

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR



**FACULTAD DE INGENIERÍA
MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN
MENCIÓN REDES DE COMUNICACIONES**

TEMA:

**“DISEÑO Y EMULACIÓN DE UNA RED DE DATOS CON
PRIORIZACIÓN DE SERVICIOS EN LA UNIDAD EDUCATIVA
SUIZO AMBATO”**

AUTOR:

ING. JUAN EDUARDO SALCEDO CASTILLO

DIRECTOR:

ING. GUSTAVO SALAZAR-CHACÓN, MSc.

Quito – 2020

AUTORÍA

Yo, Juan Eduardo Salcedo Castillo, portador de la cédula de ciudadanía No 1802916500, declaro bajo juramento que la presente investigación es de total responsabilidad del autor, y que se ha respetado las diferentes fuentes de información realizando las citas correspondientes. Esta investigación no contiene plagio alguno y es resultado de un trabajo serio desarrollado en su totalidad por mi persona.

Juan Eduardo Salcedo Castillo

Tabla de contenido

AUTORÍA	2
1 INTRODUCCIÓN	7
1.1 INTRODUCCIÓN	7
1.2 JUSTIFICACIÓN	8
1.3 ANTECEDENTES	9
1.4 OBJETIVOS	11
2 SITUACIÓN ACTUAL Y ESTUDIO PRELIMINAR	12
2.1 ANÁLISIS DE LA INFRAESTRUCTURA DE RED	14
2.2 TOPOLOGÍA DE LA RED ACTUAL	15
2.3 ANCHO DE BANDA UTILIZADO	17
2.4 ANÁLISIS DE TRÁFICO DE LA RED	22
2.5 IDENTIFICACIÓN Y CLASIFICACIÓN DE SERVICIOS CRÍTICOS	27
3 MARCO TEÓRICO	28
3.1 MODELO JERÁRQUICO DE TRES CAPAS	28
3.2 SEGMENTACIÓN DE REDES DE DATOS	32
3.3 MODELOS DE CALIDAD DE SERVICIO	40
3.4 EMULADORES GRÁFICOS DE RED	49
3.5 CHR - CLOUD HOSTED ROUTER	51
4 DISEÑO Y EMULACIÓN	53
4.1 DESCRIPCIÓN DEL DISEÑO	53
4.2 EMULACIÓN DEL DISEÑO	59
4.3 PRUEBAS DEL SISTEMA	69
5 CONCLUSIONES Y RECOMENDACIONES	81
5.1 CONCLUSIONES	81
5.2 RECOMENDACIONES	83
6 BIBLIOGRAFÍA	85
7 ANEXOS	87

Índice de Figuras

Fig 1.- Pantalla de inicio de Mikareno.....	13
Fig 2.- APP Mikareno.....	13
Fig 3.- Topología física de la red	16
Fig 4.- Bandwidth-test.....	17
Fig 5.- Speed-test.....	18
Fig 6.- Bandwidth test – Download	18
Fig 7.- Bandwidth test – Upload	18
Fig 8.- Prueba de velocidad 1, desde la red local.....	19
Fig 9.- Prueba de velocidad 2, desde la red local.....	19
Fig 10.- Prueba de velocidad 3, desde la red local.....	20
Fig 11.- Prueba de velocidad 4, desde la red local.....	20
Fig 12.- Gráfica de consumo semanal.....	21
Fig 13.- Gráfica de consumo diario.....	21
Fig 14.- Análisis de tráfico 1 – Wireshark.....	22
Fig 15.- Análisis de tráfico 2 – Wireshark.....	23
Fig 16.- Porcentaje de uso de protocolos con la herramienta PRTG	23
Fig 17.-Uso de puerto y protocolo con la herramienta PRTG	24
Fig 18.- Tráfico por Servicio 1	25
Fig 19.- Tráfico por servicio 2.....	26
Fig 20.- Modelo jerárquico de tres capas	29
Fig 21.- Capa de acceso	30
Fig 22.- Modelo de dos capas	32
Fig 23.- Segmentación por propósito	33
Fig 24.- Rendimiento	34
Fig 25.- Seguridad	35
Fig 26.- Direccionamiento en una red IPv4.....	37
Fig 27.- 802.11Q	40
Fig 28.- Priorización con QoS.....	41
Fig 29.- Mark Connection	44
Fig 30.- Mark Packet	44
Fig 31.- CIR y MIR.....	45
Fig 32.- PCQ rate=128000.....	48
Fig 33.- PCQ rate=0.....	48
Fig 34.- Objetivo de un simulador	50
Fig 35.- Propuesta de la topología física	56
Fig 36.- Emulación de la red de datos de la UES.....	60
Fig 37.- Creación de VLANs.....	61
Fig 38.- VLANs por interface en Winbox.....	61
Fig 39.- Asignación de direccionamiento IP 1.....	62
Fig 40.- Asignación de direccionamiento IP 2.....	62
Fig 41.- Direccionamiento IP en WinBox	62
Fig 42.- DHCP Server VLAN Profesores	63
Fig 43.- Creación de VLAN RB Profesores	63

Fig 44.- Creación Bridge RB Profesores	64
Fig 45.- Configuración IP de las VPCS.....	64
Fig 46.- Lista de dispositivos de la subred Profesores	65
Fig 47.- Políticas de encolamiento Subred Profesores	66
Fig 48.- Simple Queue Subred Profesores	66
Fig 49.- Simple Queue Subred Profesores con Queue Type	67
Fig 50.- Lista de direcciones IP de Mikareno	68
Fig 51.- Marcado de paquetes	68
Fig 52.- Queue Tree	69
Fig 53.- Conectividad WAN	69
Fig 54.- Prueba de conectividad hacia Internet	70
Fig 55.- Conectividad LAN	70
Fig 56.- Prueba de conectividad a RouterBoard Profesores	71
Fig 57.- Prueba de conectividad a RouterBoard Laboratorio 1	71
Fig 58.- Prueba de conectividad a RouterBoard Laboratorio 2	72
Fig 59.- Prueba de conectividad a RouterBoard Administración.....	72
Fig 60.- Prueba de conectividad a RouterBoard Rectorado.....	72
Fig 61.- Prueba de conectividad a VPCS	73
Fig 62.- Prueba de conectividad a un dispositivo de la subred Profesores.....	73
Fig 63.- Prueba de conectividad a un dispositivo de la subred Laboratorio 1	74
Fig 64.- Prueba de conectividad a un dispositivo de la subred Laboratorio 2	74
Fig 65.- Prueba de conectividad a un dispositivo de la subred Administración	74
Fig 66.- Prueba de conectividad a un dispositivo de la subred Rectorado	75
Fig 67.- Pruebas de conectividad desde un dispositivo de la red Profesores.....	75
Fig 68.- Prueba de acceso a Internet	76
Fig 69.- Lista de acceso Mikareno.....	76
Fig 70.- Prueba de acceso a Mikareno.....	77
Fig 71.- Marcado de paquetes para Mikareno	77
Fig 72.- Calidad de Servicio para Mikareno	78
Fig 73.- Simple Queue de subredes	78
Fig 74.- Saturación Simple Queue Profesores	79
Fig 75.- Torch sobre vlan-10 Profesores	79
Fig 76. Monitor de servicios 1.....	80
Fig 77. Monitor de servicios 2.....	80

Índice de Tablas

Tabla 1.- Listado de equipos.....	16
Tabla 2.- Niveles de criticidad.....	27
Tabla 3.- Especificaciones técnicas RB4011iGS+5HacQ2HnD-IN	54
Tabla 4.- Especificaciones técnicas hAP ac	55
Tabla 5.- Vlan por departamento	57
Tabla 6.- Segmentación de red	58

1 INTRODUCCIÓN

1.1 Introducción

Las instituciones educativas enfocadas al cumplimiento de la normativa para los procesos de regulación y gestión académica en las instituciones educativas (MINISTERIO DE EDUCACION DEL ECUADOR, 2016), están obligadas a implementar redes de datos cableadas e inalámbricas con altas prestaciones que garantice el acceso eficiente a servicios y aplicaciones y con ello mantener una adecuada calidad educativa.

Punto muy importante a resaltar es la innovación de las instituciones educativas que se encaminan a automatizar sus procesos educativos mediante el acceso a plataformas de gestión educativa alojadas en la nube. Es el caso particular de la Unidad Educativa “Suizo” que su objetivo primordial con el uso de este modelo de servicio SaaS, es mejorar la interacción entre los diferentes miembros de la institución, entre ellos, personal administrativo, profesores, estudiantes y padres de familia.

El presente estudio se divide en las siguientes secciones:

Inicia con el análisis de la infraestructura actual de la red de la Unidad Educativa Suizo, con el propósito de examinar su topología y elaborar un inventario de los equipos de la red de datos.

A continuación, se ejecuta un analizador de tráfico dentro de la red en periodos de alto consumo de los recursos de la infraestructura, con el objetivo de clasificar a los servicios que circulan por la red en críticos y no críticos. Adicionalmente, se realizan pruebas de velocidad para medir la capacidad contratada al proveedor en diferentes horarios.

La siguiente sección, contiene el esquema de la segmentación de la red en relación con los departamentos de la institución para optimizarla y asegurar su correcto funcionamiento.

Se continúa con el diseño de un modelo de calidad de servicio con el objetivo de priorizar el acceso a servicios prioritarios de la red de datos, de este modo, evitar la saturación de la red y asegurar la transmisión de datos de forma ágil y eficiente.

Finalmente, se realiza la emulación de la red de datos en una herramienta informática para ejecutar las pruebas de concepto y verificar el cumplimiento de los parámetros definidos en el análisis y diseño de la nueva red de la Unidad Educativa.

1.2 Justificación

Para la administración de la Unidad Educativa “Suizo”, es de mucha importancia contar con una red de datos con características técnicas que soporte y permita priorizar el acceso a servicios críticos para la gestión de plataformas web que manejan los docentes y personal administrativo, para lo cual la red inalámbrica debe ofrecer cobertura en los sitios donde los docentes ejercen su trabajo: salas de docentes y salas de atención a padres de familia, de este modo la institución logra mantener la información actualizada sobre el proceso académico de los estudiantes, monitoreo de evaluaciones por los padres de familia y control de la gestión diaria de contenidos de los profesores por parte del personal administrativo.

El desempeño eficiente de una red de datos se basa en el modelo de análisis y diseño realizado antes de la implementación, es así que, las redes que carecen de las propiedades antes mencionadas no mantienen un funcionamiento adecuado en el tiempo, bien sea a

causa de desconocimiento de un análisis crítico o por el nulo uso de herramientas tecnológicas para un afectivo diseño de una red de altas prestaciones.

Por tal razón, para el desarrollo de la presente investigación es primordial realizar un análisis técnico de toda la infraestructura de red de la institución, enfocado en su topología y modelos de equipos de comunicación que se usan en la red, así como un análisis del tráfico que circula por la red para determinar el tipo de protocolos y ancho de banda que usan los servicios a los que acceden los usuarios de la red.

Para aplicar políticas de manejo de tráfico y administración de ancho de banda, se diseña una segmentación de red con subredes por cada departamento, de este modo, se optimiza el desempeño de la red y se da un trato diferente a cada grupo de usuarios, lo que facilita por ejemplo, manejar el control de dispositivos, asignación de ancho de banda por usuarios y servicios así como la compartición equitativa de la capacidad disponible, gracias al diseño de un modelo de calidad de servicio acorde a los requerimientos de la institución.

1.3 Antecedentes

El modelo de educación de años atrás permitía que los docentes manejen la gestión de sus actividades mediante el uso de documentos o manejo de libretas donde se registraba la asistencia, evaluaciones, desempeño escolar de cada alumno, entre otras. Es así que aparecieron diferentes inconvenientes a falta de una herramienta tecnológica, como ausencia de reportes en tiempo real del aprovechamiento y asistencia de cada estudiante, inadecuado control de las actividades diarias de cada docente, y, por otro lado, los padres

de familia no podían ejecutar un seguimiento y monitoreo apropiado del desempeño académico de sus hijos.

En la actualidad existen varias plataformas digitales de gestión académica que permiten automatizar los procesos académicos con el fin de mantener una comunicación integral entre los actores del establecimiento educativo. Dichas plataformas, al estar alojadas en la nube, demanda que la Unidad Educativa “Suizo” cuente con una red de datos de altas prestaciones, con administración del flujo de datos y administración del ancho de banda contratado para evitar saturaciones en la red.

La Unidad Educativa “Suizo” cuenta con una infraestructura de red plana, sin ningún modelo de la calidad de servicio y sin una división de segmentos de red, lo que dificulta la ejecución de políticas de acceso y manejo del ancho de banda contratado a su proveedor, desembocando en saturaciones de la red, de manera que los docentes no logran mantener la información actualizada de sus alumnos como de sus actividades diarias.

De los antecedentes mencionados, es primordial realizar un análisis técnico profesional del modelo actual físico y lógico de la red, de su tráfico, recursos y servicios para presentar una propuesta de diseño de optimización con el objetivo de que la institución cuente con una red adecuada al requerimiento del manejo de la plataforma digital de gestión académica.

1.4 Objetivos

Objetivo General:

Diseñar y emular una red de datos con priorización de servicios en la Unidad Educativa Suizo.

Objetivos Específicos:

1. Examinar la situación actual de la infraestructura de la red de datos con la que cuenta la institución para determinar su topología.
2. Identificar el tráfico de datos que circula por la red mediante una herramienta de análisis para clasificarlo en crítico, medio y no crítico.
3. Plantear la segmentación de red en función de los departamentos de la institución para optimizar su rendimiento a nivel lógico.
4. Diseñar una política de QoS mediante la priorización de servicios para asegurar el acceso a aplicaciones críticas como plataforma de gestión educativa y minimizar las congestiones en la red.
5. Emular la topología de red en un software de buenas prestaciones y así comprobar la conectividad entre los dispositivos de la red.

2 SITUACIÓN ACTUAL Y ESTUDIO PRELIMINAR

La Unidad Educativa Suizo es una institución de carácter particular, ubicada en la Zona Sur del cantón Ambato, que por 15 años viene brindando servicios educativos a la comunidad en los niveles de Educación Inicial, Preparatoria, Básica Elemental, Básica Media, Básica Superior y Bachillerato.

La entidad educativa al encontrarse posicionada dentro de los mejores centros educativos de la ciudad de Ambato y con una visión innovadora, la gerencia, al margen de cumplir con el marco regulatorio, el 15 de agosto 2019, firmó un contrato de licencia para el uso del sistema de gestión educativa “Mikareno” (Mikareno, 2019) con el propósito de automatizar sus procesos educativos entre personal administrativo, docentes, padres de familia y estudiantes mediante una herramienta informática que se encargue de la gestión de la información académica y financiera de acuerdo a las normas y requerimientos del Ministerio de Educación del Ecuador.

La solución integral de gestión educativa Mikareno, es una solución que se encuentra alojada en la nube y que es accesible por medio de la URL <https://ues.mikareno.com/login.action> desde un navegador o mediante la App disponible en App Store y Google Play, como se puede observar en la Figura 1 y Figura 2.

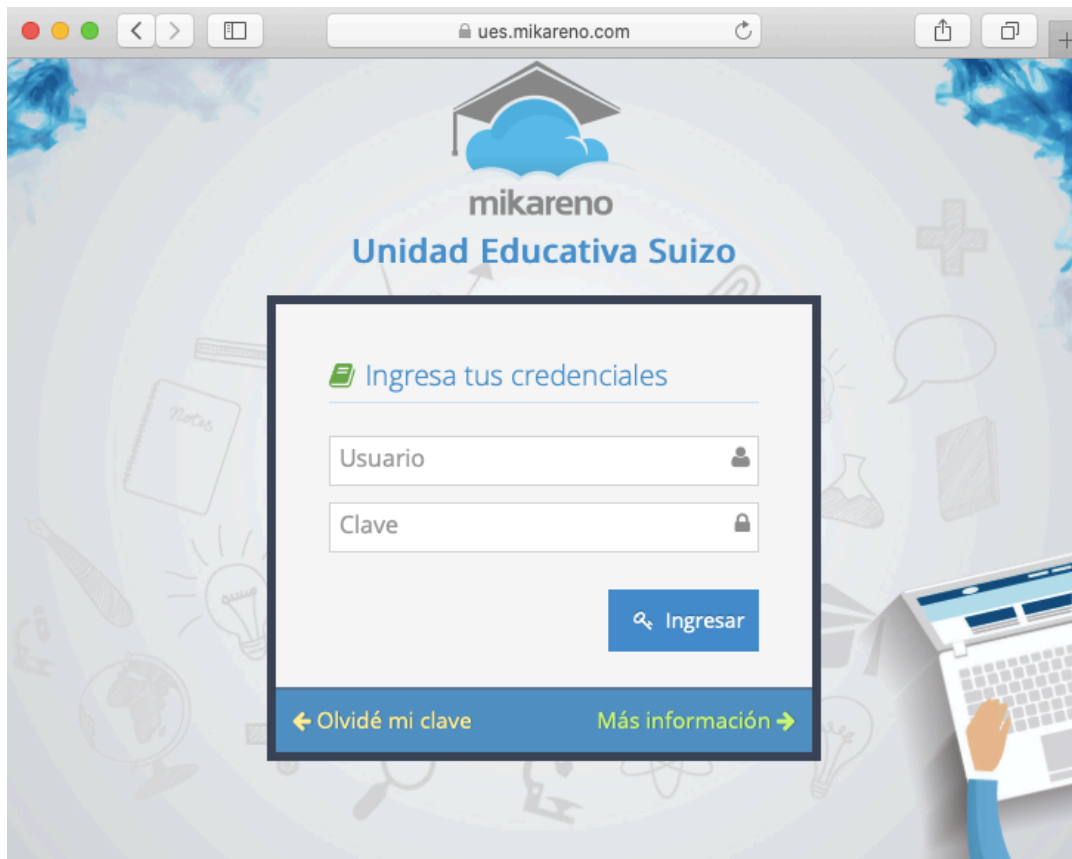


Fig 1.- Pantalla de inicio de Mikareno
Fuente: Propia

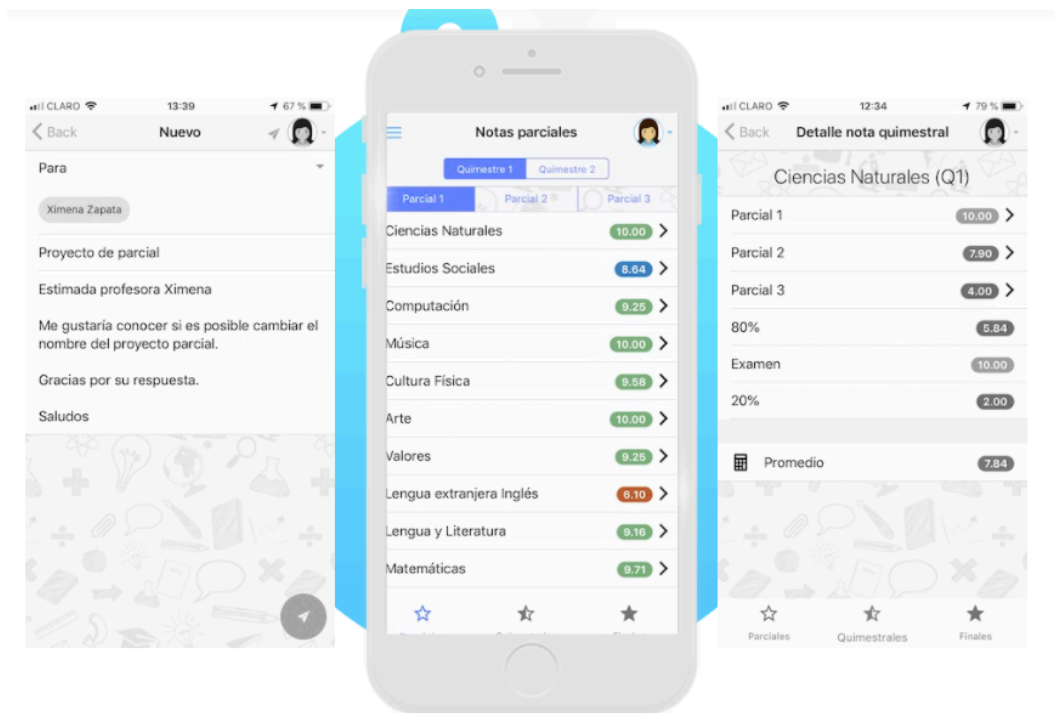


Fig 2.- APP Mikareno
Fuente: <https://mikareno.com/screenshots>

2.1 Análisis de la infraestructura de red

La UES¹ está conformada por las siguientes áreas: la Administrativa que se encuentra dividida en dos bloques, en el primero se encuentran las oficinas de Secretaría General, Colecturía, Gerencia Administrativa, Gerencia Financiera y Sala de atención a padres; en el segundo están las dependencias de Rectorado, Vicerrectorado, Inspección y el Auditorio General.

La institución, además, cuenta con dos áreas de aulas, en la primera se encuentran las instalaciones de educación básica, media y el laboratorio de inglés, el mismo que cuenta con 30 computadoras, conectadas mediante un switch de capa 2. En la segunda las aulas de básica superior y bachillerato, sala de música, sala de profesores, psicología, biblioteca y el laboratorio de computación. En este laboratorio, aparte de contar con 30 máquinas y un switch no administrable, es el lugar donde se encuentra instalado el rack de comunicaciones que es el punto de interconexión entre la fibra óptica del proveedor CNT EP y el Router de Core del establecimiento. Y, por último, un área donde se ubican las aulas de cultura física, arte, a más de la zona recreativa, canchas múltiples, piscina y comedor estudiantil.

La red inalámbrica de la institución está conformada por seis puntos de acceso inalámbricos distribuidos en puntos estratégicos para brindar cobertura a las zonas donde los docentes necesitan mantener conectividad inalámbrica en sus dispositivos móviles, como son, computadores portátiles, teléfonos inteligentes y tabletas.

Es importante indicar que todos los dispositivos de las áreas mencionadas se encuentran conectadas a una red local plana y con acceso a Internet, mediante un medio físico o

¹ Unidad Educativa Suizo

inalámbrico, en total aproximadamente 100 dispositivos. Sin embargo, la red de la UES presenta los siguientes problemas:

- La infraestructura de red no cuenta con un diseño adecuado que asegure la disponibilidad de la red.
- Lentitud en el acceso a ciertas páginas de Internet.
- Saturación a servicios en horas de alta congestión
- La interacción con la plataforma académica Mikareno no es la adecuada, ya que en ciertas ocasiones no se concluyen los procesos por lentitud.
- Toda la red maneja un mismo direccionamiento IP.
- No existe un sistema de priorización de servicios.
- Las aulas de la institución no cuentan con un punto físico de red.
- La institución no cuenta con un dominio de correo electrónico institucional para la comunicación, por lo que actualmente manejan una cuenta de correos comerciales.
- Falta de un responsable en la administración y gestión de la red física y lógica

Por lo expuesto anteriormente, es importante realizar un diseño de red adecuado para solventar esta problemática, con políticas estructuradas donde el principal objetivo sea el generar un sistema de calidad de servicio para asegurar la disponibilidad de la red de la Unidad Educativa Suizo.

2.2 Topología de la red actual

Es de mucha importancia iniciar con un listado de los equipos de comunicación que intervienen en la red de datos de la UES, a más de la marca y modelo, se incluye la

funcionalidad lo que permite tener una perspectiva de su intervención en la transmisión de datos.

Tabla 1.- Listado de equipos

CANTIDAD	MARCA	MODELO	FUNCIONALIDAD
1	Mikrotik	2011UiAS-2HnD	Router de Core
4	Mikrotik	RBwAP2nDr2	Zona Wi-Fi
2	TPLink	TL-WR740N	Zona Wi-Fi
2	D-Link	DGS-1016D	Red laboratorio 1
1	D-Link	DGS-1016D	Red laboratorio 2

Fuente: Propia

Tal como se observa en la Figura 3, el RouterBoard Mikrotik RB2011UiAS-2HnD es el equipo de Core, el mismo que realiza funciones de administración y gestión de toda la red de la institución, que se encuentra distribuida con un direccionamiento lógico único, lo que deriva a una conclusión que la topología de red que se maneja es plana.

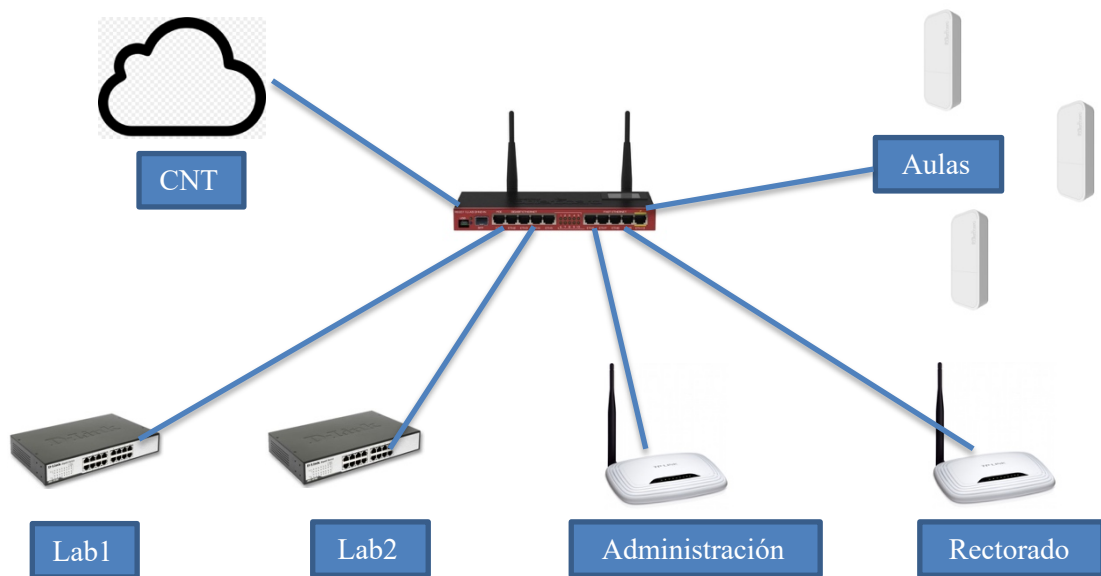


Fig 3.- Topología física de la red
Fuente: Propia

2.3 Ancho de banda utilizado

Una vez que se cuenta con el diagrama de la topología de la red en estudio, se han ejecutado pruebas de medición de la velocidad del enlace del proveedor CNT EP con el objetivo de determinar su capacidad y desempeño.

Para las mediciones se han utilizado las herramientas bandwidth-test (Mikrotik, 2018) y speed-test (Mikrotik, 2019) incluidas en el sistema operativo RouterOS del router de Core de la UES, es así que mediante los resultados de las pruebas de velocidad y tal como se muestran en las Figuras 4, 5, 6 y 7, se comprueba que la capacidad que entrega el proveedor de Internet en download es de 35Mbps y en upload de 15Mbps.

Cabe indicar que las pruebas realizadas no dependen de la red interna ni de los dispositivos de red, ya que se las realizan directamente desde el Router de Core de la institución hacia otro Router Mikrotik con una dirección IP pública disponible en Internet.

```
[admin@CORE U. E. SUIZO] > /tool bandwidth-test user= password=
direction=both
      status: running
      duration: 1m
      tx-current: 14.7Mbps
tx-10-second-average: 14.7Mbps
      tx-total-average: 14.1Mbps
      rx-current: 34.5Mbps
rx-10-second-average: 34.5Mbps
      rx-total-average: 27.0Mbps
      lost-packets: 0
      random-data: no
      direction: both
      tx-size: 1500
      rx-size: 1500
connection-count: 20
      local-cpu-load: 19%
      remote-cpu-load: 7%
```

Fig 4.- Bandwidth-test
Fuente: Propia

```

[admin@CORE U. E. SUIZO] > /tool speed-test          user=          password=
                status: done
                time-remaining: 0s
                ping-min-avg-max: 210ms / 210ms / 211ms
                jitter-min-avg-max: 15us / 348us / 924us
                loss: 72.5% (145/200)
                udp-download: 816Kbps local-cpu-load:3% remote-cpu-load:0%
                udp-upload: 15.8Mbps local-cpu-load:11% remote-cpu-load:1%

```

Fig 5.- Speed-test
Fuente: Propia

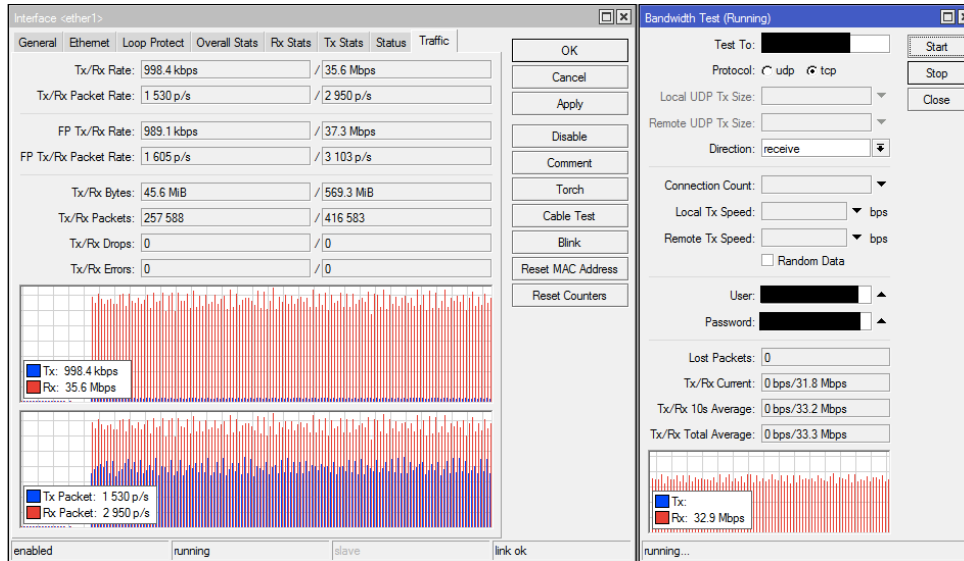


Fig 6.- Bandwidth test – Download
Fuente: Propia

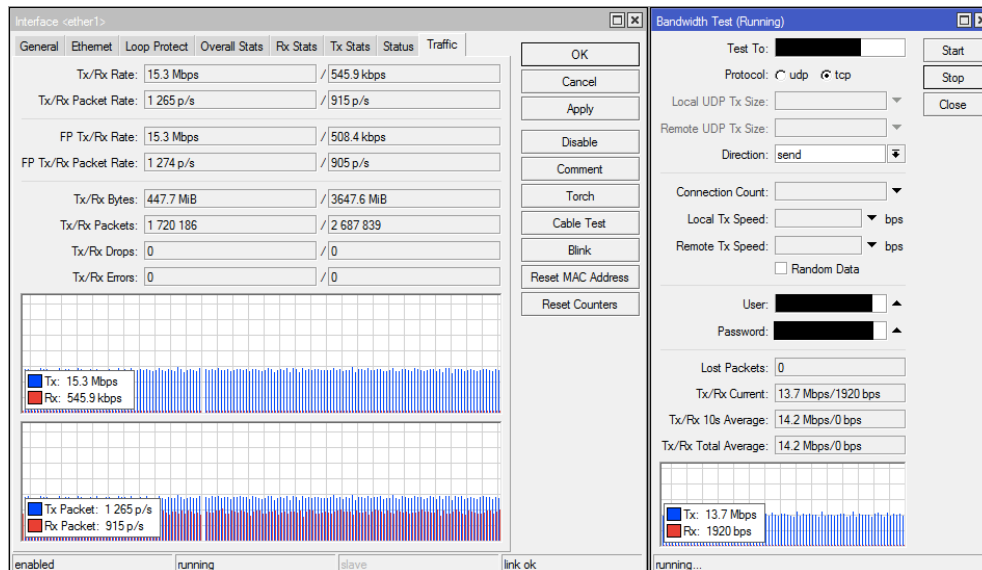


Fig 7.- Bandwidth test – Upload
Fuente: Propia

Posterior a las pruebas realizadas desde el Router de Core, se procede a realizar diferentes pruebas de velocidad desde la página www.speedtest.net hacia diferentes servidores, desde un computador conectado a la red interna de la UES, en el horario de mayor consumo de los recursos y saturación en la red.

Con los resultados obtenidos e ilustrados en las Figuras 8 a la Figura 11, podemos concluir que el dispositivo del cual se hicieron las pruebas no supera los 3Mbps de download y los 3Mbps de upload y en otras ocasiones la diferencia de los valores máximos y mínimos son considerables.

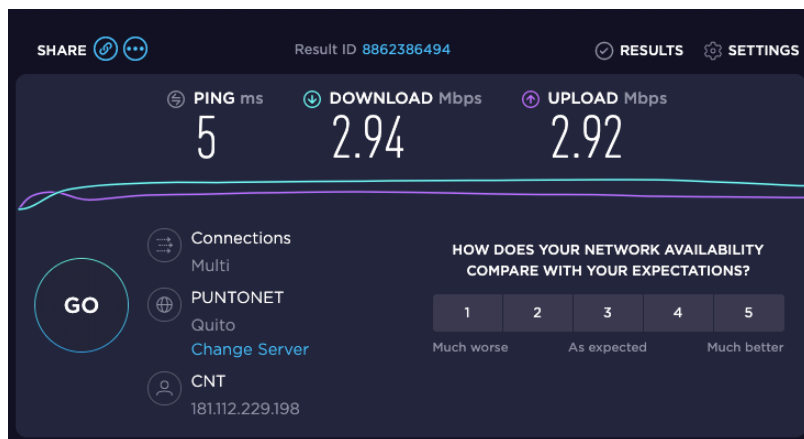


Fig 8.- Prueba de velocidad 1, desde la red local
Fuente: Propia

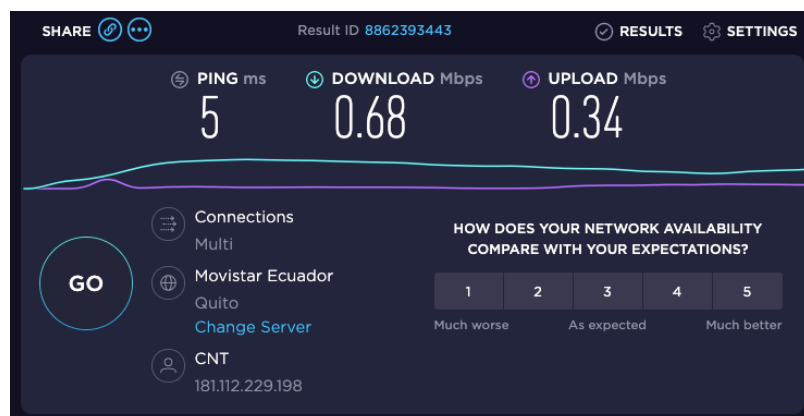


Fig 9.- Prueba de velocidad 2, desde la red local
Fuente: Propia

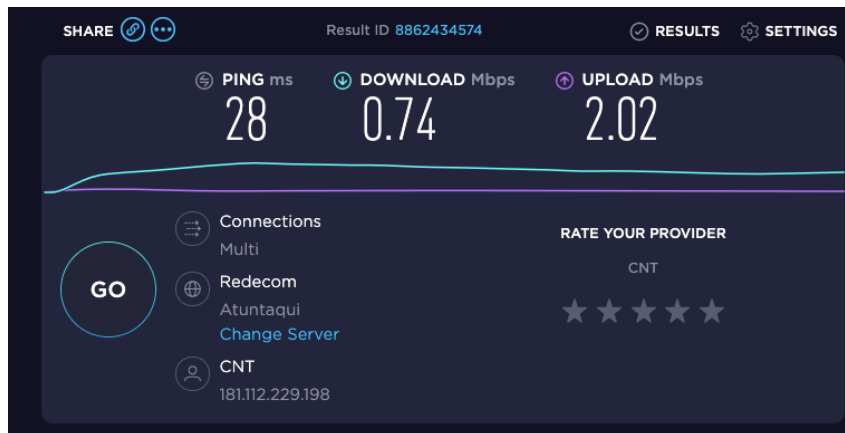


Fig 10.- Prueba de velocidad 3, desde la red local
Fuente: Propia

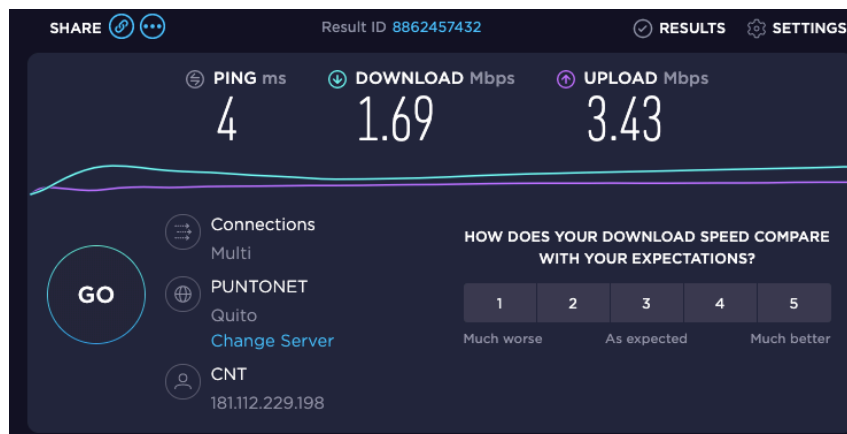


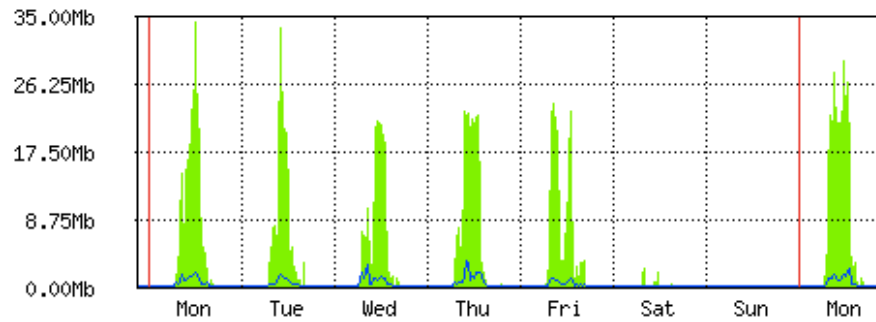
Fig 11.- Prueba de velocidad 4, desde la red local
Fuente: Propia

A más de las herramientas descritas anteriormente, debemos destacar que el sistema operativo RouterOS posee un sistema integrado MRTG para el archivo de gráficas de consumo por interfaz. A continuación, se muestran las imágenes de las gráficas de consumo de la interfaz ether1 del Router Core, la misma que se conecta con el router del proveedor del Internet CNT EP.

Las Figuras 12 y 13 permiten observar el tráfico máximo, promedio y actual del consumo de entrada y salida sobre la interfaz ether1 del Router de Core. Estos resultados permiten concluir que los dispositivos de la red interna llegan a consumir toda la capacidad de download contratada con el proveedor, pudiendo generar saturación en la red por la

heterogénea distribución de los recursos de ancho de banda a todos los dispositivos de red.

"Weekly" Graph (30 Minute Average)



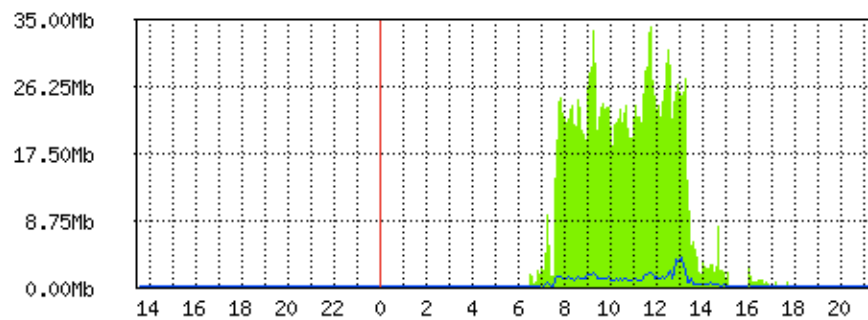
Max In: 34.61Mb; Average In: 3.52Mb; Current In: 237.33Kb;
Max Out: 3.41Mb; Average Out: 230.08Kb; Current Out: 9.37Kb;

Fig 12.- Gráfica de consumo semanal
Fuente: Propia

Interface <ether1> Statistics

• Last update: Mon Dec 16 21:27:11 2019

"Daily" Graph (5 Minute Average)



Max In: 34.11Mb; Average In: 4.66Mb; Current In: 48.14Kb;
Max Out: 3.84Mb; Average Out: 259.48Kb; Current Out: 7.21Kb;

Fig 13.- Gráfica de consumo diario
Fuente: Propia

2.4 Análisis de tráfico de la red

Para el análisis de tráfico que circula por la red de datos de la UES, se utiliza la herramienta Wireshark, con el propósito de clasificar el tráfico que luego será de vital importancia para el diseño de la calidad de servicio con una priorización adecuada.

Las muestras tomadas pertenecen a un horario de mayor concurrencia de dispositivos en la red, para que la toma de información sea proporcional. A continuación, las Figuras 14 y 15, permiten observar parte de los componentes del tráfico, como son origen, destino, protocolo, entre otros.

No.	Time	Source	Destination	Protocol	Length	Info
531.	79.937677	181.37.56.177	172.16.1.107	UDP	1455	58485 → 53552 Len=1413
531.	79.937971	172.16.1.107	181.37.56.177	UDP	62	53552 → 58485 Len=20
531.	79.938063	181.37.56.177	172.16.1.107	UDP	1455	58485 → 53552 Len=1413
531.	79.938179	172.16.1.107	181.37.56.177	UDP	62	53552 → 58485 Len=20
531.	79.942843	190.205.163.23	172.16.1.107	TCP	1514	34984 → 50747 [ACK] Seq=3869069 Ack=4383 Win=4096 Len=1448 TSval=651192898 TSecr=793350527
531.	79.942850	181.37.56.177	172.16.1.107	UDP	1455	58485 → 53552 Len=1413
531.	79.943090	172.16.1.107	181.37.56.177	UDP	62	53552 → 58485 Len=20
531.	79.947821	79.98.219.224	172.16.1.107	BitTo...	1506	Bitfield(Malformed Packet)
531.	79.947827	189.140.79.20	172.16.1.107	TCP	1466	43611 → 50743 [ACK] Seq=3484601 Ack=3862 Win=4096 Len=1400 TSval=368757128 TSecr=793350670
531.	79.948021	172.16.1.107	189.140.79.20	TCP	66	50743 → 43611 [ACK] Seq=3879 Ack=3406201 Win=2048 Len=0 TSval=793350867 TSecr=368757128
531.	79.951417	181.37.56.177	172.16.1.107	UDP	1455	58485 → 53552 Len=1413
531.	79.951423	201.218.117.209	172.16.1.107	TCP	1514	[TCP Retransmission] 6881 → 50785 [ACK] Seq=3456377 Ack=3941 Win=2048 Len=1448 TSval=416475224 TSecr=793350691
531.	79.951588	172.16.1.107	201.218.117.209	TCP	86	50785 → 6881 [ACK] Seq=3941 Ack=3457825 Win=2025 Len=0 TSval=793350870 TSecr=416475224 SLE=3465065 SRE=416475224
531.	79.951821	172.16.1.107	181.37.56.177	UDP	62	53552 → 58485 Len=20
531.	79.951999	201.218.117.209	172.16.1.107	TCP	1514	[TCP Retransmission] 6881 → 50785 [ACK] Seq=3457825 Ack=3941 Win=2048 Len=1448 TSval=416475224 TSecr=793350691
531.	79.952070	172.16.1.107	201.218.117.209	TCP	78	50785 → 6881 [ACK] Seq=3941 Ack=3462169 Win=1980 Len=0 TSval=793350870 TSecr=416475224 SLE=3465065 SRE=416475224
531.	79.952107	172.16.1.107	201.218.117.209	TCP	78	[TCP Window Update] 50785 → 6881 [ACK] Seq=3941 Ack=3462169 Win=2048 Len=0 TSval=793350870 TSecr=416475224
532.	79.960475	190.205.163.23	172.16.1.107	TCP	1514	34984 → 50747 [ACK] Seq=3870517 Ack=4383 Win=4096 Len=1448 TSval=651192936 TSecr=793350562
532.	79.960590	172.16.1.107	190.205.163.23	TCP	66	50747 → 34984 [ACK] Seq=4417 Ack=3071965 Win=2025 Len=0 TSval=793350879 TSecr=651192890
532.	79.962769	189.140.79.20	172.16.1.107	TCP	1466	43611 → 50743 [ACK] Seq=3486201 Ack=3862 Win=4096 Len=1400 TSval=368757147 TSecr=793350688
532.	79.969748	88.10.138.60	172.16.1.107	TCP	1514	6881 → 50819 [ACK] Seq=2482282 Ack=3180 Win=1066 Len=1448 TSval=78733882 TSecr=793350691 [TCP segment . . .
532.	79.970849	88.10.138.60	172.16.1.107	TCP	1514	6881 → 50819 [ACK] Seq=2483730 Ack=3180 Win=1066 Len=1448 TSval=78733882 TSecr=793350691 [TCP segment . . .
532.	79.970968	172.16.1.107	88.10.138.60	TCP	66	50819 → 6881 [ACK] Seq=3197 Ack=2485178 Win=2025 Len=0 TSval=793350888 TSecr=78733882
532.	79.973291	88.10.138.60	172.16.1.107	TCP	1514	6881 → 50819 [ACK] Seq=2485178 Ack=3180 Win=1066 Len=1448 TSval=78733882 TSecr=793350691 [TCP segment . . .
532.	79.973445	172.16.1.107	88.10.138.60	TCP	66	50819 → 6881 [ACK] Seq=3197 Ack=2486626 Win=2048 Len=0 TSval=793350890 TSecr=78733882
532.	79.975965	190.205.163.23	172.16.1.107	TCP	1514	34984 → 50747 [ACK] Seq=3871965 Ack=4383 Win=4096 Len=1448 TSval=651192936 TSecr=793350562
532.	79.976131	172.16.1.107	190.205.163.23	TCP	66	50747 → 34984 [ACK] Seq=4417 Ack=3873413 Win=2048 Len=0 TSval=793350892 TSecr=651192936

▶ Frame 1: 1466 bytes on wire (11728 bits), 1466 bytes captured (11728 bits) on interface 0
 ▶ Ethernet II, Src: Routerbo_71:93:f8 (64:d1:54:71:93:f8), Dst: Apple_08:00:18 (08:00:08:00:18:00)
 ▶ Internet Protocol Version 4, Src: 189.140.79.20, Dst: 172.16.1.107
 ▶ Transmission Control Protocol, Src Port: 43611, Dst Port: 50743, Seq: 1, Ack: 1, Len: 1400
 ▶ Data (1400 bytes)

```

0000  f0 79 60 08 db 18 64 d1 54 71 93 f8 08 00 45 00  .y...d.Tq...E.
0010  05 ac 00 00 40 00 33 06 88 30 bd 8c 4f 14 ac 10  .@3...0.0...
0020  01 6b aa 5b c6 37 a5 00 04 6d 82 fc b0 49 80 10  .k[?..m..I...
0030  0f ff 42 a4 00 01 01 08 0a 15 f9 99 0e 2f 48    .B...../H
0040  6f 0d 38 50 2b 11 15 4e 4d 37 72 14 36 5d 12 d7  o8P+...N M7r.6]..
0050  db 34 9c ec c9 62 cc 2a 98 10 b2 0e bf cb a6 06  .4...b*.....
0060  1f 7e 57 f0 d4 03 11 b6 23 3f 9e 4f 57 80 82 05  .~.....#?Ow...
0070  b7 1f 2e 28 da 5d 4c 54 b8 47 22 6e 18 3f 95 24  .(.!LT.G"n.?.$
0080  a2 86 4c 84 3b 55 77 8c 79 91 54 f0 25 3f 83 82  .L;Uw:y.T.%?..
0090  ba 4f 0f fa ed 73 19 6b 70 df a2 fe 07 19 76 e2  .0...s;k p...v.
00a0  67 91 81 27 7e 4e e1 68 36 bf 90 5f 44 cf 11 56  g...N'h..._D..V
00b0  47 9c 6c 85 a3 f5 f4 88 61 b5 a9 96 30 23 d7 c3  G.L...a...0#...
  
```

Fig 14.- Análisis de tráfico 1 – Wireshark
Fuente: Propia

No.	Time	Source	Destination	Protocol	Length	Info
412.	555.575544	186.136.55.41	172.16.1.107	TCP	566	26085 → 49779 [ACK] Seq=1619654 Ack=5547 Win=4096 Len=500 TSval=1039766171 TSecr=793796954
412.	555.575613	172.16.1.107	186.136.55.41	TCP	66	49779 → 26085 [ACK] Seq=5547 Ack=1620154 Win=2040 Len=0 TSval=793797256 TSecr=1039766171
412.	555.576627	186.136.55.41	172.16.1.107	TCP	526	26085 → 49779 [PSH, ACK] Seq=1620154 Ack=5547 Win=4096 Len=460 TSval=1039766171 TSecr=793796954
412.	555.576680	172.16.1.107	186.136.55.41	TCP	66	49779 → 26085 [ACK] Seq=5547 Ack=1620614 Win=2040 Len=0 TSval=793797257 TSecr=1039766171
412.	555.578126	90.162.156.58	172.16.1.107	UDP	1514	6881 → 53552 Len=1472
412.	555.578325	172.16.1.107	90.162.156.58	UDP	65	53552 → 6881 Len=23
412.	555.580318	186.42.100.98	172.16.1.107	TCP	78	[TCP Out-Of-Order] 443 → 51715 [ACK] Seq=8479697 Ack=50177 Win=1049600 Len=12 TSval=525970525 TSecr=793797260
412.	555.580743	172.16.1.107	186.42.100.98	TCP	86	51715 → 443 [ACK] Seq=50177 Ack=8479697 Win=131008 Len=0 TSval=793797260 TSecr=525970525 SLE=8481157 S.
412.	555.581138	186.42.100.98	172.16.1.107	TCP	1514	[TCP Out-Of-Order] 443 → 51715 [ACK] Seq=8479697 Ack=50177 Win=1049600 Len=1448 TSval=525970526 TSecr=793797260
412.	555.581287	172.16.1.107	186.42.100.98	TCP	86	51715 → 443 [ACK] Seq=50177 Ack=8481145 Win=129600 Len=0 TSval=793797260 TSecr=525970526 SLE=8481157 S.
412.	555.583689	186.42.100.98	172.16.1.107	TCP	78	[TCP Out-Of-Order] 443 → 51715 [ACK] Seq=8481145 Ack=50177 Win=1049600 Len=12 TSval=525970527 TSecr=793797260
412.	555.583780	172.16.1.107	186.42.100.98	TCP	78	51715 → 443 [ACK] Seq=50177 Ack=8484029 Win=128128 Len=0 TSval=793797263 TSecr=525970527 SLE=8485477 S.
412.	555.584204	186.133.157.210	172.16.1.107	UDP	1471	28444 → 53552 Len=1429
412.	555.584476	172.16.1.107	186.133.157.210	UDP	62	53552 → 28444 Len=20
412.	555.586476	172.16.1.107	186.42.100.98	TLSv1	1122	Application Data
412.	555.587924	186.42.100.98	172.16.1.107	TLSv1	1514	[TCP Window Update] 51710 → 443 [ACK] Seq=44796 Ack=8635666 Win=131072 Len=0 TSval=793797266 TSecr=147508189
412.	555.588013	172.16.1.107	186.42.100.98	TCP	78	[TCP Window Update] 51710 → 443 [ACK] Seq=44796 Ack=8635666 Win=131072 Len=0 TSval=793797266 TSecr=147508189
412.	555.589987	177.224.192.8	172.16.1.107	TCP	566	6881 → 59984 [ACK] Seq=3414104 Ack=7959 Win=131072 Len=500 TSval=83362468 TSecr=793796648 [TCP segment.
412.	555.591484	188.79.139.248	172.16.1.107	UDP	1514	6881 → 53552 Len=1472
412.	555.591659	172.16.1.107	188.79.139.248	UDP	65	53552 → 6881 Len=23
412.	555.594533	181.16.99.53	172.16.1.107	UDP	1514	6881 → 53552 Len=1472
412.	555.594714	172.16.1.107	181.16.99.53	UDP	65	53552 → 6881 Len=23
412.	555.595421	172.16.1.107	201.218.117.209	TCP	66	50785 → 6881 [ACK] Seq=11156 Ack=7070726 Win=2048 Len=0 TSval=793797272 TSecr=416945653
412.	555.597510	186.42.100.98	172.16.1.107	TLSv1	1514	Ignored Unknown Record
412.	555.597617	172.16.1.107	186.42.100.98	TCP	78	[TCP Window Update] 51715 → 443 [ACK] Seq=50177 Ack=8484029 Win=131072 Len=0 TSval=793797274 TSecr=525970527
412.	555.600462	181.16.99.53	172.16.1.107	UDP	1514	6881 → 53552 Len=1472
412.	555.600670	172.16.1.107	181.16.99.53	UDP	65	53552 → 6881 Len=23
412.	555.602948	186.42.100.98	172.16.1.107	TCP	182	[TCP Out-Of-Order] 443 → 51710 [ACK] Seq=8635666 Ack=44796 Win=1049600 Len=36 TSval=1470508189 TSecr=793797279
412.	555.602954	186.42.100.98	172.16.1.107	TLSv1	602	Application Data
412.	555.603101	172.16.1.107	186.42.100.98	TCP	78	51710 → 443 [ACK] Seq=44796 Ack=8635702 Win=131008 Len=0 TSval=793797279 TSecr=1470508189 SLE=8640010
412.	555.603136	172.16.1.107	186.42.100.98	TCP	66	51674 → 443 [ACK] Seq=58088 Ack=8687042 Win=130496 Len=0 TSval=793797279 TSecr=3059367713
412.	555.604651	188.79.139.248	172.16.1.107	UDP	1514	6881 → 53552 Len=1472
412.	555.604884	172.16.1.107	188.79.139.248	UDP	65	53552 → 6881 Len=23

Fig 15.- Análisis de tráfico 2 – Wireshark
Fuente: Propia

Posterior al uso de Wireshark, se ha utilizado la herramienta PRTG con una versión de prueba por 30 días, para determinar el porcentaje de uso de los diferentes tipos de tráficos; es así como en base a las Figuras 16, 17, 18 y 19, se puede apreciar que el porcentaje de paquetes de tráfico www es de 50%, seguido de la categoría otros con el 46%, además de IP fuente y destino, puerto, protocolo; así como el tráfico de cada servicio.

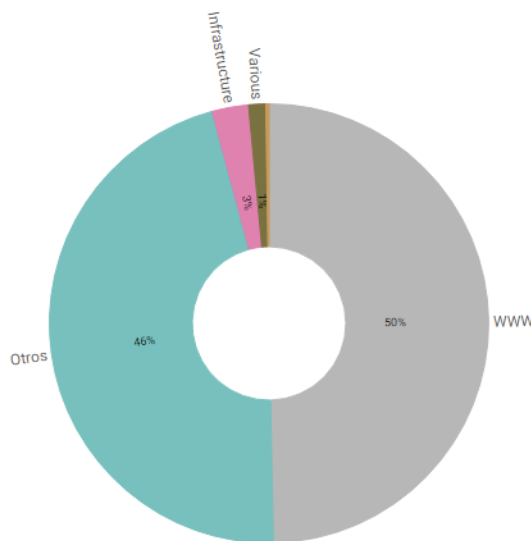


Fig 16.- Porcentaje de uso de protocolos con la herramienta PRTG
Fuente: Propia

Elementos: ▾ 50					
Pos ▾	IP fuente ▾	Puerto fuente ▾	Protocolo ▾	Bytes ▲	
Otros				521 KByte	48 %
1.	[172.217.8.142]	443	TCP	69 KByte	6 %
2.	172.217.8.68	80	TCP	48 KByte	4 %
3.	yyz08s14-in-f132.1e100.net (172.217.2.132)	80	TCP	48 KByte	4 %
4.	[216.239.34.117]	80	TCP	48 KByte	4 %
5.	[172.217.8.69]	443	TCP	48 KByte	4 %
6.	[192.168.35.1]	80	TCP	38 KByte	3 %
7.	JuanSC-PC.localdomain (10.211.55.4)	0	ICMP	28 KByte	3 %
8.	mia07s48-in-f3.1e100.net (172.217.8.99)	443	TCP	24 KByte	2 %
9.	40.241.186.35.bc.googleusercontent.com (35.1...	443	TCP	22 KByte	2 %
10.	mia09s02-in-f3.1e100.net (172.217.2.195)	443	TCP	18 KByte	2 %
11.	172.217.3.78	443	TCP	9.952 Byte	< 1 %
12.	mia09s18-in-f14.1e100.net (172.217.2.142)	443	TCP	9.573 Byte	< 1 %
13.	JuanSC-PC.localdomain (10.211.55.4)	50253	TCP	7.176 Byte	< 1 %
14.	fdb2:2c26:f4e4::198:3c07:29dd:bc1a	61915	UDP	7.086 Byte	< 1 %
15.	JuanSC-PC.localdomain (10.211.55.4)	137	UDP	6.716 Byte	< 1 %
16.	ord08s13-in-f16.1e100.net (172.217.2.80)	80	TCP	6.362 Byte	< 1 %
17.	fa90-91c-42ff-f000-101	53	UDP	6.110 Byte	< 1 %

*Fig 17.-Uso de puerto y protocolo con la herramienta PRTG
Fuente: Propia*

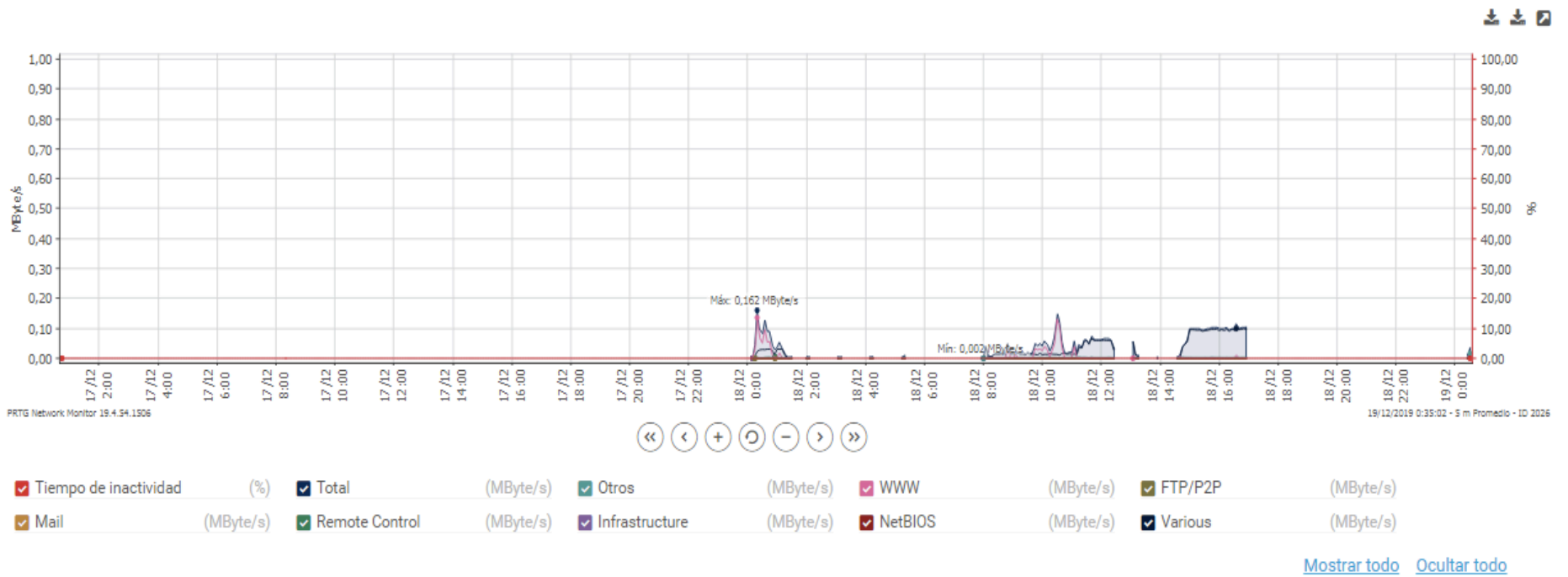
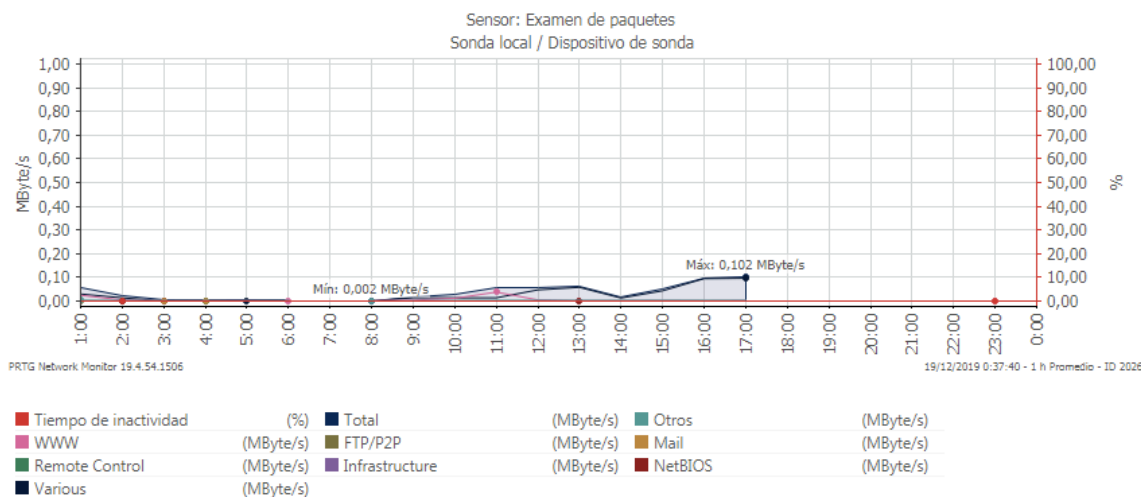


Fig 18.- Tráfico por Servicio 1
Fuente: Propia



Fecha Hora	Total (volumen)	Total (velocidad)	Otros (volumen)	Otros (velocidad)	WWW (volumen)	WWW (velocidad)	FTP/P2P (volumen)	FTP/P2P (velocidad)	Mail (volumen)	Mail (velocidad)	Remote Control (volumen)	Remote Control (velocidad)	Infrastructure (volumen)	Infrastructure (velocidad)	NetBIOS (volumen)
Sumas (de 16 valores)	1.507 MByte		71 MByte		255 MByte		0,01 MByte		0,12 MByte		< 0,01 MByte		8,70 MByte		0,25 MByte
Promedios (de 16 valores)	94 MByte	0,05 MByte/s	4,44 MByte	< 0,01 MByte/s	16 MByte	< 0,01 MByte/s	< 0,01 MByte	< 0,01 MByte/s	< 0,01 MByte	< 0,01 MByte/s	< 0,01 MByte	< 0,01 MByte/s	0,54 MByte	< 0,01 MByte/s	0,02 MByte

Fecha Hora	Total (volumen)	Total (velocidad)	Otros (volumen)	Otros (velocidad)	WWW (volumen)	WWW (velocidad)	FTP/P2P (volumen)	FTP/P2P (velocidad)	Mail (volumen)	Mail (velocidad)	Remote Control (volumen)	Remote Control (velocidad)	Infrastructure (volumen)	Infrastructure (velocidad)	NetBIOS (volumen)
18/12/2019 0:00:00 – 1:00:00	83 MByte	0,06 MByte/s	4,90 MByte	< 0,01 MByte/s	35 MByte	0,02 MByte/s	< 0,01 MByte	< 0,01 MByte/s	0,03 MByte	< 0,01 MByte/s	< 0,01 MByte	< 0,01 MByte/s	0,44 MByte	< 0,01 MByte/s	0,02 MByte
18/12/2019 1:00:00 – 2:00:00	35 MByte	0,02 MByte/s	3,68 MByte	< 0,01 MByte/s	7,73 MByte	< 0,01 MByte/s	0 MByte	0 MByte/s	0,01 MByte	< 0,01 MByte/s	< 0,01 MByte	< 0,01 MByte/s	0,54 MByte	< 0,01 MByte/s	0,03 MByte

Fig 19.- Tráfico por servicio 2
Fuente: Propia

2.5 Identificación y clasificación de servicios críticos

Finalmente, se realiza un análisis en conjunto con el personal de cada departamento de la institución, con el propósito de identificar y elaborar una clasificación de los niveles críticos de los servicios que manejan en sus actividades diarias, ilustrados en la Tabla 2. Tomando en cuenta la premisa de que lo crítico se convierte en una causa por la que sus actividades en función al uso de los recursos de Internet se verían afectadas en su totalidad, el nivel medio en el cual su desempeño no se vería afectado en su totalidad y el nivel no crítico que no interviene en el desarrollo de sus actividades y gestión en la UES.

Tabla 2.- Niveles de criticidad

DEPARTAMENTO	CRÍTICO	MEDIO	NO CRÍTICO
Administrativo	Mikareno	Correo electrónico Gmail	Navegación
Colecturía	Facturación electrónica, Bancos	Correo electrónico Gmail	Navegación
Secretaría General	Mikareno	Correo electrónico Gmail	Navegación
Laboratorios	Plataformas educativas	Navegación	Actualizaciones de software
Docentes	Mikareno	YouTube	Otros

Fuente: Propia

3 MARCO TEÓRICO

3.1 Modelo jerárquico de tres capas

Un buen diseño de una red se convierte en un requisito fundamental para que una organización se vuelva competitiva y por ende subsista en el mercado o en el medio en el que se desarrolle, en este caso, un diseño apropiado para la red de datos de la UES permitirá que los procesos académicos se automaticen en función del tiempo con un adecuado acceso a la plataforma de gestión educativa.

El diseño en capas permite implementar funciones específicas en cada una de ellas, de este modo, se simplifica el proceso de diseño de una red de datos, para su posterior implementación y finalmente en su administración.

“En arquitecturas de red mallada o **plana**, los cambios tienden a afectar a una gran cantidad de sistemas. El diseño jerárquico permite restringir los cambios operativos a un subgrupo de red, lo que facilita la administración y mejora la recuperabilidad. La estructuración modular de la red en elementos pequeños y fáciles de comprender también facilita la recuperabilidad mediante aislamiento de fallas mejorado” (Cisco System Inc, 2014)

Este modelo consta de tres capas que son y se detallan en la Figura 20.

- Capa de acceso: Switching
- Capa de distribución: Routing
- Capa de núcleo: Backbone

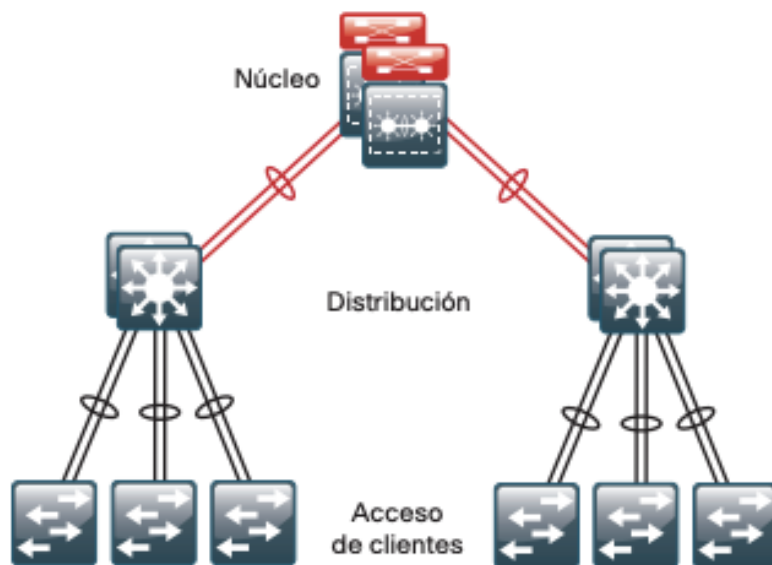


Fig 20.- Modelo jerárquico de tres capas

Fuente: Cisco System Inc 2014 - https://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/en-05_campus-wireless_wp_cte_es-xl_42333.pdf

A pesar de haber indicado que cada capa ofrece una funcionalidad diferente en la red, es importante resaltar que según la dimensión de la misma, es posible ejecutar el diseño de una red de datos con una o dos capas, esto se puede notar, en organizaciones que su infraestructura está situada en solo sitio, en ese caso se utilizarán las capas de acceso y distribución únicamente. Por el contrario, en organizaciones con infraestructuras distribuidas en varios sitios o con una sola, pero de grandes proporciones, se diseñará la red con las tres capas: acceso, distribución y núcleo.

Capa de acceso

Su principal función es ofrecer conectividad a los dispositivos finales con la red, como computadores, equipos portátiles, tablets, teléfonos inteligentes, teléfonos IP, puntos de acceso inalámbricos, medios de almacenamiento o cámaras de videovigilancia, por un medio inalámbrico o físico, como se puede observar en la Figura 21.



Fig 21.- Capa de acceso

Fuente: https://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/en-05_campus-wireless_wp_cte_es-xl_42333.pdf

Por otro lado, en esta capa también se hace referencia a la conectividad ofrecida con un ancho de banda de alta velocidad, la misma que admite administrar ráfagas en las tareas diarias de los usuarios de la red, como navegación, acceso a cuentas de correo, herramientas de gestión académica, streaming de video, etc.

Además, la capa de acceso permite administrar varias redes lógicas, por lo tanto, se justifica la segmentación de la red con el objetivo de aumentar su rendimiento, facilitar su administración y aumentar su seguridad.

Capa de distribución

Su función principal es brindar la comunicación entre las dos capas restantes, acceso y núcleo mediante un enrutamiento para llegar a su destino final. Por otro lado, agrega políticas para controlar el flujo de tráfico de la red y gestiona los dominios de broadcast de las redes LAN y VLAN definidas en la capa de acceso con el objetivo de separar el tráfico de cada subred, en nuestro caso por cada departamento existente en la UES.

Para continuar, se listan otras funciones que se implementan en esta capa:

- Enrutamiento entre redes lógicas de la red
- Políticas de seguridad y listas de acceso
- Calidad de servicio
- Gestión de broadcast y multicast

Capa Núcleo

Esta capa es el backbone de una red de alta velocidad. Su principal función es la interconectividad entre los dispositivos hacia el interior de la infraestructura, por ejemplo, los routers de la capa de distribución; por esta razón el núcleo debe estar siempre disponible y redundante. Además de la función mencionada, permite conectarse con los recursos fuera de la red de datos, como son los recursos de Internet, es decir, se encarga de transportar volúmenes de tráfico considerables en forma rápida y confiable.

Diseño de dos capas

Se lo denomina también núcleo fusionado. Bajo la condición de la dimensión de la red local, la capa de distribución puede ofrecer conectividad hacia la red WAN o servicios de perímetros de Internet en una red de mediana dimensión. En conclusión, como se muestra en la Figura 22, un dispositivo de red como un router o un switch en la capa de distribución puede convertirse en un dispositivo de capa núcleo y distribución a la vez. En este modelo la capa de acceso no sufre cambios.

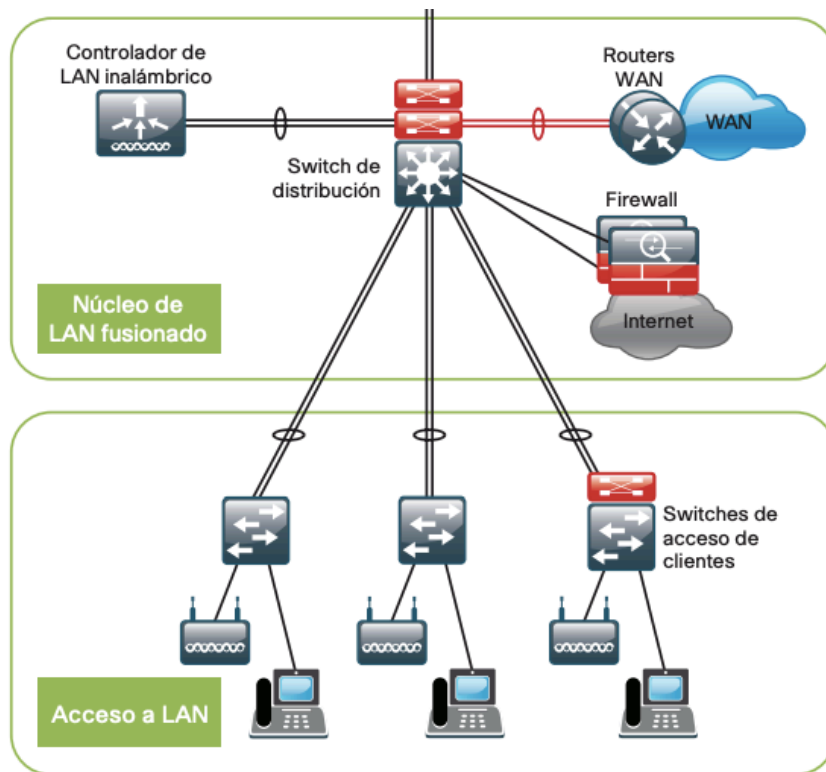


Fig 22.- Modelo de dos capas

Fuente: https://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/en-05_campus-wireless_wp_cte_es-xl_42333.pdf

3.2 Segmentación de redes de datos

A medida que una red de datos crece con respecto a su nivel físico, es decir, que se incrementa el número de equipos de red y de dispositivos finales entre fijos y móviles, aparecen problemas con respecto a la escalabilidad y al rendimiento de la red, así como en la administración de las direcciones IPs. Por tal razón, para solventar el problema generado debido al cambio de una red pequeña a una red medianamente grande, es imprescindible dividir la red y agrupar a los hosts en subredes específicas para ser interconectadas entre sí.

Al implementar una segmentación de red, se toma en cuenta características comunes que justifiquen su agrupación, como: ubicación geográfica, propósito y propiedad.

Cuando hablamos de agrupación geográfica, específicamente se define como la segmentación de subredes para cada sucursal ubicadas en diferentes localidades, con el objetivo de que cada sede opere con una subred diferente a las demás subredes, de esta manera la administración de cada una de ellas es independiente entre sí.

Si la agrupación se enfoca a la propiedad, la característica principal es la de permitir la administración y gestión de subredes donde el control de acceso y roles de cada una de ellas, difieran entre sí, ya sea entre departamentos o grupos de usuarios de cada subred.

Por último, para la presente investigación se aplica la agrupación para propósitos específicos. El aspecto clave de este método, como muestra la Figura 23, es la división en subredes por departamentos y la agrupación de usuarios según el uso de una herramienta en común, el acceso a recursos de red afines, patrones de tráfico similares y pertenezcan al mismo nivel de criticidad detallado en la tabla número 2 del capítulo anterior.

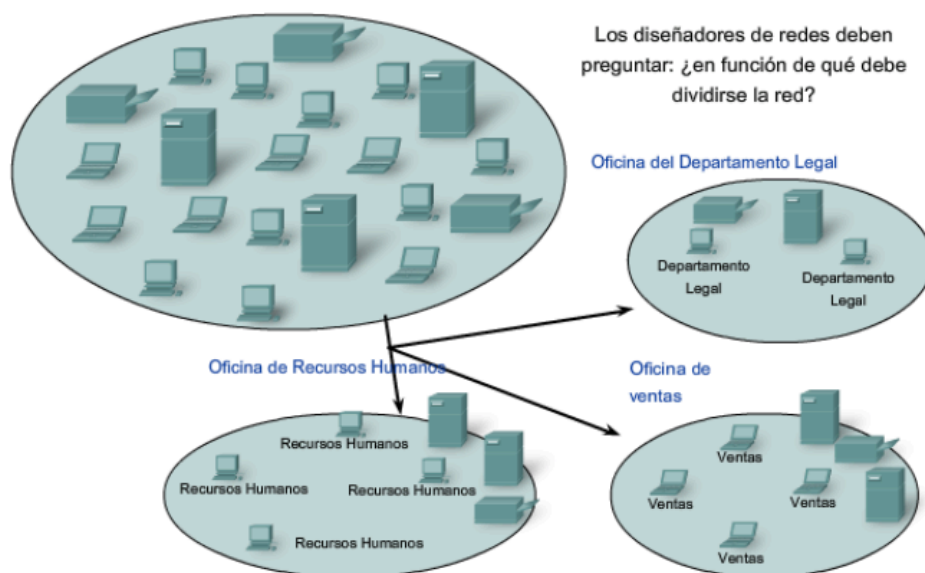


Fig 23.- Segmentación por propósito
Fuente: CCNA Exploration 4.0 Aspectos básicos de networking

Recordemos que, a medida que los dispositivos en las redes se incrementan, surgen distintos problemas, los cuales inciden principalmente en su rendimiento, seguridad y la administración de direcciones IPs.

Rendimiento

Al mantener una red plana con un solo segmento de red, se generan varias complicaciones que influyen directamente en el rendimiento, uno de ellos se produce cuando aparecen volúmenes de tráfico considerables que circulan por la red y que conllevan a la saturación del medio y afectan a la velocidad de la transmisión de datos.

Ante esto, como se muestra en la Figura 24, se propone una división de red, para agruparlos en segmentos y evitar el tráfico broadcast general de toda la red, por lo tanto, cada subred maneja su propio dominio de broadcast, de este modo se evita la saturación de la capacidad de toda la red y se asegura un apropiado rendimiento de la infraestructura.

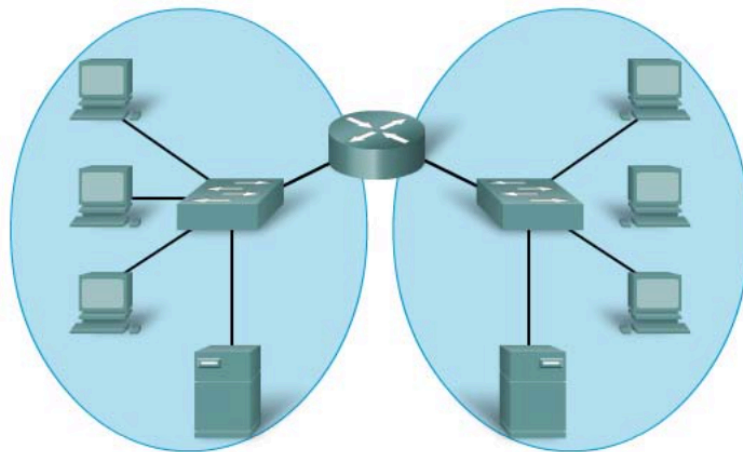


Fig 24.- Rendimiento

Fuente: CCNA Exploration 4.0 Aspectos básicos de networking

Un tráfico broadcast aparece cuando un host o dispositivo envía un mensaje broadcast a toda la red, específicamente cuando desconoce su destino, es decir, envía el mensaje a todos los host o dispositivos de la red. Si la red es de grandes proporciones con respecto

al número de host, es visible que este tráfico aumenta significativamente generando problemas de sobrecarga en la red, degradando su fluidez en los datos.

Seguridad

A más de lo tratado, la segmentación de redes nos ofrece otra ventaja en relación a la seguridad, lo que permite darle un tratamiento diferenciado a cada subred en relación a políticas de acceso según el rol que desempeña dentro de cada departamento en una red de datos.

En referencia a nuestra investigación, al proponer un diseño de una red dividida en segmentos o subredes por departamentos, se otorga la posibilidad de aplicar políticas de seguridad como permitir o prohibir el acceso a servicios según los requerimientos dados por la administración con el propósito de asegurar la disponibilidad de la red y las comunicaciones y gestionar el acceso a datos específicos dentro de la red de la institución, como se muestra en la Figura 25.

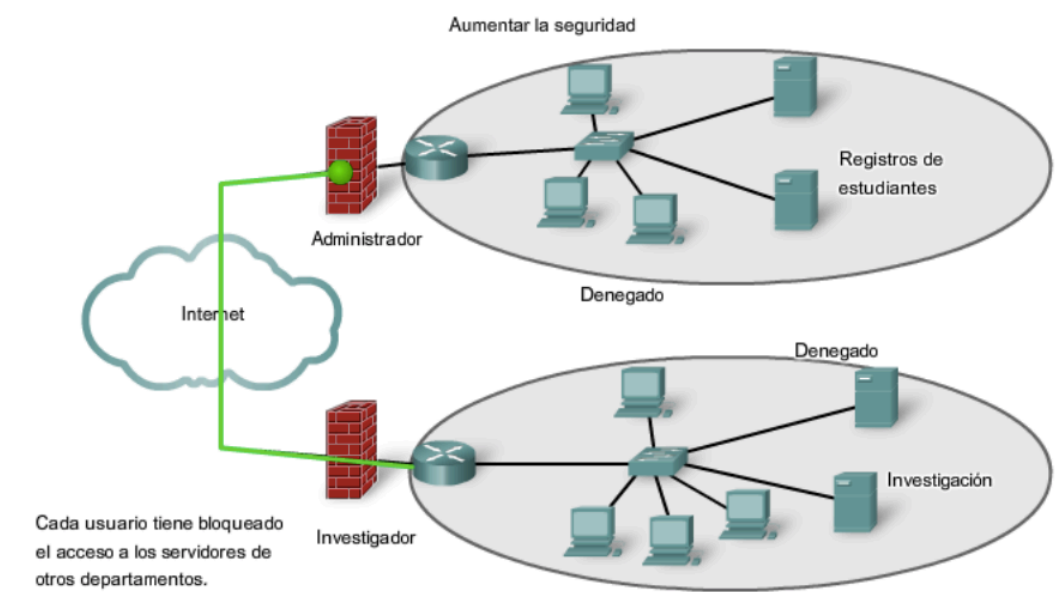


Fig 25.- Seguridad
Fuente: CCNA Exploration 4.0 Aspectos básicos de networking

Administración de direcciones IP

El direccionamiento IP en una red es muy importante para la transmisión de datos entre dispositivos pertenecientes a un mismo segmento de red o con otros de distinta subred. Por consiguiente, es fundamental desarrollar un plan que permita diseñar, implementar y administrar la asignación del direccionamiento IP, para asegurar que el rendimiento de la red sea eficaz y eficiente.

Las direcciones IPv4 de 32 bits se las representan en formato decimal punteada, por fácil interpretación y manejo humano, a diferencia del formato binario. La condición que debe cumplir es que cada dispositivo dentro de una red debe ser identificado por una dirección IP única, de este modo se identifica la dirección de origen del paquete y la dirección de destino del paquete en la comunicación entre hosts.

La siguiente dirección IP 192.168.1.23, se encuentra expresada en formato puntos decimal.

Existen tres tipos de direcciones IP:

Dirección de red: Hace referencia a la red. 192.168.1.0

Dirección de broadcast: Permite enviar paquetes a todos los hosts en una red.
192.168.1.255

Dirección de host: Es única en una red y está entre la dirección de red y broadcast.
192.168.1.23

Prefijos de red

Comúnmente es identificada como máscara de subred, consta de 32 bits al igual que la dirección IPv4 y permite conocer el rango de hosts permitidos dentro de la dirección red.

Por ejemplo, la red 192.168.1.0/24, donde la longitud de prefijo /24 indica que los primeros 24 bits son la dirección de red y los 8 restantes representa la porción de host, en este caso el número de host permitidos serían 254.

La Figura 26, permite comprender los conceptos anteriormente descritos.

Red	Dirección de red Todos los bits de hosts (rojo) = 0	Rango de host Representa todas las combinaciones de bits de host, excepto en donde los bits de host son sólo ceros o sólo unos	Dirección de broadcast Todos los bits de host (en rojo) = 1
172.16.4.0 /24	172.16.4.0	172.16.4.1 - 172.16.4.254	172.16.4.255
172.16.4.0 /25	172.16.4.0	172.16.4.1 - 172.16.4.126	172.16.4.127
172.16.4.0 /26	172.16.4.0	172.16.4.1 - 172.16.4.62	172.16.4.63
172.16.4.0 /27	172.16.4.0	172.16.4.1 - 172.16.4.30	172.16.4.31
Representación binaria 27 bits de red	10101100.00010000.000001 00.00000000	10101100.00010000.00000100.00000001 10101100.00010000.00000100.00000010 10101100.00010000.00000100.00000011 10101100.00010000.00000100.00011110	10101100.00010000.00000100.00011111

MISMA DIRECCIÓN DE RED PARA TODOS LOS PREFIJOS

DIFERENTE DIRECCIÓN DE BROADCAST PARA CADA PREFIJO

Fig 26.- Direccionamiento en una red IPv4
Fuente: CCNA Exploration 4.0 Aspectos básicos de networking

Planificación de direccionamiento de la red

Anteriormente, se había resaltado que el apropiado diseño de un plan de direccionamiento IP, asegura el correcto desempeño de una red institucional, por tal razón, la planificación tiene que ser enfocada a los siguientes puntos:

Evitar IPs duplicadas

Sin un apropiado plan de asignación de direcciones IPs se pueden generar problemas de duplicación de IPs, que consiste en que dos o más host tengan el mismo direccionamiento, incumpliendo con la premisa que cada host debe tener un único direccionamiento IP dentro de una red.

Acceso y control

A más de los host o dispositivos finales de los usuarios de una red, se cuentan con ciertos dispositivos como son los servidores, los mismos que dependiendo de su servicio deben ser accesibles tanto dentro de la red o fuera de ella. Esto significa que si no mantenemos un adecuado plan o si por algún motivo el servidor cambió su dirección IP, primero no estará disponible dentro de la red y luego las políticas de control y seguridad aplicadas al servidor quedarán sin efecto.

Monitoreo y rendimiento

Si la documentación del direccionamiento IP de una red es precisa, facilita considerablemente la solución de problemas en una red, dado que mediante el uso de una herramienta de monitoreo se podrá identificar fácilmente el host que se encuentra afectando al rendimiento mediante su dirección IP, de este modo se pueden tomar acciones correctivas sobre el dispositivo.

Asignación estática

Consiste en que el host debe ser configurado manualmente los parámetros de red, como son: dirección IP, máscara de red y gateway por defecto o puerta de enlace. Esto ocurre, con servidores, impresoras y otros dispositivos de red que son accesibles para los demás hosts de la red o en ciertos casos desde fuera de la misma, es decir, alcanzables desde otro segmento de red o desde Internet.

Asignación dinámica

A diferencia del método anterior, la asignación de las direcciones IPs a los dispositivos se lo realiza mediante el protocolo DHCP – Protocolo de configuración dinámica de host.

Puntualmente, en la red de la UES la mayor población de dispositivos finales son de tecnología inalámbrica como computadores portátiles, tablets y teléfonos inteligentes, lo que conlleva a usar un direccionamiento dinámico. De tal forma que la asignación de direcciones a los hosts será dinámica sin necesidad de configurarlos manualmente.

Es necesario resaltar que en la presente investigación, el diseño contempla el uso de direccionamiento estático y dinámico según el requerimiento, ahora bien, el actual router de Core de la UES cumple con las condiciones técnicas para utilizar el protocolo DHCP y sus parámetros asociados como grupo de direcciones, aislamiento de ciertas IPs para evitar duplicación, reutilización de direcciones; por lo tanto será el encargado de entregar la dirección IP, máscara de red, gateway y DNS, parámetros esenciales para una comunicación local como hacia Internet.

VLAN

Una red de área local virtual VLAN, es un método en capa 2 que permite múltiples LANs virtuales en una sola interface física, como ethernet, inalámbrica u otra, para segregar redes LANs de manera eficiente. (Mikrotik, 2018).

“Es un método de crear redes lógicamente independientes dentro de una misma red física. Varias VLANs pueden coexistir en un mismo conmutador físico o en una única red física. Son útiles para reducir el tamaño del dominio de difusión y ayudan en la administración de la red separando segmentos lógicos de una red de área local (como departamentos de una empresa) que no deberían intercambiar datos usando la red local (aunque podrían hacerlo a través de un enrutador de capa 3)” (Fonquernie, 2013)

802.1Q

IEEE 802.1Q es el protocolo más usado para las redes virtuales VLANs. Este estándar de encapsulación define cómo se adiciona un campo de identificación dentro de la cabecera ethernet, como se muestra en la siguiente Figura 27.

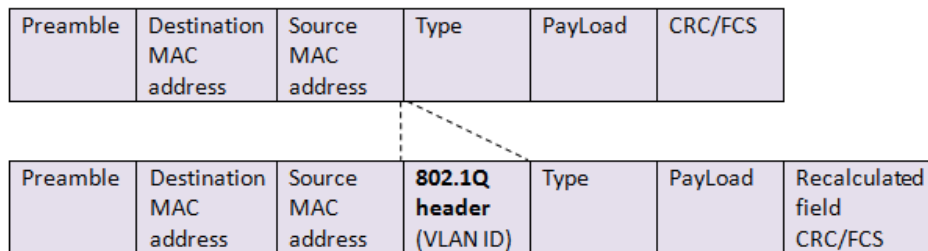


Fig 27.- 802.11Q

Fuente: <https://wiki.mikrotik.com/wiki/Manual:Interface/VLAN>

Es así que cada VLAN se maneja como una subred independiente, es decir, un host de una VLAN no podrá comunicarse con otro host que pertenezca a otra VLAN sin un dispositivo de Capa 3. Si por el contrario, se necesita establecer comunicación entre hosts de diferentes VLANs se deberá agregar al diseño de la red de la institución un enrutador que permita el intercambio de información entre dispositivos de la red, puntualmente en nuestro caso de estudio entre dispositivos de diferentes departamentos, si alguno de los requerimientos fuera el mencionado. RouterOS permite usar hasta 4095 VLANs, cada una con un identificador único por interfaz.

3.3 Modelos de calidad de servicio

La administración del tráfico con prioridades es un tema crucial en una red de datos donde el objetivo principal es garantizar el acceso a servicios críticos y más importante aún que no se vean interrumpidos debido a demoras o saturación del medio. La tecnología que permite realizar esta gestión se denomina Calidad de Servicio o por sus siglas en inglés

QoS – Quality of Service. La Figura 28 muestra la signación de prioridades en base al que genere mayor porcentaje de paquetes.

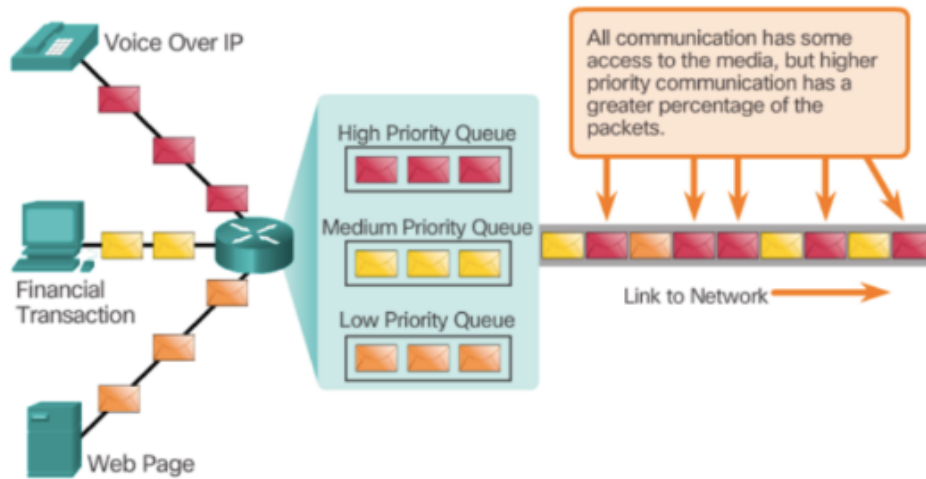


Fig 28.- Priorización con QoS

Fuente: <https://community.cisco.com/t5/blogs-routing-y-switching/fundamentos-de-qos-calidad-de-servicio-en-capa-2-y-capa-3/ba-p/3103715>

Con la implementación de una política de QoS en la red de una organización, se pueden definir reglas para los distintos tipos de tráfico y evitar un problema muy común en las redes con un mal diseño como es la congestión, la misma que puede generarse primero cuando los enlaces tienen sobresuscripción de dispositivos y luego, cuando los dispositivos generan un volumen de tráfico superior a la capacidad del enlace, precisando en esta instancia que QoS no genera ancho de banda sino que lo gestiona para distribuirlo según las políticas a ejecutar y sus prioridades.

A continuación, se listan ciertos puntos que incentivan a diseñar una red con calidad de servicio:

- Maximizar el uso del ancho de banda disponible en la red
- Gestionar el buen uso de la capacidad contratada de acceso a Internet para evitar el sobredimensionamiento de contratación de ancho de banda.

- Asegurar el acceso a aplicaciones y herramientas cruciales para la continuidad de negocio o actividades diarias en una institución.
- Equidad de acceso a aplicaciones entre los dispositivos finales de los usuarios cuando se presentan congestiones en la red.
- La priorización de aplicaciones no críticas o de entretenimiento, deben mantener un nivel inferior de prioridad comparado al de las aplicaciones cruciales o críticas del negocio.

Para la implementación de una calidad de servicio se definen las siguientes acciones:

1. Identificar el tipo de tráfico que circula por la red
2. Clasificar el tráfico de las tomas efectuadas del punto anterior
3. Priorizar el tráfico según las marcas realizadas en la clasificación

Marcado de paquetes

El módulo de RouterOS con sistema operativo de Mikrotik que permite el marcado de paquetes IPs de manera especial para un tratamiento interno se denomina Mangle. Dichas marcas no modifican al paquete, es decir, el paquete ingresa y sale tal cual. Además, las marcas pueden ser usadas en otros módulos de RouterOS como en las políticas de ruteo y en la calidad de servicio.

Adicionalmente, Mangle permite modificar ciertos campos en el encabezado del paquete IP como ToS o DSCP y TTL.

El Mangle es el 50% de una buena QoS. (Dobladez, 2019)

Estructura del Mangle

Las reglas de Mangle se organizan en cinco cadenas por defecto, que son:

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

Las acciones de mangle son:

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

Mark-Connection

La marca de conexión se la utiliza para identificar una conexión o un grupo de conexiones asociadas a una marca específica. En la siguiente figura, se muestra la regla de marcado de conexión para las conexiones TCP puerto 80 con la cadena prerouting.

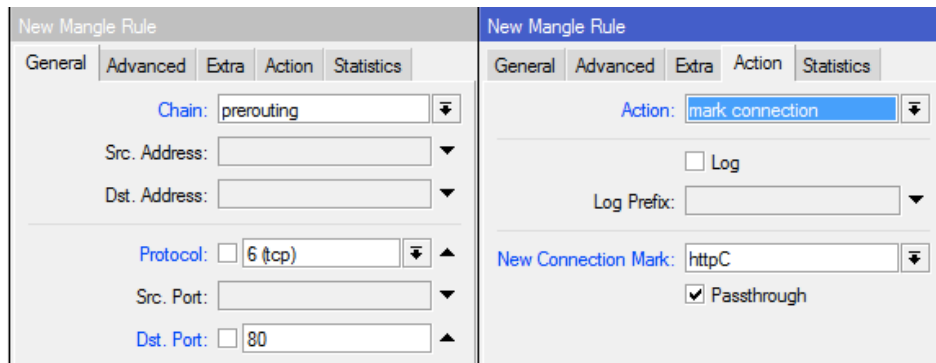


Fig 29.- Mark Connection
Fuente: Propia

Mark-Packet

Para marcar todos los flujos relacionados con una marca de conexión específica utilizamos la acción mark packet. La Figura 30 muestra la regla de marcado de paquete para la marca de conexión de la Figura 29.

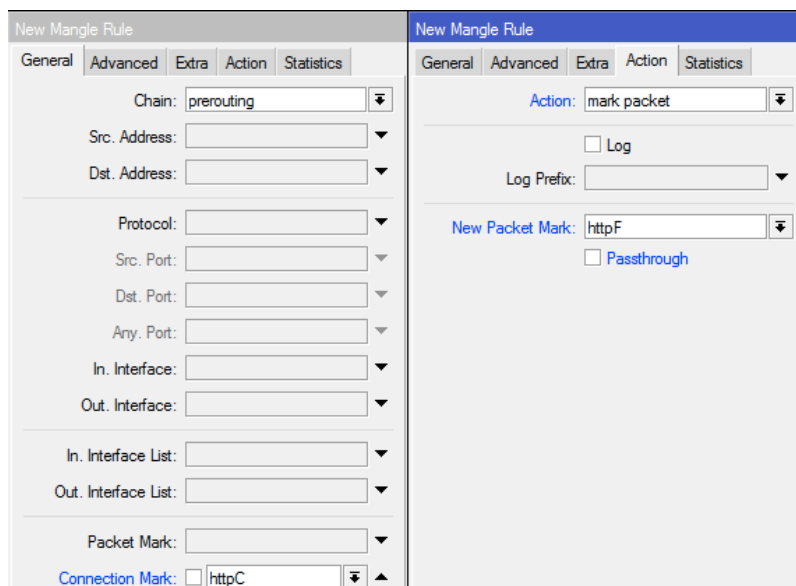


Fig 30.- Mark Packet
Fuente: Propia

Principios básicos de QoS

QoS no es solo limitación, más bien, es un intento de usar los recursos existentes de manera racional, es decir, no necesariamente debe usarse toda la capacidad disponible.

Adicional, la calidad de servicio balancea, prioriza o limita el flujo de datos, previniendo que un solo dispositivo monopolice el canal de datos.

CIR y MIR

Para utilizar los dos parámetros, es necesario agregar una Simple Queue, como se muestra en la Figura 31.

Existen dos tipos de límites:

- CIR – Committed Information Rate
Garantiza en el peor de los casos, es decir, obtendrá lo asegurado. Se lo llama Limit At en RouterOS.
- MIR – Maximal Information Rate
Es la velocidad máxima a enviar en el mejor de los casos. Denominado Max Limit en RouterOS.

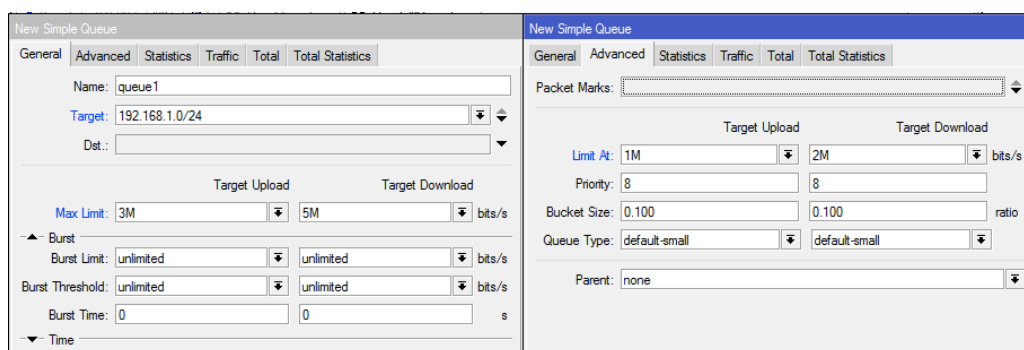


Fig 31.- CIR y MIR
Fuente: Propia

Queue Tree

La calidad de servicio que implementa RouterOS está basada en HTB. Hierchical Token Bucket permite crear estructuras jerárquicas de colas y determinar las relaciones entre colas, padres e hijos y entre colas hijos. (Mikrotik, 2019)

Cuando una queue al menos tiene una queue hija se convierte en queue padre. Las queues padres son las responsables de la distribución del tráfico, mientras que las colas hijas hacen el consumo de este, obteniendo primero el limit-at.

RouerOS maneja un código de colores en relación con el tráfico de las colas.

- Verde: 0% al 50% del tráfico disponible utilizado
- Amarillo: 51% al 75% del tráfico disponible utilizado
- Rojo: 76% al 100% del tráfico disponible utilizado

Prioridad

RouterOS maneja un esquema de prioridad que van del 1 al 8, donde 8 es la prioridad más baja y 1 la más alta. Por defecto trae incluida la prioridad 8. Para explicarlo diremos lo siguiente: la queue con más alta prioridad, ósea una queue que tenga prioridad por debajo de 8, llegará a su CIR – Limit at antes que la que tiene menos prioridad y la queue con más alta prioridad, llegará a su MIR – Max Limit antes que la que tenga menor prioridad.

La aplicación de las prioridades dependerá del tipo de red, de su utilidad y principalmente de la clasificación de los servicios críticos, por ejemplo, como prioridad 8 se mantendrían los servicios de FTP, actualizaciones de sistemas operativos, P2P y otros que no sean críticos, llegando a la mayor prioridad 1 los servicios de acceso a una específica aplicación, correo electrónico, telefonía IP o según el propósito de la red, en nuestro caso el acceso a la plataforma de gestión educativa Mikareno.

Disciplina de encolamiento PCQ

PCQ – Per Connection Queue

Es una disciplina propietaria de Mikrotik que permite subdividir el tráfico encolado según el clasificador seleccionado, de este modo, permite dividir el flujo por IP de origen e IP de destino según el sentido del tráfico.

Además, ofrece la posibilidad de limitar la velocidad de datos que se da a cada flujo, utiliza los siguientes parámetros:

- **Pcq classifier:** se puede seleccionar los identificadores, sr-address, dst-address, src-port, dst-port
- **Pcq-rate:** velocidad máxima de datos de cada sub-flujo
- **Pcq-limit:** tamaño de la cola de un sub-flujo
- **Pcq-total-limit:** cantidad máxima de datos en todos los sub-flujos

En la Figura 32, podemos observar el comportamiento del algoritmo PCQ en una cola con pcq-rate de 128kbis/s y un max-limit de 512kbis/s. Claramente se concluye que con el incremento de usuarios el ancho de banda se divide para cada uno de ellos en partes iguales, sin embargo, la capacidad máxima de cada usuario no sobrepasa los 128k que viene configurado por el pcq-rate.

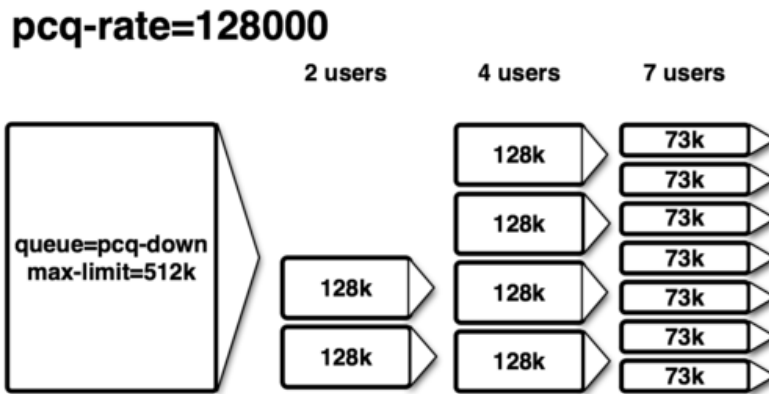


Fig 32.- PCQ rate=128000
 Fuente: https://wiki.mikrotik.com/wiki/Manual:Queues_-_PCQ

A diferencia del modelo anterior, en la Figura 33, se observa que cuando se configura un tipo de cola PCQ con $pcq\text{-rate}=0$, divide el tráfico del $max\text{-limit}$ a los usuarios en partes iguales llegando a la velocidad máxima del $max\text{-limit}$.

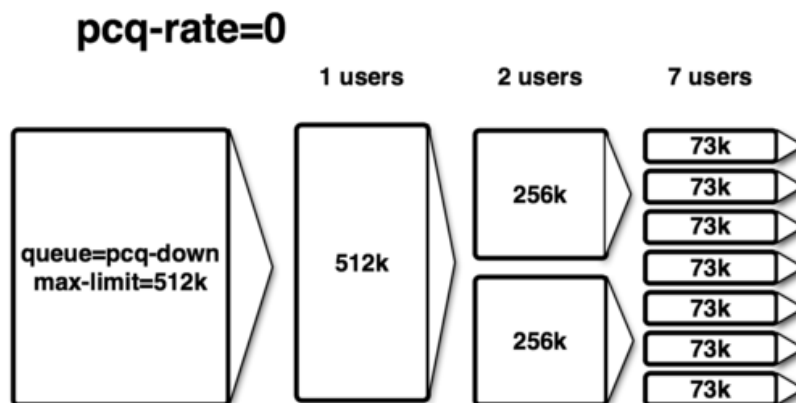


Fig 33.- PCQ rate=0
 Fuente: https://wiki.mikrotik.com/wiki/Manual:Queues_-_PCQ

Puntualmente, en la presente investigación se estudiará el modelo de $pcq\text{-rate}$ a utilizar dependiendo de las necesidades de velocidad de cada usuario y la capacidad máxima contratada al proveedor en la red de la UES. Dependerá si el caso fuese que se tenga que distribuir equitativamente la capacidad total o poner un límite máximo para cada usuario, servicio o aplicación.

3.4 Emuladores gráficos de red

Los emuladores gráficos son herramientas informáticas que permiten la emulación de escenarios de entornos de red y analizar su comportamiento, por ejemplo, en el campo educativo como entorno de enseñanza/aprendizaje donde el presupuesto es escaso para implementar laboratorios con un buen equipamiento de equipos de redes y comunicaciones, algo semejante ocurre en el área de las comunicaciones como entorno de desarrollo o pruebas pre producción, donde la emulación de una solución a diseñar o implementar, puede ser tan productiva como efectiva antes de una implementación definitiva.

Las características de este segmento de software permiten ejecutarlo como herramienta:

- Didáctica para estudio de redes con varios sistemas operativos de equipos de comunicaciones como RouterOS y otros sistemas operativos
- De pruebas para analizar el comportamiento de una red en un escenario real
- Para el desarrollo de nuevas configuraciones previo a la implementación en escenarios de alta disponibilidad
- Para la simulación de hardware sin gastar en equipamiento en la etapa de diseño

Podemos nombrar varios emuladores gráficos existentes en el mercado como EVE-NG, Mininet, Core, entre otros, sin embargo, en la presente investigación nos centraremos en el uso de GNS3 por un lado porque se cuenta con imágenes del sistema operativo de Mikrotik RouterOS, luego por la compatibilidad de la emulación del hardware de la marca antes mencionada y finalmente se justifica porque cumple con los tres elementos de una simulación que detallamos en la Figura 34.

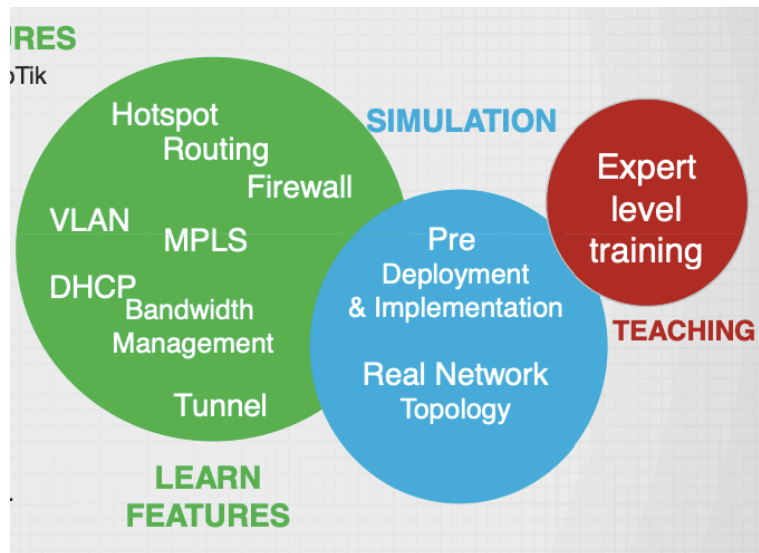


Fig 34.- Objetivo de un simulador

Fuente: MIKROTIK NETWORK SIMULATOR PRESENTED BY ROFIQ FAUZI MUM Nov Indonesia

GNS3

Es un simulador de red gráfico que puede ser ejecutado en plataformas como Windows, Mac OS y Linux, y es el esfuerzo colaborativo de algunos especialistas, talentosos y de fuerza industrial como Cristopher Fillot, Jeremy Grossman y Julien Duponchelle. (Neumann, 2015).

GNS3 permite diseñar y probar topologías de redes básicas y complejas en el computador con marcas como Cisco, Juniper, Mikrotik, Arista y Vyatt networks. Comúnmente, es usado en entornos educativos para la preparación de estudiantes en proceso de certificación de programas de Academia de Cisco como CCNA o CCNP.

Antes de la presencia de los emuladores gráficos, para realizar una simulación o emulación de un escenario de una red, por parte de especialistas en redes y estudiantes, se necesitaba contar con laboratorios equipados que permitan crear el entorno requerido, lo que demandaba costo en la adquisición de equipamiento físico de dispositivos de conexión y licencias.

GNS3 permite personalizar los ambientes de red a la necesidad de su diseño, topología y pruebas, gracias a su flexibilidad que permite combinar interfaces de equipos de red como routers y switches con sus sistemas operativos, en el caso de equipos Cisco con CiscoIOS- IOS-XE/XR y puntualmente en nuestra investigación con dispositivos Mikrotik con su sistema operativo RouterOS.

Para emular el hardware GNS3 utiliza un hypervisor que ejecuta una imagen del dispositivo, de este modo, permite ejecutar todos los comandos de configuración, además, integra la emulación del sistema operativo mediante el Quick Emulator – QEMU y VirtualBox que soporta máquinas virtuales donde se puede correr sistemas como Linux, BSD o Windows.

3.5 CHR - Cloud Hosted Router

RouterOS es el sistema operativo que viene incorporado en los RouterBoard de marca Mikrotik. También, puede ser instalado en una PC manteniendo las mismas características que un RouterBoard como son: Firewall, HotSpot, MPLS, Routing, BGP, QoS, entre otras.

Para acceder al sistema operativo RouterOS independiente del hardware donde se encuentre instalado, se lo puede realizar de las siguientes maneras:

- CLI – command-line interface, mediante Telnet, SSH, siempre y cuando no se encuentre administrado por un firewall
- GUI – graphical user interface, WebFig
- Winbox - Es una herramienta de configuración que permite conectarse a los RouterBoard mediante MAC o IP.

CHR

Es una versión de RouterOS diseñada para ejecutarse dentro de una máquina virtual, que puede ser manejada por varios hypervisores, entre los más importantes, Hyper-V, KVM, VirtualBox, VMWare y Amazon Web Services. Usa la arquitectura x86 de 64 bits.

CHR posee todas las características predeterminadas del RouterOS instalado en un RouterBoard, en lo que difieren es en el manejo de las licencias.

Requerimientos para la instalación:

- RouterOS actualizado a la última versión
- CPU del Host: 64 bits que soporte virtualización
- RAM del Host: 128MB o más
- Disk del Host: 128MB libre de espacio en disco

4 DISEÑO Y EMULACIÓN

4.1 Descripción del diseño

En el desarrollo del presente capítulo, se abordan temas orientados al diseño de la red de datos de la Unidad Educativa Suizo, con miras al cumplimiento de los requerimientos obtenidos en los capítulos anteriores, además de la emulación de la red y pruebas de conectividad del diseño.

El diseño propuesto se basa en el modelo jerárquico de Cisco de tres capas, y específicamente en una variante de este como es la de núcleo fusionado por todas las ventajas abordadas en el capítulo anterior, detallado en la Figura 22 y que se enmarcan en la ejecución del presente diseño en relación al diseño de la topología física, lógica y de funcionalidad de la red.

Núcleo Fusionado: Para el cumplimiento de los niveles de núcleo y distribución, el diseño incluye como Router de Core un equipo Mikrotik RB4011iGS+5HacQ2HnD-IN, en base al cumplimiento de las funciones que demandan los dos niveles en relación a sus recursos de hardware como sistema operativo.

Este equipo cumple con las siguientes funciones:

- Conectividad a nivel WAN con el proveedor de servicio de Internet
- Direccionamiento IP WAN y LAN
- Manejo de VLANs
- Servidor de DHCP
- Firewall
- Mangle

- Enrutamiento estático
- Calidad de Servicio

Las especificaciones técnicas del RouterBoard se detallan en la Tabla 3.

Tabla 3.- Especificaciones técnicas RB4011iGS+5HacQ2HnD-IN

Product code	RB4011iGS+5HacQ2HnD-IN	
CPU	4 core AL21400 1.4 GHz	
Size of RAM	1 GB	
Storage	NAND 512 MB	
10/100/1000 Ethernet ports	10	
SFP+ port	1	
Switch chip model	RTL8367SB	
Wireless	2.4 GHz radio	5 GHz radio
Wireless regulations	Specific frequency range may be limited by country regulations	
Operating frequency	2412 - 2484 MHz	5150 - 5875 MHz
Wireless interface model	R11e-2HnD	QCA-9984
Supported protocol	802.11b/g/n	802.11a/n/ac
Chains	2	4
Antenna beam width	360°	
Antenna gain	3 dBi (2 antennas dual band, 2 antennas single 5 GHz band)	
Power Jack	1	
PoE in	Yes (port 1), passive, 18 - 57 V	
PoE out	Yes (port 10), passive, up to 57 V	
Max power consumption	23 W without PoE out, 44 W with PoE out	
Supported input voltage	12 V - 57 V (jack)	

Fuente: https://i.mt.lv/cdn/rb_files/RB4011-IN-180919132356.pdf

Acceso: Para brindar conectividad a los dispositivos finales, en el diseño se conservan los equipos de la actual red de la institución.

En los laboratorios de computación e inglés, se mantienen los switches y su infraestructura física, al igual que los cuatro puntos de acceso de la red inalámbrica de la red de profesores. A diferencia de la red de administración y rectorado, donde se agregan equipos Mikrotik hAP ac, con mejor performance a los que actualmente se encuentran instalados.

Las especificaciones técnicas de los equipos se muestran en la Tabla 4.

Tabla 4.- Especificaciones técnicas hAP ac

Product code	RB962UiGS-5HacT2HnT (International) RB962UiGS-5HacT2HnT-US (USA)			
CPU nominal frequency	720 MHz			
Size of RAM	128 MB			
Storage type	Flash			
Flash size	16 MB			
10/100/1000 Ethernet ports	5			
SFP	1			
Wireless	5 GHz radio		2.4 GHz radio	
Wireless regulations	Specific frequency range may be limited by country regulations			
Operating frequency	International	5150 - 5875 MHz	International	2412 - 2484 MHz
	USA	5170 - 5250 MHz 5725 - 5835 MHz	USA	2412 - 2462 MHz
Protocols	802.11a/n/ac		802.11b/g/n	
Chains	Triple-chain		Triple-chain	
Antenna gain	2 dBi		2.5 dBi	
Wireless chip model	QCA9880		QCA9558	
Antenna beam width	360°			
PoE in	Yes			
PoE out	Yes (Ether5)			
Supported input voltage	11 V - 57 V (Jack or Passive PoE)			
Max Power consumption	17 W			

Fuente: https://i.mt.lv/cdn/rb_files/hAP_ac-170927121452.pdf

Diseño de Topología Física

Para el diseño de la topología física se considera la infraestructura actual del proveedor de Internet CNT EP. instalado en la red de la UES. La Figura 35 muestra la propuesta de la topología física.

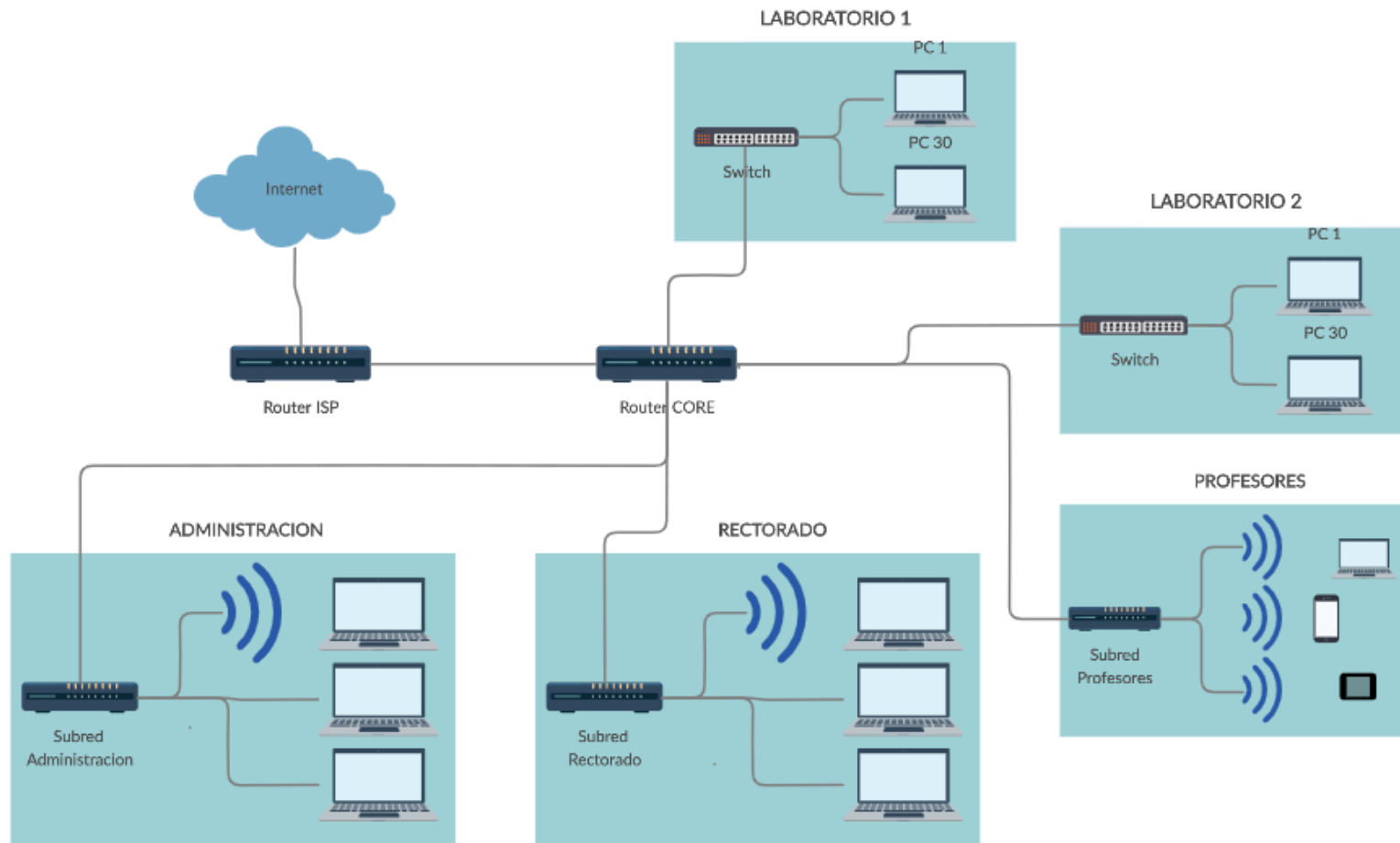


Fig 35.- Propuesta de la topología física
Fuente: Propia

Diseño de la Topología Lógica

Posterior al diseño físico, se realiza la propuesta de la topología lógica, la misma que ofrece conectividad a los departamentos de la institución como: Administración, Rectorado, Laboratorio de Computación, Laboratorio de Inglés y el conjunto de aulas con cobertura de red inalámbrica para el acceso a dispositivos de los docentes. El direccionamiento utilizado corresponde a IP versión 4 para la asignación de direcciones a los equipos de red y dispositivos finales.

A cada departamento de la institución se asigna una VLAN con un identificador diferente y por consecuencia un direccionamiento IP para cada segmento de red, de este modo, se facilita la ejecución de políticas y la priorización de servicios críticos clasificados en capítulos anteriores y detallados en la Tabla 2.

La siguiente Tabla detalla la asignación de VLANs por departamento.

Tabla 5.- Vlan por departamento

VLAN	ID	DEPARTAMENTO
vlan.profesores	10	Profesores
vlan.lab1	20	Laboratorio de Computación
vlan.lab2	30	Laboratorio de Inglés
vlan.administracion	40	Administración
vlan.rectorado	50	Rectorado

Fuente: Propia

Segmentación de red

La segmentación de la red está dimensionada según el número de dispositivos que se conectan a la subred de cada departamento. En la siguiente tabla, se observa que el direccionamiento inicia desde la red 192.168.0.0/26 y luego se segmentan las siguientes redes para cada VLAN en base al subneteo VLSM, donde el fin de una red es el inicio de otra.

Tabla 6.- Segmentación de red

DEPARTAMENTO	RED	MASCARA	PRIMER HOST	ULTIMO HOST	BROADCAST
Profesores	192.168.0.0	255.255.255.192	192.168.0.1	192.168.0.62	192.168.0.63
Laboratorio 1	192.168.0.64	255.255.255.192	192.168.0.65	192.168.0.126	192.168.0.127
Laboratorio 2	192.168.0.128	255.255.255.192	192.168.0.129	192.168.0.190	192.168.0.191
Administración	192.168.0.192	255.255.255.224	192.168.0.193	192.168.0.222	192.168.0.223
Rectorado	192.168.0.224	255.255.255.224	192.168.0.225	192.168.0.254	192.168.0.255

Fuente: Propia

Para la asignación de direcciones IPs a los distintos dispositivos finales de la red, se lo realiza mediante la configuración de un Servidor DHCP en el Router de Core, en base a la segmentación de la Tabla 6.

Calidad de servicio

Para el diseño de la calidad de servicio se utilizan tres instancias que ofrece RouterOS.

En primer lugar, se utiliza la instancia de Forward en el Mangle con el objetivo de identificar el tráfico que provenga de los servicios a priorizar y realizar las marcas de los paquetes. Además, se asigna una marca a los paquetes que provengan de una lista determinada para utilizarlas más adelante.

Posterior a las marcas de paquetes, se utiliza la disciplina de encolamiento PCQ para dividir el flujo de datos de un determinado servicio para cada IP.

Por último, se combina la marca de paquete con la disciplina de encolamiento PCQ, dentro del QueueTree con el método HTB de RouterOS, además se agrega el valor de la prioridad.

4.2 Emulación del diseño

Para la emulación de la red de datos de la UES, se utilizan las siguientes herramientas operando sobre un Sistema Operativo Windows 10:

- VMware Workstation 15 Pro
- GNS3 2.2.0
- Cloud Hosted Router Mikrotik
- Winbox
- Putty

Para intensificar la comprensión de la emulación de la red y sus configuraciones es esencial incluir un apartado de Anexos, donde se incluye:

- Instalación de GNS3
- Inclusión de RouterOS a GNS3
- Primera prueba de conexión
- Instalación de Firefox Appliance
- Creación de vlan en RouterOS
- Creación de rutas estáticas en RouterOS
- Scripts y configuración

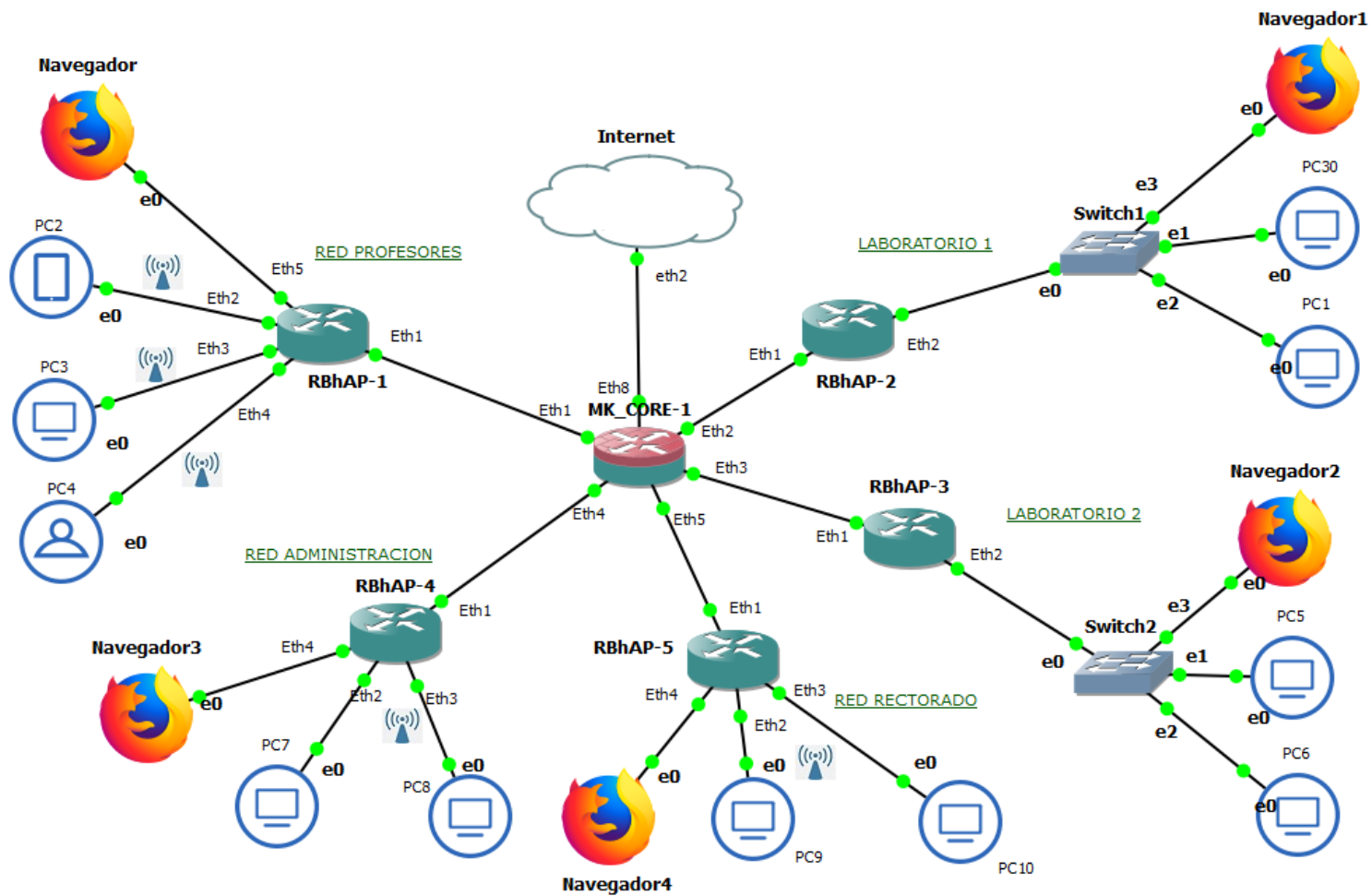


Fig 36.- Emulación de la red de datos de la UES
Fuente: Propia

Configuración de equipos

En la presente sección se desarrolla la configuración de los equipos para completar la emulación de la red y su conectividad.

Creación de VLANs

Iniciamos con la configuración de las VLANs en el Router de Core mediante línea de comandos, tal como se muestra en la Figura 37.

```
[admin@Core] /interface vlan> export
# jan/15/2020 00:26:43 by RouterOS 6.44.6
# software id =
#
#
#
/interface vlan
add comment=vlan.profesores interface=ether1 name=vlan10-1 vlan-id=10
add comment=vlan.lab1 interface=ether2 name=vlan20-2 vlan-id=20
add comment=vlan.lab2 interface=ether3 name=vlan30-3 vlan-id=30
add comment=vlan.adm interface=ether4 name=vlan40-4 vlan-id=40
add comment=vlan.rect interface=ether5 name=vlan50-5 vlan-id=50
[admin@Core] /interface vlan>
```

Fig 37.- Creación de VLANs
Fuente: Propia

La Figura 38, muestra el estado de las VLANs creadas en la Figura 37.

Interface List														
Interface	Interface List	Ethernet	EoIP Tunnel	IP Tunnel	GRE Tunnel	VLAN	VRRP	Bonding	LTE					
Name	Type	MTU	Actu...	L...	Tx	Rx	Tx...	Rx ...	FP Tx	FP Rx	FP Tx...	FP Rx ...	VLAN ID	Interface
::: vlan.profesores														
R	vlan10-1	VLAN	1500	1500	0 bps	0 bps	0	0	0 bps	0 bps	0	0	10	ether1
::: vlan.lab1														
R	vlan20-2	VLAN	1500	1500	0 bps	0 bps	0	0	0 bps	0 bps	0	0	20	ether2
::: vlan.lab2														
R	vlan30-3	VLAN	1500	1500	0 bps	0 bps	0	0	0 bps	0 bps	0	0	30	ether3
::: vlan.adm														
R	vlan40-4	VLAN	1500	1500	0 bps	0 bps	0	0	0 bps	0 bps	0	0	40	ether4
::: vlan.rect														
R	vlan50-5	VLAN	1500	1500	0 bps	0 bps	0	0	0 bps	0 bps	0	0	50	ether5

Fig 38.- VLANs por interface en Winbox
Fuente: Propia

Direcccionamiento IP

A continuación, en las Figuras 39 y 40, se muestran la asignación del direccionamiento IP de las VLANs creadas anteriormente.

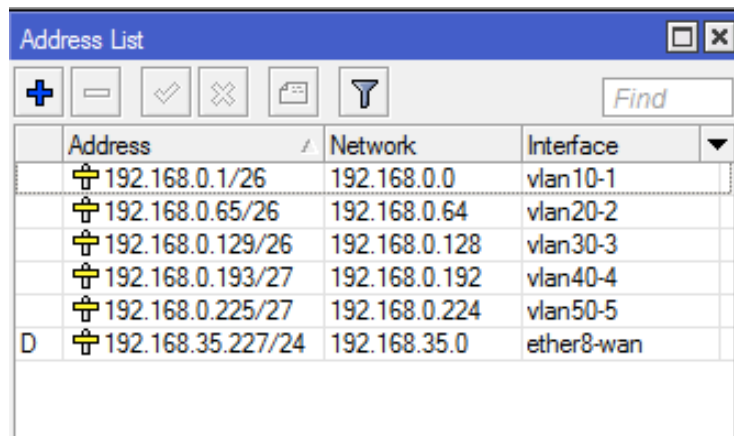
```
[admin@Core] /ip address> add address=192.168.0.1/26 interface=vlan10-1
[admin@Core] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic
#  ADDRESS          NETWORK          INTERFACE
0  D 192.168.35.227/24 192.168.35.0    ether8-wan
1  192.168.0.1/26    192.168.0.0     vlan10-1
[admin@Core] /ip address>
```

Fig 39.- Asignación de direccionamiento IP 1
Fuente: Propia

```
[admin@Core] /ip address> add address=192.168.0.65/26 interface=vlan20-2
[admin@Core] /ip address> add address=192.168.0.129/26 interface=vlan30-3
[admin@Core] /ip address> add address=192.168.0.193/27 interface=vlan40-4
[admin@Core] /ip address> add address=192.168.0.225/27 interface=vlan50-5
[admin@Core] /ip address> print
Flags: X - disabled, I - invalid, D - dynamic
#  ADDRESS          NETWORK          INTERFACE
0  D 192.168.35.227/24 192.168.35.0    ether8-wan
1  192.168.0.1/26    192.168.0.0     vlan10-1
2  192.168.0.65/26   192.168.0.64    vlan20-2
3  192.168.0.129/26 192.168.0.128   vlan30-3
4  192.168.0.193/27 192.168.0.192   vlan40-4
5  192.168.0.225/27 192.168.0.224   vlan50-5
```

Fig 40.- Asignación de direccionamiento IP 2
Fuente: Propia

Es importante indicar que la misma configuración se la pueda realizar mediante Winbox como se indica en la Figura 41.



	Address	Network	Interface
	192.168.0.1/26	192.168.0.0	vlan10-1
	192.168.0.65/26	192.168.0.64	vlan20-2
	192.168.0.129/26	192.168.0.128	vlan30-3
	192.168.0.193/27	192.168.0.192	vlan40-4
	192.168.0.225/27	192.168.0.224	vlan50-5
D	192.168.35.227/24	192.168.35.0	ether8-wan

Fig 41.- Direccionamiento IP en WinBox
Fuente: Propia

Servidor de DHCP

Para la asignación de direcciones IPs a los dispositivos finales de la red inalámbrica de profesores, se agrega un servidor DHCP sobre la interface VLAN de profesores en el Router de Core, como se muestra en la Figura 42.

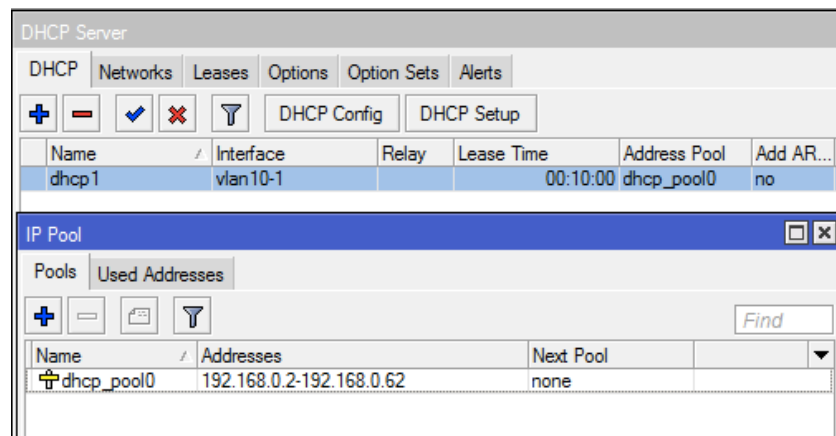


Fig 42.- DHCP Server VLAN Profesores
Fuente: Propia

Configuración RB Profesores

Paso siguiente es configurar el RBhAP-1 de la subred de Profesores. En la Figura 43 se muestran los comandos de creación de la VLAN con ID 10 sobre la interface ether1 que es la que conecta con el Router de Core.

```
[admin@RB Profesores] /interface vlan> export
# jan/15/2020 03:45:36 by RouterOS 6.44.6
# software id =
#
#
#
/interface vlan
add interface=ether1 name=vlan10 vlan-id=10
[admin@RB Profesores] /interface vlan>
```

Fig 43.- Creación de VLAN RB Profesores
Fuente: Propia

Además, se crea un bridge con las interfaces físicas del router, excepto la que conecta con el Router de Core, más la interface virtual VLAN como se muestra en la siguiente figura.

```
[admin@RB Profesores] /interface bridge port> export
# jan/15/2020 03:47:17 by RouterOS 6.44.6
# software id =
#
#
#
/interface bridge port
add bridge=local interface=ether2
add bridge=local interface=ether3
add bridge=local interface=ether4
add bridge=local interface=ether5
add bridge=local interface=vlan10
[admin@RB Profesores] /interface bridge port> █
```

Fig 44.- Creación Bridge RB Profesores
Fuente: Propia

Para que cada VPCS de la subred de Profesores, tomen una dirección IP del respectivo segmento que ofrece el servidor DHCP del Router de Core, se realiza la siguiente configuración por consola como indica la Figura 45.

```
PC3> ip dhcp
DORA IP 192.168.0.61/26 GW 192.168.0.1

PC3> ping 192.168.0.1
84 bytes from 192.168.0.1 icmp_seq=1 ttl=64 time=8.285 ms
84 bytes from 192.168.0.1 icmp_seq=2 ttl=64 time=6.107 ms
84 bytes from 192.168.0.1 icmp_seq=3 ttl=64 time=6.474 ms
84 bytes from 192.168.0.1 icmp_seq=4 ttl=64 time=6.283 ms
84 bytes from 192.168.0.1 icmp_seq=5 ttl=64 time=6.458 ms

PC3> █

PC4> ip dhcp
DORA IP 192.168.0.60/26 GW 192.168.0.1

PC4> ping 192.168.0.1
84 bytes from 192.168.0.1 icmp_seq=1 ttl=64 time=7.147 ms
84 bytes from 192.168.0.1 icmp_seq=2 ttl=64 time=6.394 ms
84 bytes from 192.168.0.1 icmp_seq=3 ttl=64 time=16.551 ms
84 bytes from 192.168.0.1 icmp_seq=4 ttl=64 time=10.623 ms
84 bytes from 192.168.0.1 icmp_seq=5 ttl=64 time=9.007 ms

PC4> █
```

Fig 45.- Configuración IP de las VPCS
Fuente: Propia

La Figura 46, muestra las direcciones IP que fueron asignadas a las VPCSs de la subred profesores.

	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address	Active Hos...	Expires After	Status
D	192.168.0.60	00:50:79:66:68:03	1:0:50:79:66:68:3	dhcp1	192.168.0.60	00:50:79:66:68:03	PC41	00:07:15	bound
D	192.168.0.61	00:50:79:66:68:02	1:0:50:79:66:68:2	dhcp1	192.168.0.61	00:50:79:66:68:02	PC31	00:06:45	bound
D	192.168.0.62	00:50:79:66:68:01	1:0:50:79:66:68:1	dhcp1	192.168.0.62	00:50:79:66:68:01	PC21	00:09:10	bound

Fig 46.- Lista de dispositivos de la subred Profesores
Fuente: Propia

Para las restantes subredes de Laboratorio 1, Laboratorio 2, Administración y Rectorado, la configuración en el Router de Core será similar tomando en cuenta el ID de VLAN e interfaz. Del mismo modo, la configuración en los routers de distribución de cada departamento mencionado debe ser la misma que se realizó en el RB Profesores respetando los parámetros de cada subred.

Disciplinas de encolamiento

Para la subred profesores se utiliza una política de encolamiento PCQ con Rate: 0, la misma que fue abordada en capítulos anteriores. En la configuración del Router de Core se crean dos Queue Types, uno para el flujo de descarga y otro para la subida, como se muestra en la Figura 47.

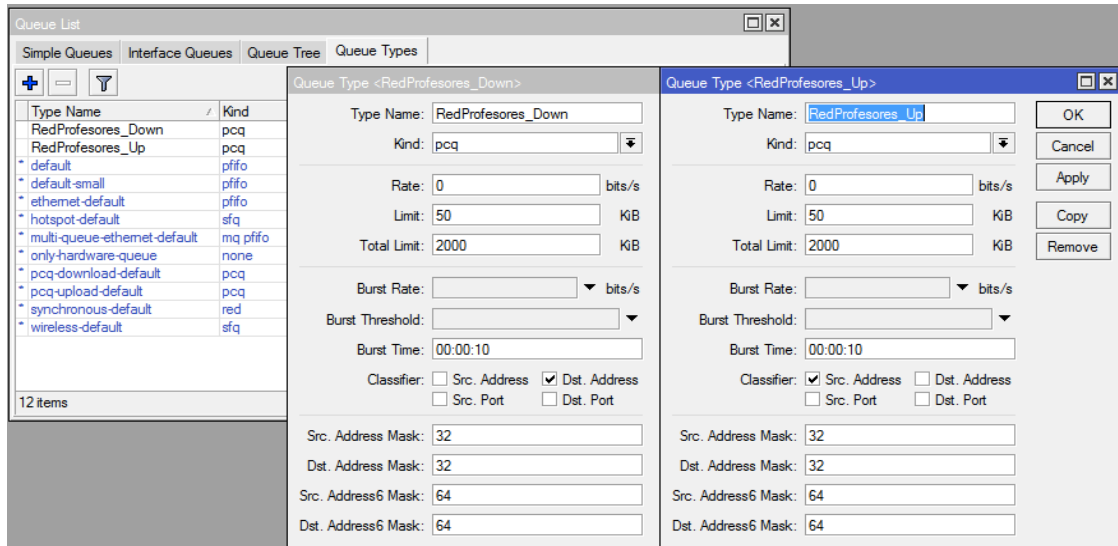


Fig 47.- Políticas de encolamiento Subred Profesores
Fuente: Propia

La Figura 48, muestra la simple queue creada para la subred de Profesores 192.168.0.0/26 que permite alcanzar un límite máximo de 10Mbps de download por 5Mbps de upload.

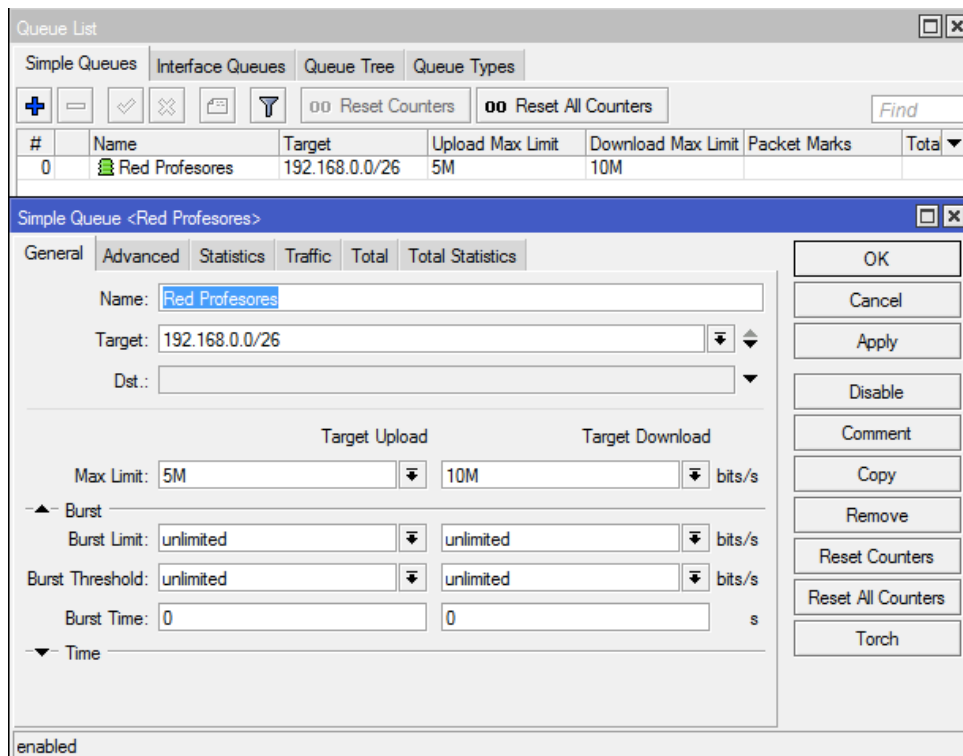


Fig 48.- Simple Queue Subred Profesores
Fuente: Propia

En la Figura 49, podemos observar la inclusión del Queue Type Red Profesores_Up y Red Profesores_DOWN creada anteriormente y detallada en la Figura 47.

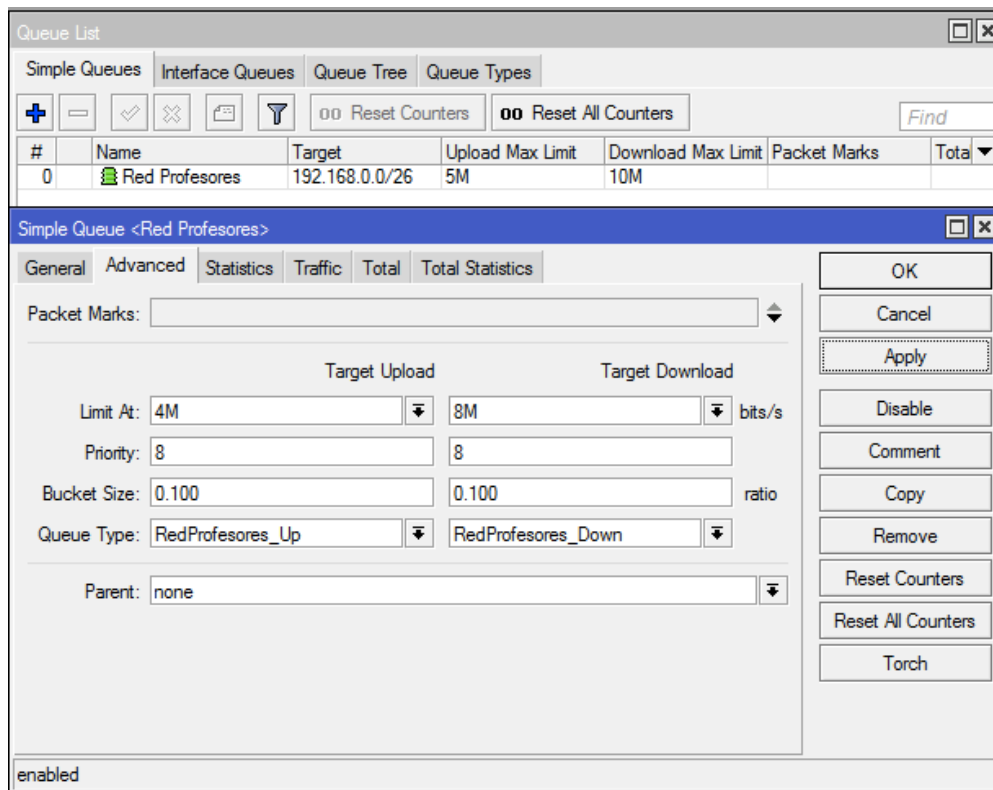


Fig 49.- Simple Queue Subred Profesores con Queue Type
Fuente: Propia

Calidad de servicio

Para asegurar la disponibilidad y el buen uso de los recursos de la red, se diseña una calidad de servicio tomando en cuenta los principales servicios y aplicaciones que circulan por la red de la institución.

En primer lugar, se realiza el marcado de los paquetes, poniendo énfasis en la herramienta de gestión educativa Mikareno, como se muestra en la Figura 50 se crea una lista para posterior tratarla en el marcado de paquetes, además se la da la prioridad más baja, como indica la teoría tratada en capítulos anteriores, de este modo se asegura la fluidez de acceso a la herramienta Mikareno.

Name	Address	Timeout	Creation Time
Mikareno	ues.mikareno.com		Jan/16/2020 00:34:20
::: ues.mikareno.com			
D Mikareno	45.79.90.108		Jan/16/2020 00:34:20
Mikareno	mikareno.com		Jan/15/2020 19:35:49
::: mikareno.com			
D Mikareno	151.101.1.195		Jan/15/2020 19:35:49
::: mikareno.com			
D Mikareno	151.101.65.195		Jan/15/2020 19:35:49

Fig 50.- Lista de direcciones IP de Mikareno
Fuente: Propia

La Figura 51, muestra el marcado de paquetes en el Mangle del Router de Core.

#	Action	Chain	Sr...	D...	Protocol	Src. Port	D...	O...	In. I...	O...	Src. Address List	Dst. Address List	Bytes	Packets
0	add src to address list	forward			17 (udp)	443					!Google		1466.7 KiB	1 125
1	mark packet	forward									Google	Redes Locales	38.5 GiB	31 680 449
2	mark packet	forward									Redes Locales	Google	16.1 MiB	175 905
3	mark packet	forward									Mikareno	Redes Locales	62.3 MiB	51 684
4	mark packet	forward									Redes Locales	Mikareno	179.0 KiB	1 503
5	mark packet	forward									Selarino	Redes Locales	4.8 MiB	3 388
6	mark packet	forward									Redes Locales	Selarino	117.0 KiB	1 807
7	mark packet	forward									Win Update	Redes Locales	26.7 MiB	18 674
8	mark packet	forward									Redes Locales	Win Update	0 B	0
9	mark packet	forward									Redes Netflix	Redes Locales	52.7 GiB	37 953 074
10	mark packet	forward									Redes Locales	Redes Netflix	18.7 MiB	347 595
11	add src to address list	forward			17 (udp)						!Zoom		8.6 KiB	100
12	add src to address list	forward			6 (tcp)						!Zoom		0 B	0
13	mark packet	forward									Zoom	Redes Locales	3435.9 MiB	6 811 752
14	mark packet	forward									Redes Locales	Zoom	1626.1 MiB	3 096 179
15	mark packet	forward									Movistar Play	Redes Locales	300.6 MiB	212 130
16	mark packet	forward									Redes Locales	Movistar Play	7.3 MiB	131 664
17	mark packet	forward			6 (tcp)							Redes Locales	3744.2 MiB	3 368 289
18	mark packet	forward			6 (tcp)						Redes Locales		0 B	0
19	add src to address list	forward			17 (udp)						!Webex		184 B	2
20	mark packet	forward									Webex	Redes Locales	364.9 MiB	1 686 563

Fig 51.- Marcado de paquetes
Fuente: Propia

Por último, en la Figura 52 se detalla el Queue Tree donde se configura la calidad de servicio jerárquico, con nombres y marcas de paquetes, y el parámetro de prioridad.

Name	Parent	Packet Marks	Priority	Limit At (bits/s)	Max Limit (bits/s)	Avg. Rate	Queued Bytes	Bytes	Packets
Download	global		8			32.0 Mbps	0 B	165.9 GiB	179 805 678
Google D	Download	Google_Down	4			0 bps	0 B	37.9 GiB	31 207 552
Mikareno D	Download	Mikareno_Down P	1			0 bps	0 B	62.0 MB	51 394
Movistar Play D	Download	MoviPlay_Down	7			1246.8 kbps	0 B	77.1 MB	54 432
Netflix D	Download	Netflix_Down	7			14.8 Mbps	0 B	52.2 GiB	37 645 444
Otros D	Download	otrosF	8			15.9 Mbps	0 B	68.3 GiB	98 957 486
Selarino D	Download	Selarino_Down P	1			0 bps	0 B	4.8 MB	3 388
Webex D	Download	Webex_Down	2			0 bps	0 B	364.9 MB	1 686 563
Win Update D	Download	Win_Update_Down P	8			0 bps	0 B	26.7 MB	19 674
Winbox D	Download	Winbox_Down	3			0 bps	0 B	3744.2 MB	3 369 289
Zoom	Download	Zoom_Down	2			0 bps	0 B	3435.9 MB	6 811 752
Upload	global		8			904.8 kbps	0 B	1696.2 MB	3 725 146
Google Up	Upload	Google_Up	4			0 bps	0 B	6.5 MB	75 030
Mikareno U	Upload	Mikareno_Up	1			0 bps	0 B	141.4 KiB	1 215
Movistar Play U	Upload	MoviPlay_Up	8			44.9 kbps	0 B	1898.6 KiB	32 603
Netflix U	Upload	Netflix_Up	7			367.0 kbps	0 B	8.5 MB	162 149
Otros U	Upload	otrosF_Up	8			492.8 kbps	0 B	4205.7 KiB	47 105
Selarino U	Upload	Selarino_Up	1			0 bps	0 B	117.0 KiB	1 807
Webex Up	Upload	Webex_Up	2			0 bps	0 B	49.0 MB	309 428
Winbox U	Upload	Winbox_Up	3			0 bps	0 B	0 B	0
Windows U	Upload	Win_Update_Up P	8			0 bps	0 B	0 B	0
Zoom Up	Upload	Zoom_Up	2			0 bps	0 B	1626.1 MB	3 096 179

Fig 52.- Queue Tree
Fuente: Propia

4.3 Pruebas del sistema

Comenzaremos por recordar que en el apartado del diseño de la red se plantea adoptar el modelo jerárquico de Cisco y puntualmente el de núcleo fusionado, por tal razón las pruebas de conectividad realizadas en el presente capítulo se basan en cumplir las funciones de la fase de núcleo – distribución y acceso que se detallan a continuación.

Pruebas de conectividad a nivel WAN

La conectividad WAN hacia la red del proveedor de Internet de la UES, se la realiza mediante la configuración de una IP pública sobre una interface del router de Core. Para efectos didácticos y emulación se ha configurado un DHCP cliente sobre la interface ether8-WAN como se observa en la Figura 53.

Interface	Use P...	Add D...	IP Address	Expires After	Status
ether8-wan	yes	yes	192.168.35.208/24	23:54:46	bound

Fig 53. Conectividad WAN
Fuente: Propia

En la Figura 54 podemos comprobar la conectividad hacia Internet mediante el uso del terminal de RouterOS del Router de Core, puntualmente haciendo un ping a www.google.com.

```
[admin@Core] > ping www.google.com
SEQ HOST                               SIZE TTL TIME  STATUS
  0 172.217.15.196                       56  53 113ms
  1 172.217.15.196                       56  53 137ms
  2 172.217.15.196                       56  53 146ms
  3 172.217.15.196                       56  53 110ms
  4 172.217.15.196                       56  53 107ms
  5 172.217.15.196                       56  53 149ms
  6 172.217.15.196                       56  53 120ms
  7 172.217.15.196                       56  53 148ms
  8 172.217.15.196                       56  53 111ms
  9 172.217.15.196                       56  53 111ms
 10 172.217.15.196                       56  53 109ms
 11 172.217.15.196                       56  53 122ms
 12 172.217.15.196                       56  53 134ms
sent=13 received=13 packet-loss=0% min-rtt=107ms avg-rtt=124ms
max-rtt=149ms
```

Fig 54. Prueba de conectividad hacia Internet
Fuente: Propia

Pruebas de conectividad a nivel LAN

Para confirmar la conectividad a nivel LAN entre el Router de Core y los routers de cada departamento, RouterOS ofrece acceder a la lista de vecinos donde se pueden observar los RouterBoards de la subred de Profesores, Laboratorio de Inglés y Computación, Administración y Rectorado, como se muestra en la Figura 55.

Interface	IP Address	MAC Address	Identity	Platform	Version	Board Name	Interface Name
ether1	172.16.0.2	0C:45:95:E8:91:00	RB Profesores	MikroTik	6.44.6 (lo...)	CHR	ether1
ether2	172.16.0.3	0C:45:95:16:D9:00	RB-Lab1	MikroTik	6.44.6 (lo...)	CHR	ether1
ether3	172.16.0.4	0C:45:95:E6:23:00	RB-Lab2	MikroTik	6.44.6 (lo...)	CHR	ether1
ether4	172.16.0.5	0C:45:95:5E:8B:00	RB-Administracion	MikroTik	6.44.6 (lo...)	CHR	ether1
ether5	172.16.0.6	0C:45:95:6F:AE:00	RB-Rectorado	MikroTik	6.44.6 (lo...)	CHR	ether1
ether8-wan	192.168.35.1	B8:69:F4:1D:C8:E5	CASA JS	MikroTik	6.44.6 (lo...)	RB952Ui-5ac2nD	bridge1/wlan1-2G
vlan10-1		0C:45:95:E8:91:00	RB Profesores	MikroTik	6.44.6 (lo...)	CHR	local/vlan10
vlan20-2		0C:45:95:16:D9:00	RB-Lab1	MikroTik	6.44.6 (lo...)	CHR	local/vlan20
vlan30-3		0C:45:95:E6:23:00	RB-Lab2	MikroTik	6.44.6 (lo...)	CHR	local/vlan30
vlan40-4		0C:45:95:5E:8B:00	RB-Administracion	MikroTik	6.44.6 (lo...)	CHR	local/vlan40
vlan50-5		0C:45:95:6F:AE:00	RB-Rectorado	MikroTik	6.44.6 (lo...)	CHR	local/vlan50

Fig 55.- Conectividad LAN
Fuente: Propia

Las Figura 56, 57, 58, 59 y 60, muestra las pruebas de conectividad mediante la herramienta ping, entre el Router de Core y cada router de las diferentes subredes de la red como RouterBoar Profesores, Laboratorio 1, Laboratorio 2, Administración y Rectorado respectivamente.

```
[admin@Core] > ping 172.16.0.2
SEQ HOST                                SIZE TTL TIME  STATUS
 0 172.16.0.2                            56 64 7ms
 1 172.16.0.2                            56 64 7ms
 2 172.16.0.2                            56 64 5ms
 3 172.16.0.2                            56 64 7ms
 4 172.16.0.2                            56 64 7ms
 5 172.16.0.2                            56 64 5ms
 6 172.16.0.2                            56 64 6ms
 7 172.16.0.2                            56 64 4ms
 8 172.16.0.2                            56 64 5ms
 9 172.16.0.2                            56 64 4ms
10 172.16.0.2                            56 64 4ms
11 172.16.0.2                            56 64 4ms
12 172.16.0.2                            56 64 7ms
13 172.16.0.2                            56 64 5ms
14 172.16.0.2                            56 64 5ms
15 172.16.0.2                            56 64 4ms
16 172.16.0.2                            56 64 5ms
17 172.16.0.2                            56 64 5ms
sent=18 received=18 packet-loss=0% min-rtt=4ms avg-rtt=5ms max-rtt=7ms
```

Fig 56.- Prueba de conectividad a RouterBoard Profesores
Fuente: Propia

```
[admin@Core] > ping 172.16.0.3
SEQ HOST                                SIZE TTL TIME  STATUS
 0 172.16.0.3                            56 64 9ms
 1 172.16.0.3                            56 64 4ms
 2 172.16.0.3                            56 64 4ms
 3 172.16.0.3                            56 64 3ms
 4 172.16.0.3                            56 64 3ms
 5 172.16.0.3                            56 64 5ms
 6 172.16.0.3                            56 64 3ms
 7 172.16.0.3                            56 64 4ms
 8 172.16.0.3                            56 64 4ms
 9 172.16.0.3                            56 64 5ms
10 172.16.0.3                            56 64 5ms
11 172.16.0.3                            56 64 3ms
12 172.16.0.3                            56 64 4ms
13 172.16.0.3                            56 64 3ms
14 172.16.0.3                            56 64 4ms
15 172.16.0.3                            56 64 4ms
16 172.16.0.3                            56 64 3ms
17 172.16.0.3                            56 64 3ms
18 172.16.0.3                            56 64 4ms
19 172.16.0.3                            56 64 4ms
sent=20 received=20 packet-loss=0% min-rtt=3ms avg-rtt=4ms max-rtt=9ms
```

Fig 57.- Prueba de conectividad a RouterBoard Laboratorio 1
Fuente: Propia

```
[admin@Core] > ping 172.16.0.4
SEQ HOST                SIZE TTL TIME STATUS
0 172.16.0.4            56 64 26ms
1 172.16.0.4            56 64 4ms
2 172.16.0.4            56 64 6ms
3 172.16.0.4            56 64 5ms
4 172.16.0.4            56 64 3ms
5 172.16.0.4            56 64 5ms
6 172.16.0.4            56 64 9ms
7 172.16.0.4            56 64 5ms
8 172.16.0.4            56 64 6ms
9 172.16.0.4            56 64 6ms
10 172.16.0.4           56 64 6ms
11 172.16.0.4           56 64 6ms
12 172.16.0.4           56 64 6ms
13 172.16.0.4           56 64 4ms
14 172.16.0.4           56 64 15ms
15 172.16.0.4           56 64 5ms
16 172.16.0.4           56 64 4ms
17 172.16.0.4           56 64 5ms
sent=18 received=18 packet-loss=0% min-rtt=3ms avg-rtt=7ms max-rtt=26ms
```

Fig 58.- Prueba de conectividad a RouterBoard Laboratorio 2

Fuente: Propia

```
[admin@Core] > ping 172.16.0.5
SEQ HOST                SIZE TTL TIME STATUS
0 172.16.0.5            56 64 30ms
1 172.16.0.5            56 64 5ms
2 172.16.0.5            56 64 6ms
3 172.16.0.5            56 64 7ms
4 172.16.0.5            56 64 5ms
5 172.16.0.5            56 64 6ms
6 172.16.0.5            56 64 5ms
7 172.16.0.5            56 64 15ms
8 172.16.0.5            56 64 8ms
9 172.16.0.5            56 64 14ms
10 172.16.0.5           56 64 7ms
11 172.16.0.5           56 64 6ms
12 172.16.0.5           56 64 6ms
13 172.16.0.5           56 64 4ms
14 172.16.0.5           56 64 4ms
15 172.16.0.5           56 64 5ms
16 172.16.0.5           56 64 4ms
17 172.16.0.5           56 64 5ms
sent=18 received=18 packet-loss=0% min-rtt=4ms avg-rtt=7ms max-rtt=30ms
```

Fig 59.- Prueba de conectividad a RouterBoard Administración

Fuente: Propia

```
[admin@Core] > ping 172.16.0.6
SEQ HOST                SIZE TTL TIME STATUS
0 172.16.0.6            56 64 47ms
1 172.16.0.6            56 64 5ms
2 172.16.0.6            56 64 8ms
3 172.16.0.6            56 64 5ms
4 172.16.0.6            56 64 5ms
5 172.16.0.6            56 64 4ms
6 172.16.0.6            56 64 4ms
7 172.16.0.6            56 64 7ms
8 172.16.0.6            56 64 6ms
9 172.16.0.6            56 64 5ms
10 172.16.0.6           56 64 6ms
11 172.16.0.6           56 64 10ms
12 172.16.0.6           56 64 6ms
13 172.16.0.6           56 64 5ms
14 172.16.0.6           56 64 5ms
15 172.16.0.6           56 64 5ms
16 172.16.0.6           56 64 4ms
sent=17 received=17 packet-loss=0% min-rtt=4ms avg-rtt=8ms max-rtt=47ms
```

Fig 60.- Prueba de conectividad a RouterBoard Rectorado

Fuente: Propia

Pruebas de conectividad a dispositivos finales

Es necesario comprobar que los hosts tomen direcciones IP de forma automática, para esto, RouterOS cuenta con una lista Leases donde muestra la dirección IP que entregó a los dispositivos dentro de cada servidor DHCP por cada VLAN, además de informar sobre otros parámetros, tal como muestra la Figura 61.

	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address	Active Host ...	Expires After	Status
D	192.168.0.59	0C:45:95:A0:83:00	1:c:45:95:a0:83:0	dhcp1-profesores	192.168.0.59	0C:45:95:A0:83:00	box	00:07:32	bound
D	192.168.0.60	00:50:79:66:68:02	1:0:50:79:66:68:2	dhcp1-profesores	192.168.0.60	00:50:79:66:68:02	PC41	00:09:00	bound
D	192.168.0.61	00:50:79:66:68:01	1:0:50:79:66:68:1	dhcp1-profesores	192.168.0.61	00:50:79:66:68:01	PC31	00:08:23	bound
D	192.168.0.62	00:50:79:66:68:00	1:0:50:79:66:68:0	dhcp1-profesores	192.168.0.62	00:50:79:66:68:00	PC21	00:07:37	bound
D	192.168.0.125	00:50:79:66:68:04	1:0:50:79:66:68:4	dhcp2-lab1	192.168.0.125	00:50:79:66:68:04	PC301	00:08:56	bound
D	192.168.0.126	00:50:79:66:68:03	1:0:50:79:66:68:3	dhcp2-lab1	192.168.0.126	00:50:79:66:68:03	PC11	00:08:41	bound
D	192.168.0.189	00:50:79:66:68:06	1:0:50:79:66:68:6	dhcp3-lab2	192.168.0.189	00:50:79:66:68:06	PC61	00:09:10	bound
D	192.168.0.190	00:50:79:66:68:05	1:0:50:79:66:68:5	dhcp3-lab2	192.168.0.190	00:50:79:66:68:05	PC51	00:09:03	bound
D	192.168.0.221	00:50:79:66:68:08	1:0:50:79:66:68:8	dhcp4-administracion	192.168.0.221	00:50:79:66:68:08	PC81	00:09:39	bound
D	192.168.0.222	00:50:79:66:68:07	1:0:50:79:66:68:7	dhcp4-administracion	192.168.0.222	00:50:79:66:68:07	PC71	00:09:30	bound
D	192.168.0.253	00:50:79:66:68:09	1:0:50:79:66:68:9	dhcp5-rectorado	192.168.0.253	00:50:79:66:68:09	PC91	00:09:24	bound
D	192.168.0.254	00:50:79:66:68:0A	1:0:50:79:66:68:a	dhcp5-rectorado	192.168.0.254	00:50:79:66:68:0A	PC101	00:09:18	bound

Fig 61.- Prueba de conectividad a VPCS
Fuente: Propia

Para comprobar la conectividad desde el Router de Core a los dispositivos finales de la red listados en la Figura 61, utilizamos la herramienta ping de RouterOS. Las Figuras 62, 63, 64, 65 y 66 muestran la conectividad hacia los dispositivos finales de la subred Profesores, Laboratorio 1, Laboratorio 2, Administración y Rectorado respectivamente.

```
[admin@Core] > ping 192.168.0.60
SEQ HOST                                SIZE TTL TIME STATUS
0 192.168.0.60                          56 64 22ms
1 192.168.0.60                          56 64 6ms
2 192.168.0.60                          56 64 7ms
3 192.168.0.60                          56 64 7ms
4 192.168.0.60                          56 64 8ms
5 192.168.0.60                          56 64 7ms
6 192.168.0.60                          56 64 7ms
7 192.168.0.60                          56 64 7ms
8 192.168.0.60                          56 64 10ms
9 192.168.0.60                          56 64 6ms
10 192.168.0.60                         56 64 5ms
sent=11 received=11 packet-loss=0% min-rtt=5ms avg-rtt=8ms max-rtt=22ms
```

Fig 62.- Prueba de conectividad a un dispositivo de la subred Profesores
Fuente: Propia

```
[admin@Core] > ping 192.168.0.125
SEQ HOST                                SIZE TTL TIME  STATUS
0 192.168.0.125                          56 64 23ms
1 192.168.0.125                          56 64 26ms
2 192.168.0.125                          56 64 9ms
3 192.168.0.125                          56 64 8ms
4 192.168.0.125                          56 64 8ms
5 192.168.0.125                          56 64 7ms
6 192.168.0.125                          56 64 10ms
7 192.168.0.125                          56 64 9ms
8 192.168.0.125                          56 64 7ms
9 192.168.0.125                          56 64 8ms
sent=10 received=10 packet-loss=0% min-rtt=7ms avg-rtt=11ms max-rtt=26ms
```

Fig 63.- Prueba de conectividad a un dispositivo de la subred Laboratorio 1
Fuente: Propia

```
[admin@Core] > ping 192.168.0.189
SEQ HOST                                SIZE TTL TIME  STATUS
0 192.168.0.189                          56 64 21ms
1 192.168.0.189                          56 64 9ms
2 192.168.0.189                          56 64 8ms
3 192.168.0.189                          56 64 9ms
4 192.168.0.189                          56 64 8ms
5 192.168.0.189                          56 64 7ms
6 192.168.0.189                          56 64 8ms
7 192.168.0.189                          56 64 8ms
8 192.168.0.189                          56 64 7ms
9 192.168.0.189                          56 64 9ms
10 192.168.0.189                         56 64 8ms
11 192.168.0.189                         56 64 8ms
sent=12 received=12 packet-loss=0% min-rtt=7ms avg-rtt=9ms max-rtt=21ms
```

Fig 64.- Prueba de conectividad a un dispositivo de la subred Laboratorio 2
Fuente: Propia

```
[admin@Core] > ping 192.168.0.221
SEQ HOST                                SIZE TTL TIME  STATUS
0 192.168.0.221                          56 64 23ms
1 192.168.0.221                          56 64 7ms
2 192.168.0.221                          56 64 13ms
3 192.168.0.221                          56 64 8ms
4 192.168.0.221                          56 64 8ms
5 192.168.0.221                          56 64 10ms
6 192.168.0.221                          56 64 13ms
7 192.168.0.221                          56 64 24ms
8 192.168.0.221                          56 64 9ms
9 192.168.0.221                          56 64 8ms
10 192.168.0.221                         56 64 7ms
sent=11 received=11 packet-loss=0% min-rtt=7ms avg-rtt=11ms max-rtt=24ms
```

Fig 65.- Prueba de conectividad a un dispositivo de la subred Administración
Fuente: Propia

```
[admin@Core] > ping 192.168.0.253
SEQ HOST                                SIZE TTL TIME  STATUS
0 192.168.0.253                          56 64 17ms
1 192.168.0.253                          56 64 6ms
2 192.168.0.253                          56 64 7ms
3 192.168.0.253                          56 64 6ms
4 192.168.0.253                          56 64 8ms
5 192.168.0.253                          56 64 7ms
6 192.168.0.253                          56 64 7ms
7 192.168.0.253                          56 64 9ms
8 192.168.0.253                          56 64 9ms
9 192.168.0.253                          56 64 7ms
10 192.168.0.253                         56 64 8ms
sent=11 received=11 packet-loss=0% min-rtt=6ms avg-rtt=8ms max-rtt=17ms
```

Fig 66.- Prueba de conectividad a un dispositivo de la subred Rectorado
Fuente: Propia

Pruebas de navegación

Las pruebas de conectividad realizadas desde las VPCS o dispositivos finales en el presente diseño se detallan a continuación.

Como se puede observar en la Figura 67, la VPCS de la subred profesores toma dirección IP, máscara, gateway y DNS, por consiguiente, se ejecuta un ping hacia el dominio www.google.com, con lo que se concluye que el dispositivo tiene conectividad a Internet.

```
PC2 - PuTTY
PC2> show ip
NAME           : PC2 [1]
IP/MASK        : 192.168.0.62/26
GATEWAY        : 192.168.0.1
DNS            : 192.168.0.1
DHCP SERVER    : 192.168.0.1
DHCP LEASE     : 384, 600/300/525
MAC            : 00:50:79:66:68:00
LPORT         : 10076
RHOST:PORT    : 127.0.0.1:10077
MTU           : 1500

PC2> ping www.google.com
www.google.com resolved to 172.217.1.100
84 bytes from 172.217.1.100 icmp_seq=1 ttl=51 time=100.680 ms
84 bytes from 172.217.1.100 icmp_seq=2 ttl=51 time=124.722 ms
84 bytes from 172.217.1.100 icmp_seq=3 ttl=51 time=126.776 ms
84 bytes from 172.217.1.100 icmp_seq=4 ttl=51 time=127.175 ms
84 bytes from 172.217.1.100 icmp_seq=5 ttl=51 time=121.302 ms
PC2> █
```

Fig 67.- Pruebas de conectividad desde un dispositivo de la red Profesores
Fuente: Propia

Para realizar una prueba de navegación desde un dispositivo final, es necesario instalar Firefox Appliance que ofrece GNS3 detallados en el ANEXO 4. INSTALACION DE FIREFOX APPLIANCE. En la Figura 68, se demuestra que el nodo Navegador tiene acceso a Internet por lo que se realiza una prueba de velocidad en el sitio www.speedtest.net.

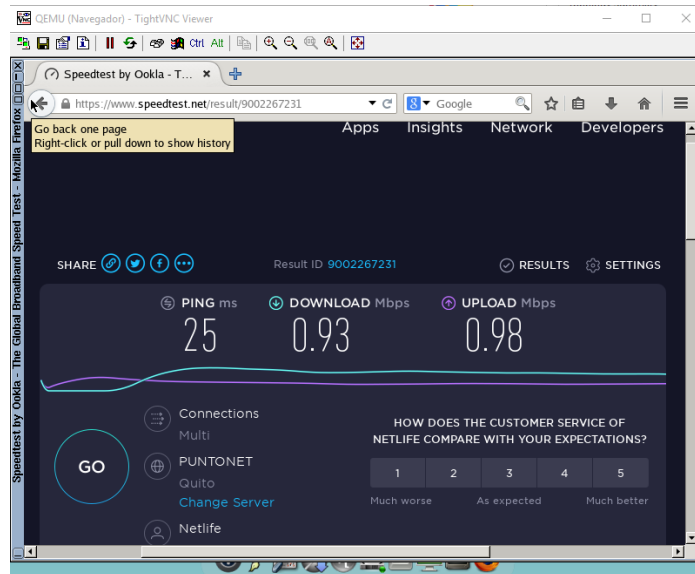


Fig 68.- Prueba de acceso a Internet
Fuente: Propia

Pruebas de marcado de paquetes

Para comprobar que las reglas del marcado de paquetes en el Mangle se encuentren ejecutando, primero se debe verificar que en la lista Mikareno se encuentren listadas las IPs del dominio ues.mikareno.com, como se muestra en la Figura 69.

Name	Address	Tim...	Creation Time
Mikareno	ues.mikareno.com		Jan/16/2020 00:34:20
::: ues.mikareno.com			
D Mikareno	45.79.90.108		Feb/02/2020 09:44:12
Mikareno	mikareno.com		Jan/15/2020 19:35:49
::: mikareno.com			
D Mikareno	151.101.1.195		Feb/02/2020 09:44:12
::: mikareno.com			
D Mikareno	151.101.65.195		Feb/02/2020 09:44:12

Fig 69.- Lista de acceso Mikareno
Fuente: Propia

A continuación, en el QEMU Navegador, acceder al sitio <https://ues.mikareno.com> como se observa en la Figura 70.

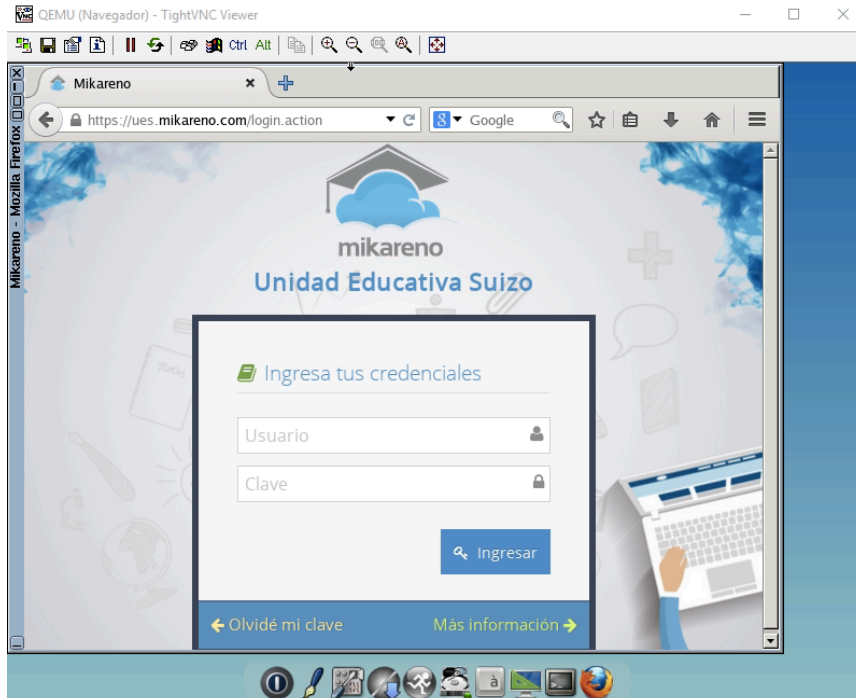


Fig 70.- Prueba de acceso a Mikareno
Fuente: Propia

Finalmente, la Figura 71 indica que las dos reglas para la plataforma de gestión educativa Mikareno cuentan Bytes y Packets, concluyendo que el marcado de paquetes está actuando como de acuerdo a su diseño.

#	Action	Chain	Sr...	D...	Protocol	Src. Port	D...	O...	In. I...	O...	Src. Address List	Dst. Address List	Bytes	Packets
:::	Mikareno Down										Mikareno	Redes Locales	62.3 MiB	51 684
3	mark packet	forward									Mikareno	Redes Locales	62.3 MiB	51 684
:::	Mikareno Up										Redes Locales	Mikareno	179.0 KiB	1 503
4	mark packet	forward									Redes Locales	Mikareno	179.0 KiB	1 503
:::	Selarino Down										Selarino	Redes Locales	4.8 MiB	3 388
5	mark packet	forward									Selarino	Redes Locales	4.8 MiB	3 388
:::	Selarino Up										Redes Locales	Selarino	117.0 KiB	1 807
6	mark packet	forward									Redes Locales	Selarino	117.0 KiB	1 807

Fig 71.- Marcado de paquetes para Mikareno
Fuente: Propia

Pruebas de Calidad de Servicio

Una vez que el marcado de paquetes se encuentra ejecutando, es posible observar en el Queue Tree que la calidad de servicio de Mikareno con prioridad 1, registra una tasa promedio de 1013Kbps y a la vez almacena los Bytes y Packets como muestra la Figura 72.

Name	Parent	Packet Marks	Priority	Limit A...	Max Li...	Avg. Rate	Queued Bytes	Bytes	Packets
Download	global		8			1016.7 kbps	0 B	167.3 GiB	180 876 527
Google D	Download	Google_Down	4			0 bps	0 B	38.5 GiB	31 694 502
Mikareno D	Download	Mikareno_Down P	1			1013.0 kbps	0 B	67.6 MiB	55 716

Fig 72.- Calidad de Servicio para Mikareno
Fuente: Propia

Pruebas de control de velocidad

La Figura 73, muestra el diseño de las colas simples por las redes de cada departamento de la red de datos de la UES.

#	Name	Target	Upload Max Li...	Download Max Limit
0	Red Profesores	192.168.0.0/26	5M	10M
1	Red Laboratorio 1	192.168.0.64/26	5M	10M
2	Red Laboratorio 2	192.168.0.128/26	5M	10M
3	Red Administracion	192.168.0.192/27	5M	10M
4	Red Rectorado	192.168.0.224/27	5M	10M

Fig 73.- Simple Queue de subredes
Fuente: Propia

Para ejecutar una prueba de saturación de la cola simple de la subred Profesores y por temas didácticos de emulación se modifica el campo de Download Max Limit y Upload Max Limit a 1Mbps. A continuación, se ejecuta una prueba de velocidad desde el appliance Navegador y como se observa en la Figura 74 la capacidad máxima es de 1Mbps saturando la cola simple.

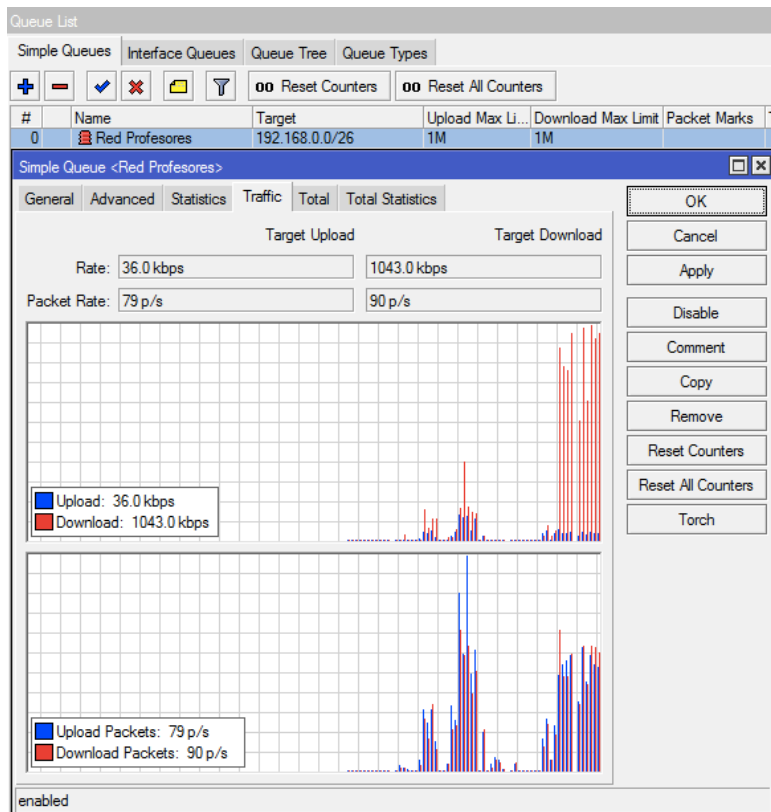


Fig 74.- Saturación Simple Queue Profesores
Fuente: Propia

Adicional a las pruebas anteriores, se ejecuta la herramienta Torch sobre la vlan10-1 que representa a la red de Profesores, con lo que se observa que el tráfico, en este caso, de la prueba de velocidad realizada, fue ejecutada desde el dispositivo con dirección IP 192.168.0.59, como se indica en la Figura 75.

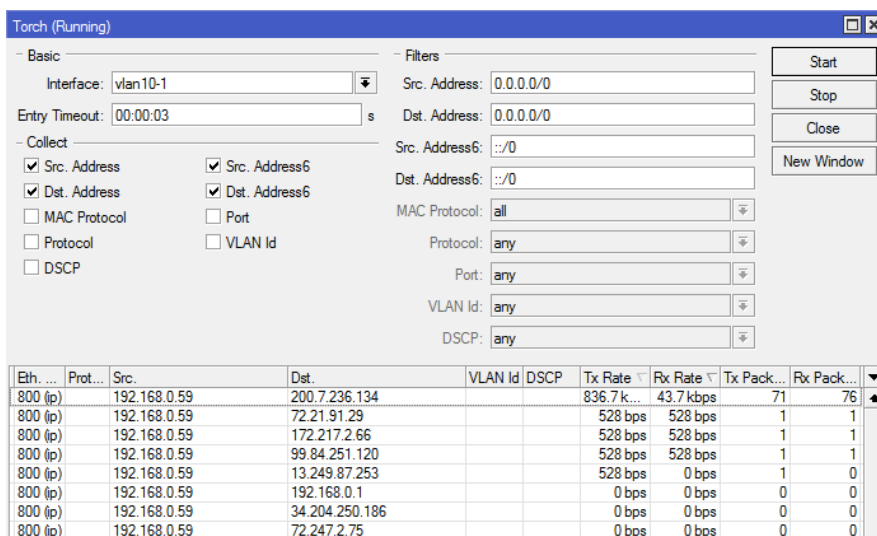


Fig 75.- Torch sobre vlan-10 Profesores
Fuente: Propia

Monitor de servicios

Finalmente, es importante incorporar una herramienta útil para el monitoreo del tráfico de la red, para lo cual se diseña un Webfig skin (Mikrotik, 2019) dentro del sistema operativo RouterOS que permite visualizar el tráfico de los servicios priorizados anteriormente dentro del Mangle, como se muestran en las Figuras 76 y 77.

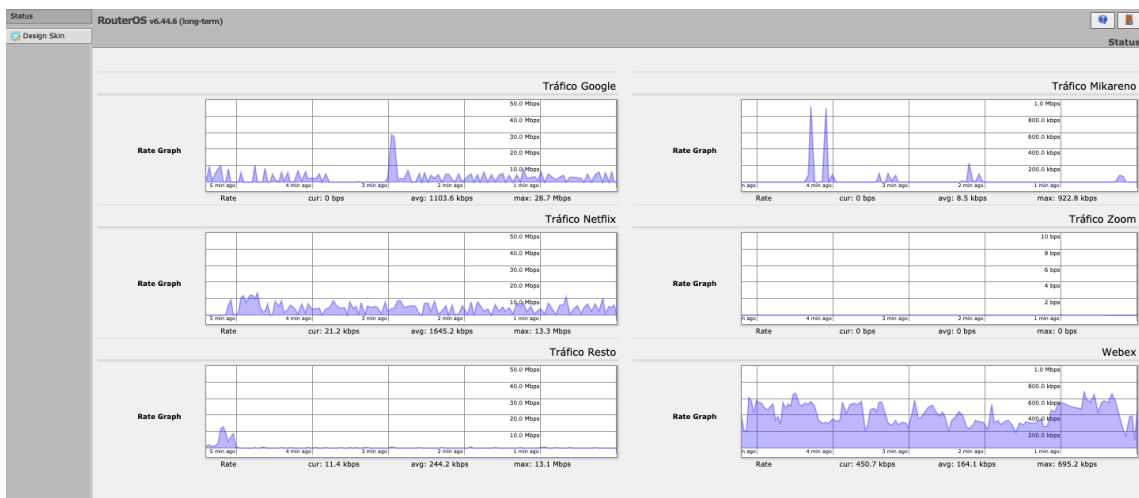


Fig 76. Monitor de servicios 1
Fuente: Propia

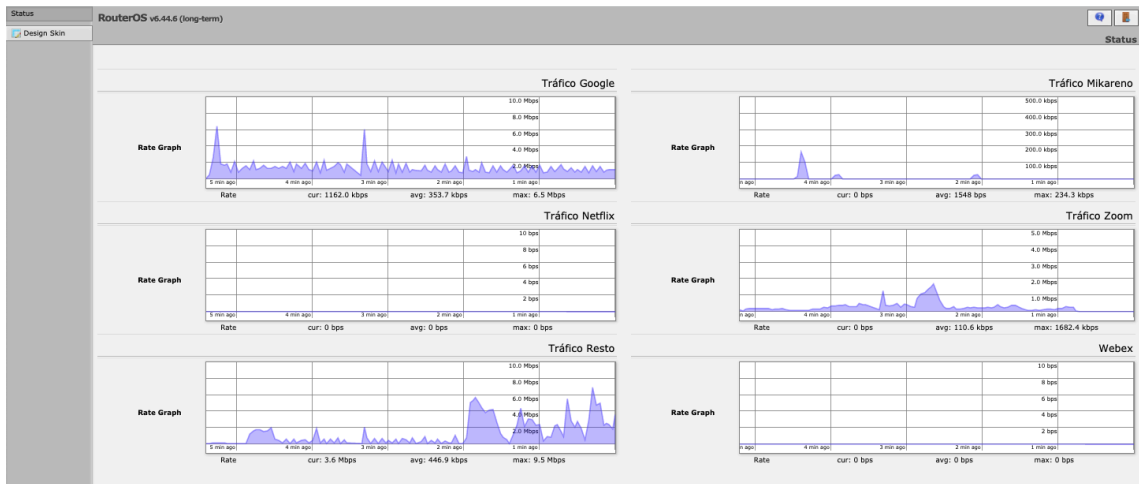


Fig 77. Monitor de servicios 2
Fuente: Propia

5 CONCLUSIONES Y RECOMENDACIONES

5.1 Conclusiones

Una vez concluido el diseño del presente trabajo de investigación se exponen las siguientes conclusiones:

A través del análisis de tráfico se logra identificar los servicios que circulan por la red y principalmente se puede concluir que mediante la priorización de servicios se logra minimizar la vulnerabilidad a la que está expuesto el personal de la Unidad Educativa Suizo como es la afectación del acceso a la plataforma de gestión educativa Mikareno en momentos de saturación de la red de datos.

En virtud al estudio de las ventajas de la utilización de VLANs en una red de datos, se concluye que mediante la segmentación se logra dividir y agrupar a los hosts por cada departamento con un distinto direccionamiento de red, de este modo, el diseño resulta efectivo para la administración y gestión del direccionamiento IP de cada subred y para la implementación de las políticas para cada subred.

Por medio del estudio del modelo jerárquico de tres capas realizado en el Capítulo 3, en base al volumen de la infraestructura de red de la Unidad Educativa Suizo y a las especificaciones técnicas del Router de Core con respecto a su hardware y sistema operativo, se concluye que el modelo aplicado en el diseño de dos capas o núcleo fusionado es el adecuado ya que el equipo antes mencionado logra cumplir la conectividad con el Internet y con los equipos de acceso.

Gracias al estudio y diseño de un modelo de calidad de servicio con manejo de prioridades dentro del Queue Tree de RouterOS, es importante concluir que para asegurar que el flujo

de datos hacia la plataforma de gestión educativa Mikareno previamente marcados dentro Mangle circulen en momentos de saturación, tiene que ser asignado con la mayor prioridad equivalente al valor 1, mientras que al resto de flujos de tráfico con valores de menor prioridad.

A través del estudio de la disciplina de encolamiento propietaria de Mikrotik `pcq-rate=0`, se concluye que en momentos de saturación de una cola simple la disciplina mencionada se ejecuta y divide de una forma equitativa el valor máximo configurado en la cola simple para el número de dispositivos concurrentes de cada VLAN o segmento de red.

En base al análisis de las pruebas del diseño realizadas en GNS3, se comprueba que el diseño permite la conectividad a los dispositivos de red a nivel WAN y LAN, en base a las capas de núcleo y distribución. Además, se puede concluir que el modelo de calidad de servicio diseñado ejecuta la priorización de servicios por medio del registro del flujo de tráfico de las reglas del marcado de paquetes en el Mangle, a través del incremento de número de bytes y paquetes en las disciplinas de encolamiento y mediante la saturación de los valores máximos en el Queue Tree.

Finalmente, es valioso comentar que debido a la actual pandemia mundial que derivó en una cuarentena obligatoria que ocasionó una saturación considerable en varias redes de datos, se puede concluir que el diseño planteado ofrece escalabilidad, ya que a través de un estudio previo para el marcado del tráfico de Zoom, se logró agregar la priorización del flujo de datos de la plataforma de reuniones virtuales mencionada al convertirse en una herramienta tecnológica primordial para el acceso a clases virtuales de instituciones educativas como para el desarrollo de teletrabajo.

5.2 Recomendaciones

Posterior a la ejecución del presente diseño, se recomienda implementar un sistema de autenticación de dispositivos a la red mediante un servidor HotSpot propietario del sistema operativo RouterOS de Mikrotik.

Para el correcto funcionamiento de la actual red inalámbrica de la UES es importante recomendar mantener un cronograma de ejecución de un análisis del desempeño de la red inalámbrica, mediante el uso de herramientas que permitan ejecutar pruebas de cobertura inalámbrica, frecuencias usadas y mapas de calor.

En caso de que se requiera emular las pruebas de saturación de las colas simples a una capacidad mayor a 1Mbit, se recomienda actualizar la licencia del CHR de Free a P1 para aumentar la capacidad de todas las interfaces a 1Gbit.

Para la identificación y marcado de tráfico en el Mangle de RouterOS no existen un método específico, por lo que se recomienda el uso de las diferentes cadenas como métodos: puertos, interfaces, protocolos, listas de IPs y finalmente la acción a realizar.

Con respecto a los recursos del computador para la emulación del diseño en GNS3, se aconseja ejecutarlo en un terminal con un procesador Core i5 y al menos 4GB de RAM para evitar la saturación del consumo de CPU y memoria cuando se ejecuta la emulación total de toda la red.

Designar un administrador de red que cumpla funciones como la actualización de versión del sistema operativo de los equipos Mikrotik, manejo de backup de todos los routers, gestión en el registro de los usuarios y dispositivos en la red, análisis de las gráficas de

consumo de cada departamento de la institución y gestión de eventos que se generen en la red de datos.

Se sugiere realizar un análisis técnico económico para ejecutar una migración de la red de núcleo fusionado mediante fibra óptica, ya que tanto el Router de Core como los routers de cada departamento que se incluyen en el presente diseño cuentan con un puerto óptico que ofrece una conectividad mediante ese medio.

6 Bibliografía

- MINISTERIO DE EDUCACION DEL ECUADOR. (11 de Diciembre de 2016). ACUERDO Nro. MINEDUC-ME-2016-00122-A. Quito, Pichincha, Ecuador.
- GNS3. (18 de Junio de 2019). *GNS3 installation on MacOS X*. Obtenido de <https://docs.gns3.com/1MIG-VjKfQVEDVwGMxE3sJ15eU2KTDsktnZZH8HSR-IQ/index.html#h.58r8c4xfogtu>
- Wireshark. (23 de Octubre de 2019). *Wireshark User's Guide*. Obtenido de https://www.wireshark.org/docs/wsug_html_chunked/
- MIKROTIK. (14 de January de 2017). *Wiki Mikrotik*. Obtenido de https://wiki.mikrotik.com/wiki/NetworkPro_on_Quality_of_Service
- MIKROTIK. (19 de Octubre de 2018). *Wiki Mikrotik*. Obtenido de <https://wiki.mikrotik.com/wiki/Manual:Interface/VLAN>
- Mikareno. (2019). *Mikareno, plataforma de gestión educativa y administrativa K-12*. Obtenido de www.mikareno.com
- Neumann, J. C. (2015). THE BOOK OF GNS3. En J. C. Neumann, *THE BOOK OF GNS3* (págs. 1-6).
- diseño, R. d. (Abril de 2013). Obtenido de CCNA EXPLORATION 3 V: https://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/en-05_campus-wireless_wp_cte_es-xl_42333.pdf
- (Abril de 2014). Obtenido de Cisco System Inc: https://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/en-05_campus-wireless_wp_cte_es-xl_42333.pdf
- Fonquernie, A. (23 de Enero de 2013). Obtenido de <https://fonquernie.wordpress.com/2013/01/23/vlan-definicion-y-montaje-de-una-red-virtual/>
- Dobladez, M. (Febrero de 2019). MTCTCE. Rio Cuarto, Córdoba, Argentina.
- Mikrotik. (1 de Marzo de 2019). *Wiki Mikrotik*. Obtenido de https://wiki.mikrotik.com/wiki/Manual:Tools/Speed_Test
- Mikrotik. (01 de Febrero de 2019). *Wiki Mikrotik*. Obtenido de <https://wiki.mikrotik.com/wiki/Manual:Webfig>
- Mikrotik. (22 de April de 2019). *Wiki Mikrotik*. Obtenido de <https://wiki.mikrotik.com/wiki/Manual:HTB>
- Mikrotik. (3 de Diciembre de 2018). *Wiki Mikrotik*. Obtenido de https://wiki.mikrotik.com/wiki/Manual:Tools/Bandwidth_Test#Bandwidth_Test_Server

Mikrotik. (19 de Octubre de 2018). *Mikrotik Wiki*. Obtenido de <https://wiki.mikrotik.com/wiki/Manual:Interface/VLAN>

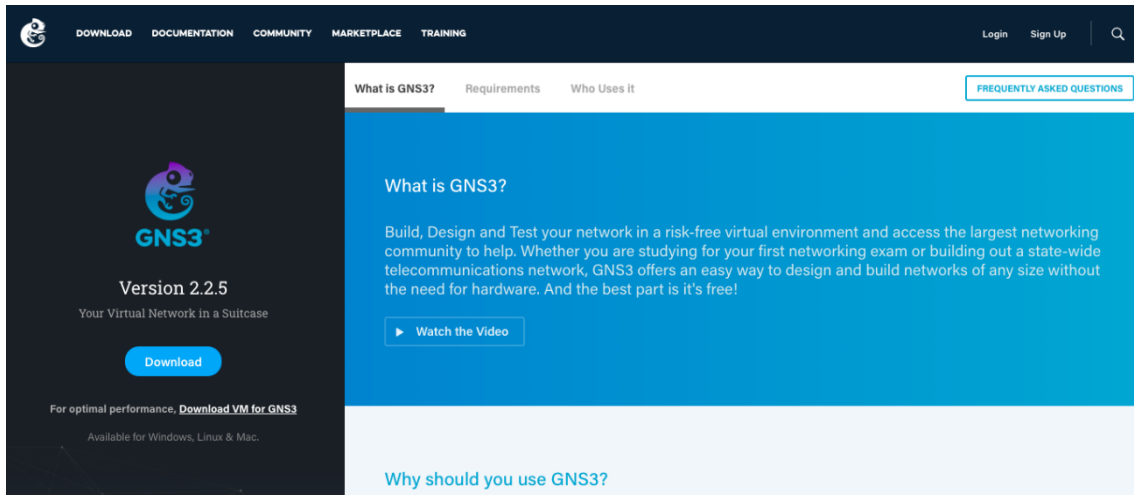
Salazar Chacón, G., & Chafía Altamirano, G. (2015). EMPLEO DE PATH-CONTROL TOOLS EN UNA RED EMPRESARIAL MODERNA MEDIANTE POLITICAS DE ENRUTAMIENTO. *EC Tecnología- Glosas De Innovación Aplicadas a La Pyme*, 4(1), 1 -18. Recuperado a partir de <http://ojs.3ciencias.com/index.php/3c-tecnologia/article/view/233>

E.F. Naranjo and G. D. Salazar Ch, "Underlay and overlay networks: The approach to solve addressing and segmentation problems in the new network era: VXLAN encapsulation with Cisco and open source networks," 2017 IEEE Second Ecuador Technical Chapters Meeting (ETCM), Salinas, 2017, pp 1-6

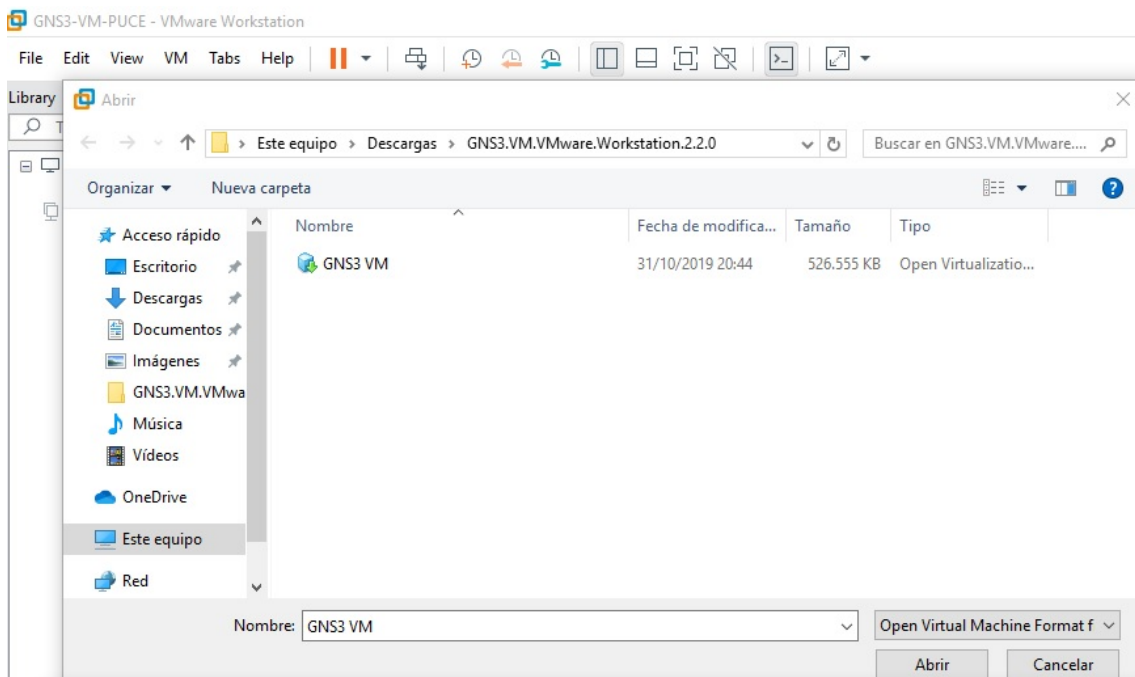
7 ANEXOS

ANEXO 1. INSTALACION DE GNS3

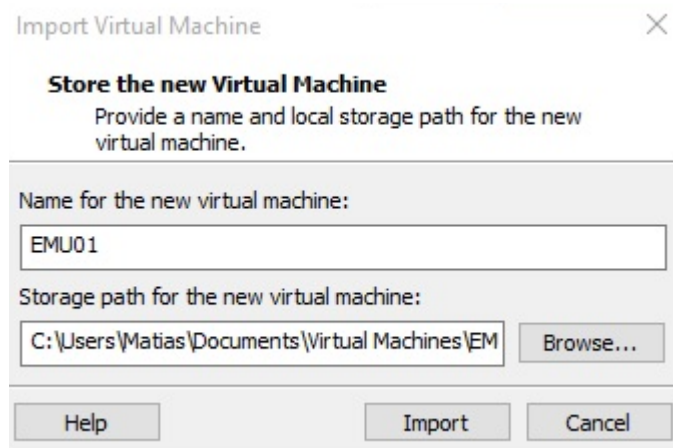
1. Descargar el archivo GNS3.ova del sitio web <https://www.gns3.com/software>



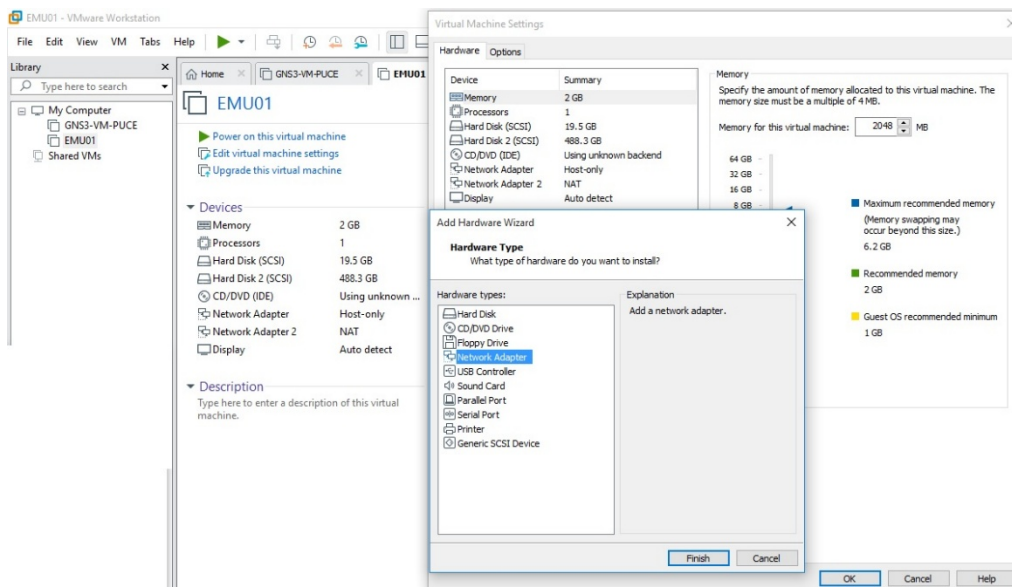
2. Abrir el programa VMware Workstation. File / Open y seleccionar el GNS3 VM descargado. Abrir



3. Agregar un nombre a la nueva máquina virtual. Import



4. Añadir tarjeta de red. VM / Settings / Add Network Adapter / Finish



5. Vmnet Information: Bridged / Bridged to: Interface por la cual se usan los datos.
Ok

The image shows the VMware Workstation interface. At the top, the 'Virtual Network Editor' window is open, displaying a table of network configurations:

Name	Type	External Connection	Host Connection	DHCP	Subnet Address
VMnet0	Bridged	Realtek PCIe GBE Family Co...	-	-	-
VMnet1	Host-only	-	Connected	Enabled	192.168.253.0
VMnet8	NAT	NAT	Connected	Enabled	192.168.122.0

Below the table, the 'VMnet Information' section for VMnet0 is shown. The 'Bridged' radio button is selected, and the 'Bridged to' dropdown menu is set to 'Realtek PCIe GBE Family Controller'. Other options like 'NAT' and 'Host-only' are unselected. There are also checkboxes for 'Connect a host virtual adapter to this network' and 'Use local DHCP service to distribute IP address to VMs'. At the bottom of this section, there are input fields for 'Subnet IP' and 'Subnet mask'.

The main VMware Workstation window shows the 'EMU01' VM. A terminal window is open, displaying the following output:

```
GNS3 2.2.0

GNS3 server version: 2.2.0
Release channel: 2.2
VM version: 0.10.19
Ubuntu version: bionic
Qemu version: 3.1.0
Virtualization: vmware
KVM support available: False

IP: 192.168.253.129

To log in using SSH:
ssh gns3@192.168.253.129
Password: gns3

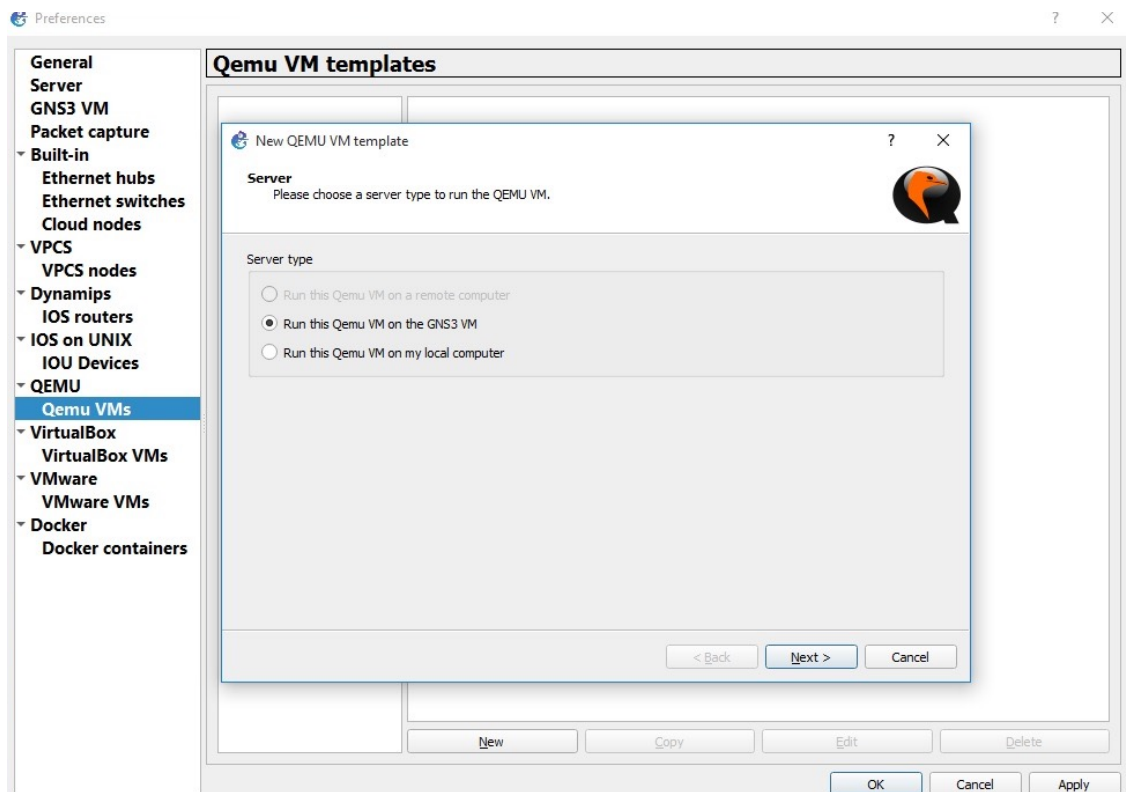
Images and projects are stored in '/opt/gns3'
```

The terminal window has an 'OK' button at the bottom.

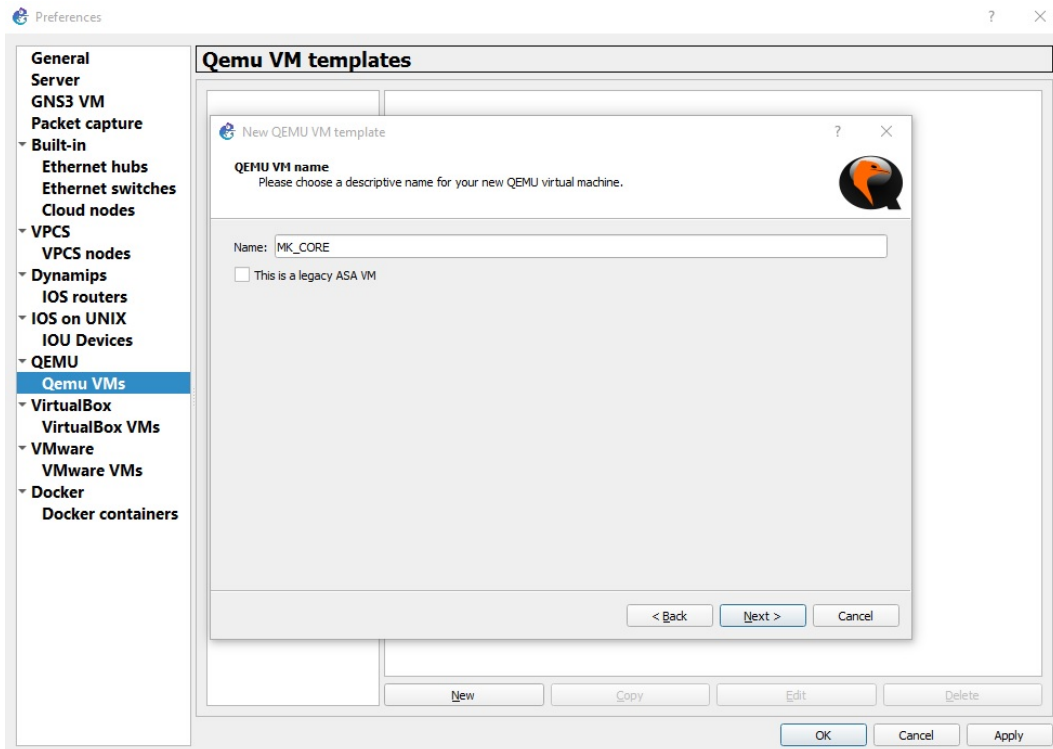
ANEXO 2. INCLUSIÓN DE ROUTEROS A GNS3

El presente anexo ilustra la importación de una máquina virtual con el sistema operativo de Mikrotik RouterOS, mediante el QEMU.

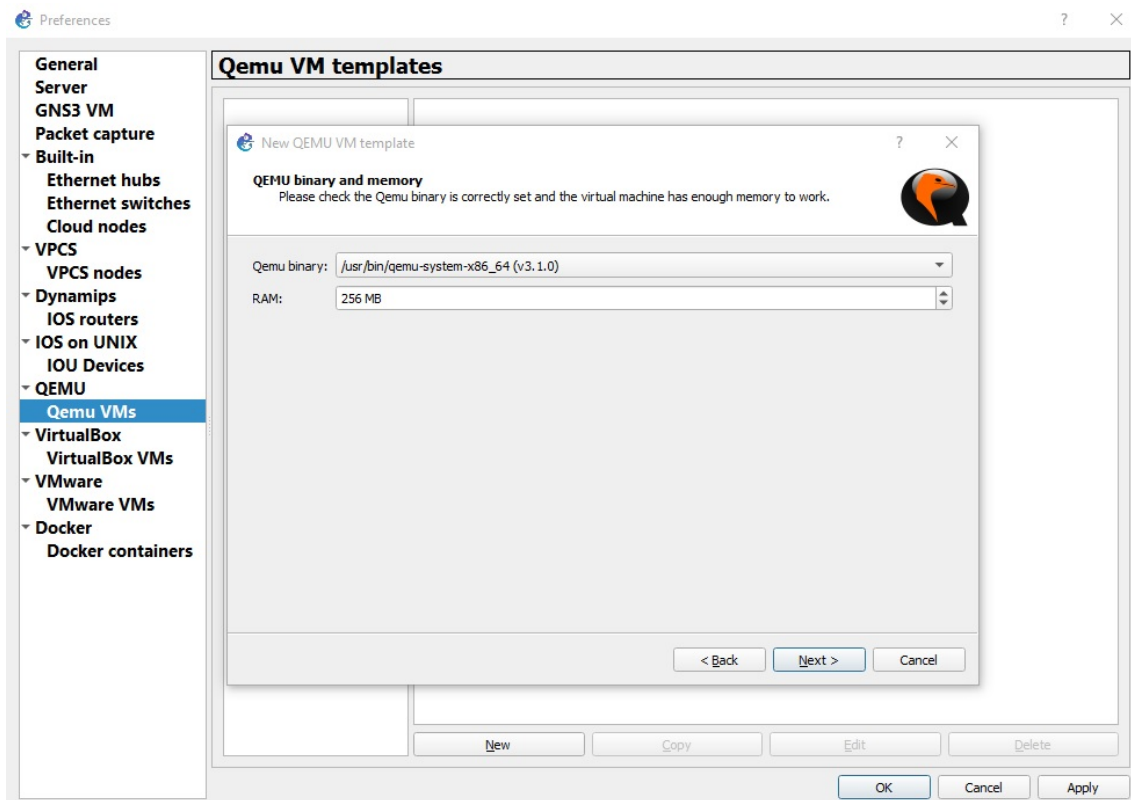
1. Iniciar el VMWare Workstation
2. Iniciar GNS3 y crear un nuevo proyecto
3. Dentro de GNS3: Edit / Preferences / Qemu VMs / New
4. Run this Qemu on the GNS3 VM
5. Next



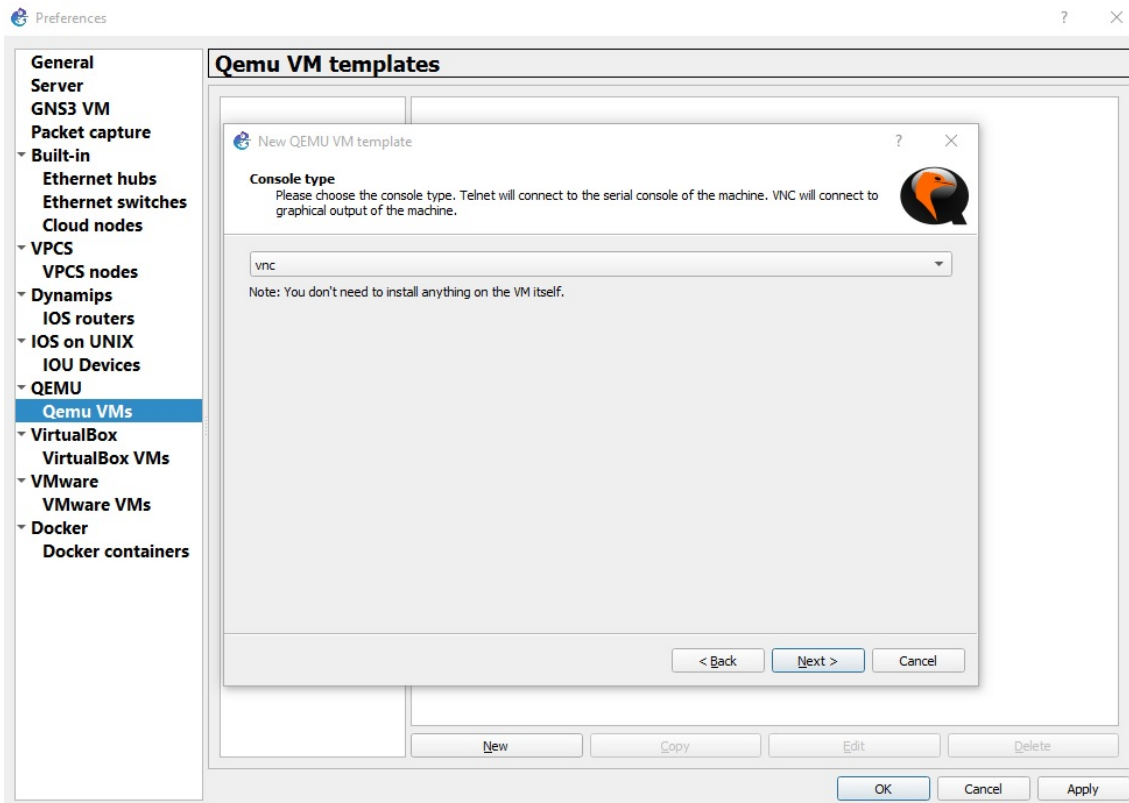
6. Ingresar un nombre al QEMU VM. Next



7. Agregar la cantidad de memoria RAM de la máquina a virtualizar. Next



- Escoger el tipo de consola con el que vamos a conectarnos con la máquina virtual.
Next



- Descargar la imagen del CHR de la página www.mikrotik.com/download - Raw Disk Image. Se recomienda descargar la versión Long Term

MikroTik

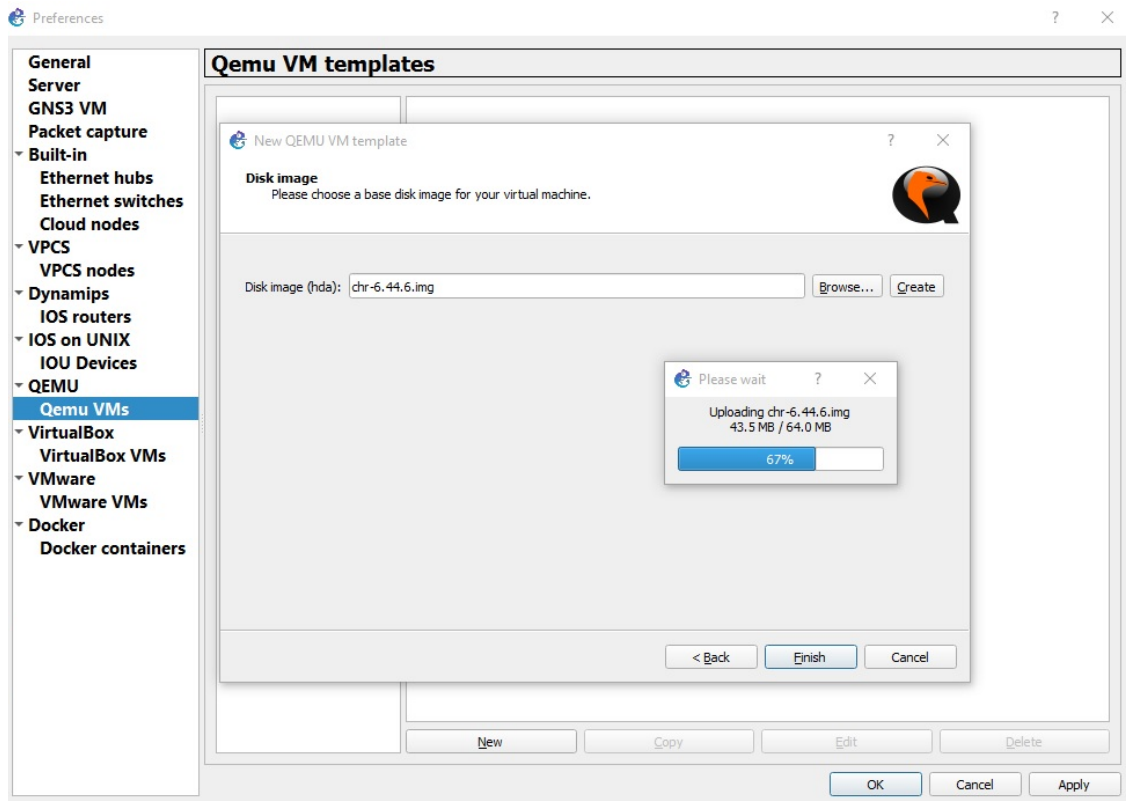
Home About Buy Jobs Hardware Software Support Training Account

Software Downloads Changelogs Download archive RouterOS The Dude Mobile app

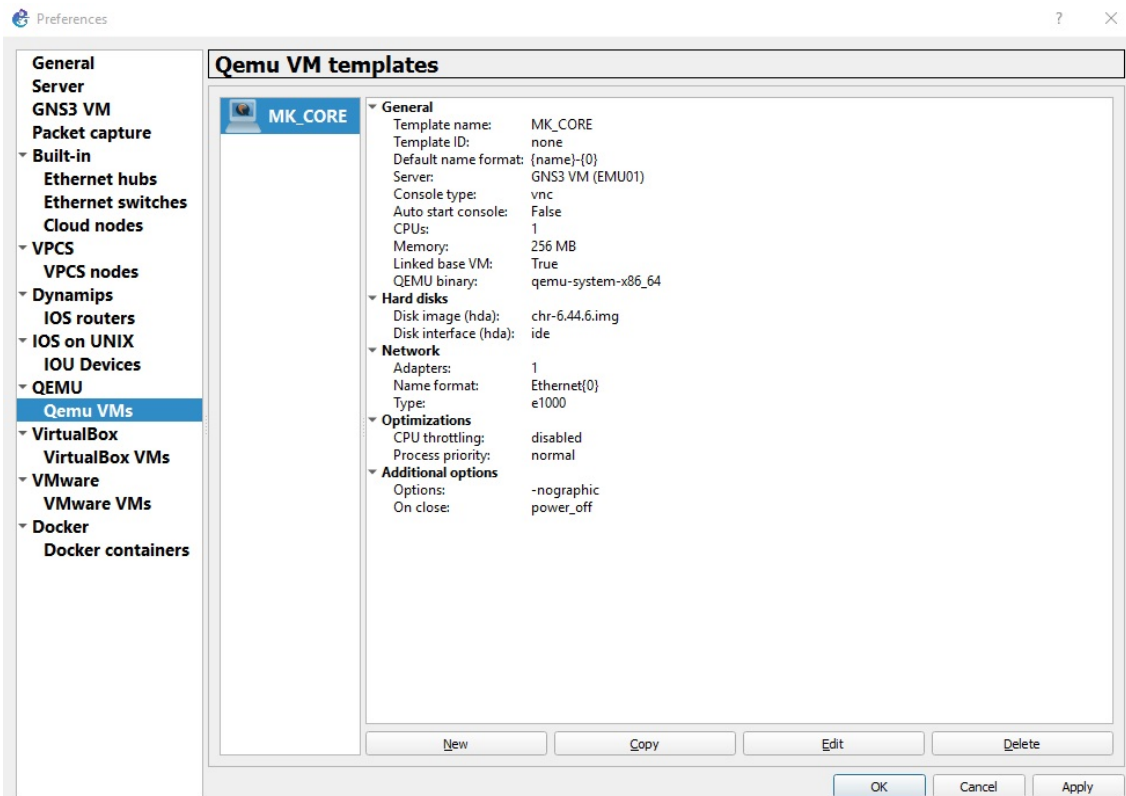
Cloud Hosted Router ?

	6.44.6 (Long-term)	6.46.1 (Stable)	6.47beta19 (Testing)	7.0beta4 (Development)
Images	vmdk, vhdx, vdi, ova, img			
VHDX image				
VMDK image				
VDI image				
OVA template				
Raw disk image				
Extra packages				
The Dude server				-
The Dude client				-
Changelog				
Checksum	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

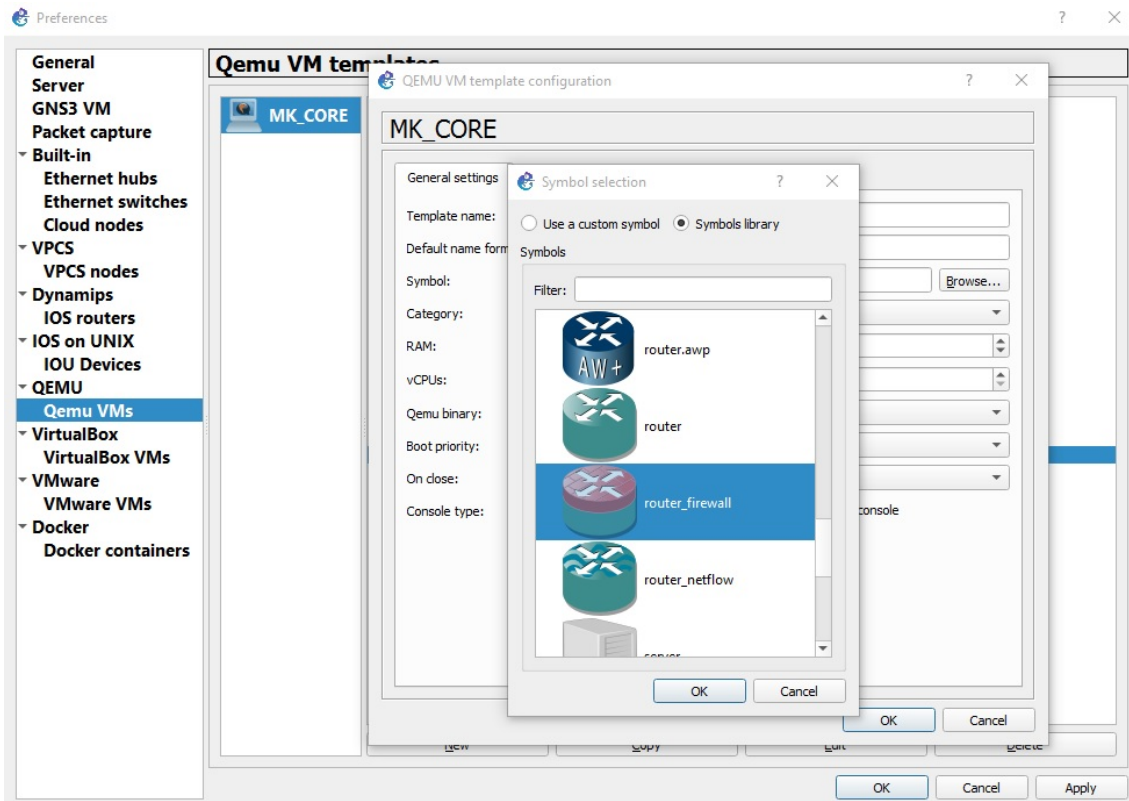
10. Cargar la imagen del CHR – Cloud Hosted Router. Finish



11. Se observa que la importación de la máquina virtual finalizó con éxito al GNS3

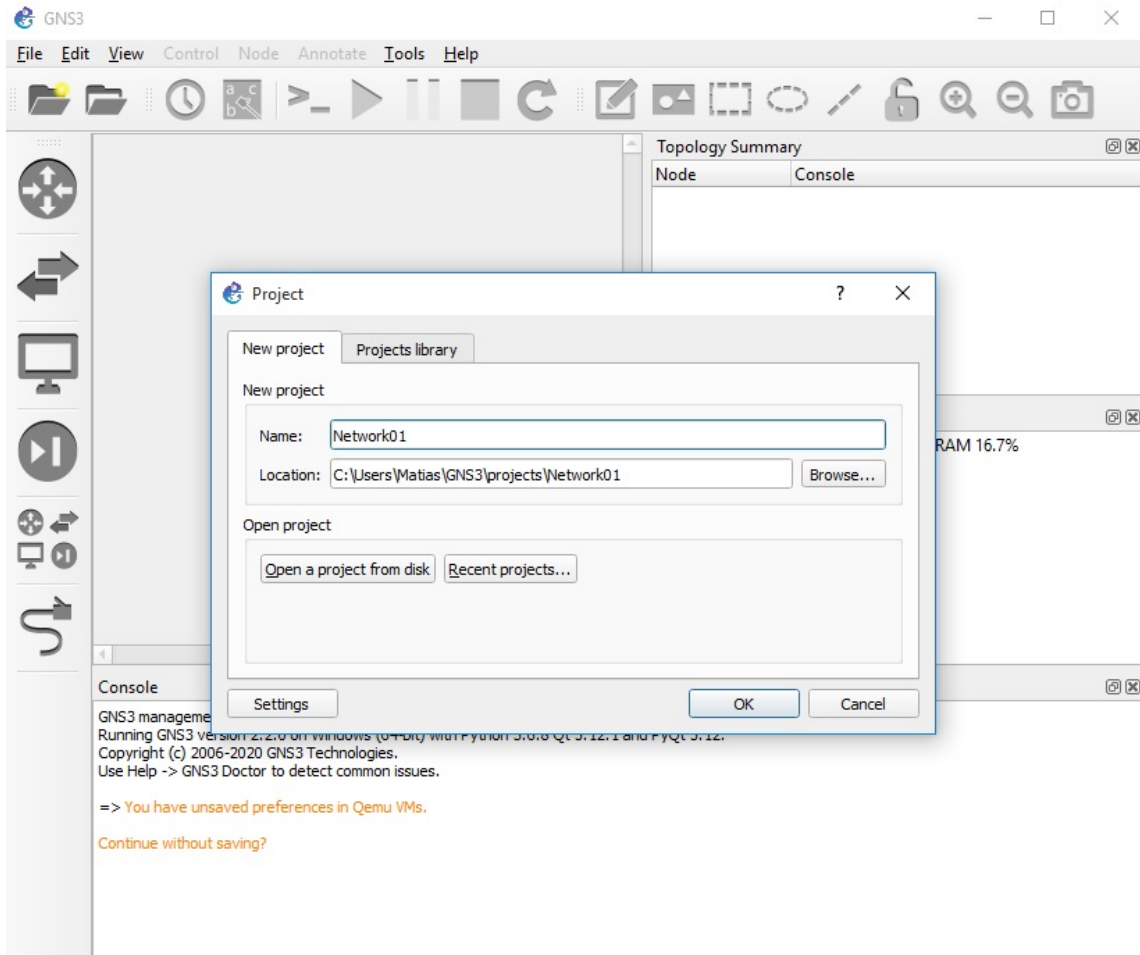


12. Cambiar el símbolo de la máquina virtual. Edit / General Settings / Symbol / Browse

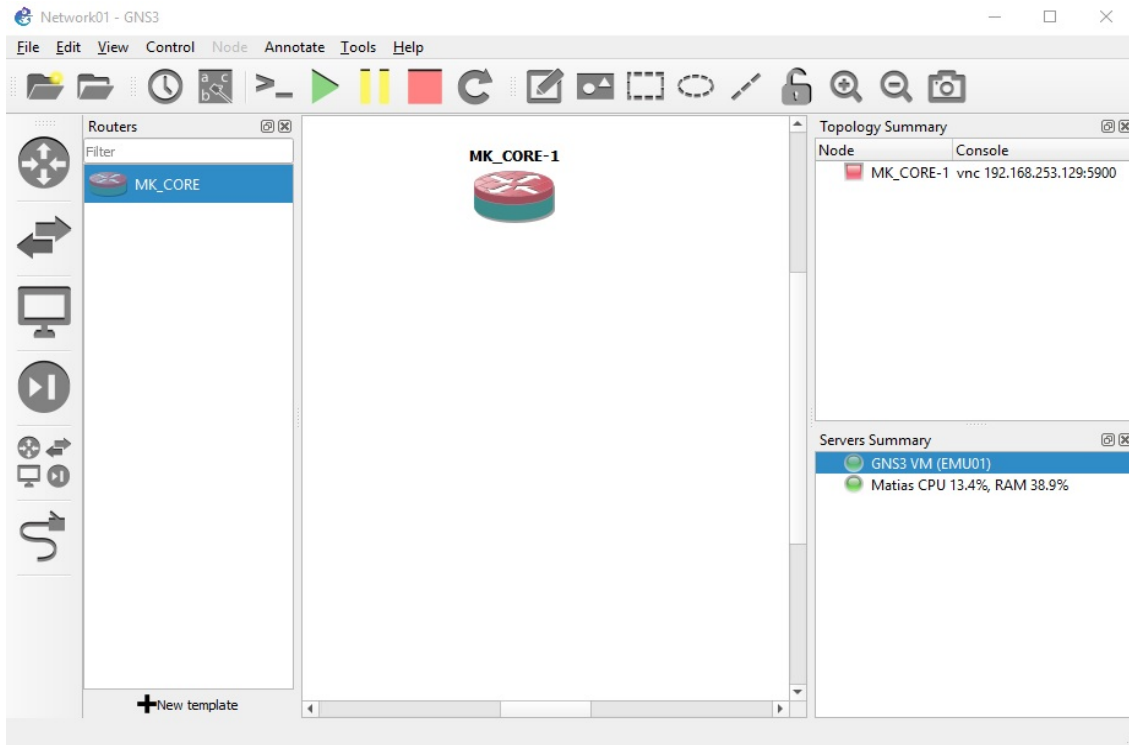


ANEXO 3. PRIMERA PRUEBA DE CONEXION

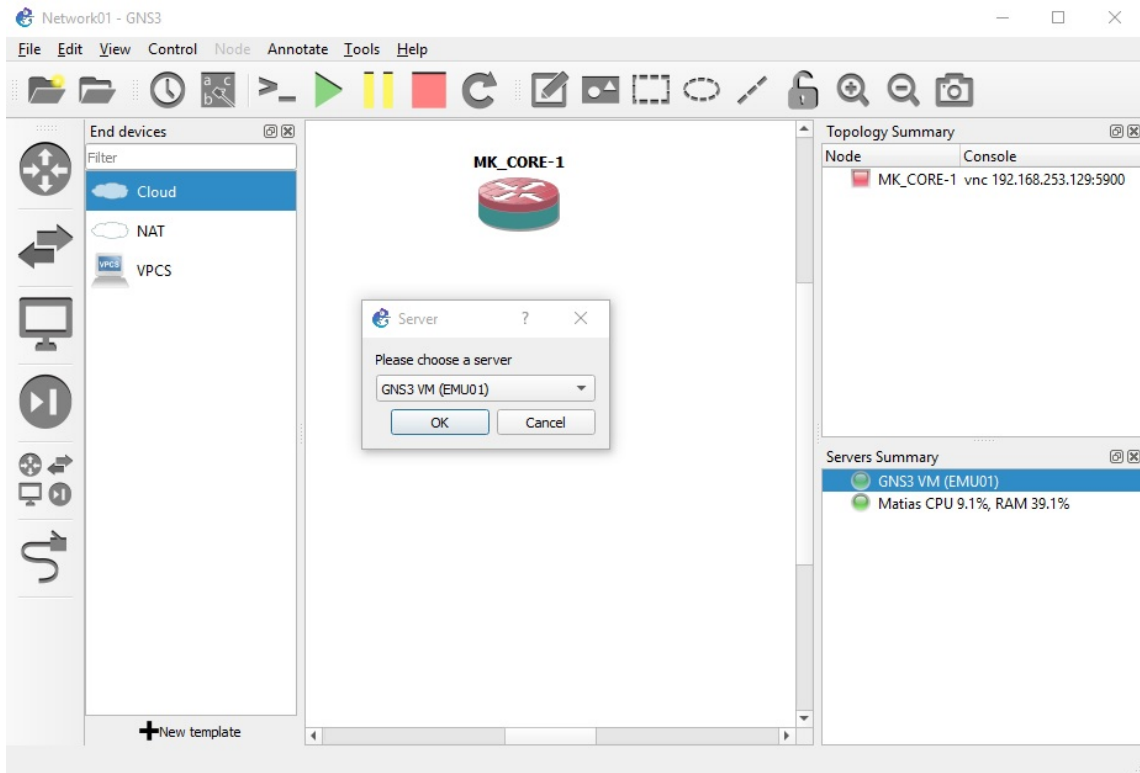
1. Abrir VMWare y GNS3. En GNS3: File / New blank project



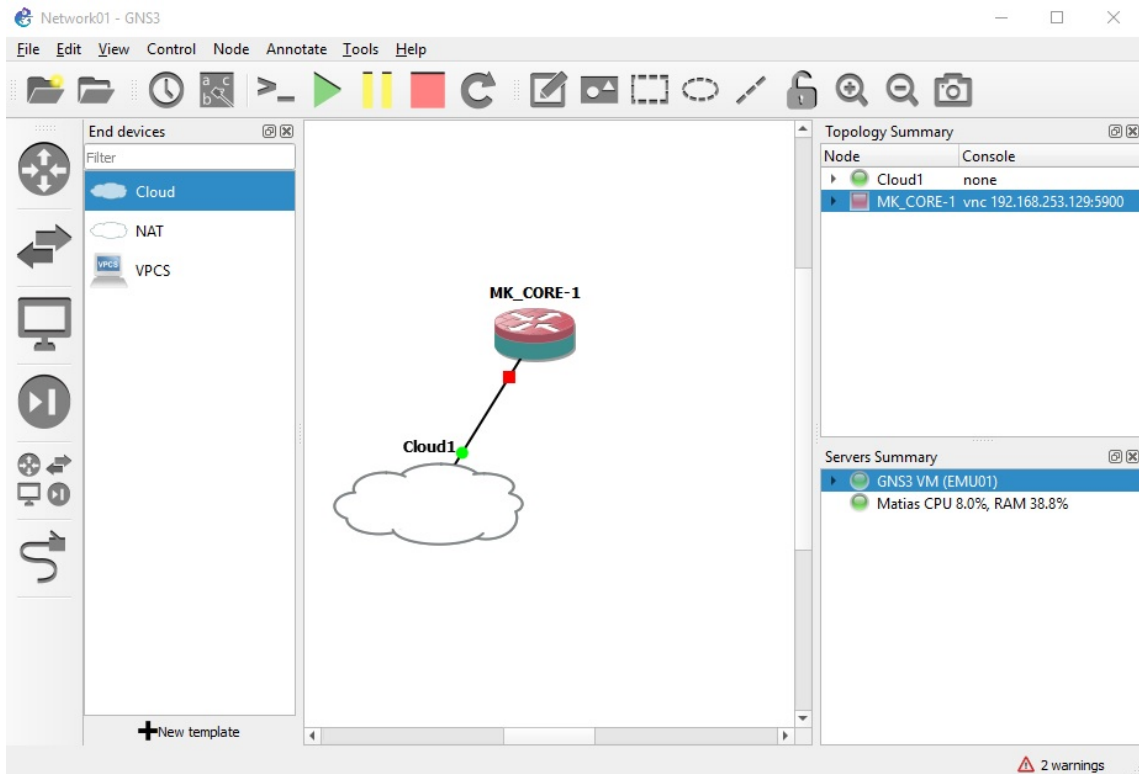
2. Agregar el router MK_CORE



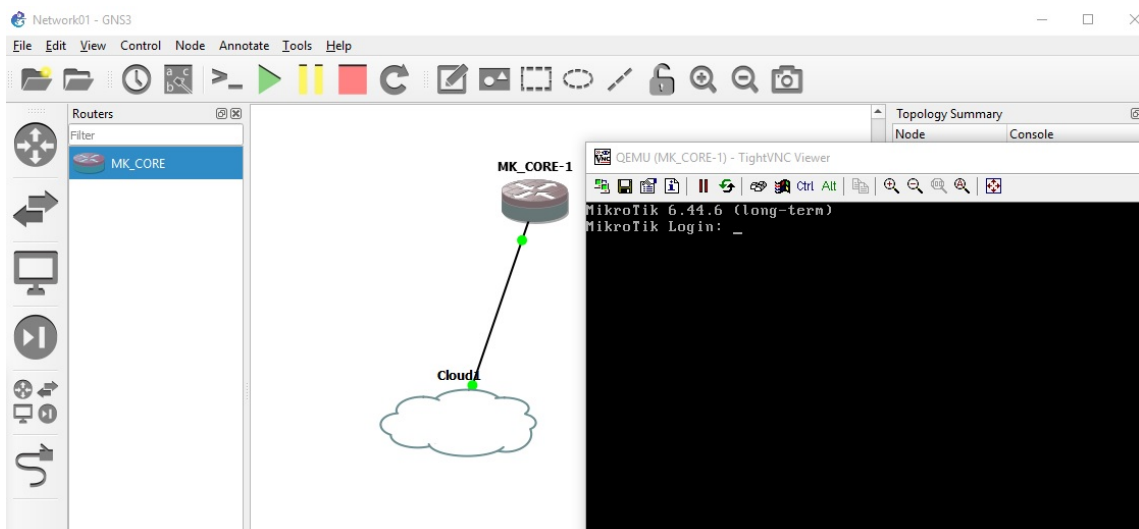
3. Agregar un Cloud al GNS3 VM



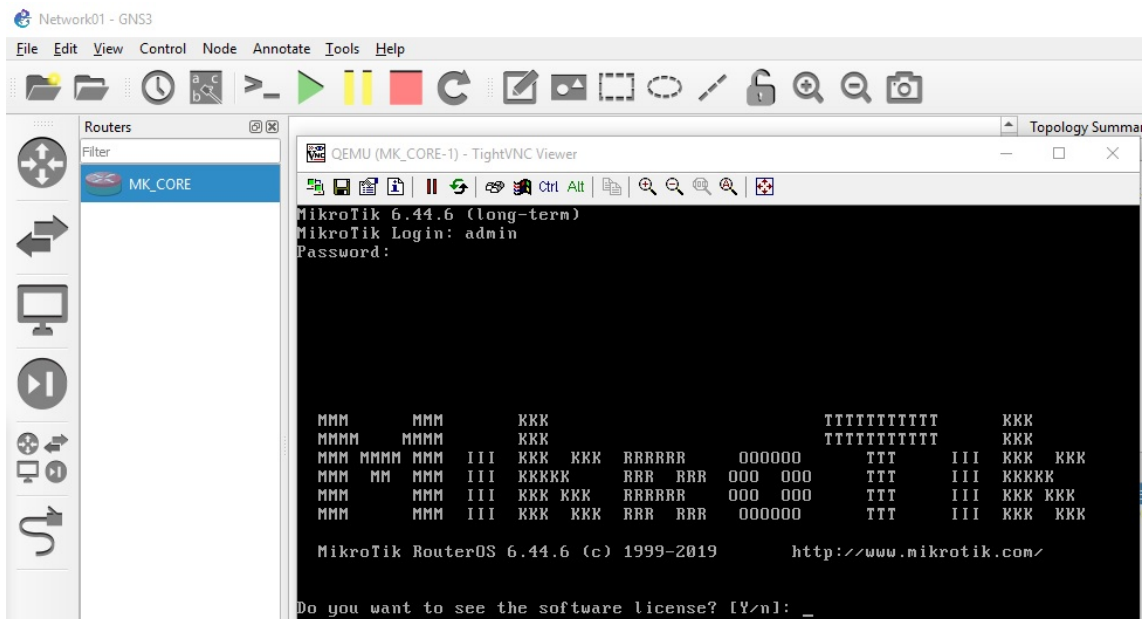
4. Agregar un link entre el router MK_CORE-1 y el Cloud1 con sus las interfaces que vayamos a vincularlos.



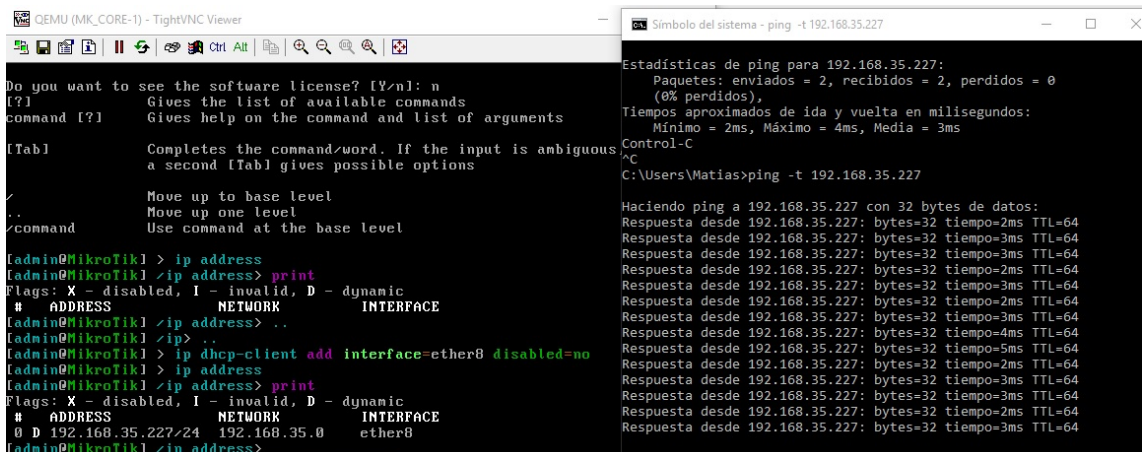
5. En GNS3 dar click en Start / Resume all nodes. Click derecho sobre el device MK_CORE-1 / Console



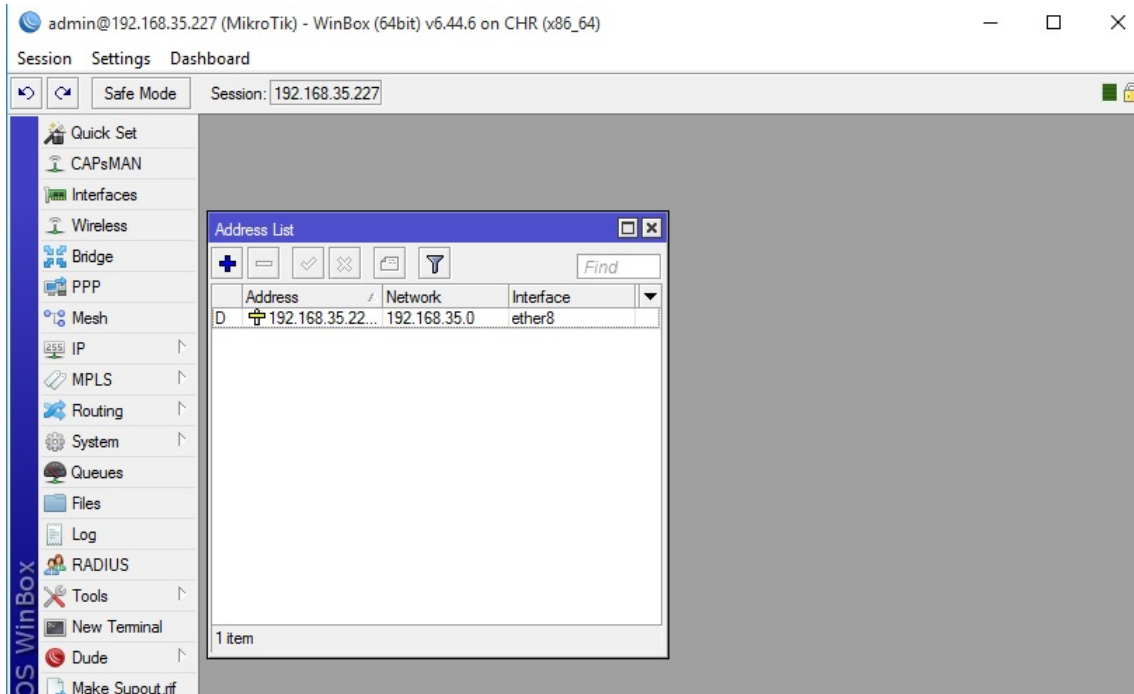
- Para acceder a RouterOS ingresar como Login: admin, sin password. Enter.
License? n



- Agregar el comando para adquirir IP automáticamente sobre la interface (en este caso ether8) que conecta el MK_CORE_1 con el Cloudy verificar con un ping la conectividad desde la PC al router

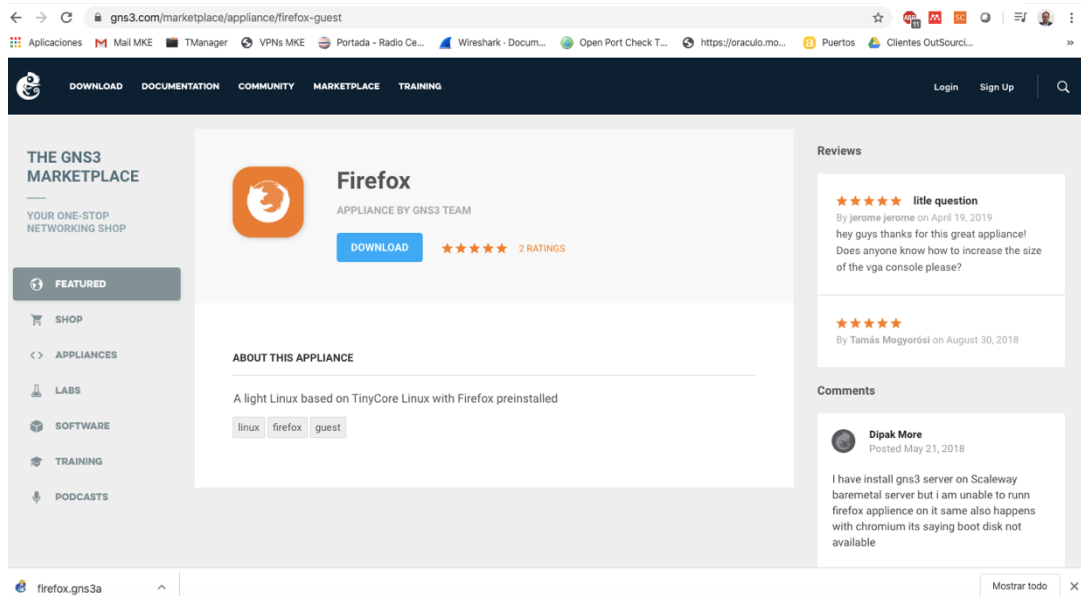


- Una vez que se tiene respuesta mediante un ping desde nuestro computador hacia la IP de MK_CORE_1. Comprobamos el acceso al router mencionado mediante Winbox.

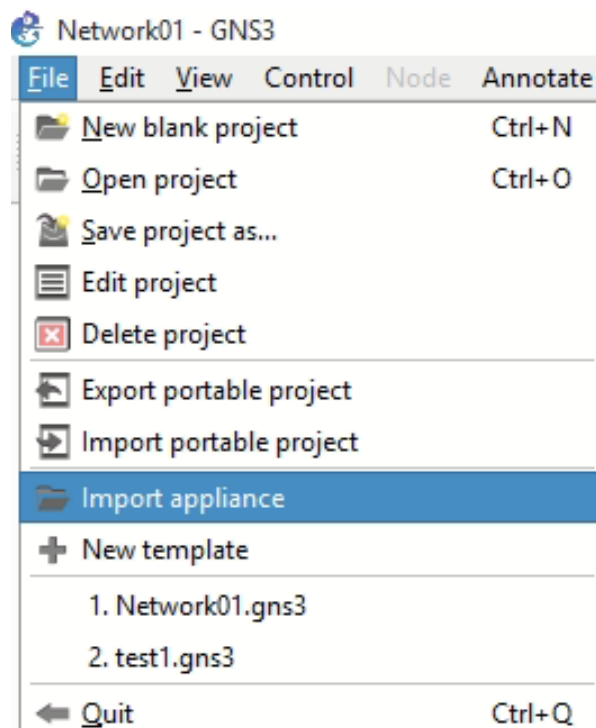


ANEXO 4. INSTALACION DE FIREFOX APPLIANCE

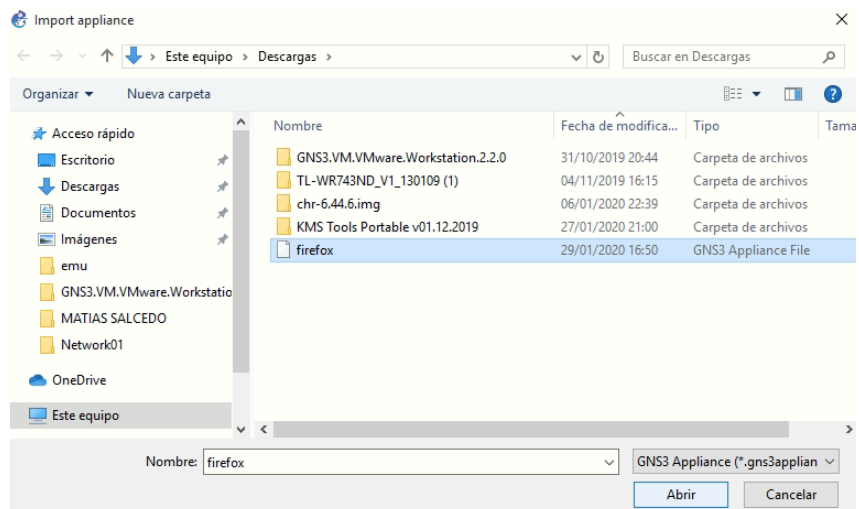
1. Descargar Firefox del sitio www.gns3.com



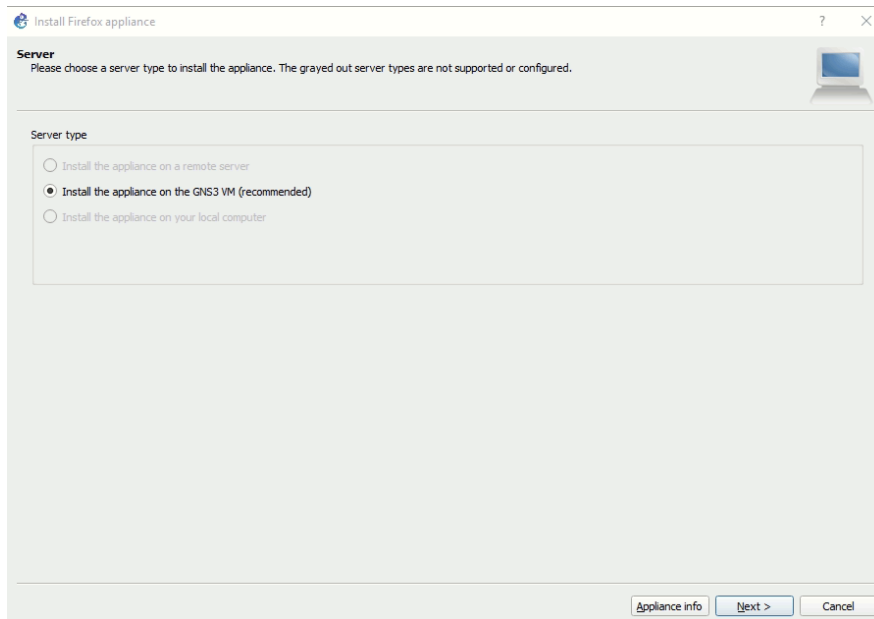
2. Importar el appliance



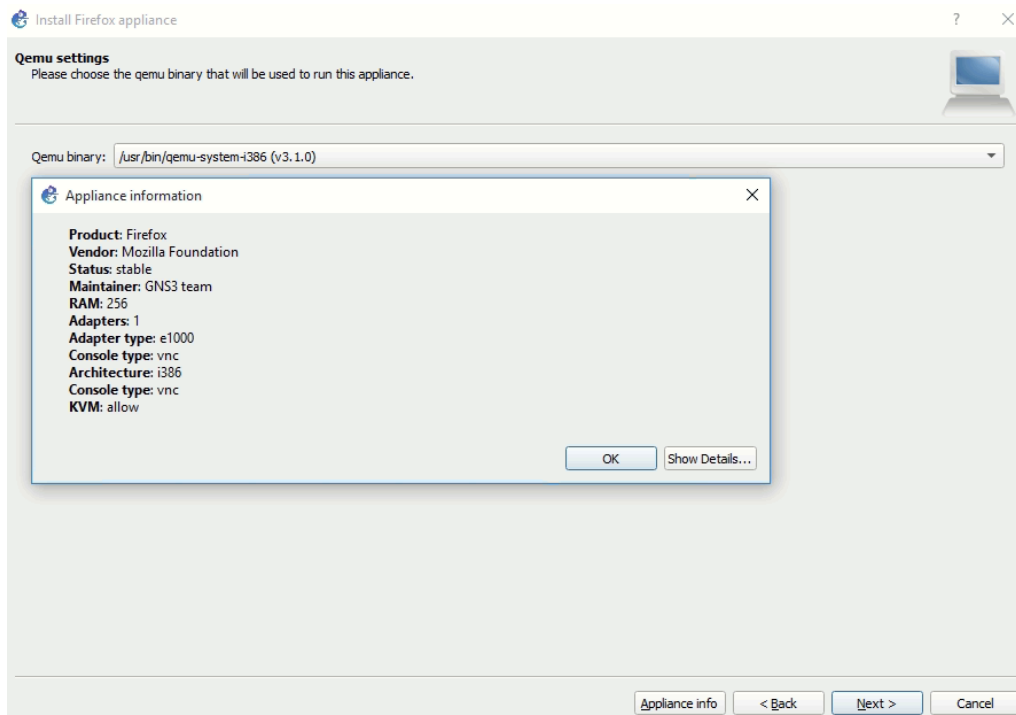
3. Seleccionar el appliance descargado



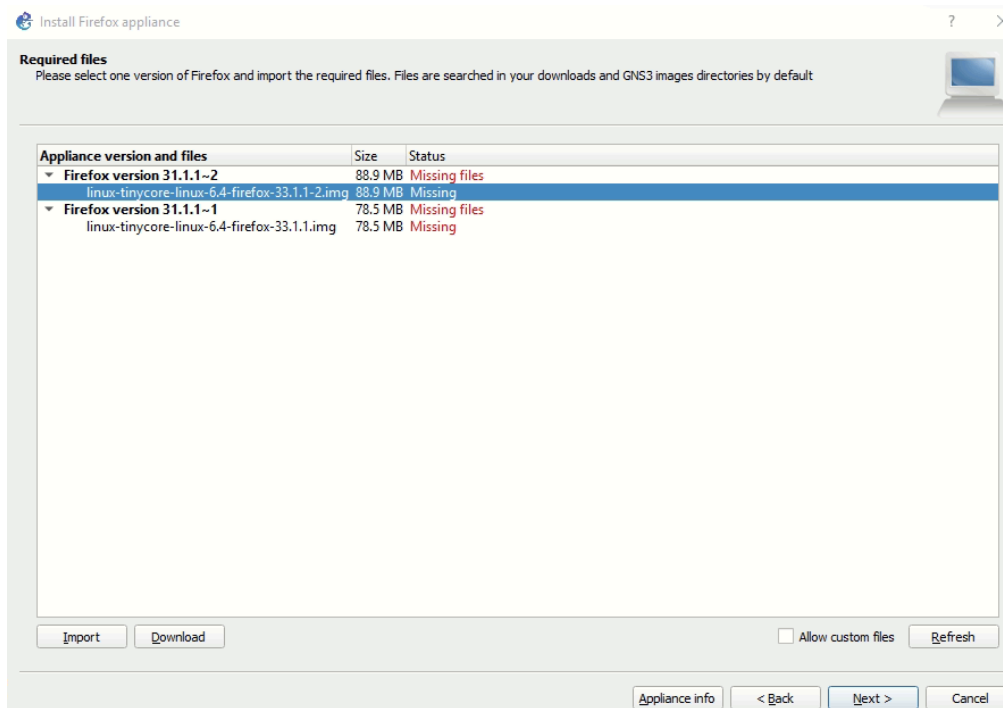
4. Instalar el appliance en GNS3 VM. Next



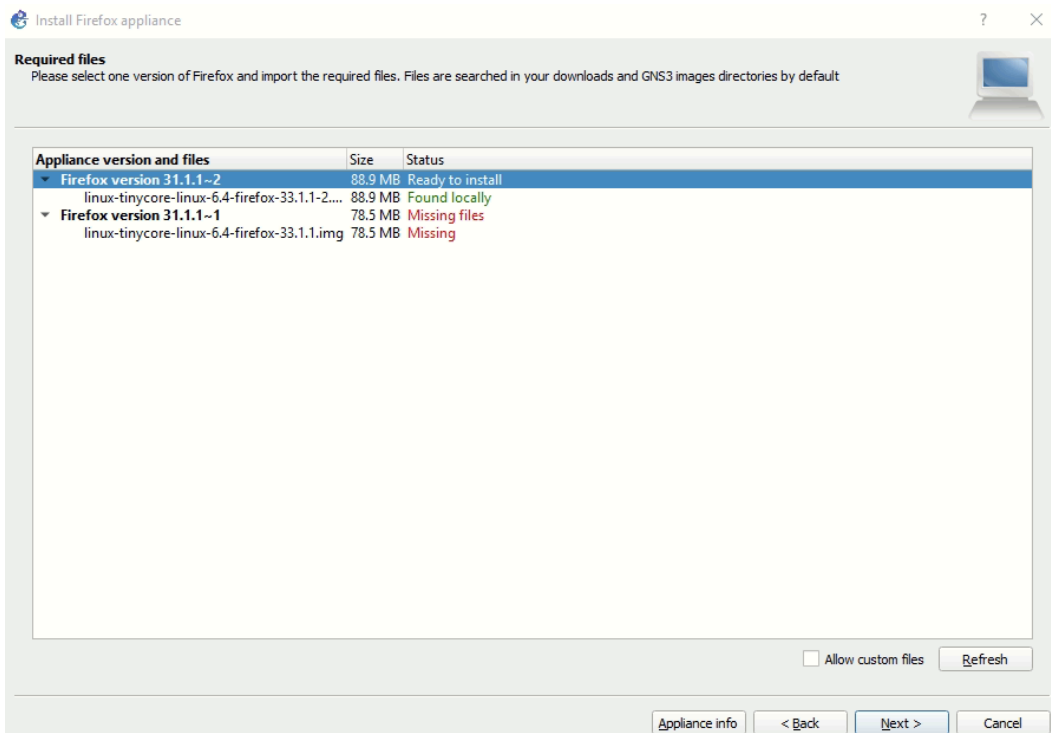
5. Seleccionar el binario de qemu. Next



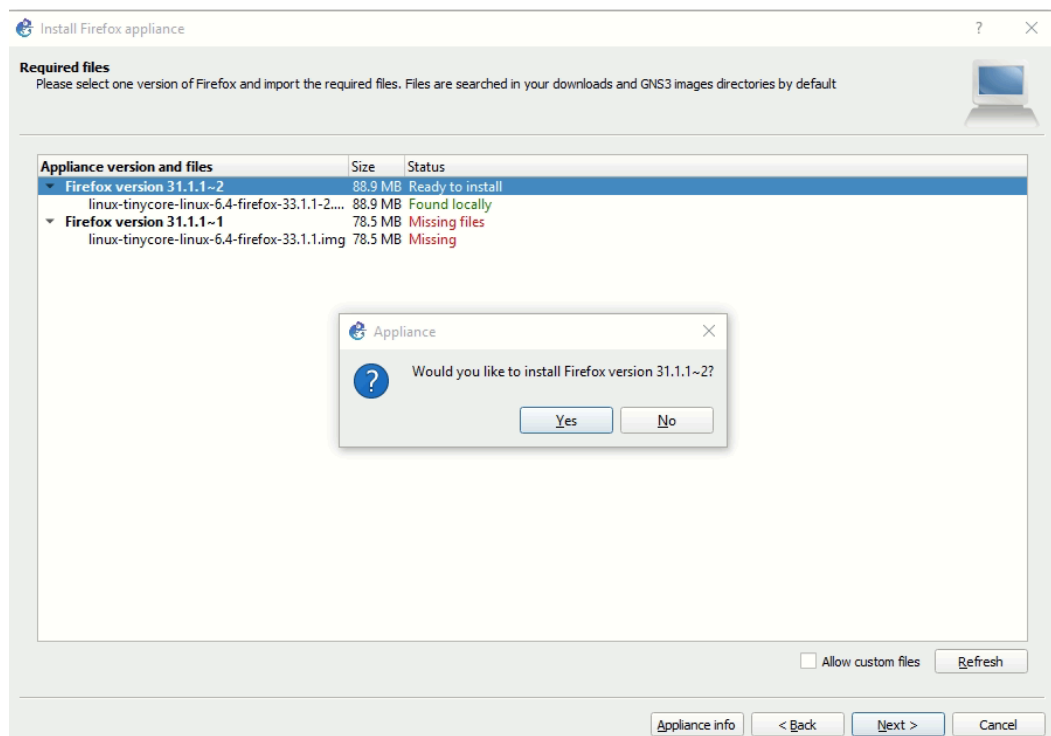
6. Seleccionar la versión del appliance faltante. Download

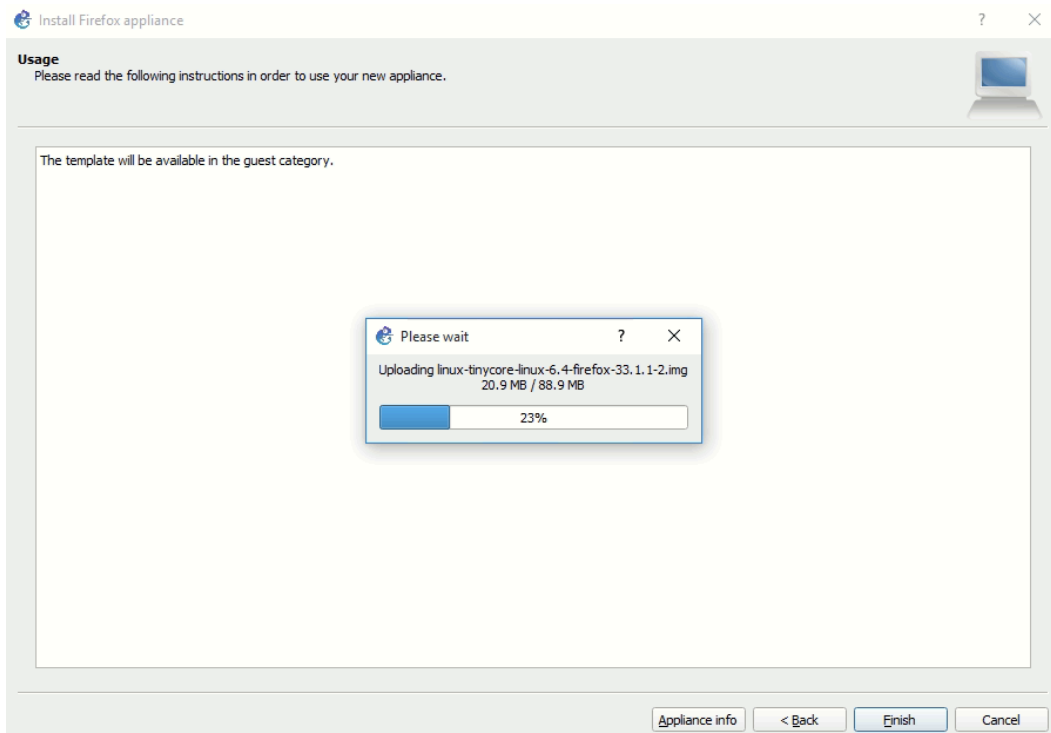


7. Una vez descargado y con el Status en Ready to install y Found locally. Next

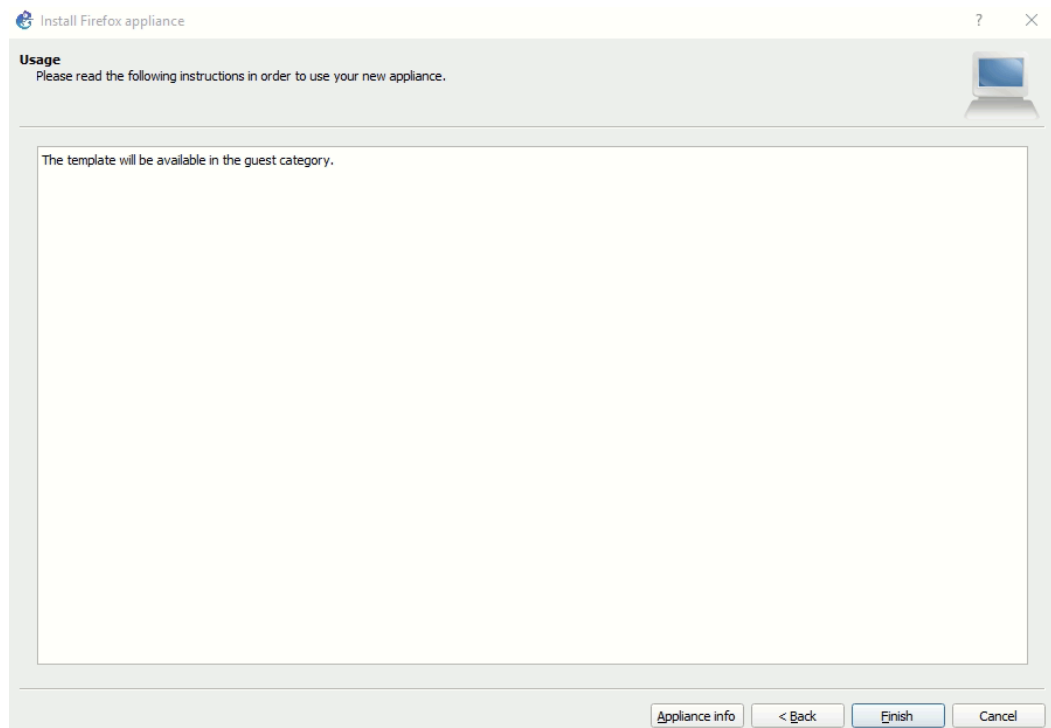


8. Aceptar la instalación del Firefox. Yes

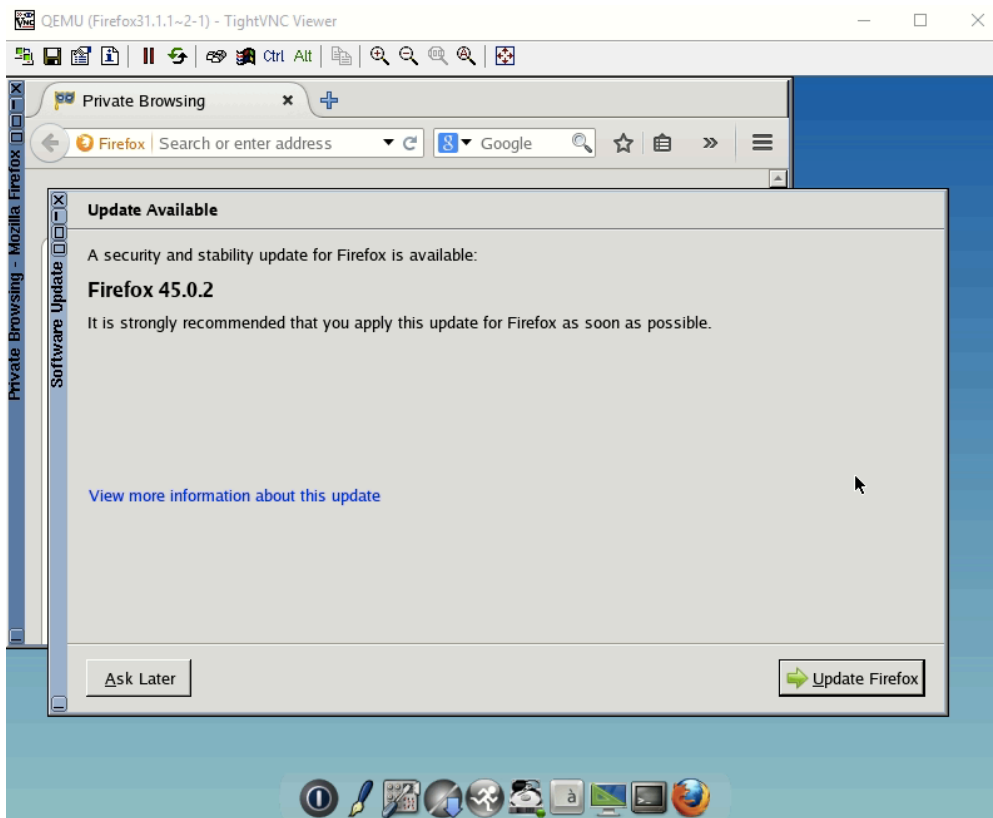
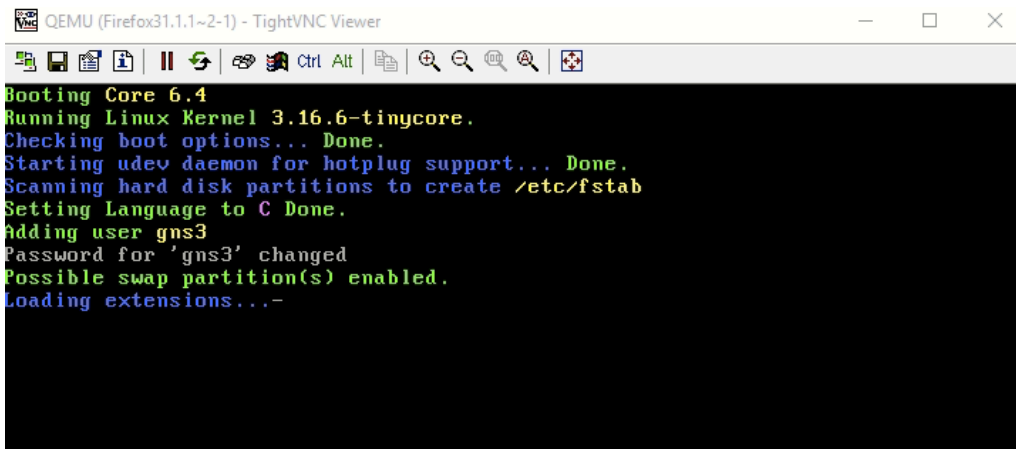


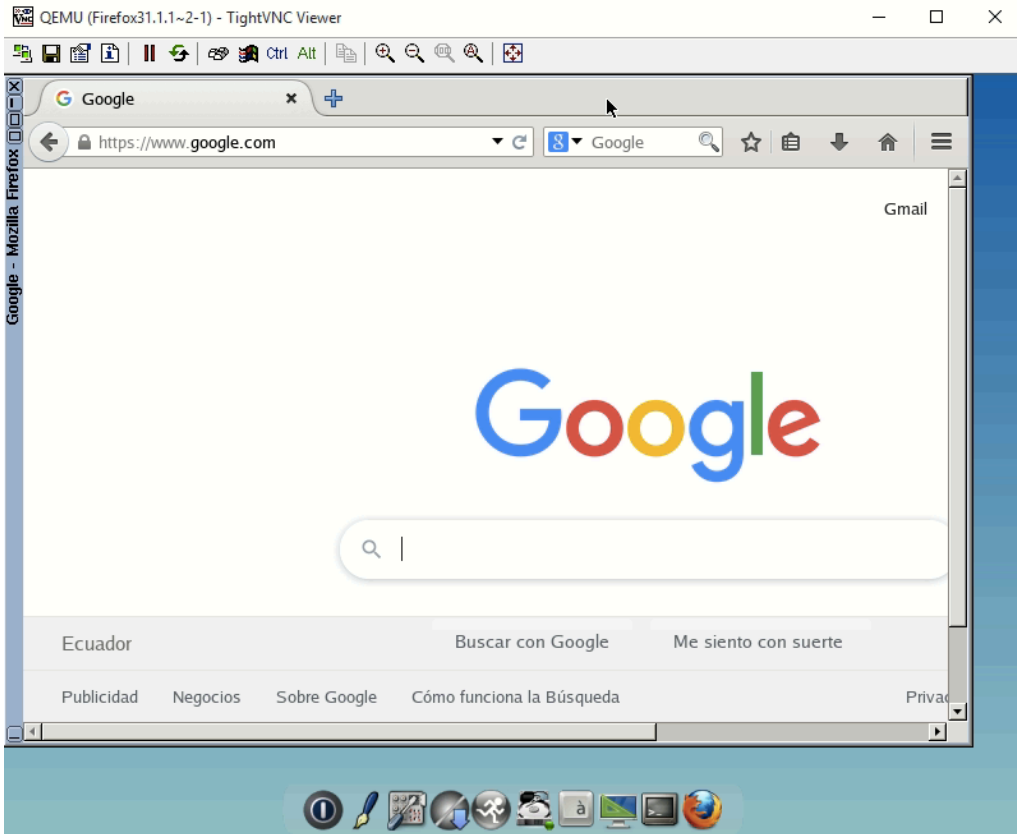


9. Finalizar la instalación



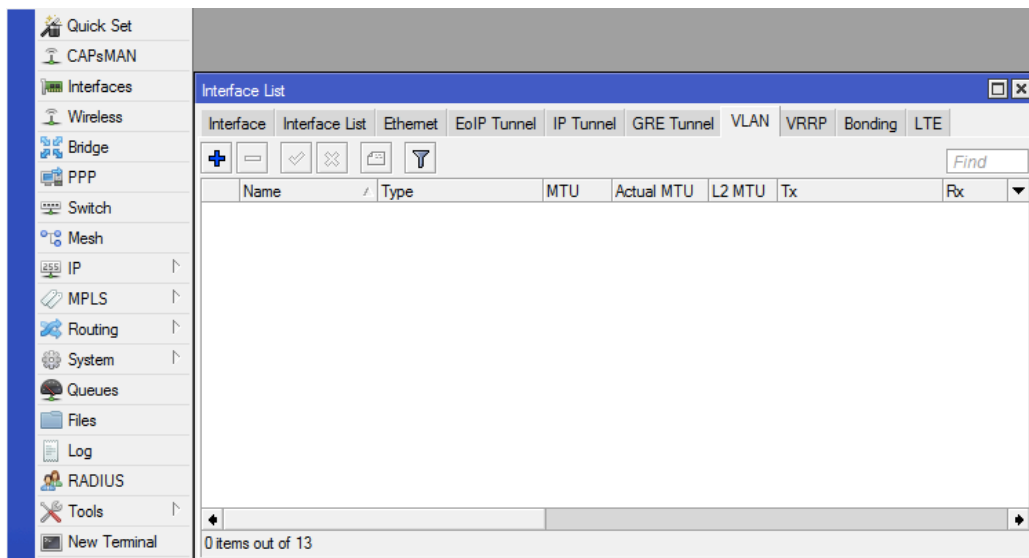
10. Iniciar QEMU Firefox



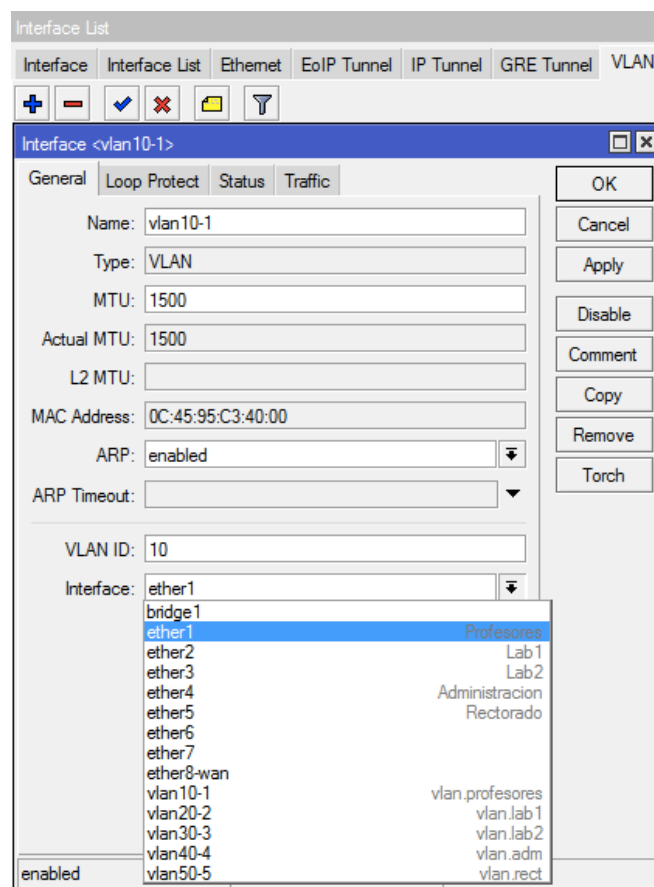


ANEXO 5. CREACIÓN DE VLANS EN ROUTEROS

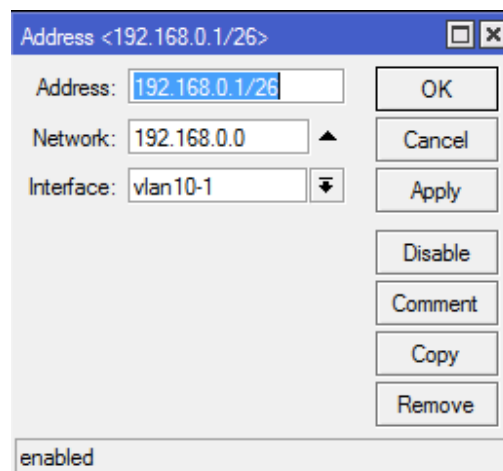
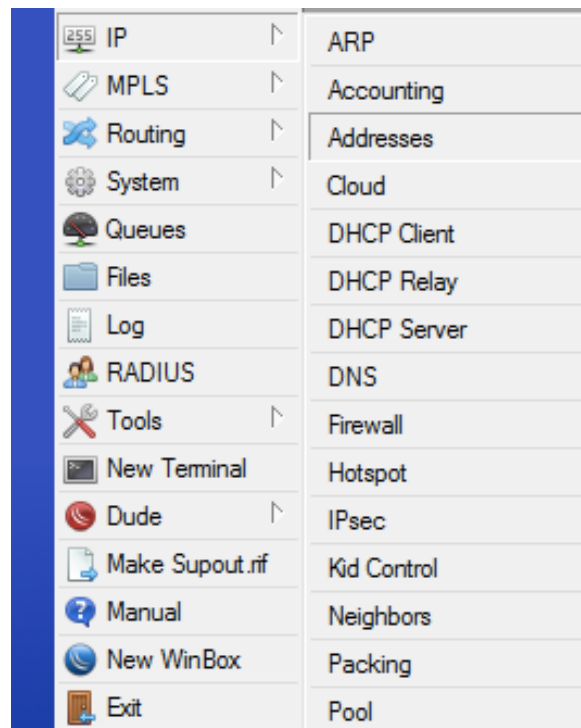
1. Interfaces / Interface List / VLAN



2. Para agregar una VLAN, seleccionamos +. Ingresamos los parámetros de Name, VLAN ID e Interface. Apply / Ok

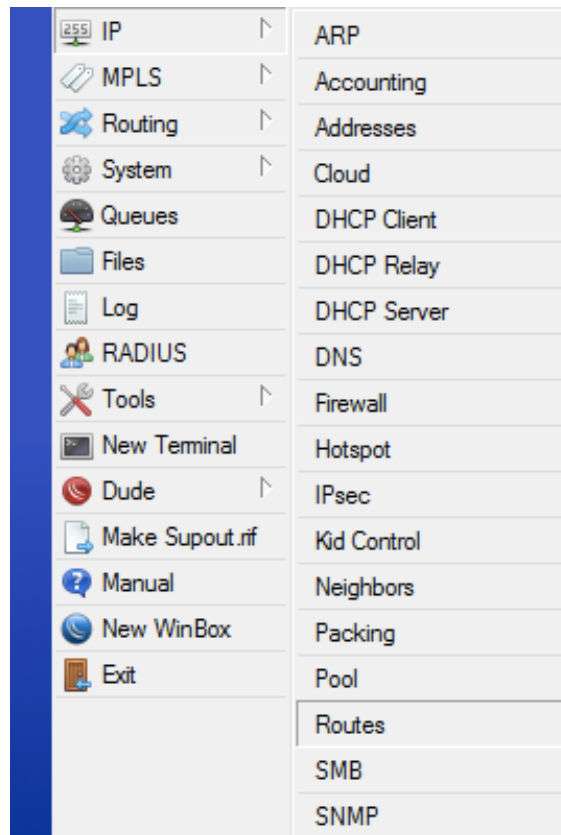


3. Para agregar un direccionamiento IP a la VLAN, seleccionamos IP / Address / +

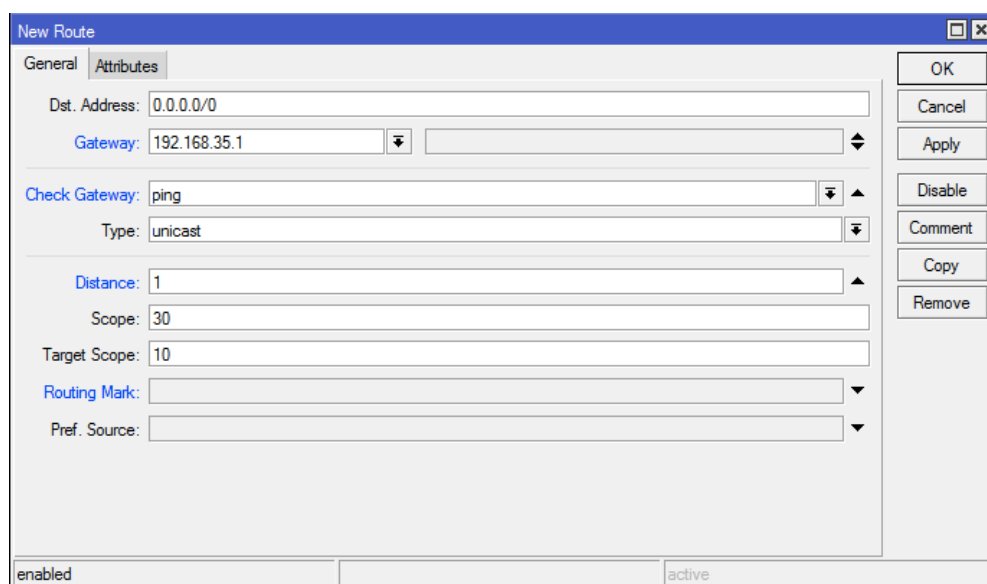


ANEXO 6. CREACIÓN DE RUTAS ESTÁTICAS EN ROUTEROS

1. Para crear rutas estáticas, seleccionamos: IP / Routes / +



2. Para crear una ruta por defecto se define la red de destino, gateway y distancia.



- Para crear una ruta estática alcanzable a una red local detrás de otra router, se definen los parámetros al igual que para la ruta por defecto, en este caso para alcanzar a la red de destino 192.168.2.0/24 se lo hace mediante el router con IP 172.16.1.1

New Route

General | Attributes

Dst. Address: 192.168.2.0/24

Gateway: 172.16.1.1

Check Gateway:

Type: unicast

Distance:

Scope: 30

Target Scope: 10

Routing Mark:

Pref. Source:

enabled active

- Lista de rutas conectadas. IP / Routes

Route List

Routes | Nexthops | Rules | VRF

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAS	0.0.0.0/0	192.168.35.1 reachable ether8-wan	1		
DAC	172.16.0.0/28	bridge1 reachable	0		172.16.0.1
DAC	192.168.0.0/26	vlan10-1 reachable	0		192.168.0.1
DAC	192.168.0.64/26	vlan20-2 reachable	0		192.168.0.65
DAC	192.168.0.128/26	vlan30-3 reachable	0		192.168.0.129
DAC	192.168.0.192/27	vlan40-4 reachable	0		192.168.0.193
DAC	192.168.0.224/27	vlan50-5 reachable	0		192.168.0.225
DAC	192.168.35.0/24	ether8-wan reachable	0		192.168.35.208

8 items

Address <192.168.0.1/26>

Address: 192.168.0.1/26

Network: 192.168.0.0

Interface: vlan10-1

enabled

Route <192.168.0.0/26>

General | Attributes

Dst. Address: 192.168.0.0/26

Gateway: vlan10-1 reachable

Check Gateway:

Type: unicast

Distance: 0

Scope: 10

Target Scope: 10

Routing Mark:

Pref. Source: 192.168.0.1

dynamic active connected

ANEXO 7. SCRIPTS Y CONFIGURACIONES

Router de Core

```
[admin@Core] > export
# jan/15/2020 21:04:06 by RouterOS 6.44.6
# software id =
#
#
#
/interface bridge
add name=bridge1
/interface ethernet
set [ find default-name=ether1 ] comment=Profesores
set [ find default-name=ether2 ] comment=Lab1
set [ find default-name=ether3 ] comment=Lab2
set [ find default-name=ether4 ] comment=Administracion
set [ find default-name=ether5 ] comment=Rectorado
set [ find default-name=ether8 ] name=ether8-wan
/interface vlan
add comment=vlan.profesores interface=ether1 name=vlan10-1 vlan-id=10
add comment=vlan.lab1 interface=ether2 name=vlan20-2 vlan-id=20
add comment=vlan.lab2 interface=ether3 name=vlan30-3 vlan-id=30
add comment=vlan.adm interface=ether4 name=vlan40-4 vlan-id=40
add comment=vlan.rect interface=ether5 name=vlan50-5 vlan-id=50
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/ip pool
add name=dhcp_pool0 ranges=192.168.0.2-192.168.0.62
/ip dhcp-server
add address-pool=dhcp_pool0 disabled=no interface=vlan10-1 name=dhcp1
/queue type
set 0 pfifo-limit=100
add kind=pcq name=RedProfesores_Down pcq-classifier=dst-address pcq-dst-address6-
mask=64 pcq-src-address6-mask=64
add kind=pcq name=RedProfesores_Up pcq-classifier=src-address pcq-dst-address6-
mask=64 pcq-src-address6-mask=64
add kind=sfq name=BAJADA
add kind=sfq name=SUBIDA
add kind=sfq name=SFQ
add kind=pcq name="NETFLIX DOWN" pcq-classifier=dst-address pcq-dst-address6-
mask=64 pcq-rate=2M pcq-src-address6-mask=64 pcq-total-limit=200000KiB
add kind=pcq name="GOOGLE DOWN" pcq-classifier=dst-address pcq-dst-address6-
mask=64 pcq-rate=3M pcq-src-address6-mask=64 pcq-total-limit=200000KiB
/interface bridge port
add bridge=bridge1 hw=no interface=ether1
/ip address
add address=192.168.0.1/26 interface=vlan10-1 network=192.168.0.0
add address=192.168.0.65/26 interface=vlan20-2 network=192.168.0.64
add address=192.168.0.129/26 interface=vlan30-3 network=192.168.0.128
```

```

add address=192.168.0.193/27 interface=vlan40-4 network=192.168.0.192
add address=192.168.0.225/27 interface=vlan50-5 network=192.168.0.224
add address=172.16.0.1/28 interface=bridge1 network=172.16.0.0
/ip dhcp-client
add disabled=no interface=ether2
add dhcp-options=hostname,clientid disabled=no interface=ether8-wan
/ip dhcp-server network
add address=192.168.0.0/26 dns-server=192.168.0.1 gateway=192.168.0.1
/ip dns
set allow-remote-requests=yes servers=8.8.8.8
/ip firewall address-list
add address=ues.mikareno.com list=Mikareno
add address=mikareno.com list=Mikareno
add address=192.168.0.0/24 list="REDES LOCALES"
/interface bridge port
add bridge=bridge1 hw=no interface=ether1
/ip address
add address=192.168.0.1/26 interface=vlan10-1 network=192.168.0.0
add address=192.168.0.65/26 interface=vlan20-2 network=192.168.0.64
add address=192.168.0.129/26 interface=vlan30-3 network=192.168.0.128
add address=192.168.0.193/27 interface=vlan40-4 network=192.168.0.192
add address=192.168.0.225/27 interface=vlan50-5 network=192.168.0.224
add address=172.16.0.1/28 interface=bridge1 network=172.16.0.0
/ip dhcp-client
add disabled=no interface=ether2
add dhcp-options=hostname,clientid disabled=no interface=ether8-wan
/ip dhcp-server network
add address=192.168.0.0/26 dns-server=192.168.0.1 gateway=192.168.0.1
/ip dns
set allow-remote-requests=yes servers=8.8.8.8
/ip firewall address-list
add address=ues.mikareno.com list=Mikareno
add address=mikareno.com list=Mikareno
add address=192.168.0.0/24 list="REDES LOCALES"
/ip firewall mangle
add action=mark-packet chain=servicios comment=MIKARENO dst-address-
list="REDES LOCALES" new-packet-mark=Mikareno_DOWN_P passthrough=no src-
address-list=Mikareno
add action=mark-packet chain=servicios comment=MIKARENO dst-address-
list=Mikareno new-packet-mark=Mikareno_UP_P passthrough=no src-address-
list="REDES LOCALES"
add action=accept chain=input disabled=yes dst-address-list="REDES LOCALES" src-
address-list="REDES LOCALES"
add action=add-src-to-address-list address-list=Google address-list-timeout=2d
chain=prerouting in-interface=ether8-wan protocol=udp src-address-list=!Google src-
port=443
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether8-wan
/system clock
set time-zone-name=America/Guayaquil

```

```
/system identity
set name=Core
```

Router Profesores

```
[admin@RB Profesores] > export
# jan/16/2020 02:02:43 by RouterOS 6.44.6
# software id =
#
#
#
/interface bridge
add name=local
/interface vlan
add interface=ether1 name=vlan10 vlan-id=10
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/interface bridge port
add bridge=local interface=ether2
add bridge=local interface=ether3
add bridge=local interface=ether4
add bridge=local interface=ether5
add bridge=local interface=vlan10
/ip address
add address=172.16.0.2/29 interface=ether1 network=172.16.0.0
/system identity
set name="RB Profesores"
```