

**ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL**

**FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y  
COMPUTACIÓN**

“Estudio, diseño y simulación de sistemas de telecomunicación para  
el mejoramiento de control y calidad de servicios de internet y  
televisión en la compañía NETSURTV”

**PROYECTO INTEGRADOR**

Previo la obtención del Título de:

**Ingeniería en Telecomunicaciones**

**Presentado por:**

Puero Soriano Ericka Adriana

Tandazo Castillo Oscar Javier

**GUAYAQUIL – ECUADOR**

Año: 2022

## **AGRADECIMIENTOS**

Agradecemos a Dios por darnos la sabiduría e inteligencia para cumplir con las metas que tenemos trazadas en nuestras vidas y permitirnos terminar esta etapa con nuevos aprendizajes tanto académicos como personales. A nuestros padres por ser el pilar fundamental del desarrollo de nuestras vidas, siendo un gran ejemplo de perseverancia, resiliencia y superación. A nuestros maestros, amigos y compañeros de carrera.

## **DEDICATORIA**

Este trabajo está dedicado a nuestros padres por su ardua labor, apoyo incondicional y siempre confiar en nuestras capacidades para lograr cumplir nuestras metas.

## **DECLARACIÓN EXPRESA**

“La responsabilidad y autoría del presente Trabajo de Titulación corresponde exclusivamente a Puerio Soriano Ericka Adriana y Tandazo Castillo Oscar Javier; y damos nuestro consentimiento para que la ESPOL realice la comunicación pública de la obra por cualquier medio con el fin de promover la consulta, difusión y uso público de la producción intelectual”

.....  
Puerio Soriano Ericka

.....  
Tandazo Castillo Oscar

# EVALUADORES

.....  
**Ing. Washington Medina**  
PROFESOR DE LA MATERIA

.....  
**Msc. Verónica Soto**  
TUTORA ACADEMICA

## RESUMEN

En este documento se realizará el estudio de los sistemas de telecomunicación que utiliza la empresa NETSURTV para brindar los servicios de internet y TV por cable, en donde se analizó la infraestructura del sistema de transmisión de televisión y la red de acceso a internet para determinar los problemas principales que tenía cada sistema. Una vez realizado el análisis, en el Capítulo III se diseñó la propuesta de solución para cada problema detectado, dentro de las soluciones se propuso un sistema que permita realizar transmisiones de televisión en alta definición e implementar configuraciones requeridas para el correcto funcionamiento y manejo de una ISP. En el Capítulo IV se presenta los resultados de ambas soluciones, primero un cuadro comparativo entre el sistema de televisión actual y el sistema propuesto, y después los resultados que se obtuvieron en la simulación de la topología de red propuesta para la red de acceso a internet en el software GNS3, donde se plantearon configuraciones para mejorar la seguridad del Firewall, calidad de servicio, control de ancho de banda e implementación de un sistema autónomo.

***Palabras Claves:*** TV Digital, CATV, Mikrotik: Firewall, Control de ancho de Banda, Sistema Autónomo.

## ABSTRACT

In this document a study of the telecommunication systems used by NETSURTV to provide internet and cable TV services was carried out, where the infrastructure of the television transmission system and the internet access network were analyzed to determine the main problems of each system. Once the analysis was done, in Chapter III a solution proposal was designed for each detected problem. Among the solutions, a system was proposed to allow high-definition television transmissions and to implement the required configurations for the correct operation and management of an ISP. Chapter IV presents the results of both solutions, first a comparative table between the current television system and the proposed system, and then the results obtained in the simulation of the proposed network topology for the internet access network in the GNS3 software, where configurations were proposed to improve the security of the Firewall, quality of service, bandwidth control and implementation of an autonomous system.

***Keywords:*** *Digital TV, CATV, Mikrotik: Firewall, Bandwidth Control, Autonomous System.*

# ÍNDICE

<b>RESUMEN</b> .....	6
<b>ABSTRACT</b> .....	7
<b>ÍNDICE</b> .....	8
<b>ABREVIATURAS</b> .....	11
<b>ÍNDICE DE FIGURAS</b> .....	13
<b>ÍNDICE DE TABLAS</b> .....	14
<b>CAPITULO I</b> .....	15
<b>1. INTRODUCCIÓN</b> .....	15
1.1. Definición del problema.....	16
1.2. Justificación del problema.....	17
1.3. Objetivos.....	18
1.3.1. Objetivo general.....	18
1.3.2. Objetivo específico.....	18
1.4. Estado del arte.....	18
1.5. Alcance del proyecto.....	24
1.6. Metodología.....	25
1.6.1. Sistema de transmisión para televisión o CATV:.....	25
1.6.2. Red de acceso a internet.....	26
<b>CAPÍTULO II</b> .....	27
<b>2. MARCO TEÓRICO</b> .....	27
2.1. Sistema de televisión.....	27
2.1.1. Televisión analógica.....	28
2.1.2. Televisión digital.....	28
2.1.2.1. Televisión digital por cable.....	29
2.1.2.1.1. Estructura de un sistema CATV.....	30
2.1.2.1.2. Televisión por protocolo de internet (IPTV).....	30
2.2. Configuraciones para el sistema de televisión.....	31
2.2.1. Modulación de amplitud en cuadratura (QAM).....	31
2.3. Proveedor de servicio de internet (ISP).....	33
2.3.1. Infraestructura de una ISP.....	33
2.3.2. Elementos principales de una red.....	35
2.3.2.1. Router.....	35
2.3.2.2. Switch.....	35
2.3.2.3. Sistema operativo.....	35



2.4.	RouterOS.....	35
2.4.1.	Winbox.....	36
2.4.2.	Firewalls.....	36
2.4.2.1.	Firewall: Filter rules .....	36
2.4.2.2.	Firewall: NAT .....	37
2.4.2.3.	Firewall: Mangle .....	37
2.4.3.	Calidad de servicio o QoS .....	38
2.4.3.1.	Queues.....	38
2.4.3.2.	Queues simple .....	39
2.4.3.3.1.	HTB.....	39
2.5.	Sistema autónomo .....	40
2.5.1.	BGP.....	40
2.5.1.1.	iBGP.....	41
2.5.1.2.	eBGP .....	41
<b>CAPÍTULO III.....</b>		<b>42</b>
3.	<b>DISEÑO DE PROTOTIPO .....</b>	<b>42</b>
3.1.1.	Descripción de cada equipo de la infraestructura actual .....	44
3.1.2.	Equipos para el sistema CATV/IPTV propuesto .....	46
3.1.2.1.	Codificador.....	46
3.1.3.	Presupuesto inicial de la empresa .....	47
3.1.4.	Presupuesto total para el nuevo sistema.....	47
3.1.5.	Configuraciones para los nuevos equipos del sistema de televisión .....	48
3.1.5.1.	Configuraciones para el codificador .....	48
3.1.5.2.	Configuraciones para la IP-QAM .....	48
3.2.	Red de acceso a internet .....	50
3.2.1.	Análisis de la topología de red de la empresa .....	50
3.2.2.	Router principal de la empresa .....	50
3.2.3.	Análisis de configuraciones del equipo central.....	51
3.2.3.1.	Configuraciones de puertos ethernet.....	51
3.2.3.2.	Configuraciones de enrutamiento .....	52
3.2.3.3.	Configuraciones del firewall.....	54
3.2.3.4.	Configuraciones del queues .....	55
3.2.4.	Análisis del tráfico de la red .....	56
3.2.5.	Análisis de consumo del CPU .....	58
3.2.6.	Propuesta de solución .....	59
3.2.6.1.	Topología de red propuesta .....	59

3.2.6.2.	Configuraciones propuestas al equipo central.....	60
3.2.6.2.1.	Mejoras de seguridad del firewall.....	60
3.2.6.2.2.	Control de ancho de banda por PCQ + Queues tree.....	60
3.2.6.2.3.	Calidad de servicio o QoS.....	61
3.2.6.2.4.	Sistema Autónomo y BGP.....	61
<b>CAPITULO IV.....</b>		<b>62</b>
<b>4. ANÁLISIS DE RESULTADOS.....</b>		<b>62</b>
4.1.	Sistema de televisión.....	62
4.2.	Red de acceso a internet.....	63
4.2.1.	Escalabilidad y redundancia.....	64
4.2.2.	Sistema autónomo.....	64
4.2.2.1.	Implementación del protocolo eBGP.....	64
4.2.3.	Seguridad.....	67
4.2.3.1.	Bloqueo de denegación distribuida de servicio (DDoS).....	68
4.2.3.2.	Permisos de acceso al equipo central.....	69
4.2.4.	Control de ancho de banda por PCQ + Queues tree.....	71
4.2.5.	Notificación de corte de servicio.....	73
<b>CONCLUSIONES.....</b>		<b>75</b>
<b>RECOMENDACIONES.....</b>		<b>76</b>
<b>ANEXOS.....</b>		<b>82</b>

## ABREVIATURAS

CATV	Community Antenna Television
TV-HD	Televisión en Alta Calidad
ISP	Proveedor de Servicios de Internet
UIT	Unión Internacional de las Telecomunicaciones
IPTV	Televisión por Protocolo de Internet
HDMI	High-Definition Multimedia Interface
VHF	Muy Alta Frecuencia
QoS	Calidad de Servicio
PQ	Priority Queuing
WFQ	Weighted Fair Queuing
CQ	Common Queuing
FTTH	Fiber to the Home
GPON	Gigabit-capable Passive Optical Network
QAM	Modulación de Amplitud en Cuadratura
DLS	Digital Subscriber Line
LAN	Red de Área Local
WAN	Red de Área Amplia
SSH	Secure Shell
FTP	File Transfer Protocol
ICMP	Protocolo de Control de Mensajes de Internet
TCP	Protocolo de Control de Transmisión
NAT	Network Address Translation
IP	Protocolo de Internet
VLAN	Virtual LAN
P2P	Punto a Punto

AS	Sistema Autónomo
ASN	Número de Sistema Autónomo
BGP	Border Gateway Protocol
SMATV	Single Master Antenna Television
OLT	Terminal de Línea Óptica
ONU	Unida de Red Óptica
CPU	Unidad Central de Proceso
SFP	Small Form-Factor Pluggable
RAM	Memoria de Acceso Aleatorio
DDoS	Ataque de Denegación de Servicio

## ÍNDICE DE FIGURAS

Figura 1. Diagrama de bloques para la solución del sistema de televisión. ....	25
Figura 2. Diagrama de bloques de la solución para la red de acceso a internet. ....	26
Figura 3. Diagrama universal de receptores digitales [20].....	29
Figura 4. Estructura de un sistema de cabecera [22].....	30
Figura 5. Sistema FFTH IPTV [24].....	31
Figura 6. Los diferentes órdenes de modulaciones QAM [27] .....	32
Figura 7. Ejemplo de cantidad de bits por símbolo [26].....	32
Figura 8. Modulación 256-QAM con diferentes SNR [26] .....	33
Figura 9. a) Modelo jerárquico de 3 capas. b) Modelo de Núcleo contraído [29].....	34
Figura 10. Topología del sistema de transmisión de TV actual de la empresa. ....	42
Figura 11. Diseño de prototipo de televisión. ....	43
Figura 12. Receptor Satelital Cisco D9865 [40].....	44
Figura 13. Panel Frontal del Receptor Satelital Cisco D9865 [40].....	44
Figura 14. Modulador PCM55SAW [41] .....	45
Figura 15. CATV Mixer [43] .....	45
Figura 16. Transmisor Óptico [44].....	45
Figura 17. Codificador AOURI [45] .....	46
Figura 18. IPQAM mux scrambler [46] .....	46
Figura 19. DVB-T MPEG2/4 HDMI con TDT salida RF modulador codificador [47].....	47
Figura 20. Topología de Red actual de la empresa NETSURTV. ....	50
Figura 21. Mikrotik CCR1036-12G-4S [48] .....	51
Figura 22. Configuraciones de puertos ethernet en el MikroTik de la empresa NETSURTV. ....	52
Figura 23. Configuraciones de enrutamiento en el MikroTik de la empresa NETSURTV. ....	53
Figura 24. Reglas de filtros en el firewall del Mikrotik de la empresa NETSURTV. ....	54
Figura 25. Árbol de colas implementadas en el Simple Queues en del MikroTik de la empresa NETSURTV.....	56
Figura 26. Monitoreo de consumo de ancho de banda el día 26/05/2022. ....	56
Figura 27. Monitoreo de consumo de ancho de banda semanal. ....	57
Figura 28. Monitoreo de consumo de ancho de banda mensual. ....	58
Figura 29. Monitoreo de consumo de CPU. ....	59
Figura 30. Topología de red propuesta. ....	59
Figura 31. Simulación de la Topología de Red propuesta en GNS3.....	63
Figura 32. Instancia BGP implementada. ....	65
Figura 33. Creación del Peer BGP.....	65
Figura 34. Sesión eBGP establecida dentro del Peers. ....	66
Figura 35. Segmentos de Direcciones IP compartidas con AS del proveedor. ....	66
Figura 36. Tabla de rutas.....	67
Figura 37. Reglas de Filtro implementadas en el Firewall de la red simulada. ....	67
Figura 38. Reglas implementadas para evitar ataques DDoS. ....	68
Figura 39. a) Inicio de ataque DDoS. b) Supresión de ataques DDoS. ....	69
Figura 40. Regla implementada para dar acceso al equipo principal. ....	70
Figura 41. a) Negación de acceso al router. b) Permiso de acceso al router. ....	70
Figura 42. Árbol de colas implementado para el control de ancho de banda. ....	71
Figura 43. Mangle realizado para el marcado de paquete del control de ancho de banda. ....	72
Figura 44. Test de velocidad realizado en el computador de prueba. ....	72
Figura 45. Configuración del NAT para la notificación del corte de servicio.....	73

Figura 46. Agregar la dirección 10.10.20.5 dentro del address list Deudores .....	74
Figura 47. Mensaje de notificación de corte de servicio.....	74

## ÍNDICE DE TABLAS

Tabla 1. Presupuesto para el sistema digital .....	47
Tabla 2. Configuraciones para el codificador.....	48
Tabla 3. Configuraciones para el IPQAM [46].....	49
Tabla 4. Direccionamiento IP de las Interfaces LAN.....	53
Tabla 5. Comparación entre el sistema actual y el diseño digital propuesto.....	62

# CAPITULO I

## 1. INTRODUCCIÓN

La empresa de Red de Telecomunicaciones del Sur, NETSURTV, ubicada en la ciudad El Cambio de la provincia El Oro, ha surgido desde el 2015 y comenzó su emprendimiento con el servicio de televisión por cable. A partir del 2019 instalan una red de acceso con fibra óptica para brindar navegación a internet en los hogares; a través del tiempo han adquirido un incremento en la cantidad de clientes, pero el sistema actual que poseen no permite ampliar ni mejorar la calidad de sus servicios.

Actualmente, la mayoría de empresas competitivas de telecomunicaciones utilizan sistemas digitales para ofrecer televisión con canales en alta definición y administran las redes con todos sus protocolos correspondientes para proveer acceso a internet. Es por eso que el propósito de este proyecto es analizar la infraestructura actual de NETSURTV, proponer un diseño que brinde mejoras estructurales y puedan ser aplicadas en la actualidad o en un futuro.

En sí, el sistema de Antena Comunitaria de Televisión (CATV) que usa NETSURTV es análogo y digital; la resolución de imagen se limita a ser estándar y para cambiar la calidad de las señales se quiere un sistema totalmente digital. Para esto se ha investigado de los diferentes modelos de los sistemas digitales de televisión y de tal manera que la infraestructura actual se pueda acoplar con la solución más factible de implementar.

Adicional, el router Mikrotik no presenta todas las configuraciones respectivas para una empresa proveedor de servicios de internet (ISP), las cuales brindan un control seguro de la red y disminución de latencias por tráfico de paquetes. Por lo tanto, se realizará una simulación de la red actual que posee la empresa a través del GNS3 y se comparará sus resultados con los obtenidos en la simulación del diseño propuesto.

Se presentará un estudio de los sistemas actuales que posee NETSURTV y de la solución que se propone en este proyecto, dado los resultados obtenidos se concluirá que infraestructura le favorece a la empresa de manera económica y también las configuraciones que necesita en la red proveedora de internet.

### **1.1. Definición del problema**

La empresa de “Red de Telecomunicaciones del Sur”, NETSURTV S.A., es un proveedor de servicios de internet y televisión por cable de fibra óptica, creada en el año 2015. Desde un principio la empresa ofreció servicios de TV por cable y a partir del año 2019 empezaron a ofrecer los servicios de internet en la ciudad del El Cambio, ubicada en la provincia del El Oro.

Debido al incremento de proveedores de servicio de internet en la zona, según la ARCOTEL hay un total de 789 ISP que prestan sus servicios en diferentes modalidades a nivel nacional [1], y a la gran demanda de clientes que han obtenido en los últimos años; NETSURTV requiere mejorar la calidad de sus servicios tanto en televisión e internet. De esta manera los usuarios podrán experimentar la visualización de canales en alta definición (HD) y eficaz conectividad a internet.

La infraestructura actual de la empresa cuenta con un sistema de transmisión de televisión que está compuesto por Receptores de Satélites con la capacidad de recibir audios, videos y datos encriptados [2]. Las señales de audio y video que son captados por el receptor satelital son moduladas y después son combinadas a través de un mezclador de señales, CATV Mixer de 2400 MHz, pero este modelo implementado no le permite a la empresa brindar transmisión en alta definición (TV HD), por lo tanto, su competitividad se ve reducida en el mercado de las telecomunicaciones.



Por otra parte, los equipos de red que da el acceso a internet no poseen una administración y configuración acorde a una empresa ISP, dado que no cuentan con una correcta gestión en el tráfico de la red, control de ancho de banda, implementaciones de seguridad, entre otras. Por ende, los clientes han presentado falencias en la navegación de internet en horarios donde los usuarios utilizan con más frecuencia este servicio.

## **1.2. Justificación del problema**

En la actualidad, el servicio de acceso a internet se ha convertido en una herramienta fundamental para promover el desarrollo económico y social de la comunidad poblacional, gracias a su acceso, las personas pueden utilizar aplicaciones relacionadas a la educación online, el teletrabajo, la telesalud, los cuales son esenciales en los contextos actuales [3].

Por ello, masificar su acceso no solo debe ser tratado como un interés comercial, sino que también involucra el interés social, ya que muchas veces estos servicios no suelen ser los más óptimos y presentan muchas falencias. Por tal razón el rol que cumple la empresa proveedora del servicio de internet es de brindar un servicio alta calidad.

Los proveedores de servicio de internet son los responsables de conectar a los usuarios finales y las empresas al internet público. En el 2020, acorde a la ARCOTEL, el número de proveedores ha aumentado en los últimos años en aproximadamente 21 veces a nivel nacional y debido al elevado número de proveedores existe una fuerte competencia en términos de precio, calidad, garantía, entre otros. [4] Por lo tanto, la necesidad de las ISP en estar en constante evolución y desarrollo, con el incentivo de ser una empresa competitiva y de cumplir con las necesidades de sus usuarios.

Es por eso que la empresa NETSURTV S.A. se ve en la obligación de optimizar la red actual que tiene para garantizar un servicio de alta calidad y así competir con las otras empresas que se posicionan en este mercado. Además, los cambios propuestos pueden mejorar su imagen corporativa lo cual le permitirá a atraer a nuevos clientes y conservar a los actuales.

### **1.3. Objetivos**

#### **1.3.1. Objetivo general**

- Determinar las soluciones tecnológicas que requiere la empresa NETSURTV para mejorar sus servicios de televisión y de internet.

#### **1.3.2. Objetivo específico**

- Estudiar los sistemas actuales de telecomunicaciones que posee la empresa para la identificación del problema.
- Diseñar un sistema alternativo para el sistema CATV Análogo que brinde servicio de televisión en alta definición a los usuarios.
- Simular la topología de red que posee NETSURTV en el software GNS3 con las configuraciones importantes para una empresa ISP.
- Realizar un presupuesto para el sistema CATV Digital que sea factible implementar y proporcione satisfacción al cliente.
- Implementar las configuraciones simuladas en el Mikrotik de la empresa una vez se haya obtenido resultados exitosos en el software GNS3.

### **1.4. Estado del arte**

A través de los años ha surgido avances en el área de las telecomunicaciones, tal como la transición de la televisión analógica a digital, la Unión Internacional de las

Telecomunicaciones (UIT) [5] menciona que la televisión digital brinda una mejor calidad de multimedia y variedad de canales. Además de proporcionar un servicio mejorado, indican que este cambio ayuda a reducir la emisión de gases de efecto invernadero, dado que el sistema de transmisión digital reduce casi diez veces el consumo.

Así mismo, en la Universidad Nacional de Colombia [6] se ha realizado un estudio sobre las ventajas y desventajas de la televisión digital terrestre y la televisión análoga a nivel ambiental; basándose en la norma técnica colombiana NTC-ISO 14040, es importante evaluar las entradas, salidas e impactos ambientales de los sistemas a lo largo de su ciclo de vida.

En [6] se toma como referencia un estudio práctico de los diferentes sistemas o estándares para la emisión terrestre de programas digitales, los cuales son: Advanced Television Standards Committee (ATSC), Digital Video Broadcasting-Terrestrial (DVB-T/DVB-T2), Digital Terrestrial Multimedia Broadcast (DTMB) y Integrated Services Digital Broadcasting – Terrestrial (ISDB-T). Se pudo concluir a través de estas pruebas que los estándares DVB-T, ATSC y ISDB-T poseen la capacidad de operar en un ancho de banda de 6 MHz, transmitir en alta definición y mejor cobertura.

En [7] se realizó un proyecto teórico para la construcción de un sistema cabecera de televisión por cable, en el cual es simulada dentro de una plataforma general de transmisión con las funciones de cada equipo. En este proyecto se analiza las distintas tecnologías y estándares DVB: DVB-C, DVB-C2 y DVB-IPTV, dado que la más acertada es DVB-IPTV por su mayor aceptación y los beneficios que brinda en velocidad, seguridad y calidad.

El artículo de Ir India, [8], habla sobre las últimas tendencias en las comunicaciones de televisión por cable, se menciona que el sistema de televisión por antena comunitaria (CATV) con línea analógica es una red simple que puede expandirse en lugares limitados, pero en caso que se requiera ampliar la red, la calidad de servicio decrece y tiene un alto costo.

Un problema en este tipo de red analógica es que no se puede mantener la calidad de transmisión y aumentar el número de canales; en cambio, el mismo sistema de televisión con línea digital brinda imagen en alta definición y variedad de canales, también a un costo alto en implementación [8].

En [8] la estructura básica para el sistema de televisión por cable con línea digital está compuesta de un splitter 1:4, un receptor satelital digital para cada puerto del splitter y un encoder MPEG-2/4 para cada receptor, cada canal codificado es multiplexiado para obtener el contenido de cada canal. Por último, se modula la señal y entra al transmisor óptico para amplificar y combinar la señal.

En el proyecto integrador [9] considera el sistema IPTV como algo innovador dado que obtienen una oferta ilimitada de canales de televisión digital y música, programación pagada por evento, Video On Demand (VOD) y la grabación de video (PVR). También se puede unir esta infraestructura a una red para brindar servicios de conexión a internet, donde se requiere un mínimo de 4 Mbps para recibir la señal TV comprimida en formato MPEG-2 o MPEG-4.

Es por eso que [9] utiliza una estructura en base de satélites conectados a un Super Head End (SHE), en donde se almacena el contenido original de los proveedores de programación, se convierte en señal digital para ser entregada a la red de IPTV y es transmitida al VSO y servidores. En sí, el SHE tiene la función de agregar contenido de

diferentes proveedores, convertir la señal en formato estándar, transportar la señal comprimida a cada Video Serving Office y por último debe ser codificado y convertido en un formato que pueda interpretar el Set top Box (STB).

En Quito se realizó análisis sobre la televisión digital del grupo TVCable, empresa de telecomunicaciones del Ecuador, se menciona que la función de la red Core de televisión digital es de recepcar, digitalizar y combinar las diferentes señales de televisión. [10] Dicha señal es amplificada y combinadas nuevamente con las señales que genera el Sistema de Terminación de Cablemódems (CMTS), y, por último, son enviadas a través de la red de fibra óptica hacia la red troncal.

En sí, el grupo TvCable utiliza 6 fases para el servicio de televisión pagada y los elementos que se utilizan son: receptores satelitales, amplificadores, convidadores y divisores de señales [10].

En este proyecto [10] se denota el diagrama de la red de Core de Tv, en su primera fase usan los canales inalámbricos, antenas parabólicas; splitters satelital ATX y el receptor satelital Cisco D-9854. En la fase 2, Digitalización, se utiliza un encoder Arris y un Modular Media Converter, ambas señales de salida se dirigen a un switch Cisco 6509 y los puertos IP entran al Broadcast Network Process. En la fase 3 se realiza la combinación de señales, en la fase 4 se amplifica la señal, en la quinta fase se distribuye y al final es transmitida.

Así también se hizo un estudio y diseño de una red para brindar servicio de televisión e internet para la empresa Cabletel-Sepormul en Cuenca, en [11] tomaron como referencia una infraestructura cabecera que receptan la señal desde una antena de muy alta frecuencia (VHF). Para este estudio y diseño se realizó la comparación de los

diferentes sistemas Headend, de los cuales escogieron la Digital por el buen servicio que brinda al usuario.

En un estudio realizado por estudiantes de la Corporación Universitaria Tecnológica de Bolívar se proponen varias técnicas para optimizar el ancho de banda [12], de las cuales se destaca el control de calidad de servicio (QoS) por su versatilidad en varias aplicaciones como la de administración de congestión de tráfico, administración de colas, adecuación de tráfico y monitoreo, etc. Además, recomienda el uso de técnicas de encolado para la administración del tráfico de la red, dentro de las cuales se menciona el encolado equitativo ponderado distribuido, encolado equitativo, prioridad de encolado, encolado común, etc. Este último mencionado es el que planeamos aplicar a nuestra solución, ya que se realiza a través de un esquema de tráfico ordenado que especifica el ancho de banda mínimo para controlar ciertos tipos específicos de tráfico.

Por otro lado, en un estudio realizado en la Pontificia Universidad Católica del Ecuador se planteó la aplicación de QoS para la optimización del ancho de banda de una red [13], bajo el modelo de Servicios Diferenciado (DiffServ) debido a que este modelo ofrece flexibilidad, escalabilidad, distinción de diferentes clases de servicios, entre otros. Además de la utilización de listas de control de acceso (ACL) para la clasificación del tráfico de la red, DiffServ Code Point (DSCP) para el marcado de paquetes y finalmente como técnica de encolamiento a Priority Queuing (PQ) y Weighted Fair Queuing (WFQ). Para nuestro proyecto el modelo de calidad de servicios se basará en DiffServ, ya que este modelo se aplica mediante en el marcado de paquetes, pero para nuestro caso la técnica de encolamiento escogida será encolado común o Common Queuing (CQ).

En un estudio realizado en la Universidad Católica de Santiago de Guayaquil [14] en el cual se analizaron los fundamentos teóricos de control de tráfico mediante colas y

calidad de servicio se determinó que para tener un mejor control del tráfico de una red es indispensable el marcado de paquetes, ya que esto ayudara a una correcta distribución del uso de ancho de banda disponible en un segmento de la red, además se comprobó que al aplicar este tipo de control de tráfico es beneficioso para que no exista saturación en la red.

En un estudio realizado en la Escuela Politécnica de Ejercito basado en el manejo del ancho de banda [15] se propuso la implementación de QoS y control de ancho de banda para la optimización de los recursos de la red de la Escuela Politécnica de Ejército sede Sangolquí, en base a la creación de una estructura mangle para la obtención de paquetes y la implementación de colas a través del árbol de colas Queue tree, lo cual les permitió la manipulación y clasificación del tráfico de la red, obteniendo como resultado una mayor seguridad y mejor calidad de servicios en la red.

En el estudio realizado en la Universidad Estatal Peninsular de Santa Elena se planteó la implementación de un sistema de red [16], en el cual usan la herramienta Graphs para el monitoreo de consumo de red, el uso de un servidor denominado ThunderCache para el manejo del tráfico de la red y mark ruting para el marco de paquetes, además de la implementación de Simple Queues para el control de ancho de banda de los usuarios, permitiéndoles obtener hasta un 56% del ahorro de consumo de ancho de banda. Lo cual nos muestra que si realizamos un uso adecuado de las técnicas para el manejo del tráfico y ancho de banda de una red nos permitirá obtener resultados óptimos no solo para mejorar la calidad de los servicios, sino que también dar una mejora operativa de nuestras redes.

En un estudio realizado por un alumno de la Escuela Politécnica Nacional se propuso rediseñar la infraestructura de red de la ISP READYNET, para conversión de la ISP a

un sistema autónomo. El rediseño se planteó como la necesidad de tener una red que pueda crecer sin problemas (alta escalabilidad), permita aplicar procesos eficientes de enrutamiento y tener recursos de direccionamiento IP que les eviten depender de otros proveedores. Además, recalca que la adquisición de un sistema autónomo se la plantea solo cuando las políticas de enrutamiento a implementarse difieren con las políticas de las empresas proveedoras [17].

### **1.5. Alcance del proyecto**

El objetivo de este proyecto es obtener dos soluciones para los servicios que brinda la empresa NETSURTV S.A., el diseño para un sistema digital de televisión por cable y la simulación de la red de internet con los parámetros y configuraciones correspondientes a una compañía ISP.

La estructura del sistema de televisión actual transmite alrededor de 40 canales en definición estándar, donde su calidad de imagen no es mayor de 480p, para aumentar la resolución de imagen se debe obtener las señales audio y video por una interfaz multimedia de alta definición. Por lo tanto, el diseño se basará en acoplar equipos robustos y que transmitan el contenido en alta definición, sin tener que cambiar toda la estructura actual.

Por otro lado, para la red de acceso a internet, compuesta por dos partes, una de acceso y la otra de distribución por fibra óptica (FTTH-GPON), la solución se centrará en los problemas presenten en la red de acceso. Es por eso que se realizará la simulación de la red de acceso mediante el programa GNS3 y después se procederá a aplicar todas las soluciones que se podrían implementar dentro de su equipo Mikrotik para la optimización de la red y para la aplicación de las mismas quedara a disposición del cliente.



Cabe mencionar que para el análisis del estado actual de la red se realizarán configuraciones que no afectaran al desempeño de la red como es la captura de paquetes, monitoreo de tráfico, graficas de consumo, ping a clientes, etc.

## 1.6. Metodología

La empresa cuenta con 2 servicios diferentes, por lo tanto, se plantearán dos metodologías distintas para llegar a una solución para cada servicio.

### 1.6.1. Sistema de transmisión para televisión o CATV:

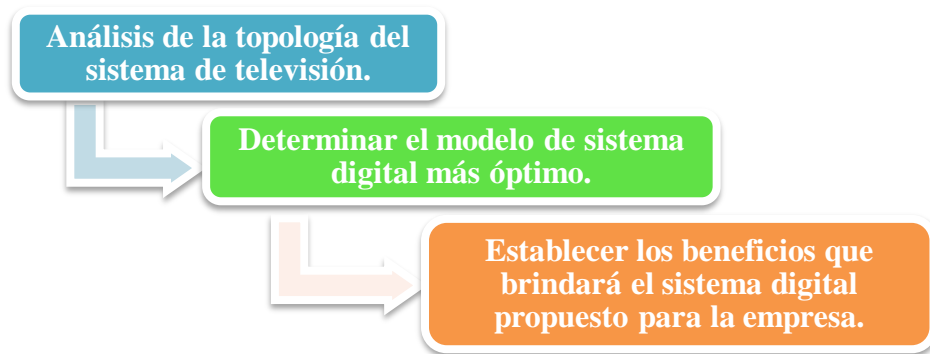


Figura 1. Diagrama de bloques para la solución del sistema de televisión.

En la Figura 1 se plantea primero el análisis de la estructura actual que posee la empresa, tomando en cuenta que posee equipos que cumplen funciones correspondientes para realizar la transmisión de canales. Acorde a las investigaciones, un sistema de televisión realiza 4 fases: Recepción, Digitalización, Modulación y Transmisión; por lo tanto, el diseño propuesto debe efectuar con cada etapa.

En la segunda etapa del diagrama se determina el tipo de modelo CATV que cumple con los requerimientos de NETSURTV S.A. y a su vez se ajuste a la estructura actual, de esta manera se considerará un diseño que reemplace los equipos analógicos y realice la transmisión de contenido en línea digital.

Por último, se realizará la comparación entre los beneficios que proveerá el diseño propuesto con el actual, tanto en calidad, costo, configuraciones y proyectos futuros.

### 1.6.2. Red de acceso a internet



Figura 2. Diagrama de bloques de la solución para la red de acceso a internet.

En cambio, en la Figura 2 se plantea una fase de análisis de red en la que se determinarán todos los posibles problemas que se presentan en la red, en especial dentro de las configuraciones del equipo de administración central de la red (Mikrotik CCR1036) para esto se realizarán capturas de paquetes, monitoreo de tráfico de la red, graficas de consumo, etc. Con los resultados obtenidos en el análisis de la red, se plantearán las posibles soluciones acorde a cada problema detectado; las cuales serán probadas en la fase de la simulación.

Dentro de la fase de simulación se recreará la topología red de acceso de internet planteada en la fase anterior mediante el simulador GNS3 y se aplicaran todas las posibles soluciones diseñadas. Finalmente, para la fase de aplicación se presentará la simulación al cliente para que observe los posibles cambios que se pueden aplicar a su red y así los apruebe para aplicarlos dentro de su equipo principal.

## **CAPÍTULO II**

### **2. MARCO TEÓRICO**

#### **2.1. Sistema de televisión**

Es un medio de comunicación que provee servicios de multimedia, este sistema realiza la transmisión de imagen, video y sonido desde una fuente hasta su receptor. La señal de televisión es entregada a través de diferentes medios como: ondas de radio terrestres, cables coaxiales, satélites e internet [18].

### **2.1.1. Televisión analógica**

Esta tecnología utiliza señales analógicas para la transmisión de video y audio; características como el brillo, colores y sonido son representados a través de variaciones rápidas de la señal según su frecuencia, amplitud o fase [19].

En sí, este sistema utiliza la modulación por amplitud (AM) para la transmisión de video y la modulación por frecuencia (FM) para transmitir la señal de audio, por lo tanto, el sistema presenta interferencias, imágenes fantasmas y nieve [19].

### **2.1.2. Televisión digital**

La televisión digital realiza la transmisión de audio y video como bits de información de datos, lo que hace que la señal tenga dos estados: 1 y 0, “encendido” y “apagado”. Dado esto, las señales digitales son finitas y no permite que su calidad varíe dentro una distancia, este sistema previene las pérdidas graduales de la señal a pesar de las largas distancias entre el transmisor y receptor [19].

El sistema digital de televisión fue diseñado desde cero, proporcionando más servicios como audio en múltiples idiomas, sonido envolvente, subtítulos, mayor cantidad de canales en un mismo ancho de banda y alta definición de imagen [19].

Existen diferentes topologías de televisión digital, como se muestra en la Figura 3, en la parte de recepción de señal digital se utiliza distintos elementos como: satélite, coaxial, internet, terrestre, etc [20] .

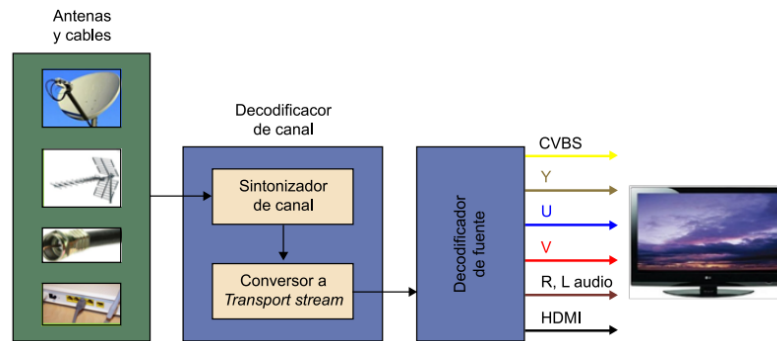


Figura 3. Diagrama universal de receptores digitales [20]

Es esencial que el circuito de receptores conste de dos fases, decodificador de canal y decodificador de fuente. En sí, el chip de codificador de canal dependerá del medio por el cual se extrae los paquetes de información encapsulados, consta de un sintonizador de canal y el convertor a paquetes de *Transport Stream*, este último se obtendrá mediante la modulación y decodificación de la señal. La siguiente fase fundamental es la decodificación de fuente, donde se convertirá los paquetes de *Transport Stream* en información de audio y video en banda base [20].

#### 2.1.2.1. Televisión digital por cable

La señal se distribuye a través de un cable de red, puede ser coaxial o de fibra óptica. A través de esta red, el proveedor puede admitir servicios de telefonía y conexión a internet.

De aquí parte el sistema Community Antenna Television (CATV), su implementación es ideal en zonas con mala recepción satelital. Existe el sistema CATV análogo y digital, donde este último provee servicios más interactivos y de mejor calidad [21].

### 2.1.2.1.1. Estructura de un sistema CATV

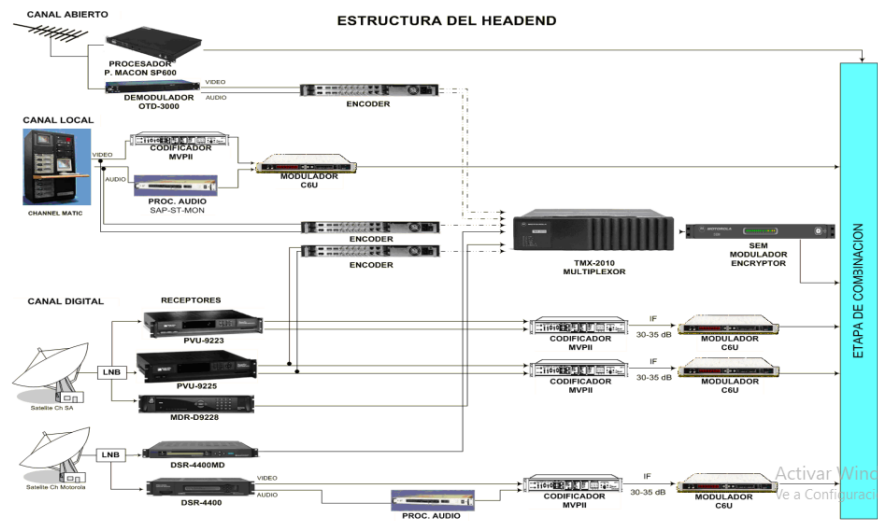


Figura 4. Estructura de un sistema de cabecera [22]

En la Figura 4 se muestran las diferentes soluciones para implementar un sistema CATV digital, se utilizan equipos como receptores satelitales, decodificadores, moduladores, multiplexores, etc. Este sistema posee la versatilidad de recibir el contenido multimedia por varias fuentes, DVB-S/S2, DVB-T/T2, DVB-C, ASTC, ISDB-T e IPTV y después convertirla en un formato estándar [22].

### 2.1.2.1.2. Televisión por protocolo de internet (IPTV)

El sistema de protocolo de internet la señal se distribuye mediante un protocolo de red hasta su usuario final, usualmente a través de conexiones de datos ADSL de alta velocidad [23].

Se puede acoplar un sistema IPTV en un sistema CATV, tal como se presenta en la Figura 5, en este caso se usa un encoder o decodificador para obtener una señal de dato IP y que es compatible con diferentes equipos de red.

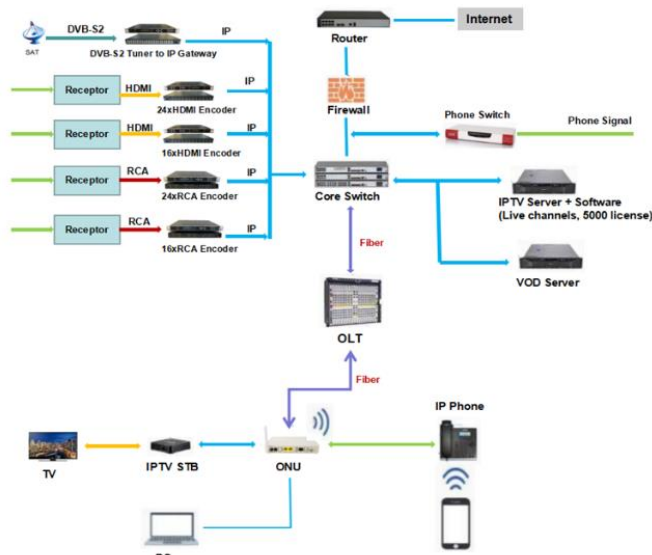


Figura 5. Sistema FFTH IPTV [24]

## 2.2. Configuraciones para el sistema de televisión

### 2.2.1. Modulación de amplitud en cuadratura (QAM)

Es una técnica que transporta dos señales de manera independiente y mediante la modulación, tanto en fase y amplitud, de una señal portadora. Para esto se modula una misma portadora con desfase de  $90^\circ$ , a diferencia de otros tipos de modulación digital, el QAM combina la modulación de fase y amplitud [25].

Su mayor ventaja es la inmunidad al ruido, consumo de energía eléctrica y su gran capacidad para transportar más información en comparación a los métodos analógicos. Permite la transmisión de información en mejor calidad y seguridad de datos [25].

La modulación QAM se representa a través de diagramas de constelación, donde el número de puntos de constelaciones es en potencia de 2 y es el orden de modulación. Los formatos comunes son 16QAM, 64QAM, 256QAM, etc.; tal como se muestra en la Figura 6 [26].

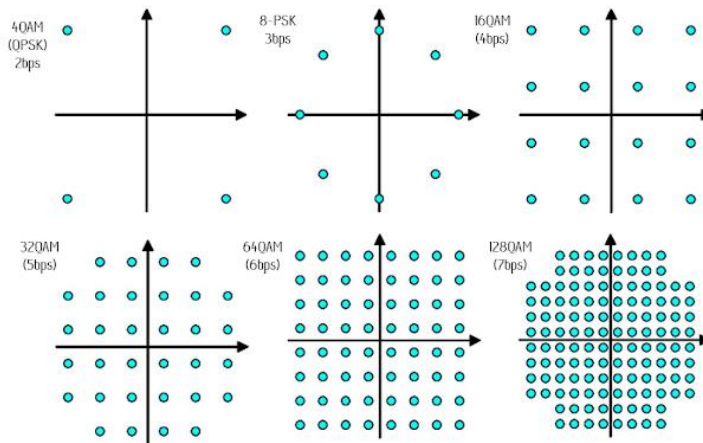


Figura 6. Los diferentes órdenes de modulaciones QAM [27]

Mientras mayor es el orden de modulación, se puede transportar más bits por símbolo, lo que implica una mejor velocidad de datos y tal como se explica en la Figura 7, en un esquema de modulación de orden alto, se puede transmitir mayor información [26].

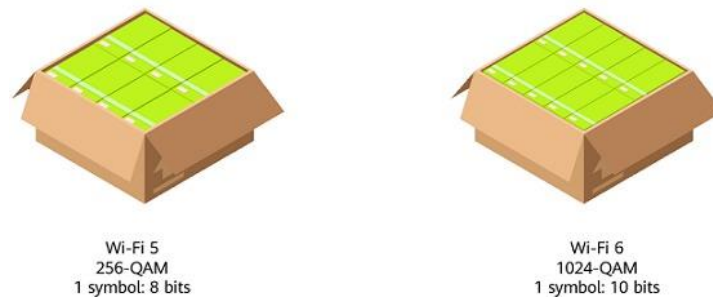


Figura 7. Ejemplo de cantidad de bits por símbolo [26]

El orden de modulación dependerá de las condiciones del entorno, ya que, si la información se transmite en un ambiente “ruidoso”, es difícil modular una gran cantidad de símbolos [26].



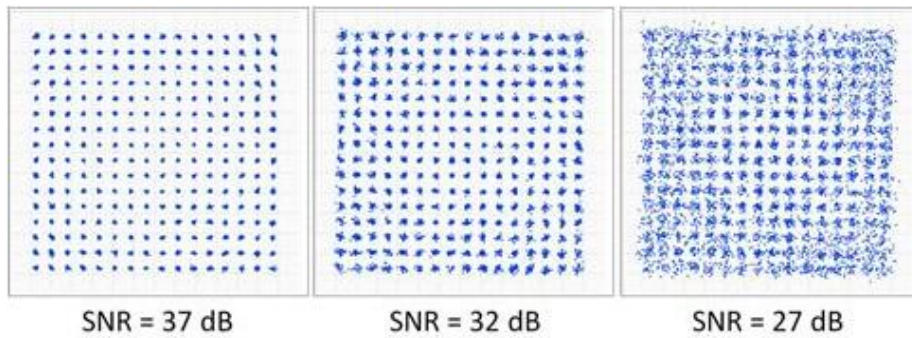


Figura 8. Modulación 256-QAM con diferentes SNR [26]

En la Figura 8 se muestra tres casos de modulación de orden 256 y con diferentes valores de relación señal/ruido, a medida que disminuye, las constelaciones muestran mayor separación entre ellas y la información se modula con errores [26].

Por lo tanto, ante escenarios con interferencias, es ideal realizar modulaciones de orden inferior, aunque este implique reducir la velocidad de transmisión de datos.

### 2.3. Proveedor de servicio de internet (ISP)

Un ISP (Del término en inglés Internet Service Provider) es un término utilizado para identificar a las empresas que brindan conectividad a internet, tanto a usuarios individuales como a hogares u otras empresas. Estos servicios de acceso al internet lo realizan mediante distintas tecnologías como Digital Subscriber Line (DSL), Cablemódem, Dial-up, GSM, Wifi, etc [28].

#### 2.3.1. Infraestructura de una ISP

Una infraestructura de ISP se refiere a todos los componentes tanto de hardware (computadoras, routers, switches, servidores, cableado, etc.) como del software (sistemas operativos, aplicaciones, etc.) y servicios externos como firewalls. La infraestructura de red representa en conjunto todas las comunicaciones y conectividades de una empresa.

Las infraestructuras de red suelen estar estructuradas en base a un modelo jerárquico. Los modelos jerárquicos ayudan a la organización de una red permitiendo el control del tráfico a nivel local y evitando que se disperse innecesariamente por la red.

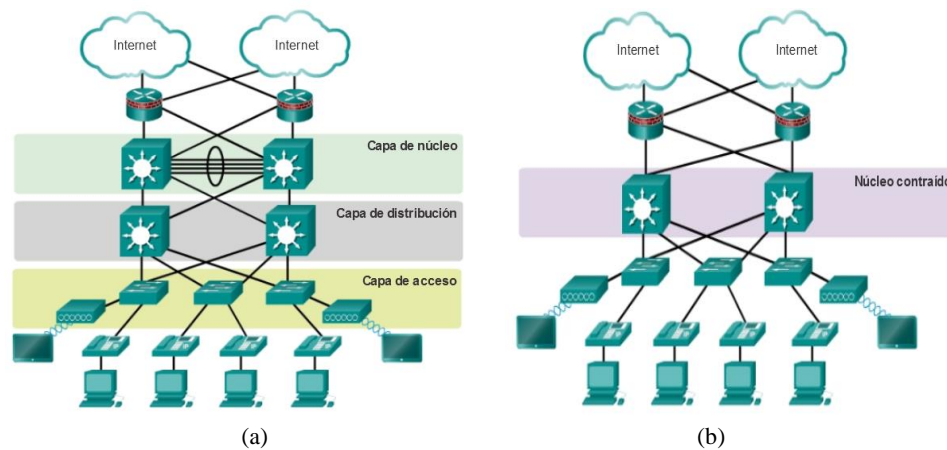


Figura 9. a) Modelo jerárquico de 3 capas. b) Modelo de Núcleo contraído [29]

En la Figura 9.a, se muestra un modelo jerárquico que reparte las funciones de la red en tres diferentes capas. La capa de acceso se encarga de dar conectividad a los usuarios, mientras que en la capa de distribución se envía el tráfico de una red de área local (LAN) a otra y finalmente la capa de núcleo es la troncal de la red que proporciona conectividad de alta velocidad a toda la red.

A pesar que el modelo jerárquico de 3 capas es muy utilizado, existen redes que se implementan basadas en 2 niveles de jerarquía, tal como se muestra en la Figura 9.b. El modelo de núcleo contraído combina la funcionalidad de las capas de distribución y núcleo en una sola capa, esto se suele hacer para reducir costos de implementación y complejidad en una red [29].

## **2.3.2. Elementos principales de una red**

### **2.3.2.1. Router**

El router o enrutador es un dispositivo encargado de proporcionar conectividad a redes informáticas, mediante el enrutamiento o encaminamiento de paquetes de datos a través de la red para llegar a su destino por la ruta más adecuada. [30]

### **2.3.2.2. Switch**

Un switch o también denominado conmutador, es el dispositivo que se encarga de interconectar varios equipos en una misma red, formando las conocidas redes de área local o LAN. Por sí solo no puede proporcionar conectividad hacia otras redes o a internet, es por eso que trabajan en conjunto con los routers, permitiendo el escalado de una red. [31]

### **2.3.2.3. Sistema operativo**

Un sistema Operativo es el software que permite administrar todos los dispositivos de un equipo, proporcionando una interfaz más simple para que los usuarios mediante programas o aplicaciones puedan comunicarse con el hardware [32].

## **2.4. RouterOS**

Es un sistema operativo desarrollado por Mikrotik, el cual ofrece una interfaz que permite configurar y operar un enrutador con todas las funciones necesarias: enrutamiento, firewall, administración de ancho de banda, punto de acceso inalámbrico, puerta de enlace de punto de acceso, servidor VPN, etc [33].

### 2.4.1. Winbox

Es una aplicación desarrollada por Mikrotik que permite a través de una interfaz gráfica la administración sencilla de Mikrotik RouterOS. Esta aplicación tiene la capacidad de establecer conexiones vía telnet, SSH y FTP. [34]

### 2.4.2. Firewalls

El firewall se utiliza menudo como una herramienta de seguridad para impedir el acceso no autorizado de agentes externos a la red interna o al propio enrutador, denegar y bloquear varios tipos de ataques y controlar la fuga de datos de entrada y salida. Las reglas que a menudo se configuran se las organiza en cadenas, de las cuales existen 3 de ellas:

- **Input:** Cadenas de paquetes que ingresan al enrutador, a través de una interface que tiene un direccionamiento IP destino conocida por el enrutador.
- **Forward:** Cadena de paquetes que pasan por el enrutador.
- **Output:** Cadena de paquetes originados dentro del enrutador.

#### 2.4.2.1. Firewall: Filter rules

Son el conjunto de reglas de filtrado implementadas dentro del Firewall, las cuales permiten el control de paquetes de datos hacia, desde y a través del enrutador. Dentro de las cuales destacamos las siguientes:

- **Accept:** Acepta un paquete predeterminado de datos, el cual no pasara por otra regla dentro de las reglas de filtrado.
- **Passthrough:** Permite contabilizar paquetes que coinciden, al pasar por esta regla.
- **Drop:** Excluye paquetes de datos.
- **Reject:** Dropea paquetes de datos y transmite un mensaje ICMP de descarte.

- **Tarpit:** Contiene y detiene paquetes de conexiones TCP (envía mensajes SYN/ACK al TCP SYN de paquetes entrante).
- **Established:** Consiste en paquetes generados por conexiones existentes.
- **New:** Consiste en paquetes originados por nuevas conexiones o están relacionados a conexiones que comparten por primera vez paquetes.
- **Invalid:** Son paquetes que no está relacionados u originados por alguna conexión conocida o establecida.

#### 2.4.2.2. Firewall: NAT

Las NAT o nateo es un método que permite a los hosts utilizar un conjunto de direcciones IP en una red LAN para realizar comunicaciones internas y externas. Existe dos tipos de NAT los cuales son:

- **Source NAT (srcnat):** Paquetes originados en una red NAT, se producen cuando el enrutador sobrescribe la dirección IP de origen privada por una dirección IP pública.
- **Destination NAT (dstnat):** Paquete de destinados en una red NAT, esta acción produce que un enrutador reemplace la dirección IP de destino por un paquete IP que viaja a una red privada.

#### 2.4.2.3. Firewall: Mangle

El Mangle permite realizar marcado de paquetes que pasan por el enrutador y se las utiliza para realizar acciones como el control de ancho de banda, calidad de servicio o QoS, NAT, etc. La regla del Mangle está organizada en una secuencia y sigue la misma regla general de la regla de filtro, dentro de las cuales destacamos las siguientes:

- **Prerouting:** Marca de paquetes antes que ingresen al router.
- **Postrouting:** Marca de paquetes antes que salgan del router.
- **Mark-connection:** Realiza una marca a una conexión establecida.
- **Mark-packet:** Realiza una marca a paquetes específicos.

- **Mark-routing:** Realiza una marca de paquetes bajo una política de enrutamiento.

### 2.4.3. Calidad de servicio o QoS

La calidad de servicios (QoS) se utiliza para priorizar, gestionar, controlar o administrar el tráfico en una red, con la finalidad de reducir las pérdidas de paquetes de datos y evitar el congestionamiento del tráfico en una red. Entre las ventajas de la aplicación de QoS están: [35]

- Dar un mejor rendimiento del ancho de banda disponible.
- Prevenir la monopolización del tráfico en una red.
- Priorizar el tráfico de servicios sensibles.
- Brindar un valor agregado al servicio que se está prestando.

Las desventajas son:

- El incremento del uso de recurso de CPU.
- Análisis exhaustivos para conocer las necesidades de una red.

#### 2.4.3.1. Queues

El Queues permite la manipulación y el manejo de tráfico a través de:

- Limitar el ancho de banda en puertos de enlace, segmentos de direcciones IP, VLANs, protocolos, y entre otros parámetros.
- Priorizar el flujo de determinados paquetes de datos sobre otros.
- Limitar el tráfico de redes punto a punto (p2p).
- Crear límites de ancho de banda en franjas horarias predeterminadas.
- Gestionar el ancho de banda que contrate cada cliente dependiendo de las necesidades que este disponga.

Existe dos maneras distintas de manipular Queues dentro de Mikrotik RouterOS: Queues Simple y Queues Tree.

### 2.4.3.2. Queues simple

Mediante el uso de Queues Simple se facilita mucho la aplicación de límites de ancho de banda específicos a direcciones IP o subredes, y además permite la configuración de QoS avanzados. Entre las características útiles tenemos [36]:

- Encolamiento de tráfico p2p.
- Crear colas con determinados patrones en cierto lapso de tiempo.
- Priorizar tráfico en la red.
- Utilizar marcas de paquetes creadas en el firewall mangle.
- Configurar colas bidireccionales para limitar el tráfico de carga y descarga.

### 2.4.3.3. Queues tree

Queue Tree se emplea para realizar colas avanzadas permitiendo aplicar políticas de prioridad global, implementar límites de tasa de datos a dirección de IP, protocolos, puerta de enlace, etc. Para su implementación es necesario crear marca de paquetes dentro del firewall mangle y crear una cola direccional dentro de los HTB. [36]

#### 2.4.3.3.1. HTB

HTB (Del término “Hierarchical Token Bucket”) es un método útil para manejar diferentes tipos de tráfico mediante el uso de colas de clases. Para aplicar este método se debe de seguir los tres siguientes pasos [37]:

- **Coincidencia y marcado del tráfico:** Consiste en clasificar el tráfico y elegir paquetes que tengan coincidencias para una clase de cola predeterminada.

- **Implementar políticas para el marcado del tráfico:** Colocar específicamente una clase de tráfico en una cola predeterminada y elegir qué acciones se aplicarán para cada clase.
- **Incluir políticas para una o más interfaces específicas:** Añadir políticas para distintas interfaces (global-in, global-out o global-total) o para una determinada cola padre.

## 2.5. Sistema autónomo

Se considera Sistema Autónomo (AS) al conjunto de redes de direcciones IP que aplica una política de enrutamiento independiente y propia. Cada AS se les asigna un número único que lo identifica como sistema autónomo y les permite compartir información con otros AS en el internet. El número de sistemas autónomos (ASN), en un inicio eran números enteros de 16 bits, pero debido al crecimiento de los ISP se crearon los ASN de 32 bits [38].

Los AS comparten información mediante la comunicación de enrutadores, utilizando protocolos como BGP (Border Gateway Protocol) para la actualización de las tablas de rutas y además comparten tráfico de una red a otra.

### 2.5.1. BGP

El protocolo BGP (Del término “Border Gateway Protocol”) es utilizado para compartir y recibir información de enrutamiento entre distintas redes. Dentro del mundo de las ISP el protocolo BGP intercambia la información de las tablas de enrutamiento de un sistema autónomo a otro, permitiendo encontrar las mejores rutas de origen y destino, y agilizando el tráfico en el internet [39].

Para el intercambio de información se configuran sesiones de BGP tanto internas (iBGP) como externas (eBGP) dentro de las redes de un sistema autónomo.



### **2.5.1.1. iBGP**

Se implementa dentro de un AS y se utilizan para anunciar:

- Todo o algunos de los prefijos de direccionamiento IP mediante el backbone del proveedor.
- Todos los prefijos asignados a los usuarios de una ISP.

### **2.5.1.2. eBGP**

Se implementa fuera de un AS y se utilizan para:

- Intercambiar información entre AS.
- Configurar políticas de enrutamiento.

## CAPÍTULO III

### 3. DISEÑO DE PROTOTIPO

Para el llegar al diseño del prototipo se seguirá el proceso planteado en la metodología del CAPÍTULO I, lo cual se desarrollará continuación.

#### 3.1. Sistema de televisión

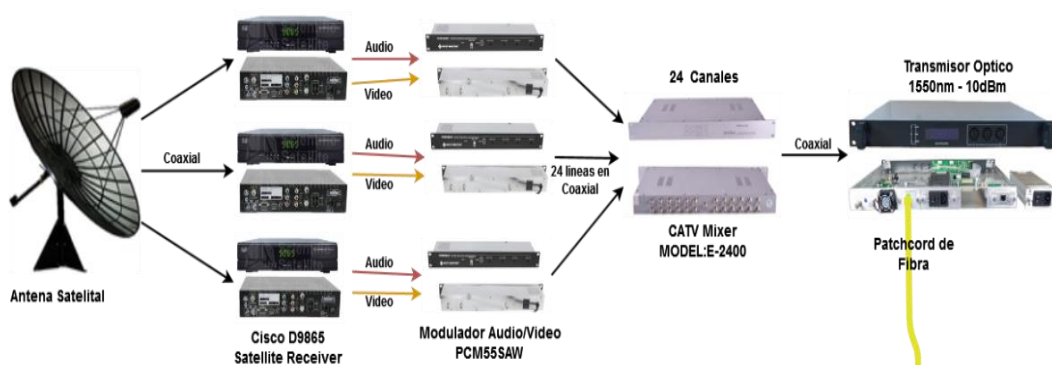


Figura 10. Topología del sistema de transmisión de TV actual de la empresa.

En la Figura 10 se muestra la topología actual del sistema de televisión, el cual comienza con la recepción de canales encapsulados a través de 6 antenas satelitales, cada una se conecta por cable coaxial a un grupo de receptores satelitales, Cisco D9865H, el cual capta las señales de audio, video y datos encriptados.

La empresa posee alrededor de 40 receptores satelitales para procesar cada canal de televisión, estos equipos están conectados directamente por el modulador PCM55SAW a través de cables auxiliares de audio y video. Este dispositivo realiza la modulación analógica por amplitud y frecuencia de las señales de video y audio, respectivamente, lo cual limita la resolución de imagen al usuario.

Por consiguiente, se realiza la combinación de ambas señales analógicas y las convierte en digital a través del CATV Mixer de 24 entradas coaxiales, se obtiene una señal que contiene 24 canales y las convierte en señal óptica por el transmisor óptico.

Dado el sistema actual que posee la empresa se concluyó que a través del puerto HDMI de los 24 receptores satelitales se obtendría las señales digitales de audio y video combinadas, por lo tanto, se necesitaría equipos que admita entradas en HDMI y a su vez realice las funciones de digitalización y modulación de canales.

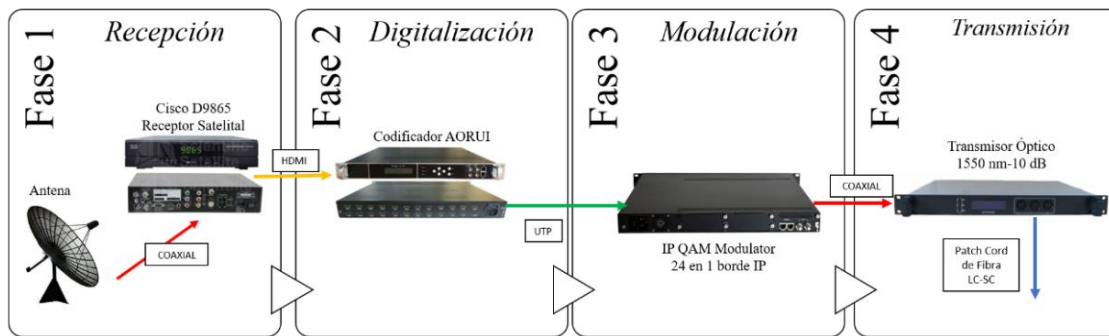


Figura 11. Diseño de prototipo de televisión.

En el diseño propuesto de la Figura 11 se considera las 4 fases que requiere un sistema de televisión, en la fase de Recepción está las antenas satelitales y los receptores Cisco, dichos componentes posee actualmente la empresa.

En la fase de digitalización se reemplazó los 24 moduladores analógicos por un codificador digital que permite las entradas en HDMI y salida IP, después se conecta al modulador IPQAM que realiza la modulación de señales con mayor rapidez y con menor interferencias de ruido, de esta manera se haría ahorro en el consumo de energía para la empresa y en se mejoraría la calidad de servicio.

Dicho modulador que se encuentra en la fase 3 de la Figura 11, es compatible con el transmisor óptico, el cual transforma la señal eléctrica en óptica y de esta manera se obtiene un sistema IPTV que ofrece servicio de televisión a través de fibra óptica.

### 3.1.1. Descripción de cada equipo de la infraestructura actual



Figura 12. Receptor Satelital Cisco D9865 [40]

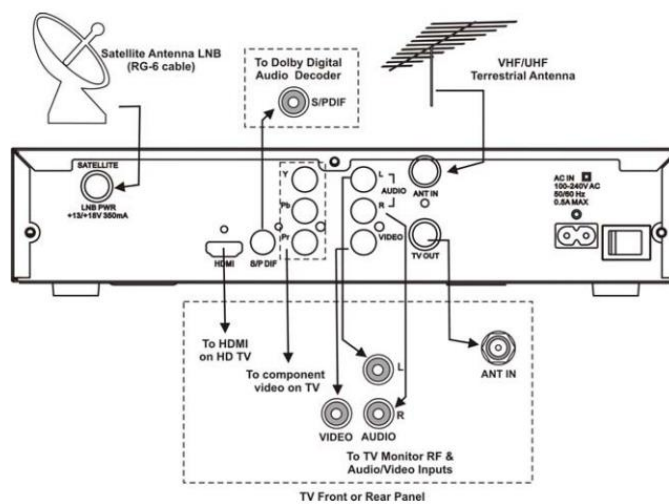


Figura 13. Panel Frontal del Receptor Satelital Cisco D9865 [40]

El receptor satelital contiene entrada para el satélite de tipo LNB PWR y salidas de HDMI, Audio y Video, tal como se muestra en la Figura 13. Está diseñado para la distribución de contenido satelital y se aplica en el entorno de transmisión, televisión comercial, redes privadas y SMATV. Su función es recibir video, audio, VBI y datos encryptados digitalmente. Provee decodificación MPEG-2 y MPEG-4 AVC en estándar y alta definición, tasa de símbolos QPSK tanto para DVB-S y DVB-S2 [40].



Figura 14. Modulador PCM55SAW [41]

El modulador analógico, mostrado en la Figura 14, realiza la modulación de la señal de audio y video, por frecuencia y amplitud, respectivamente. Este dispositivo admite entradas auxiliares y su salida es coaxial, su rango de frecuencia es de 55 a 408 [MHz]. Para cada canal de televisión se utiliza un modulador PCM55SAW, y se combina las señales de audio y video a través del CATV Mixer de 24 canales (Ver Figura 15) [42].



Figura 15. CATV Mixer [43]

El CATV Mixer combina las señales de audio y video, a su vez realiza la codificación de canales, es decir; se le da una característica a cada canal y una frecuencia para que pueda ser sintonizada.

Para ofrecer servicio de televisión por fibra óptica, se convierte las señales electrónicas en óptica a través del transmisor óptico de 10 dB (Ver Figura 16).



Figura 16. Transmisor Óptico [44]

### 3.1.2. Equipos para el sistema CATV/IPTV propuesto

#### 3.1.2.1. Codificador

El codificador de la Figura 17 admite 24 entradas HDMI y dos puertos Gigabit, realiza la codificación de video por formato MPEG-4 AVC/H.64 y la codificación de audio con formato MPEG1 Layer2, su datasheet completo se muestra en Anexo 1 [45].



Figura 17. Codificador AOURI [45]

#### 3.1.2.2. IPQAM

El codificador, mostrado en la Figura 18, tiene como función la modulación de los canales según su estándar, se puede realizar la modulación en diferentes constelaciones: 16QAM, 32QAM, 64QAM, 128QAM y 256QAM; el datasheet del equipo está en Anexo 2. También permite la administración a través del navegador web, dado que así se puede configurar cada canal a su frecuencia de muestreo respectiva, al tipo de modulación y el rango de bits [46].



Figura 18. IPQAM mux scrambler [46]

### 3.1.3. Presupuesto inicial de la empresa

NETSURTV tiene como propuesta el cambio de los 24 moduladores analógicos por digitales, tal como se muestra en la Figura 19. Este equipo admite entrada HDMI y salida coaxial, dado que se podría obtener las señales digitales de audio y video combinadas.



Figura 19. DVB-T MPEG2/4 HDMI con TDT salida RF modulator codificador [47]

El costo de cada modulador es aproximadamente de \$1.200 dólares americanos y sin considerar los aranceles e impuestos, por lo tanto, se requiere una inversión de aproximadamente \$28.800.

### 3.1.4. Presupuesto total para el nuevo sistema



24 en 1 borde IPQAM mux scrambler		2.600 US\$
Codificador AORUI		1.780 US\$
TOTAL	No incluye los aranceles	4.380 US\$

Tabla 1. Presupuesto para el sistema digital

Según el valor de la Tabla 1, el presupuesto no superó los \$28.800 dólares estadounidenses que quería la empresa invertir para obtener canales en alta

definición, es decir, existe un ahorro del 84,79% para la implementación de sistema CATV digital e IPTV.

### **3.1.5. Configuraciones para los nuevos equipos del sistema de televisión**

#### **3.1.5.1. Configuraciones para el codificador**

Por cada canal de televisión, la empresa posee un receptor satelital, por lo tanto, se necesita un decodificador de 24 puertos de entrada HDMI para transmitir los 24 canales en alta definición. Este decodificador tiene como función la decodificación de información y también de combinar los canales para que salga a través del puerto de datos, además los canales presentarán sus configuraciones personalizadas como el bit rate para el video, tipo de video, tipo de audio, bit rate para el audio, el nombre del canal y el volumen en dB.

Tipo de video	Video bitrate [Kbps]	Tipo de audio	Audio bitrate [Kbps]	Volumen (dB)
H.264	6000	AAC	128	10

Tabla 2. Configuraciones para el codificador.

En la Tabla 2 se muestra las configuraciones que debe tener cada canal que se emite en el equipo a través del puerto HDMI, estos valores y estándares van acorde a las normativas que se aplican en el Ecuador y según el Ministerio de Telecomunicaciones.

#### **3.1.5.2. Configuraciones para la IP-QAM**

El IP-QAM es un dispositivo robusto que puede modular hasta 144 canales, se puede combinar 3 redes en la serie cabecera de alta velocidad y basada en IP. Se propone este dispositivo que admite 24 canales en un puerto IP, presenta



configuraciones flexibles y mecanismo de licencia. Permite la modulación en cada tipo de orden QAM, un rango de velocidad de bits de datos de salida 15,5 a 51,6 [Mbps], cada placa admite 24 frecuencias de modulación y ajuste de ganancia de 0 a 20 [dB].

Se sugiere la modulación en orden 32, para que el sistema no presente pérdidas ante altas interferencias o ruido y pueda preservar la calidad de imagen y velocidad de datos.

<b>Constelación</b>	32-QAM
<b>Velocidad de bits mínima [Mbps]</b>	5
<b>Velocidad de bits máxima [Mbps]</b>	35
<b>Ancho de banda mínimo [MHz]</b>	1,15
<b>Ancho de banda máximo [MHz]</b>	8,05
<b>Índice mínimo de símbolos</b>	1
<b>Tasa máxima de símbolos [Mbaud]</b>	7
<b>C/N umbral</b>	25 dB
<b>Canal tasa de utilización</b>	4 bits/Hz

Tabla 3. Configuraciones para el IPQAM [46]

Actualmente, el receptor satelital tiene habilitado los puertos auxiliares de salida de audio y video, pero para brindar un sistema digital y redundante, se propone habilitar la salida HDMI para conectarlos a los equipos que realizan la codificación y modulación de información en digital.

En caso que se presente problemas en el nuevo sistema, se sugiere mantener habilitados las salidas analógicas y conectadas al sistema anterior para que los usuarios mantengan su servicio de televisión a pesar de las fallas.

## 3.2. Red de acceso a internet

### 3.2.1. Análisis de la topología de red de la empresa

En la actualidad NETSURTV tiene una topología de red basada en el modelo jerárquico de núcleo contraído, como se puede observar en la Figura 20. Es por eso que el equipo central Mikrotik CCR1036 maneja la capa del núcleo y la capa de distribución, dado que es un proveedor de internet por fibra óptica como medio de transporte se utiliza una red de acceso FTTH-GPON mediante una OLT Huawei MA5680T, mientras que la capa de acceso está encargada por una ONU Huawei HG8310M. Además, tiene contratado un solo proveedor de servicio con ancho de banda de 1,80GB el cual da acceso a internet a toda la red mediante 2 puertos WAN.

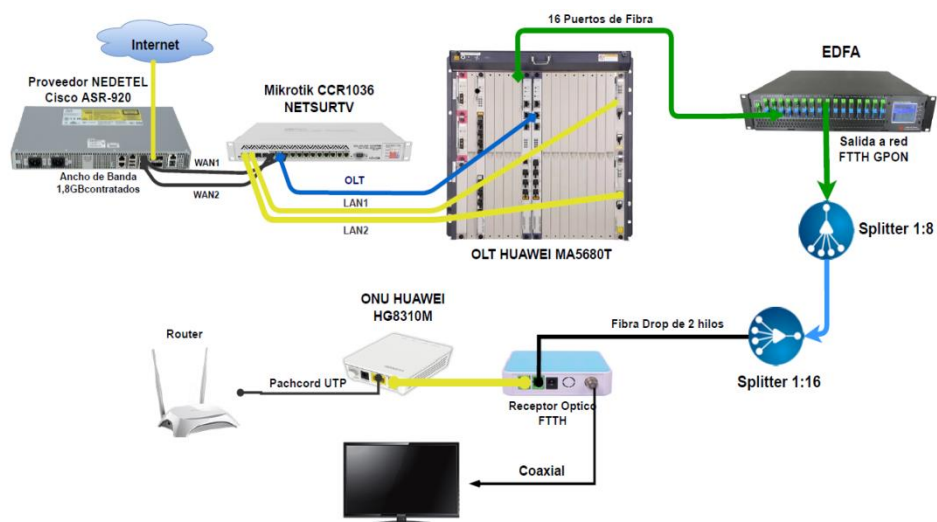


Figura 20. Topología de Red actual de la empresa NETSURTV.

### 3.2.2. Router principal de la empresa

La empresa opera con un router Mikrotik CCR1036 (véase la Figura 21) como equipo central en el cual se maneja tanto la capa de núcleo como de distribución de la red. Es decir, este equipo controla tanto el tráfico de salida como de entrada de la red, es por eso que es importante conocer sus características.

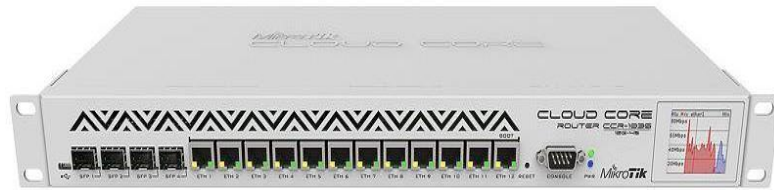


Figura 21. Mikrotik CCR1036-12G-4S [48]

El router Mikrotik CCR1036 es un enrutador con un CPU de 36 núcleos con una frecuencia de operación de 1.2 GHz, tiene 4 puertos SFP, 12 puertos Gigabits Ethernet, un puerto USB y un cable de consola serie. Una memoria RAM de 4GB con capacidad expansible hasta 16 GB de RAM. Opera con sistema operativo RouterOS versión 6.42.10 compatible con enrutamiento dinámico, estático, PPPoE, Firewall, MPLS, VPN, BGP y entre otras más funciones [48].

### 3.2.3. Análisis de configuraciones del equipo central

#### 3.2.3.1. Configuraciones de puertos ethernet

El router tiene configurado los puertos ethernet 1 y ethernet 3 como interfaces WAN denominadas “*BONDING\_NEDETEL\_1*” y “*BONDING\_NEDETEL\_2*”, tienen esta denominación debido a que estos enlaces provienen del mismo proveedor “NEDETEL” y fueron agregados aun Bonding para aprovechar el máximo ancho de banda contratado.

Por otro lado, los puertos sfp 1 y sfp 2 están configurados como interfaces LAN, las cuales le dan acceso a internet a cada cliente y también han sido agregadas a un Bonding, ya que cada puerto sfp tiene una capacidad máxima de 1GB y como el ancho de banda contratado es de 1,8GB se utilizaron 2 puertos sfp para cubrir todo el ancho de banda disponible.

Además, se utiliza el puerto ethernet 2 para conectarse a la OLT y poder acceder a este equipo a través del Mikrotik y además se utiliza el puerto ethernet

11 como enlace de administración para poder acceder a las configuraciones del equipo Mikrotik. Todos estos detalles se pueden observar en la Figura 22.

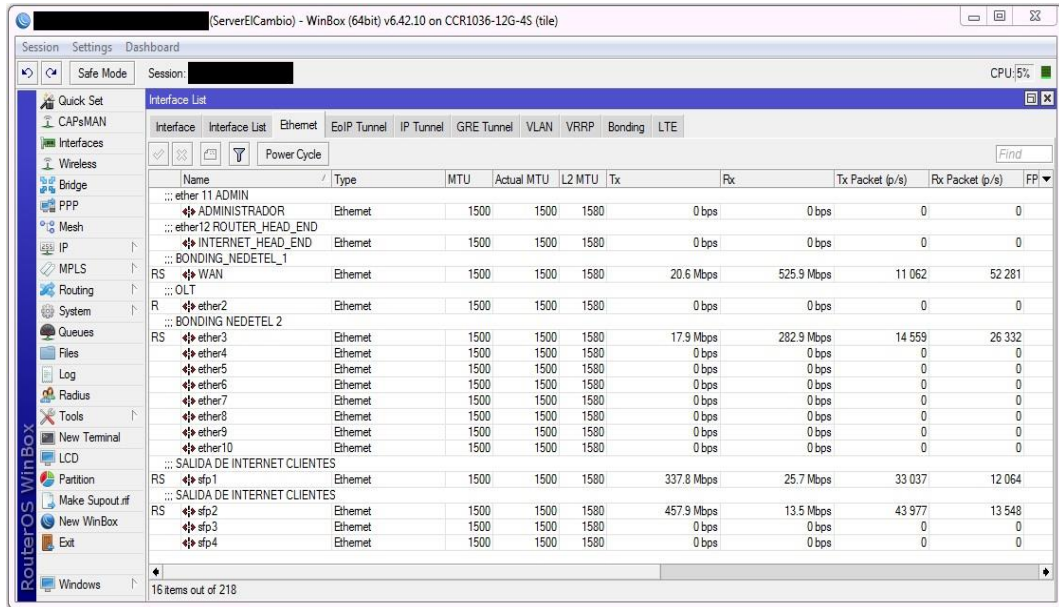


Figura 22. Configuraciones de puertos ethernet en el MikroTik de la empresa NETSURTV.

### 3.2.3.2. Configuraciones de enrutamiento

La empresa Netsurtv para dar acceso a internet a sus clientes emplea el enrutamiento estático y el protocolo PPPoE, para lo cual ha realizado una segmentación de su red por medio de VLANs creando la VLAN 500 denominada “INTERNET CLIENTES” para dar direccionamiento IP estáticas y la VLAN 100 denominada “CLIENTES PPPoE” para clientes PPPoE. El direccionamiento IP se encuentra detallado en la Figura 23 y se los resumirá en la Tabla 4, en la cual no se incluirá las direcciones IP de las interfaces WAN por seguridad de la empresa.

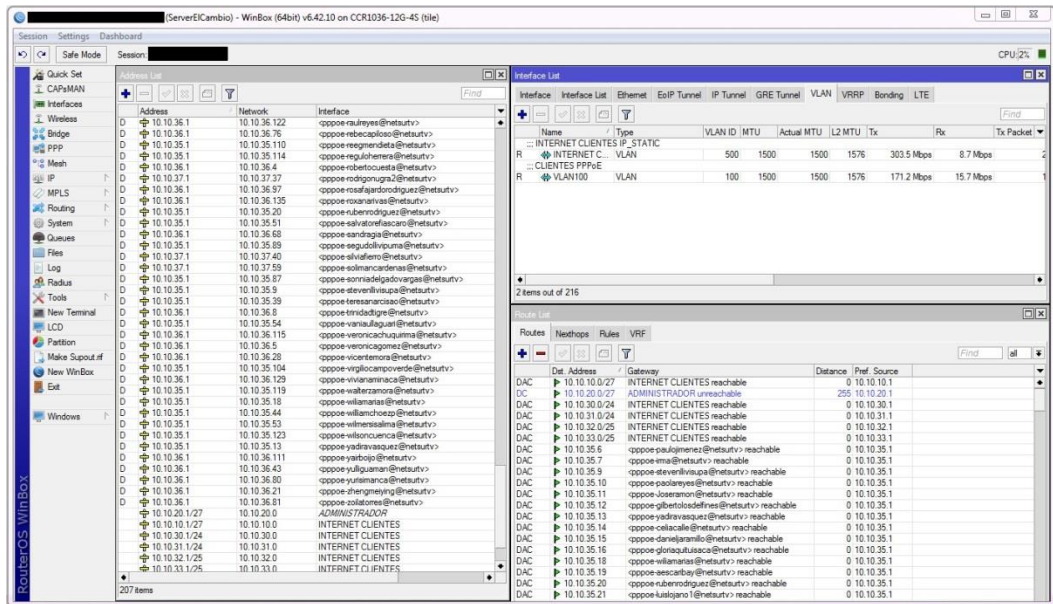


Figura 23. Configuraciones de enrutamiento en el MikroTik de la empresa NETSURTV.

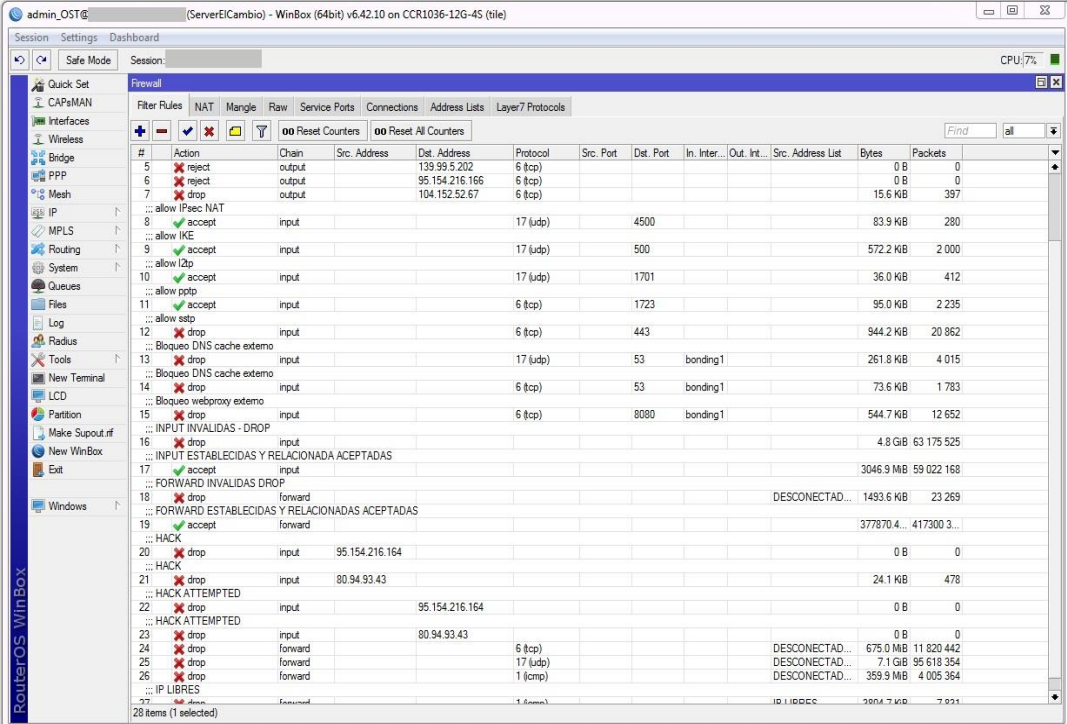
Interfaces	Address	Gateway	VLAN/ Denominación
Ethernet 5 "ADMINISTRACIÓN"	10.10.20.0/27	10.10.20.1	
SFP 1 "Salida de Internet Clientes"	10.10.10.0/27	10.10.10.1	VLAN 500 "INTERNET CLIENTES"
	10.10.30.0/24	10.10.30.1	
	10.10.31.0/24	10.10.31.1	
	10.10.32.0/25	10.10.32.1	
SFP 2 "Salida de Internet Clientes"	10.10.33.0/25	10.10.33.1	VLAN 100 "CLIENTES PPPoE"
	10.10.35.0/25	10.10.35.1	
	10.10.36.0/25	10.10.36.1	
	10.10.37.0/25	10.10.37.1	

Tabla 4. Direccionamiento IP de las Interfaces LAN.

La Tabla 4 muestra el direccionamiento IP de las interfaces LAN utilizado por la empresa lo cual indica que no se está utilizando métodos adecuados de direccionamiento IP, ya que los prefijos usados en la actualidad son arbitrario y además con las direcciones actuales pueden tener 794 direcciones para clientes de IP estática y 380 para clientes PPPoE lo cual da un total de 1178 direcciones IP, pero en la actualidad la empresa tiene alrededor de 600 clientes por ende se estaría desaprovechando las IP creadas.

### 3.2.3.3. Configuraciones del firewall

El Firewall es una de las configuraciones más importantes en el equipo principal ya que se encarga de la seguridad de la red, aquí se encuentran las configuraciones como el bloqueo de ataques a la red, restricción de accesos no autorizados al equipo, controlar el flujo de salida y entrada de datos, denegación de servicios a usuarios, entre otras.



The screenshot shows the Mikrotik WinBox interface for configuring Firewall Filter Rules. The window title is 'admin\_OST@ (ServerElCambio) - WinBox (64bit) v6.42.10 on CCR1036-12G-4S (title)'. The left sidebar shows the 'RouterOS WinBox' menu with options like Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, LCD, Partition, Make Supout.rf, New WinBox, and Exit. The main window displays the 'Firewall' configuration page with tabs for Filter Rules, NAT, Mangle, Raw, Service Ports, Connections, Address Lists, and Layer7 Protocols. The 'Filter Rules' tab is active, showing a table of 28 rules. The table has columns for #, Action, Chain, Src. Address, Dest. Address, Protocol, Src. Port, Dest. Port, In. Inter..., Out. Int..., Src. Address List, Bytes, and Packets. The rules are numbered 5 through 28. Rules 5, 6, 7, 12, 13, 14, 15, 18, 20, 21, 22, 23, 24, 25, and 26 are marked with a red 'X' icon, indicating they are disabled. Rules 8, 9, 10, 11, 16, 17, 19, 27, and 28 are marked with a green checkmark icon, indicating they are enabled. The table shows various actions such as 'reject', 'drop', 'accept', 'forward', and 'input'. Some rules have specific source and destination addresses and protocols. For example, rule 24 is a 'drop' action on the 'input' chain for protocol 'tcp' on destination port 80. Rule 25 is a 'drop' action on the 'forward' chain for protocol 'udp' on destination port 17. Rule 26 is a 'drop' action on the 'forward' chain for protocol 'icmp' on destination port 1. Rule 28 is a 'drop' action on the 'input' chain for protocol 'libres' on destination port 10.1.1.1.

#	Action	Chain	Src. Address	Dest. Address	Protocol	Src. Port	Dest. Port	In. Inter...	Out. Int...	Src. Address List	Bytes	Packets
5	reject	output		139.59.5.202	6 (tcp)						0 B	0
6	reject	output		95.154.216.166	6 (tcp)						0 B	0
7	drop	output		104.152.52.67	6 (tcp)						15.6 KB	397
8	accept	input			17 (udp)	4500					83.9 KB	280
9	accept	input			17 (udp)	500					572.2 KB	2 000
10	accept	input			17 (udp)	1701					36.0 KB	412
11	accept	input			6 (tcp)	1723					95.0 KB	2 235
12	drop	input			6 (tcp)	443					944.2 KB	20 862
13	drop	input			17 (udp)	53	bonding1				261.8 KB	4 015
14	drop	input			6 (tcp)	53	bonding1				73.6 KB	1 783
15	drop	input			6 (tcp)	8080	bonding1				544.7 KB	12 652
16	INPUT INVALIDAS - DROP	input									4.8 GB	63 175 525
17	FORWARD ESTABLECIDAS Y RELACIONADA ACEPTADAS	forward									3046.9 MB	59 022 168
18	FORWARD ESTABLECIDAS Y RELACIONADAS ACEPTADAS	forward								DESCONECTAD...	1493.6 KB	23 269
19	FORWARD ESTABLECIDAS Y RELACIONADAS ACEPTADAS	forward									377870.4...	417300.3...
20	drop	input	95.154.216.164								0 B	0
21	HACK	input	80.94.93.43								24.1 KB	478
22	HACK ATTEMPTED	input		95.154.216.164							0 B	0
23	HACK ATTEMPTED	input		80.94.93.43							0 B	0
24	drop	forward			6 (tcp)					DESCONECTAD...	675.0 MB	11 820 442
25	drop	forward			17 (udp)					DESCONECTAD...	7.1 GB	95 618 354
26	drop	forward			1 (icmp)					DESCONECTAD...	359.9 MB	4 005 364
27	IP LIBRES	input									2604.7 KB	7 821
28	IP LIBRES	input									2604.7 KB	7 821

Figura 24. Reglas de filtros en el firewall del Mikrotik de la empresa NETSURTV.

En la Figura 24 se presenta las configuraciones actuales que están implementadas en el Firewall del equipo principal. Dentro de las reglas implementadas se puede notar configuraciones para la denegación de ataques externos por medio de la acción de “reject” y “drop” (estas acciones realizan el descarte y bloque de paquetes provenientes de otras redes); además se ha implementado configuraciones para el bloqueo de servicios en las reglas 24, 25 y 26 por medio de la acción “drop”, lo cual bloquea todos los paquetes tcp, udp

e icmp provocando que no se permite la navegación a los usuarios que pertenezcan a la address list “DESCONECTADO”; y también existen configuraciones que permiten la aceptación de paquetes tanto externos como internos, este tipo de configuraciones se las observa en las reglas 8, 9, 10, 11, 17 y 18.

Haciendo un análisis de las reglas implementadas en el equipo central, se pudo notar que existe una prioridad arbitraria, ya que podemos encontrar reglas de bloqueo de ataques que tiene una mayor prioridad (como lo son las reglas 5, 6 y 7) y otras con menor prioridad (como lo son las reglas 20, 21, 22 y 24); lo mismo ocurre con otras configuraciones implementadas. Esto nos dice, que estas reglas fueron implementadas con forme el equipo las fue necesitando; es decir no siguen ningún orden jerárquico o prioridad lo cual no es recomendable, ya que siempre es necesario tener un orden prioritario al configurar las reglas de filtrado porque de esto dependerá la rapidez en la que reacciona nuestro equipo.

#### **3.2.3.4. Configuraciones del queues**

El Queues permite crear colas para el control del ancho de banda de subida y bajada que se asigne a cada cliente, para el caso de la empresa NETSURTV, como se observa en la Figura 25, el árbol de colas implementado no está siendo usado ya que en la actualidad la empresa realiza el control del ancho de banda mediante la ONU Huawei HG8310M que se instala en la residencia de cada cliente.

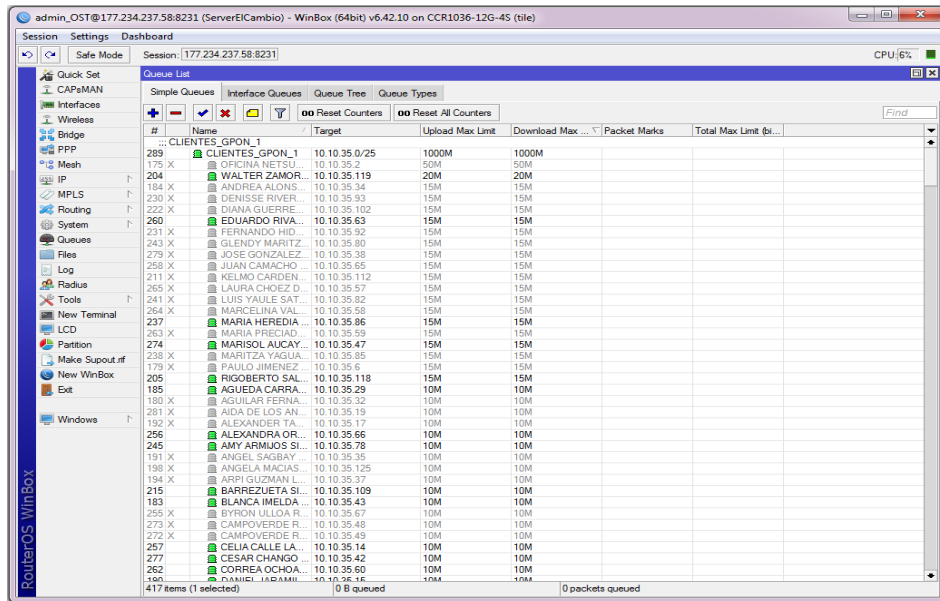


Figura 25. Árbol de colas implementadas en el Simple Queues en del Mikrotik de la empresa NETSURT.V.

El control de ancho de banda que realiza la empresa no está implementado adecuadamente, ya que al equipo central llega todo el flujo de salida y entrada de datos por ende es el más adecuado para llevar este control, además que tiene las capacidades necesarias para hacerlo adecuadamente.

### 3.2.4. Análisis del tráfico de la red

La realización de este análisis se basó en un monitoreo por etapas, primero se monitoreo el tráfico de la red para determinar las horas donde existe mayor consumo del ancho de banda, este monitoreo se muestra en la Figura 24.

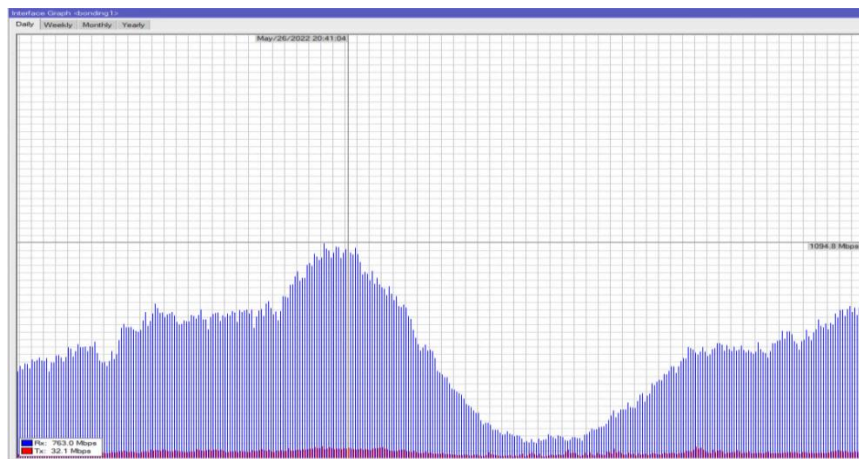


Figura 26. Monitoreo de consumo de ancho de banda el día 26/05/2022.



Como resultado de este monitoreo se pudo determinar que el mayor consumo de ancho de banda ocurre en el horario de 20H00 a 21H00 con un pico máximo de 1094.8 Mbps. Con este resultado se procedió a realizar un monitoreo semanal para determinar el pico máximo de consumo en la red, el cual se puede observar en la Figura 26.

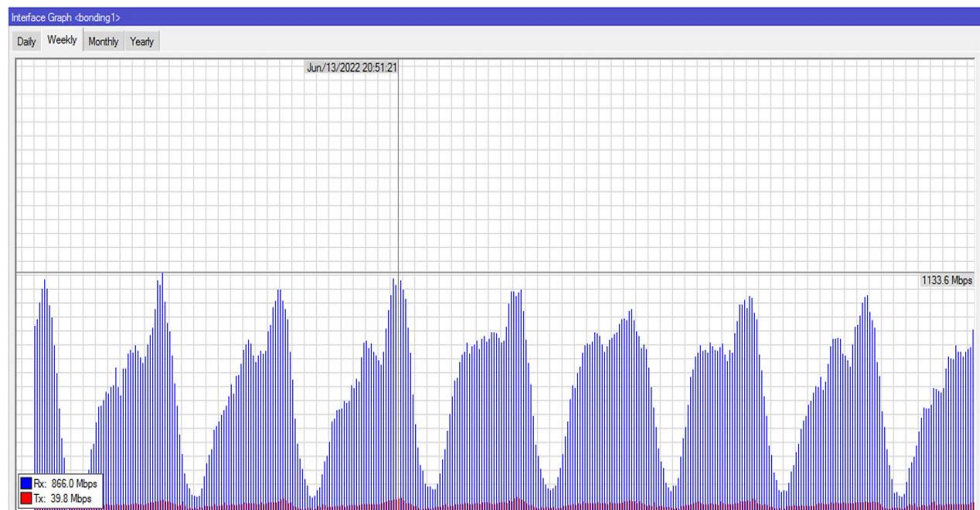


Figura 27. Monitoreo de consumo de ancho de banda semanal.

Se monitoreo el tráfico de la red en la semana del 10 de junio al 17 de junio de 2022, obteniendo como resultado un pico máximo de 1133.6 Mbps y en promedio 1055.7 Mbps. Tal como se muestra en la Figura 27, los horarios de máximo consumo siguen estando alrededor de las 20H00 a 21H00 y además los días de mayor consumo fueron los días sábado y lunes.

Finalmente se realizó un monitoreo mensual del tráfico de la red durante el 05 de Julio al 10 de agosto de 2022 obteniendo como resultado las gráficas mostradas en la Figura 28.

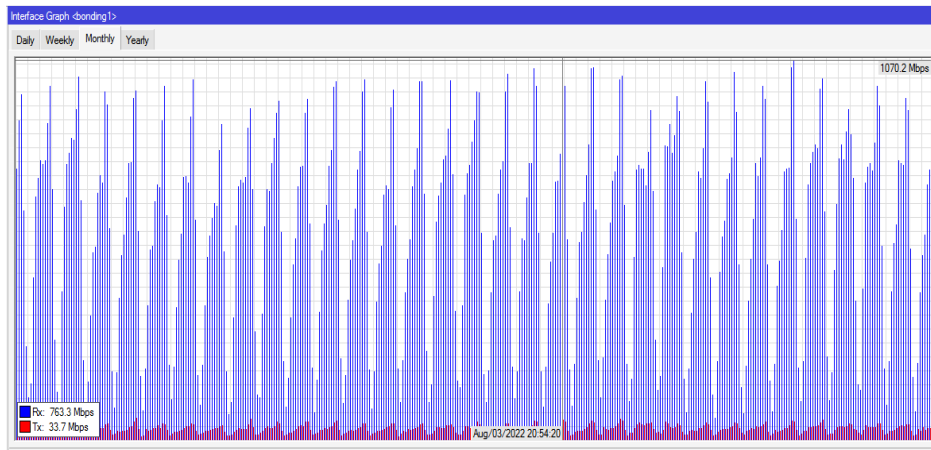


Figura 28. Monitoreo de consumo de ancho de banda mensual.

Los datos que se obtenidos fueron un pico promedio de 1064.1 Mbps, la franja horaria de mayor consumo está alrededor de las 20H30 a 22H30, además los días de mayor consumo fueron variados dentro de una semana existía mayor consumo los días sábados por ejemplo el día 16 de Julio se registra un pico de 1034.6 Mbps mientras que en otras semanas los días fueron lunes y martes como el día 03 de Agosto que registro un pico de 1070.2 Mbps, lo que nos indica que existes un mayor consumo dentro de los días cercanos al fin de semana e inicios de semana.

Como resultado de este análisis tenemos que el mayor consumo de la red se registra en los horarios de 20H30 a 21H30 con picos máximos de 1064.1 Mbps en promedio. Es decir que estos horarios son los de mayor riesgo y en los cuales se debe tener mayor prioridad en el manejo del tráfico de la red para que así los clientes no presentes problemas de conectividad.

### 3.2.5. Análisis de consumo del CPU

Para este análisis se obtuvieron las gráficas de consumo del CPU durante un mes para saber los porcentajes picos del equipo central, lo cual se pude observar en la Figura 29.

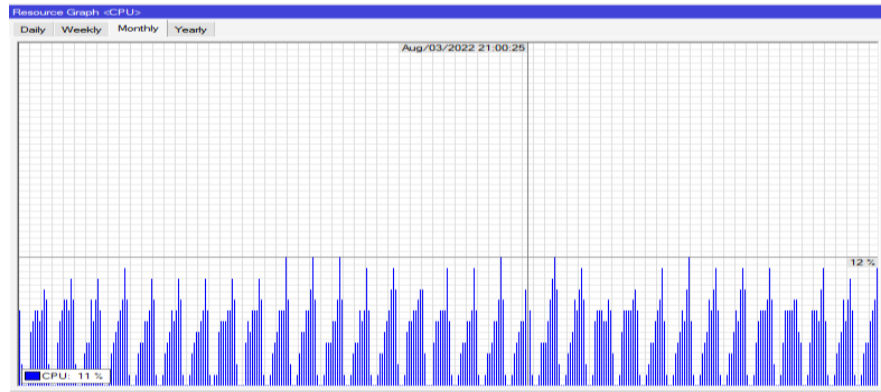


Figura 29. Monitoreo de consumo de CPU.

Como resultado tenemos que el mayor consumo del CPU es del 12% alrededor de las 21H00, este resultado tiene relación con el horario donde ocurre el mayor tráfico de la red. A pesar que el consumo máximo no es un valor de preocupación que puede afectar al correcto funcionamiento del equipo central, si nos reafirma que el horario de mayor riesgo que presenta la red es alrededor de las 21H00.

### 3.2.6. Propuesta de solución

Con el análisis realizado se pudo conocer los factores de mayor riesgo y las problemáticas que presenta la red de la empresa NETSURTV, con lo cual se presenta la siguiente propuesta de solución.

#### 3.2.6.1. Topología de red propuesta

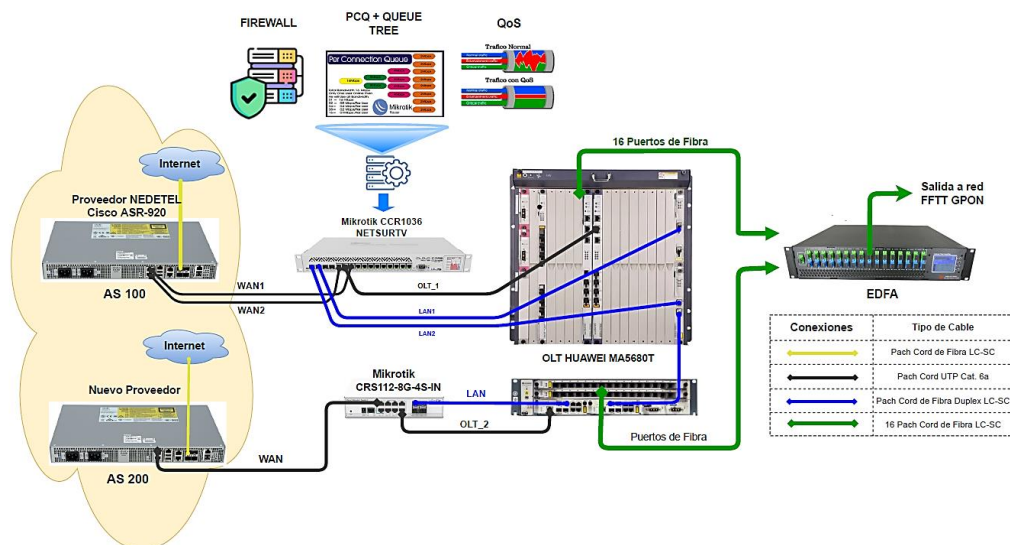


Figura 30. Topología de red propuesta.

La figura 30 muestra el diseño de la topología de red propuesto a implementarse en la empresa NETSURTV; en la cual se puede observar que se han agregados equipos nuevos que permitirá tener una red con mayor escalabilidad y seguridad a fallos.

Además, el requerimiento de contratar otro proveedor de servicios, ya que así, si un proveedor falla el otro servirá de respaldo y también como agregado la adquisición de un sistema autónomo que les permita tener independencia absoluta en las políticas de direccionamiento IP que se utilice en la empresa.

### **3.2.6.2. Configuraciones propuestas al equipo central**

#### **3.2.6.2.1. Mejoras de seguridad del firewall**

Dentro del Firewall del equipo central se encontraron varias inconsistencias en cuanto a las reglas implementadas para la protección de la red, por lo cual se propone realizar una reorganización de las reglas de filtros implementadas y agregar nuevas reglas para prevención de ataques externos como es la denegación distribuida de servicios (DDoS), detección de intrusos, creación de listas negras, etc. Estas implementaciones se las realizaran en el CAPITULO IV, además se detallaran como se realizó cada configuración.

#### **3.2.6.2.2. Control de ancho de banda por PCQ + Queues tree**

Se determinó que el control de ancho de banda configurado en el equipo central no era el adecuado y estaba en desuso, además que este control se lo hacía mediante otro equipo. Por lo cual se propone realizar la configuración del controla de ancho de banda mediante la creación de Colas PCQ usando el árbol Queues Tree, ya que este método se lo realiza mediante

el marcado de paquetes aplicado al Firewall lo cual permitirá tener un mayor control del ancho de banda que la empresa asigne a cada cliente.

#### **3.2.6.2.3. Calidad de servicio o QoS**

Configurar la calidad de servicio en el equipo central le permitirá tener la capacidad de controlar y priorizar el tráfico de la red mediante el marcado de paquetes que ingresan y salen en el enrutador. Para esto se utilizara el Mangle en donde se realizara las distintas marcas de paquetes y mediante el uso del Queues Tree se limite el ancho de banda; todas estas configuraciones se podrán apreciar en detalle en el CAPITULO IV.

#### **3.2.6.2.4. Sistema Autónomo y BGP**

Para la creación del sistema autónomo se deberá adquirir un rango de direcciones IP las cuales se compartirán mediante el protocolo de puerta de enlace de frontera o BGP, es decir que esta configuración de deberá implementar en el equipo central para el intercambio de información con el resto de sistemas autónomos. Para realizar esta configuración primero es necesario crear una instancia BGP utilizando el ASN que se adquiere al momento de comprar el rango de direcciones IP a un proveedor, luego se creara un Peer BGP con la información del AS de nuestro proveedor de servicios de internet y finalmente se crearán los prefijos de direcciones IP que desean anunciar al exterior; todas estas configuraciones se podrán apreciar en detalle en el CAPITULO IV.

## CAPITULO IV

### 4. ANÁLISIS DE RESULTADOS

En este capítulo se presentará dos resultados para el proyecto, siendo el primero un cuadro comparativo de las características de un sistema de televisión analógico y digital, es decir; se reflejará las ventajas que tendrá la empresa al cambiar su estructura a televisión por cable con línea digital.

Por otra parte, se presentará los resultados de las simulaciones realizadas en el software GNS3, en donde se estableció el diseño propuesto para la red de internet y las configuraciones necesarias en los equipos de administración de red.

#### 4.1. Sistema de televisión

Sistema Actual de Televisión	Sistema de Televisión Propuesto
En el sistema actual, el modulador PCM55SAW realiza la modulación de audio y video por frecuencia y amplitud, por lo tanto, no se recupera la señal al 100%.	La televisión digital realiza la modulación digital de amplitud en cuadratura, el cual contiene la información digital en la amplitud y en la fase de la señal portadora que se transmite.
Ofrece calidad de audio y video limitada, una resolución menor igual a 720x480 pixeles.	En sistemas digitales solo existe 0 y 1, es decir; apagado o encendido, lo cual no permite que la calidad de la señal varíe. Su resolución de imagen llega hasta 1920x720 pixeles.
Realizando solo el cambio de los moduladores analógicos a digital, por canal, se requiere una inversión de aproximadamente \$28.800, limitando a su vez la opción de añadir más canales al sistema de televisión.	Acoplado el sistema digital a la estructura actual de la empresa se requiere una inversión de \$4.380 aproximadamente, sin incluir impuestos y aranceles, esto permitirá que se recupere la inversión en menor tiempo y así poder amplificar sus servicios con menor costo.

Tabla 5. Comparación entre el sistema actual y el diseño digital propuesto.

Para que el cliente pueda diferenciar las características que posee la infraestructura actual de televisión y el diseño propuesto, se plasma un cuadro comparativo en la Tabla 5, reflejando el tipo de modulación que se aplica en cada sistema, costos y la resolución de imagen que brinda.

#### 4.2. Red de acceso a internet

Para la aplicación de las soluciones propuestas se ha implementado una simulación mediante el programa GNS3, la cual podemos observar en la Figura 31. En la simulación se replicará la topología de red propuesta y se aplicarán todas las configuraciones plateadas en la propuesta de solución, con la finalidad de comprobar la funcionalidad de las mismas.

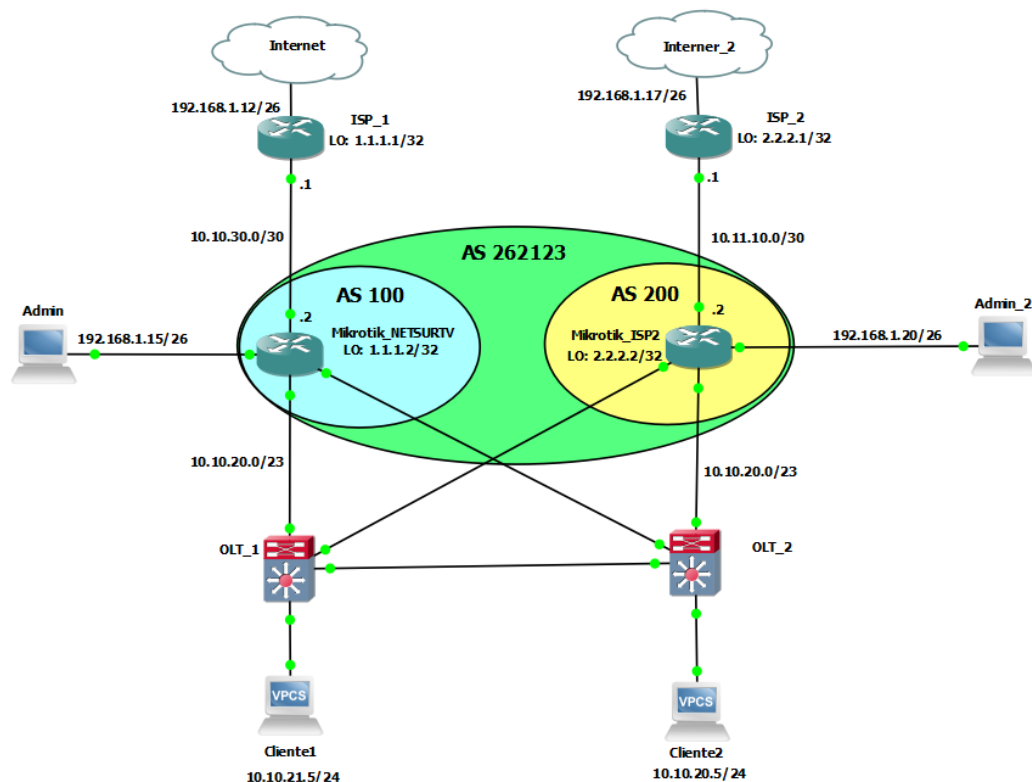


Figura 31. Simulación de la Topología de Red propuesta en GNS3.

#### **4.2.1. Escalabilidad y redundancia**

El diseño propuesto, mostrada en la Figura 31, se basó en un modelo jerárquico de 3 capas, donde la capa del núcleo está representada por los routers Mikrotik\_NETSURTV y Mikrotik\_ISP2, cada dispositivo está conectado a una OLT (OLT\_1 y OLT\_2) y a su vez estos últimos presenta redundancia entre sí para dar mayor seguridad al usuario en caso que exista desconexiones o fallas en los equipos principales.

Para mejorar la escalabilidad de la red se propone la adquisición de un sistema autónomo, dado que así la empresa podrá tener sus propios recursos de direccionamiento IP pública e independencia absoluta en las políticas de enrutamiento que desea implementar.

#### **4.2.2. Sistema autónomo**

Para realizar esta implementación fue necesaria la simulación de los sistemas autónomos de cada proveedor de servicio de internet denominados “ISP\_1” e “ISP\_2” (Ver Anexo 3), además se asume que se cuenta con un ASN 262123 con el dominio de segmentos de IPv4: 10.10.20.0/23 tal como se puede apreciar en la topología de red de la Figura 31.

##### **4.2.2.1. Implementación del protocolo eBGP**

Un sistema autónomo comparte la información de sus redes mediante el protocolo BGP y como el acceso a internet proviene de un proveedor con sus propias políticas de enrutamiento, es decir otro sistema autónomo es necesario levantar una sesión eBGP. Para lo cual primero debemos crear la instancia BGP que se nos asigne, para este caso se utilizara un ASN 262123 y con la ID 1.1.1.2



que es una interface virtual “loopback” creada mediante un bridge; dicha implementación la podemos observar en la Figura 32.

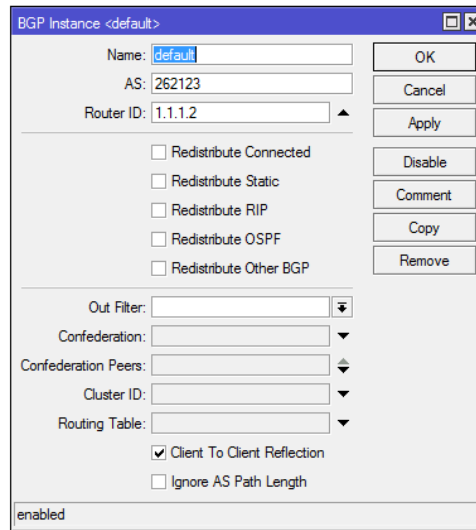


Figura 32. Instancia BGP implementada.

Después se procede a levantar la sesión eBGP mediante la creación del Peer BGP, en el cual se utilizarán la información del AS de nuestro proveedor de servicios, como se aprecia en la Figura 33.

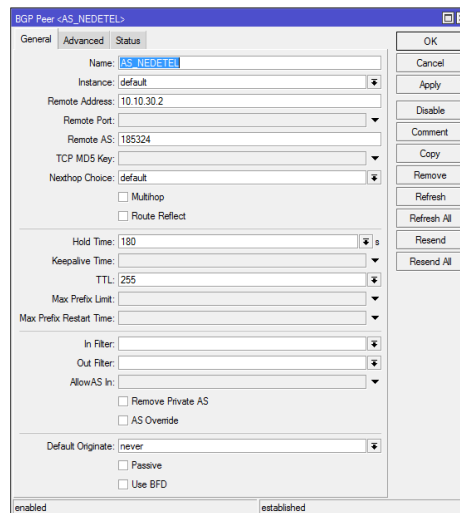


Figura 33. Creación del Peer BGP.

Dentro del Peer BGP se introducirá un nombre de identificación de la sesión que se va a establecer, además la dirección remota será la dirección IP por donde el proveedor entrega el servicio de internet, es decir la dirección WAN y por

último se coloca el ASN del proveedor de servicios para este caso se utilizó el AS Remoto 185324 (AS creado en el router ISP\_1).

Cuando la sesión esta levantada en la ventana de Peers aparecerá el estado “establecido”, tal como se puede observar en la Figura 34, lo cual indica que se está intercambiando información con el AS de nuestro proveedor.

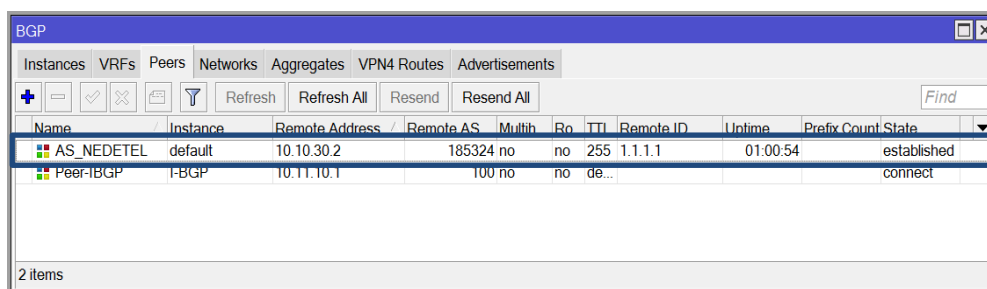


Figura 34. Sesión eBGP establecida dentro del Peers.

Finalmente, se crearán los prefijos de direcciones IP que desean anunciarse, esto dependerá de las políticas de enrutamiento que implemente la empresa; para el caso de la simulación se compartirán las direcciones IP con prefijo 24, es decir 10.10.20.0/24 y 10.10.21.0/24. Esta configuración la podemos observar en la Figura 35.

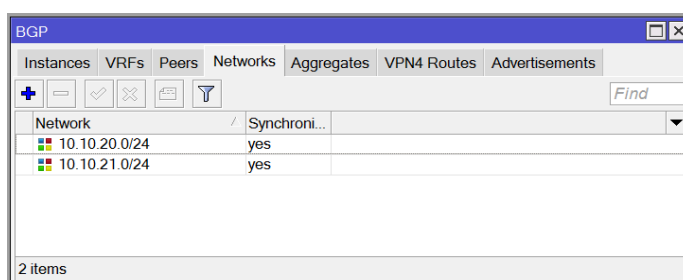


Figura 35. Segmentos de Direcciones IP compartidas con AS del proveedor.

Una prueba de que se están compartiendo las direcciones IP correctas es ver la tabla de rutas, en la cual aparecerán los prefijos de las direcciones publicadas, como se puede apreciar en la Figura 36.

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source	BGP AS Path	BGP Origin
AS	0.0.0.0/0	192.168.1.1 reachable ether7	1				
DAC	1.1.1.1	Loopback reachable	0		1.1.1.1		
DAb	10.10.21.0/24	10.10.30.1 reachable ether2	20			262123	igp
DAC	10.10.30.0/30	ether2 reachable	0		10.10.30.2		
DAC	192.168.1.0/25	ether7 reachable	0		192.168.1.12		

Figura 36. Tabla de rutas.

Estas mismas implementaciones deberán realizar en el router “Mikrotik\_IPS2” de la Figura 31, pero con la información del AS del otro proveedor que se contrate.

### 4.2.3. Seguridad

La seguridad del equipo central siempre deberá ser una de las principales prioridades de una empresa, es por eso que para las reglas de filtro implementadas dentro del Firewall se dará la mayor prioridad a las reglas de bloqueo y denegación de ataques. Seguidamente continuarán las reglas de cortes de servicio y finalmente las reglas que permitirán dar acceso o negar servicios de red.

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. interface	Out. Int.	Src. Address List
0	Denegar conexiones invalidad	input								
1	Bloques de Ataque	input								
2	reject	input		104.152.52.67	6 (tcp)					
3	drop	input		80.94.93.43	6 (tcp)					
4	drop	input		95.154.216.164	6 (tcp)					
5	Bloque DNS cache externo	input								
6	drop	input			6 (tcp)					
7	drop	input			17 (udp)		53		bonding1	
8	Escaneo de Puertos	input			6 (tcp)					
9	Suprecion de Ataques DoS	input			6 (tcp)					
10	Denegacion DoS	input			6 (tcp)					Lista_negra_DoS
11	add src to address list	input			6 (tcp)					
12	Corte de Servicio	forward			6 (tcp)		190.443			Deudores
13	drop	forward			17 (udp)		190.443			Deudores
14	drop	forward			1 (icmp)					Deudores
15	Permisio al Router	input	10.10.30.0/25						bonding1	
16	Permitir conexiones estabilidad y relacionadas	input								
17	accept	input								
18	Permitir Ping	input			1 (icmp)					
19	accept	input								
20	Denegar todo lo demas	input								
21	drop	input								

Figura 37. Reglas de Filtro implementadas en el Firewall de la red simulada.

En la Figura 37 se observa cómo se reorganizaron las reglas implementadas dentro de la simulación plateada, además se añadieron nuevas reglas que se explicaran a continuación.

#### 4.2.3.1. Bloqueo de denegación distribuida de servicio (DDoS)

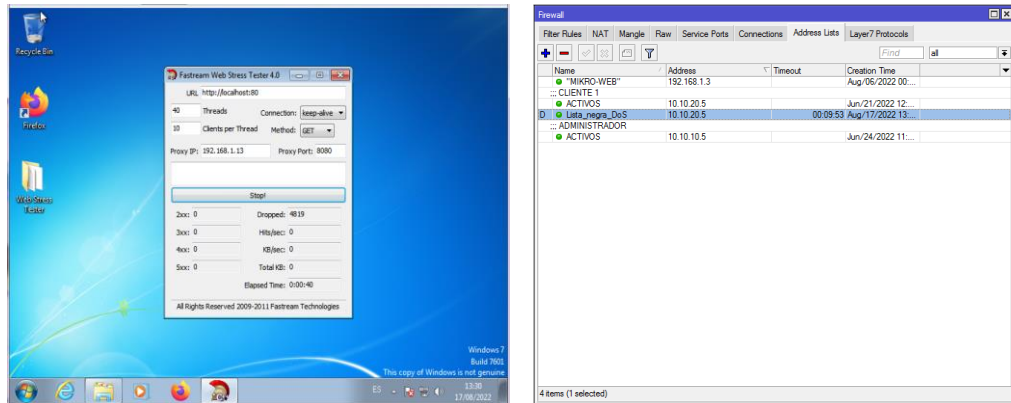
Uno de los ataques más comunes que reciben los ISP son la denegación de servicios o comúnmente conocida ataques DDoS, este tipo de ataque se centra en causar estragos en las redes por medio del envío de grandes paquetes de datos provocando la saturación del tráfico de la red y haciendo que el equipo principal consuma más recursos de CPU. Es por eso que para evitar este tipo de ataques se han implementado reglas dentro del equipo central que se pueden visualizar en las reglas 7 y 8 de la Figura 38.

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. Int..	Src. Address List	
3	drop	input		95.154.216.164	6 (tcp)						
... Bloque DNS cache externo											
4	drop	input			6 (tcp)		53	bonding1			
5	drop	input			17 (udp)		53	bonding1			
... Escaneo de Puertos											
6	drop	input			6 (tcp)						
... Supresion de Ataques DoS											
7	tarpit	input			6 (tcp)					Lista_negra_DoS	
... Denegacion DoS											
8	add src to address list	input			6 (tcp)						
... Corte de Servicio											
9	drop	forward			6 (tcp)		!80,443			Deudores	
10	drop	forward			17 (udp)		!80,443			Deudores	
11	drop	forward			!1 (icmp)					Deudores	
... Permiso al Router											
12	accept	input	10.10.30.0/25					!bonding1			
... Permitir conexiones estabilidad y relacionadas											
13	accept	input									
... Permitir Ping											
14	accept	input			1 (icmp)						
... Denegar todo lo demas											

Figura 38. Reglas implementadas para evitar ataques DDoS.

El proceso de implementación de estas reglas se encuentra detallado en Anexo 5. Estas reglas funcionan a partir de la detección de paquetes de datos tcp, por medio de las funciones *Connection Limit* y *PSD*, con lo cual se detectar la IP que está

realizando el ataque y se la agrega a una lista negra por un determinado tiempo. Finalmente, el ataque es suprimido usando la acción *tarpit*, la cual no descarta los paquetes de datos, sino los captura y retiene permitiendo ralentizar el ataque que se esté efectuando.



(a) (b)  
 Figura 39. a) Inicio de ataque DDoS. b) Supresión de ataques DDoS.

El la Figura 39.a se puede observar cómo se realiza un ataque DDoS desde el computador de prueba y en la Figura 39.b se observa cómo se añade la dirección IP atacante a una lista negra dentro de address list, para que posteriormente el ataque sea suprimido.

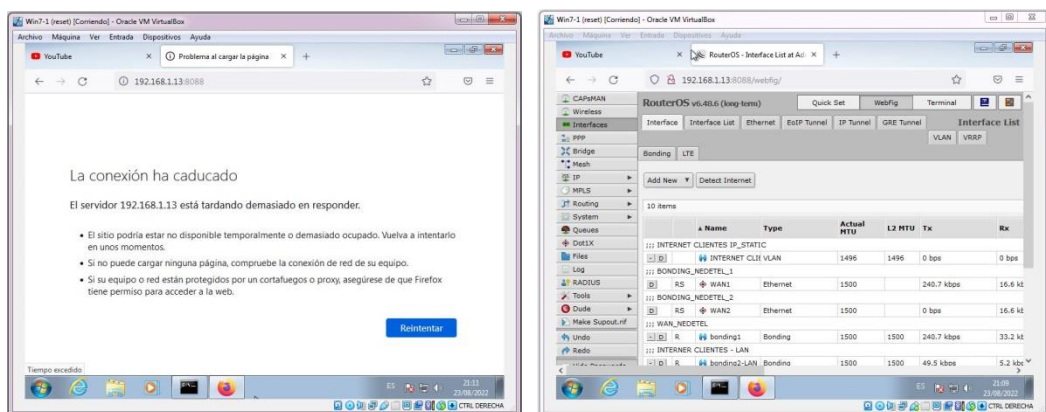
#### 4.2.3.2. Permisos de acceso al equipo central

Otra de las configuraciones planteadas para mejorar la seguridad del equipo principal es la creación de permisos de acceso para segmentos de direcciones IP conocidos (Ver Figura 40).

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. Int.	Src. Address List
3	drop	input		95.154.216.164	6 (tcp)					
4	drop	input			6 (tcp)		53	bonding1		
5	drop	input			17 (udp)		53	bonding1		
6	drop	input			6 (tcp)					
7	target	input			6 (tcp)					Lista_negra_DoS
8	add src to address list	input			6 (tcp)					
9	drop	forward			6 (tcp)		!80,443			Deudores
10	drop	forward			17 (udp)		!80,443			Deudores
11	drop	forward			11 (icmp)					Deudores
12	accept	input	10.10.30.0/25					!bonding1		
13	accept	input								
14	accept	input			1 (icmp)					

Figura 40. Regla implementada para dar acceso al equipo principal.

Esta configuración se la crea a partir de la acción *accept*, con la cual se acepta todos los paquetes de datos que ingresan al router únicamente por el puerto Ethernet *bonding1* y desde el segmento de direcciones IP 10.10.30.0/25. Para mayores detalles de configuración ver Anexo 6.



(a)

(b)

Figura 41. a) Negación de acceso al router. b) Permiso de acceso al router.

En la Figura 41.a se puede observar cómo no se permite el acceso al router principal, mientras que en la Figura 41.b se observa que se puede ingresar al router principal. Esto demuestra el funcionamiento de esta regla implementada.

#### 4.2.4. Control de ancho de banda por PCQ + Queues tree

El control de ancho de banda es una de las implementaciones más importantes que debe tener un equipo central, ya que por medio de este control se limita la velocidad de subida y bajada que tiene cada cliente. Este control se lo ha implementado utilizando el algoritmo de colas PCQ para crear una cola principal y mediante el árbol de colas Queues Tree se crearán el control de ancho de banda de subida y bajada para cada cliente como se observa en la Figura 42.

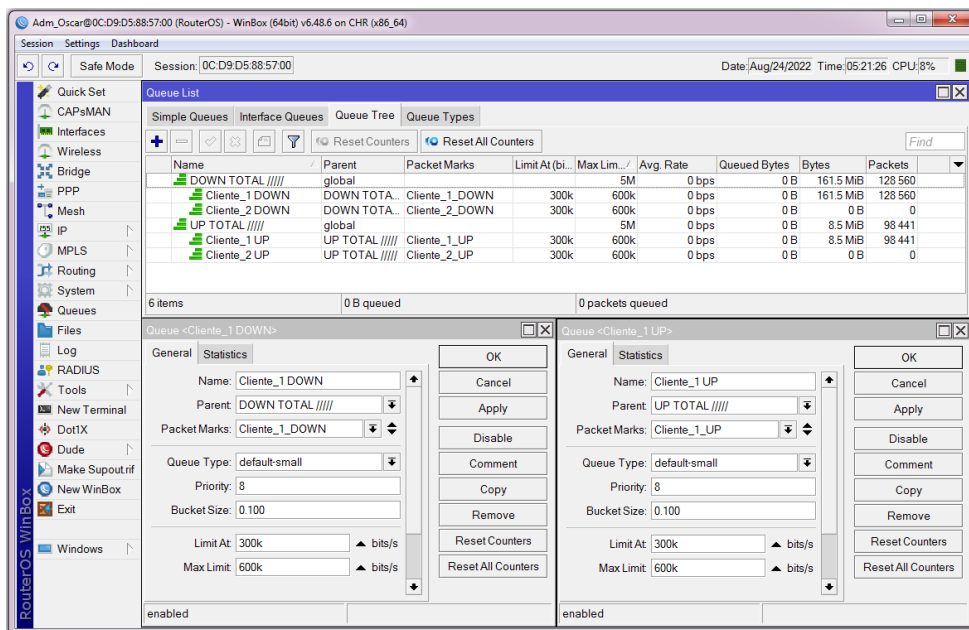


Figura 42. Árbol de colas implementado para el control de ancho de banda.

Para este proceso de control de ancho de banda es necesario el uso del Mangle dentro del Firewall, en donde se realiza el marcado de los paquetes tanto de entrada como de salida hacia el router de cada dirección IP a la cual se quiera controlar la velocidad de subida y baja, este proceso lo podemos observar en la Figura 43.

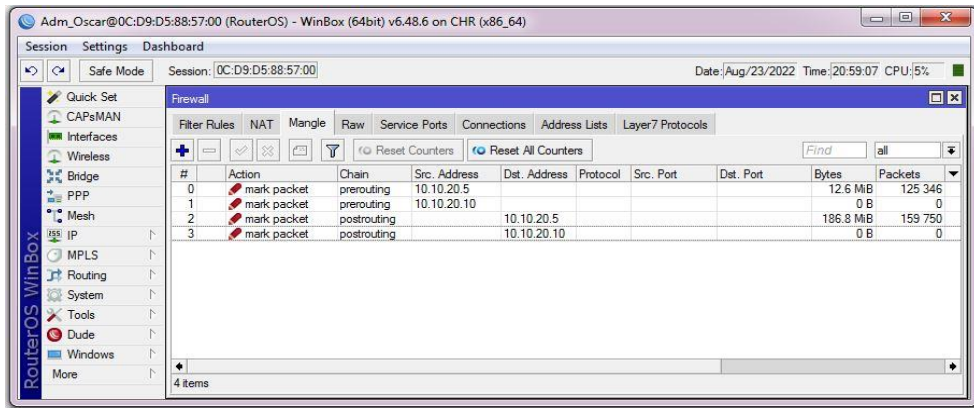


Figura 43. Mangle realizado para el marcado de paquete del control de ancho de banda.

Finalmente, para comprobar el correcto funcionamiento del control de ancho de banda de subida y baja se realizaron test de velocidad, dando como resultado lo siguiente.

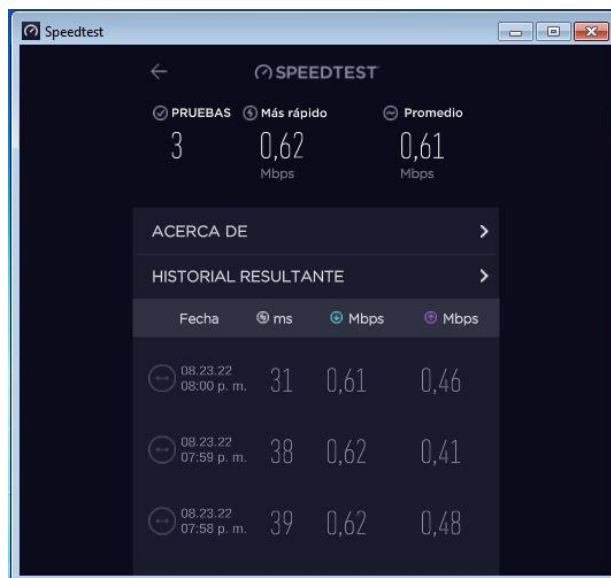


Figura 44. Test de velocidad realizado en el computador de prueba.

En la Figura 44 se observa los resultados del test de velocidad aplicado en el computador de prueba, en donde se determinó que la tasa promedio de bajada es de 0,62 Mbps es decir 620Kbps y la tasa de subida es de 0,61 Mbps es decir 610 Kbps lo cual demuestra que el control de ancho de banda realizado funciona correctamente, ya que como se puede comprobar en la Figura 24 el valor seteado para el ancho de banda de subida y baja es de 600 Kbps.



#### 4.2.5. Notificación de corte de servicio

Otra mejora a las configuraciones realizadas es la creación de un mensaje que notifique al cliente que su servicio asido suspendido por falta de pagos, para lo cual se utilizaron las reglas de corte de servicio ya implementadas y se añadió un redireccionamiento a una Webproxy mediante la configuración del Firewall NAT que se observa en la Figura 45.

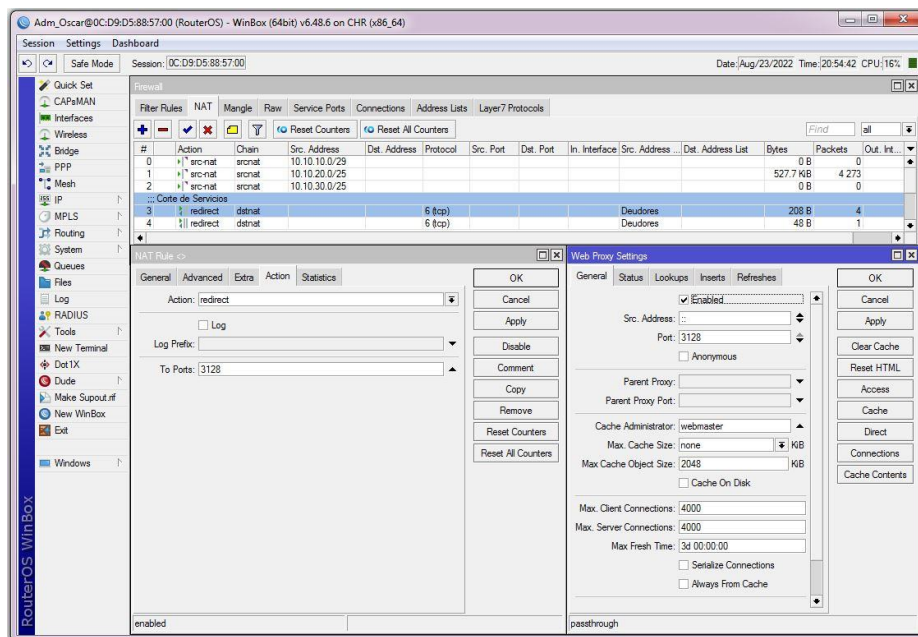


Figura 45. Configuración del NAT para la notificación del corte de servicio.

Para esta configuración se ha utilizado la acción *redirect*, la cual realiza el direccionamiento de todos los paquetes proveniente de la address list *Deudores* hacia el puerto 3128, este puerto es creado en la Web Proxy Setting del equipo principal en la cual se puede almacenar una página web html con el mensaje creado de la notificación de corte de servicio.

Para comprobar el correcto funcionamiento de esta configuración primero debemos agregar un cliente dentro del address list *Deudores* tal como se observa en la Figura 46.

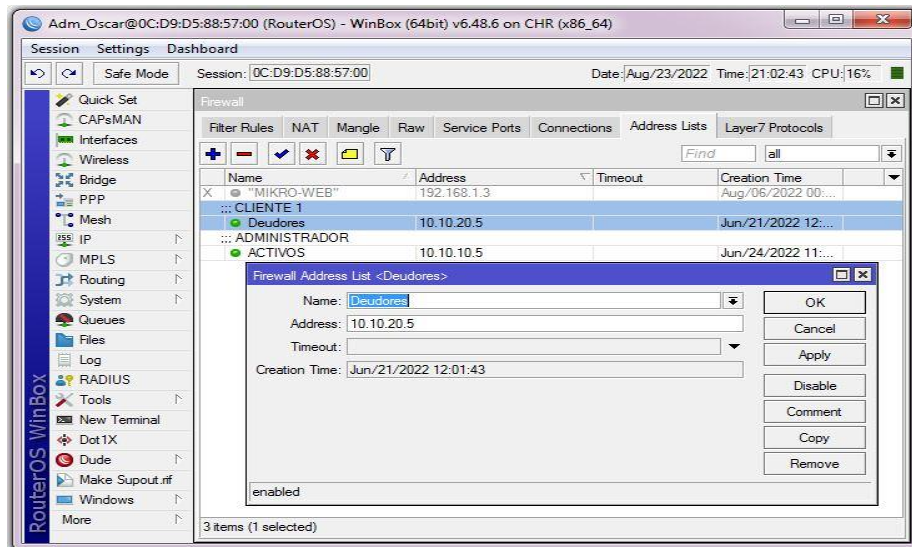


Figura 46. Agregar la dirección 10.10.20.5 dentro del address list Deudores.

Al agregar la dirección IP 10.10.20.5 dentro del address list *Deudores*, se aplicarán todas las reglas de corte de servicio y además el redireccionamiento hacia la página creada en Webproxy dando como resultado que aparezca el siguiente mensaje de notificación mostrado en la Figura 47. Cabe mencionar como Webproxy solo soporta páginas web http el mensaje de corte de servicio solo pasara a las cargas páginas web que utilicen el puerto 80.



Figura 47. Mensaje de notificación de corte de servicio.

## CONCLUSIONES

- Se realizó el estudio a la estructura actual de televisión de la empresa para determinar los equipos compatibles al sistema, dado que se pueda realizar la digitalización y modulación de canales en digital. Para esto, la compañía solo debería hacer el cambio de los moduladores analógicos y el CATV mixer por equipos robustos, económicos y digitales que soportan la transmisión en alta calidad.
- En este proyecto se diseñó una propuesta que permite ofertar 24 canales televisión de 48 en alta definición, haciendo atractivo los servicios de NETSURTV a sus clientes y futuros en la ciudad El Cambio. El diseño está basado en los equipos actuales que se encuentran en la fase de recepción y transmisión, añadiendo un codificador de canales que admite 24 entradas HDMI para cada canal de televisión y enlazado al modulador IPQAM que realiza la modulación de los 24 canales sin necesidad de usar un modulador por canal. En caso que se presente fallas en la nueva estructura, se propone un sistema redundante con los equipos actuales y de esta manera se asegurará que el cliente tenga servicio de televisión.
- Se realizó el presupuesto de los equipos necesarios para que NETSURTV brinde servicio de televisión en alta definición, con un costo de \$4.380 sin incluir aranceles, dándole a la empresa un ahorro del 85% en comparación de la cotización que presentó al inicio del proyecto. Considerando que el cambio de los 24 moduladores analógicos a digitales daba un costo de \$24.880, sin incluir aranceles, es más factible y económico utilizar un equipo robusto que realice la modulación digital de hasta 24 señales.
- Según el análisis realizado al tráfico de la red se determinó que el consumo máximo de ancho de banda era de 1070.2 Mbps, mientras que del CPU es del 12%; lo cual nos indicó que el equipo central (Mikrotik CCR1036) tiene la capacidad suficiente para soportar el crecimiento de la red. Pero el diseño actual de la topología de red no permitía un crecimiento adecuado, por lo cual se propuso implementar un nuevo diseño de la red que permita tener una mayor escalabilidad de la red y seguridad contra fallos de equipos; además de la adquisición de un sistema autónomo que le permita a la empresa aplicar una política de enrutamiento independiente y propia.

- Mediante la simulación de la topología de red propuesta en el software GNS3 se planteó mejoras en la seguridad de la red, ya que se determinó que las reglas de filtro actuales no cumplían con algún orden jerárquico o política de implementación; por lo cual se reorganizaron las reglas de filtro dentro del Firewall dando mayor prioridad a las reglas de bloqueo y denegación de ataques, seguido de las reglas de cortes de servicios y finalmente las reglas que dan acceso al router principal de la red.
- En cuanto a las mejoras de la calidad y servicio se planteó configuraciones para el control del ancho de banda utilizando el algoritmo PCQ, el cual permite crear una cola principal mediante el Queues Tree y a través de marcas de paquetes predeterminados en el Mangle se crearán las colas secundarias a las cuales se podrá asignar un ancho de banda predeterminado tanto de subida como de bajada, así la empresa podrá tener un mejor control del ancho de banda que consumen sus clientes.

## **RECOMENDACIONES**

- Como los sistemas de telecomunicaciones se encuentran en constante evoluciones es importante que las empresas puedan acoplar sus sistemas a las tecnologías actuales para que así puedan brindar un servicio de calidad.
- En una empresa que brinda servicios tecnológicos, es importante contar con un sistema de respaldo o redundante para que sus servicios no se vean afectador por daños internos.
- Es importante considerar la hoja de datos de los equipos, para saber el alcance de los proyectos, dado que ciertas configuraciones que se puede implementar en el sistema no sean compatibles con equipos integrados.
- En este proyecto se realizaron simulaciones para comprobar la funcionalidad de algunas soluciones, para lo cual fue necesario analizar todos los softwares compatibles a las necesidades que se tenían y así determinar cuál era el más adecuado.

- Al momento de realizar las simulaciones es importante utilizar un equipo que tengas las capacidades necesarias de soportar procesos que ocupan un alto consumo de CPU y memoria RAM.

## BIBLIOGRAFIA

- [1] ARCOTEL, «Participación de Mercado e Indices de Contracción de los Servicios de Telecomunicaciones,» 10 Diciembre 2021. [En línea]. Available: <https://www.arcotel.gob.ec/wp-content/uploads/2021/12/Boleti%CC%81n-estadistico-noviembre-2021.pdf>. [Último acceso: 30 Mayo 2022].
- [2] C. Systems, «Cisco D9865 Satellite Receiver Software,» Enero 2013. [En línea]. Available: [https://www.churchofjesuschrist.org/help/support/bc/clerksupport/meetinghouse-technology/pdf/Cisco\\_9865D\\_Manual.pdf?lang=jpn](https://www.churchofjesuschrist.org/help/support/bc/clerksupport/meetinghouse-technology/pdf/Cisco_9865D_Manual.pdf?lang=jpn). [Último acceso: 28 Mayo 2022].
- [3] ARCOTEL, «Boletín Estadístico: Servicio de Acceso a Internet,» Pag. 03, 25 Noviembre 2020. [En línea]. Available: <https://www.arcotel.gob.ec/wp-content/uploads/2020/12/BOLETIN-NOVIEMBRE-2020-25-11-2020.pdf>. [Último acceso: 30 Mayo 2022].
- [4] ARCOTEL, «Boletín Estadístico: Servicio de Acceso a Intener,» Pag. 12, 25 Noviembre 2020. [En línea]. Available: <https://www.arcotel.gob.ec/wp-content/uploads/2020/12/BOLETIN-NOVIEMBRE-2020-25-11-2020.pdf>. [Último acceso: 30 Mayo 2022].
- [5] «Actualidades de la UIT,» septiembre 2009. [En línea]. Available: <https://www.itu.int/net/itunews/issues/2009/07/18-es.aspx>. [Último acceso: 30 mayo 2022].
- [6] J. C. Amaya, 2014. [En línea]. Available: <https://repositorio.unal.edu.co/bitstream/handle/unal/55297/Jimena%20Chilito%20Amaya.2014.pdf?sequence=1&isAllowed=y>. [Último acceso: 30 mayo 2022].
- [7] S. Fernández, «Cabecera de Televisión Por Cable,» Septiembre 2012. [En línea]. Available: [https://oa.upm.es/14077/1/PFC\\_SERGIO\\_FERNANDEZ\\_MESAS.pdf](https://oa.upm.es/14077/1/PFC_SERGIO_FERNANDEZ_MESAS.pdf). [Último acceso: 30 Mayo 2022].
- [8] M. S. ., A. S. Sibasis Bandyopadhyay, «Ird India,» 2015. [En línea]. Available: [http://www.irdindia.in/journal\\_ijraet/pdf/vol3\\_iss5/3.pdf](http://www.irdindia.in/journal_ijraet/pdf/vol3_iss5/3.pdf). [Último acceso: 30 Mayo 2022].
- [9] A. Morales, 2010. [En línea]. Available: <https://repositorio.espe.edu.ec/bitstream/21000/2645/1/T-ESPE-029824.pdf>. [Último acceso: 2 Junio 2022].

- [10] D. P. Cedeño, Enero 2016. [En línea]. Available: <https://dspace.ups.edu.ec/bitstream/123456789/12398/1/UPS%20-%20ST002128.pdf>. [Último acceso: 2 Junio 2022].
- [11] J. Coronel, 2013. [En línea]. Available: <https://dspace.ups.edu.ec/bitstream/123456789/3473/1/UPS-CT002563.pdf>. [Último acceso: 2 Junio 2022].
- [12] C. Villadiego, «Técnicas de optimización del ancho de banda en las redes LAN - Parte II,» 17 Noviembre 2003. [En línea]. Available: <https://biblioteca.utb.edu.co/notas/tesis/0024205.pdf>. [Último acceso: 04 Junio 2022].
- [13] P. Juca, «Estudio de la implementación de Calidad de Servicio (QoS) para el mejoramiento de la red de datos que optimice el acceso a los servicios en la Planta de Producción de la Compañía Yanbal Ecuador S.A.,» 2016. [En línea]. Available: <http://repositorio.puce.edu.ec/handle/22000/12463>. [Último acceso: 04 Junio 2022].
- [14] A. Zamora, «Evaluación para el Control de Tráfico y QoS en el entorno de redes de datos mediante Tecnología MIKROTIK,» Agosto 2014. [En línea]. Available: <http://repositorio.ucsg.edu.ec/bitstream/3317/2816/1/T-UCSG-PRE-TEC-ITEL-72.pdf>. [Último acceso: 05 Junio 2022].
- [15] X. Jaramillo, «Estudio de catálogo de las aplicaciones y estructuras de ancho de banda en la red interna institucional de la Escuela Politécnica de Ejército basada en mikrotik para garantizar los servicios de red,» Enero 2013. [En línea]. Available: <http://repositorio.espe.edu.ec/handle/21000/6307>. [Último acceso: 06 Junio 2022].
- [16] G. Saona, «IMPLEMENTACIÓN DE UN SISTEMA DE RED ESTRUCTURADO EN LA EMPRESA PROVEEDORA DE INTERNET TUVENTURA S.A. - SALINASNET,» Julio 2015. [En línea]. Available: <repositorio.upse.edu.ec/bitstream/46000/2435/1/UPSE-TET-2015-0012.pdf>. [Último acceso: 06 Junio 2022].
- [17] F. A. Moya Leimberg, «Rediseño de la red del ISP Readynet Cía. Ltda., procedimiento para convertir al ISP en un sistema autónomo,» Septiembre 2009. [En línea]. Available: <http://bibdigital.epn.edu.ec/handle/15000/1819>. [Último acceso: 04 Junio 2022].
- [18] D. E. ., F. .. M. J. ., F. .. D. G. a. N. .. A. M. Fisher, «Television,» 31 enero 2020. [En línea]. Available: <https://www.britannica.com/technology/television-technology>. [Último acceso: 6 julio 2022].
- [19] T. Marte, «La Transición de la TV analógica a la Tv digital,» 13 diciembre 2018. [En línea]. Available: <https://www.tomasmarte.com/2018/12/13/la-transicion-de-la-tv-analoga-a-la-tv-digital/>. [Último acceso: 10 julio 2022].
- [20] J. G. Barrio, «Transmisión y recepción de la señal de televisión,» septiembre 2013. [En línea]. Available: [http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72305/5/Televisi%C3%B3n\\_M%C3](http://openaccess.uoc.edu/webapps/o2/bitstream/10609/72305/5/Televisi%C3%B3n_M%C3)

- %B3dulo%206\_Transmisi%C3%B3n%20y%20recepti%C3%B3n%20de%20la%20se%C3%B1al%20de%20televisi%C3%B3n.pdf. [Último acceso: 10 julio 2022].
- [21] «Headend Techs,» [En línea]. Available: <https://headendinfo.com/digital-headend/>. [Último acceso: 30 mayo 2022].
- [22] «Alibaba,» [En línea]. Available: <https://spanish.alibaba.com/product-detail/24-in-1-Edge-IP-qam-60771417216.html>. [Último acceso: 12 julio 2022].
- [23] «¿Qué es IPTV? Ventajas y puntos negativos. ¿Qué canales puedo ver?,» [En línea]. Available: <https://selectra.es/internet-telefono/que-es/iptv>. [Último acceso: 12 julio 2022].
- [24] «Alibaba,» [En línea]. Available: <https://spanish.alibaba.com/product-detail/Catcast-Encoders-para-tv-Digital-tv-60769145660.html>. [Último acceso: 12 julio 2022].
- [25] M. Zapata, «Modulación QAM,» SYSCOM, julio 2022. [En línea]. Available: <https://soporte.syscom.mx/es/articles/2334170-modulacion-qam>. [Último acceso: 18 julio 2022].
- [26] «Wi-Fi 6, publicación 5: Modulación de alto orden 1024-QAM,» HUAWEI, 25 marzo 2021. [En línea]. Available: <https://forum.huawei.com/enterprise/es/wi-fi-6-publicaci%C3%B3n-5-modulaci%C3%B3n-de-alto-orden-1024-qam/thread/710853-100239>. [Último acceso: 19 julio 2022].
- [27] L. Vásquez, «Teleco in a nutshell v8.7: Modulación de Amplitud en Cuadratura,» FULPROJECT, 20 noviembre 2019. [En línea]. Available: <https://www.flu-project.com/2019/11/teleco-in-nutshell-v87-modulacion-amplitud-cuadratura.html>. [Último acceso: 19 julio 2022].
- [28] E. Etecé, «ISP,» 05 Agosto 2021. [En línea]. Available: <https://concepto.de/isp/>. [Último acceso: 18 Julio 2022].
- [29] C. N. Acedemy, «Implementación de un diseño de red,» [En línea]. Available: <https://www.sapalomera.cat/moodlecf/RS/3/course/module1/index.html#1.1.1.3>. [Último acceso: 23 Julio 2022].
- [30] Wikipedia, «Router,» [En línea]. Available: <https://es.wikipedia.org/wiki/Router>. [Último acceso: 25 Julio 2022].
- [31] M. Gonzalez, «El switch: cómo funciona y sus principales características,» 08 11 2013. [En línea]. Available: <https://redstelematicas.com/el-switch-como-funciona-y-sus-principales-caracteristicas/>. [Último acceso: 26 Julio 2022].
- [32] J. C. e. a. Pérez, «Sistemas operativos,» McGraw-Hill Interamericana, 2001.
- [33] D. Burgess, «Learn RouterOS,» Lulu. com, 2011.

- [34] R. Anrrango, «Conceptos Generales de WINBOX,» 30 Septiembre 2014. [En línea]. Available: <https://configurarmikrotikwireless.com/blog/conceptos-winbox-configurar-mikrotik.html>. [Último acceso: 26 Julio 2022].
- [35] M. Clep, «Calidad de Servicio Implementación de un Sistema de QoS en RouterOS,» 28 Noviembre 2009. [En línea]. Available: [http://mum.mikrotik.com/presentations/AR09/mario\\_clep.pdf](http://mum.mikrotik.com/presentations/AR09/mario_clep.pdf). [Último acceso: 25 Julio 2022].
- [36] M. Wiki, «Manual:Queue,» 31 Agosto 2021. [En línea]. Available: <https://wiki.mikrotik.com/wiki/Manual:Queue>. [Último acceso: 25 Julio 2022].
- [37] M. Wiki, «Manual:HTB,» 22 Abril 2019. [En línea]. Available: <https://wiki.mikrotik.com/wiki/Manual:HTB>. [Último acceso: 01 Agosto 2022].
- [38] Lacnic, «3. DISTRIBUCIÓN DE NÚMEROS DE SISTEMA AUTÓNOMO,» 03 08 2022. [En línea]. Available: <https://www.lacnic.net/546/1/lacnic/>. [Último acceso: 05 Agosto 2022].
- [39] C. Vicente, «Introduccion a BGP,» 21 09 2011. [En línea]. Available: [https://nsrc.org/workshops/2011/walc/routing/raw-attachment/wiki/Agenda/Intro\\_BGP.pdf](https://nsrc.org/workshops/2011/walc/routing/raw-attachment/wiki/Agenda/Intro_BGP.pdf). [Último acceso: 15 Agosto 2022].
- [40] «Cisco D9865 Satellite Receiver Software,» junio 2013. [En línea]. Available: [https://www.churchofjesuschrist.org/help/support/bc/clerksupport/meetinghouse-technology/pdf/Cisco\\_9865D\\_Manual.pdf?lang=spa](https://www.churchofjesuschrist.org/help/support/bc/clerksupport/meetinghouse-technology/pdf/Cisco_9865D_Manual.pdf?lang=spa). [Último acceso: 31 julio 2022].
- [41] [En línea]. Available: [https://sifis.fisoluciones.com/shop/page/5?order=list\\_price+asc](https://sifis.fisoluciones.com/shop/page/5?order=list_price+asc). [Último acceso: 31 julio 2022].
- [42] [En línea]. Available: <https://www.ocompra.com/mexico/item/modulador-pico-macom-pcm55saw-canal-29-692933329/>. [Último acceso: 31 julio 2022].
- [43] «Combinador pasivo RF Canal 16/24 Mezclador, Combinadora CATV,» [En línea]. Available: [https://es.made-in-china.com/co\\_softel-optic/product\\_16-24-Channel-RF-Combiner-Passive-Mixer-CATV-Combiner\\_eoiyusnsy.html](https://es.made-in-china.com/co_softel-optic/product_16-24-Channel-RF-Combiner-Passive-Mixer-CATV-Combiner_eoiyusnsy.html). [Último acceso: 31 julio 2022].
- [44] «1550nm transmisor óptico de modulación de la Interna con 10dB de potencia de salida óptica,» [En línea]. Available: [https://es.made-in-china.com/co\\_softel-optic/product\\_1550nm-Internal-Modulation-Optical-Transmitter-with-10dB-Optic-Power-Output\\_egrhnyy.html](https://es.made-in-china.com/co_softel-optic/product_1550nm-Internal-Modulation-Optical-Transmitter-with-10dB-Optic-Power-Output_egrhnyy.html). [Último acceso: 31 julio 2022].
- [45] «AliExpress,» [En línea]. Available: <https://es.aliexpress.com/item/10000136572332.html>. [Último acceso: 12 julio 2022].
- [46] «Alibaba,» [En línea]. Available: <https://spanish.alibaba.com/product-detail/24-in-1-Edge-IP-qam-60771417216.html>. [Último acceso: 12 julio 2022].



- [47] «DVB-T MPEG2/4 HDMI con TDT salida RF Modulador codificador,» [En línea]. Available: [https://es.made-in-china.com/co\\_catcast/product\\_DVB-T-MPEG2-4-HDMI-with-DVB-T-RF-out-Encoder-Modulator\\_eohneryeg.html](https://es.made-in-china.com/co_catcast/product_DVB-T-MPEG2-4-HDMI-with-DVB-T-RF-out-Encoder-Modulator_eohneryeg.html). [Último acceso: 31 julio 2022].
- [48] «Mikrotik,» [En línea]. Available: <https://mikrotik.com/product/CCR1036-12G-4S-149>. [Último acceso: 15 Julio 2022].

## ANEXOS

### Anexo 1: Datasheet del codificador

#### Características principales

Admite entrada HDMI de 24 canales. (compatible con HDCP)  
Admite 1 entrada/salida IP Gigabit, salida SPTS / MPTS, protocolo UDP / RTP (multicast), salida unicorast RTSP.  
Admite 2 entradas ASI  
Admite 2 salidas independientes de ASI  
Compatible con LCD y funciones clave  
Admite Administración de Red (Web)  
Soporte de actualización en línea

#### Índice técnico

Entrada HDMI (24 HDMI)  
2 entradas ASI  
1 entrada de Puerto IP Gigabit Ethernet  
Salida 2 salidas ASI independientes  
Salida IP (salida SPTS, salida MPTS), UDP, protocolo RTP.  
Formato de codificación de video MPEG-4 AVC / H.264  
Interfaz de entrada HDMI  
Entrada de resolución: 1920 × 1080 60P/50P/30P / 1920 × 1080i / 1280 × 720P / 720x576i / 720x480i @ 50/59,94Hz  
Salida: 1920 × 1080\_60P/50P/30P, 1920 × 1080\_30P, 1280 × 720\_30P, 720x576\_25P, 720x480\_25P  
Velocidad de bits 1Mbps ~ 13Mbps (cada canal)  
Modo de velocidad CBR, VBR  
Formato de codificación de Audio MPEG1 Layer2  
Frecuencia de muestreo: 48KHz  
Velocidad de bits 64kbps, 128Kbps, 192kbps, 224kbps, 256kbps, 320kbps, 384kbps.  
Administración de Red del sistema (Web) compatible con actualización de red  
Interfaz de operación en chino/inglés  
Tamaño general (largo x ancho x alto): 482mm x 410mm x 44 mm.  
Peso 8kg  
Rango de temperatura 0 ~ 45 °C (funcionamiento); -20 ~ 80 °C (almacenamiento)  
Requisitos de potencia AC100 ~ 240V, 50 / 60Hz  
Consumo de energía <90W

Figura 1. Datasheet del codificador

En la Figura 1 se muestra las características principales del codificador AOURI, mostrando sus compatibilidades y la resolución de imagen que brinda, dado que la mayor resolución de salida es de 1920x1080 pixeles.

## Anexo 2: Datasheet del IPQAM mux scrambler

Entrada IP (módulo QAM)	
Interfaz	2 x100/1000 Base-T Ethernet RJ-45 puertos
Modo de operación	Independiente o redundante
Formato de los datos	MPEG TS--IP/UDP/RTP
Capa MAC acceso	IEEE 802.3, IEEE 802.3u, IEEE 802.3ab
Abordar y Protocolo	Multicast y Unicast
Codificación de flujo de transporte (opciones de Software)	
Algoritmo de cifrado	Cumplir con DVB-CSA
Número de codificador incorporado	128
Número de CAS	Opcional hasta cuatro DVB simulación CAS(s)
CAS de interfaz	TCP/UDP (a través del puerto de administración de red)
Protocolo	0 ~ 1Mbps/TS
EMM ancho de banda	Hasta 60 Mbps por canal QAM
Salida de modulación (módulo QAM)	
Conector de salida	1 x salida de RF 1 puerto de prueba RF-20dB
Conector, tipo A	Tipo F (hembra, 75 Ω)
RF rango de frecuencia	47MHz ~ 900MHz
Ancho de banda	6 o 8MHz
Cantidad de QAM canal	24 canales QAM (o portadores)
La modulación de las	ITU-T J.83
Las constelaciones	Anexo A: 16 /32 /64 /128 /256QAM Anexo B: 64 /256QAM Anexo C: 32 /64 /128 /256QAM
Símbolo de	Cuadro de 4,2 A 7 M Anejo B: 5,057 M en memoria Cuadro de 4,2 a 5,3 M
Potencia de salida de RF nivel	98 a 119 dBuV (puerto de salida RF) 70 a 90 dBuV (puerto de prueba de-20dB)
MER	≥ 38dB (64QAM 6.875M Baud)
SNR (fuera de banda)	≥ 50dB
Pérdida de retorno	≥ 12dB
Portador de represión	> 58dB
Ganancia de Fine-tune	0 a 5,0dB, tamaño de paso 0,25dB
DE GESTIÓN DE	
Interfaz	1x10/100 Base-T Ethernet
Conector	RJ-45 (Panel frontal accesible)
DE GESTIÓN DE	Navegador Web y administración de SNMP
Medio ambiente	
Fuente de alimentación	Módulo de fuente de alimentación integrado Opcional 1 + 1 Fuente de alimentación intercambiable en caliente y superflua
Tensión de entrada	100-240 VCA, 50/60Hz
Rango de temperatura de	5 °C ~ 40 °C (41 °F ~ 104 °F)
Rango de presión	-25 °C 70 70 °C (-13 °F ~ 158 °F)
Rango de humedad	86 ~ 106KPa
Potencia nominal	10% ~ 90%
Dimensiones	125W
Peso	490mm × 490mm × 45mm

Figura 2. Datasheet del IPQAM

En la Figura 2 se muestra las características del modulador IP-QAM, reflejando el tipo de entrada y salida que soporta, la potencia que emite, la frecuencia en que trabaja y las configuraciones que realiza.

### Anexo 3: Configuración de sistema autónomo de ISP\_1 Y ISP\_2

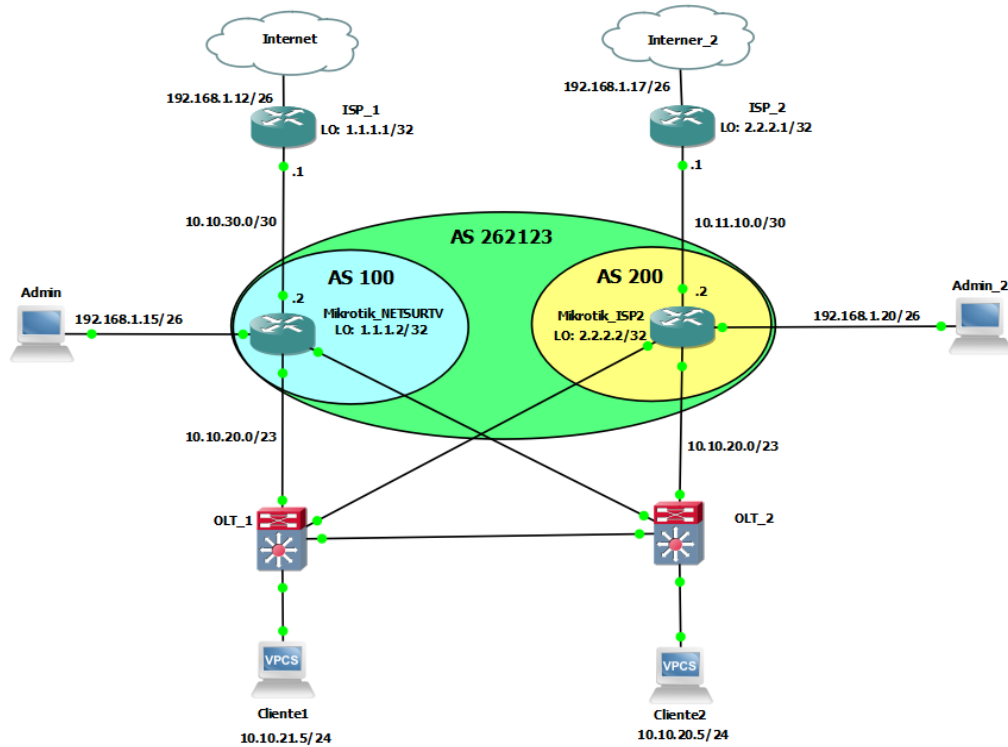


Figura 3. Topología de Red Simulada

Para la simulación del sistema autónomo del ISP\_1 y ISP\_2 se partirá de la base que la topología mostrada en la Figura 3 se implementó en el software GNS3, además se utilizará la aplicación de WinBox para facilitar las configuraciones y se procederá a realizar los siguientes pasos:

- 1. Asignación de direcciones IP:** Una vez ingresado la router ISP\_1 o ISP\_2 nos dirigiremos a IP>>Addresses, y se abrirá la siguiente ventana (Ver Figura 4).

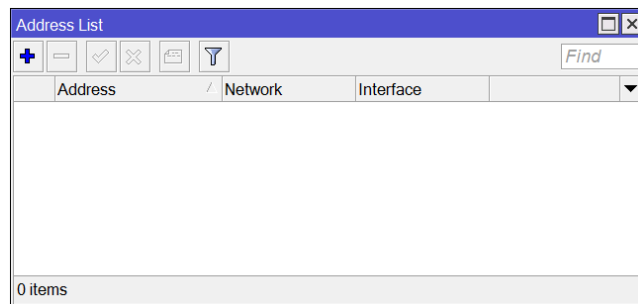


Figura 4. Ventana de Address List.

Daremos clic sobre el símbolo “+” y agregaremos las direcciones IP guiándonos con la topología de red de la Figura 3, teniendo como resultado lo siguiente.

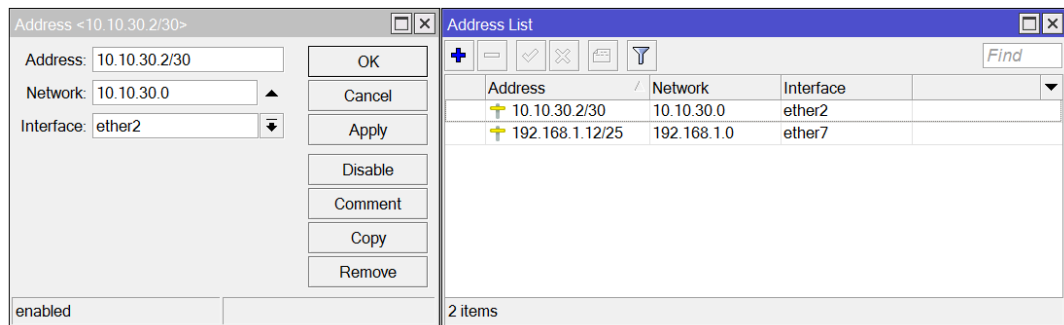


Figura 5. Asignación de direcciones IP en router ISP\_1.

En la figura 5 podemos apreciar las direcciones IP que se han asignado a las respectivas interfaces Ethernet, el mismo procedimiento deberá realizarse en el router del ISP\_2.

- 2. Creación de la interface loopback:** Las interfaces de loopback se crearán mediante interface virtuales Bridge (esta opción estará en la ventana principal del WinBox), tal como se puede notar en la Figura 6.

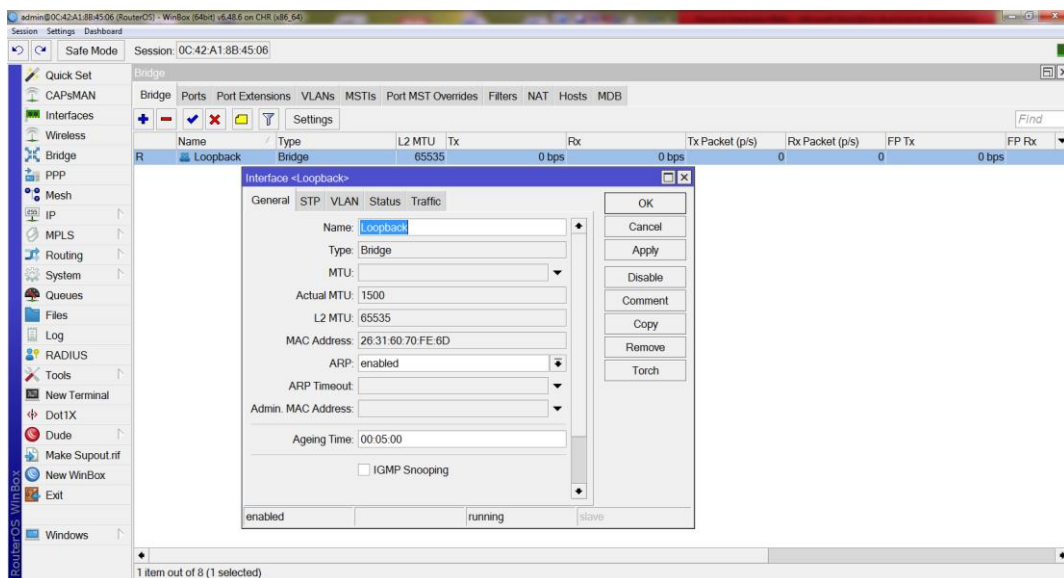


Figura 6. Creación de Interface loopback.

Una vez creada la interface loopback se le deberá asignar la dirección IP que indica en la topología de red, como se muestra en la Figura 7.

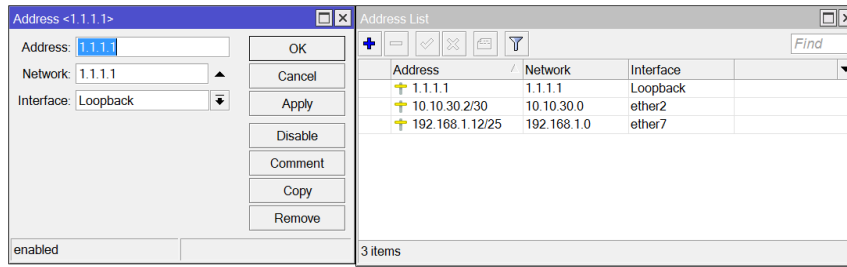


Figura 7. Asignación de dirección IP a la interface Loopback en el router ISP\_1.

El mismo procedimiento deberá realizarse para las configuraciones del router ISP\_2 y se tendrá el resultado mostrado en la Figura 8.

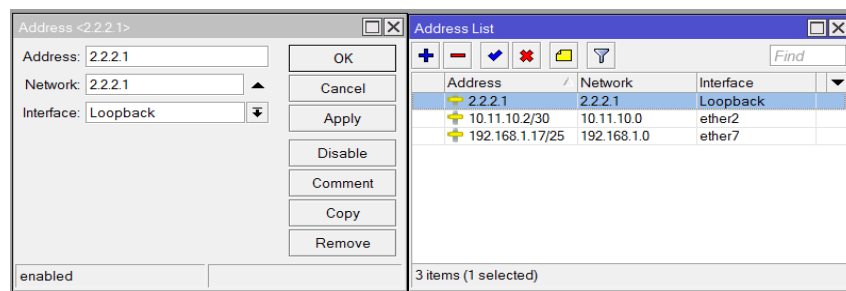


Figura 8. Asignación de dirección IP a la interface Loopback en el router ISP\_2.

**3. Configuraciones BGP:** Como un sistema autónomo se comunica mediante el protocolo BGP se debe levantar una sesión para dicho protocolo, este procedimiento se lo realiza ingresando en la opción Routing>>BGP. En esta ventana (Ver Figura 9) primero se crea la Instancia BGP en la cual se pondrá el ASN del sistema autónomo, para el caso de la simulación se utilizó el AS 185324 y como Router ID la dirección de loopback.

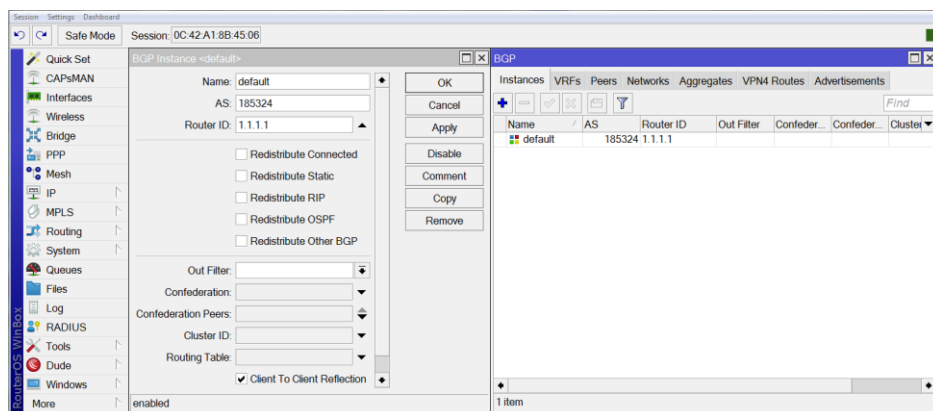


Figura 9. Creación de Instancia BGP en router ISP\_1.

El mismo procesamiento se deberá implementarse en la router ISP\_2 y se obtendrá el siguiente resultado (ver Figura 10).

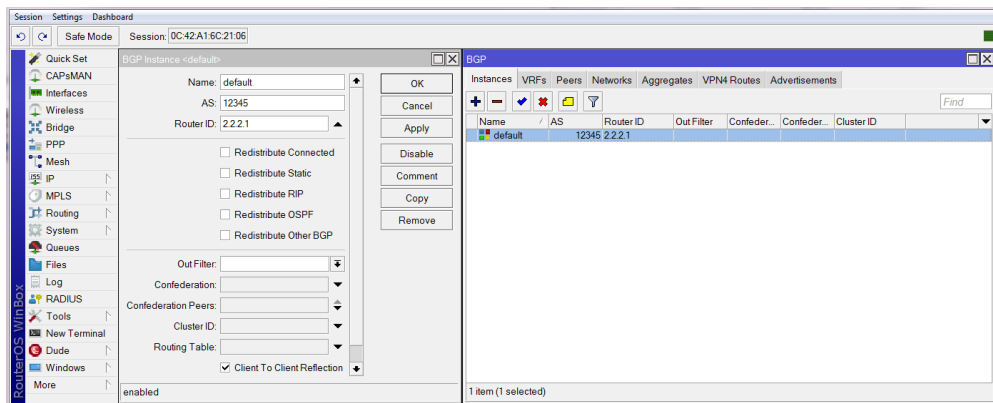


Figura 10. Creación de Instancia BGP en router ISP\_2.

#### Anexo 4: Configuración de peers del ISP\_1 Y ISP\_2

Esta configuración es necesaria para que exista comunicación entre AS del proveedor y AS que se levantara en el router de Core (Mikrotik\_Netsurtv).

Primero debemos ingresar a opción Routing>>BGP y abrir la pestaña Peers; a continuación, se creara uno nuevo presionando sobre “+” y llenaremos las casillas con la información del AS que se creó en el router Mikrotik\_Netsurtv (Ver Figura 11).

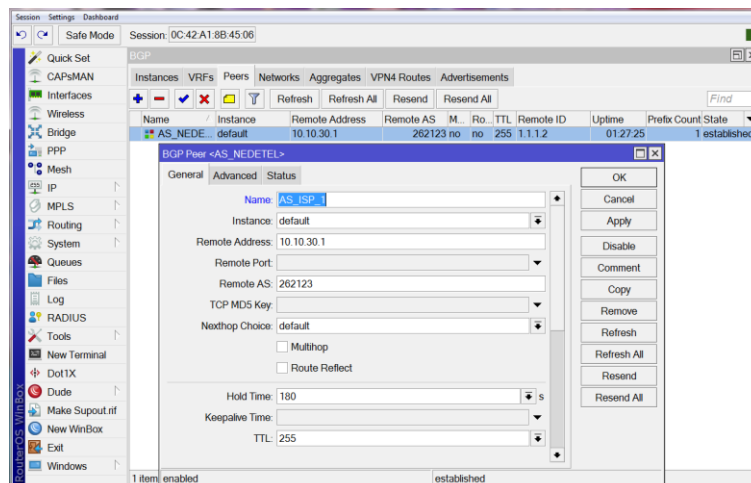


Figura 11. Creación del Peer en router ISP\_1.

Este mismo procedimiento servirá para crear el peer en el router ISP\_2 y para tener constancia que existe comunicación entre sistemas autónomos se deberá revisar la tabla de rutas del router ISP\_1.

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source	BGP AS Path	BGP Origin
AS	0.0.0.0/0	192.168.1.1 reachable ether7	1				
DAC	1.1.1.1	Loopback reachable	0		1.1.1.1		
DAb	10.10.21.0/24	10.10.30.1 reachable ether2	20			262123	igp
DAC	10.10.30.0/30	ether2 reachable	0		10.10.30.2		
DAC	192.168.1.0/25	ether7 reachable	0		192.168.1.12		

Figura 12. Tabla de rutas del router ISP\_1.

Como podemos notar en la Figura 12 el router ISP\_1 está recibiendo los prefijos 10.10.21.0/24 desde el AS 262123, esto nos indica que la sesión BGP se ha establecido correctamente.

## Anexo 5: Configuración para bloqueo de DDoS

Como esta configuración está compuesta por 2 reglas principales primero se explicará la regla para la detección del ataque:

1. Ingresar al router que se desea configurar mediante Winbox e ir a IP>>Firewall (ver Figura 13).

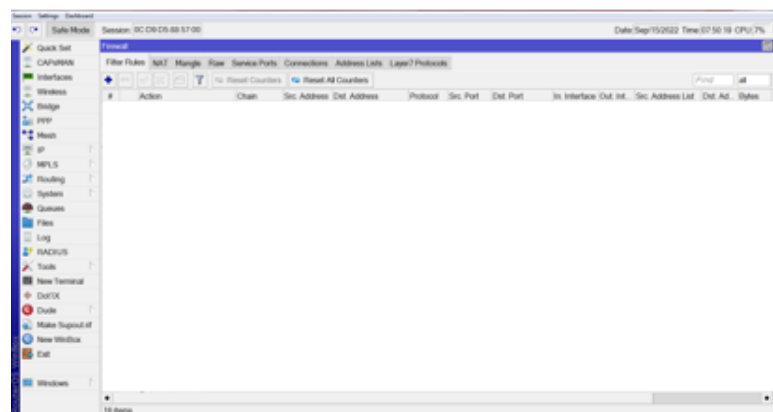


Figura 13. Ingreso al Firewall por WinBox.



- Una vez dentro dar click sobre “+” para añadir una nueva regla. En la ventana que se despliegue se deberá colocar en la pestaña “Chain” la opción “input” y escoger el Protocolo TCP (Ver Figura 14).

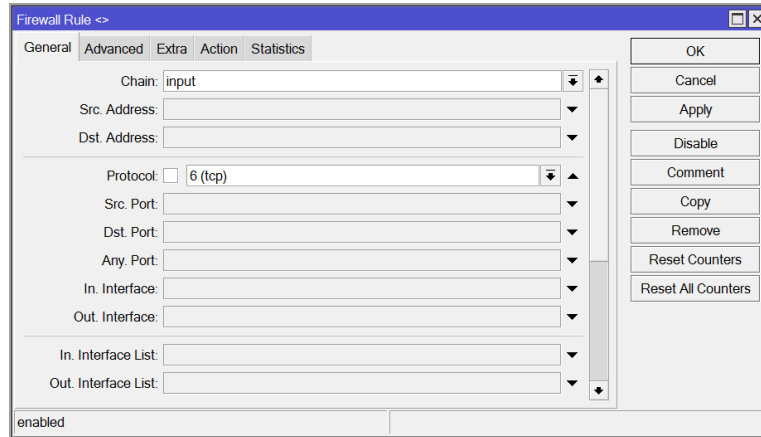


Figura 14. Configuraciones “General” para detección de ataque DDoS.

- Después continuamos en la pestaña “Action” en la cual se elige la opción “add src to address list” esto nos permitirá añadir direcciones IP a un address list la cual la llamaremos “Lista\_negra\_DoS” con un tiempo de duración de 10 minutos (Ver Figura 15).

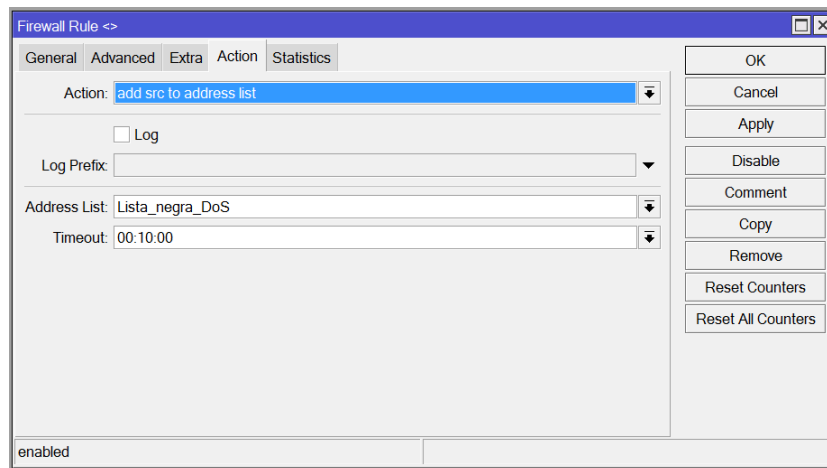


Figura 15. Configuraciones “Action” para detección de ataque DDoS.

- Finalmente vamos a la pestaña “Extra” en la que se pondrá los parámetros 10 en “Limit” y 32 “Netmask”, dichos parámetros son los más indicados para detectar este tipo de ataques (Ver Figura 16).

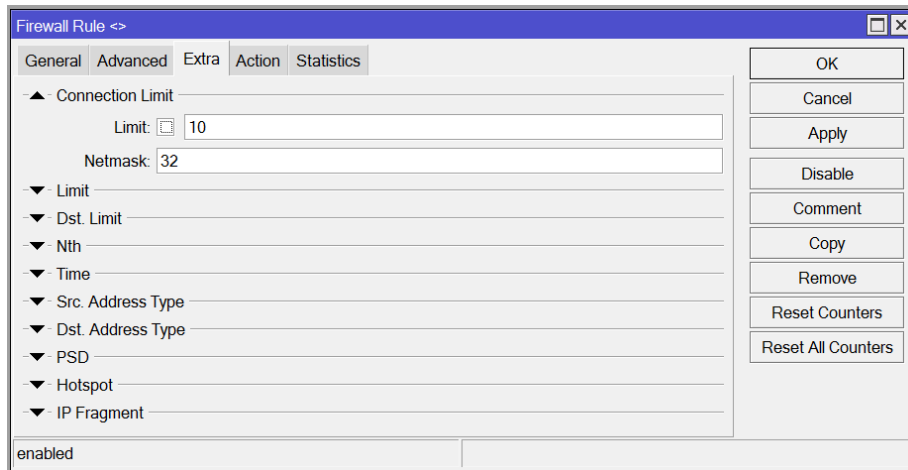


Figura 16. Configuraciones “Extra” para detección de ataque DDoS.

Para la regla de supresión del ataque se realizará el siguiente procedimiento.

1. Una vez estemos dentro del Firewall añadiremos una nueva regla con las mismas configuraciones del paso 2 y 4 de la configuración pasada.
2. Después en la pestaña “Advanced” se añadirá la address liste “Lista\_negra\_DoS” dentro de la opción “Src. Address List”, lo cual permite realizar solo aplicar esta regla a las direcciones que pertenecen a esa lista (Ver Figura 17).

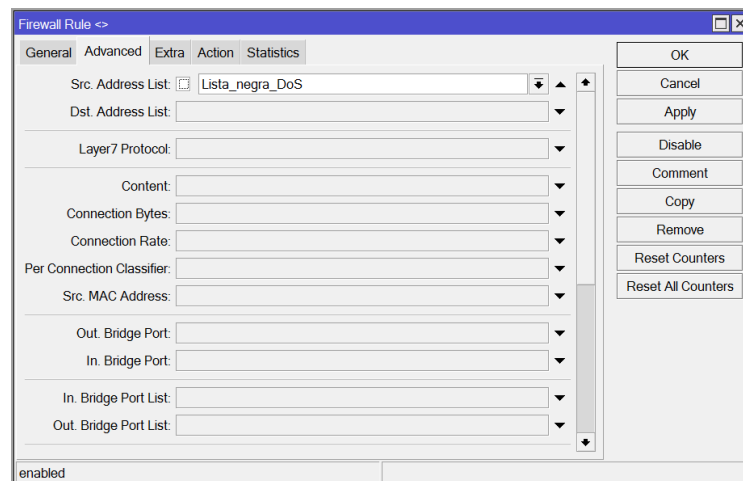


Figura 17. Configuraciones “Advanced” para la supresión del ataque DoS.

3. Finalmente, en la pestaña “Action” se escogerá la opción “tarptit”, esta configuración permitirá contener los paquetes de datos que se envían durante un ataque DDoS (Ver Figura 18).

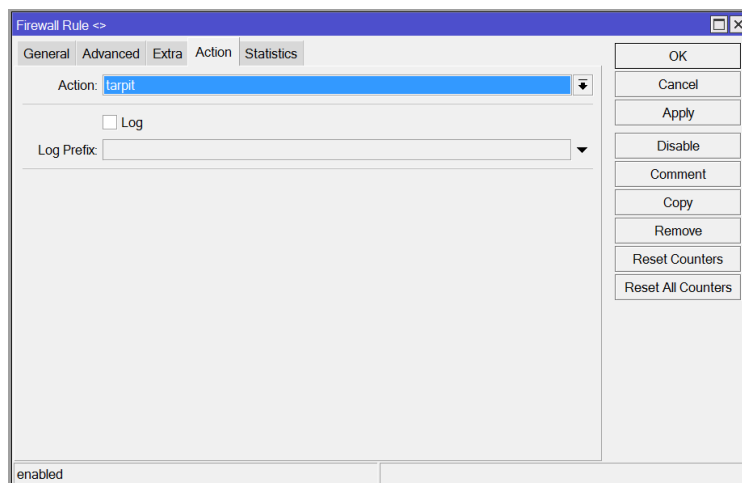


Figura 18. Configuración “Action” para la supresión del ataque DDoS.

## Anexo 6: Configuración para dar acceso al equipo central

Para implementar esta configuración debemos realizar el siguiente procedimiento:

1. Dentro del Firewall añadiremos una nueva regla. En la ventana que se despliegue se deberá colocar en la pestaña “Chain” la opción “input”, para el parámetro “Src. Address” se escribirá el segmento o prefijos de IP a los cuales se les quiere dar el acceso al equipo central y en opción “In. Interface” se pondrá el puerto ethernet WAN y activar la casilla de exclusión, lo cual permitirá dar acceso al router a todas las IP que entren dentro del rango escogido y pasen por cualquier puerto menos el puerto WAN, como se muestra en la Figura 19.

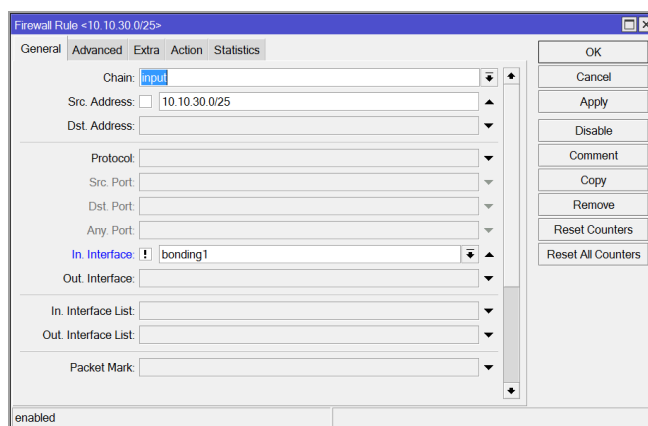


Figura 19. Configuración “General” para dar acceso a segmentos de IP al equipo central.

2. Finalmente, en la pestaña “Action” se escogerá la opción “accept” (Ver Figura 20), lo cual permitirá aceptar todas las acciones que provengan de las direcciones IP escogidas

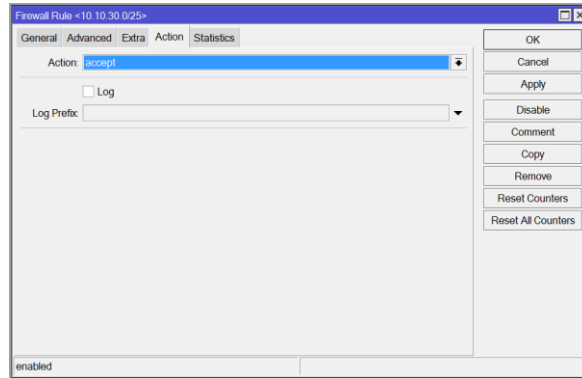


Figura 20. Configuración “Action” para dar acceso a segmentos de IP al equipo central.