



UNIVERSIDAD TÉCNICA DE AMBATO

**FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E
INDUSTRIAL**

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y COMUNICACIONES

Tema:

**MIGRACIÓN DE LA RED Y GESTIÓN EN LA CONFIGURACIÓN
AUTOMÁTICA DE EQUIPOS EN EL ISP GRUPO MEGARED**

Trabajo de Titulación Modalidad: Proyecto de Investigación, presentado previo a la obtención del título de Ingeniera en Electrónica y Comunicaciones.

ÁREA: Programación y redes

LÍNEA DE INVESTIGACIÓN: Programación y redes

AUTOR: Betsy Samanta Guerrero Vayas

TUTOR: Ing. Víctor Santiago Manzano Villafuerte, Mg.

Ambato - Ecuador

marzo – 2023

APROBACIÓN DE TUTOR

En calidad de tutor del Trabajo de Titulación con el tema: MIGRACIÓN DE LA RED Y GESTIÓN EN LA CONFIGURACIÓN AUTOMÁTICA DE EQUIPOS EN EL ISP GRUPO MEGARED, desarrollado bajo la modalidad Proyecto de Investigación por la señorita Betsy Samanta Guerrero Vayas, estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que la estudiante ha sido tutorada durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 15 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y el numeral 7.4 del respectivo instructivo.

Ambato, marzo 2023.

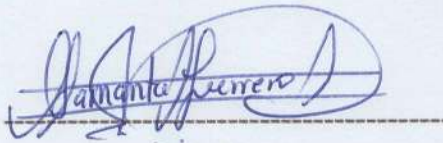
Ing. Víctor Santiago Manzano Villafuerte, Mg.

TUTOR

AUTORÍA

El presente Proyecto de Investigación titulado: MIGRACIÓN DE LA RED Y GESTIÓN EN LA CONFIGURACIÓN AUTOMÁTICA DE EQUIPOS EN EL ISP GRUPO MEGARED, es absolutamente original, auténtico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, marzo 2023.



Betsy Samanta Guerrero Vayas

C.C. 1805085014

AUTORA

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación en favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las regulaciones de la institución.

Ambato, marzo 2023.



Betsy Samanta Guerrero Vayas

C.C. 1805085014

AUTORA

APROBACIÓN DEL TRIBUNAL GRADO

En calidad de par calificador del Informe Final del Trabajo de Titulación presentado por la señorita, Betsy Samanta Guerrero Vayas, estudiante de la Carrera de Ingeniería en Electrónica y Comunicaciones, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado **MIGRACIÓN DE LA RED Y GESTIÓN EN LA CONFIGURACIÓN AUTOMÁTICA DE EQUIPOS EN EL ISP GRUPO MEGARED**, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 17 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y al numeral 7.6 del respectivo instructivo. Para cuya constancia suscribimos, conjuntamente con la señora Presidente del Tribunal.

Ambato, marzo 2023.

Ing. Pilar Urrutia, Mg.
PRESIDENTE DEL TRIBUNAL

Ing. Mg. Andrea Sánchez
PROFESOR CALIFICADOR

PhD. José Vicente Morales
PROFESOR CALIFICADOR

DEDICATORIA

A Dios, por ser mi guía en los momentos difíciles.

A mi padre, Juan Guerrero, por sus enseñanzas y su enorme sacrificio.

A mi madre, Mariana Vayas, por su amor y apoyo incondicional.

A mi hermana, Joanna Guerrero, por confiar en mí.

A mi novio, Álvaro por estar siempre presente.

A mis amigos y compañeros de aula, por motivarme y apoyarme.

A mí, por todo el esfuerzo realizado.

AGRADECIMIENTO

A la Facultad de Ingeniería en Sistemas Electrónica e Industrial por todo el conocimiento brindado.

A la Empresa Grupo Megared, por permitirme aportar ideas para su desarrollo.

Al mi tutor, Ingeniero Santiago Manzano, por guiarme en la elaboración de este proyecto.

ÍNDICE GENERAL

PORTADA.....	I
APROBACIÓN DE TUTOR.....	II
AUTORÍA.....	III
DERECHOS DE AUTOR.....	IV
APROBACIÓN DEL TRIBUNAL GRADO.....	V
DEDICATORIA.....	VI
AGRADECIMIENTO.....	VII
ÍNDICE GENERAL.....	VIII
ÍNDICE DE FIGURAS.....	XII
ÍNDICE DE TABLAS.....	XV
RESUMEN EJECUTIVO.....	XVII
ABSTRACT.....	XVIII
CAPÍTULO I.....	19
MARCO TEÓRICO.....	19
1.1. Tema de Investigación.....	19
1.2. Antecedentes Investigativos.....	19
1.3. Contextualización del problema.....	21
1.4. Fundamentación Teórica.....	23
1.4.1. Red de Comunicaciones.....	23
1.4.2. Clasificación de red.....	23
1.4.2.1. Topología de red.....	24
1.4.2.2. Tipos de red según su alcance geográfico.....	25
1.4.2.3. Medios de transmisión.....	26
1.4.2.4. Modelo OSI.....	27
1.4.2.5. Modelo TCP/IP.....	30
1.4.2.6. Dispositivos de interconexión.....	31

1.4.3.	Enrutamiento	33
1.4.3.1.	Clasificación de enrutamiento	33
1.4.3.1.1.	Enrutamiento estático	33
1.4.3.1.2.	Enrutamiento dinámico.....	33
1.4.3.1.2.1.	Ventajas y Desventajas de enrutar	35
1.4.4.	Ciclo de vida de la red.....	36
1.4.5.	Diagrama de red	36
1.4.5.1.	SolarWinds Network Topology Mapper.....	37
1.4.5.2.	CADE.....	37
1.4.5.3.	Dia Diagram Editor.....	37
1.4.5.4.	Microsof Visio	37
1.4.6.	Emuladores de red.....	38
1.4.7.	Automatización de Red	38
1.4.7.1.	Importancia	39
1.5.	Objetivos	39
1.5.1.	Objetivo General	39
1.5.2.	Objetivos Específicos.....	39
CAPÍTULO II		40
METODOLOGÍA		40
2.1.	Materiales	40
2.1.1.	Recurso de Hardware	40
2.1.2.	Recurso de Software	40
2.2.	Métodos	41
2.2.1.	Modalidad de la Investigación	41
2.2.2.	Población y Muestra.....	42
2.2.3.	Recolección de la información.....	42
2.2.3.1.	Entrevista	42

2.2.3.2.	Observación	45
2.2.4.	Procedimiento y Análisis de Datos	45
2.2.5.	Propuesta de solución.....	45
2.2.6.	Desarrollo del proyecto	46
CAPÍTULO III.....		47
RESULTADOS Y DISCUSIÓN		47
3.1.	Análisis y discusión de los resultados	47
3.2.	Análisis de factibilidad.....	47
3.2.1.	Desarrollo de la Propuesta	48
3.2.1.1.	Levantamiento de la información de la empresa	48
3.2.1.2.	Análisis de tráfico de la red	56
3.2.1.3.	Simulación en configuración bridge.....	57
3.2.1.4.	Simulación de red ruteada propuesta.....	66
3.2.1.5.	Gestión en la administración automática de equipos.....	91
3.3.	Análisis de Resultados.....	93
3.4.	Resultados	94
CAPÍTULO IV.....		97
CONCLUSIONES Y RECOMENDACIONES.....		97
4.1.	Conclusiones	97
4.2.	Recomendaciones	98
BIBLIOGRAFÍA		100
ANEXOS		103
Anexo 1.	Investigación de campo a los diferentes nodos de comunicaciones	103
Anexo 2.	Verificación de tráfico en nodos de red	105
Anexo 3.	Instalación EVE-NG	108
Anexo 4.	Tabla de enrutamiento IPv6 por equipo.....	113

Anexo 5. Código de programación de enrutamiento dinámico OSPF en ruta propuesta	115
Anexo 6. Programación de archivos .json y .py	129

ÍNDICE DE FIGURAS

Figura 1. Topologías de red física.....	24
Figura 2. Tipos de red según su alcance geográfico.	26
Figura 3. Medios de transmisión guiada	26
Figura 4. Medios de transmisión no guiada	27
Figura 5. Capa física del modelo OSI.....	28
Figura 6. Comparación entre el modelo OSI y el modelo TCP/IP	31
Figura 7. Protocolos de enrutamiento.	34
Figura 8. Ciclo de Investigación NDLC	36
Figura 9. Nodos de comunicación de la Empresa Grupo Megared	49
Figura 10. Diagrama de topología física del ISP Grupo Megared.....	54
Figura 11. Diagrama lógico de red del ISP Grupo Megared	55
Figura 12. Simulación de red bridge actual de la ISP Grupo Megared	58
Figura 13. Prueba de tráfico en la configuración actual del ISP Grupo Megared: BRIDGE.....	61
Figura 14. Prueba de tráfico en configuración BRIDGE con la herramienta jperf: 20,09 kbps	62
Figura 15. Captura de tráfico UDP en prueba en configuración BRIDGE con 20,09kbps	62
Figura 16. Prueba de tráfico con 20,09kbps en configuración Bridge.....	64
Figura 17. Prueba de tráfico en configuración BRIDGE con la herramienta jperf: 679,79 kbps	64
Figura 18. Prueba de tráfico con 679,79 kbps en configuración Bridge.....	66
Figura 19. Router CCR2004-16GB-2S+PC para nodo Quero 2 de respaldo	68
Figura 20. Diagrama de red física propuesta	70
Figura 21. Diagrama de crecimiento de usuarios con servicio inalámbrico en el ISP Grupo Megared	72
Figura 22. Propuesta de topología lógica de red para el ISP Grupo Mgeraed	76
Figura 23. Simulación propuesta de red ruteada OSPF	77
Figura 24. Asignación de direcciones IP a cada interfaz	78
Figura 25. Asignación del parámetro de Router ID en OSPF.....	78
Figura 26. Designación de redes OSPF al área backbone	79

Figura 27. Rutas del router BALANCEADOR son desactivar interfaz bridge.	79
Figura 28. Ingreso a router La Independencia vía Winbox.....	80
Figura 29. Ruta por defecto redistribuida por router Balanceador	80
Figura 30. Inhabilitar la ruta por defecto con gateway 192.168.x.x	81
Figura 31. Métrica OSPF consideraba para rutas de respaldo	82
Figura 32. Costo de rutas de respaldo en router del nodo Shaushi	83
Figura 33. Simulación de caída de interfaz ether8 del router de borde: Balanceador	84
Figura 34. Rutas OSPF alcanzables por interfaz ether8.....	85
Figura 35. Desactivación de interfaz ether8 del router balanceador.....	85
Figura 36. Recalculo de ruta OSPF una vez desactivada la interfaz ether8.....	86
Figura 37. Prueba de tráfico en la configuración actual del ISP Grupo Megared: OSPF	87
Figura 38. Envío de paquetes UDP para prueba de tráfico en red OSPF	88
Figura 39. Captura de tráfico UDP en red OSPF con Wireshark	89
Figura 40. Prueba de tráfico con 20,09kbps en configuración OSPF.....	89
Figura 41. Prueba de tráfico con 679,79kbps en configuración OSPF.....	91
Figura 42. Eliminación de la dirección de loopback para prueba de configuración automática	92
Figura 43. Ejecución de script.py para la reconfiguración de equipo.....	93
Figura 44. Configuración de interfaz loopback mediante api-rest.....	93
Figura 45. Comparación de pruebas de tráfico UDP con 20,09 y 679,79 kbps en red BRIDGE.....	94
Figura 46. Comparación de pruebas de tráfico UDP con 20,09 y 679,79 kbps en red OSPF	94
Figura 47. Comparación de pruebas de tráfico UDP entre red bridge y red OSPF con 20,09kbps	95
Figura 48. Comparación de pruebas de tráfico UDP entre red bridge y red OSPF con 679,79kbps	96
Figura 49. Documentación de EVE-NG	108
Figura 50. Software de virtualización VMware.....	109
Figura 51. Archivo VMDK para simulación de RouterOs	109
Figura 52. Utilización del Software FilleZila para la transferencia de archivos.....	110

Figura 53. Entorno de emulación EVE-G.....	110
Figura 54. Ingreso a la consola de router mediante la Putty	111
Figura 55. Ingreso a equipos internos de red mediante RoMON	112
Figura 56. Equipos de red accesibles mediante conexión RoMON.....	112

ÍNDICE DE TABLAS

Tabla 1. Dispositivos de interconexión según niveles de comunicación	32
Tabla 2. Ventajas y desventajas de enrutar una red	35
Tabla 3. Recursos de Hardware	40
Tabla 4. Recursos de Software	40
Tabla 5. Coordenadas de los nodos del ISP Grupo Megared.....	48
Tabla 6. Tabla de equipos por nodo e interfaces.....	49
Tabla 7. Configuración de router CCR1072-1G-8S+ en nodo Quero 1	50
Tabla 8. Configuración de router CCR1072-1G-8S+ en nodo Tisaleo.....	51
Tabla 9. Configuración de router CCR1036-8G-2S+ en el nodo Quero 2.....	51
Tabla 10. Configuración de router/switch CRS326-24G-2S+ en el nodo Quero 1 ..	52
Tabla 11. Configuración de router 3011UiAS en el nodo Mocha	52
Tabla 12. Configuración de router CCR2004-1G-12S+2XS en el nodo San Pedro de Sabañag	52
Tabla 13. Configuración de router RB750Gr3 en el nodo de Santa Fe de Galán	53
Tabla 14. Configuración de router CCR1016-12G en el nodo Shaushi.....	53
Tabla 15. Velocidad de bajada por nodo en horas pico de consumo	56
Tabla 16. Cantidad de Radioelaces, antenas sectoriales y clientes por nodo.....	57
Tabla 17. Ancho de banda del ISP Grupo Megared y Ancho de banda soportada en la simulación	59
Tabla 18. Comparación de velocidad máxima de bajada en el ISP Grupo Megared y en EVE-NG	60
Tabla 19. Escenarios de emulación de tráfico.....	61
Tabla 20. Pruebas de tráfico UDP con 20,09 kbps en configuración bridge	63
Tabla 21. Pruebas de tráfico UDP con 679,79 kbps en configuración bridge	65
Tabla 22. Características para elección de equipos de enrutamiento	67
Tabla 23. Cuadro comparativo de especificaciones de routers Mikrotik para nodo Quero 2.....	67
Tabla 24. Cuadro comparativo de especificaciones de routers Mikrotik para nodos: Quero 1 y La Independencia	68
Tabla 25. Comparación física de router Mikrotik para nodos: Quero 1 y La Independencia	69

Tabla 26. Crecimiento del servicio inalámbrico en el ISP Grupo Megared	71
Tabla 27. Direccionamiento IP para enlaces de routers principales	74
Tabla 28. Direccionamiento IP para clientes con servicio inalámbrico	75
Tabla 29. Métricas OSPF en rutas de respaldo	82
Tabla 30. Pruebas de tráfico UDP con 20,09 kbps en configuración OSPF	87
Tabla 31. Pruebas de tráfico UDP con 679,79 kbps en configuración OSPF	90

RESUMEN EJECUTIVO

Este proyecto investigativo se realizó con el propósito de mejorar la disponibilidad del servicio de los clientes que pertenecen al ISP Grupo Megared. Para ello se realizó una investigación campo, visitando cada nodo de la red y verificando sus conexiones con el fin de obtener un diagrama físico y lógico de la red mediante la utilización de herramientas como Winbox para el acceso a los dispositivos de red y Microsoft Visio para la representación gráfica de la estructura de la red.

Posteriormente, se propuso un diagrama de red físico analizando los requerimientos de rutas de respaldo, en donde se agregaron 3 routers Mikrotik en nodos que manejan un alto tráfico y gran cantidad de clientes. A la vez, se propone un diagrama lógico de red tomando como referencia la tasa de crecimiento del sector inalámbrico del ISP Grupo Megared. Este diagrama lógico posee una configuración de enrutamiento dinámico OSPF, permitiendo la creación de rutas de respaldo.

Toda la migración de red y pruebas de su funcionamiento se las realizó en el simulador EVE-NG por su sencillez en la configuración de equipos. Para las pruebas se utilizó la herramienta jperf que trabaja con java, creando un servidor jperf en una interfaz del router de borde y un cliente jperf en el nodo más alejado de la red, obteniendo resultados de latencia, rendimiento y pérdida de paquetes UDP de lo cual se concluyó que la configuración bridge posee una pérdida de paquetes del 1,08% en comparación a la configuración OSPF que posee una pérdida de paquetes del 0,4% pero la red OSPF posee un mayor tiempo de respuesta en comparación a la red bridge.

Finalmente, se utilizó la herramienta API-REST para la configuración de equipos, en donde se creó un script de ejecución .py. La prueba se realiza asumiendo que por error humano se haya eliminado una dirección IP del router de borde, y que al ejecutar script.py pueda reconfigurar la dirección eliminada.

Palabras clave: OSPF, bridge, jperf, eve-ng, api-rest, RTT, Packet Loss, UDP

ABSTRACT

The purpose of this research project was to improve the availability of internet service of the Grupo Megared company. A field investigation was conducted, visiting each node of the network and verifying its connections in order to obtain a physical and logical diagram of the network using tools such as Winbox for access to network devices and Microsoft Visio for graphical representation of the network structure.

A physical network diagram was then proposed analyzing backup path requirements where 3 Mikrotik routers were added in nodes handling high traffic and large number of clients. At the same time, a logical network diagram is proposed taking as reference the growth rate of the wireless sector of the ISP Grupo Megared. This logical diagram has an OSPF dynamic routing configuration, allowing the creation of backup routes.

All the network migration and tests of its operation were carried out in the EVE-NG simulator for its simplicity in the configuration of equipment. For the tests, the jperf tool that works with java was used, creating a jperf server in an interface of the border router and a jperf client on the farthest node in the network, obtaining results of latency, throughput and loss of UDP packets which was concluded that the bridge configuration has a packet loss of 1.08% compared to the OSPF configuration which has a packet loss of 0.4% but the OSPF network has a longer response time compared to the bridge network.

Finally, the API-REST tool was used for the configuration of computers, where a .py execution script was created. The test is performed assuming that an IP address has been removed from the border router by human error, and that running script.py can reconfigure the removed address.

Keywords: OSPF, bridge, jperf, ene-ng, api-rest, RTT, Packet Loss, UDP

CAPÍTULO I

MARCO TEÓRICO

1.1. Tema de Investigación

Migración de la red y gestión en la configuración automática de equipos en el ISP Grupo Megared.

1.2. Antecedentes Investigativos

En los últimos tiempos, la eficiencia de administración manual de red se ha visto afectada a medida que la red empresarial crece. Si existe algún cambio en servidores o almacenamiento de la empresa, la configuración de red debería cambiar automáticamente.

En el año 2015, según el trabajo investigativo realizado por Johnny Bayas, denominado: “Servidor de control de dispositivos y servicios mediante el protocolo SNMP para la red de datos CELEC.E.P. unidad de negocios Hydroagoyan” menciona que es importante tener una representación gráfica del comportamiento de la red para que el usuario administrativo pueda acceder a la información de manera eficaz y rápida. De esta manera optimizar el tiempo de solución a problemas presentados en el funcionamiento de equipos en la red. [1]

En el año 2018, según el trabajo investigativo realizado por Freddy Freire, denominado: “Análisis y Propuesta de mejoramiento del sistema de seguridad perimetral aplicable a institución pública de seguridad social” propone un mejor control lógico de red mediante la utilización del Protocolo STP (Spanning Tree Protocol) en cada uno de los dispositivos switch, ya que las conexiones de red se encuentran en modo bridge. Este protocolo evita las tormentas de difusión debido a su característica de “crear una topología lógica sin bucles” en la red. [2] A la vez, menciona que la creación de VLAN (Red de Área Local Virtual) segmenta subredes

dentro de una red y se utiliza para una mejor administración en red plana, pero al tener en cuenta que los switches crean “dominios de broadcast” los cuales aumentan la posibilidad de generar una tormenta de difusión en la comunicación, es necesario implementar direccionamiento a las tramas, mencionando que para evitar este inconveniente es necesario implementar dispositivos de enrutamiento. [2]

En el año 2020, según el trabajo investigativo realizado por Manuel Jesús Mendoza, denominado: “Automatización de redes informáticas con Python”, resalta que en la actualidad la utilización de herramientas de automatización de redes informáticas es un ente fundamental en grandes empresas, puesto que permite el control de todo tipo de red. [3]

En el año 2020, según el trabajo investigativo realizado por Fiade, Augustin y Masruroh denominado: “Analysis of Failover Link System Performance in OSPF, EIGRP, RIPV2 Routing Protocol with BGP” menciona que al realizar pruebas de convergencia para rutas de respaldo entre los protocolos OSPF, EIGRP y RIPv2. OSPF posee el menor tiempo de convergencia de la red actualizando sus tablas de enrutamiento en un tiempo estimado de 7,23 segundos a diferencia de EIGRP con 10,45 segundos y RIPv2 con 9,96 segundos. [4]

En el año 2021, según el trabajo investigativo realizado por Byron Oviedo, denominado: “Voz IP seguras implementadas en Redes Definidas por Software” realizó una implementación de una red pequeña utilizando un switch, un router Mikrotik y 2 teléfonos, en donde efectuó pruebas de ancho de banda, tiempo de respuesta y latencia utilizando la herramienta jperf como simulador de tráfico UDP. En donde se obtiene parámetros del rendimiento emulando el envío de 500 paquetes de datos UDP solo con 1 prueba de ejecución. [5]

Entonces, es importante mencionar que debido a los estudios citados: tener una representación física de la red ayuda a optimizar tiempos de respuesta para problemas que surgen en la misma. Sin embargo, es necesario poseer una correcta conexión física y lógica de la red, para evitar inconvenientes generados en la transmisión y direccionamiento de la información, adaptando la misma a una nueva

conexión lógica cuando una empresa ya se encuentre establecida. [2][6]. Así mismo, la implementación de nuevas herramientas administrativas de código abierto, es una opción innovadora en el manejo administrativo de la red ya que permite la automatización de redes mitigando fallas humanas cometidas por el administrador de red al momento de solucionar bucles o inconvenientes producidos en la misma. Mejorando así, el tiempo de respuesta a cortes del servicio. [3]

1.3.Contextualización del problema

Desde el inicio de la pandemia se intensifica la necesidad de utilizar el acceso a internet para que las personas puedan estar conectadas en su trabajo, en sus estudios y, a la vez, que puedan comunicarse entre sí. Es por esto que las estructuras de los Proveedores de Servicios de Internet (ISP) en América Latina, han evidenciado un gran crecimiento debido al incremento de usuarios que acceden a una conexión del servicio de internet. En el año 2021 los usuarios que cuentan con una conexión de internet incrementaron en un 17.3% en comparación a los usuarios con acceso a internet en el año 2020[7]. Así mismo, en el año 2021, Ecuador evidencia un crecimiento del 1,5% de usuarios de internet fijo, en comparación al año anterior.

Es por esta razón que la mayoría de emprendedores que implementaron un sistema de telecomunicaciones, iniciaron con un diagrama de red muy básico, como, por ejemplo: una conexión a internet, un router y un nodo con cierta cantidad de Access Point. Para la utilización de estos equipos, resulta muy práctico conectar estos dispositivos en modo Bridge [8] que, según Bradley Mitchell en su publicación “Use a Bridge to Expand Your Local Network” menciona que Una Red Plana o red Bridge “permite la comunicación entre dos redes y proporciona una forma de que funcionen como una sola red”. [9]

Dado esto, la eficacia de implementar una red plana en un nodo será óptima si en el mismo existe una cantidad minúscula de clientes. Pero al existir un crecimiento en la red del WISP (Proveedor de Servicio de Internet Inalámbrico), la red plana comienza a generar dificultades propias de capa 2. [8] En la cual, la principal causa de problemas en una conexión de capa 2, es la tormenta de difusión, generando bucles

en la red tipo bridge mediante la creación de copias de tramas en el envío de datos provocando que el tráfico aumente exponencialmente. Este tráfico vuelve a generar bucles en la red e induce a que el CPU de los switches o routers trabaje al 100% de su capacidad, reduciendo su funcionalidad y presentando una caída eminente en la red. [10]

Otro aspecto importante por el cual la red de comunicaciones no puede tener una correcta funcionalidad es porque no existe una manipulación de equipos de administración de red. El administrador de red necesita ingresar a cada uno de los equipos de administración como, por ejemplo: routers, switches, puntos de acceso y servidores, en donde el peor escenario es un error humano, “este error ha entregado entre el 40% al 80% de las causas de falla en la implementación de red. Dicho escenario mitiga la funcionalidad de la red hasta el punto de negar el acceso al servicio de internet, por lo cual existirá inconformidad por parte de los usuarios. [11]

En Latinoamérica, según un comunicado de prensa emitido por la empresa Subtel el 29 de marzo del 2022, menciona que existe un 0,000504% de reclamos de internet fijo en el informe presentado en octubre del 2021 que, en comparación al promedio de reclamos del año 2020 se ha reducido en un 55%. [7] No obstante, los reclamos de la funcionalidad de internet fijo lideran los resultados de la encuesta conjuntamente con telefonía.

En Ecuador, ARCOTEL (Agencia de Regulación y Control de las Telecomunicaciones) menciona que ha atendido alrededor de 3505 solicitudes por parte de la ciudadanía ecuatoriana, tomando en cuenta que ARCOTEL trabaja como último medio de requerimiento ciudadano después de la atención brindada en los ISP, “el 90.81% de estos requerimientos corresponden a reclamos” de los cuales el 0,15% pertenecen a la provincia de Tungurahua[9]. Así también, entre los principales reclamos destacan la “Calidad de la comunicación, cobertura y cortes de servicio”[9].

La empresa Grupo Megared ubicada en el Cantón Quero de la provincia de Tungurahua se enfoca en brindar un soporte técnico de manera rápida y eficaz, con distribución de personal técnico y administrativo. Sin embargo, en el transcurso del

año 2021 e inicios del 2022 ha presentado bucles en la red inalámbrica que posee una conexión tipo Bridge y a la vez han existido errores humanos en la configuración de equipos por parte del administrador de red, esto ha generado diversas dificultades empresariales, como, por ejemplo: gastos financieros inesperados, pérdida de tiempo, reorganización de personal técnico, malestar en los clientes y solicitud de retiros del servicio de internet.

Con el fin de mitigar los inconvenientes presentados en la red y mejorar el tiempo de respuesta a la solución de bucles en la misma, se pretende desarrollar un estudio en donde se apliquen nuevas herramientas de administración de la red, se mejore la comprensión de conexiones mediante diagramas y a la vez, generar nuevas rutas lógicas de conexión para mejorar funcionalidad y la administración remota de la red.

1.4.Fundamentación Teórica

1.4.1. Red de Comunicaciones

Una red de comunicaciones es el conjunto de dispositivos interconectados mediante la utilización de medios guiados (cable, fibra óptica, etc.) y/o medios no guiados (señales de transmisión, etc). Los cuales permitan el intercambio de información.
[10]

1.4.2. Clasificación de red

La red posee varios tipos de interconexión, sea este lógico o físico, y distinto alcance geográfico según la necesidad de los usuarios conectados a la misma. Dado esto, las redes pueden clasificarse según: su topología, tipo, tecnología utilizada, arquitectura y por su medio de conexión. A continuación se detalla cada una de las clasificaciones.

1.4.2.1.Topología de red

La topología de red es el modo de conexión mediante el cual varios dispositivos pueden comunicarse entre sí. Existen 2 tipos de topologías de red: física y lógica. [12]

Topología de red física

La topología de red física se refiere a la forma estructural de conexión de los distintos componentes de una red, que pueden estar conectados mediante cables o medios inalámbricos. [13] Existen 3 tipos de conexión física más utilizadas en una red de comunicación: Estrella, anillo y bus.

- Estrella: Todos los dispositivos de red se encuentran conectados a un nodo central.
- Anillo: Cada dispositivo se encuentra conectado con su vecino, el último dispositivo se conecta con el primero formando un círculo. Si un elemento de red falla, toda la red cae.
- Bus: Especialmente utilizados en redes LAN, todos los dispositivos o nodos se encuentran conectados a “un mismo medio que transporta información”.

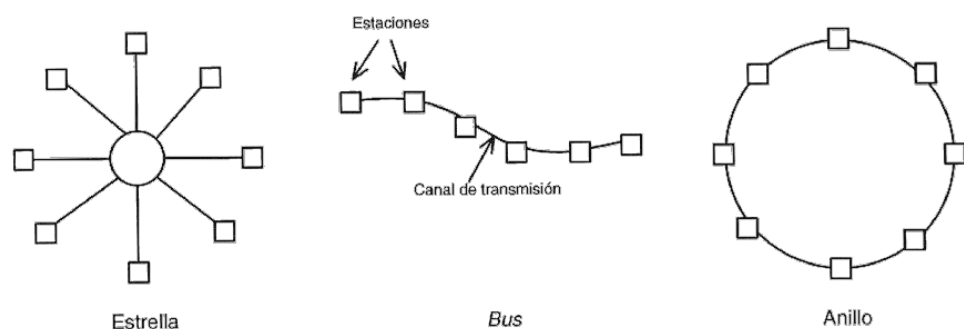


Figura 1. Topologías de red física

Fuente: <https://thales.cica.es/rd/Recursos/rd99/ed99-0432-01/seccion/topolog.html>

Topología de red lógica

La topología de red lógica está relacionada al modo en que son transmitidos los datos mediante el medio de comunicación. Existen 2 topologías lógicas de red: broadcast, también conocida como topología bus y transmisión de tokens conocida como topología de anillo. [14]

- Broadcast (difusión): Es el modo de transmisión en la que todos los dispositivos pertenecientes a la red, reciben el mensaje transmitido.
- Trasmisión de tokens: Los datos se transmiten de un punto a otro. Cada dispositivo conectado al anillo recibe y envía la señal, si el mensaje no está dirigido a él, el dispositivo lo pasa al siguiente.

1.4.2.2. Tipos de red según su alcance geográfico

- PAN (Red de Área Personal): Interconexión inalámbrica entre dispositivos que se encuentran a pocos metros o centímetros unos de otros.
- LAN (Red de Área Local): Se encuentran en conexiones de dispositivos que pertenecen a un mismo edificio y/o que alcanzan distancias de 200m hasta 450m (en tecnología inalámbrica). [15]
- MAN (Red de Área Metropolitana): También conocida como red de “banda ancha”, está ubicado en ciudades o empresas que poseen distancias de hasta 7km. [15]
- WAN (Red de Área Mundial): Red que surge de la interconexión de redes, estas redes se encuentran ubicadas en continentes o a nivel mundial.

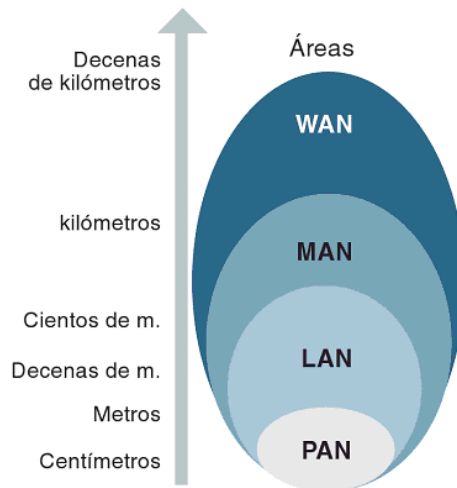


Figura 2. Tipos de red según su alcance geográfico.

Fuente: Redes locales [15]

1.4.2.3. Medios de transmisión

Un medio transmisión es aquel que permite la conexión entre dispositivos. Estos medios pueden clasificarse como guiados o no guiados.

Los medios de transmisión guiados son aquellos que poseen un conductor físico para poder conectar los dispositivos entre sí. Como, por ejemplo: par trenzado, fibra óptica, cable coaxial, etc. [16]



Figura 3. Medios de transmisión guiada

Elaborado por: La investigadora.

Los medios de transmisión no guiados pueden conectar dispositivos, pero sin la utilización de un medio de conexión físico. Como, por ejemplo: Radioenlaces, transmisión satelital, transmisión inalámbrica, microondas, etc.



Figura 4. Medios de transmisión no guiada

Fuente: <https://docplayer.es/>

1.4.2.4. Modelo OSI

El modelo OSI (Interconexión de sistemas abiertos), fue un diseño creado para simplificar la complejidad de la red y facilitar la solución de problemas de red. Es un modelo de referencia que define la manera en que los mensajes podrían ser transmitidos entre 2 puntos o nodos en una red de comunicación. [17]

El modelo OSI divide la red de telecomunicación en 7 capas:

1. Capa física
2. Capa de enlace de datos
3. Capa de red
4. Capa de transporte
5. Capa de sesión
6. Capa de presentación
7. Capa de aplicación

Capa física: Define las especificaciones eléctricas, mecánicas y funcionales para la activación, mantenimiento y desactivación de la conexión física entre 2 sistemas de comunicación de red. [18]

Así también, convierte las señales a bits. Esta capa especifica la manera en la que un dispositivo envía y recibe información.

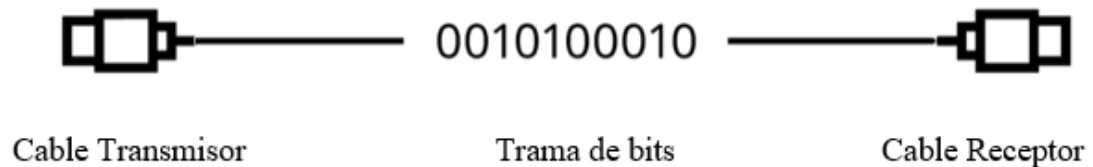


Figura 5. Capa física del modelo OSI

Fuente: <https://www.siemxpert.com/>

Capa de enlace de datos: Brinda la transmisión confiable de datos a través del enlace físico de red. En esta capa interviene el direccionamiento físico, la topología de red, las notificaciones de error, la secuencia de la trama y el control de flujo. [18]

- Direccionamiento físico (direccionamiento de red): Explica como los dispositivos están dirigidos o encaminados a la capa de enlace de datos.
- La Topología de red: define en como los dispositivos de red se encuentran conectados físicamente, mencionados con anterioridad.
- Notificación de error: Alerta a las capas superiores que ha ocurrido un error en la transmisión.
- Secuencia de la trama: Reordena los datos de las tramas que son transmitidas fuera de la secuencia.
- Control de flujo: Modera la transmisión de datos para que los dispositivos receptores no se saturen con el tráfico.

La capa de enlace de datos fue subdividida en 2 capas por la IEEE (Instituto de Ingenieros Eléctricos y Electrónicos) las cuales fueron: LLC y MAC. [18]

LLC (Control de Enlace Lógico): Administra la comunicación entre dispositivos a través de un único enlace de red, admite servicios orientados a la conexión (“establecimiento de la conexión, transferencia de datos, y fin de la conexión”) y sin

conexión (“elección dinámica de camino y asignación dinámica del ancho de banda”). [18]

MAC (Control de Acceso al Medio): La especificación IEEE MAC define las direcciones MAC, que permitir que múltiples dispositivos se identifiquen de forma única entre sí en la capa de enlace de datos.

Capa de red: Ofrece un método de comunicación desde un sistema a otro, en donde se encarga de brindar una ruta para que los datos puedan llegar a su destino, para ello se utilizan las direcciones IP pertenecientes a conjuntos de subredes. [19]

La capa 3 del modelo OSI posee un proceso de comunicación que se dividen en 4 pasos: [20]

1. Direccionamiento
2. Encapsulación
3. Enrutamiento
4. Desencapsulación

1. Direccionamiento: Mecanismo que direcciona los equipos terminales. Si la información desea ser enviada a un equipo final, dicho equipo o host debe tener una dirección única. [20]
2. Encapsulación: La capa de red recibe el protocolo de unidades de datos (PDU) y con una etiqueta de capa 3. Cuando se crea dicho paquete, el encabezado o etiqueta de capa 3 debe tener la dirección de destino y la dirección de origen. [20]
3. Enrutamiento: El paquete debe estar guiado a través de la red para llegar a su destino final mediante equipos enrutadores, estos equipos seleccionan las rutas y las dirigen hacia su destino. [20]
4. Desencapsulación: El dispositivo final elimina el encabezado del protocolo de unidades de datos (PDU) insertados antes del enrutamiento de información. [20]

Capa de transporte: Acepta los datos desde la capa de sesión y los segmenta para transportarlos a través de la red. En esta capa ocurre el control de flujo.

El control de flujo administra la transmisión de datos entre dispositivos debido a que los equipos de transmisión no deben enviar más información que los dispositivos de recepción puedan procesar. Los protocolos de transporte utilizados en internet son: TCP y UDP. [18]

Capa de sesión: Se encarga de administrar y configurar sesiones de comunicación que consisten en los servicios de pregunta y respuesta que ocurren entre la capa de aplicación localizada en los diferentes equipos de red. [18] Así también coordina la comunicación, organizándola de 3 modos diferentes: simplex, half dúplex y full dúplex. [21]

Capa de presentación: Esta capa provee código y funciones de conversión. Los computadores están configurados para recibir los datos encriptados y después de esto los transforman a su formato inicial antes de la transmisión, por ejemplo, código EBCDIC, ASCII. Esta capa posee protocolos que definen cómo los datos deberían ser formateados o encriptados. Procesos como: compresión, descompresión, encriptación y desencriptación de datos están relacionados a esta capa. [21]

Capa de aplicación: Proporciona los servicios de red a los usuarios finales, como, por ejemplo: La transferencia, acceso y administración de archivos (FTAM), servicios de correos y de directorios.

1.4.2.5. Modelo TCP/IP

El modelo TCP/IP fue creado antes que el modelo OSI, cuenta con 4 capas en total:

1. Capa de enlace de datos
2. Capa de red
3. Capa de transporte
4. Capa de aplicación

La diferencia entre el modelo OSI con el modelo TCP/IP es que en este modelo la capa de aplicación es el conjunto de capas de presentación, sesión y aplicación del modelo OSI.

A continuación, se presenta un cuadro comparativo entre los 2 modelos.

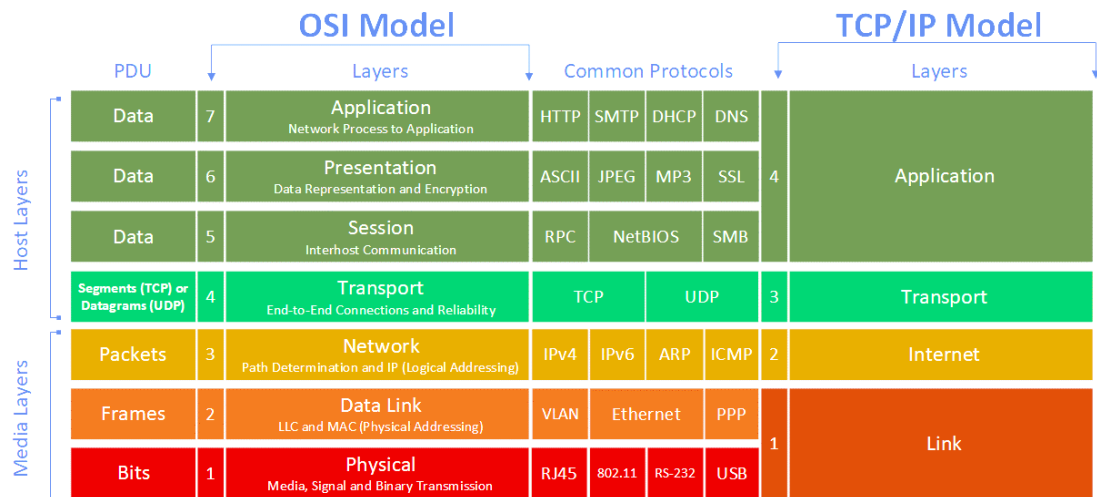


Figura 6. Comparación entre el modelo OSI y el modelo TCP/IP

Fuente: <https://itadmins.es/>

1.4.2.6. Dispositivos de interconexión

Tomando como referencia la información del modelo OSI, se presenta los distintos tipos de dispositivos según su capa de aplicación. Estos dispositivos permiten la interconexión con los equipos finales de red y constituyen el hardware de la misma.

[22]

Tabla 1. Dispositivos de interconexión según niveles de comunicación

Elaborado por: La investigadora [22]

Nivel	Dispositivo	Imagen	Descripción
Nivel Físico	Repetidor		Extienden las señales transmitidas.
	Hub o concentradores		Permiten un solo punto de conexión para varios dispositivos.
	Modem		Modula y demodula señales pertenecientes al canal de tx.
Nivel de enlace de datos	Puentes o bridge		Seleccionan la transmisión de tramas de datos locales y no locales mitigando la congestión de a red.
	Switch		Enlazan la comunicación de redes LAN preservando el ancho de banda.
Nivel de red	Router		Dirige o enruta el tráfico de red seleccionando varios caminos de transmisión.
	Switch Capa 3		Realiza las funciones de un router con la diferencia que utiliza enrutamiento mediante hardware.
Nivel superior	Switch capa 4		Conmuta paquetes utilizando direcciones IP y puertos TCP/UDP. Brinda acceso a capa de aplicación.

1.4.3. Enrutamiento

“El enrutamiento es un proceso que facilita a elementos o dispositivos de interconexión disponer de la mejor ruta en la emisión y recepción de los mensajes. La cual está basada en la capa de red del modelo OSI” [23]

1.4.3.1. Clasificación de enrutamiento

Se establece por la configuración de las tablas de enrutamiento existentes en dispositivos de capa 3, dependiendo de la forma que se ingresen los datos, se clasifica en 2 tipos: enrutamiento estático y dinámico. [24]

1.4.3.1.1. Enrutamiento estático

Es el proceso de configurar rutas entre dispositivos de forma manual. Si el diseño de la red cambia las rutas deberán configurarse nuevamente debido a que las tablas de enrutamiento estático no se actualizan automáticamente. [25]

1.4.3.1.2. Enrutamiento dinámico

Permite que las tablas de enrutamiento presentes en los dispositivos de capa 3, se modifiquen en tiempo real mientras que el diseño de la red lógica cambia. Los protocolos y algoritmos de este tipo permiten que la tabla se cree y se actualice. [26]

A continuación, se presentan los protocolos pertenecientes al enrutamiento.

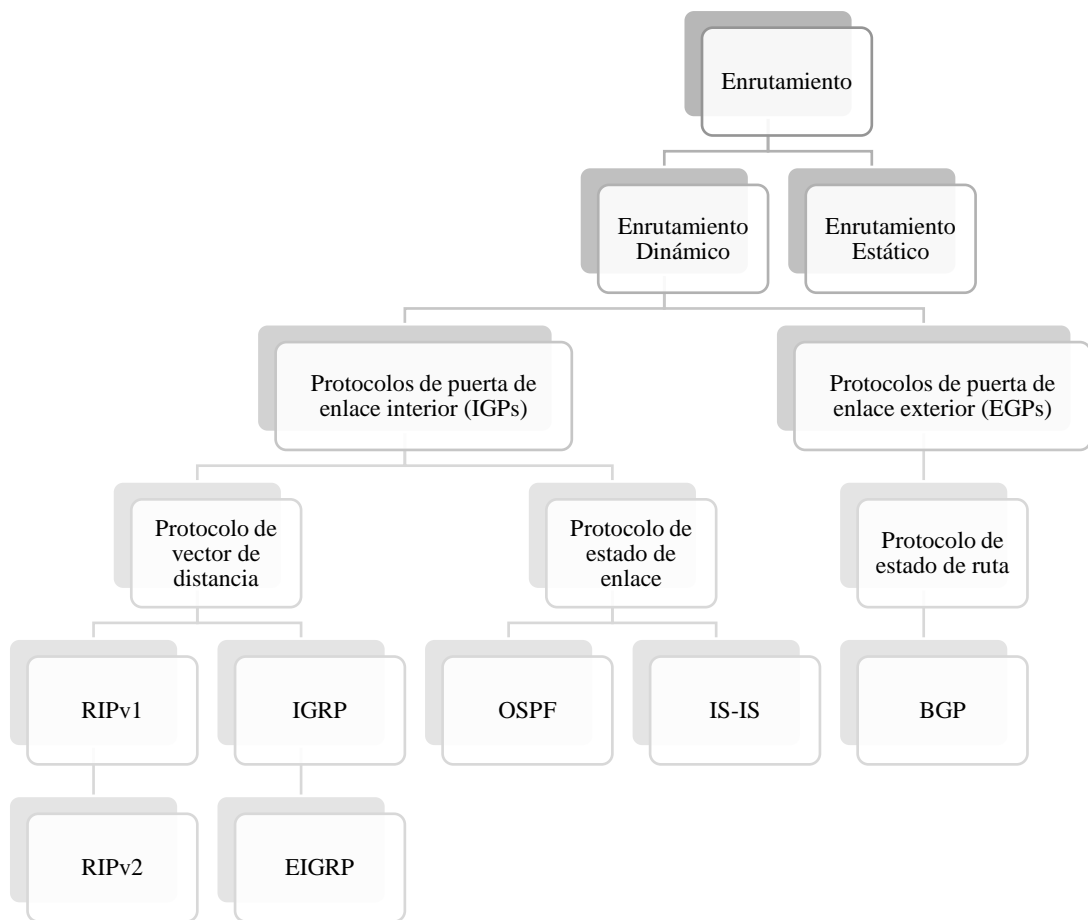


Figura 7. Protocolos de enrutamiento.

Elaborado por: La investigadora

Los protocolos de enrutamiento fueron creados para que los dispositivos pertenecientes a la capa de red del modelo OSI intercambien sus tablas de enrutamiento. Existen 2 tipos de protocolos de enrutamiento dinámico basados en los algoritmos que utilizan: Vector distancia y Estado de enlace.

Vector distancia: Original de ARPANET utilizado en Internet con el nombre de RIP, en donde cada nodo tiene una tabla de encaminamiento y, a la vez, conoce el coste y la distancia del enlace que une con sus vecinos. [27]

Estado de enlace: Permite crear una tabla de enrutamiento definiendo los caminos que tomará un paquete hasta llegar el destino basándose en la medición del coste y la distancia del router con sus vecinos. Funcionando de la siguiente manera:

- Utiliza el algoritmo de Dijkstra para poder calcular las rutas óptimas con un valor de coste mínimo. [28]
- Construye un paquete LSP (Link State Packet – Paquete de estado de enlace) en donde indica la información del remitente y un listado de los equipos vecinos con la distancia entre ellos (coste). [28]
- Se envía un LSP por inundación a todos los routers de la red cuando existen cambios en la misma. Los paquetes de estado de enlace se enumeran con un tiempo de vida limitado, y se actualice la tabla de enrutamiento. [28]

1.4.3.1.2.1. Ventajas y Desventajas de enrutar

Siendo la capa de red la responsable del direccionamiento lógico y enrutamiento IP, ICMP, ARP, RIP, IGRP y enrutadores, posee ciertas ventajas y desventajas al momento de implementar una red. Dicha información se detalla en la siguiente tabla.

Tabla 2. Ventajas y desventajas de enrutar una red

Fuente: [29]

Ventajas	Desventajas
Se adapta a la topología física enrutando el tráfico	La ruta tomada depende de la topología actual
Evita el inundamiento de la información transmitida	Aumento en el consumo de CPU, RAM
La mayoría de las empresas necesitan control de la red. Los controles de enrutamiento ocurren en la capa 3.	La velocidad debido a toda la sobrecarga adicional, y eso puede ser mortal en redes de sitios múltiples donde las comunicaciones rápidas entre decenas o cientos de computadoras
Proporciona tecnologías de conmutación y enrutamiento, creando rutas lógicas, para transmitir datos de nodo a nodo.	Inversión económica elevada debido al costo que posee cada enrutador.

1.4.4. Ciclo de vida de la red

El Ciclo de Vida de Desarrollo de Redes (NDLC) es un método que utiliza la planificación de la estrategia empresarial, la aplicación ciclo de vida de desarrollo de red y análisis de distribución de datos. [30]. A continuación, se presenta el diagrama NDLC:

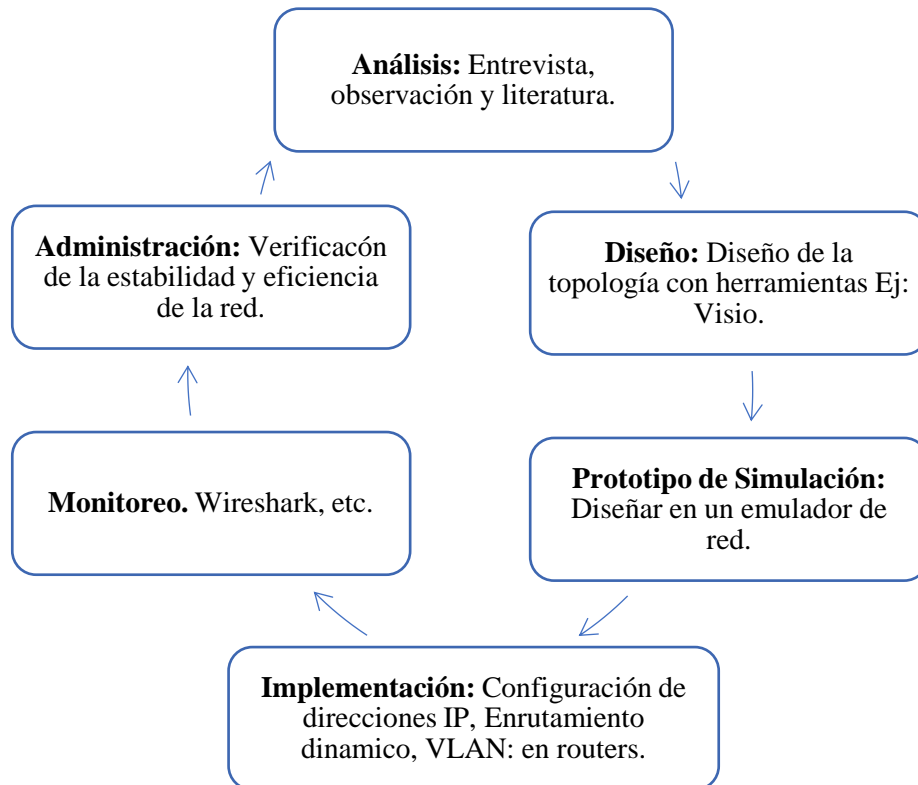


Figura 8. Ciclo de Investigación NDLC

Fuente: [30]

1.4.5. Diagrama de red

Un diagrama de red es la representación gráfica de la estructura de una red, en donde se simbolizan los elementos y su funcionalidad dentro de la red informática. Un diagrama de red, puede contener varios detalles como, por ejemplo, direccionamiento IP en cada enlace, identificación de equipos, etc. Estos diagramas pueden ser físicos o lógicos. [31]

- Diagrama físico de red: Proporciona información de los componentes físicos de red, tales como los equipos, tipos de cables conectados, etc.

- Diagrama lógico de red: Representa la manera en que la información se transmite dentro de la red informática: direccionamiento, protocolos de enrutamiento, etc.

A continuación, se describen las distintas herramientas utilizadas para elaboración de diagramas de red. Estas herramientas fueron analizadas por DNSstuff, destacándolas por su facilidad de uso, su alcance y su rentabilidad. [32]

1.4.5.1. SolarWinds Network Topology Mapper

En el 2020, SolarWinds Network Topology Mapper fue considerada la mejor herramienta para la representación de una red, debido a su interfaz intuitiva para el usuario, y debido a que se puede trabajar por capas para identificar los distintos segmentos de red. [32]

1.4.5.2. CADE

CADE es una herramienta versátil en donde no solo se representan diagramas de red si no también se pueden construir diagramas de flujo o la creación de circuitos eléctricos. Puede modelar mapas en 2D y en 3D. [32]

1.4.5.3. Dia Diagram Editor

Programa OSS, con una amplia estantería de elementos de red. A la vez, brinda facilidad en la representación topológica de red. [32]

1.4.5.4. Microsoft Visio

Microsoft Visio se caracteriza por su interfaz gráfica intuitiva, óptima y sofisticada, su amplia gama de plantillas y elementos, y principalmente su utilización gratuita donde no existe un límite de utilización de los mismos, convirtiéndolo en una de las herramientas para la creación de diagramas de red más potentes. [32]

1.4.6. Emuladores de red

Los softwares de emulación permiten la comprensión y simulación de procesos antes de su implementación física. Esto permite que los estudiantes o interesados puedan recrear escenarios en un entorno virtual, reduciendo inversión y mejorando el diseño final del proyecto. [33]

Además de ser útiles para la comprensión de procesos, los emuladores poseen varias ventajas, entre ellas se puede mencionar:

- Aprendizaje por descubrimiento.
- Promoción de la creatividad.
- Ahorro de tiempo y dinero.
- Confianza.
- Enseñanza individualizada y domiciliaria.
- Autoevaluación.
- Evita riesgos (no se expone a situaciones de peligro).
- Repetición.
- Escenarios complejos. [34]

Entre los principales emuladores de red, se tiene: GNS3, EVE-NG.

1.4.7. Automatización de Red

La automatización es la transformación de un proceso de trabajo (generalmente humano) a un control automático que, a la vez, permite la reorganización profunda de dicho proceso. [35] Entonces, “La automatización de la red es el proceso de utilizar software para automatizar el aprovisionamiento y la gestión de la red con el fin de maximizar continuamente la eficiencia y la funcionalidad de la red” [36]

La automatización de red gestiona servicios mediante programación, la cual permite incrementar las estructuras de red optimizando la rapidez, consumando así con los requisitos de respuesta inmediata a cambios que se realicen en la red. [37]

1.4.7.1. Importancia

Según el reporte “NetOps Meets DevOps: The State of Network Automation” presentado por Red Hat en 2018, menciona que existen 4 principales objetivos empresariales por los cuales se busca automatizar la red: [38]

1. Mejorar la productividad
2. Cumplir con configuraciones
3. Mejorar la seguridad
4. Aumentar la disponibilidad

Disponibilidad, aspecto importante para este proyecto, mediante el cual se reduce la probabilidad de cometer errores humanos por parte del administrador de red, debido a la gestión automática de los dispositivos y cambios presentados. [37]

1.5. Objetivos

1.5.1. Objetivo General

- Proponer la migración de la red y gestión en la configuración automática de equipos en el ISP Grupo Megared.

1.5.2. Objetivos Específicos

- Analizar el modelo de la conexión física y lógica de la red actual del ISP Grupo Megared para su mejoramiento administrativo.
- Rediseñar la estructura lógica de la red del ISP Grupo Megared.
- Gestionar la configuración automática de equipos de red mediante la utilización de herramientas de administración.

CAPÍTULO II

METODOLOGÍA

2.1. Materiales

Esta investigación se basó en un enfoque cualitativo, en donde se utilizan herramientas como la entrevista y la observación mediante el cual se obtuvo el estado funcional actual de la empresa Grupo Megared.

Para el desarrollo de este proyecto investigativo se utilizó varias fuentes bibliográficas como son: tesis, libros digitales, artículos académicos, publicaciones de revisas. Así también el uso de una conexión a internet.

Finalmente, se utilizó materiales físicos como laptop, esferos, cuadernos, impresiones, etc. Y softwares como emuladores de red y gestores de configuración.

2.1.1. Recurso de Hardware

Tabla 3. Recursos de Hardware

Fuente: La Investigadora

Elemento	Descripción
Laptop	lenovo ideapad 320-14ikb
RAM	8,00 GB (7,88 GB usable)
Procesador	Intel(R) Core(TM) i7-7500U CPU @ 2.70GHz 2.90 GHz

2.1.2. Recurso de Software

Tabla 4. Recursos de Software

Fuente: La Investigadora

Elemento	Descripción
Sistema Operativo	Windows 10 Pro Ubuntu 10.04.2
Software de oficina	Microsoft Office Profesional Plus 2019
Software para emulación	VMware Workstation 16 player, Winbox
Varios	Wireshark, Iperf, Jperf, Visual Studio Code

2.2. Métodos

2.2.1. Modalidad de la Investigación

Investigación bibliográfica

Con el presente proyecto investigativo se planteó encontrar una solución a los inconvenientes presentados en la red, por lo tanto, es importante hacer uso de libros, revistas científicas, repositorios de la Universidad Técnica de Ambato, sitios web, etc. Ya que, con estos, se definió una vía óptima para el funcionamiento lógico y físico de la red, basándose en investigaciones anteriores.

Investigación aplicada

Ya que conjuntamente con la investigación bibliográfica, se trabajó aplicando los conocimientos adquiridos a lo largo de la carrera de Ingeniería en Electrónica y Comunicaciones. A la vez, se enlazó los conceptos teóricos con los trabajos prácticos realizados.

Investigación exploratoria

El proyecto de investigación se guió también mediante una investigación exploratoria, la cual permitió reconocer las principales causas de las fallas presentadas en la red. Y así, tener una solución más visible y óptima al problema.

Investigación de campo

Finalmente, se utilizó una investigación de campo, en donde se realizaron visitas a la Empresa Grupo Megared, con el objetivo de presenciar los inconvenientes suscitados en administración de red y conexiones de la misma, y como ha sido la reacción de los empleados y personal administrativo en la toma de decisiones.

2.2.2. Población y Muestra

Debido a que el proyecto es una propuesta de solución, no se tiene la necesidad de presentar la población y muestra, ya que se basa netamente en la funcionalidad lógica de la red.

2.2.3. Recolección de la información

Investigaciones como: tesis, artículos científicos y conferencias de investigación fueron la principal fuente de información bibliográfica. Así también el uso de un enfoque cualitativo para poder obtener información del estado actual del ISP Grupo Megared, en donde se utilizaron herramientas como la entrevista y la observación.

2.2.3.1. Entrevista

La entrevista tuvo el propósito de conocer el estado de la empresa en la actualidad. La misma que se subdivide en 3 etapas.

A continuación, se presenta la serie de preguntas realizadas al administrador de red y sus respectivas respuestas:

Parte 1: Estructura y funcionalidad de red

1. Como primer punto: nos podría comentar. ¿Con qué diseño se encuentra implementada la red?

Respuesta: Claro, la red está configurada en modo bridge, y posee una topología de red física jerárquica.

2. ¿Cuál fue el motivo por el cual se implementó aquel diseño en la red?

Respuesta: Debido a la fácil implementación de la configuración lógica modo bridge, así también existió fácil manejo en la administración de la red.

3. ¿Ha tenido inconvenientes con la funcionalidad de la red?

Respuesta: Si, en el 2021 y al inicio del primer semestre del 2022 existieron bucles de red.

4. ¿Cuáles fueron los inconvenientes detectados?

Respuesta: El principal problema que se tuvo, fue en la red inalámbrica. Debido a la lluvia, en un cable de cierto nodo de la red hubo un corto circuito, eso generó un bucle en el nodo, y como se encuentra configurado en modo bridge, ese bucle se esparció por toda la red.

5. ¿Cuál fue la solución a dichos inconvenientes?

Respuesta: Lo que primero se identifica es el acceso a los dispositivos, debido a que no se tenía acceso se deriva al personal técnico a trasladarse a cada nodo cercado de la red para determinar el inconveniente en ese sector.

6. ¿Los problemas generados han vuelto a suscitarse?

Respuesta: Si, aunque no muy seguidos.

Parte 2: Funciones del administrador de red

7. En el departamento de administración de la red de comunicación, ¿Cuántas personas se encuentran a cargo?

Respuesta: Solo una, mi persona.

8. ¿Cuáles son las funciones que realiza el administrador de red?

Respuesta: Bueno, el administrador de red brinda soporte técnico a clientes, asesora al personal técnico, por ejemplo, en la activación de equipos o configuración de los mismos. Y finalmente, está pendiente de algún fallo que se presente en la red.

9. ¿Cuál es el método de monitorización que emplean para verificar que la red se encuentre funcionando?

Respuesta: Por el momento no disponemos de un método de monitorización, pero utilizamos el software UCRM para identificar si algún dispositivo de la red haya perdido conexión con la misma.

10. Al momento de presentarse un fallo en la red. ¿Cuál es el procedimiento que sigue el administrador de red para solucionarlo?

Respuesta: Pues, verificamos si tenemos acceso a los enlaces principales o al AP con inconveniente, se visualiza el “log” en equipos y según eso se verifica la funcionalidad del resto de la red.

11. ¿Cuáles son las consecuencias que tiene la empresa mediante el fallo de la red?

Respuesta: Existe demora en la solución de los problemas al intentar buscar la fuente de error. Así mismo, el traslado del personal técnico a cada nodo de la red es una pérdida de tiempo debido a que ya existen actividades planificadas con anterioridad. Entonces, al ocurrir este inconveniente, los clientes suelen molestarse por los cortes de servicio y, por otra parte, los soportes técnicos no son atendidos a las horas programadas, eso hace que los clientes que ya tenían un soporte técnico agendado también se encuentren ofendidos por la falta de seriedad en el cumplimiento de tareas por parte de la empresa.

Parte 3: Futuro

12. Mediante los sucesos presentados en la red. ¿Posee alguna estrategia para el mejoramiento administrativo de la red?

Respuesta: Quisiera que cada nodo tenga su propia red administrativa, debido a que en la configuración modo bridge, hay que buscar el error en cada nodo de la red y no en un nodo específico como debería ser.

13. Según la estrategia analizada, ¿Cuáles sería los beneficios que espera obtener?

Respuesta: Creo que el principal objetivo es brindar un servicio de calidad a los clientes. Y también, tener un tiempo de respuesta casi inmediato a la solución de problemas para cumplir con dicho objetivo.

2.2.3.2. Observación

En este punto se realizó una inspección de las conexiones y equipos utilizados en cada nodo o torre para detallarlos en un diagrama físico de red del ISP.

2.2.4. Procedimiento y Análisis de Datos

Para determinar un procedimiento y analizar los datos se toma en consideración las siguientes actividades:

1. Analizar la investigación bibliográfica realizada.
2. Aplicar la metodología de investigación con enfoque cualitativo.
3. Determinar los principales inconvenientes presentados del ISP Grupo Megared.
4. Plantear una propuesta de solución a dicha problemática.
5. Presentar los resultados de la propuesta de solución.

2.2.5. Propuesta de solución

Migración de la red configurada en modo bridge a una red ruteada con la misma topología física implementada en la empresa, así también utilizar herramientas para la gestión en la configuración automática de los equipos pertenecientes a la red. Esta propuesta pretende brindar una solución a la tormenta de difusión generada por bucles en capa 2 “modo bridge” y a la vez, mitigar la intervención humana en los equipos de administración.

2.2.6. Desarrollo del proyecto

Para cumplir con los objetivos planteados en este proyecto de investigación, se propone la ejecución de las siguientes actividades:

- Detalle de los conceptos básicos de redes informáticas.
- Verificación de las conexiones físicas de los equipos de cada nodo mediante investigación de campo.
- Inspección de los inconvenientes presentados en la red plana del ISP Grupo Megared.
- Verificación del tráfico de la red por nodo, para la selección del equipo que se adapte a las necesidades requeridas.
- Diseño topológico de red plana actual del ISP Grupo Megared.
- Relaciones topológicas de conexión de red y protocolos de enrutamiento dinámico.
- Presentación del esquema topológico físico y lógico de la red mediante Visio.
- Selección de software de simulación de redes adecuado para la emulación de redes ruteadas complejas.
- Simulación la red ruteada propuesta con software de virtualización seleccionado.
- Validación del funcionamiento de la red mediante posibles fallos de red y su respuesta a dichos escenarios.
- Propuesta las posibles herramientas de administración de red aptas para la implementación.
- Gestión de red mediante la utilización de herramientas de administración.

CAPÍTULO III

RESULTADOS Y DISCUSIÓN

3.1. Análisis y discusión de los resultados

Resultados de entrevista:

Para emitir un resultado de la entrevista se empleó el método de análisis temático identificando ideas a partir de las respuestas del entrevistado. Esta entrevista fue realizada al administrador de red de la Empresa Grupo Megared ubicada en el Cantón Quero de la provincia de Tungurahua.

Mediante el análisis realizado, la red del ISP Grupo Megared posee bucles propios de capa 2 debido a su configuración en modo bridge. Así también, se identifica que los nodos pueden estar constituidos en una sola red y no con subredes que tengan direccionamiento. Otro punto importante es que el tiempo de respuesta a la solución de problemas es elevado, generando cortes del servicio de internet por tiempos considerablemente altos causando malestar e inconformidad en los clientes.

3.2. Análisis de factibilidad

Factibilidad Técnica

El presente proyecto de investigación cuenta con factibilidad técnica, debido a que existen todas las herramientas para la ejecución de la misma, como, por ejemplo, software de simulación, herramientas de control de tráfico, materiales de oficina, laptop, etc.

Factibilidad Económica

El proyecto es factible en el ámbito económico debido a que se trata de la reconfiguración de una red ya establecida, para lo cual se utiliza software de simulación. Así también, los gastos posteriores al proyecto como compra de equipos Mikrotik lo realizará la Empresa Grupo Megared.

Factibilidad Bibliográfica

El proyecto cuenta con factibilidad bibliográfica, ya que se hizo uso de documentos, libros, revistas, papers que se encuentran en internet o en bibliotecas locales.

3.2.1. Desarrollo de la Propuesta

3.2.1.1. Levantamiento de la información de la empresa

La Empresa Grupo Megared se encuentra ubicada en el Cantón Quero perteneciente a la provincia de Tungurahua y posee una cobertura para de servicio de internet en fibra óptica y/o medio inalámbrico el cual abarca zonas como: Ambato, Quero, Pelileo, Tisaleo, Mocha, Guano y Urbina.

Para realizar la investigación de campo se extrae la información de las coordenadas de cada nodo que se encuentran en la plataforma de administración UCRM.

Tabla 5. Coordenadas de los nodos del ISP Grupo Megared

Fuente: Grupo Megared

Nodo	Coordenadas
Urbina	-1.47559126495, -78.7165823221
Atillo	-1.43210827971, -78.6871553423
Mocha	-1.42086547148, -78.662355212
San Vicente de Rumipamba	-1.43356218458, -78.6296671639
Santa Fe de Galán	-1.49107685069, -78.5638803775
San Pedro de Sabañag	-1.4588332503, -78.5802874927
Hualcanga San Francisco	-1.45091018874, -78.5754311399
Shaushi	-1.40569106275, -78.5790133513
San Vicente La Independencia	-1.38411240209, -78.5928771769
Llimpe	-1.38202358788, -78.5780748011
Quero Centro 2	-1.38105461298, -78.6083818346
Quero Centro Principal	-1.37957731826, -78.6065231733
Tisaleo	-1.35155249659, -78.6740114233
Palahua	-1.32226201998, -78.6009603718
Nitón	-1.28271561733, -78.5414700199
Ambato	-1.26831417954, -78.6317210727

En base a la información de coordenadas, se representa la ubicación geográfica de cada nodo en el software Google Earth.

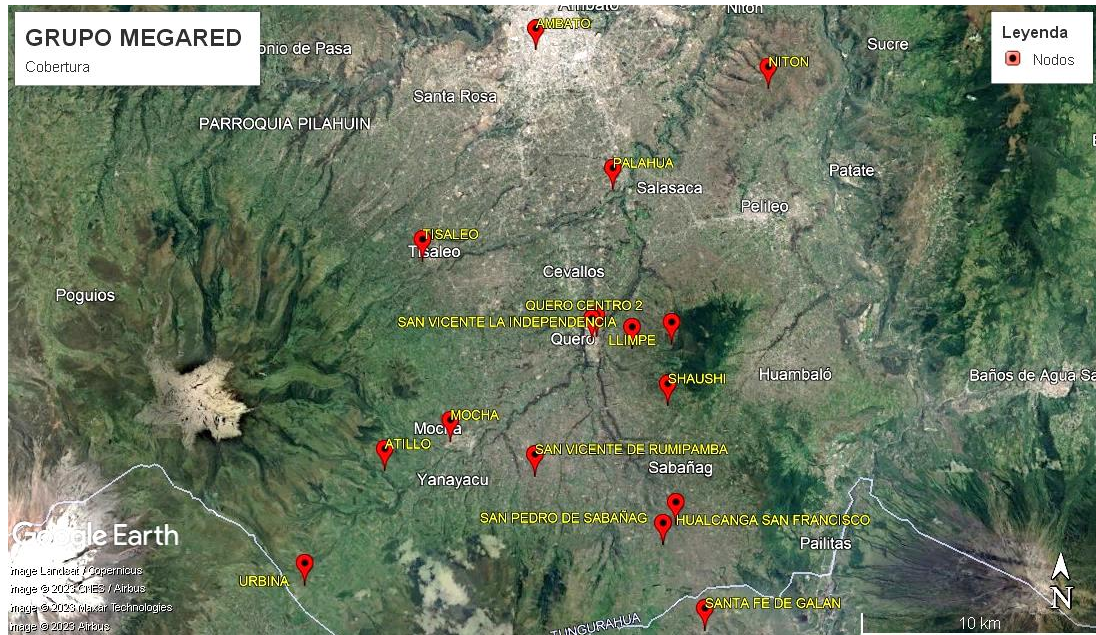


Figura 9. Nodos de comunicación de la Empresa Grupo Megared

Elaborado por: La Investigadora

Mediante la investigación de campo realizada (véase en Anexo 1), se extrae información de equipos utilizados en cada nodo, así como también el tipo y cantidad de interfaces para su comunicación. Como se muestra en la tabla 6.

Tabla 6. Tabla de equipos por nodo e interfaces

Fuente: La Investigadora

Nodo	Router	Switch	Interfaces SPF	Interfaces Ethernet
Urbina	x	WI-PS311G-24V	-	11
Atillo	x	DES-1008D	-	8
Mocha	3011UiAS	x	1	10
San Vicente de Rumipamba	x	WI-PS311G-24V	-	11
Santa Fe de Galan	RB750Gr3	x	-	5
	x	TL-SF1008D	-	8
San Pedro de Sabañag	CCR2004-1G-12S+2XS	x	14	1
	x	WI-PS311G-24V	-	11

Hualcanga San Francisco	x	DES-1008D	-	8
Shaushi	CCR1016-12G	x	-	12
	CRS326-24G-2S+	x	2	24
	x	WI-PS311G-24V	-	11
San Vicente La Independencia	x	WI-PS311G-24V	-	11
Llimpe	x	WI-PS311G-24V	-	11
Quero Centro 2	CCR1036-8G-2S+	x	2	8
	x	TL-SG1016G	-	16
Quero Centro Principal	CCR1072-1G-8S+	x	8	1
	CRS326-24G-2S+	x	2	24
	CRS326-24G-2S+	x	2	24
	x	WI-PS311G-24V	-	11
Tisaleo	CCR1072-1G-8S+	x	8	1
Palahua	x	DES-1008D	-	8
Niton	x	TL-SG108	-	8
Ambato	x	TL-SG108	-	8

Según los datos de información de los equipos e interfaces por nodos, mencionados en la tabla 6, se concluye que la empresa Grupo Megared utiliza equipos Mikrotik la estructura de su red de comunicaciones. Es por esta razón que se utiliza la herramienta Winbox, para identificar la configuración actual de la red. Dicha configuración se detalla en las tablas: 7,8,9,10,11,12,13,14 y 15. (Por confidencialidad no se detallan específicamente las direcciones de red).

Tabla 7. Configuración de router CCR1072-1G-8S+ en nodo Quero 1

Fuente: La Investigadora

ROUTER BALANCEADOR			
Interfaz de dispositivo	Dirección IP	Máscara de Red	Network
sfp-sfpplus1	157.100.x.x	/x	157.100.x.x
bridge1 Puertos: sfp-sfpplus8	172.16.x.x	/x	172.16.x.x
	192.168.x.x	/x	192.168.x.x
	192.168.x.x	/x	192.168.x.x
	192.168.x.x	/x	192.168.x.x
	192.168.x.x	/x	192.168.x.x
	192.168.x.x	/x	192.168.x.x
	192.168.x.x	/x	192.168.x.x
	192.168.x.x	/x	192.168.x.x

	192.168.x.x	/x	192.168.x.x
	192.168.x.x	/x	192.168.x.x
	192.168.x.x	/x	192.168.x.x
	192.168.x.x	/x	192.168.x.x
	192.168.x.x	/x	192.168.x.x
	192.168.x.x	/x	192.168.x.x
	192.168.x.x	/x	192.168.x.x
	192.168.x.x	/x	192.168.x.x
	192.168.x.x	/x	192.168.x.x

Tabla 8. Configuración de router CCR1072-1G-8S+ en nodo Tisaleo

Fuente: La Investigadora

ROUTER TISALEO			
Interfaz de dispositivo	Dirección IP	Máscara de Red	Network
sfp-sfpplus1	172.16.x.x	/x	172.16.x.x
sfp-sfpplus2	192.168.x.x	/x	192.168.x.x
WAN BRIDGE Puertos: sfp-sfpplus2	192.168.x.x	/x	192.168.x.x

Tabla 9. Configuración de router CCR1036-8G-2S+ en el nodo Quero 2

Fuente: La Investigadora

ROUTER QUERO 2			
Interfaz de dispositivo	Dirección IP	Máscara de Red	Network
Bridge1-RED-PRINCIPAL Puertos: Ether1	192.168.x.x	/x	192.168.x.x
Bonding1-OLT Esclavos: Ether5 Ether6 Ether7 Ether8	Vlan200 172.16.x.x 172.16.x.x Vlan201 172.16.x.x 172.16.x.x	/x /x /x /x /x	172.16.x.x 172.16.x.x 172.16.x.x 172.16.x.x 172.16.x.x

Tabla 10. Configuración de router/switch CRS326-24G-2S+ en el nodo Quero 1

Fuente: La Investigadora

ROUTER QUERO 1			
Interfaz de dispositivo	Dirección IP	Máscara de Red	Network
Bridge1 Puertos: todos	192.168.x.x	/x	192.168.x.x

Tabla 11. Configuración de router 3011UiAS en el nodo Mocha

Fuente: La Investigadora

ROUTER MOCHA			
Interfaz de dispositivo	Dirección IP	Máscara de Red	Network
Bridge1 Puertos: Ether1 Ether2 Ether3 Ether4 Ether5	192.168.x.x	/x	192.168.x.x

Tabla 12. Configuración de router CCR2004-1G-12S+2XS en el nodo San Pedro de Sabañag

Fuente: La Investigadora

ROUTER SAN PEDRO			
Interfaz de dispositivo	Dirección IP	Máscara de Red	Network
Bridge1 Puertos: Sfp-sfpplus1	192.168.x.x	/x	192.168.x.x

Tabla 13. Configuración de router RB750Gr3 en el nodo de Santa Fe de Galán

Fuente: La Investigadora

ROUTER SANTA FE DE GALÁN			
Interfaz de dispositivo	Red	Máscara de Red	Network
Ether1	192.168.x.x	/x	192.168.x.x
Bridge2 Puertos: Ether1 Ether5	192.168.x.x	/x	192.168.x.x

Tabla 14. Configuración de router CCR1016-12G en el nodo Shaushi

Fuente: La Investigadora

ROUTER SHAUSHI			
Interfaz de dispositivo	Dirección IP	Máscara de Red	Network
Bridge1 Puertos: Ether1 Ether2 Ether3 Ether7 Ether8 Ether12	192.168.x.x	/x	192.168.x.x

Según la investigación de campo realizada se determina que: Grupo Megared cuenta con 1 proveedor de internet: NEDETEL, a la vez posee 1 router de borde y 6 routers internos en la red. Estos equipos utilizan el sistema operativo RouterOs pertenecientes a Mikrotik.

Como resultado se detallan los siguientes diagramas de red actual.

- Diagrama de red físico
- Diagrama de red lógico

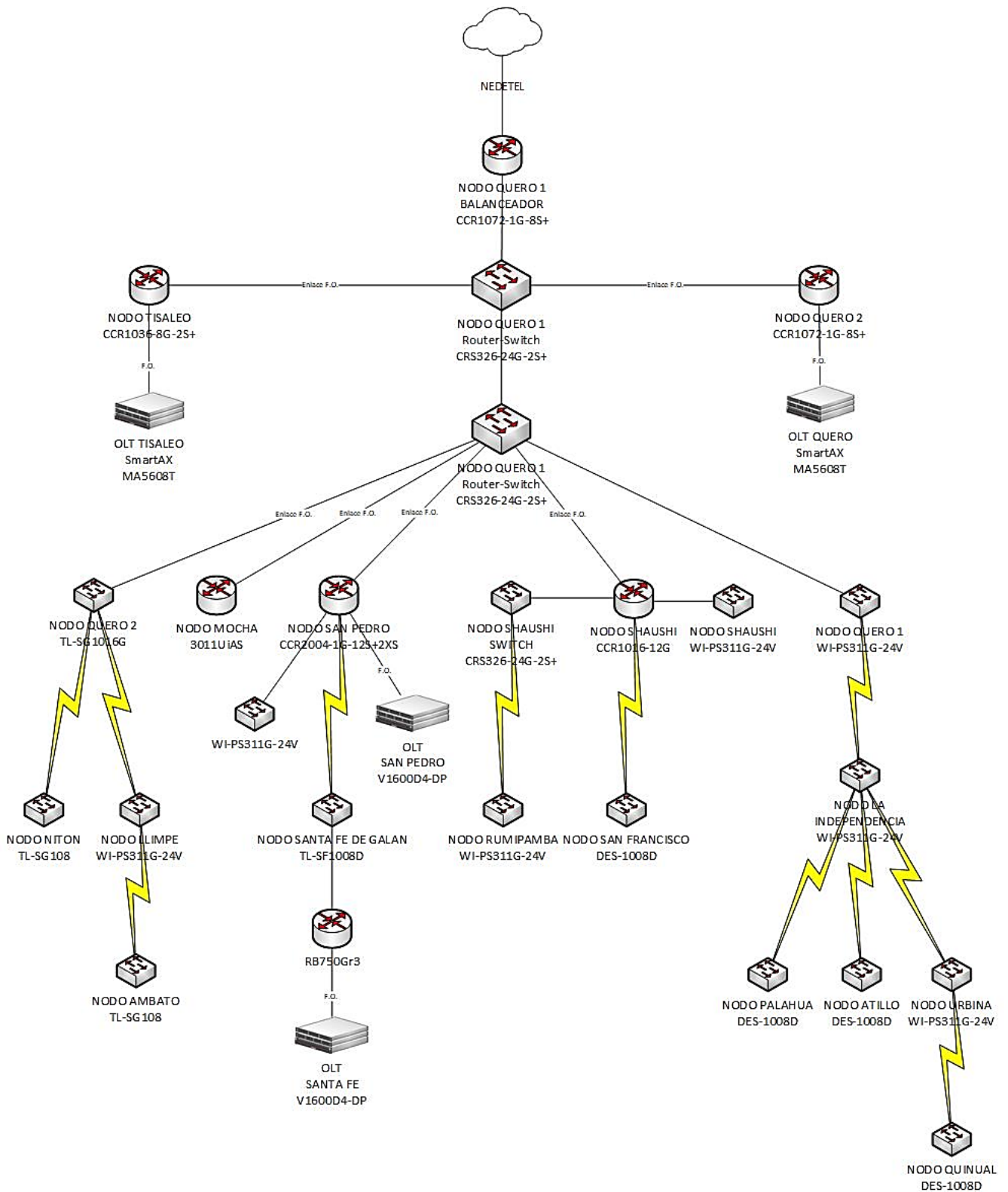


Figura 10. Diagrama de topología física del ISP Grupo Megared

Elaborado por: La Investigadora

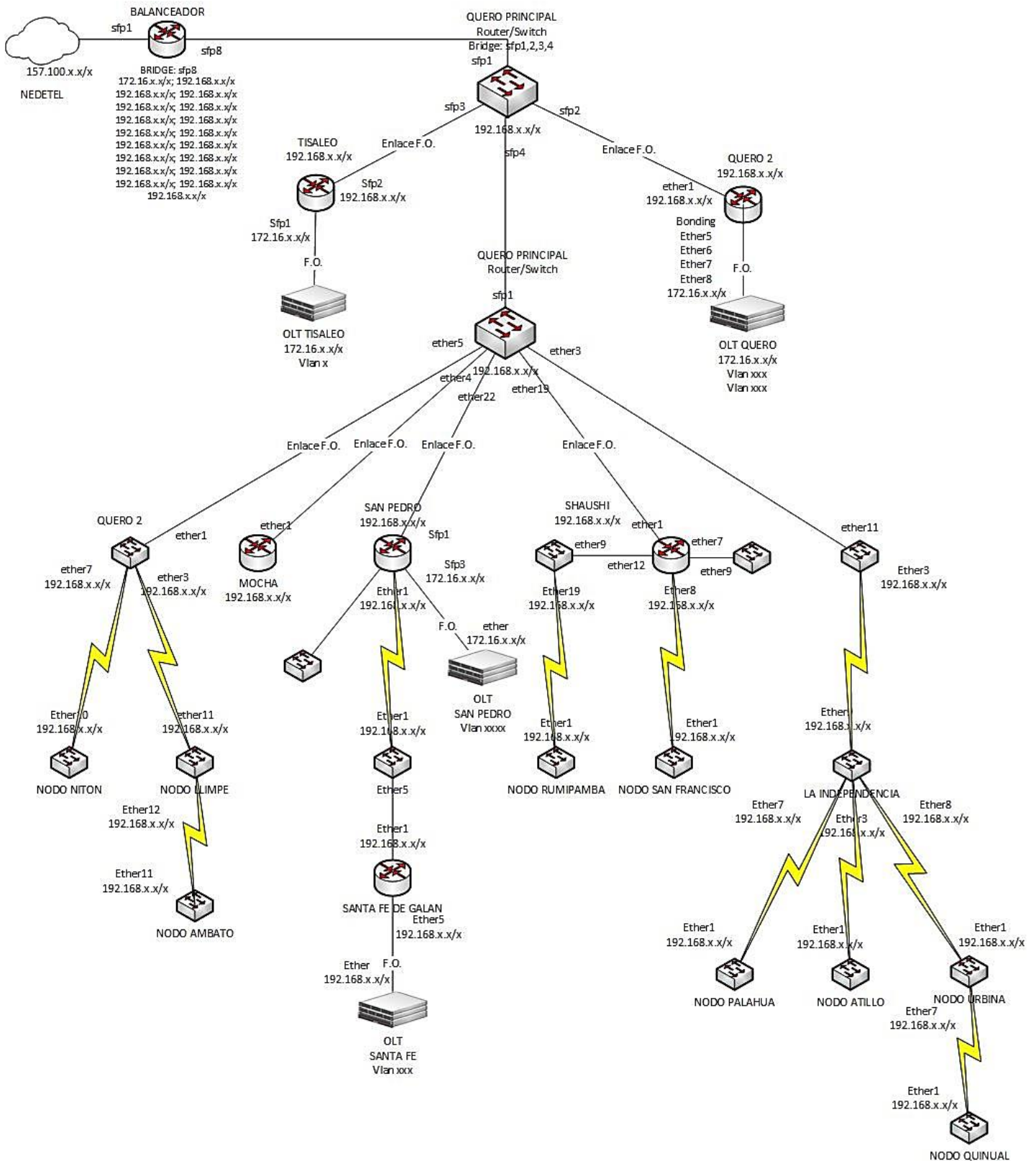


Figura 11. Diagrama lógico de red del ISP Grupo Megared

Elaborado por: La Investigador

3.2.1.2. Análisis de tráfico de la red

Se verifica el tráfico en cada uno de los nodos, para la identificación de equipos a utilizar en el rediseño lógico de la red, (Véase en Anexo 2). Este análisis fue realizado para horas pico de consumo que van de las 6:30pm a las 10:30pm. A continuación, se detalla la síntesis del análisis de tráfico de toda la red:

Tabla 15. Velocidad de bajada por nodo en horas pico de consumo

Fuente: La Investigadora, Grupo Megared

Nodo	Velocidad máxima (Mbps)
Palahua	2
Quinual	4,3
Atillo	11,8
Ambato	9,3
San Francisco	11,1
Niton	37,66
Urbina	43
La Independencia	63,1
San Vicente de Rumipamba	114,554
Llimpe	172,7
Shaushi	181,346
San Pedro	332,4
Santa Fe de Galan	38,1
Quero 2	15,34
Mocha	46,8
OLT Tisaleo	619,3
OLT Quero	2500
TOTAL	4202,8

Así mismo, mediante los diagramas topológicos presentados en las Figuras: 10 y 11, se extrae información adicional ingresando a cada uno de los AP pertenecientes a cada nodo de red. Esto permitió obtener una visión de la cantidad de usuarios que maneja la empresa. A continuación, se presenta la cantidad de enlaces, antenas sectoriales y clientes pertenecientes en cada nodo.

Tabla 16. Cantidad de Radioelaces, antenas sectoriales y clientes por nodo

Fuente: La Investigadora

NODO	Enlaces	Sectoriales	Clientes
<i>Palahua</i>	1	1	1
<i>Quinual</i>	1	1	1
<i>Atillo</i>	1	1	4
<i>Ambato</i>	1	2	5
<i>San Francisco</i>	1	2	6
<i>Quero 1</i>	2	3	5
<i>Quero 2</i>	2	2	27
<i>Niton</i>	2	4	29
<i>Mocha</i>	1	4	30
<i>Santa Fe de Galan</i>	2	3	36
<i>Urbina</i>	2	3	45
<i>La Independencia</i>	4	4	53
<i>Rumipamba</i>	1	8	84
<i>San Pedro</i>	1	6	96
<i>Llimpe</i>	2	12	131
<i>Shaushi</i>	4	17	173
TOTAL	28	73	726

Mediante la información recolectada, se deduce que existen 28 antenas que se encuentran utilizadas para la comunicación entre nodos mediante radio-enlaces y 73 antenas sectoriales en toda la red.

3.2.1.3. Simulación en configuración bridge

Posterior a la representación de la topología de red lógica y física. Se inicia con la emulación, comprobando la comunicación entre todos los dispositivos y nodos pertenecientes a la red. Esta emulación de red se realizó mediante el software EVE-NG, para lo cual se utilizó una máquina virtualizada. El objetivo de simular la red mediante la virtualización se basa en consumir menos recursos físicos del ordenador, como CPU y Memoria RAM.

Al iniciar esta simulación se probó con el software GNS3, pero al emular de 2 a 3 routers el CPU y Memoria RAM (8GB) ascendían hasta el 90% de la utilización de los recursos. Por esta razón se opta realizar la simulación mediante un software virtualizado, y debido a que EVE-NG se especializa en la emulación de dispositivos que manejen el sistema operativo RouterOS. (Véase en Anexo 3)

Guiándose en el diagrama de red lógico actual se tiene la siguiente simulación:

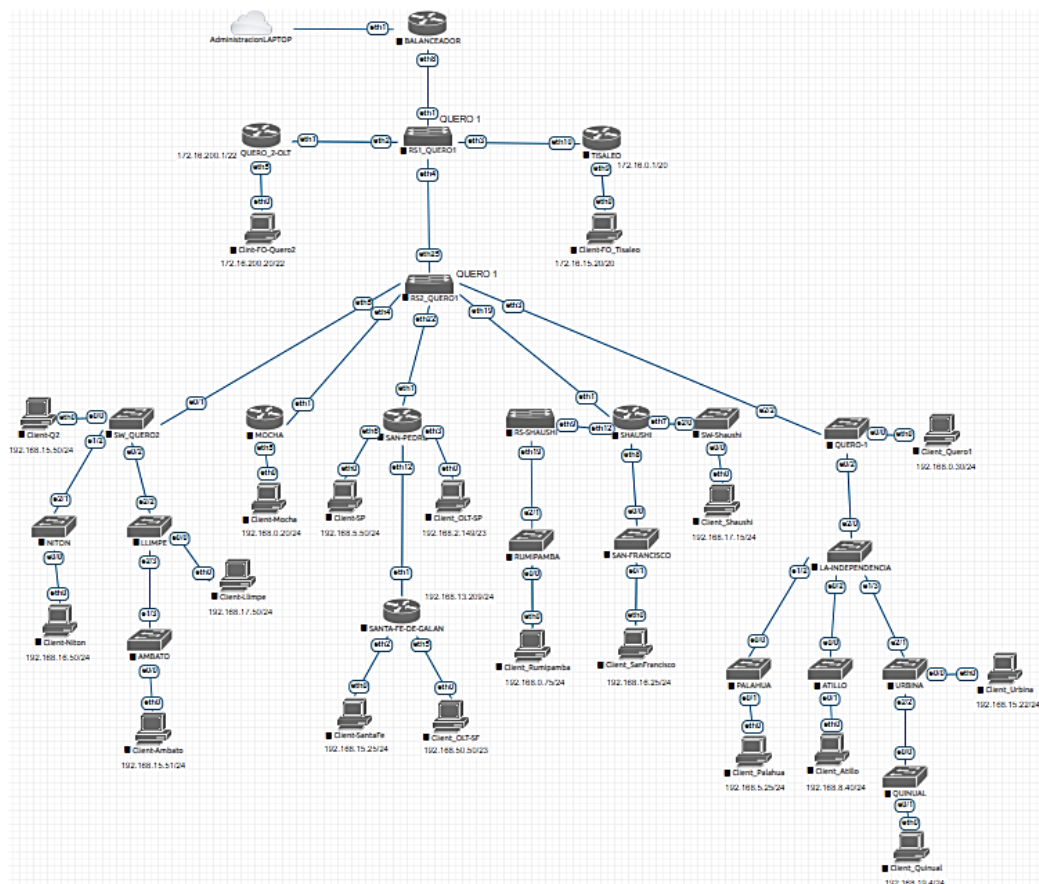


Figura 12. Simulación de red bridge actual de la ISP Grupo Megared

Fuente: La Investigadora

Datos para pruebas de tráfico

Estas pruebas se ejecutaron con la herramienta jperf la cual trabaja con java, mostrando la gráfica de resultados luego de un tiempo estimado de envío de paquetes UDP.

Para realizar estas pruebas se utilizan 2 máquinas con sistema operativo Windows que se encuentran conectadas a cada extremo de la red respectivamente. El servidor de jperf se encuentra directamente conectado al router Balanceador por la interfaz ether7 y posee la dirección IP 192.168.255.20. El cliente de jperf se encuentra conectado en el router de La Independencia en la interfaz ether10 con la dirección IP IP 192.168.19.4.

Para emular los datos más cercanos a la configuración y tráfico, fue necesario comparar el tráfico de red actual (Tabla 15) con el tráfico que soporta la simulación.

Para esto se ejecuta la primera prueba entre el servidor y el cliente jperf, donde se utilizan 2Mbps y se verifica si hay o no saturación de datos. A lo cual, se observa que se ejecuta la prueba hasta un máximo de 1,019Mbps.

Tabla 17. Ancho de banda del ISP Grupo Megared y Ancho de banda soportada en la simulación

Fuente: La Investigadora

Ancho de banda de ISP Grupo Megared (Mbps):	6300
Ancho de Banda de simulación (Mbps)	1,019

Para obtener una relación equivalente para las pruebas de tráfico, se calcula el porcentaje de consumo en la red actual y se la compara con el ancho de banda soportada en la simulación con una regla de 3 simple. A continuación, se presentan los cálculos realizados.

Cálculo de porcentaje de consumo por nodo:

$$Porcentaje \% = \frac{6300Mbps * 100\%}{nMbps}$$

Donde;

- 6300Mbps es el ancho de banda contratado por el ISP Grupo Megared
- nMbps es la velocidad máxima de en el ISP Grupo Megared en horas de saturación

Cálculo para determinar el valor de velocidad máxima para simulación

$$Velocidad (kbps) = \frac{1019kbps * Porcentaje \%}{100\%}$$

Donde;

- 1019kbps es el ancho de banda que soporta la simulación
- Porcentaje % es el valor calculado según tráfico del ISP

Los valores obtenidos se detallan en la siguiente tabla:

Tabla 18. Comparación de velocidad máxima de bajada en el ISP Grupo Megared y en EVE-NG

Fuente: La Investigadora

Nodo	Velocidad máxima ISP (Mbps)	Porcentaje (%)	Velocidad para simulación (Kbps)
La Independencia	124,2	1,97	20,09
Shaushi	307	4,87	49,66
San Pedro	370,5	5,88	59,93
Quero 2	235	3,73	38,01
Mocha	46,8	0,74	7,57
OLT Tisaleo	619,3	9,83	100,17
OLT Quero	2500	39,68	404,37
TOTAL	4202,8	66,71	679,79

Para la obtención de los datos previamente mostrados, se toma con consideración el tráfico generado por los equipos de administración principales.

Para las pruebas de tráfico de la red se utilizará el nodo más lejano: La Independencia con el router de borde: Balanceador.

Finalmente se realizarán 30 pruebas en cada escenario propuesto, dichas pruebas tendrán un periodo de duración de 60, en donde se compara los 60 segundos con las

24 horas del día y a su vez las 4 horas de saturación, obteniendo que de los 60, 10 segundos se aplicará el tráfico de saturación.

Tabla 19. Escenarios de emulación de tráfico

Fuente: La Investigadora

Escenario	Tráfico UDP (kbps)
Velocidad máxima en el nodo La Independencia	20,09
Velocidad máxima en toda la red	679,79

Pruebas de tráfico en la configuración actual del ISP Grupo Megared: BRIDGE

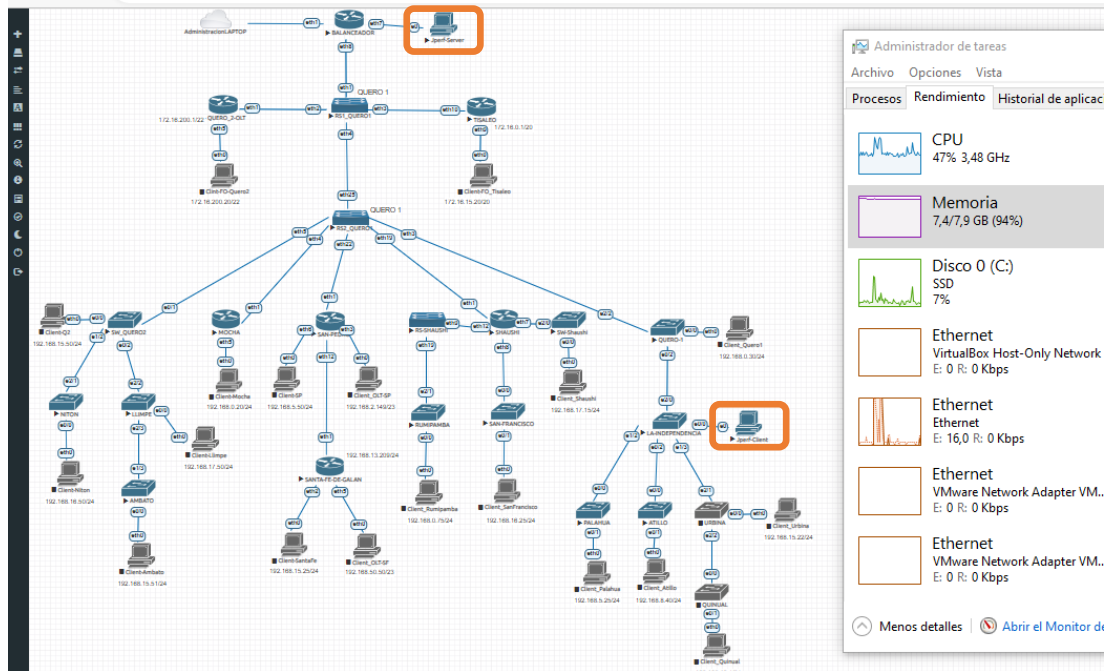


Figura 13. Prueba de tráfico en la configuración actual del ISP Grupo Megared: BRIDGE

Dicha simulación se ejecuta solo con los dispositivos principales de red más los switches de cada nodo, con el propósito de optimizar recursos de hardware.

Primer escenario

- Se realizan 30 pruebas consecutivas con un conteo de 60 segundos por cada prueba, y entre ellos 10 segundos de tráfico de 20,02kbps.

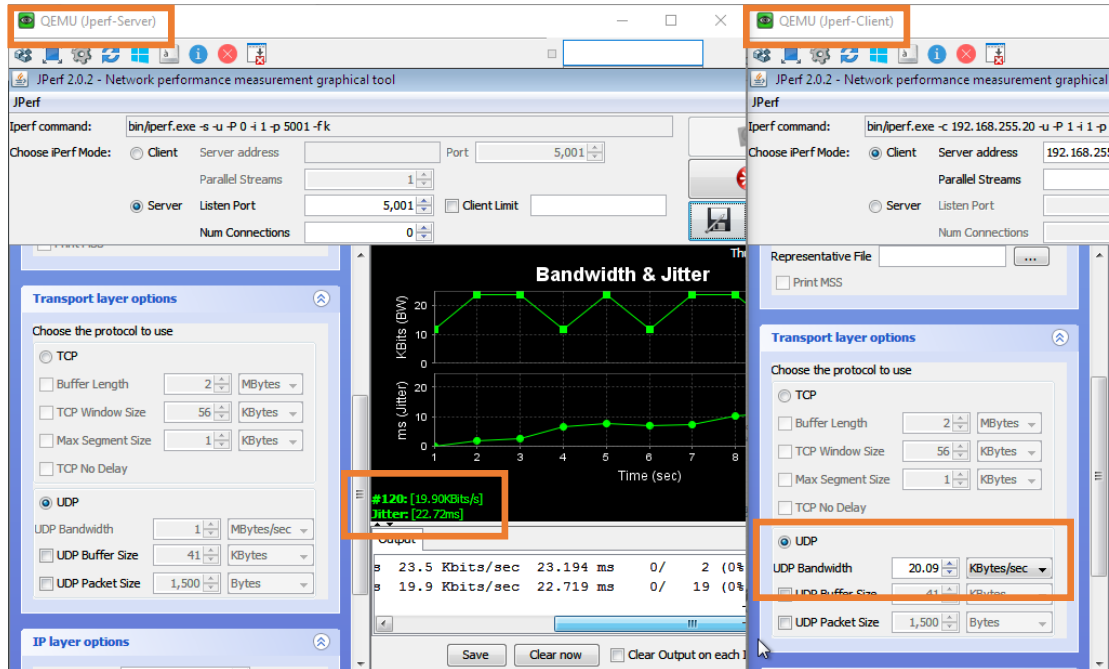


Figura 14. Prueba de tráfico en configuración BRIDGE con la herramienta jperf: 20,09 kbps

Captura de Wireshark

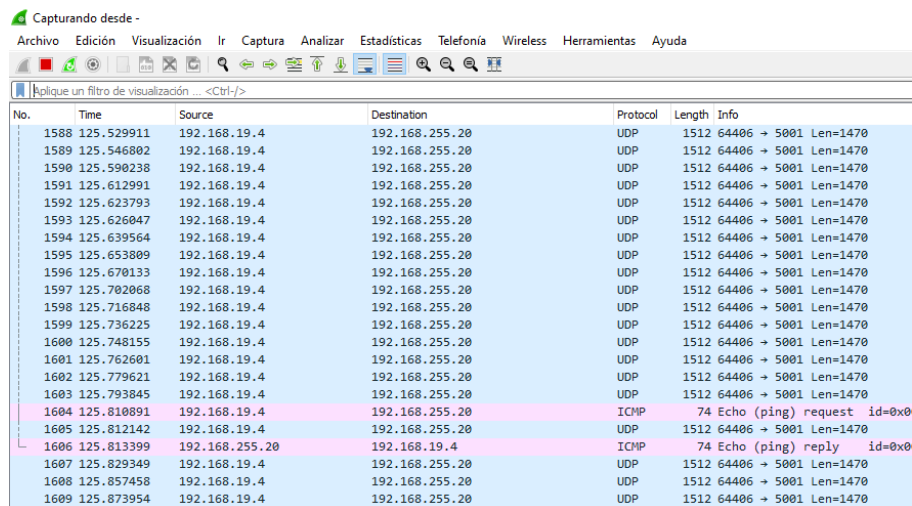


Figura 15. Captura de tráfico UDP en prueba en configuración BRIDGE con 20,09kbps

A continuación, se presentan los datos tomados en cada una de las pruebas realizadas. Con el comando ping desde el cliente iperf hacia el servidor por 60 segundos se obtiene el valor del tiempo de respuesta RTT y avg el cual es el promedio de la misma, el jitter y el packet loss obtenido de las pruebas con UDP.

Tabla 20. Pruebas de tráfico UDP con 20,09 kbps en configuración bridge

Fuente: La investigadora

RED BRIDGE: TRAFICO UDP: 20,09 kbps				
RTT min	RTT max	AVG	Jitter (ms)	Packet Loss (%)
5	180	28	22,72	0
5	113	21	17,86	0
5	814	39	22,49	0
5	305	25	13,97	0
5	118	19	13,41	0
5	103	22	16,34	0
5	164	12	18,25	0
4	44	10	10,53	0
5	55	11	8,54	0
5	560	24	24,28	0
5	194	21	29,03	0
4	47	9	11,41	0
5	81	12	14,31	0
5	99	13	8,76	0
4	101	10	11,71	0
4	128	15	4,66	0
4	214	17	4,32	0
5	38	10	11,8	0
5	43	11	6,52	0
5	46	9	8,84	0
4	144	15	17,39	0
5	85	12	10,26	0
4	37	11	30,63	0
4	109	12	28,31	0
4	105	11	14,46	0
4	45	10	13,52	0
4	94	12	22,75	0
5	1056	28	11,36	0
4	82	10	14,03	0
4	28	8	10,42	0
4,57	174,40	15,57	15,32	0,00

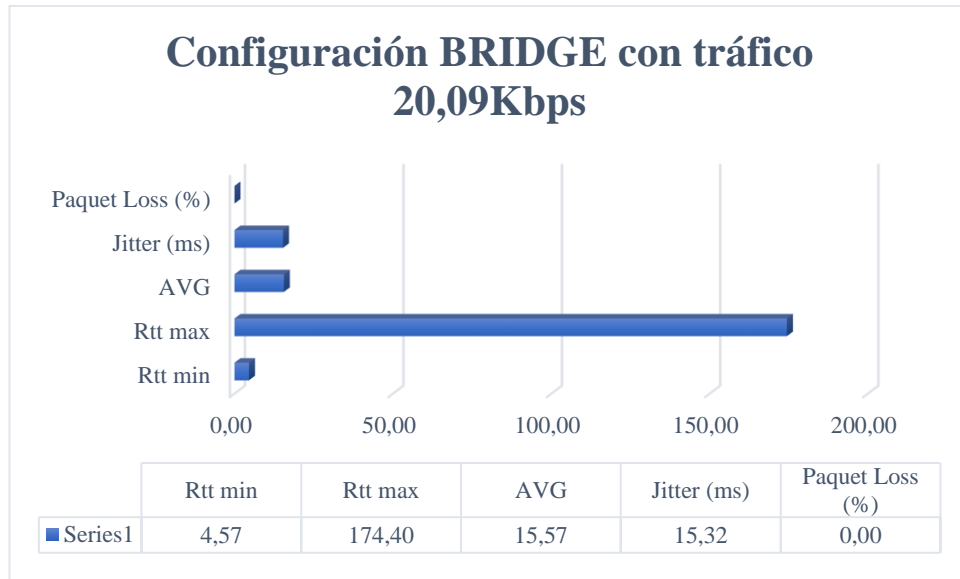


Figura 16. Prueba de tráfico con 20,09kbps en configuración Bridge

Fuente: La Investigadora

Segundo escenario

- Se realizan 30 pruebas consecutivas con un conteo de 60 segundos por cada prueba, y entre ellos 10 segundos de tráfico de 679,79kbps. Obteniendo los siguientes resultados.

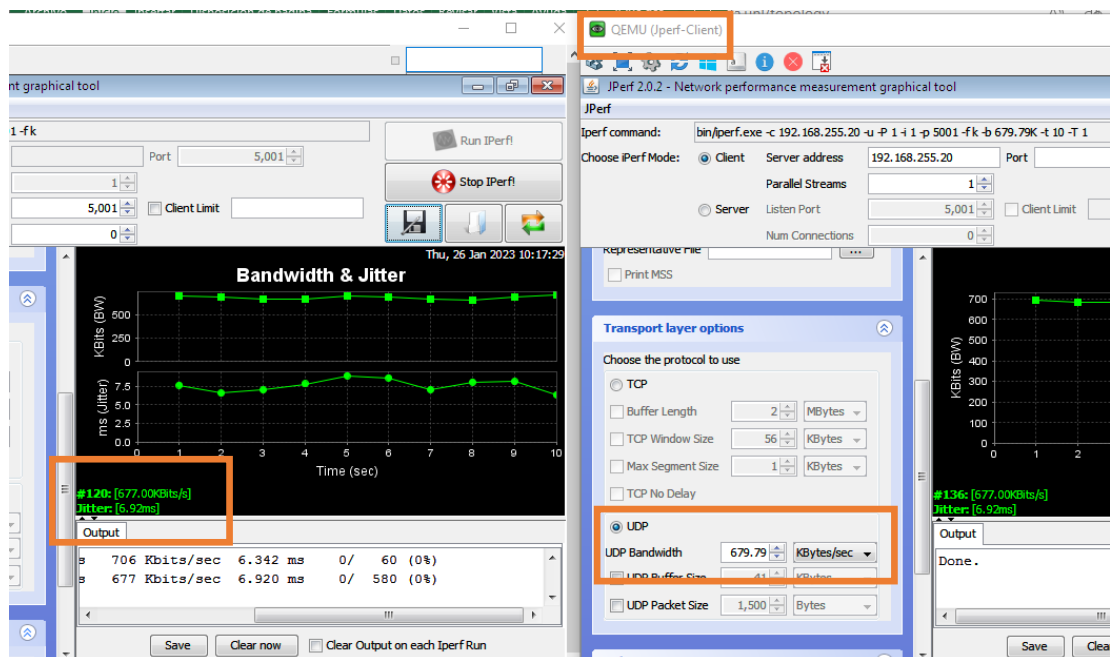


Figura 17. Prueba de tráfico en configuración BRIDGE con la herramienta jperf: 679,79 kbps

Tabla 21. Pruebas de tráfico UDP con 679,79 kbps en configuración bridge

Fuente: La Investigadora

RED BRIDGE: TRAFICO UDP: 679,79 kbps				
RTT min	RTT max	AVG	Jitter	Packet Loss (%)
4	344	21	23,52	8,4
4	110	14	7,55	0,35
5	38	10	10,69	0,17
4	167	14	7,78	0,52
5	103	11	9,18	0
5	56	10	3,21	0
5	34	9	6,95	0,52
5	84	14	12,45	0,18
5	106	10	12,12	0,35
5	33	9	9,38	0
5	33	9	12,83	1,4
2	802	34	8,79	0
4	79	10	14,54	0
4	68	12	8,65	2,1
4	163	14	11,46	0
5	44	9	9,32	3,1
5	61	10	11,98	0,34
4	56	11	6,6	0,34
4	72	14	10,41	0
5	40	11	10,32	0
4	34	9	5,2	1,6
4	128	11	12,09	2,4
4	141	12	4,65	3,3
5	68	13	10,95	3,8
5	42	10	10,82	0,69
4	243	17	10,06	1,6
5	39	10	8,19	0
4	700	23	11,72	0,38
4	45	10	19,27	0,87
5	41	8	6,92	0
4,43	132,47	12,63	10,25	1,08

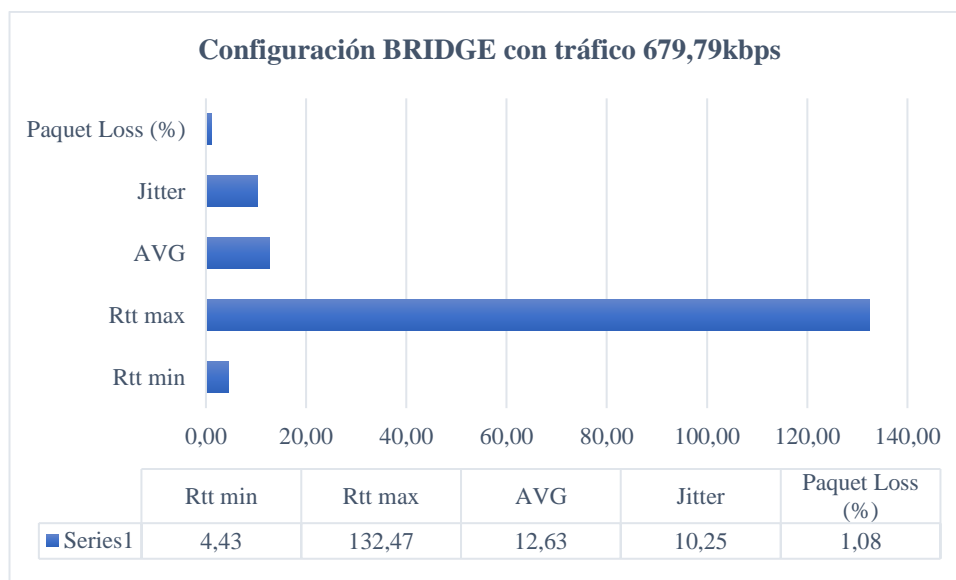


Figura 18. Prueba de tráfico con 679,79 kbps en configuración Bridge

Fuente: La Investigadora

3.2.1.4. Simulación de red ruteada propuesta

Una vez analizados los diagramas de red: físico y lógico (Figura 10 y 11) y al simular equipos con la configuración actual de la empresa, se detecta que no posee una correcta distribución de equipos, en donde todo el tráfico de la red lo soporta la interfaz sfp8 del router de borde. Así también no se encuentran rutas de respaldo activas, siendo estas muy importantes ante la caída del enlace principal. Finalmente, se verifica que no se tiene una segmentación de red por nodo y clientes.

En base a este análisis se proponen las siguientes soluciones:

- Segmentación y enrutamiento de red
- Creación de rutas de respaldo

Para brindar direccionamiento a los nodos que pertenecen a Quero 2 (antenas), Quero 1 (antenas) y San Vicente La Independencia se propone el cambio de switches (Tabla 6), por routers Mikrotik.

Tomando en cuenta estas características de consumo (Tabla 15), se desea determinar los dispositivos que se debe agregar a la red para ello, se tomó en consideración los siguientes aspectos:

Tabla 22. Características para elección de equipos de enrutamiento

Fuente: La Investigadora

Nodo	Características
Quero 2 (antenas)	Al menos 6 puertos Ethernet para antenas sectoriales y 2 puertos SFP+ de 10GB para enlace y backup.
Quero 1 (antenas)	Puertos para antenas sectoriales y 1 puertos SFP
La Independencia	Puertos Ethernet /1000 para radioenlaces

Selección de router para nodo Quero 2 (antenas)

Mediante las características establecidas en la tabla 22, se obtiene información de la página oficial de Mikrotik. Filtrando las opciones brindadas se tiene:

Tabla 23. Cuadro comparativo de especificaciones de routers Mikrotik para nodo Quero 2

Fuente: Página oficial de Mikrotik [39]

Nombre del producto	Número de núcleos de CPU	Tamaño de RAM	Consumo de energía máximo (W)	Puertos Ethernet 10/100/1000	Puertos SFP+	Precio estimado (USD)
CRS326-24G-2S+IN	1	512 MB	21	24	2	199
CRS326-24G-2S+RM	1	512 MB	24	24	2	209
CCR2004-16G-2S+	4	4 GB	35	16	2	465
CCR2004-16G-2S+PC	4	4 GB	30	16	2	465
CCR1036-8G-2S+	36	4 GB	73	8	2	1195
CCR1036-8G-2S+EM	36	8 GB	73	8	2	1395

Comparando los 6 routers presentados, se elige a: CCR2004-16G-2S+PC, ya que no solamente cumple con las características establecidas, si no también posee un precio accesible y menor consumo de energía en comparación a: CCR2004-16G-2S+.

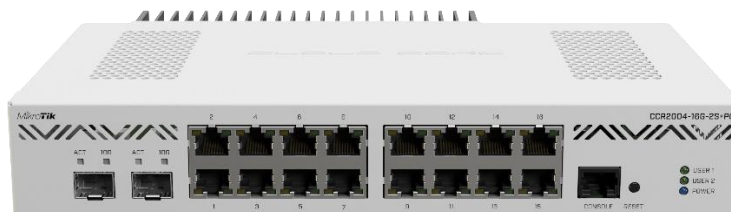


Figura 19. Router CCR2004-16GB-2S+PC para nodo Quero 2 de respaldo

Fuente: Página oficial de Mikrotik

Selección de equipos para nodos: Quero 1 (antenas) y La Independencia

Mediante las características establecidas en la tabla 22, se obtiene información de la página oficial de Mikrotik. Filtrando las opciones brindadas se tiene:

Tabla 24. Cuadro comparativo de especificaciones de routers Mikrotik para nodos: Quero 1 y La Independencia



Fuente: Página oficial de Mikrotik [39]

Nombre del producto	Numero de Núcleos de CPU	Tamaño de RAM	Consumo de energía máxima (W)	Puertos Ethernet 10/100	Puertos Ethernet 10/100 /1000	Puerto SFP	Precio estimado (USD)
RB2011UiAS-IN	1	128 MB	6	5	5	1	119
RB2011UiAS-RM	1	128 MB	6	5	5	1	119
RB3011UiAS-RM	2	1 GB	10	None	10	1	179

Comparando los 3 routers que cumplen con las características mencionadas, existen 2 productos con las mismas características y precios, para lo cual se realiza una comparativa en su presentación física

Tabla 25. Comparación física de router Mikrotik para nodos: Quero 1 y La Independencia

Fuente: Absxperts [40], [41]

Nombre	RB2011UiAS-RM	RB2011UiAS-IN
Imagen		
Parámetro físico	Montaje en rack 1U	Caja metálica de escritorio

Como resultado al análisis de equipos realizado para los nodos Quero 1 y La Independencia, se elige el router: RB2011UiAS-RM por su característica adicional de montaje en rack.

En total se agregan 3 routers nuevos a la red y se propone un enlace de backup mediante fibra óptica en el nodo Quero 2 con el router que se comunica a la OLT y con el nuevo router CCR2004-16G-2S+ agregado.

A su vez, se activan los enlaces de backup para que permanezcan siempre encendidos y que no sean activados manualmente cuando el enlace principal cae.

Tomando en consideración los aspectos mencionados, se propone el siguiente diagrama físico de red.

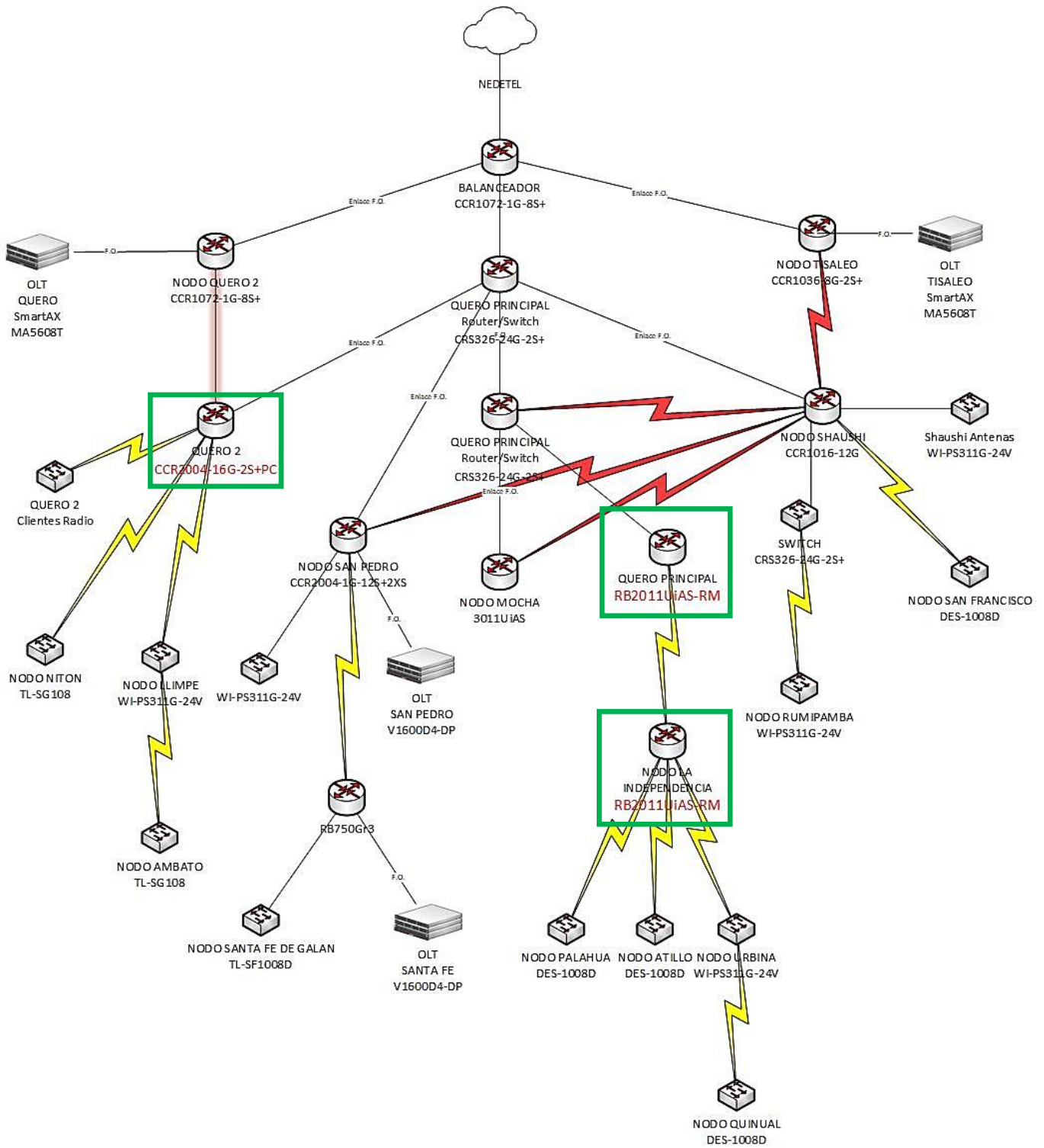


Figura 20. Diagrama de red física propuesta

Fuente: La Investigadora

Tasa de crecimiento del servicio inalámbrico del ISP Grupo Megared

Para iniciar con la propuesta de red ruteada y representación de su diagrama lógico, es importante calcular la tasa de crecimiento de clientes que posee Grupo Megared, en donde se enfatiza el sector inalámbrico, ya que el mismo no cuenta con un direccionamiento IP por nodo y es el principal afectado en los bucles generados por tormenta de difusión. Para lo cual se analiza el crecimiento de usuarios con servicio inalámbrico, considerando nuevos ingresos y retiros en el periodo de: octubre 2021 y septiembre 2022, obteniendo los siguientes resultados:

Tabla 26. Crecimiento del servicio inalámbrico en el ISP Grupo Megared

Fuente: Datos de la empresa Grupo Megared

AÑO	MES	NUEVOS INGRESOS	RETIRADOS	DIFERENCIA
2021	Octubre	7	22	-15
2021	Noviembre	5	11	-6
2021	Diciembre	5	19	-14
2022	Enero	5	11	-6
2022	Febrero	7	7	0
2022	Marzo	10	0	10
2022	Abril	1	0	1
2022	Mayo	1	14	-13
2022	Junio	19	15	4
2022	Julio	15	11	4
2022	Agosto	10	23	-13
2022	Septiembre	14	23	-9
TOTAL		99	156	-57

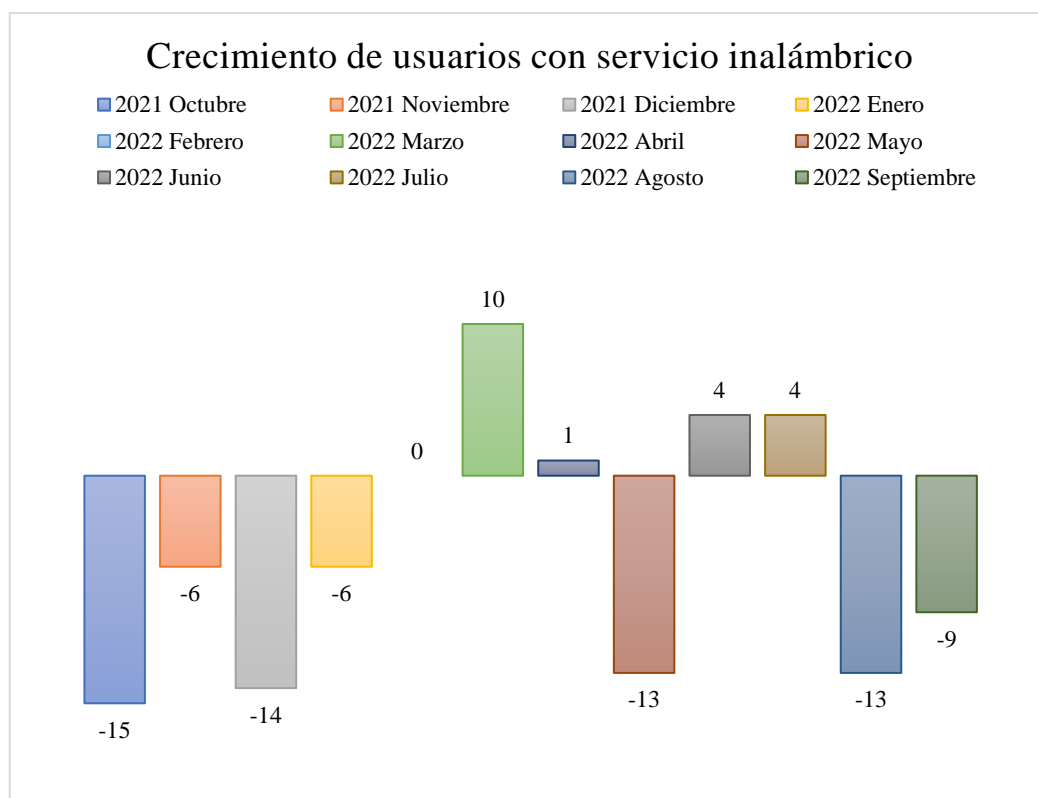


Figura 21. Diagrama de crecimiento de usuarios con servicio inalámbrico en el ISP Grupo Megared

Fuente: Tomado de datos del ISP Grupo Megared

Para calcular la tasa de crecimiento se utiliza la fórmula para determinar la demanda final:

$$D_f = D_i * (1 + r)^t$$

En donde;

- D_f : Demanda final
- D_i : Demanda Inicial
- r : Taza de crecimiento
- t : tiempo en años

$$D_f = D_i * (1 + r)^t$$

$$747 = (747 - (-57)) * (1 + r)^1$$

$$747 = 804 * (1 + r)^1$$

$$747 = 804 + 804r$$

$$-57 = 804r$$

$$-\frac{57}{804} = r$$

$$r = -0,07089$$

Como resultado se tiene que la tasa de crecimiento anual es del $-0,07089$, por lo tanto, el ISP Grupo Megared posee una disminución de clientes con servicio inalámbrico, si con esta información se calcula la demanda final en 10 años, se tendría el siguiente resultado:

$$D_f = D_i * (1 + r)^t$$

$$D_f = 747 * (1 + (-0,07089))^{10}$$

$$D_f = 358,09 == 359 \text{ clientes}$$

En 10 años los clientes con servicio inalámbrico disminuirán a casi la mitad en comparación a la actualidad, se toma como referencia la misma cantidad de usuarios para crear el direccionamiento IP por nodo.

Tomando como referencia esta información, se propone las siguientes tablas de direccionamiento:

Tabla 27. Direccionamiento IP para enlaces de routers principales**Fuente:** La Investigadora

Enlace	Nº de Hosts	IP de red	Máscara	Primer Host	Último Host	Broadcast
Quero 1 (2) - La Independencia	6	10.255.0.0 /29	255.255.255.248	10.255.0.1	10.255.0.6	10.255.0.7
San Pedro - Santa Fe de Galan	6	10.255.0.8 /29	255.255.255.248	10.255.0.9	10.255.0.14	10.255.0.15
Balanceador - Tisaleo	2	10.255.0.16 /30	255.255.255.252	10.255.0.17	10.255.0.18	10.255.0.19
Balanceador - Quero 2	2	10.255.0.20 /30	255.255.255.252	10.255.0.21	10.255.0.22	10.255.0.23
Balanceador - Quero 1	2	10.255.0.24 /30	255.255.255.252	10.255.0.25	10.255.0.26	10.255.0.27
Quero 1 - Quero 2	2	10.255.0.28 /30	255.255.255.252	10.255.0.29	10.255.0.30	10.255.0.31
Quero 1 - San Pedro	2	10.255.0.32 /30	255.255.255.252	10.255.0.33	10.255.0.34	10.255.0.35
Quero 1 - Mocha	2	10.255.0.36 /30	255.255.255.252	10.255.0.37	10.255.0.38	10.255.0.39
Quero 1 - Shaushi	2	10.255.0.40 /30	255.255.255.252	10.255.0.41	10.255.0.42	10.255.0.43
Quero 1 - Quero 1 (2)	2	10.255.0.44 /30	255.255.255.252	10.255.0.45	10.255.0.46	10.255.0.47
Balanceador - Quero 1	2	10.255.0.48 /30	255.255.255.252	10.255.0.49	10.255.0.50	10.255.0.51
Backup fibra: Quero 2 - Quero 2 (2)	2	10.255.0.52 /30	255.255.255.252	10.255.0.53	10.255.0.54	10.255.0.55
Backup Radio: Quero 1 - Shaushi	6	10.255.1.0 /29	255.255.255.248	10.255.1.1	10.255.1.6	10.255.1.7
Backup Radio: Shaushi - Tisaleo	6	10.255.1.8 /29	255.255.255.248	10.255.1.9	10.255.1.14	10.255.1.15
Backup Radio: Shaushi - San Pedro	6	10.255.1.16 /29	255.255.255.248	10.255.1.17	10.255.1.22	10.255.1.23
Backup Radio: Shaushi - Mocha	6	10.255.1.24 /29	255.255.255.248	10.255.1.25	10.255.1.30	10.255.1.31

Tabla 28. Direccionamiento IP para clientes con servicio inalámbrico

Fuente: La Investigadora

Nodo	Clientes	N° de Hosts	Dirección de red	Mascara	Rango de hosts disponibles	Broadcast	Interface
Shaushi	196	254	172.16.100.0	/24	172.16.100.1 - 172.16.100.254	172.16.100.255	vlan 500
Llimpe	145	254	172.16.101.0	/24	172.16.101.1 - 172.16.101.254	172.16.101.255	vlan 505
San Pedro	104	126	172.16.102.0	/25	172.16.102.1 - 172.16.102.126	172.16.102.127	vlan 510
Rumipamba	93	126	172.16.102.128	/25	172.16.102.129 - 172.16.102.254	172.16.102.255	vlan 515
La Independencia	61	62	172.16.103.0	/26	172.16.103.1 - 172.16.103.62	172.16.103.63	vlan 520
Urbina	50	62	172.16.103.64	/26	172.16.103.65 - 172.16.103.126	172.16.103.127	vlan 525
Santa Fe de Galan	42	62	172.16.103.128	/26	172.16.103.129 - 172.16.103.190	172.16.103.191	vlan 530
Mocha	36	62	172.16.103.192	/26	172.16.103.193 - 172.16.103.254	172.16.103.255	vlan 535
Niton	35	62	172.16.104.0	/26	172.16.104.1 - 172.16.104.62	172.16.104.63	vlan 540
Quero 2	32	62	172.16.104.64	/26	172.16.104.65 - 172.16.104.126	172.16.104.127	vlan 545
Quero 1	12	14	172.16.104.128	/28	172.16.104.129 - 172.16.104.142	172.16.104.143	vlan 550
San Francisco	9	14	172.16.104.144	/28	172.16.104.145 - 172.16.104.158	172.16.104.159	vlan 555
Ambato	8	14	172.16.104.160	/28	172.16.104.161 - 172.16.104.174	172.16.104.175	vlan 560
Atillo	3	6	172.16.104.176	/29	172.16.104.177 - 172.16.104.182	172.16.104.183	vlan 565
Palahua	3	6	172.16.104.184	/29	172.16.104.185 - 172.16.104.190	172.16.104.191	vlan 570
Quinual	3	6	172.16.104.192	/29	172.16.104.193 - 172.16.104.198	172.16.104.199	vlan 575

Para poder enrutar la red es importante utilizar un protocolo de enrutamiento dinámico, el cual permita configurar rutas de respaldo para evitar la indisponibilidad del servicio. Finalmente, con toda la información recolectada propone el siguiente diagrama de red lógico con enrutamiento OSPF.

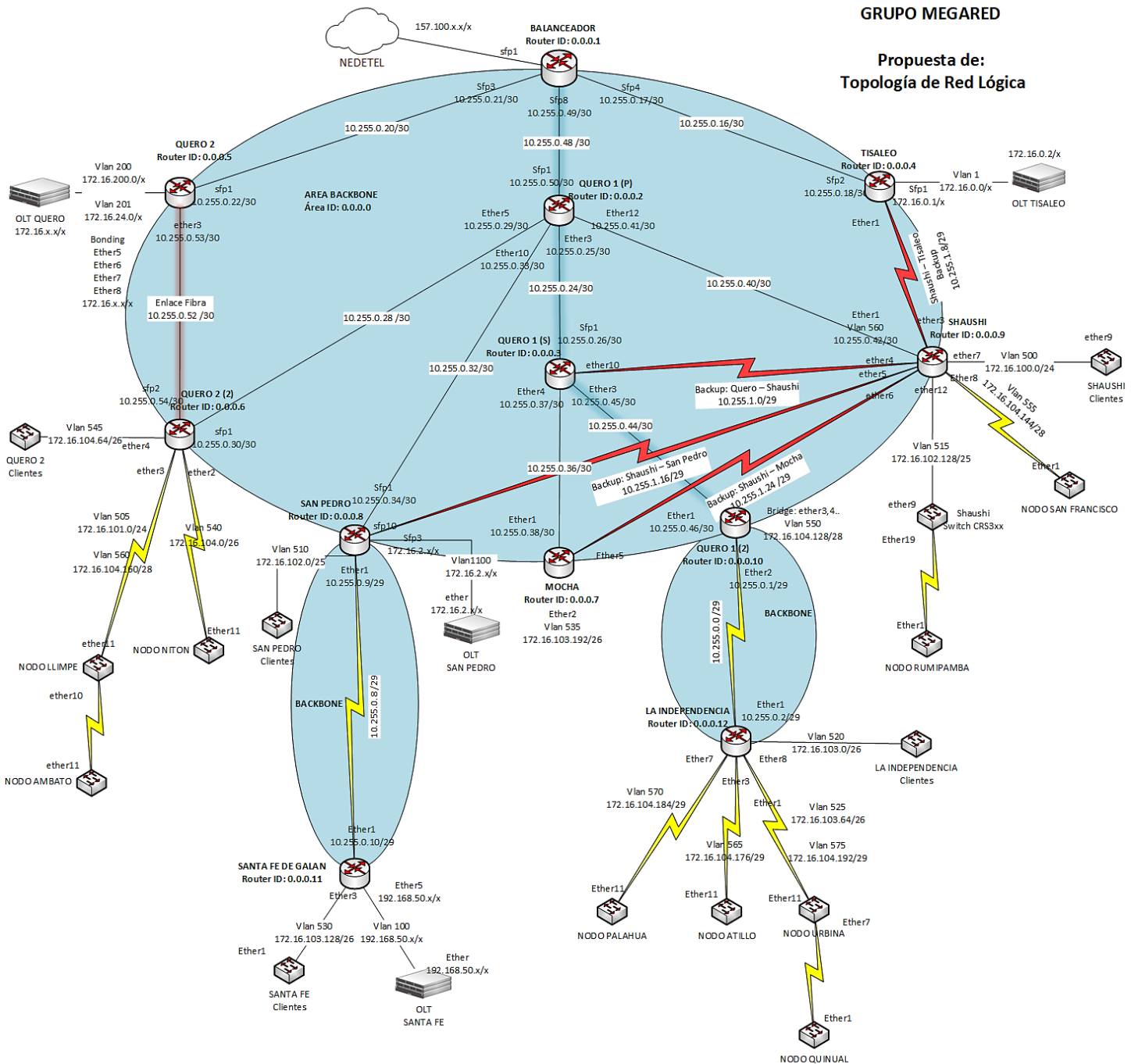


Figura 22. Propuesta de topología lógica de red para el ISP Grupo Mgeraed

Fuente: La Investigadora

Simulación del enrutamiento OSPF propuesto.

Para iniciar la configuración es necesario ubicar los equipos en la interfaz de EVE-NG, tal como lo muestra la topología propuesta.

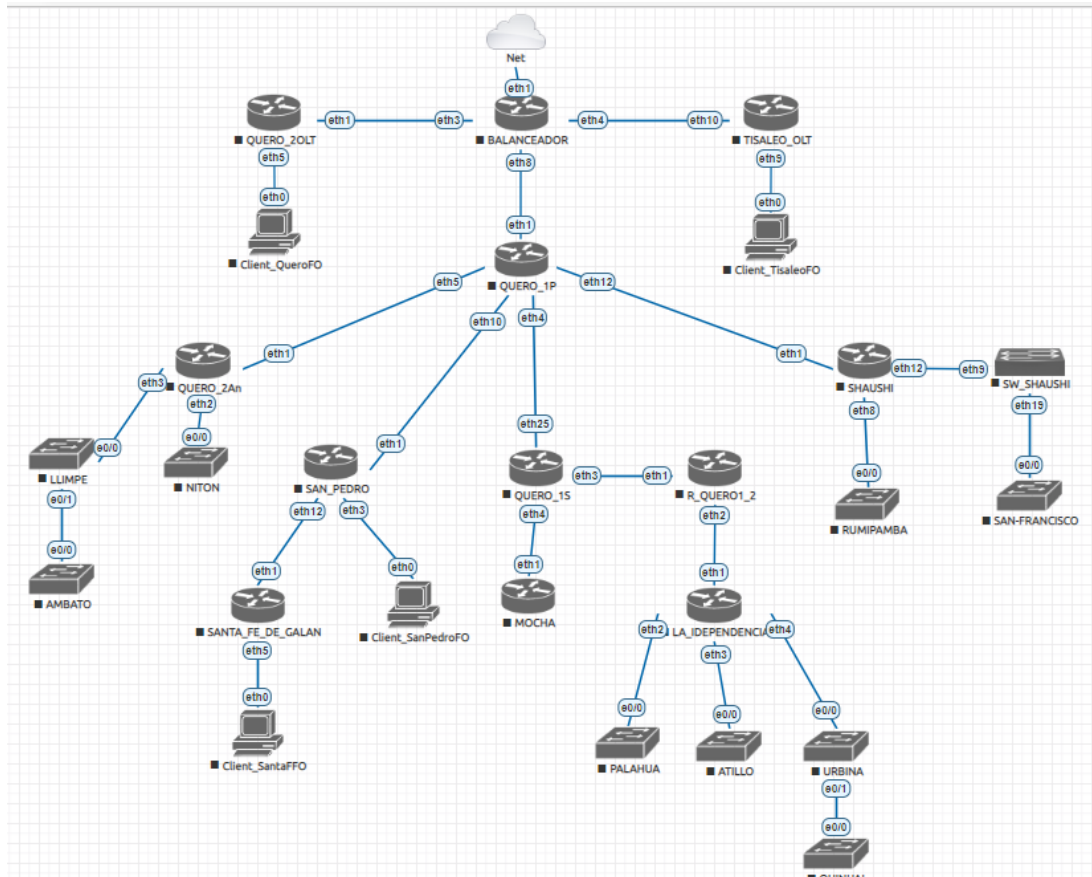


Figura 23. Simulación propuesta de red ruteada OSPF

Fuente: La Investigadora

Debido a que la red se encuentra configurada en modo bridge, el cambio de interfaces no afecta en la configuración lógica ya existente, se mejora la distribución de tráfico de interfaces.

Así también para que los clientes dispongan del servicio durante la migración, lo que se realiza es la configuración del enrutamiento dinámico OSPF sobre la configuración BRIDGE.

Para ello se toma como referencia la configuración del router de borde llamado: **BALANCEADOR**.

Pasos para configurar el enrutamiento dinámico OSPF

- Creación de una interfaz loopback, la cual tendrá como dirección IP en router ID del equipo.
- Agregar todas las redes pertenecientes a cada interfaz
- Asignar la dirección del Router ID
- Registro de redes en la sección de Networks en OSPF
- Asignar como redes pasivas a todas las redes que pertenecen a clientes, mismas que no compartirán mensajes LSA

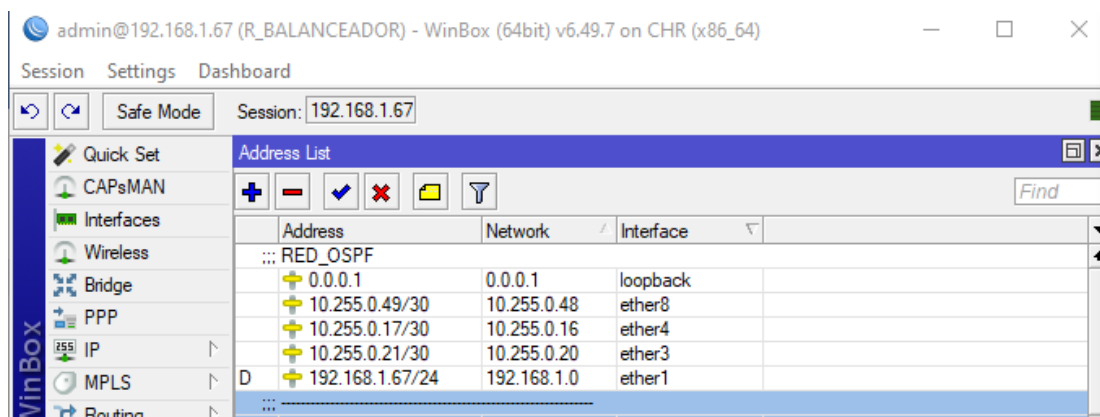


Figura 24. Asignación de direcciones IP a cada interfaz

Fuente: La Investigadora

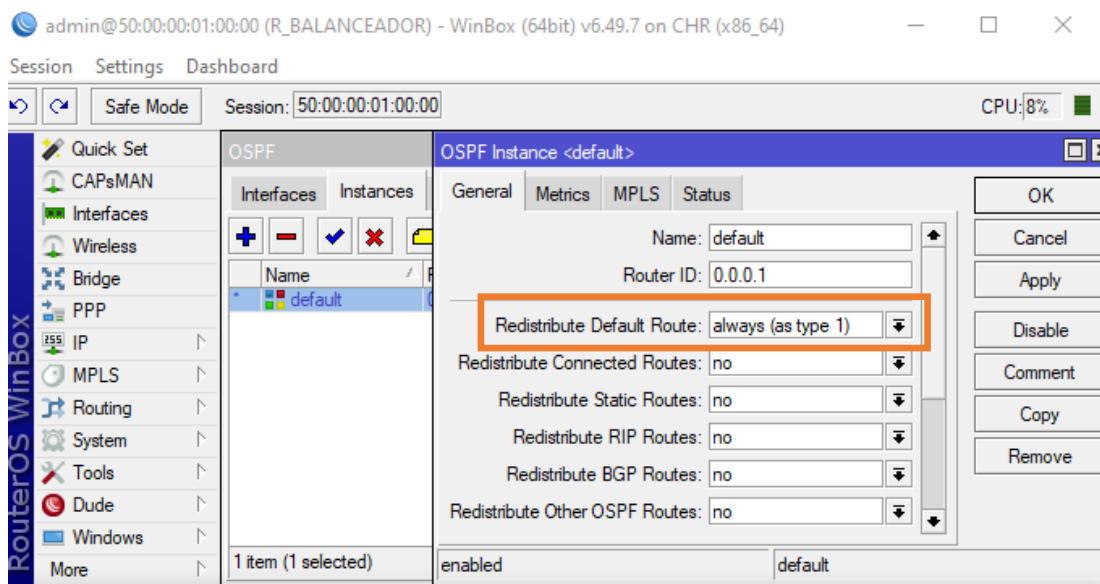


Figura 25. Asignación del parámetro de Router ID en OSPF

Fuente: La Investigadora

Solo en el router de borde es necesario activar la redistribución de la ruta por defecto, para que una vez enrutado, todos los routers puedan conocer esa ruta.

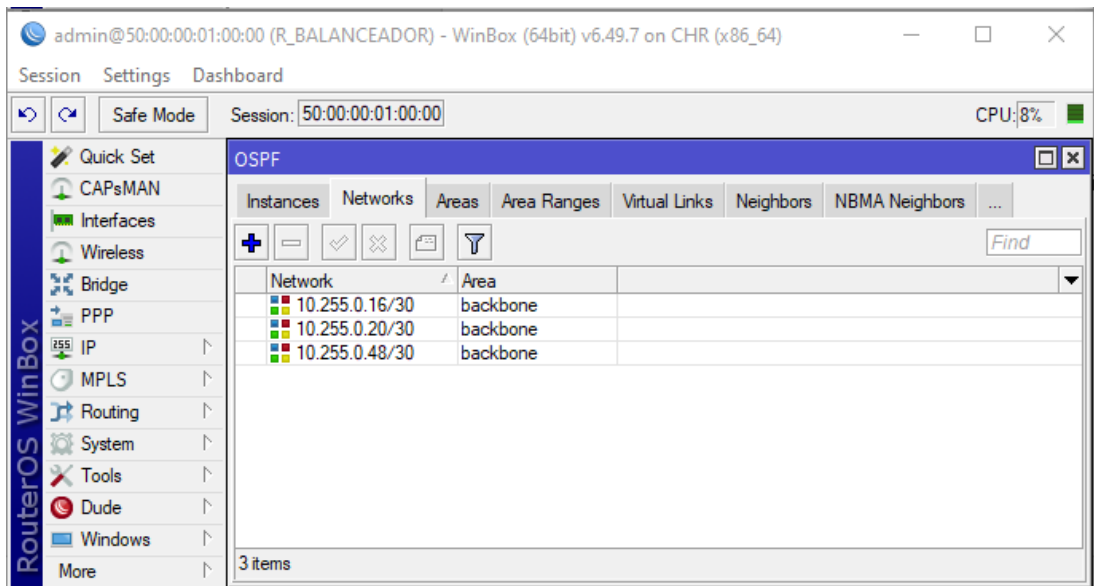


Figura 26. Designación de redes OSPF al área backbone

Fuente: La Investigadora

Finalmente, como todas las interfaces están conectadas a la interfaz bridge, la asignación de redes OSPF no será visible hasta que se haya desactivado la interface bridge.

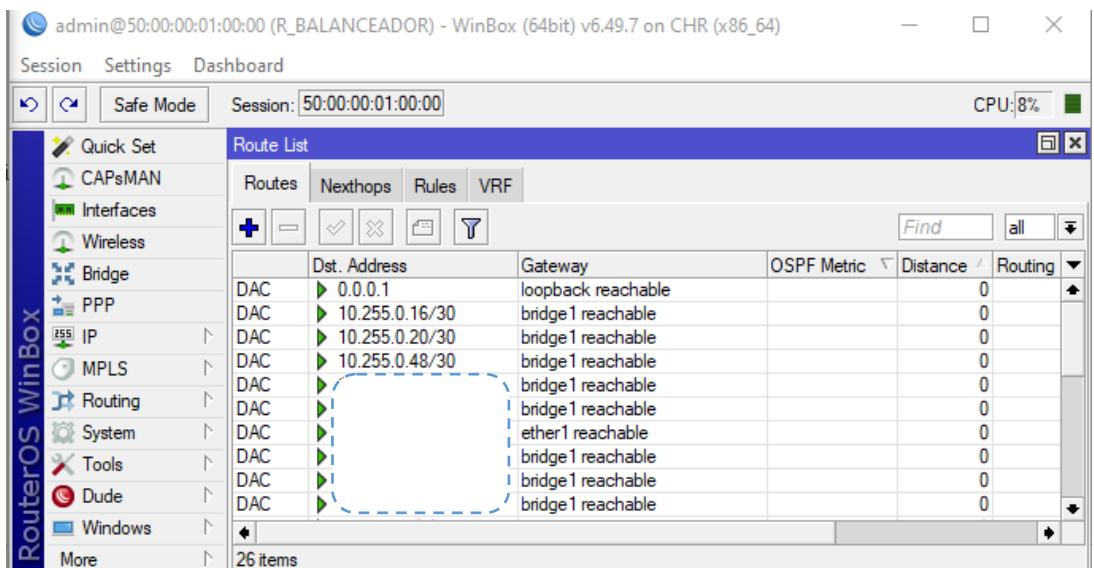


Figura 27. Rutas del router BALANCEADOR son desactivar interfaz bridge.

Fuente: La Investigadora

Este mismo procedimiento se debe aplicar para cada uno de los routers pertenecientes en la red. Cuando ya todo se encuentre configurado es momento de desactivar la interfaz bridge.

Pasos para desactivar la interfaz bridge

Para dichas pruebas se tomará como ejemplo al nodo: La Independencia ya que posee el router más alejado de la red según el diagrama lógico propuesto.

Address	Cost	Hops	Identity	Path	L2MTU	Version	Board
50:00:00:04:00:00	200	1	R_QUERO1_P	50:00:00:04:00:00	1500	6.49.7	CHR
50:00:00:02:00:03	200	1	R_QUERO2	50:00:00:02:00:03	1500	6.49.7	CHR
50:00:00:03:00:02	200	1	R_TISALEO	50:00:00:03:00:02	1500	6.49.7	CHR
50:00:00:08:00:02	400	2	QUERO_1An	50:00:00:04:00:00, 50:00:00:08:00:02	1500	6.49.7	CHR
50:00:00:05:00:03	400	2	R2_QUERO1_S	50:00:00:04:00:00, 50:00:00:05:00:03	1500	6.49.7	CHR
50:00:00:0A:00:00	400	2	R_SAN_PEDRO	50:00:00:04:00:00, 50:00:00:0A:00:00	1500	6.49.7	CHR
50:00:00:08:00:04	400	2	R_SHAUSHI	50:00:00:04:00:00, 50:00:00:08:00:04	1500	6.49.7	CHR
50:00:00:0D:00:00	600	3	RS_SHAUSHI	50:00:00:04:00:00, 50:00:00:08:00:04, 50:00:00:0D:00:00	1500	6.49.7	CHR
50:00:00:09:00:01	600	3	R_MOCHA	50:00:00:04:00:00, 50:00:00:05:00:03, 50:00:00:09:00:01	1500	6.49.7	CHR
0A:29:86:3A:9A:63	600	3	R_QUERO1_2	50:00:00:04:00:00, 50:00:00:05:00:03, 0A:29:86:3A:9A:63	1500	6.49.7	CHR
50:00:00:0C:00:01	600	3	R_SANTA_FE	50:00:00:04:00:00, 50:00:00:0A:00:00, 50:00:00:0C:00:01	1500	6.49.7	CHR
50:00:00:07:00:01	800	4	LA_INDEPENDENCIA	50:00:00:04:00:00, 50:00:00:05:00:03, 0A:29:86:3A:9A:63, 50:00:00:07:00:01	1500	6.49.7	CHR

Figura 28. Ingreso a router La Independencia vía Winbox

Fuente: La Investigadora

Routes	Nexthops	Rules	VRF
AS	0.0.0.0/0		reachable bridge 1
Do	0.0.0.0/0		10.255.0.1 reachable bridge 1
DAC	0.0.0.12		loopback reachable
DAC	10.255.0.0/29		bridge 1 reachable
DAo	10.255.0.8/29		10.255.0.1 reachable bridge 1
DAo	10.255.0.16/30		10.255.0.1 reachable bridge 1
DAo	10.255.0.20/30		10.255.0.1 reachable bridge 1
DAo	10.255.0.24/30		10.255.0.1 reachable bridge 1
DAo	10.255.0.28/30		10.255.0.1 reachable bridge 1
DAo	10.255.0.32/30		10.255.0.1 reachable bridge 1
DAo	10.255.0.36/30		10.255.0.1 reachable bridge 1
DAo	10.255.0.40/30		10.255.0.1 reachable bridge 1

Figura 29. Ruta por defecto redistribuida por router Balanceador

Fuente: La investigadora

Para que la red entienda la ruta que debe tomar una vez desactivada la interfaz bridge hay que inhabilitar la ruta por defecto compartida por la dirección 192.168.x.x

admin@50:00:00:07:00:01 (LA_INDEPENDENCIA) via 50:00:00:01:00:00 - WinBox (64bit) v6.49.7 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 50:00:00:07:00:01

- Quick Set
- CAPsMAN
- Interfaces
- Wireless
- Bridge
- PPP
- Mesh
- IP
- MPLS
- Routing
- System
- Queues

Route List

Routes Nexthops Rules VRF

+ - ✓ ✗ 📁 🔍

	Dst. Address	Gateway
XS	0.0.0.0/0	<input type="text"/>
DAo	0.0.0.0/0	10.255.0.1 reachable bridge1
DAC	0.0.0.12	loopback reachable
DAC	10.255.0.0/29	bridge1 reachable
DAo	10.255.0.8/29	10.255.0.1 reachable bridge1
DAo	10.255.0.16/30	10.255.0.1 reachable bridge1
DAo	10.255.0.20/30	10.255.0.1 reachable bridge1
DAo	10.255.0.24/30	10.255.0.1 reachable bridge1
DAo	10.255.0.28/30	10.255.0.1 reachable bridge1
DAo	10.255.0.32/30	10.255.0.1 reachable bridge1

Figura 30. Inhabilitar la ruta por defecto con gateway 192.168.x.x

Fuente: La Investigadora

Como se observa en la figura anterior, ahora la ruta por defecto es alcanzable por el Gateway 10.255.0.1. Este proceso hay que realizarlo en cada uno de los routers. Con esto tendrá la salida a internet por la nueva distribución OSPF. Finalmente se elimina la interfaz bridge de cada uno de los routers de la red, y ya se tendrán las nuevas rutas dinámicas OSPF.

Configuración de rutas de respaldo

Una vez ya migrada la red, el último paso es agregar la configuración de rutas de respaldo con distintos costos, esto previene la caída de la red brindando solución a los largos periodos de tiempo de clientes sin servicio, hasta que el administrador de red logre activar las rutas de respaldo.

A continuación, se presenta el diagrama de costos aplicados a las rutas de respaldo.

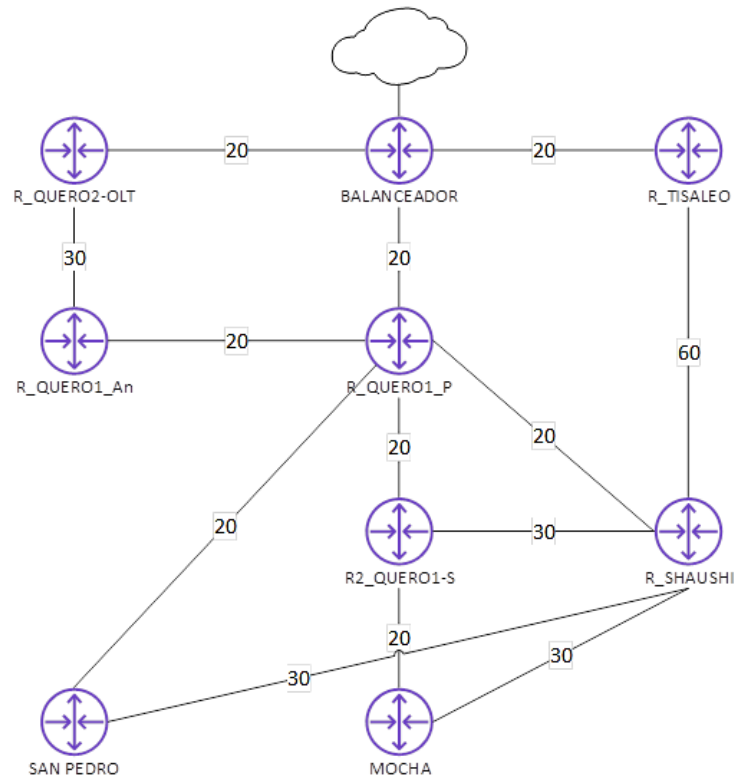


Figura 31. Métrica OSPF consideraba para rutas de respaldo

Fuente: La Investigadora

La métrica OSPF por defecto es de 10 en cada interfaz, los valores que se modificarán son las métricas de las interfaces conectadas a las rutas de respaldo. Como, por ejemplo:

Tabla 29. Métricas OSPF en rutas de respaldo

Fuente: La Investigadora

Ruta	Métrica en interfaz router 1	Métrica en interfaz router 2
Shaushi - Tisaleo	30	30
Shaushi - Mocha	15	15
Shaushi – Quero 1	15	15
Shaushi – San Pedro	15	15
Quero OLT – Quero 2	15	15

Cabe destacar que las rutas de respaldo son mediante enlaces inalámbricos a excepción de la ruta Quero Olt a Quero 2 que fue propuesta mediante fibra óptica, es por esa razón que en el enlace de Shaushi a Tisaleo el costo es mayor que en el resto de respaldos, ya que, si llegaran a caerse 2 rutas principales simultáneamente, tome como última opción el tráfico de Shaushi a Tisaleo porque este enlace tiene un consumo elevado de Mbps y si tomara esa ruta, habría saturación de tráfico.

A continuación, se muestra la configuración del costo OSPF en el router de Shaushi, puesto que posee mayor número de rutas de respaldo.

admin@50:00:00:06:00:00 (R_SHAUSHI) via 50:00:00:01:00:00 - WinBox (64bit) v6.49.7 on CHR (x86_64)

Session Settings Dashboard

Safe Mode Session: 50:00:00:06:00:00

OSPF

Interfaces Instances Networks Areas Area Ranges Virtual Links

	Interface	Cost	P Address	Area
D	ether1	10	10.255.0.42	backbone
	ether3	30	10.255.1.10	backbone
	ether4	15	10.255.1.2	backbone
	ether5	15	10.255.1.18	backbone
	ether6	15	10.255.1.26	backbone
P	vlan500-Shaush	10	172.16.100.1	backbone
P	vlan515-Rumip...	10	172.16.102.129	backbone
P	vlan555-SanFr...	10	172.16.104.145	backbone

Figura 32. Costo de rutas de respaldo en router del nodo Shaushi

Fuente: La Investigadora

En la figura anterior, también se detallan las rutas pasivas configuradas para los clientes del nodo de Shaushi. Se les asignan en modo pasivo para que los mensajes LSA no sean tomados para esas rutas, ya que solo son importantes en enlaces con otro router.

Tiempo de respuesta de creación de rutas OSPF

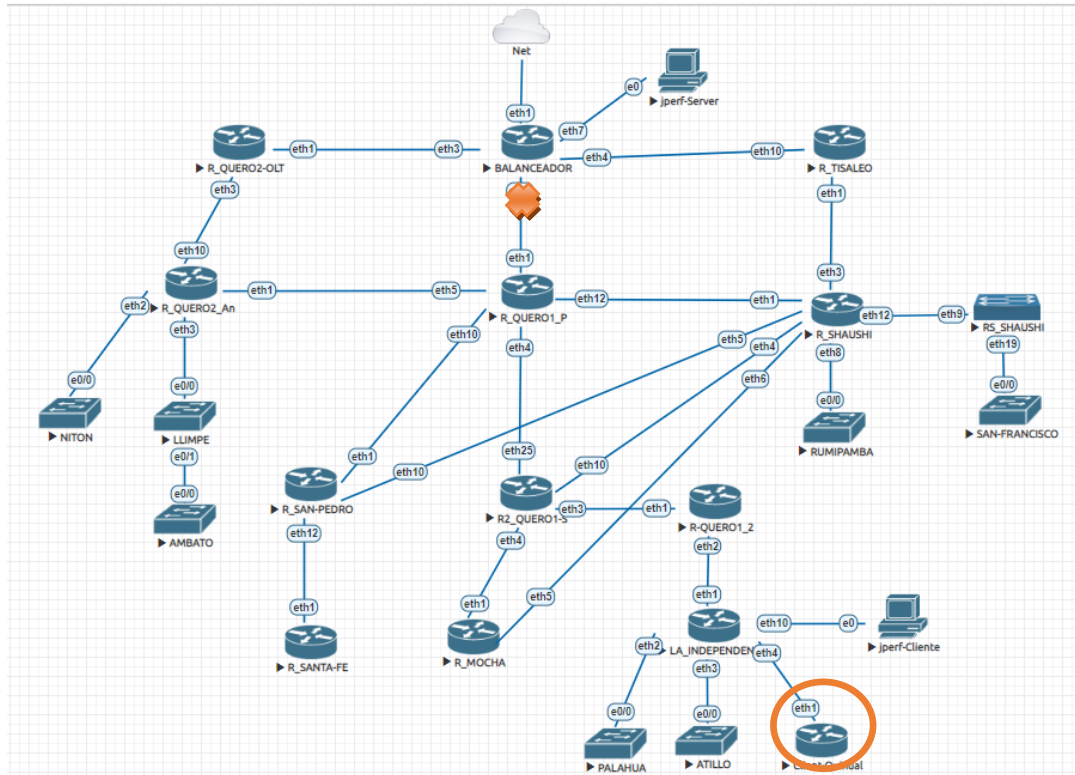


Figura 33. Simulación de caída de interfaz ether8 del router de borde: Balanceador

Fuente: La Investigadora

Como primer punto se analizan las rutas que se encuentran conectadas o distribuidas por la interfaz ether8 del router de borde, en donde la ruta con mayor métrica OSPF de 50: es la de clientes finales del router conectado al nodo La Independencia. Para esta prueba se crea un cliente en dicho nodo con configuración dhcp en el rango de ip de clientes de Quinual. Este cliente obtiene la dirección 172.16.104.198/24 alcanzable por la interface vlan575.

Desde dicho cliente se realizó pruebas con el comando ping hacia el servidor de jperf utilizado en esta ocasión para pruebas, dicho servidor posee la IP: 192.168.255.20.

A continuación, se muestran 3 escenarios: rutas configuradas cuando la interfaz ether8 se encuentra activa, detección de caída de ruta, recalculation de ruta.

Rutas OSPF cuando se mantiene activa la interfaz ether8

Se verifica que las rutas son alcanzables por la interfaz ether 8 y que la mayor métrica OSPF es de 50

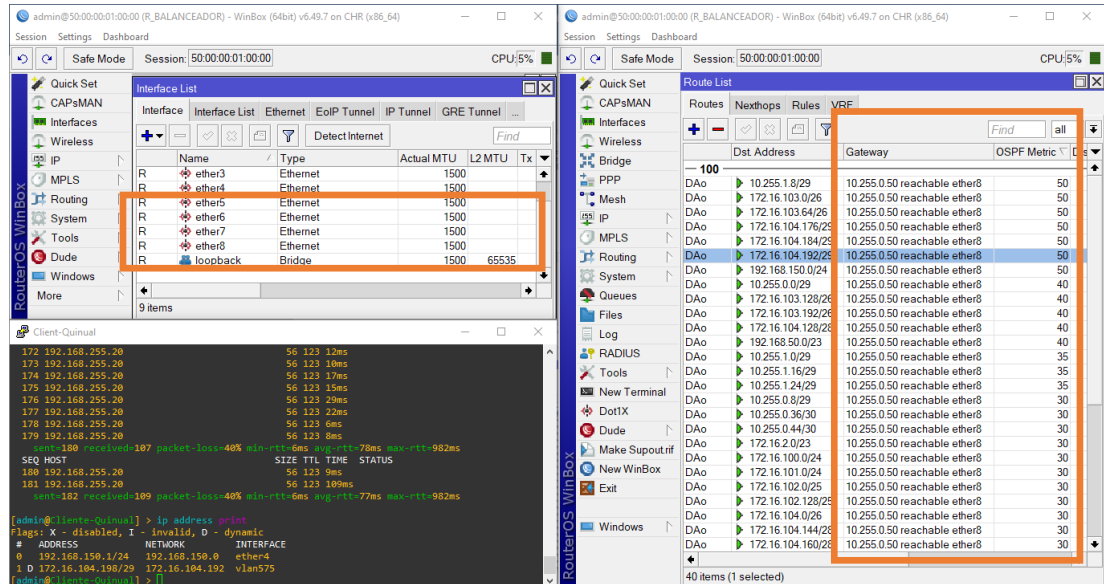


Figura 34. Rutas OSPF alcanzables por interfaz ether8

Fuente: La Investigadora

Desactivación de interfaz ether8 como simulación de caída de ruta

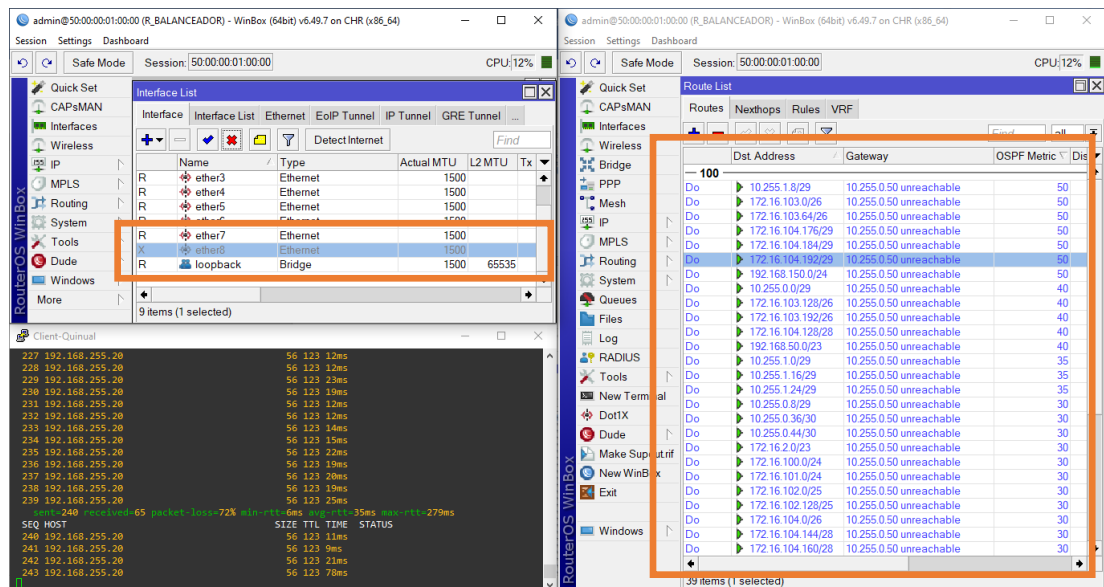


Figura 35. Desactivación de interfaz ether8 del router balanceador

Fuente: La Investigadora

La captura realizada fue con se perdieron todas las rutas pero que aun no había transcurrido más de 1 segundo de la desactivación de la interfaz.

Recálculo de ruta OSPF

El cliente de Quinual posee una pérdida de 4 paquetes ping hasta que el protocolo de enrutamiento dinámico OSPF haya recalculado la ruta mediante el uso del algoritmo de Dijkstra. Ahora la métrica OSPF es mayor a la ruta establecida por la interfaz ether8. A su vez las redes se encuentran siendo alcanzables por la interfaz ether3, el cual pertenece al router de Quero2-OLT, como se observa en la siguiente figura.

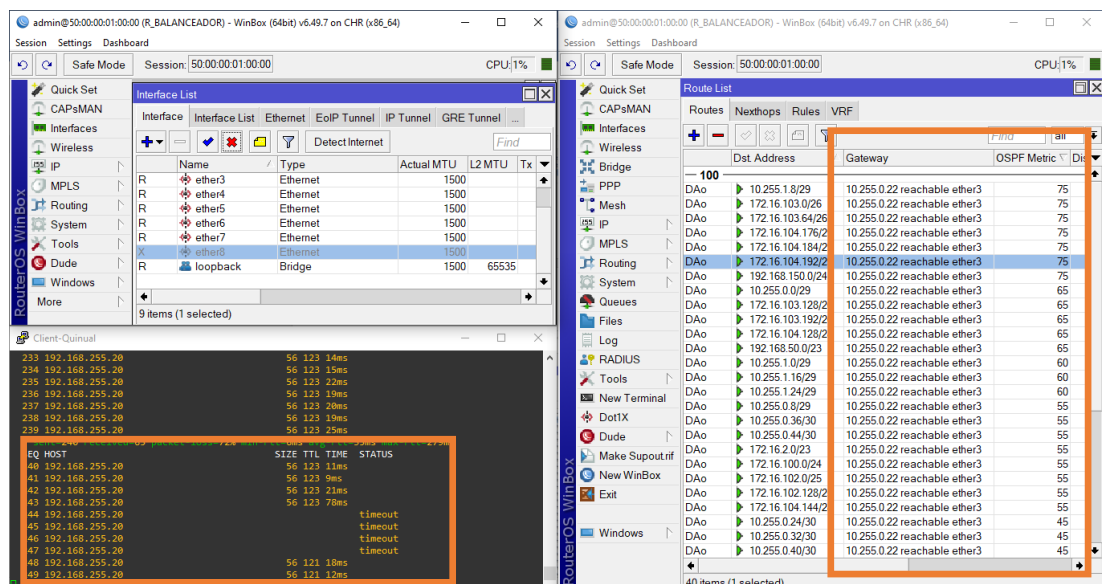


Figura 36. Recálculo de ruta OSPF una vez desactivada la interfaz ether8

Fuente: La Investigadora

Resultado:

Mediante las pruebas de caída de ruta ether8 del router de borde, el cliente más alejado de la red posee 4 pérdidas de paquetes, tiempo estimado en el que el enrutamiento dinámico OSPF recalcula la ruta más corta basándose en los costos de cada interfaz. Comparando este diseño propuesto tanto lógico como físico con la posible caída de la interfaz ether8 en la configuración física y lógica actual, el diseño propuesto brinda un tiempo de reconexión casi inmediato a diferencia de la configuración actual que el tiempo de reconexión del servicio está relacionado con el tiempo que se demore el administrador de red y los técnicos en levantar la ruta.

Pruebas de tráfico en la configuración propuesta para el ISP Grupo Megared: OSPF

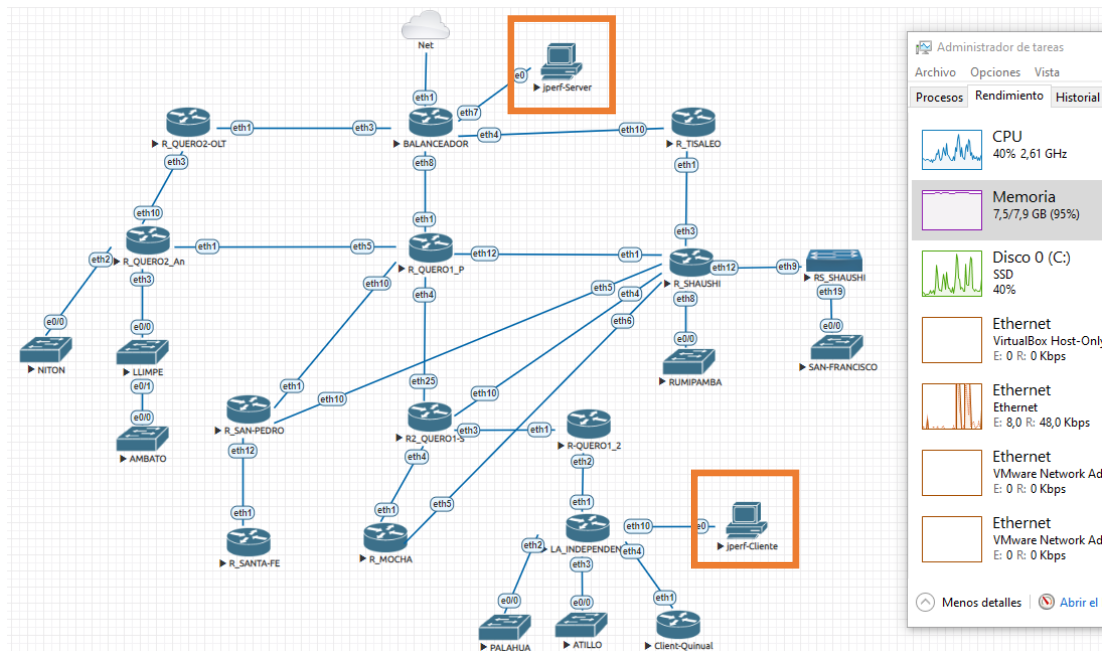


Figura 37. Prueba de tráfico en la configuración actual del ISP Grupo Megared: OSPF

Fuente: La Investigadora

Para realizar las pruebas de tráfico para la red con enrutamiento dinámico OSPF, se toma en cuenta los mismos escenarios que la prueba de tráfico en red bridge (tabla 19), y los mismos valores de paquetes UDP. Obteniendo los siguientes resultados:

Tabla 30. Pruebas de tráfico UDP con 20,09 kbps en configuración OSPF

Fuente: La Investigadora

RED OSPF: TRAFICO UDP: 20,09 kbps				
RTT min	RTT max	AVG	Jitter (ms)	Packet Loss (%)
5	56	14	3,93	0
6	88	19	5,96	0
6	50	15	3,49	0
6	85	19	5,47	0
6	108	20	11,9	0
6	89	168	9,97	0
6	49	16	5,33	0
6	80	18	2,81	0

6	39	14	7,22	0
6	271	23	20,04	0
6	56	16	5,84	0
6	66	16	2,98	0
6	70	15	3,5	0
6	75	18	6,2	0
6	56	16	8,73	0
6	311	32	2,97	0
6	123	21	9,54	0
6	437	27	43,62	0
6	66	18	10,5	0
5	70	14	4,68	0
6	130	18	7,19	0
5	91	18	1,03	0
6	42	14	3,06	0
6	64	18	8,32	0
6	99	17	8,87	0
6	93	19	30,89	0
6	55	16	8,24	0
6	35	13	5,9	0
6	39	15	4,22	0
6	43	15	6,032	0
5,90	97,87	22,73	8,61	0,00

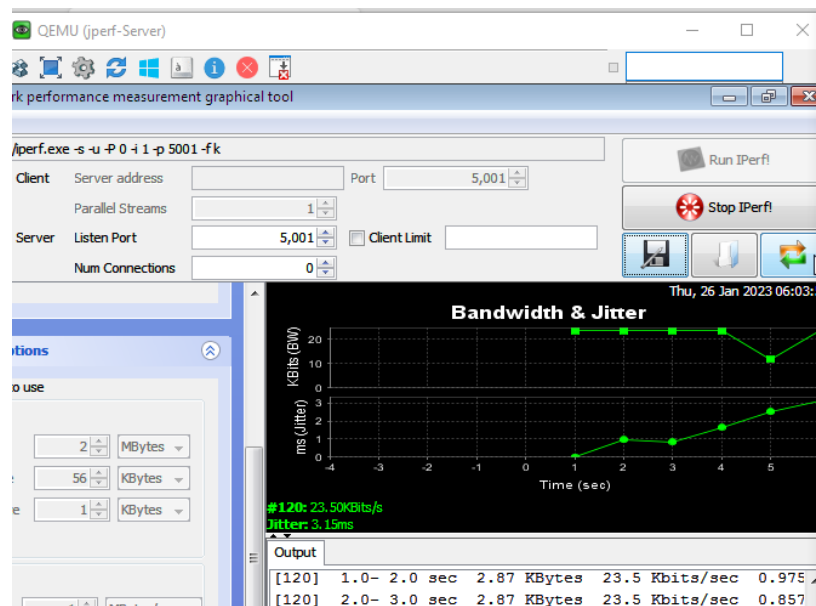


Figura 38. Envío de paquetes UDP para prueba de tráfico en red OSPF

Fuente: La Investigadora

Cabe recalcar que mientras se realizaba la prueba de tráfico UDP, también se mantenía un ping constante de 60 segundos de duración, debido a lo mencionado, se presenta la siguiente captura de wireshark mientras se generaba tráfico en la red OSPF y se ejecutaba el protocolo ICMP para verificar el tiempo de respuesta de la red.

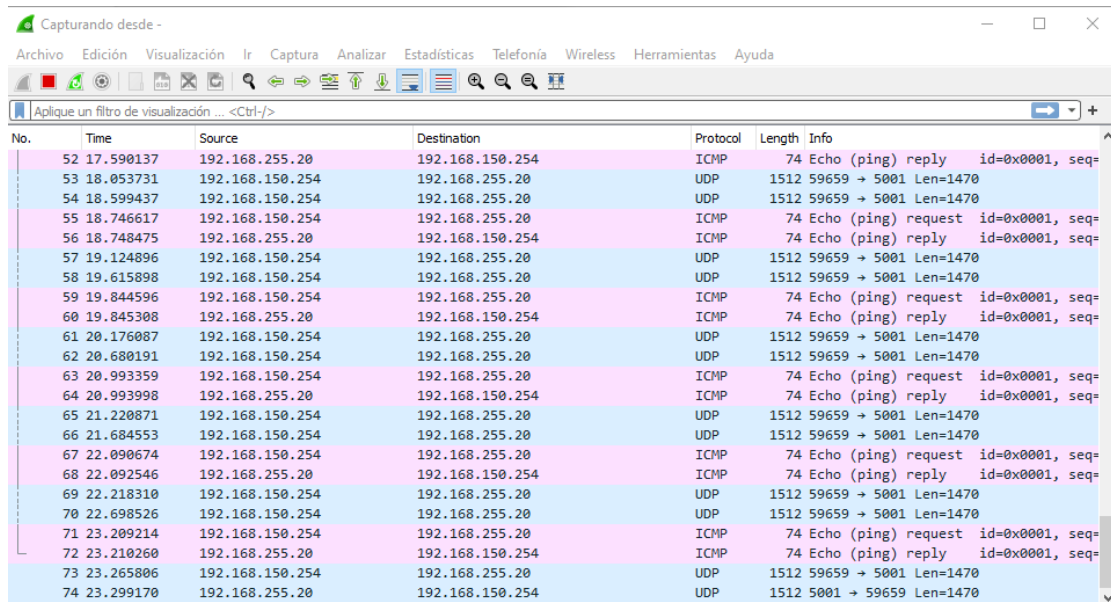


Figura 39. Captura de tráfico UDP en red OSPF con Wireshark

Fuente: La Investigadora

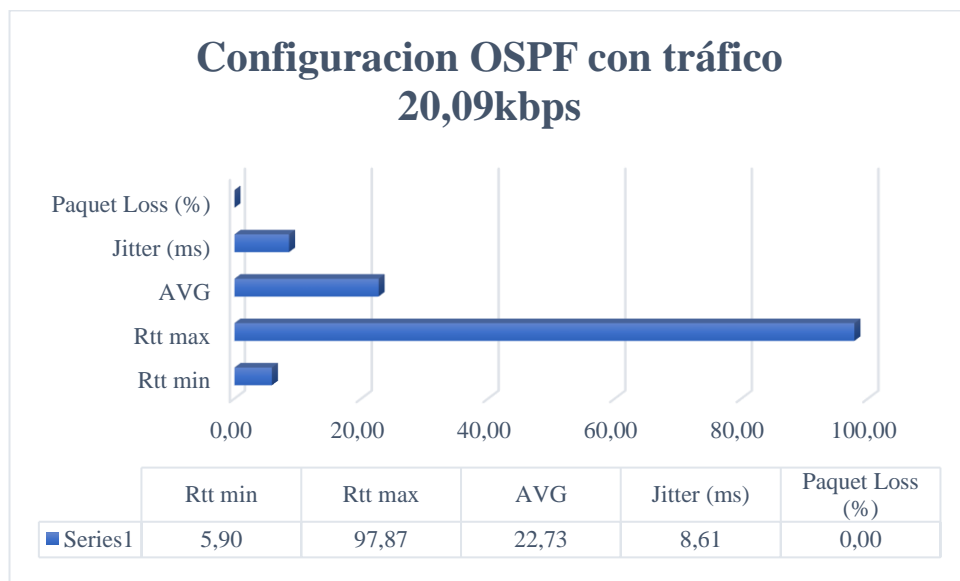


Figura 40. Prueba de tráfico con 20,09kbps en configuración OSPF

Fuente: La Investigadora

A continuación, se presenta la tabla de resumen de las pruebas de segundo escenario en la red propuesta OSPF con 679,69kbps

Tabla 31. Pruebas de tráfico UDP con 679,79 kbps en configuración OSPF

Fuente: La Investigadora

RED OSPF: TRAFICO UDP: 679,79 kbps				
RTT min	RTT max	AVG	Jitter	Packet Loss (%)
6	42	15	1,75	0,17
6	109	16	3,1	0,69
7	62	62	2,2	0,69
6	93	17	6,54	0
6	104	18	4,9	0
6	66	15	6,27	0,52
7	294	29	2,4	1,2
6	64	17	1,07	0,2
5	93	17	1,97	0,17
6	61	17	5,72	1,6
6	52	15	2,59	0,17
6	66	14	3,71	0
6	76	17	3,96	0,69
6	57	16	0,66	1
6	50	16	1,36	0
6	61	18	1,15	0,17
7	62	19	2,73	0,17
6	38	12	8,421	0
6	56	18	3,06	0,17
5	59	15	1,3	0,34
6	54	14	0,42	0,17
6	48	16	4,32	0,69
6	120	17	1,48	0,17
6	76	18	2,91	0
6	50	17	1,16	0,86
6	58	14	0,3	0,52
6	53	17	0,53	0,52
5	102	21	2,6	0,69
7	63	21	2,21	0
6	111	17	5,61	0,52
6,03	76,67	18,50	2,88	0,40

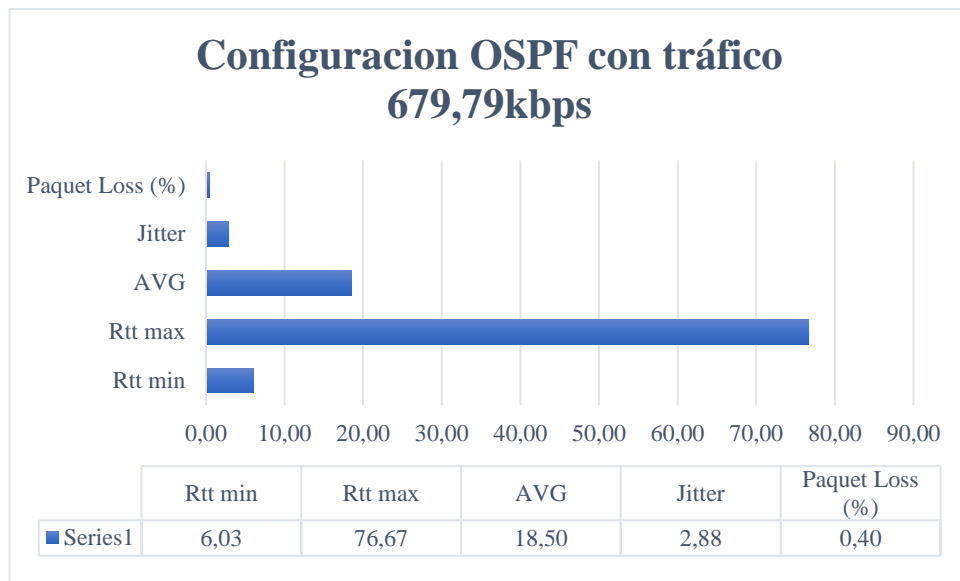


Figura 41. Prueba de tráfico con 679,79kbps en configuración OSPF

Fuente: La Investigadora

3.2.1.5. Gestión en la administración automática de equipos

Se crea un script.py en donde se colocan los métodos HTTP: get y set para obtener información y asignar si es que ha existido un cambio.

El en archivo se agregan librerías que permitirán la conexión con el api del router de borde y permitirá la ejecución de archivos. Json

- import json
- import requests
- import routers_api
- from routers_api

El archivo.json debe contener la estructura específica para la configuración OSPF siguiente:

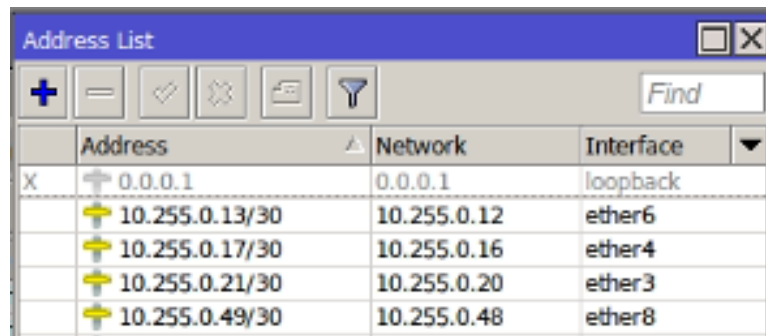
```

{
  "config_id": {
  },
  "ip_address": {
  },
  "interfaces": {
  },
  "protocols": {
  }
}

```

En donde se detalla la configuración actual de los equipos, en este caso se toma como referencia la configuración del router de borde.

Para la configuración automática de equipos, se crea un script.py donde realiza el llamado al archivo: config.json en donde se encuentra la configuración OSPF del router balanceador. Posteriormente realiza una comparativa de los parámetros que se encuentren ya configurados, si el parámetro no es encontrado el archivo: config.json lo reconfigurará.



	Address	Network	Interface
X	0.0.0.1	0.0.0.1	loopback
	10.255.0.13/30	10.255.0.12	ether6
	10.255.0.17/30	10.255.0.16	ether4
	10.255.0.21/30	10.255.0.20	ether3
	10.255.0.49/30	10.255.0.48	ether8

Figura 42. Eliminación de la dirección de loopback para prueba de configuración automática

Fuente: La Investigadora

Para la ejecución del archivo se utiliza el siguiente comando:

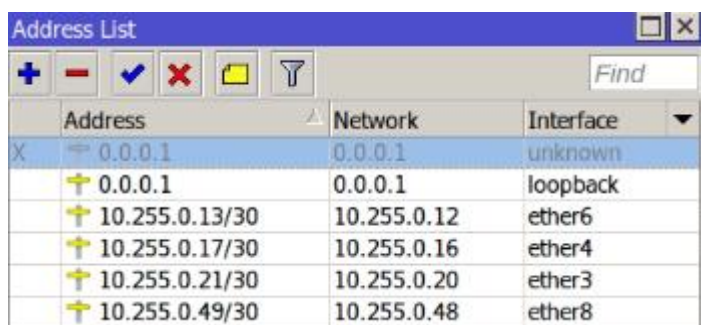
- *Python3 script.py*

```
_R_Red_ospf/balanceador$ python3 scpt2.py
loopback 0.0.0.1/32 Bridge
loopback loopback
#g
```

Figura 43. Ejecución de script.py para la reconfiguración de equipo

Fuente: La Investigadora

Una vez ejecutado el archivo, y detectado la eliminación de la dirección de loopback, ejecutará el archivo.json para que mediante la opción set, agregue la dirección IP faltante.



Address	Network	Interface
0.0.0.1	0.0.0.1	unknown
0.0.0.1	0.0.0.1	loopback
10.255.0.13/30	10.255.0.12	ether6
10.255.0.17/30	10.255.0.16	ether4
10.255.0.21/30	10.255.0.20	ether3
10.255.0.49/30	10.255.0.48	ether8

Figura 44. Configuración de interfaz loopback mediante api-rest

Fuente: La Investigadora

3.3. Análisis de Resultados

Pruebas de tráfico

El análisis que se realizó para las pruebas de tráfico dentro de la red, tomó como referencia la investigación denominada, “Analysis of Failover Link System Performance in OSPF, EIGRP, RIPv2 Routing Protocol with BGP2”, en donde se realizó pruebas de: rendimiento, fluctuación, pérdida de paquetes y retraso utilizando la herramienta jperf que a su vez trabaja con ipfer. [4]

3.4. Resultados

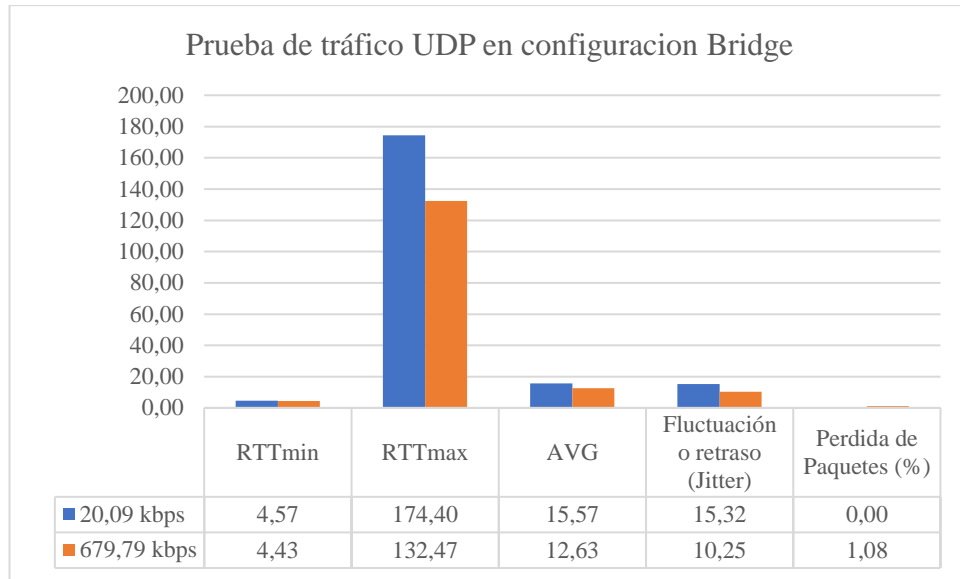


Figura 45. Comparación de pruebas de tráfico UDP con 20,09 y 679,79 kbps en red BRIDGE

Resultado:

En la prueba de tráfico realizada en la configuración bridge, en donde se ejecutaron 30 pruebas con un tráfico UDP de 20,09kbps y de 679,79kbps, se concluye que el tiempo de respuesta (RTT) y el tiempo de retraso o fluctuación es menor mientras existe un mayor tráfico, pero aumenta el porcentaje de pérdidas de paquetes. A un rango considerable de 1,08% que, si se compara con el tráfico real de la red, se perderían 43,29Mbps.

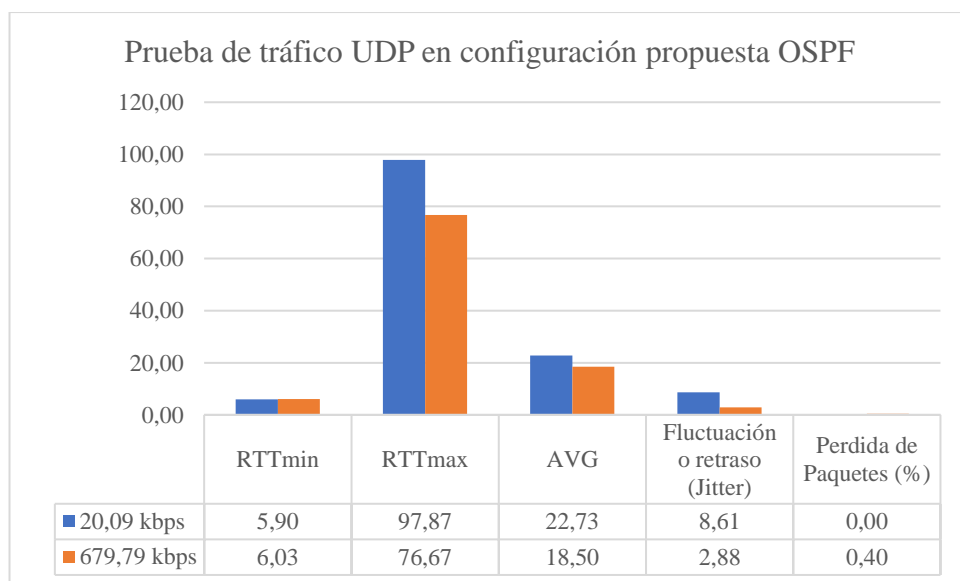


Figura 46. Comparación de pruebas de tráfico UDP con 20,09 y 679,79 kbps en red OSPF

Resultado:

En la prueba de tráfico realizada en la configuración OSPF, en donde se ejecutaron 30 pruebas con un tráfico UDP de 20,09kbps y de 679,79kbps, se concluye que el tiempo de retraso o fluctuación disminuye considerablemente, pero existe igual una pérdida de paquetes del 0,40%, lo que en el tráfico real representa: a 16,81Mbps en toda la red.

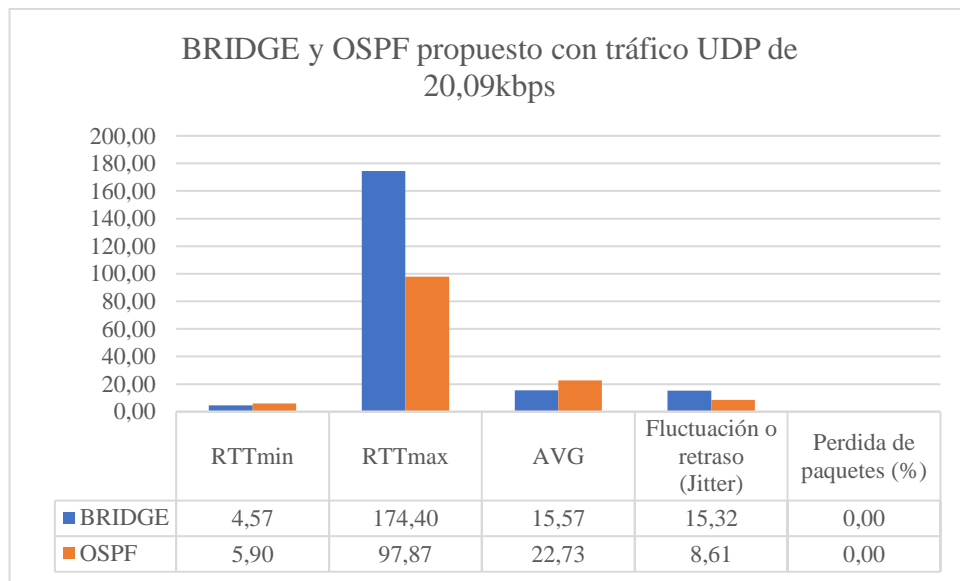


Figura 47. Comparación de pruebas de tráfico UDP entre red bridge y red OSPF con 20,09kbps

Resultado:

En la prueba de tráfico realizada con la configuración BRIDGE y la configuración OSPF, en donde se ejecutaron 30 pruebas con un tráfico UDP de 20,09kbps se concluye que la configuración BRIDGE posee un tiempo de respuesta menor a la configuración OSPF, pero presenta casi el doble de fluctuación o retraso del paquete. En ninguno de los 2 casos se presentan pérdidas de paquetes con el valor de tráfico analizado.

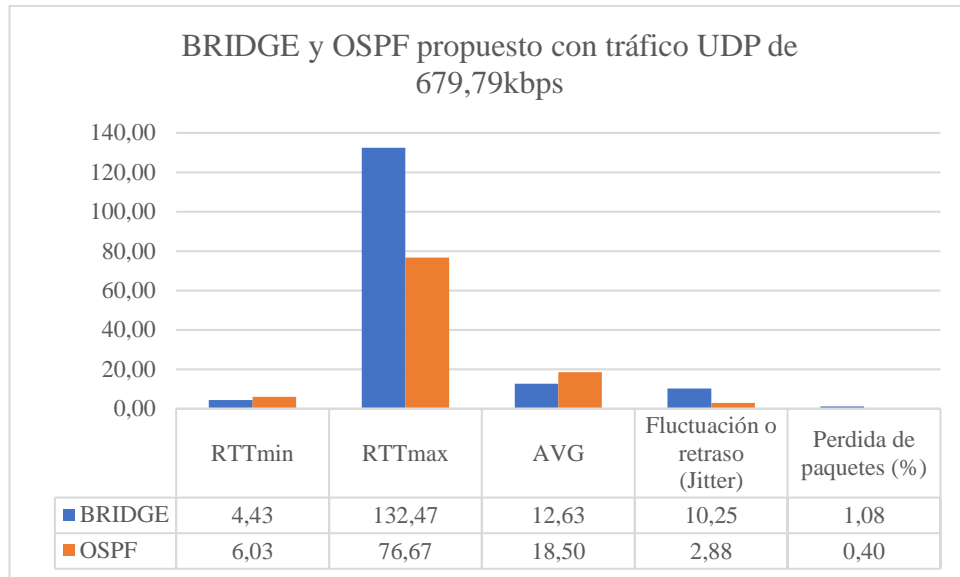


Figura 48. Comparación de pruebas de tráfico UDP entre red bridge y red OSPF con 679,79kbps

Resultado:

En la prueba de tráfico realizada con la configuración BRIDGE y la configuración OSPF, en donde se ejecutaron 30 pruebas con un tráfico UDP de kbps se concluye que la configuración BRIDGE posee un tiempo de respuesta menor a la configuración OSPF, pero posee un retraso del paquete (jitter) de casi 5 veces más que en la configuración OSPF. Así mismo, OSPF posee menor porcentaje de pérdida de paquetes, en donde si se realiza una comparativa con el tráfico real de la red la configuración bridge pierde: 43,29Mbps y la configuración OSPF: 16,81Mbps de un total de 4202,8Mbps.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

Una vez finalizado el trabajo de investigación se concluye:

- Mediante el análisis del diagrama físico de red obtenido a partir de la investigación de campo realizada se logra determinar que la empresa Grupo Megared proveedora de servicios de internet, cuenta con una topológica física jerárquica de red y una configuración tipo bridge sin enrutamiento que, según el análisis temático realizado en la entrevista al gerente de la empresa, dicha configuración ha generado 2 inconvenientes de tormentas de difusión en toda la red: 1 en el año 2021 y otro a inicios del año 2022, especialmente para los usuarios que poseen servicio inalámbrico.
- En base a los diagramas de red: físico y lógico, elaborados a partir de la investigación de campo se determinó que el diseño actual en la empresa Grupo Megared es vulnerable a caídas de red ya que no cuenta con rutas de respaldo debido a la configuración lógica tipo bridge utilizada. Por tal razón, se concluye que la implementación de un protocolo de enrutamiento dinámico mejora la disponibilidad del servicio de internet a los usuarios debido a que posee un menor tiempo de convergencia en el cálculo de rutas y actualización de tablas de enrutamiento.
- Se diseñó el diagrama de topología física en donde se adicionaron 1 router CCR2004-16G-2S+PC en el nodo Quero 2 que será útil para el manejo de rutas de respaldo debido a que posee 2 puertos SFP+ con velocidad de transmisión de hasta 10Gbps. También se agregaron 2 routers RB2011UiAS-RM para los nodos de Quero 1 y La Independencia, para brindar direccionamiento a cada nodo de la red.

- Mediante los cálculos realizados se logra determinar que la empresa Grupo Megared posee una tasa de crecimiento de: -0,07089 en el sector inalámbrico representando pérdida de clientes. Para lo cual se propuso una tabla de direccionamiento tomando en cuenta la cantidad actual de usuarios en el servicio inalámbrico.
- Las pruebas de tráfico realizadas entre la configuración bridge actual y la configuración OSPF propuesta con un tamaño de paquete UDP de 679,79 kbps donde se determinó que la configuración bridge posee un mejor tiempo de respuesta ping con un resultado avg de 12,63 milisegundos, en comparación a OSPF que posee un avg de 18,50ms. Por otra parte, OSPF posee un menor porcentaje de pérdida de paquetes UDP con 0,4% y menor variación de latencia con 2,58ms en comparación a la configuración bridge con un porcentaje de pérdida de paquetes del 1,8% y una variación de latencia de 10,25 ms.
- Se generó la configuración automática de equipos con la ejecución de un script.py de configuración, realizando una prueba de eliminación de una IP estática agregada al router de borde. En donde se ejecutó el script.py, mismo que se comunica con el router de borde y reconfigura la IP eliminada realizando una comparación entre las IP ya configuradas para evitar la sobrescritura.

4.2. Recomendaciones

- En la investigación de campo se pudo verificar que existen cables que no se encuentran conectados en sus extremos y no poseen etiquetas, esto puede generar confusión para los técnicos y cometer fallos humanos, por lo cual se recomienda reorganizar los elementos físicos del nodo de red para evitar interferencias e incorrecta manipulación de equipos, se sugiere la utilización de normas: ANSI/TIA/EIA-568-B.2 para el cableado de par trenzado,

ANSI/TIA/EIA-568-B.3 para el cableado de fibra óptica y EIA/TIA-606 para el etiquetado de cables.

- Para la simulación de red, es necesario trabajar con los requerimientos del software de emulación, puesto a que si se colocan varios equipos configurables y VPCs virtuales el rendimiento de CPU como de RAM pueden llegar a sus niveles máximos y afectar el resultado de los de prueba.
- Grupo Megared no cuenta con acceso a internet mediante direccionamiento IPv6, se recomienda optar por un paquete de proveedor que incluya dicho direccionamiento o netamente el cambio de proveedor. Para una futura migración IPv4 a IPv6 se propone la tabla de direccionamiento IPv6 que consta en el Anexo 5.

BIBLIOGRAFÍA

- [1] J. I. Bayas Villagomez, “Servidor de control de dispositivos y servicios mediante el protocolo SNMP para la red de datos en CELEC.E.P. Unidad de negocio HIDROAGOYAN.,” Jul. 2015.
- [2] F. A. Freire Aragón, “Análisis y propuesta de mejoramiento del sistema de seguridad perimetral aplicable a institución pública de seguridad social,” 2018.
- [3] A. M. Conde Gil, “Automatización de redes informáticas con Python,” Jan. 2020.
- [4] A. Fiade, M. A. Agustian, and S. U. Masrurroh, “Analysis of Failover Link System Performance in OSPF, EIGRP, RIPv2 Routing Protocol with BGP,” May 2020.
- [5] Byron Oviedo, Emilio Zhua, Genesis Bowen, and Bryan Patiño, “Voz IP seguras implementadas en Redes Definidas por Software,” *Rev Cienc Soc*, vol. 27, 2021.
- [6] Cisco, “Problemas de STP y consideraciones de diseño relacionadas,” Dec. 05, 2017. https://www.cisco.com/c/es_mx/support/docs/lan-switching/spanning-tree-protocol/10556-16.html
- [7] Bnamericas, “Ranking de Calidad: reclamos caen 50% y telefonía e internet fijas presentan las tasas más altas,” Mar. 29, 2022.
- [8] W. Almazan, “OSPF: CONCEPTO Y MIGRACIÓN DE UNA RED BRIDGE A RED RUTEADA,” Jul. 2018. [Online]. Available: https://mum.mikrotik.com/presentations/HN18/presentation_5623_1532719027.pdf
- [9] ARCOTEL, “ARCOTEL dispone de un Sistema de Atención de Reclamos para atender a la ciudadanía,” Apr. 21, 2021. <https://www.arcotel.gob.ec/atencion-reclamos-denuncias-pedidos-informacion/#:~:text=ATENCI%C3%93N%20DE%20RECLAMOS%2C%20DENUNCIAS%2C%20PEDIDOS%20DE%20INFORMACI%C3%93N,-Definici%C3%B3n%3A&text=Este%20servicio%20se%20lo%20ofrece,llamadas%20al%201800%20567%2D567.>
- [10] C. María Batista Díaz, Z. Lujo Aliaga, L. Victoria Cedeño Galindo, A. Pérez Céspedes, and R. Ernesto Pantaleón Fernández, “Propuesta e implementación de la arquitectura de la red LAN en la empresa ACINOX LAS TUNAS,” *RITI Journal*, vol. 6, 2018.
- [11] G S Santyadiputra, I M E Listartha, and G A J Saskara, “The effectiveness of Automatic Network Administration (ANA) in network automation simulation at Universitas Pendidikan Ganesha,” *J Phys Conf Ser*, 2020, doi: 10.1088/1742-6596/1810/1/012028.







- [12] L. Luis De, Z. Buigas, L. Augusto, and S. Avilés, “Elementos conceptuales básicos útiles para comprender las redes de telecomunicación,” 2002.
- [13] Philippe Dugerdil, “Topologie,” in *Impact des décisions informatiques: introduction à l’informatique pour le décideur non-informaticien*, 2005, pp. 39–41.
- [14] J. Wynekoop, “Local Area Networks,” *Encyclopedia of Information Systems*, pp. 91–102, 2003, doi: 10.1016/B0-12-227240-4/00106-4.
- [15] J. A. Gómez, “Tipos de redes de datos,” in *Redes locales*, Editex, Ed. 2011, pp. 23–24.
- [16] C. J. Trujillo Allauca, “Estudio de los principales medios de transmisión utilizado en redes y comunicaciones,” 2004.
- [17] G. Bora, S. Bora, S. Singh, and M. Arsalan, “OSI Reference Model: An Overview,” *International Journal of Computer Trends and Technology*, vol. 7, no. 4, 2014, [Online]. Available: <http://www.ijcttjournal.org>
- [18] Cisco Systems Inc, “OSI Model and Communication Between Systems,” in *Internetworking Technologies Handbook*, 2004.
- [19] P. Mora Pérez, “Correspondencia entre modelo de referencia para la interconexión de sistemas abiertos (OSI) y la arquitectura TCP/IP,” in *UF1879 - Equipos de interconexión y servicios de red*, Elearning., 2016, pp. 36–38.
- [20] Cisco Systems, “OSI Network Layer OSI Layer 3,” *Network Fundamentals – Chapter 5*, 2007. https://www.uobabylon.edu.iq/eprints/publication_9_22443_27.pdf (accessed Sep. 22, 2022).
- [21] J. S. Wiley, “Interworking,” in *CCNA: Cisco Certified Network Associate Study Guide: Exam 640-802*, 2007.
- [22] K. C. Piñeros Orozco and D. Gonzalo Zuñiga, “Dispositivos de interconexión de redes y medios de transmisión,” 2004.
- [23] R. López Bulla, *Enrutamiento y configuración de redes*. Bogotá, 2018.
- [24] A. Malhotra and S. Kaur, “A comprehensive review on recent advancements in routing protocols for flying ad hoc networks,” *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 3, Mar. 2022, doi: 10.1002/ett.3688.
- [25] CISCO, “Configuring Static Routing,” *Information About Static Routing*, 2022.
- [26] Techopedia, “Dynamic Routing,” *Dynamic Routing*, Sep. 23, 2014.
- [27] F. Boronat Seguí, “Algoritmo de encaminamiento de vector distancias,” 2010, Accessed: Sep. 25, 2022. [Online]. Available: <https://riunet.upv.es:443/handle/10251/7560>

- [28] F. Boronat Segui, “Encaminamiento por estado del enlace,” Apr. 2011, Accessed: Sep. 25, 2022. [Online]. Available: <https://riunet.upv.es:443/handle/10251/10755>
- [29] Craig Sutton, “Technology Trends,” *Is the Extra Layer Better? Layer 2 Versus Layer 3 Networking*, Sep. 11, 2013.
- [30] Ida Nurhaida, Desi Ramayanti, and Imay Nur Islamiyah, “Performance Comparison based on Open Shortest Path First (OSPF) Routing Algorithm for IP Internet Networks,” Sep. 2019. [Online]. Available: www.caeaccess.org
- [31] Lucidchart, “What is a Network Diagram,” *What are your network diagram needs?*, Oct. 02, 2018. <https://www.lucidchart.com/pages/network-diagram> (accessed Jan. 16, 2023).
- [32] saint Leo University, “Sistemas Computacionales: ¿cuáles son las mejores herramientas para el diseño de diagramas de red de computadoras?,” *Las 4 mejores programas para diseñar una red de computadoras*, Jan. 16, 2023.
- [33] L. Marcela, E. Paz, A. García, A. V. Mejía, and A. N. Cadavid, “Método de evaluación y selección de herramientas de simulación de redes,” 2011. [Online]. Available: www.icesi.edu.co/sistemas_telematica
- [34] J. A. Torres, D. Arias Figueroa, and J. Díaz, “Herramientas de Software de Simulación para Redes de Comunicaciones.”
- [35] Slava Gerovitch, “Automation,” Jan. 2003.
- [36] VMWARE, “What is network automation?,” *Network Automation*, 2022. <https://www.vmware.com/topics/glossary/content/network-automation.html> (accessed Oct. 01, 2022).
- [37] Red Hat, “Automatización de red para todos,” 2019.
- [38] Red Hat, “NetOps Meets DevOps The State of Network Automation,” 2018.
- [39] Mikrotik, “Mikrotik,” *Products*. <https://mikrotik.com/products/matrix> (accessed Jan. 19, 2023).
- [40] Abcxperts, “Router,” *RB2011UiAS-RM*, Aug. 19, 2021. <https://abcxperts.com/rb2011uias-rm/> (accessed Jan. 19, 2023).
- [41] Abcxperts, “Routers,” *RB2011UiAS-IN*, Aug. 19, 2021. <https://abcxperts.com/rb2011uias-in/> (accessed Jan. 19, 2023).

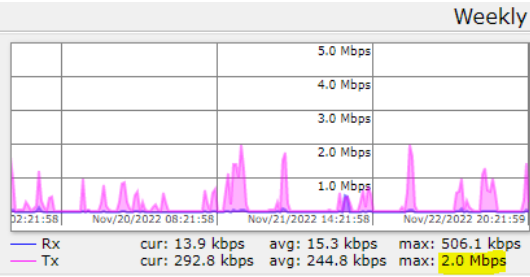
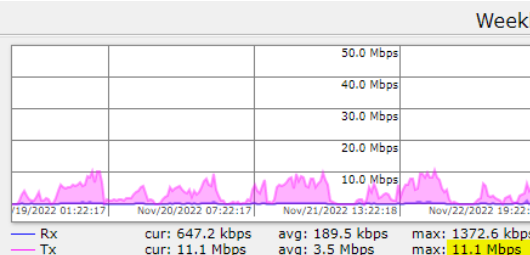
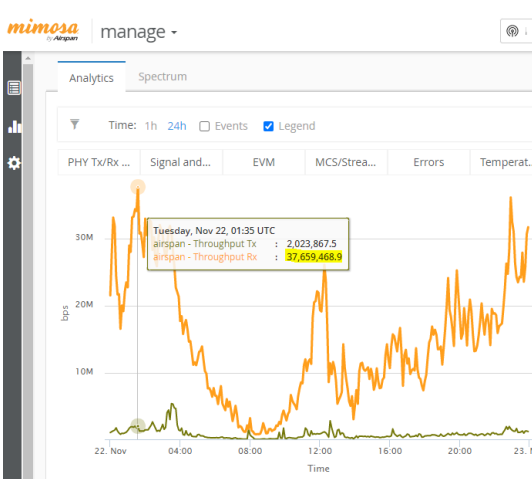
ANEXOS

Anexo 1. Investigación de campo a los diferentes nodos de comunicaciones

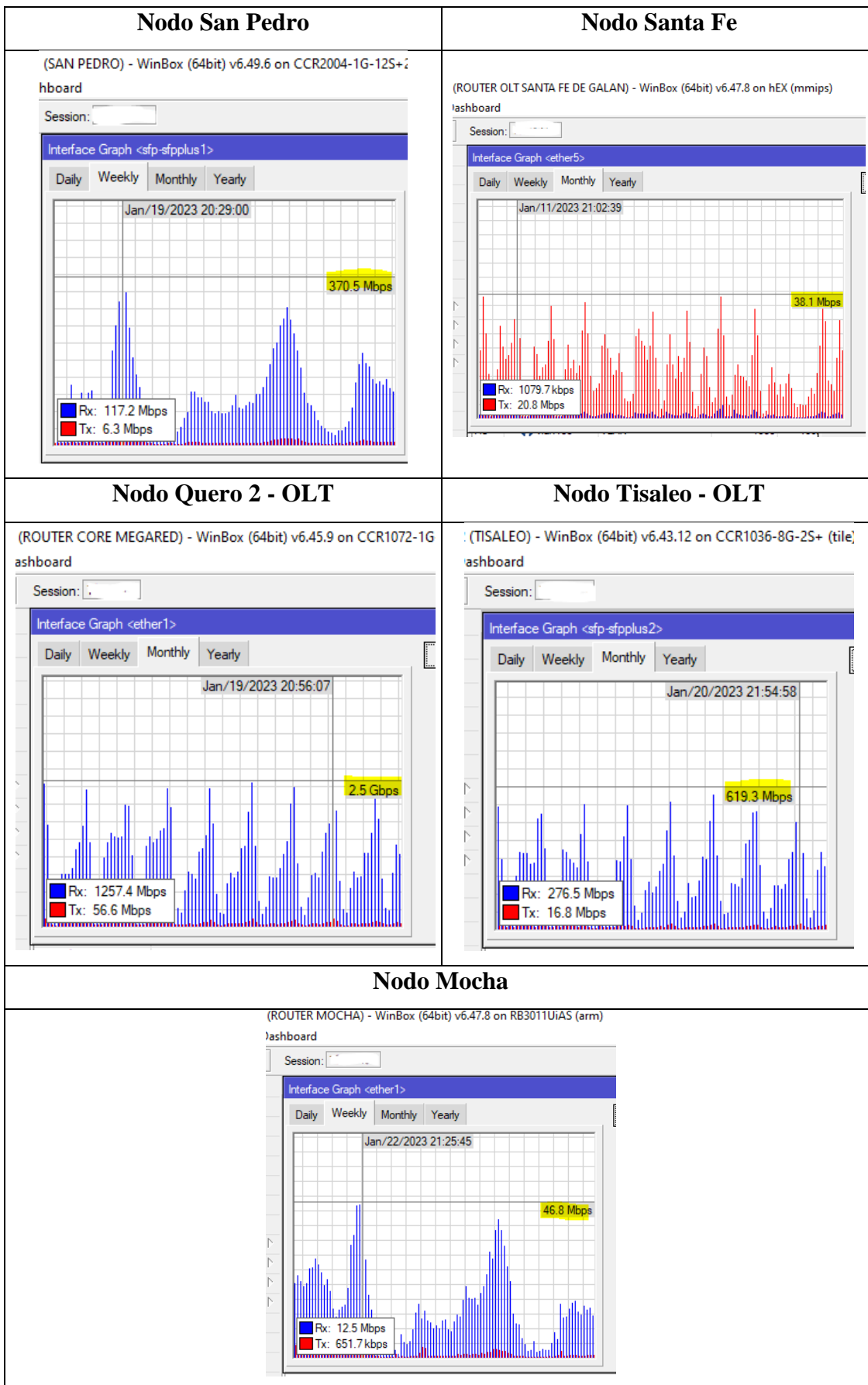
Nodo Quero 1	Nodo Santa Fe de Galán
 A woman with dark hair, wearing a blue and black jacket, is sitting at a desk in a server room. She is looking at a laptop. In the background, there are several racks of server equipment with many yellow and white cables connected to them.	 A woman with long dark hair, wearing a blue and black jacket, is standing outdoors. She is looking at a laptop that is placed on a white surface. Below the laptop, there is a piece of electronic equipment with many yellow cables connected to it. The background shows a stone wall and some foliage.
Nodo Shaushi	Nodo San Francisco
 A server rack is shown with its door open. Inside, there are several pieces of electronic equipment, including what looks like a power supply unit, a network switch, and a server. There are many cables of different colors (white, black, red) connected to the equipment. The rack is outdoors, and a landscape with hills is visible in the background.	 A woman in a blue jacket is standing next to a utility pole. The pole has a satellite dish mounted on it. The background shows a landscape with hills and a cloudy sky. The woman is looking at a notebook or a piece of paper she is holding.

<p align="center">Nodo Quero 2 - Antenas</p>	<p align="center">Nodo Tisaleo</p>
	
<p align="center">Nodo San Vicente de Rumipamba</p>	<p align="center">Nodo Mocha</p>
	
<p align="center">Quero 2 nodo OLT</p>	<p align="center">San Pedro de Sabañag</p>
	

Anexo 2. Verificación de tráfico en nodos de red

Nodo Palahua	Quinual
 <p>Weekly</p> <p>5.0 Mbps 4.0 Mbps 3.0 Mbps 2.0 Mbps 1.0 Mbps</p> <p>02:21:58 Nov/20/2022 08:21:58 Nov/21/2022 14:21:58 Nov/22/2022 20:21:59</p> <p>Rx cur: 13.9 kbps avg: 15.3 kbps max: 506.1 kbps Tx cur: 292.8 kbps avg: 244.8 kbps max: 2.0 Mbps</p>	<p>(CPE-QUINUAL) - WinBox (64bit) v6.49.2 on LHG 5 (mipsbe) board</p> <p>Session: 192.168.</p> <p>Interface Graph <ether1></p> <p>Daily Weekly Monthly Yearly</p> <p>Nov/16/2022 22:04:46</p> <p>4.3 Mbps</p> <p>Rx: 304 bps Tx: 30.6 kbps</p>
Nodo Atillo	Nodo Ambato
<p>(CPE ATILLO) - WinBox (64bit) v6.45.8 on LHG 5 (mipsbe) board</p> <p>Session: 192.168.</p> <p>Interface Graph <ether1></p> <p>Daily Weekly Monthly Yearly</p> <p>Nov/19/2022 22:05:48</p> <p>11.8 Mbps</p> <p>Rx: 623.8 kbps Tx: 8.9 Mbps</p>	<p>(GM-AP-LLIMPE-AMBATO) - WinBox (64bit) v6.45.8 on Lf board</p> <p>Session: 192.168.</p> <p>Interface Graph <ether1></p> <p>Daily Weekly Monthly Yearly</p> <p>Nov/17/2022 22:13:20</p> <p>9.3 Mbps</p> <p>Rx: 8.2 Mbps Tx: 277.4 kbps</p>
Nodo San Francisco	Nodo Niton
 <p>Weekly</p> <p>50.0 Mbps 40.0 Mbps 30.0 Mbps 20.0 Mbps 10.0 Mbps</p> <p>19/2022 01:22:17 Nov/20/2022 07:22:17 Nov/21/2022 13:22:18 Nov/22/2022 19:22:18</p> <p>Rx cur: 647.2 kbps avg: 189.5 kbps max: 1372.6 kbps Tx cur: 11.1 Mbps avg: 3.5 Mbps max: 11.1 Mbps</p>	 <p>mimosa manage -</p> <p>Analytics Spectrum</p> <p>Time: 1h 24h Events Legend</p> <p>PHY Tx/Rx ... Signal and... EVM MCS/Strea... Errors Temperat...</p> <p>30M 20M 10M 0</p> <p>Tuesday, Nov 22, 01:35 UTC airspan - Throughput Tx : 2 023,867.5 airspan - Throughput Rx : 37,659,468.9</p> <p>22. Nov 04:00 08:00 12:00 16:00 20:00 23. Nov</p> <p>Time</p>

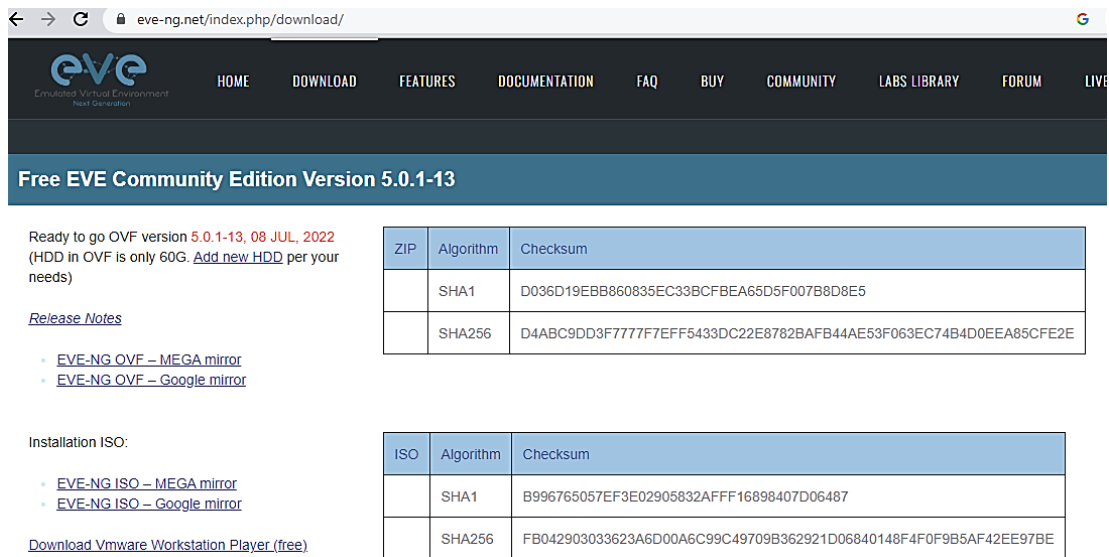
<h3 style="text-align: center;">Nodo Urbina</h3> <p>(ESTACION URBINA) - WinBox (64bit) v6.48.1 on LHG XL HF shboard</p> <p>Session: 192.168.1</p> <p>Interface Graph <ether1></p> <p>Daily Weekly Monthly Yearly</p> <p>Nov/22/2022 19:52:32</p> <p>Rx: 1815.2 kbps Tx: 28.7 Mbps</p> <p>43.0 Mbps</p>	<h3 style="text-align: center;">Nodo La Independencia</h3> <p>(ESTACION LA INDEPENDENCIA) - WinBox (64bit) v6.48.1 on hboard</p> <p>Session: 192.168.1</p> <p>Interface Graph <ether1></p> <p>Daily Weekly Monthly Yearly</p> <p>Rx: 3.6 Mbps Tx: 58.9 Mbps</p> <p>124.2 Mbps</p>
<h3 style="text-align: center;">Nodo San Vicente de Rumipamba</h3> <p>mimosa manage -</p> <p>Time: 1h 24h Events Legend CPE-SAN VIC</p> <p>PHY Tx/... Signal a... EVM MCS/Str... Errors Temper...</p> <p>Tuesday, Nov 22, 01:10 UTC CPE-SAN VICENTE EL MIRADOR - Throughput Tx : 5,691,153.5 CPE-SAN VICENTE EL MIRADOR - Throughput Rx : 114,554,295.8</p> <p>100M 75M 50M 25M bps</p> <p>06:00 12:00 18:00 23. Nov</p> <p>Time</p>	<h3 style="text-align: center;">Nodo Llimpe</h3> <p>(MEGARED-QUERO-LLIMPE-A1) - WinBox (64bit) v6.44.6 on NetMetal 5SHP (mipsb shboard</p> <p>Session: 192.168.1</p> <p>Interface Graph <ether1></p> <p>Daily Weekly Monthly Yearly</p> <p>Nov/11/2022 21:54:03</p> <p>Rx: 6.4 Mbps Tx: 107.1 Mbps</p> <p>172.7 Mbps</p>
<h3 style="text-align: center;">Switch Quero 2</h3>	<h3 style="text-align: center;">Nodo Shaushi</h3>
<p>(MikroTik) - WinBox (64bit) v6.45.9 on CRS326-24G-25+ (a shboard</p> <p>Session: 192.168.1</p> <p>Interface Graph <ether5></p> <p>Daily Weekly Monthly Yearly</p> <p>Nov/16/2022 21:27:34</p> <p>Rx: 11.2 Mbps Tx: 171.8 Mbps</p> <p>232.2 Mbps</p>	<p>(ROUTER SHAUSHI) - WinBox (64bit) v6.49.6 on CCR1016-12G (tile) Dashboard</p> <p>Session:</p> <p>Interface Graph <ether1></p> <p>Daily Weekly Monthly Yearly</p> <p>Jan/18/2023 20:43:08</p> <p>Rx: 114.3 Mbps Tx: 7.3 Mbps</p> <p>307.0 Mbps</p>



Anexo 3. Instalación EVE-NG

Instalación de emulador EVE-NG

El ISO de instalación del software de emulación EVE-NG se encuentra en el sitio oficial y contiene los pasos para su instalación. En esta ocasión se utiliza la versión gratuita “Community”.



The screenshot shows the 'Free EVE Community Edition Version 5.0.1-13' download page. It includes a navigation menu, a header, and two tables of checksums. The first table lists ZIP file checksums for SHA1 and SHA256. The second table lists ISO file checksums for SHA1 and SHA256. There are also links for release notes and mirrors.

Ready to go OVF version **5.0.1-13, 08 JUL, 2022**
(HDD in OVF is only 60G. [Add new HDD](#) per your needs)

[Release Notes](#)

- [EVE-NG OVF – MEGA mirror](#)
- [EVE-NG OVF – Google mirror](#)

ZIP	Algorithm	Checksum
	SHA1	D036D19EBB860835EC33BCFBEA65D5F007B8D8E5
	SHA256	D4ABC9DD3F7777FEFF5433DC22E8782BAFB44AE53F063EC74B4D0EEA85CFE2E

Installation ISO:

- [EVE-NG ISO – MEGA mirror](#)
- [EVE-NG ISO – Google mirror](#)

[Download VMware Workstation Player \(free\)](#)

ISO	Algorithm	Checksum
	SHA1	B996765057EF3E02905832AFF16898407D06487
	SHA256	FB042903033623A6D00A6C99C49709B362921D06840148F4F0F9B5AF42EE97BE

Figura 49. Documentación de EVE-NG

Fuente: <https://www.eve-ng.net/index.php/download/>

EVE-NG posee un entorno virtualizado para lo cual se necesita un software de virtualización para ejecutarlo. En donde, el mismo sitio oficial de EVE-GN recomienda la utilización de VMware Workstation.

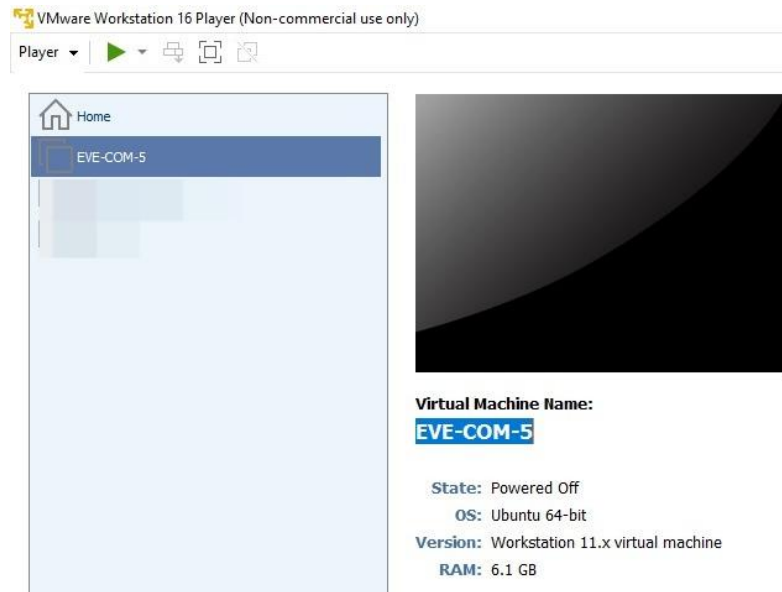


Figura 50. Software de virtualización VMware

Fuente: La Investigadora

Una vez instalada la máquina virtual de EVE-NG, se agregan imágenes de emulación RouterOs, Windows y Linux. Todas las imágenes y su proceso de instalación también se encuentran disponibles en la documentación de EVE-NG. Para la simulación de RouterOs se descarga el archivo VMDK con la última versión estable: 6.49.7

MIKROTIK

Home About Bu

Software Downloads Char

Cloud Hosted Router

	6.48.6 Long-term	6.49.7 Stable
Images	vmdk, vhdx, vdi, ova, img	
Main package		
VHDX image		
VMDK image		

Figura 51. Archivo VMDK para simulación de RouterOs

Fuente: www.mikrotik.com/download

A su vez, para la transferencia de imágenes se utiliza el software FilleZila:

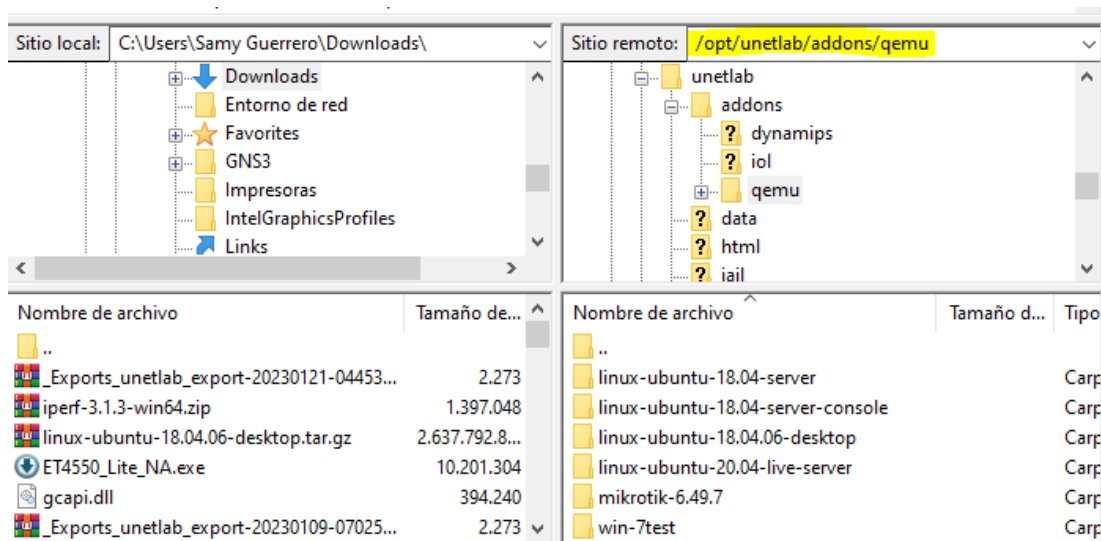


Figura 52. Utilización del Software FileZilla para la transferencia de archivos

Fuente: La Investigadora

Una vez agregadas las ISO de los routers y de máquinas virtuales a utilizar, es necesario conectarse a la maquina EVE-NG mediante navegador con usuario: admin y contraseña: eve, en donde se obtienen la siguiente interfaz gráfica:

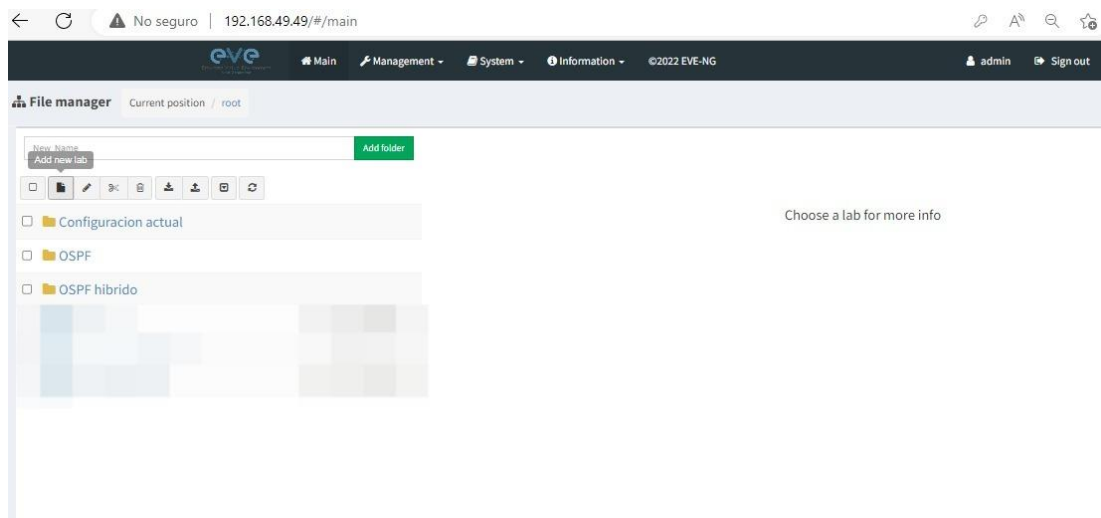


Figura 53. Entorno de emulación EVE-G

Fuente: La Investigadora

También es importante recalcar que, para la configuración de equipos, EVE-NG propone varias alternativas de acceso, como, por ejemplo: telnet, ncp y rdp. En esta ocasión se hará uso de telnet con el programa Putty, así como también de VNC para

la utilización de máquinas virtuales dentro de simulación, y finalmente, la herramienta Winbox que es una interfaz gráfica que permite configurar los equipos con sistema operativo RouterOs.

Ingreso a router mediante Putty

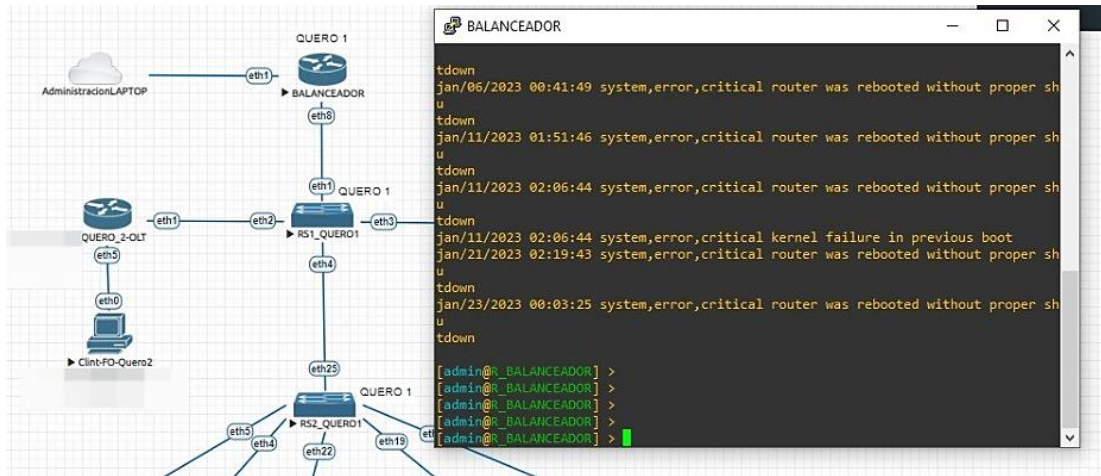


Figura 54. Ingreso a la consola de router mediante la Putty

Fuente: La Investigadora

Ingreso al router mediante Winbox

Para poder ingresar a la topología mediante Winbox es necesario activar la opción RoMON en cada uno de los equipos que cuentan con sistema operativo RouterOs. Para ello es necesario ejecutar el siguiente comando en la consola.

- *tools romon set enabled=yes*

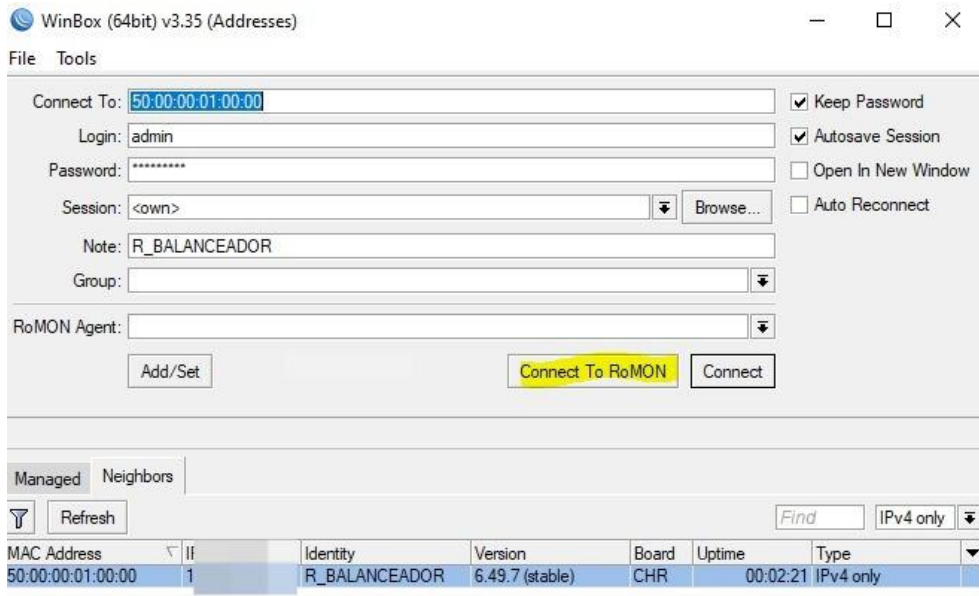


Figura 55. Ingreso a equipos internos de red mediante RoMON

Fuente: La Investigadora

Al seleccionar la opción Connect To RoMON, se enlistará los routers que se encuentran dentro de la red simulada, para poder ingresar a cada uno de ellos. Como se muestra en la siguiente figura:

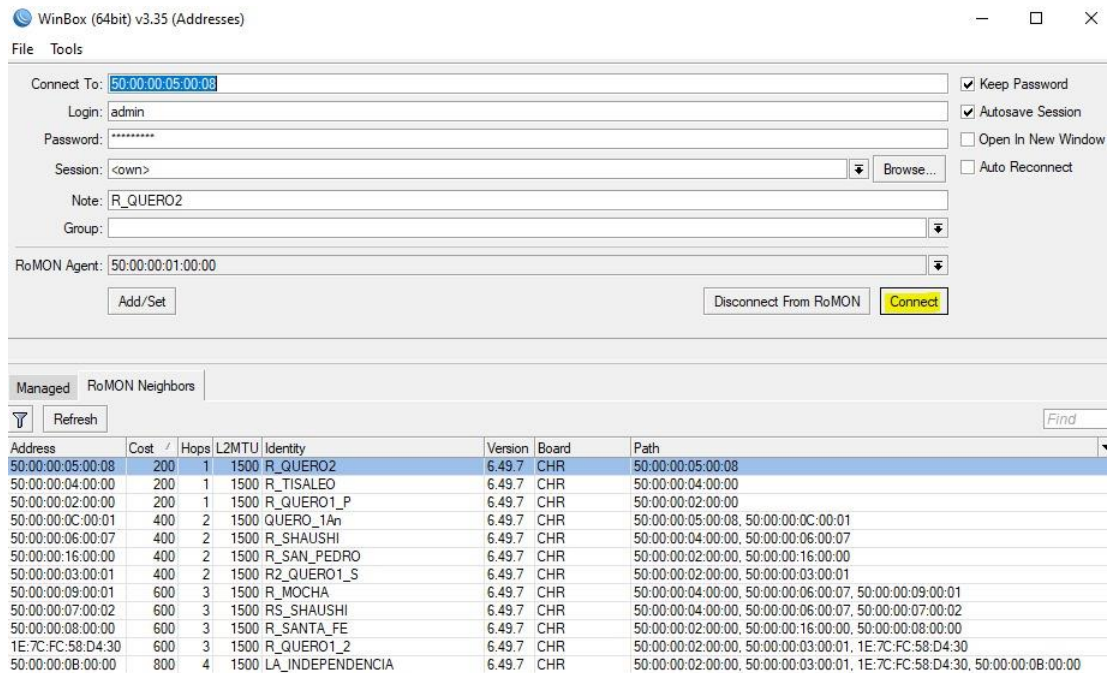


Figura 56. Equipos de red accesibles mediante conexión RoMON

Fuente: La Investigadora

Anexo 4. Tabla de enrutamiento IPv6 por equipo

BALANCEADOR			
Interfaz	Interfaz simulada	Dirección IPv6	Link local
sfp-sfpplus1	ether1	PROVEEDOR	
sfp-sfpplus3	ether3	2001:ab:100:1::1/64	FE80::1
sfp-sfpplus4	ether4	2001:ab:100:2::1/64	FE80::1
sfp-sfpplus8	ether8	2001:ab:100:3::1/64	FE80::1

QUERO 2 - OLT			
Interfaz	Interfaz simulada	Dirección IPv6	Link local
ether1	ether1	2001:ab:100:1::2/64	FE80::2
ether3	ether3	2001:ab:100:5::1/64	FE80::2
<i>ether5</i>	<i>ether5</i>	2001:db8:c0de::1/64	
<i>ether6</i>	<i>ether6</i>	2001:db8:c0de:1::1/64	
<i>ether7</i>	<i>ether7</i>	2001:db8:c0de:2::1/64	
<i>ether8</i>	<i>ether8</i>	2001:db8:c0de:3::1/64	

TISALEO			
Interfaz	Interfaz simulada	Dirección IPv6	Link local
ether1	ether1	2001:ab:100:21::2/64	FE80::3
<i>sfp-sfpplus1</i>	<i>ether9</i>	2001:db8:c0de:4::1/64	
sfp-sfpplus2	ether10	2001:ab:100:2::2/64	FE80::3

QUERO 1 (P)			
Interfaz	Interfaz simulada	Dirección IPv6	Link local
sfp-sfpplus1	ether1	2001:ab:100:3::2/64	FE80::4
sfp-sfpplus4	ether4	2001:ab:100:9::1/64	FE80::4
sfp-sfpplus5	ether5	2001:ab:100:a::1/64	FE80::4
sfp-sfpplus10	ether10	2001:ab:100:b::1/64	FE80::4
sfp-sfpplus12	ether12	2001:ab:100:c::1/64	FE80::4

QUERO 1 (S)			
Interfaz	Interfaz simulada	Dirección IPv6	Link local
ether3	ether3	2001:ab:100:d::1/64	FE80::5
ether4	ether4	2001:ab:100:e::1/64	FE80::5
ether10	ether10	2001:ab:100:f::1/64	FE80::5
sfp-sfpplus1	ether25	2001:ab:100:9::2/64	FE80::5

QUERO 1 (2)			
Interfaz	Interfaz simulada	Dirección IPv6	Link local
sfp-sfpplus1	ether1	2001:ab:100:d::2/64	FE80::6
ether1	ether2	2001:ab:100:12::1/64	FE80::6
<i>ether2</i>	<i>ether3</i>	2001:db8:c0de:5::1/64	

LA INDEPENDENCIA			
Interfaz	Interfaz simulada	Dirección IPv6	Link local
ether1	ether1	2001:ab:100:12::2/64	FE80::7
<i>ether2</i>	<i>ether2</i>	2001:db8:c0de:6::1/64	FE80::7
<i>ether3</i>	<i>ether3</i>	2001:db8:c0de:7::1/64	FE80::7
<i>ether4</i>	<i>ether4</i>	2001:db8:c0de:8::1/64	FE80::7
<i>ether5</i>	<i>ether5</i>	2001:db8:c0de:9::1/64	

QUERO 2 - Antenas			
Interfaz	Interfaz simulada	Dirección IPv6	Link local
sfp-sfpplus1	ether1	2001:ab:100:a::2/64	FE80::8
<i>ether1</i>	<i>ether2</i>	2001:db8:c0de:a::1/64	
<i>ether2</i>	<i>ether3</i>	2001:db8:c0de:b::1/64	
<i>ether3</i>	<i>ether4</i>	2001:db8:c0de:c::1/64	
sfp-sfpplus2	ether10	2001:ab:100:5::2/64	FE80::8

MOCHA			
Interfaz	Interfaz simulada	Dirección IPv6	Link local
sfp-sfpplus1	ether1	2001:ab:100:e::2/64	FE80::9
ether5	ether5	2001:ab:100:1c::1/64	FE80::9
<i>ether4</i>	<i>ether4</i>	2001:db8:c0de:d::1/64	

SAN PEDRO			
Interfaz	Interfaz simulada	Dirección IPv6	Link local
sfp-sfpplus1	ether1	2001:ab:100:b::2/64	FE80::10
sfp-sfpplus10	ether10	2001:ab:100:1e::1/64	FE80::10
sfp-sfpplus12	ether12	2001:ab:100:1f::1/64	FE80::10
<i>sfp-sfpplus1</i>	<i>ether2</i>	2001:db8:c0de:e::1/64	

SHAUSHI			
Interfaz	Interfaz simulada	Dirección IPv6	Link local
ether1	ether1	2001:ab:100:c::2/64	FE80::11
ether3	ether3	2001:ab:100:21::1/64	FE80::11
ether4	ether4	2001:ab:100:f::2/64	FE80::11
ether5	ether5	2001:ab:100:1e::2/64	FE80::11
ether6	ether6	2001:ab:100:1c::2/64	FE80::11
<i>ether7</i>	<i>ether7</i>	2001:db8:c0de:f::1/64	
<i>ether8</i>	<i>ether8</i>	2001:db8:c0de:10::1/64	
<i>ether12</i>	<i>ether12</i>	2001:db8:c0de:11::1/64	

SANTA FE DE GALAN			
Interfaz	Interfaz simulada	Dirección IPv6	Link local
ether1	ether1	2001:ab:100:1f::2/64	FE80::12
<i>ether5</i>	<i>ether5</i>	2001:db8:c0de:12::1/64	

Anexo 5. Código de programación de enrutamiento dinámico OSPF en ruta propuesta

BALANCEADOR

```

/interface bridge
add disabled=yes name=bridge1
add name=loopback
/interface ethernet
set [ find default-name=ether1 ] loop-protect=on
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing ospf instance
set [ find default=yes ] distribute-default=always-as-type-1 router-id=\
0.0.0.1
/ip address
add address=172.16.2.1/24 comment=\
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1
/ip route

```

```

add distance=1 dst-address=172.16.0.0/20 gateway=192.168.14.215
add distance=1 dst-address=172.16.200.0/22 gateway=192.168.13.210
add distance=1 dst-address=192.168.50.0/23 gateway=192.168.13.209

/routing ospf network
add area=backbone network=10.255.0.16/30
add area=backbone network=10.255.0.20/30
add area=backbone network=10.255.0.48/30

/system identity
set name=R_BALANCEADOR

/tool graphing interface
add

/tool romon
set enabled=yes

```

R_QUERO2

```

/interface bridge
add name=loopback

/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik

/routing ospf instance
set [ find default=yes ] router-id=0.0.0.5

/ip address
add address=192.168.13.210/24 comment=WAN disabled=yes interface=ether1 \
    network=192.168.13.0
add address=172.16.200.1/22 comment=ONU interface=ether5 network=172.16.200.0
add address=172.16.24.1/22 comment=BRIDGE interface=ether5 network=\
    172.16.24.0
add address=0.0.0.5 comment=OSPF interface=loopback network=0.0.0.5
add address=10.255.0.22/30 interface=ether1 network=10.255.0.20
add address=10.255.0.53/30 interface=ether3 network=10.255.0.52

/ip dhcp-client
add disabled=no interface=ether1

/ip route
add disabled=yes distance=1 gateway=192.168.13.1

```

```

/routing ospf interface
add interface=ether5 passive=yes
add cost=15 interface=ether3

/routing ospf network
add area=backbone network=10.255.0.20/30
add area=backbone network=172.16.200.0/22
add area=backbone network=172.16.24.0/22
add area=backbone network=10.255.0.52/30

/system identity
set name=R_QUERO2

/tool romon
set enabled=yes

```

TISALEO

```

/interface bridge
add disabled=yes name="WAN BRIDGE"
add name=loopback

/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik

/routing ospf instance
set [ find default=yes ] router-id=0.0.0.4

/interface bridge port
add bridge="WAN BRIDGE" interface=ether10

/ip address
add address=192.168.14.215/24 interface=ether10 network=192.168.14.0
add address=172.16.0.1/20 comment=\
----- \
interface=ether9 network=172.16.0.0
add address=0.0.0.4 comment=OSPF interface=loopback network=0.0.0.4
add address=10.255.0.18/30 interface=ether10 network=10.255.0.16
add address=10.255.1.9/29 interface=ether1 network=10.255.1.8

/ip dhcp-client
add disabled=no interface=ether1

/ip route

```

```

add disabled=yes distance=1 gateway=192.168.14.1
/routing ospf interface
add interface=ether9 passive=yes
add cost=30 interface=ether1
/routing ospf network
add area=backbone network=10.255.0.16/30
add area=backbone network=172.16.0.0/20
add area=backbone network=10.255.1.8/29
/system identity
set name=R_TISALEO
/tool romon
set enabled=yes

```

QUERO1_P

```

/interface bridge
add disabled=yes name=bridge1
add name=loopback
/interface ethernet
set [ find default-name=ether1 ] comment=WAN
set [ find default-name=ether4 ] comment="Hacia SW"
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing ospf instance
set [ find default=yes ] router-id=0.0.0.2
/ip address
add address=192.168.14.4/24 comment=\
----- \
interface=bridge1 network=192.168.14.0
add address=0.0.0.2 comment=OSPF interface=loopback network=0.0.0.2
add address=10.255.0.50/30 interface=ether1 network=10.255.0.48
add address=10.255.0.29/30 interface=ether5 network=10.255.0.28
add address=10.255.0.33/30 interface=ether10 network=10.255.0.32
add address=10.255.0.25/30 interface=ether4 network=10.255.0.24

```

```

add address=10.255.0.41/30 interface=ether12 network=10.255.0.40
/ip dhcp-client
add disabled=no interface=ether1
/ip route
add disabled=yes distance=1 gateway=192.168.14.1
/routing ospf network
add area=backbone network=10.255.0.24/30
add area=backbone network=10.255.0.28/30
add area=backbone network=10.255.0.32/30
add area=backbone network=10.255.0.40/30
add area=backbone network=10.255.0.48/30
/system identity
set name=R_QUERO1_P
/tool romon
set enabled=yes

```

QUERO_1An

```

/interface bridge
add disabled=yes name=bridge1
add name=loopback
/interface vlan
add interface=ether3 name=vlan505 vlan-id=505
add interface=ether2 name=vlan540 vlan-id=540
add interface=ether3 name=vlan560 vlan-id=560
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing ospf instance
set [ find default=yes ] router-id=0.0.0.6
/ip address
add address=0.0.0.6 comment=OSPF interface=loopback network=0.0.0.6
add address=10.255.0.30/30 interface=ether1 network=10.255.0.28
add address=172.16.104.1/26 interface=vlan540 network=172.16.104.0
add address=172.16.101.1/24 interface=vlan505 network=172.16.101.0

```

```

add address=172.16.104.161/28 interface=vlan560 network=172.16.104.160
add address=10.255.0.54/30 comment=Backup interface=ether10 network=\
    10.255.0.52
/ip dhcp-client
add disabled=no interface=ether1
/ip route
add disabled=yes distance=1 gateway=192.168.14.1
/routing ospf interface
add interface=vlan505 passive=yes
add interface=vlan540 passive=yes
add interface=vlan560 passive=yes
add cost=15 interface=ether10
/routing ospf network
add area=backbone network=172.16.101.0/24
add area=backbone network=172.16.104.0/26
add area=backbone network=172.16.104.160/28
add area=backbone network=10.255.0.28/30
add area=backbone network=10.255.0.52/30
/system identity
set name=QUERO_1An
/tool graphing interface
add
/tool romon
set enabled=yes

```

SAN PEDRO

```

/interface bridge
add disabled=yes name=bridge1
add name=loopback
/interface vlan
add interface=ether2 name=vlan510 vlan-id=510
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing ospf instance

```



```

set [ find default=yes ] router-id=0.0.0.8
/ip address
add address=172.16.2.1/23 interface=ether3 network=172.16.2.0
add address=0.0.0.8 comment=OSPF interface=loopback network=0.0.0.8
add address=10.255.0.34/30 interface=ether1 network=10.255.0.32
add address=172.16.102.1/25 interface=vlan510 network=172.16.102.0
add address=10.255.0.9/29 interface=ether12 network=10.255.0.8
add address=10.255.1.17/29 interface=ether10 network=10.255.1.16
/ip dhcp-client
add disabled=no interface=ether1
/ip route
add disabled=yes distance=1 gateway=192.168.14.1
/routing ospf interface
add interface=vlan510 passive=yes
add interface=ether3 passive=yes
add cost=15 interface=ether10
add interface=ether12
/routing ospf network
add area=backbone network=10.255.0.32/30
add area=backbone network=172.16.2.0/23
add area=backbone network=172.16.102.0/25
add area=backbone network=10.255.0.8/29
add area=backbone network=10.255.1.16/29
/system identity
set name=R_SAN_PEDRO
/tool romon
set enabled=yes

```

R2_QUERO_S

```

/interface bridge
add disabled=yes name=bridge1
add name=loopback
/interface wireless security-profiles

```

```

set [ find default=yes ] supplicant-identity=MikroTik
/routing ospf instance
set [ find default=yes ] router-id=0.0.0.3
/ip address
add address=0.0.0.3 comment=OSPF interface=loopback network=0.0.0.3
add address=10.255.0.26/30 interface=ether25 network=10.255.0.24
add address=10.255.0.37/30 interface=ether4 network=10.255.0.36
add address=10.255.0.45/30 interface=ether3 network=10.255.0.44
add address=10.255.1.1/29 interface=ether10 network=10.255.1.0
/ip dhcp-client
add disabled=no interface=ether1
/ip route
add disabled=yes distance=1 gateway=192.168.14.1
/routing ospf interface
add cost=15 interface=ether10
add interface=ether3 priority=0
/routing ospf network
add area=backbone network=10.255.0.24/30
add area=backbone network=10.255.0.36/30
add area=backbone network=10.255.0.44/30
add area=backbone network=10.255.1.0/29
/system identity
set name=R2_QUERO1_S
/tool romon

```

R_SANTA_FE

```

/interface bridge
add disabled=yes name=bridge1
add name=loopback
/interface vlan
add interface=ether1 name=vlan1 vlan-id=1
add interface=ether3 name=vlan530 vlan-id=530
/interface wireless security-profiles

```

```

set [ find default=yes ] supplicant-identity=MikroTik
/routing ospf instance
set [ find default=yes ] router-id=0.0.0.11
/ip address
add address=192.168.13.209/24 disabled=yes interface=ether1 network=\
    192.168.13.0
add address=192.168.50.1/23 interface=ether5 network=192.168.50.0
add address=0.0.0.11 comment=OSPF interface=loopback network=0.0.0.11
add address=172.16.103.129/26 interface=vlan530 network=172.16.103.128
add address=10.255.0.10/29 interface=ether1 network=10.255.0.8
/ip dhcp-client
add disabled=no interface=ether1
/ip route
add disabled=yes distance=1 gateway=192.168.13.1
/routing ospf interface
add interface=vlan530 passive=yes
add interface=ether3 passive=yes
add interface=ether5 passive=yes
add interface=ether1
/routing ospf network
add area=backbone network=192.168.50.0/23
add area=backbone network=172.16.103.128/26
add area=backbone network=10.255.0.8/29
/system identity
set name=R_SANTA_FE
/tool romon
set enabled=yes

```

R_QUERO1_2

```

/interface bridge
add disabled=yes name=bridge1
add name=bridge2_clientes-antenas
add name=loopback

```

```

/interface vlan
add interface=bridge2_clientes-antenas name=vlan550 vlan-id=550
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing ospf instance
set [ find default=yes ] router-id=0.0.0.10
/ip address
add address=0.0.0.10 comment=OSPF interface=loopback network=0.0.0.10
add address=10.255.0.1/29 interface=ether2 network=10.255.0.0
add address=172.16.104.129/28 interface=vlan550 network=172.16.104.128
add address=10.255.0.46/30 interface=ether1 network=10.255.0.44
/ip dhcp-client
add disabled=no interface=ether1
/ip route
add disabled=yes distance=1 gateway=192.168.14.1
/routing ospf interface
add interface=vlan550 passive=yes
/routing ospf network
add area=backbone network=10.255.0.0/29
add area=backbone network=10.255.0.44/30
add area=backbone network=172.16.104.128/28
/system identity
set name=R_QUERO1_2
/tool romon
set enabled=yes

```

R_MOCHA

```

/interface bridge
add disabled=yes name=bridge1
add name=loopback
/interface vlan
add interface=ether2 name=vlan535 vlan-id=535
/interface wireless security-profiles

```

```

set [ find default=yes ] supplicant-identity=MikroTik
/routing ospf instance
set [ find default=yes ] router-id=0.0.0.7
/ip address
add address=0.0.0.7 comment=OSPF interface=loopback network=0.0.0.7
add address=10.255.0.38/30 interface=ether1 network=10.255.0.36
add address=172.16.103.193/26 interface=vlan535 network=172.16.103.192
add address=10.255.1.25/29 interface=ether5 network=10.255.1.24
/ip dhcp-client
add disabled=no interface=ether1
/ip route
add disabled=yes distance=1 gateway=192.168.14.1
/routing ospf interface
add interface=vlan535 passive=yes
add cost=15 interface=ether5
/routing ospf network
add area=backbone network=10.255.0.36/30
add area=backbone network=172.16.103.192/26
add area=backbone network=10.255.1.24/29
/system identity
set name=R_MOCHA
/tool romon
set enabled=yes

```

LA_INDEPENDENCIA

```

/interface bridge
add disabled=yes name=bridge1
add name=loopback
/interface vlan
add interface=ether5 name=vlan520-LaIndependencia vlan-id=520
add interface=ether4 name=vlan525-Urbina vlan-id=525
add interface=ether3 name=vlan565-Atillo vlan-id=565
add interface=ether2 name=vlan570-Palahua vlan-id=570

```

```

add interface=ether4 name=vlan575-Quinual vlan-id=575
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
/routing ospf instance
set [ find default=yes ] router-id=0.0.0.12
/ip address
add address=0.0.0.12 comment=OSPF interface=loopback network=0.0.0.12
add address=10.255.0.2/29 interface=ether1 network=10.255.0.0
add address=172.16.104.185/29 interface=vlan570-Palahua network=\
    172.16.104.184
add address=172.16.104.177/29 interface=vlan565-Atillo network=172.16.104.176
add address=172.16.104.193/29 interface=vlan575-Quinual network=\
    172.16.104.192
add address=172.16.103.65/26 interface=vlan525-Urbina network=172.16.103.64
add address=172.16.103.1/26 interface=vlan520-LaIndependencia network=\
    172.16.103.0
/ip dhcp-client
add disabled=no interface=ether1
/ip route
add disabled=yes distance=1 gateway=192.168.14.1
/routing ospf interface
add interface=vlan520-LaIndependencia passive=yes
add interface=vlan525-Urbina passive=yes
add interface=vlan565-Atillo passive=yes
add interface=vlan570-Palahua passive=yes
add interface=vlan575-Quinual passive=yes
/routing ospf network
add area=backbone network=10.255.0.0/29
add area=backbone network=172.16.103.0/26
add area=backbone network=172.16.104.176/29
add area=backbone network=172.16.103.64/26
add area=backbone network=172.16.104.184/29
add area=backbone network=172.16.104.192/29

```

```
/system identity
set name=LA_INDEPENDENCIA

/tool romon
set enabled=yes
```

R_SHAUSHI

```
/interface bridge
add disabled=yes name=bridge1
add name=loopback

/interface vlan
add interface=ether7 name=vlan500-Shaushi vlan-id=500
add interface=ether12 name=vlan515-Rumipamba vlan-id=515
add interface=ether8 name=vlan555-SanFrancisco vlan-id=555

/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik

/routing ospf instance
set [ find default=yes ] router-id=0.0.0.9

/ip address
add address=0.0.0.9 comment=OSPF interface=loopback network=0.0.0.9
add address=10.255.0.42/30 interface=ether1 network=10.255.0.40
add address=172.16.102.129/25 interface=vlan515-Rumipamba network=\
    172.16.102.128
add address=172.16.104.145/28 interface=vlan555-SanFrancisco network=\
    172.16.104.144
add address=172.16.100.1/24 interface=vlan500-Shaushi network=172.16.100.0
add address=10.255.1.10/29 interface=ether3 network=10.255.1.8
add address=10.255.1.2/29 interface=ether4 network=10.255.1.0
add address=10.255.1.18/29 interface=ether5 network=10.255.1.16
add address=10.255.1.26/29 interface=ether6 network=10.255.1.24

/ip dhcp-client
add disabled=no interface=ether1

/ip route
add disabled=yes distance=1 gateway=192.168.14.1
```

```
/routing ospf interface
add interface=vlan500-Shaushi passive=yes
add interface=vlan515-Rumipamba passive=yes
add interface=vlan555-SanFrancisco passive=yes
add cost=30 interface=ether3
add cost=15 interface=ether4
add cost=15 interface=ether5
add cost=15 interface=ether6

/routing ospf network
add area=backbone network=10.255.0.40/30
add area=backbone network=172.16.100.0/24
add area=backbone network=172.16.104.144/28
add area=backbone network=172.16.102.128/25
add area=backbone network=10.255.1.24/29
add area=backbone network=10.255.1.16/29
add area=backbone network=10.255.1.0/29
add area=backbone network=10.255.1.8/29

/system identity
set name=R_SHAUSHI

/tool romon
set enabled=yes
```

RS_SHAUSHI

```
/interface bridge
add name=bridge1

/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik

/interface bridge port
add bridge=bridge1 interface=ether9
add bridge=bridge1 interface=ether19

/ip address
add address=192.168.14.3/24 interface=bridge1 network=192.168.14.0

/ip dhcp-client
```



```
add disabled=no interface=ether1
/ip route
add distance=1 gateway=192.168.14.1
/system identity
set name=RS_SHAUSHI
/tool romon
set enabled=yes
```

Anexo 6. Programación de archivos .json y .py

config.json

```
{
  "config_id": {
    "router_ip": "192.168.1.67",
    "user": "admin",
    "password": "*****"
  },
  "ip_address": {
    "interface": {
      "ether3": [
        "10.255.0.21/30",
        "10.255.0.20"
      ],
      "ether8": [
        "10.255.0.49/30",
        "10.255.0.48"
      ],
      "ether4": [
        "10.255.0.17/30",
        "10.255.0.16"
      ],
      "loopback": [
        "0.0.0.1/32",
```

```

        "0.0.0.0"
    ]
}
},
"interfaces": {
    "loopback": [
        "0.0.0.1/32",
        "Bridge"
    ]
},
"protocols": {
    "protocol": "ospf",
    "area_id": "0.0.0.0",
    "areas": [
        "10.255.0.16/30",
        "10.255.0.20/30",
        "10.255.0.48/30",
        "10.255.0.12/30"
    ],
    "instances": "0.0.0.1",
    "interfaces": [
        "ether3",
        "ether4",
        "ether8",
    ]
}
}
}

```

Script.py

```

import json
import requests
import routers_api
from routers_api import RouterOsApiPool

```

```

# Archivo JSON con la configuración de OSPF
config_file = 'config.json'
with open(config_file) as json_file:
    config_data = json.load(json_file)

# Dirección IP y credenciales del dispositivo Mikrotik
ip_address = config_data["config_id"]["router_ip"]
userid=config_data["config_id"]["user"]
passwd=config_data["config_id"]["password"]

api_pool = RouterOsApiPool(ip_address, username=userid,password=passwd,
plaintext_login=True)
api = api_pool.get_api()

tinterfaces = api.get_resource('/interface/bridge/')
ip_address = api.get_resource('/ip/address/')
p_ospf = api.get_resource('/routing/ospf/network/')

for key1 in (config_data["interfaces"]):
    ip=config_data["interfaces"][key1][0]
    type_interface = config_data["interfaces"][key1][1]
    print(key1 + " " + ip+ " " + type_interface)
    lista = tinterfaces.get()
    # print(lista)
    for lista2 in lista:
        print((lista2["name"]) + " " + key1)
        if key1 in lista2["name"]:
            print((tinterfaces.get(name=key1)[0]['id']))
            tinterfaces.remove(id=(tinterfaces.get(name=key1)[0]['id']))

params = {'type': type_interface}
tinterfaces.add(name=key1)

```

```
# Configuración de direcciones ip en las interfaces
for key1 in (config_data["ip_address"]["interface"]):
    ip=config_data["ip_address"]["interface"][key1][0]
    netw = config_data["ip_address"]["interface"][key1][1]
    lista = ip_address.get()
    for lista2 in lista:
        if key1 in lista2["interface"]:
            ip_address.remove(id=(ip_address.get(interface=key1)[0]['id']))
    params = {'address': ip}
    ip_address.add(interface=key1, **params)

api_pool.disconnect()
```