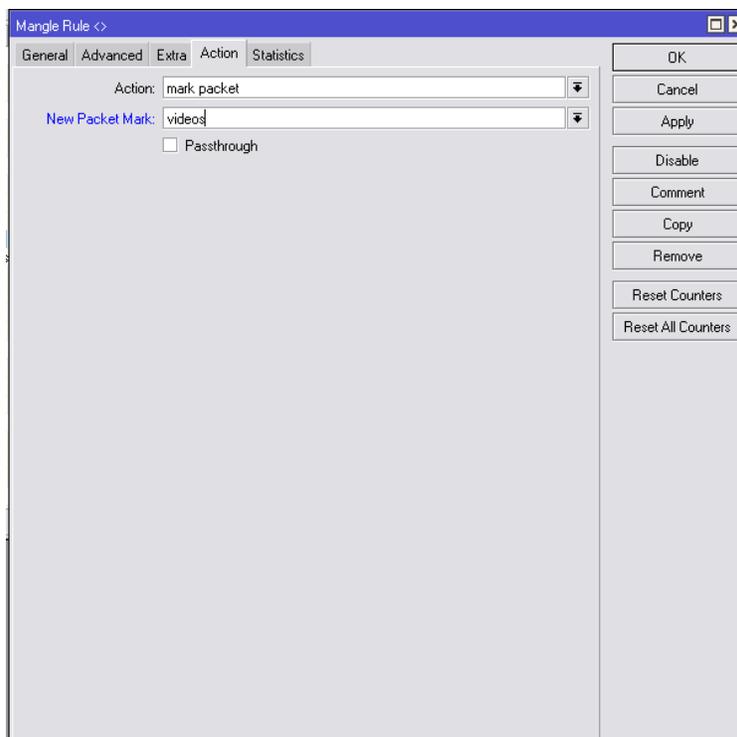
28. Se repite el paso 25
29. Se repite el paso 26 pero en el campo "Content" se escribe "daylimotion"



30. Se repite el paso 27.
31. Se repite el paso 25.
32. Se repite el paso 26 pero en el campo "Content" se escribe "vimeo".
33. Se repite el paso 27.
34. Se hace click en el símbolo "+" en la parte superior izquierda para crear una nueva regla, en el campo "Chain" se selecciona la opción "prerouting", posteriormente en el campo "Connection Mark" se selecciona "video" y se dirige a la pestaña "Action"

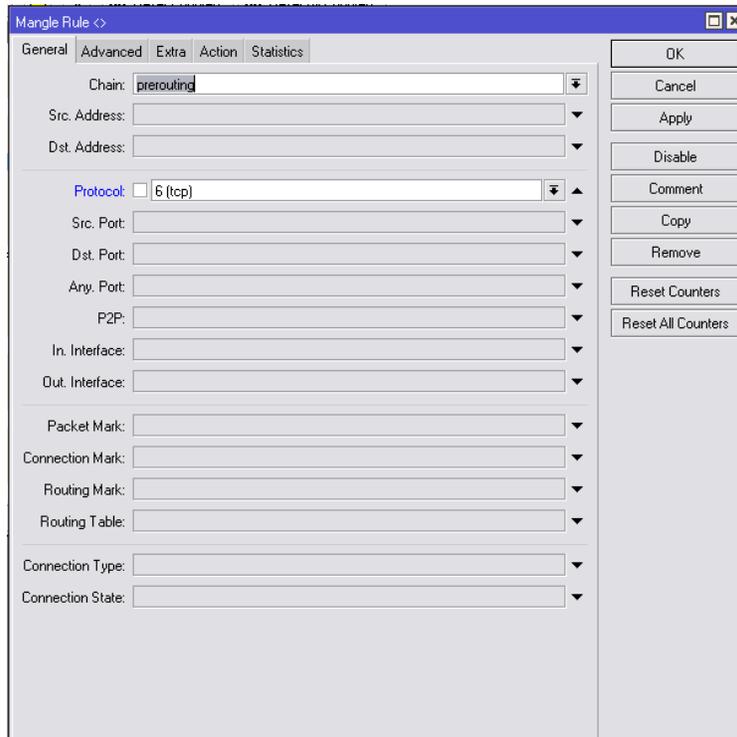


35. En la pestaña "Action", en el campo "Action" se selecciona la opción "mark packet", y el campo "New Packet Mark" se escribe "videos", se deshabilita la opción "Passthrough"

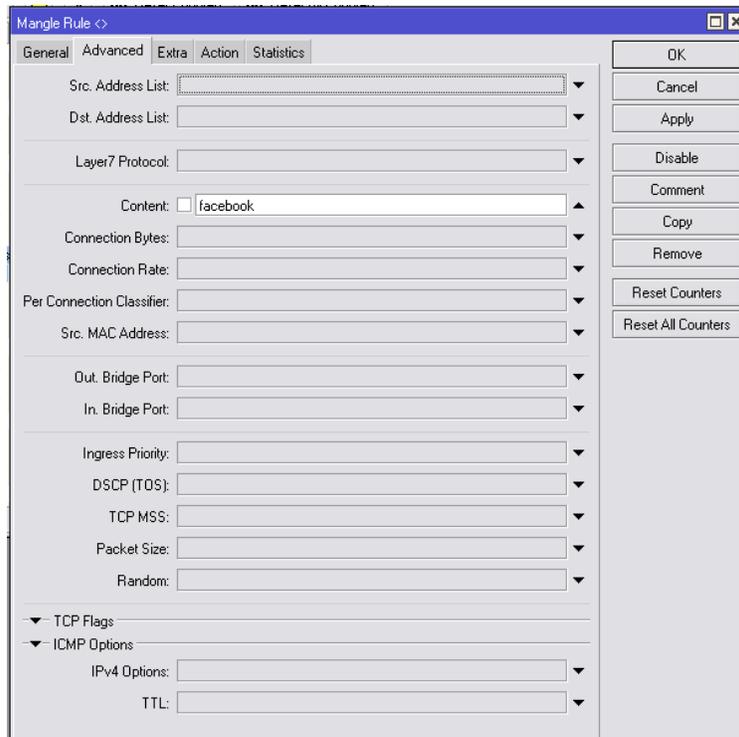


36. Se hace click en "ok"

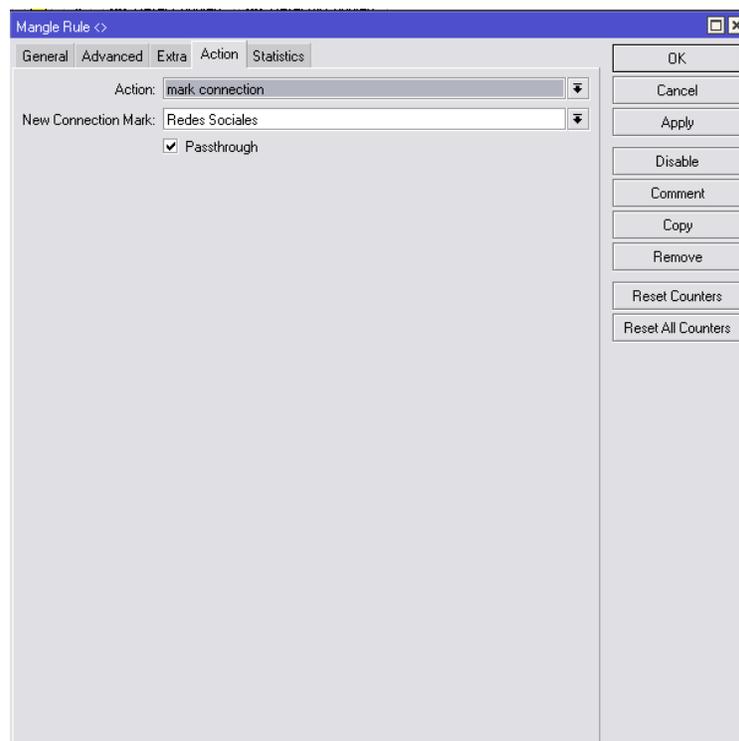
37. Se hace click en “+” para generar una nueva regla, en el campo “Chain” se selecciona la opción “prerouting”, en el campo “Protocol” se selecciona “6 (tcp)” y se dirige a la pestaña “Advanced”



38. En la pestaña “Advanced” en el campo “Content” se escribe “facebook”



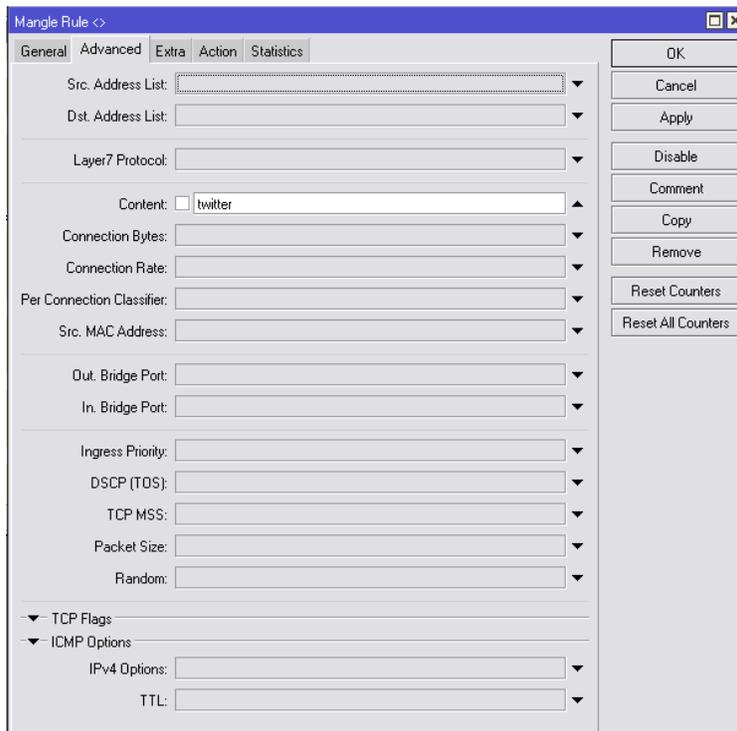
39. Posteriormente se dirige a la pestaña "Action", en el menú "Action" se selecciona "Mark Connection" y en el campo "New Connection Mark" se escribe "Redes Sociales", se deja habilitada la opción "Passthrough", se hace click en "OK".



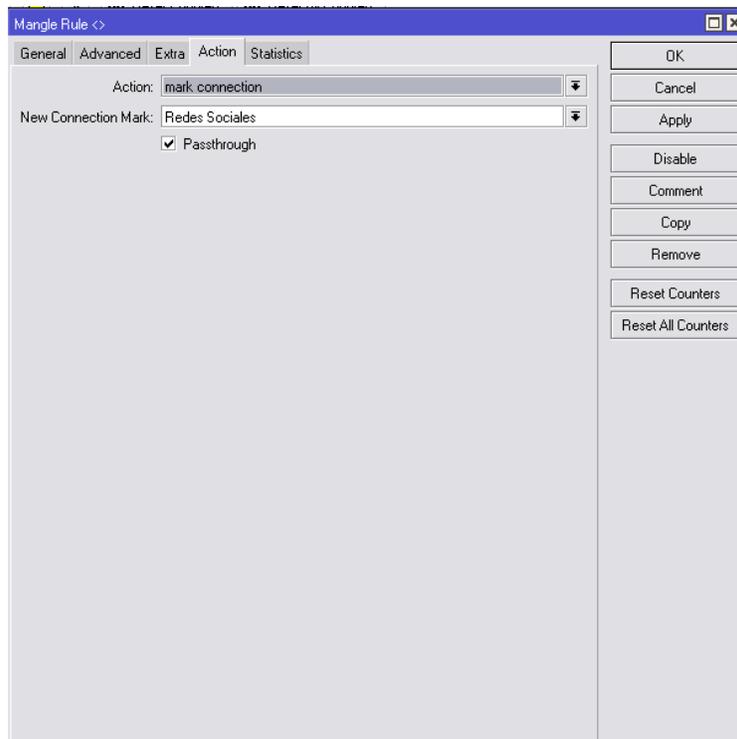
40. Se hace click en “+” para generar una nueva regla, en el campo “Chain” se selecciona la opción “prerouting”, en el campo “Protocol” se selecciona “6 (tcp)” y se dirige a la pestaña “Advanced”



41. En la pestaña “Advanced” en el campo “Content” se escribe “twitter”



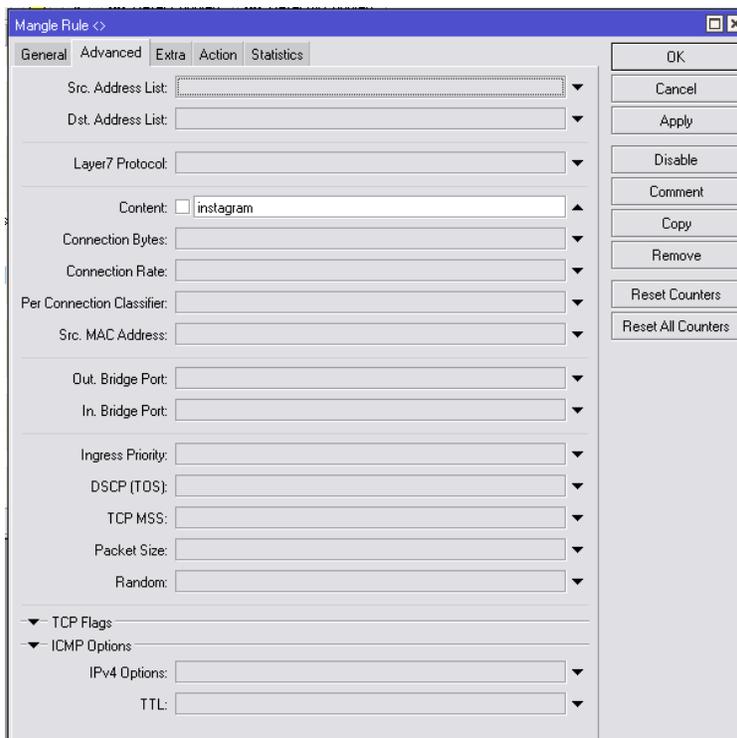
42. Posteriormente se dirige a la pestaña “Action”, en el menú “Action” se selecciona “Mark Connection” y en el campo “New Connection Mark” se escribe “Redes Sociales”, se deja habilitada la opción “Passthrough”, se hace click en “OK”.



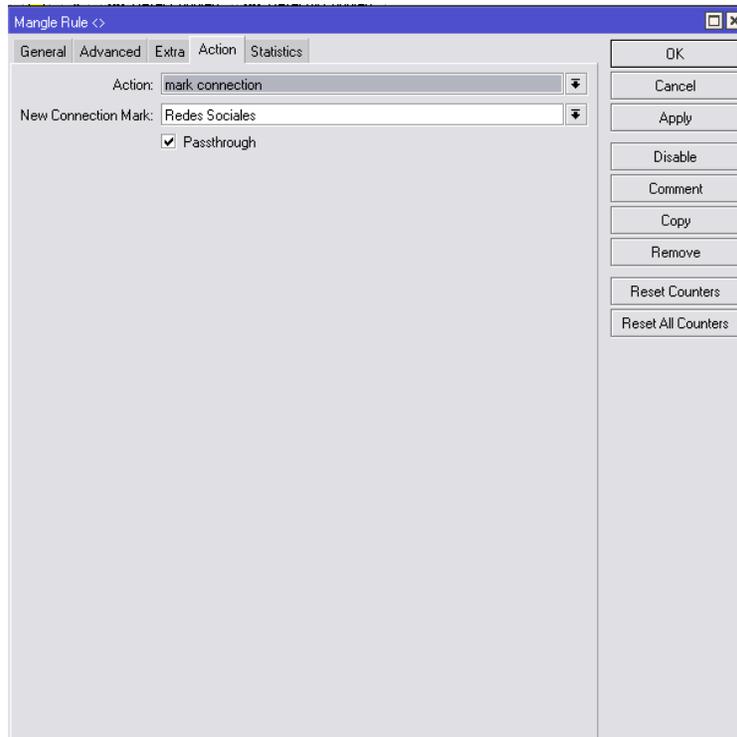
43. Se hace click en “+” para generar una nueva regla, en el campo “Chain” se selecciona la opción “prerouting”, en el campo “Protocol” se selecciona “6 (tcp)” y se dirige a la pestaña “Advanced”



44. En la pestaña “Advanced” en el campo “Content” se escribe “instagram”



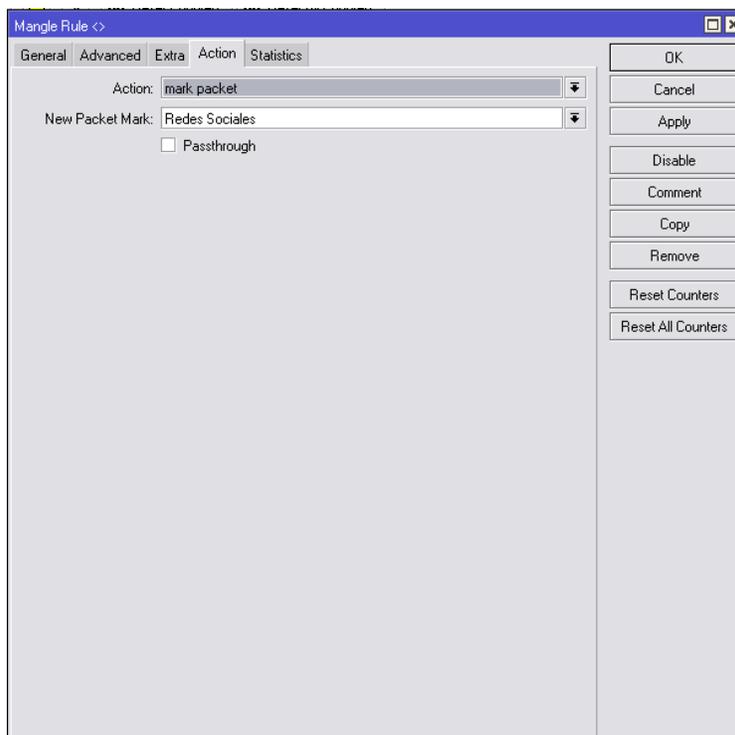
45. Posteriormente se dirige a la pestaña “Action”, en el menú “Action” se selecciona “Mark Connection” y en el campo “New Connection Mark” se escribe “Redes Sociales”, se deja habilitada la opción “Passthrough”, se hace click en “OK”.



46. Se hace click en el símbolo “+” en la parte superior izquierda para crear una nueva regla, en el campo “Chain” se selecciona la opción “prerouting”, posteriormente en el campo “Connection Mark” se selecciona “Redes Sociales” y se dirige a la pestaña “Action”

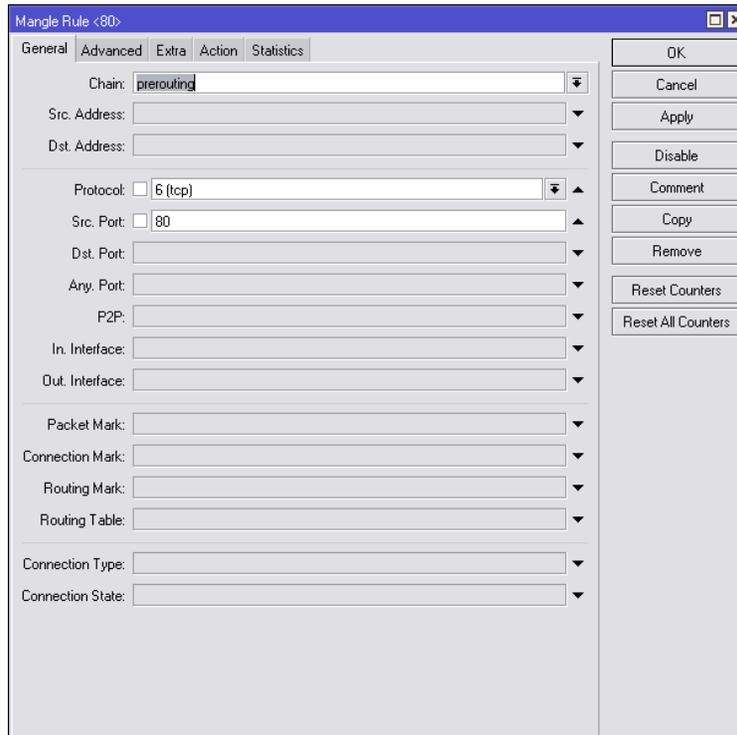


47. En la pestaña "Action", en el campo "Action" se selecciona la opción "mark packet", y el campo "New Packet Mark" se escribe "Redes Sociales", se deshabilita la opción "Passthrough"



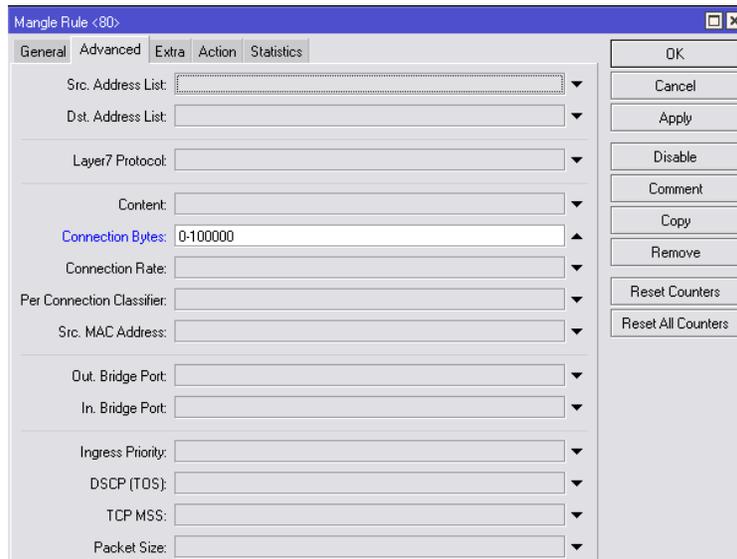
48. Se hace click en "ok"
 49. Se hace click en el símbolo "+" en la parte superior izquierda, para crear una nueva regla

50. En el campo "Chain" se selecciona la opción "prerouting" en el campo "protocol" se selecciona "6(tcp)" y en el campo "src port" se coloca el valor "80".



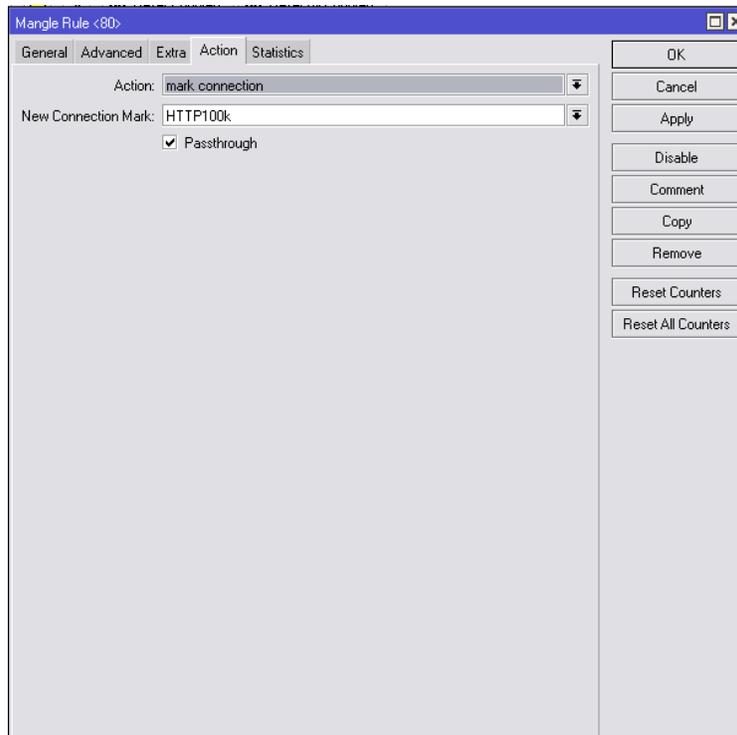
The screenshot shows the 'Mangle Rule' configuration window with the 'General' tab selected. The 'Chain' dropdown is set to 'prerouting'. The 'Protocol' dropdown is set to '6 (tcp)'. The 'Src. Port' field contains the value '80'. Other fields like 'Dst. Address', 'Dst. Port', 'Any. Port', 'P2P', 'In. Interface', 'Out. Interface', 'Packet Mark', 'Connection Mark', 'Routing Mark', 'Routing Table', 'Connection Type', and 'Connection State' are empty. On the right side, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', and 'Reset All Counters'.

51. Se dirige a la pestaña "Advanced" en el campo "Connection Bytes" se coloca el valor "0-100000" y se dirige a la pestaña "Action"



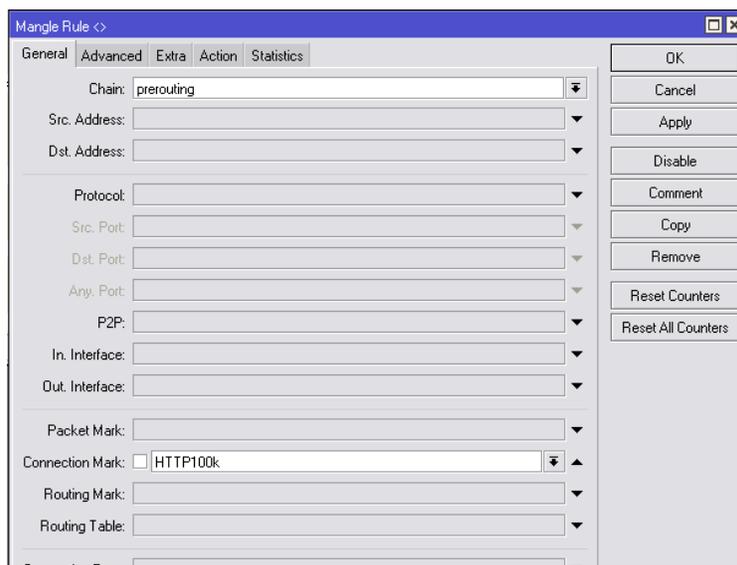
The screenshot shows the 'Mangle Rule' configuration window with the 'Advanced' tab selected. The 'Connection Bytes' field contains the value '0-100000'. Other fields like 'Src. Address List', 'Dst. Address List', 'Layer7 Protocol', 'Content', 'Connection Rate', 'Per Connection Classifier', 'Src. MAC Address', 'Out. Bridge Port', 'In. Bridge Port', 'Ingress Priority', 'DSCP (TOS)', 'TCP MSS', and 'Packet Size' are empty. The right side buttons are the same as in the previous screenshot.

52. En la pestaña "Action" en el campo "Action" se selecciona , "mark connection" y en el campo "New Connection Mark" se escribe "HTTP100k", se deja habilitada la opción "Passthrough", se hace click en "OK"

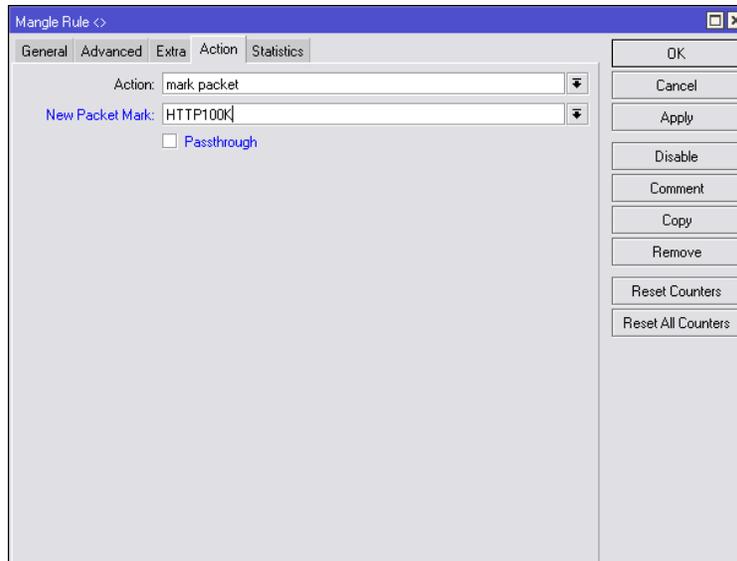


53. Se hace click en el símbolo “+” en la parte superior izquierda para crear una nueva regla

54. En el campo “Chain” se selecciona la opción “prerouting”, en el campo “protocol” se selecciona “6(tcp)” y en el campo “Connection Mark” se selecciona “HTTP100k”, posteriormente se dirige a la pestaña “Action”

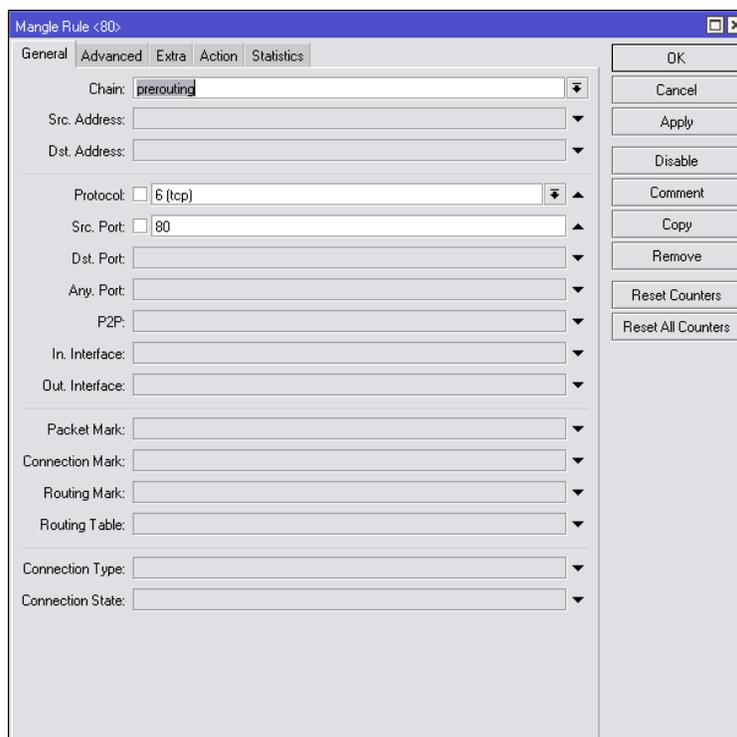


55. En la pestaña “Action”, en el menú “Action” se selecciona la opción “mark packet” y en el campo “New Packet Mark” se escribe “HTTP100k”, se deshabilita la opción “Passthrough” y se hace click en “OK”

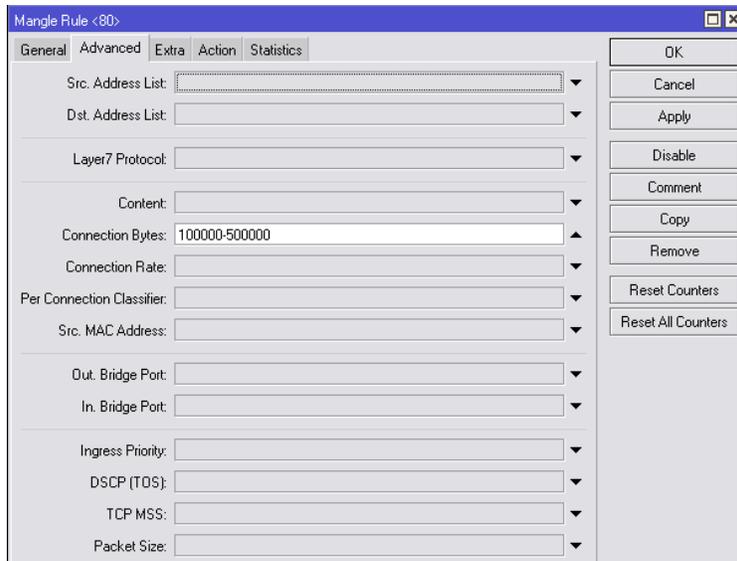


56. Se hace click en el símbolo “+” en la parte superior izquierda, para crear una nueva regla

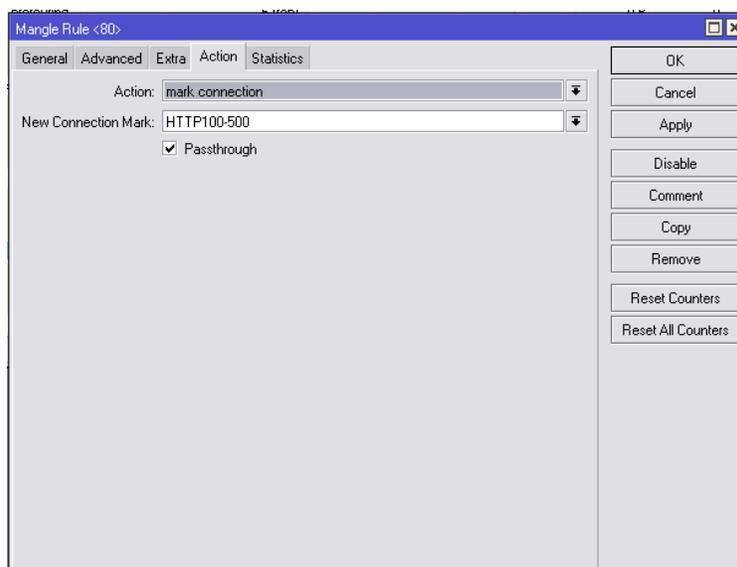
57. En el campo “Chain” se selecciona la opción “prerouting” en el campo “protocol” se selecciona “6(tcp)” y en el campo “src port” se coloca el valor “80”.



58. Se dirige a la pestaña “Advanced” en el campo “Connection Bytes” se coloca el valor “100000-500000” y se dirige a la pestaña “Action”

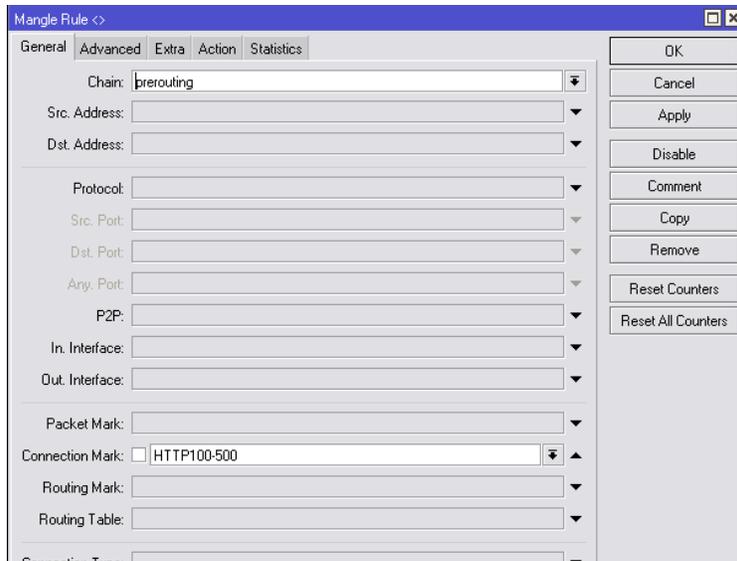


59. En la pestaña "Action" en el campo "Action" se selecciona , "mark connection" y en el campo "New Connection Mark" se escribe "HTTP100-500", se deja habilitada la opción "Passthrough", se hace click en "OK"



60. Se hace click en el símbolo "+" en la parte superior izquierda para crear una nueva regla

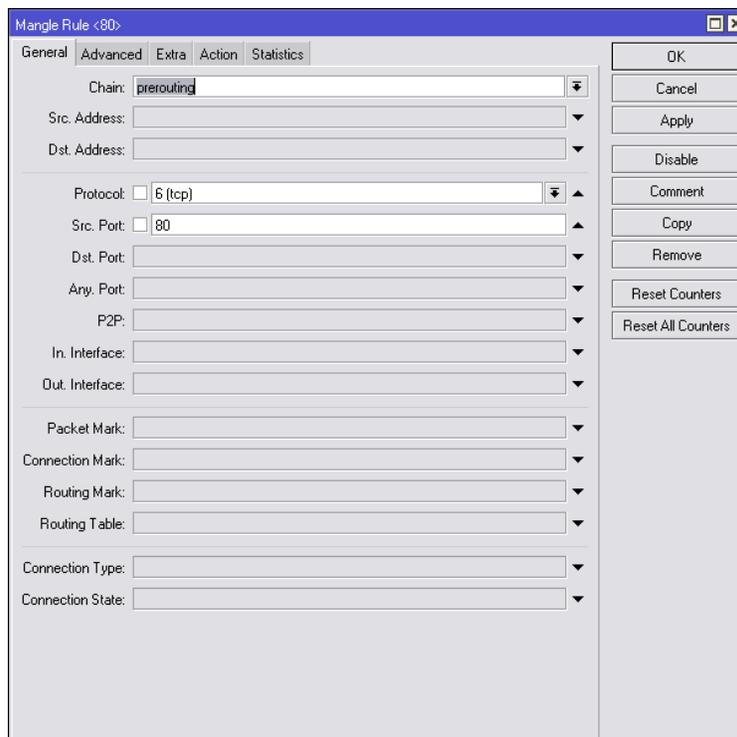
61. En el campo "Chain" se selecciona la opción "prerouting", en el campo "protocol" se selecciona "6(tcp)" y en el campo "Connection Mark" se selecciona "HTTP100-500", posteriormente se dirige a la pestaña "Action"



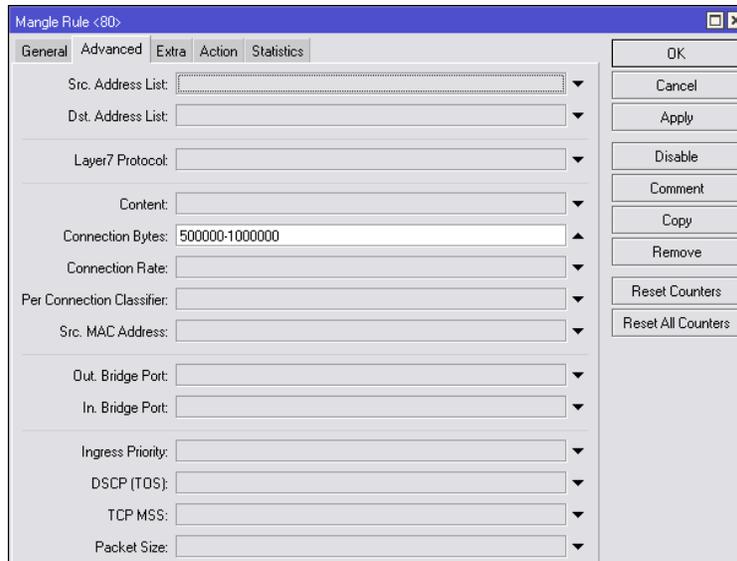
62. En la pestaña "Action", en el menú "Action" se selecciona la opción "mark packet" y en el campo "New Packet Mark" se escribe "HTTP100k", se deshabilita la opción "Passthrough" y se hace click en "OK"

63. Se hace click en el símbolo "+" en la parte superior izquierda, para crear una nueva regla

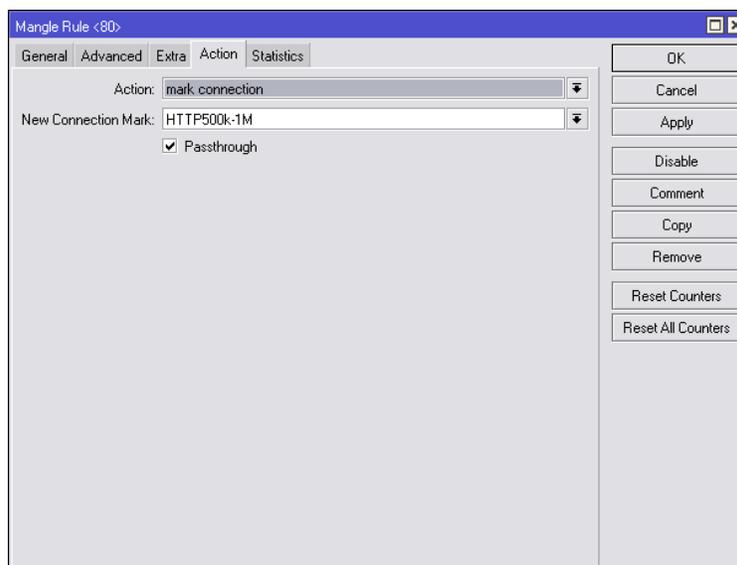
64. En el campo "Chain" se selecciona la opción "prerouting" en el campo "protocol" se selecciona "6(tcp)" y en el campo "src port" se coloca el valor "80".



65. Se dirige a la pestaña "Advanced" en el campo "Connection Bytes" se coloca el valor "100000-500000" y se dirige a la pestaña "Action"



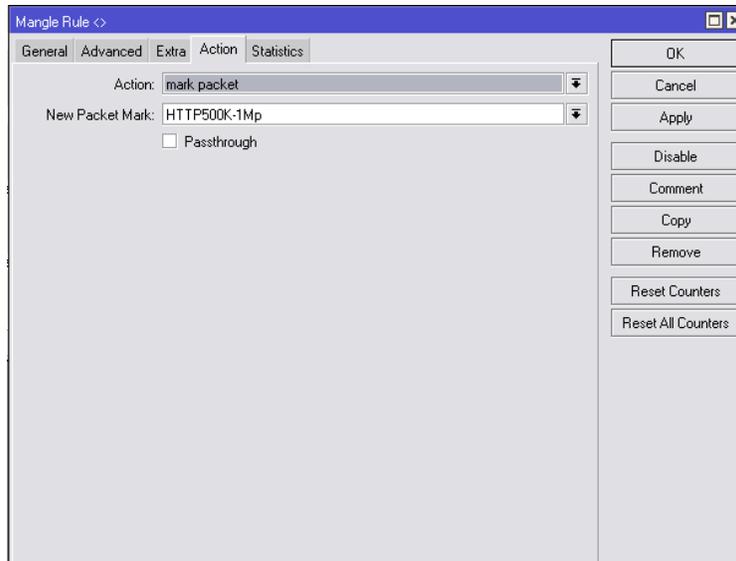
66. En la pestaña "Action" en el campo "Action" se selecciona , "mark connection" y en el campo "New Connection Mark" se escribe "HTTP500-1M", se deja habilitada la opción "Passthrough", se hace click en "OK"



67. Se hace click en el símbolo "+" en la parte superior izquierda para crear una nueva regla

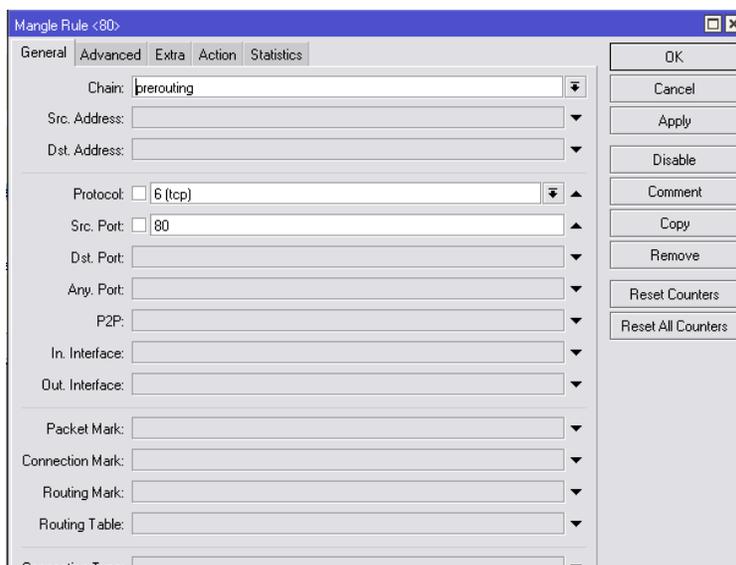
68. En el campo "Chain" se selecciona la opción "prerouting", en el campo "protocol" se selecciona "6(tcp)" y en el campo "Connection Mark" se selecciona "HTTP500-1M", posteriormente se dirige a la pestaña "Action"

69. En la pestaña "Action", en el menú "Action" se selecciona la opción "mark packet" y en el campo "New Packet Mark" se escribe "HTTP500-1M", se deshabilita la opción "Passthrough" y se hace click en "OK"

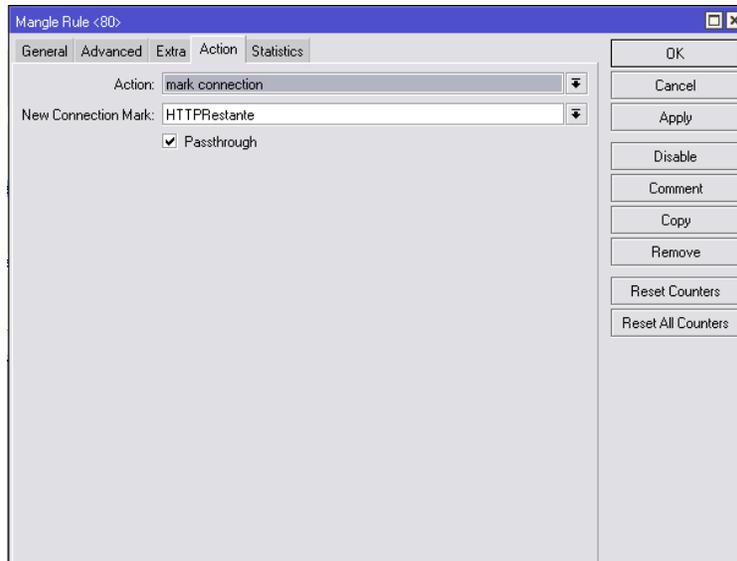


70. Se hace click en el símbolo “+” en la parte superior izquierda, para crear una nueva regla

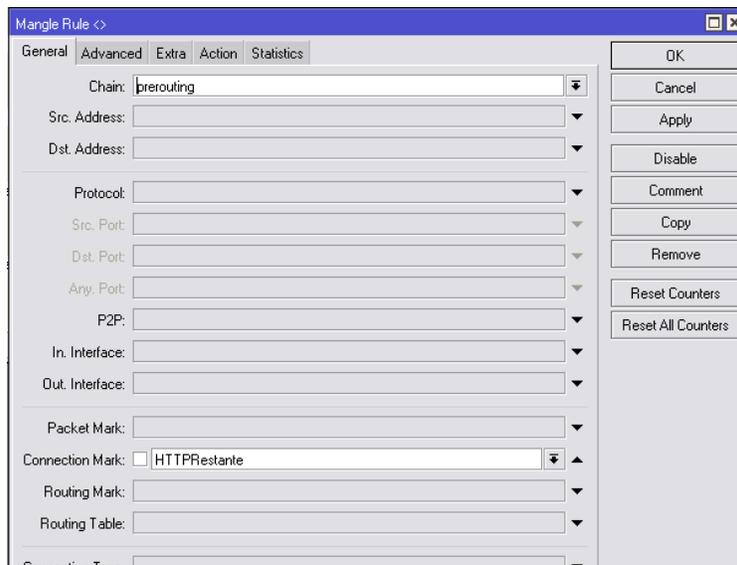
71. En el campo “Chain” se selecciona la opción “prerouting” en el campo “protocol” se selecciona “6(tcp)” y en el campo “src port” se coloca el valor “80”.



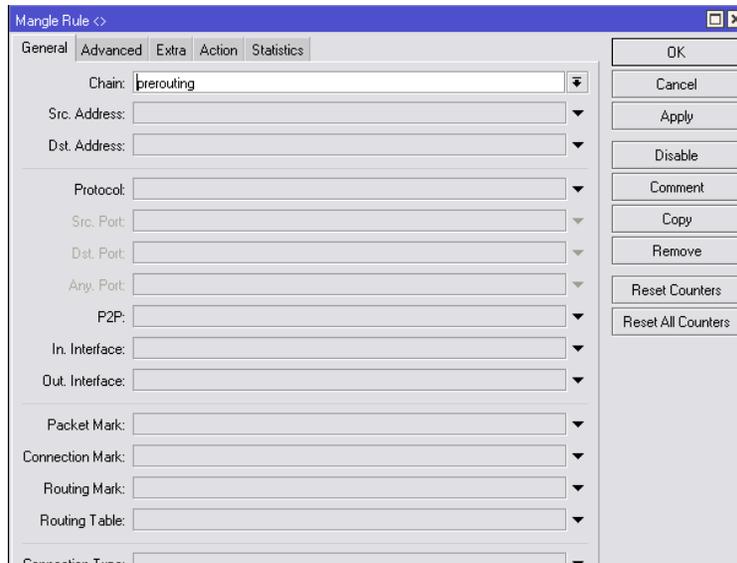
72. Se dirige a la pestaña “Action” y en el campo “Action” se selecciona la opción “mark connection”, en el campo “New Connection Mark” se escribe “HTTPRestante”, se deja habilitada la opción “Passthrough”, se hace click en “OK”



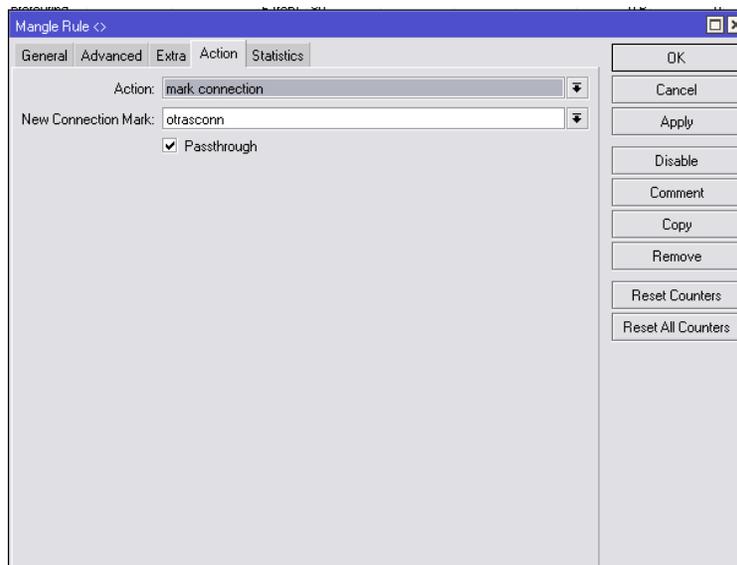
73. Se hace click en el símbolo “+” en la parte superior izquierda, para crear una nueva regla



74. Se hace click en el símbolo “+” en la parte superior izquierda, para crear una nueva regla
75. En el campo “Chain” se selecciona la opción “prerouting”.



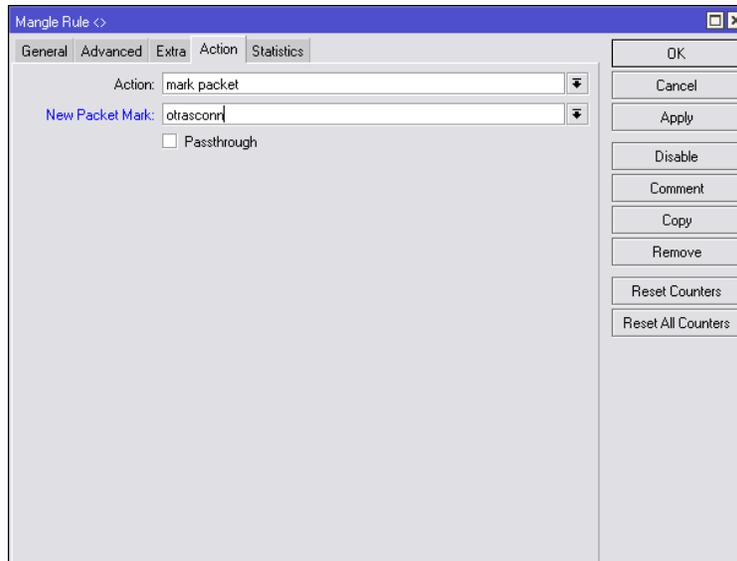
76. Se dirige a la pestaña "Action", en el campo "Action" se selecciona la opción "mark connection" y en el campo "New Connection Mark" se escribe "otrasconn", se hace click en "OK".



77. Se hace click en el símbolo "+" en la parte superior izquierda, para crear una nueva regla

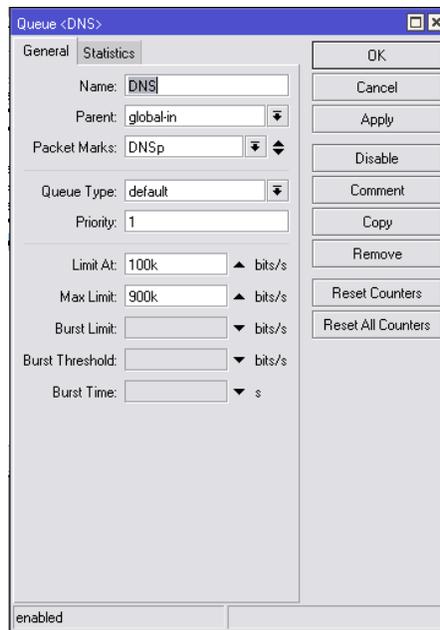
78. En el campo "Chain" se selecciona la opción "prerouting", en "Connection Mark" se selecciona "otrasconn" y se dirige a la pestaña "Action"

79. En el campo "Action" se selecciona la opción "mark packet" y en "New Packet Mark" se escribe "otrasconn", se deshabilita la opción "Passthrough" y se hace click en "OK".

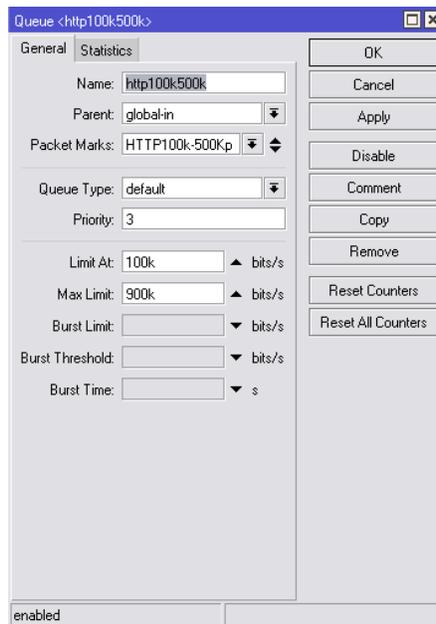


Con esto se finaliza la etapa del marcado de paquetes y procedemos a armar el árbol de colas:

80. Se hace click en la opción "Queue" en el menú principal, se dirige a la pestaña "Queue Tree", se hace click en el símbolo "+" ubicado en la parte superior izquierda para agregar una nueva cola
81. En el campo "Name" se coloca "DNS", en el campo "Parent" se selecciona la opción "global-in", y en el campo "Packet Marks" se selecciona "DNS" (la marca establecida previamente en el mangle)
82. En el campo "Queue Type" se selecciona la opción "default".
83. En el campo "Priority" se escribe el valor "1"
84. En el campo "Limit At" se escribe el valor "100k"
85. En el campo "Max Limit" se escribe el valor "900k"

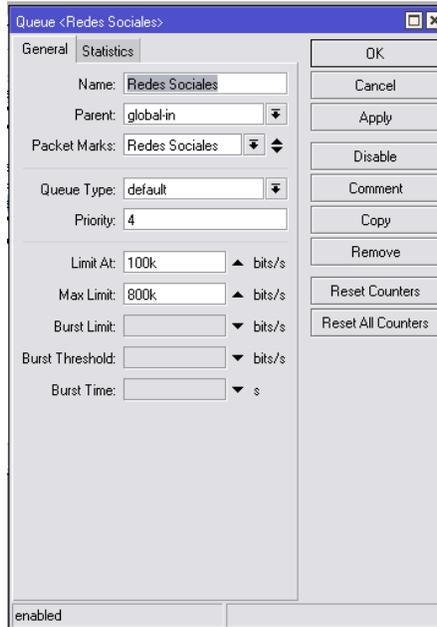


86. Se hace click en "OK"
87. Se hace click en el símbolo "+" ubicado en la parte superior izquierda para agregar una nueva cola
88. En el campo "Name" se coloca "http100k", en el campo "Parent" se selecciona la opción "global-in", y en el campo "Packet Marks" se selecciona "HTTP100k" (la marca establecida previamente en el mangle)
89. En el campo "Queue Type" se selecciona la opción "default".
90. En el campo "Priority" se escribe el valor "2"
91. En el campo "Limit At" se escribe el valor "100k"
92. En el campo "Max Limit" se escribe el valor "900k"
93. Se hace click en "OK"
94. Se hace click en el símbolo "+" ubicado en la parte superior izquierda para agregar una nueva cola
95. En el campo "Name" se coloca "http100k-500k", en el campo "Parent" se selecciona la opción "global-in", y en el campo "Packet Marks" se selecciona "HTTP100k-500k" (la marca establecida previamente en el mangle)
96. En el campo "Queue Type" se selecciona la opción "default".
97. En el campo "Priority" se escribe el valor "3"
98. En el campo "Limit At" se escribe el valor "100k"
99. En el campo "Max Limit" se escribe el valor "900k"



100. Se hace click en "OK"
101. Se hace click en el símbolo "+" ubicado en la parte superior izquierda para agregar una nueva cola
102. En el campo "Name" se coloca "Redes Sociales", en el campo "Parent" se selecciona la opción "global-in", y en el campo "Packet Marks" se selecciona "redes sociales" (la marca establecida previamente en el mangle)
103. En el campo "Queue Type" se selecciona la opción "default".
104. En el campo "Priority" se escribe el valor "4"

105. En el campo "Limit At" se escribe el valor "100k"
106. En el campo "Max Limit" se escribe el valor "800k"



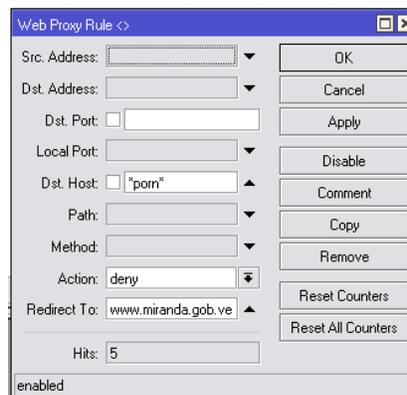
107. Se hace click en "OK"
108. Se hace click en el símbolo "+" ubicado en la parte superior izquierda para agregar una nueva cola
109. En el campo "Name" se coloca "Videos Online", en el campo "Parent" se selecciona la opción "global-in", y en el campo "Packet Marks" se selecciona "videos" (la marca establecida previamente en el mangle)
110. En el campo "Queue Type" se selecciona la opción "default".
111. En el campo "Priority" se escribe el valor "5"
112. En el campo "Limit At" se escribe el valor "200k"
113. En el campo "Max Limit" se escribe el valor "900k"
114. Se hace click en "OK"
115. Se hace click en el símbolo "+" ubicado en la parte superior izquierda para agregar una nueva cola
116. En el campo "Name" se coloca "http500k-1M", en el campo "Parent" se selecciona la opción "global-in", y en el campo "Packet Marks" se selecciona "HTTP500-1M" (la marca establecida previamente en el mangle)
117. En el campo "Queue Type" se selecciona la opción "default".
118. En el campo "Priority" se escribe el valor "6"
119. En el campo "Limit At" se escribe el valor "200k"
120. En el campo "Max Limit" se escribe el valor "900k"
121. Se hace click en "OK"
122. Se hace click en el símbolo "+" ubicado en la parte superior izquierda para agregar una nueva cola
123. En el campo "Name" se coloca "http>1M", en el campo "Parent" se selecciona la opción "global-in", y en el campo "Packet Marks" se selecciona "HTTPRestante" (la marca establecida previamente en el mangle)

124. En el campo "Queue Type" se selecciona la opción "default".
125. En el campo "Priority" se escribe el valor "7"
126. En el campo "Limit At" se escribe el valor "100k"
127. En el campo "Max Limit" se escribe el valor "900k"
128. Se hace click en "OK"
129. Se hace click en el símbolo "+" ubicado en la parte superior izquierda para agregar una nueva cola
130. En el campo "Name" se coloca "Otras Conexiones", en el campo "Parent" se selecciona la opción "global-in", y en el campo "Packet Marks" se selecciona "otrasconn" (la marca establecida previamente en el mangle)
131. En el campo "Queue Type" se selecciona la opción "default".
132. En el campo "Priority" se escribe el valor "8"
133. En el campo "Limit At" se escribe el valor "100k"
134. En el campo "Max Limit" se escribe el valor "900k"

Una vez cumplidos estos pasos habremos terminado de configurar el árbol de colas

135. Para configurar el servidor webproxy, se hace click en la opción "IP" del menú y posteriormente se selecciona la opción "Webproxy", en la ventana que se despliega, se mantiene en la pestaña "Access" y se hace click en el símbolo "+" ubicado en la parte superior izquierda, para agregar una nueva regla.

136. En esta ventana en el campo "Dst. Host" vamos a escribir "*porn*", en el campo "Action" se selecciona la opción "deny" y en el campo "Redirect To" se escribe www.miranda.gob.ve y se hace click en "OK"

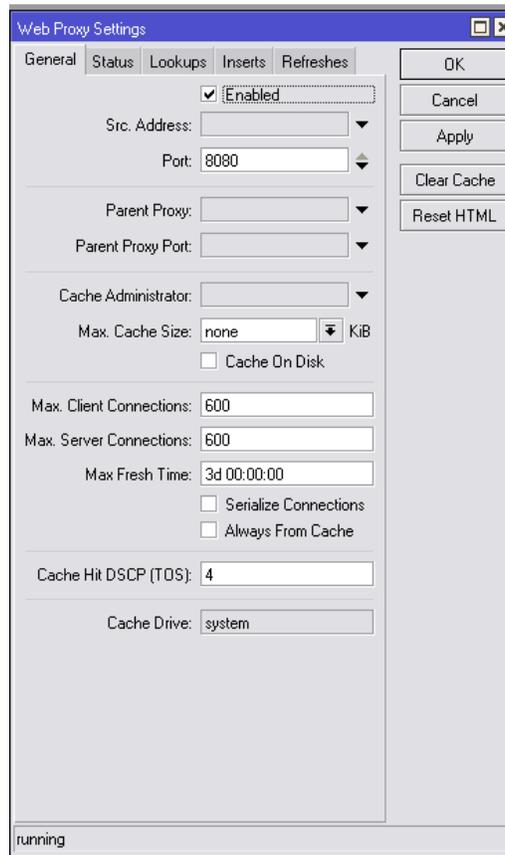


137. Se repite el paso anterior sustituyendo el término "porn" por cada una de las siguientes palabras (de ser necesario agregar otras palabras):

- Sex
- XXX
- Naked
- Gay

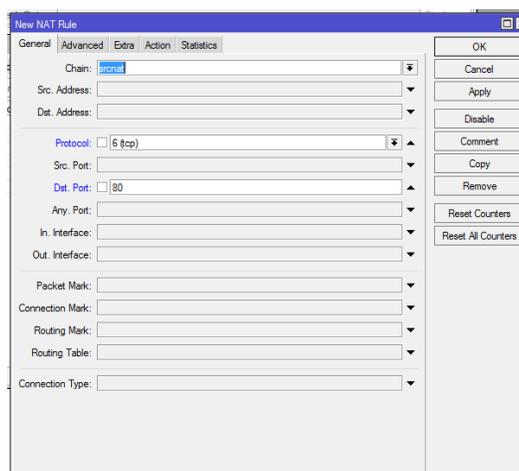
138. Se hace click en la parte superior, en el botón "Web Proxy Settings" y se habilita la opción "Enable", en el campo "Port" se coloca el valor "8080" se deja las demás opciones por defecto y se

acepta haciendo click en “OK”, una vez activado el webproxy es necesario redirigir todo el trafico web al puerto 8080, ya no se reciben solicitudes al puerto 80.

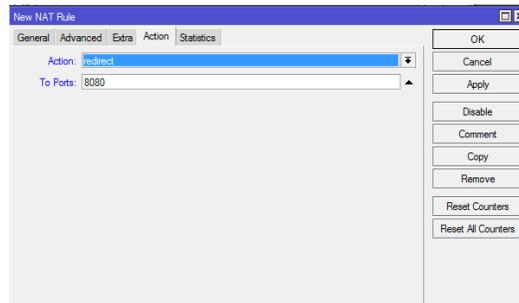


139. Se dirige a la opción “IP” en el menú y se selecciona el apartado “NAT”, se hace click en la parte superior izquierda en el símbolo “+” para agregar una nueva regla.

140. En el campo “Chain” se selecciona la opción “dstnat”, en el campo “Protocol” se selecciona la opción “6(tcp)” y en el campo “Ports” se escribe el valor “80”.



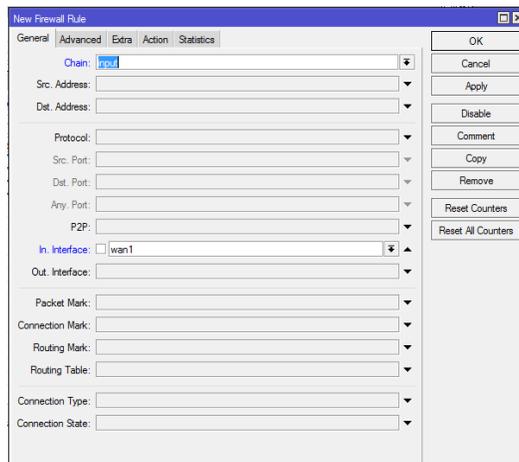
141. Se dirige a la pestaña “Action” y en el campo “Action” se selecciona la opción “redirect”, en el campo “To Ports” se escribe el valor “8080”.



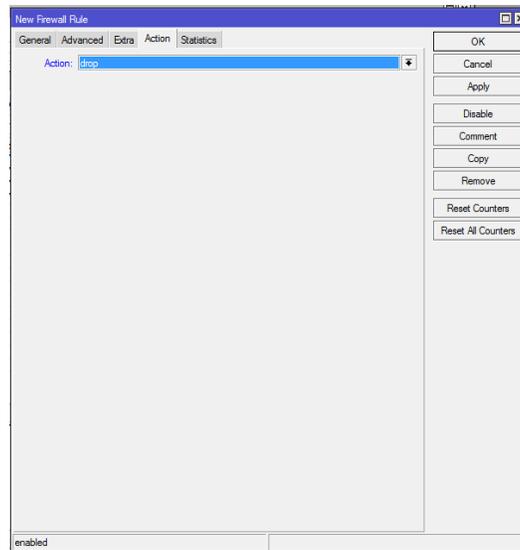
142. Se dirige a la opción “IP” en el menú y se selecciona el apartado “Firewall”, se dirige a la pestaña “Firewall”.

143. Se hace click en el símbolo “+” en la parte superior izquierda para agregar una nueva regla

144. En esta nueva regla, se selecciona en el campo “Chain” la opción “input” y en “In Interface” se selecciona “WAN”



145. Posteriormente se dirige a la pestaña “Action” y en el campo “Action” se selecciona la opción “drop”



146. Se hace click en “OK” y de esta forma finalizamos la configuración del dispositivo, lo que resta es hacer las conexiones físicas necesarias (si aún no se han hecho).