



FACULTAD DE CIENCIA Y TECNOLOGÍA

ESCUELA DE INGENIERÍA ELECTRÓNICA

Implementación de un programa para la virtualización de una red basada en equipos MikroTik para el laboratorio de redes de la Universidad del Azuay.

**Trabajo de graduación previo a la obtención del título de:
INGENIERO ELECTRÓNICO**

Autores:

**CUEVA MÉNDEZ HENRY RAÚL
POZO NEIRA FERNANDO ESTEBAN**

Director:

DANIEL ESTEBAN ITURRALDE PIEDRA

CUENCA, ECUADOR

2016

Dedicatoria

Este trabajo va dedicado
a toda mi familia,
por guiarme y apoyarme
a lo largo de mi vida.

Henry Cueva

Dedicatoria

A mi familia,
por su comprensión y
apoyo incondicional,
a mis amigos
por su ayuda y
sus sabios consejos.

Fernando Pozo

Agradecimientos

A nuestros profesores por haber guiado nuestra formación académica con sus enseñanzas y sus aportes. De manera especial, agradecemos a quienes nos han permitido culminar este trabajo, a nuestro director de tesis, Ing. Daniel Iturralde, por su paciencia y orientación, y a Geovanny por su colaboración.

ÍNDICE DE CONTENIDOS

DEDICATORIA	ii
AGRADECIMIENTOS	iv
ÍNDICE DE CONTENIDOS	v
ÍNDICE DE FIGURAS.....	ix
ÍNDICE DE TABLAS	xii
RESUMEN.....	xiii
ABSTRACT.....	xiii
INTRODUCCIÓN	1
CAPÍTULO 1: GENERALIDADES	2
1.1. Descripción del problema.....	2
1.2. Alcances y limitaciones	4
1.3. Hipótesis.....	5
1.4. Metodología utilizada.....	6
1.5. Organización del trabajo	6
CAPÍTULO 2: ESTADO DEL ARTE.....	8
2.1. Conceptos preliminares	8
2.1.1. Red de computadoras	8
2.1.2. Simulación	9
2.1.3. Virtualización.....	9
2.1.4. Virtualización de red.....	10
2.2. Herramientas para virtualización y simulación de redes.....	10
2.2.1. GNS3.....	11
2.2.2. VNUML.....	13
2.2.3. VNX.....	14
2.2.4. Packet Tracer.....	15
2.2.5. PRTG	16
2.2.6. Resumen comparativo.....	17

CAPÍTULO 3: SITUACIÓN ACTUAL	19
3.1. Distribución de la red	19
3.1.1. Esquema de la red	19
3.1.2. Configuración actual	20
3.1.3. Resumen de direccionamiento	22
3.2. Equipos utilizados	23
3.2.1. Capa de núcleo: <i>router</i> RB2011UiAS-RM	23
3.2.2. Capa de distribución: <i>router</i> hEX lite	25
3.2.3. Capa de acceso: <i>switch</i> RB260GSP	27
CAPÍTULO 4: IMPLEMENTACIÓN DEL PROGRAMA DE VIRTUALIZACIÓN.....	29
4.1. Requisitos de instalación	29
4.1.1. Java.....	29
4.1.2. Librerías de Java	30
4.1.2.1. Apache Commons Net.....	30
4.1.2.2. MySQL Connector/J.....	31
4.1.3. Xampp.....	31
4.2. Explicación del programa.....	32
4.2.1. Diagramas de flujo	32
4.2.2. Funcionamiento general	35
4.3. Estructura del programa	35
4.3.1. Ventana de inicio.....	35
4.3.2. Ventana principal	36
4.3.3. Elementos de red.....	38
4.3.3.1. Nodos.....	38
4.3.3.2. Crear Enlaces.....	39
4.3.3.3. Routers.....	39
a. Interfaces	41
b. Direccionamiento estático	42
c. Direccionamiento dinámico.....	43
d. VLANs	44
e. Servidor DHCP.....	44

f. Cliente DHCP	45
g. NAT	46
4.3.3.4. Switch	47
4.3.3.5. Access point	48
4.3.3.6. Computador	49
4.3.4. Eliminar	50
4.3.4.1. Eliminar un nodo	50
4.3.4.2. Eliminar un enlace	51
4.3.4.3. Eliminar un proyecto	51
4.3.5. Comunicación: terminal Telnet	51
4.3.6. Acerca de	53
4.3.7. Opciones	54
4.3.7.1. Ayuda	54
4.3.7.2. Salir	54
4.4. Comandos MikroTik	54
4.4.1. Interfaces	54
4.4.2. Ping	55
4.4.3. Enrutamiento estático	55
4.4.4. VLANs	55
4.4.5. Enrutamiento dinámico OSPF	56
4.4.6. Cliente DHCP	56
4.4.7. Servidor DHCP	57
4.4.8. NAT	58
CAPÍTULO 5: RESULTADOS	59
5.1. Planteamiento de la red	59
5.2. Diseño de la red	62
5.3. Configuraciones en los equipos	67
5.3.1. Capa de acceso	69
5.3.2. Capa de distribución	72
5.3.3. Capa de núcleo	82
5.4. Pruebas de comunicación	87

CONCLUSIONES	90
RECOMENDACIONES	91
BIBLIOGRAFÍA	93

ÍNDICE DE FIGURAS

Figura 1.1. Universidades que usan <i>software</i> para la virtualización de redes.....	4
Figura 2.1. Logo del programa GNS3.....	11
Figura 2.2. Ventana principal del programa GNS3.....	12
Figura 2.3. Virtual Network User Mode Linux (VNUML).	13
Figura 2.4. Virtual Networks over Linux (VNX).	14
Figura 2.5. Logo de Cisco Packet Tracer.....	15
Figura 2.6. Cisco Packet Tracer.	16
Figura 2.7. PRTG Network Monitor.	16
Figura 3.1. Esquema de red del laboratorio de redes de la Universidad del Azuay...	20
Figura 3.2. Diagrama de direcciones IP de la red actual.....	21
Figura 3.3. Distribución de VLANs de la red actual.....	21
Figura 3.4. <i>Router</i> RB2011UiAS-RM.	24
Figura 3.5. Esquema interno del <i>router</i> RB2011UiAS-RM.	25
Figura 3.6. <i>Router</i> hEX lite.	26
Figura 3.7. <i>Switch</i> RB260GSP.	27
Figura 3.8. MikroTik SwOS.	28
Figura 4.1. Selección de servicios en la instalación de Xampp.	32
Figura 4.2. Diagrama de flujo de la interfaz gráfica de ENDS.	33
Figura 4.3. Diagrama de flujo para establecer la comunicación con un equipo del laboratorio.	34
Figura 4.4. Ventana de inicio de ENDS.	36
Figura 4.5. Ventana principal de ENDS.....	36
Figura 4.6. Opciones del panel de equipo de la ventana principal.....	37
Figura 4.7. Ventana “ <i>Nodos de Red</i> ”.	38
Figura 4.8. Creación de un enlace entre dos nodos.....	39
Figura 4.9. Ventana “ <i>Router</i> ”.....	40
Figura 4.10. Ventana “ <i>Interfaces</i> ”.	42
Figura 4.11. Interfaz de la ventana “ <i>Dir. Estático</i> ”.....	42
Figura 4.12. Interfaz de la ventana “ <i>OSPF</i> ”.....	43
Figura 4.13. Interfaz de la ventana “ <i>VLANs</i> ”.....	44
Figura 4.14. Ventana “ <i>Servidor DHCP</i> ”.....	45
Figura 4.15. Ventana “ <i>Cliente DHCP</i> ”.....	46
Figura 4.16. Ventana “ <i>NAT</i> ”.....	46

Figura 4.17. Ventana “Switch”.....	48
Figura 4.18. Ventana “Access Point”.....	49
Figura 4.19. Ventana “PC”.....	50
Figura 4.20. Eliminación de un nodo.....	50
Figura 4.21. Ventana “Eliminar Enlaces”.....	51
Figura 4.22. Confirmación para eliminar un proyecto.....	51
Figura 4.23. Terminal Telnet.....	53
Figura 4.24. Ventana “Acerca De”.....	53
Figura 4.25. Confirmación de salida.....	54
Figura 5.1. Diseño de la red.....	61
Figura 5.2. Redes locales virtuales de la red.....	61
Figura 5.3. Selección del equipo a agregar a la interfaz.....	62
Figura 5.4. Nombramiento del nodo de red.....	62
Figura 5.5. Ingreso de nuevo elemento en la base de datos.....	63
Figura 5.6. Creación de un nuevo nodo.....	63
Figura 5.7. Adición de <i>routers</i> en el área de trabajo.....	64
Figura 5.8. Ingreso de un nodo tipo <i>switch</i>	64
Figura 5.9. Ingreso de un nodo tipo PC.....	64
Figura 5.10. Distribución de los nodos de la red en el área de trabajo.....	65
Figura 5.11. Selección del botón <i>Crear Enlaces</i>	65
Figura 5.12. Creación de un enlace entre dos nodos.....	66
Figura 5.13. Visualización del enlace creado.....	66
Figura 5.14. Diseño final de la red.....	67
Figura 5.15. Propiedades de conexión de área local de Windows 7.....	68
Figura 5.16. Cambio de dirección IP.....	68
Figura 5.17. Ingreso a la configuración del <i>switch</i>	69
Figura 5.18. Autenticación de ingreso de un usuario.....	69
Figura 5.19. Creación de VLANs en MikroTik SwOS.....	70
Figura 5.20. Configuración de parámetros en cada puerto.....	70
Figura 5.21. Cambio de dirección IP del Switch 1.....	71
Figura 5.22. Actualización del campo IP del Switch 1.....	71
Figura 5.23. Cambio de dirección IP del “switch 2”.....	72
Figura 5.24. Actualización del campo IP del “switch 2”.....	72
Figura 5.25. Mensaje de configuración de fábrica del <i>router</i>	73
Figura 5.26. Modificación de parámetros de una interfaz.....	74

Figura 5.27. Visualización de la lista de interfaces Ethernet del router.....	74
Figura 5.28. Adición de VLANs a las interfaces físicas del equipo.	75
Figura 5.29. Listado de VLANs del “router 1”.....	75
Figura 5.30. Configuración de <i>gateway</i> para cada VLAN.....	76
Figura 5.31. Presentación de <i>gateway</i> configurado para cada interfaz.	76
Figura 5.32. Redes para los servidores DHCP.	77
Figura 5.33. Rangos de direcciones dinámicas para DHCP.	78
Figura 5.34. Creación de servidores DHCP.	78
Figura 5.35. Configuración de servidores DHCP para cada subred.	79
Figura 5.36. Designación de la puerta de salida de todas las subredes.....	79
Figura 5.37. Tabla de enrutamiento del “router 1”.	80
Figura 5.38. Eliminación de reglas en las tablas de los servidores DHCP.	80
Figura 5.39. Eliminación del cliente DHCP.....	81
Figura 5.40. Borrado de la dirección 192.168.88.1 predefinida por configuración de fábrica.....	81
Figura 5.41. Actualización de dirección IP del “router 1”.....	81
Figura 5.42. Mensaje de configuración de fábrica del “router core”.....	82
Figura 5.43. Cambio de nombre y estado de las interfaces.....	83
Figura 5.44. Redes virtuales locales del “router core”.....	83
Figura 5.45. Eliminación de parámetros en el apartado cliente DHCP.	84
Figura 5.46. Establecimiento de un cliente DHCP.	84
Figura 5.47. Configuración de NAT.	85
Figura 5.48. Visualización de un NAT tipo masquerade.	85
Figura 5.49. Eliminación de reglas en la ventana Servidor DHCP.....	86
Figura 5.50. Tabla de direcciones de red de las interfaces del “router core”.....	86
Figura 5.51. Tabla de enrutamiento del “router core”.	86
Figura 5.52. Tabla de enrutamiento del “router core”.	87
Figura 5.53. Resumen de los nodos de red del proyecto.....	87
Figura 5.54. Comprobación de funcionamiento de la red.	88
Figura 5.55. Comunicación entre las capas de núcleo y distribución.	88
Figura 5.56. Comunicación entre las capas de núcleo y acceso.....	89

ÍNDICE DE TABLAS

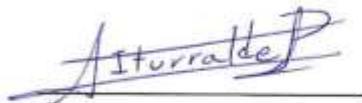
Tabla 1.1. Encuesta realizada a estudiantes sobre los programas VNUML Y GNS3.	3
Tabla 2.1. Herramientas para virtualización de redes de comunicación.....	17
Tabla 3.2. Rangos de direccionamiento estático y dinámico de cada subred.	23
Tabla 3.3. Características del <i>router</i> RB2011UiAS-RM.	24
Tabla 3.4: Características del <i>router</i> hEX lite.....	26
Tabla 3.5: Características del <i>switch</i> RB260GSP	28
Tabla 4.1. Comandos para la configuración de interfaces de equipos MikroTik.	54
Tabla 4.2. Comando para realizar un ping en equipos MikroTik.	55
Tabla 4.3. Comandos para enrutamiento estático en equipos MikroTik.....	55
Tabla 4.4. Comandos para crear VLANs en equipos MikroTik.	55
Tabla 4.5. Comandos para enrutamiento dinámico OSPF en equipos MikroTik.	56
Tabla 4.6. Comandos para habilitar un cliente DHCP en equipos MikroTik.	56
Tabla 4.7. Comandos para configurar un servidor DHCP en equipos MikroTik.	57
Tabla 4.8. Comandos para configurar un NAT en equipos MikroTik.	58
Tabla 5.1. Tabla de direccionamiento de la red.	60
Tabla 5.2. Rangos de direccionamiento fijo y dinámico de cada subred.	60

**“IMPLEMENTACIÓN DE UN PROGRAMA PARA LA VIRTUALIZACIÓN
DE UNA RED BASADA EN EQUIPOS MIKROTIK PARA EL
LABORATORIO DE REDES DE LA UNIVERSIDAD DEL AZUAY”**

RESUMEN

Considerando que es de vital importancia la familiarización con la aplicación real de conocimientos al configurar, administrar y gestionar los equipos de una red de comunicaciones, el presente trabajo de graduación describe el diseño, desarrollo e implementación de un programa de código abierto, denominado ENDS (Easy Network Designer Software), que permite realizar la virtualización de la red y la configuración remota de parámetros básicos de los equipos MikroTik del laboratorio de redes de la Universidad del Azuay mediante una interfaz gráfica. El software fue elaborado con lenguaje de programación Java en el entorno NetBeans y hace uso de una base de datos MySQL en donde se guardan los proyectos creados. El programa fue probado mediante una red relativamente compleja y los resultados mostrados fueron satisfactorios.

Palabras claves: Virtualización, Redes de Comunicación, Java, MikroTik.



Daniel Esteban Iturralde Piedra

Director de Titulación

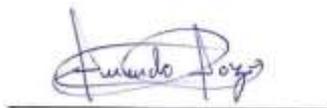


Hugo Marcelo Torres Salamea

Director de Escuela



Cueva Méndez Henry Raúl



Pozo Neira Fernando Esteban

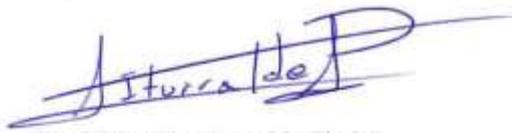
Autores

**“IMPLEMENTATION OF A PROGRAM FOR NETWORK
VIRTUALIZATION TECHNOLOGY BASED ON MIKROTIK EQUIPMENT
FOR THE NETWORKS SERVICE SYSTEMS LABORATORY AT
UNIVERSIDAD DEL AZUAY”**

ABSTRACT

This graduation work discusses the design, development and implementation of an open source program, called ENDS (Easy Network Designer Software), because it is of vital importance to become familiar with the application of knowledge in order to configure, administer and manage the computers on a communications network; which will allow to perform network virtualization and remote configuration of MikroTik equipment basic parameters through a graphical interface at the network laboratory of *Universidad del Azuay*. The software was developed with Java programming language in NetBeans environment, and it uses MySQL database where the projects created are saved. The program was tested by a relatively complex network, and the results shown were satisfactory.

Keywords: Virtualization, Communications Networks, Java, MikroTik.



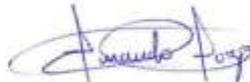
Daniel Esteban Iturralde Piedra
Thesis Director



Hugo Marcelo Torres Salamea
School Director



Cueva Méndez Henry Raúl



Pozo Neira Fernando Esteban

Authors



UNIVERSIDAD DEL
AZUAY
Dpto. Idiomas



Translated by,
Lic. Lourdes Crespo

Cueva Méndez Henry Raúl
Pozo Neira Fernando Esteban
Trabajo de Graduación
Daniel Iturralde, Mst.
Marzo 2016

**IMPLEMENTACIÓN DE UN PROGRAMA PARA LA VIRTUALIZACIÓN
DE UNA RED BASADA EN EQUIPOS MIKROTIK PARA EL
LABORATORIO DE REDES DE LA UNIVERSIDAD DEL AZUAY.**

INTRODUCCIÓN

En la Universidad del Azuay la enseñanza de la materia de redes de comunicación está enfocada mayormente en la parte teórica pues las prácticas son limitadas y, considerando que es de vital importancia la familiarización con la aplicación real de conocimientos al configurar, administrar y gestionar los equipos de una red, se ve necesario incluir un programa que facilite su estudio de una forma más interactiva y transparente.

La adquisición de un programa especializado de virtualización implicaría recursos económicos por gastos en versiones del software y, además, capacitación por parte de la empresa proveedora a los docentes de la universidad.

Por esta razón, el siguiente trabajo describe el diseño, desarrollo e implementación de un programa de código abierto realizado en lenguaje Java que permite realizar la virtualización de la red y la configuración remota de parámetros básicos de los equipos Mikrotik del laboratorio mediante una interfaz gráfica.

CAPÍTULO 1

GENERALIDADES

1.1. Descripción del problema

En la actualidad las redes de comunicaciones ya sea para instituciones, empresas o pequeños negocios, son de vital importancia, razón por la cual los estudiantes deben prepararse tanto en la parte teórica como en la práctica. En la Universidad del Azuay la falta de un laboratorio de redes y de un software orientado a la enseñanza de la materia dificulta el aprendizaje de los estudiantes ya que sus conocimientos son enfocados más en la teoría de redes, descuidando así la aplicación práctica de los conocimientos.

Para la universidad, la obtención de un software especializado que funcione de acuerdo al laboratorio de redes representaría la adquisición de licencias costosas, capacitación de los docentes y actualizaciones de versiones y librerías por parte de la empresa contratada para el mantenimiento; además, el laboratorio se vería limitado a trabajar con equipos y software de un solo proveedor, sin tener oportunidad a futuras mejoras en la compra de equipos y en la adecuación del programa a las necesidades que se presenten.

Además, la complejidad de la configuración de equipos debido a la gran cantidad de comandos es muy notoria, y no existe un software que permita su configuración, menos aún que lo haga de una forma interactiva y transparente facilitando la comprensión de lo que los estudiantes están realizando.

Aunque en el mercado actual existen varios programas destinados al diseño de redes de comunicaciones, todos presentan trabas que dificultan la aplicación en tareas específicas, por ejemplo: su costo, la compatibilidad con diferentes marcas, su facilidad de uso y sobre todo el permiso para modificar su código fuente y adaptarlo en diferentes entornos.

Siendo un aspecto importante en la virtualización de redes, la facilidad de manejar y entender el programa, sobre su robustez y funciones, se han realizado en la Universidad de Murcia, encuestas a estudiantes donde se indica de manera resumida qué es lo que piensan sobre un programa con muchas funciones pero sin interfaz gráfica (VNUML), versus un *software* desarrollado para presentar al usuario una pantalla que con simple intuición permite trabajar en un proyecto (GNS3).

Tabla 1.1. Encuesta realizada a estudiantes sobre los programas VNUML Y GNS3.

Cuestión	VNUML	GNS3
No he dedicado tiempo a solventar problemas de la herramienta	2,22 (1,22)	3,50 (1,20)
La información disponible es adecuada y de gran utilidad	3,17 (1,20)	3,50 (0,92)
Es fácil de instalar y configurar	2,50 (1,34)	4,11 (1,32)
Es fácil de usar	2,61 (1,46)	4,67 (0,97)
La configuración del escenario de red es sencilla	2,44 (1,50)	4,44 (0,92)
Muestra alta fiabilidad durante la virtualización del escenario	2,63 (1,50)	3,39 (1,24)
Es eficiente incluso con topologías complejas	2,00 (1,14)	3,78 (1,31)

Fuente: (Pereñíguez-García, Ruiz, Ros, Marín, & Ruiz, 2012).

Dicha encuesta consta de 20 afirmaciones que el alumno valora en una escala del 1 al 5, siendo 5 la máxima satisfacción. La mayoría de estudiantes encuestados considera que las herramientas de virtualización son muy útiles para afianzar los conceptos teóricos de las asignaturas, así como para desarrollar las destrezas necesarias para la configuración y gestión de redes de comunicaciones en la práctica. La satisfacción media en este punto es muy elevada (4.61), al tiempo que existe un gran consenso (desviación típica de 0.77). Sólo existe un caso en el que la evaluación del alumno es menor de 4 puntos (Pereñíguez-García, Ruiz, Ros, Marín, & Ruiz, 2012).

Varias universidades han realizado investigaciones y estudios en virtualización de redes para sus campus y sus laboratorios. Las pioneras, y que incluso imparten cursos y seminarios sobre ello, son las universidades de Standford en California, la Universidad de la Ciudad de Londres y la Universidad de Lancaster. Éstas últimas utilizan equipos HP y Cisco respectivamente, situación que implica el uso de *software* privado. (Scroxton, Lancaster University supports SDN development with HP Networking, 2014) (Scroxton, City University London moves towards SDN with Avaya Fabric Connect, 2015)



Figura 1.1. Universidades que usan *software* para la virtualización de redes.

1.2. Alcances y limitaciones

En este proyecto se crea un *software* capaz de diseñar una red de comunicaciones de manera gráfica y que permita además la configuración de los equipos de una red existente.

El programa a desarrollarse deberá ser capaz de configurar equipos de la marca MikroTik, instalados en el Laboratorio de Redes de la Universidad del Azuay, de forma interactiva al hacer uso de una ventana gráfica.

Las funciones de configuración de equipos que podrá hacer nuestro programa incluyen opciones básicas como lo son cambios de usuario y contraseñas, direccionamiento IP, enrutamiento estático y dinámico, creación de VLANs, agregar reglas en el firmware, y la posibilidad de hacer ping entre equipos con el fin de comprobar la conexión de los mismos. Para todas las opciones se hará uso de la ventana gráfica que muestre los campos principales a fin de que, para el usuario, la configuración del equipo sea transparente. Todo esto se llevará a cabo mediante conexiones remotas a través del protocolo TCP.

El proyecto será de código abierto, desarrollado en lenguaje Java, por lo que servirá de punto de partida para futuros trabajos de investigación, ya que al permitir su modificación, tanto como para mejorar su rendimiento o para ampliar la compatibilidad con distintas marcas, los estudiantes tendrán que aplicar los conocimientos adquiridos en Java a lo largo de la carrera.

1.3. Hipótesis

En la actualidad existe una gran variedad de *software* que permite realizar diseños de redes y simulación de equipos, tanto de forma gráfica como texto plano, los mismos que están disponibles de forma gratuita o poseen algún costo. Muchos de los programas combinan estas funciones, pero no existe el *software* que diseñe una red y que sea capaz de configurar los equipos físicos de la misma en tiempo real, menos aún que lo haga de una manera transparente para el usuario.

Para elaborar topologías que muestren la distribución de dispositivos en una red es necesario contar con una interfaz gráfica y controles fáciles de usar, esto permitiría que sea sencillo de captar para cualquier usuario.

Para facilitar la configuración de equipos de una red, se programará algoritmos que permitan establecer conexiones remotas y, de acuerdo a parámetros ingresados por el usuario, se ejecuten comandos preestablecidos que realicen los cambios de manera transparente, es decir, sin la necesidad de tener el conocimiento de los comandos usados por MikroTik.

1.4. Metodología utilizada

Inicialmente se utilizará un método bibliográfico al revisar documentos que nos permitan conocer los conceptos teóricos sobre las redes de computadoras, los equipos que emplean, su configuración y protocolos de comunicación. También se hará una breve explicación sobre el lenguaje de programación utilizado, las librerías adicionales necesarias y su funcionalidad. De igual manera, se documentará los programas de virtualización de redes existentes en el mercado, destacando sus características principales y las limitaciones que puedan presentar.

Para el diseño y explicación del funcionamiento del programa se usará metodología descriptiva con el objeto de indicar, mediante diagramas de bloques y de flujo, las partes que compondrán el *software* y las actividades específicas que llevarán a cabo. Se realizará también un esquema representativo que abarque los aspectos generales y que sintetice la labor del programa.

En cuanto se refiere al desarrollo del programa como tal, con la misma metodología citada para la explicación de su funcionamiento, se procederá a la elaboración del código de programación del entorno de trabajo de la aplicación y de la administración y gestión de los equipos de la red.

Una vez desarrollado el *software* se deberá emplear una metodología experimental y un trabajo de laboratorio donde se compruebe el funcionamiento adecuado del programa en cuanto al diseño de la red, comunicación con los equipos y su configuración de forma remota.

En último término, haciendo uso de una metodología exploratoria, se llevará a cabo la evaluación del proyecto, se detectarán fallas y errores, prosiguiendo con su respectiva corrección.

1.5. Organización del trabajo

El proyecto está dividido en 5 capítulos que abarcan tanto conceptos teóricos fundamentales para entender el trabajo realizado como el análisis de la situación actual del laboratorio y la implementación del programa en el mismo.

El capítulo primero trata sobre la problemática y la motivación que lleva a los autores a realizar un programa de virtualización de redes; los alcances y limitaciones que tiene el programa; y, la metodología utilizada en el desarrollo del proyecto.

El segundo capítulo constituye el estado del arte, es decir, se presenta un análisis breve de algunos de los programas más conocidos para la virtualización de redes. Se hace énfasis principalmente en sus características más importantes y en lo que son capaces de realizar, además se destacan sus usos más comunes. Se mencionan también varias universidades que los han implementado en sus laboratorios, virtuales y físicos, y los resultados que han obtenido con sus estudiantes.

El capítulo tercero trata sobre la situación actual del laboratorio de redes de la Universidad del Azuay y su distribución. Se listan los equipos de la marca MikroTik que están instalados, enrutadores y *switches*, las conexiones llevadas a cabo y la topología de red existente.

En el cuarto capítulo se elabora la implementación del programa de virtualización de redes para el laboratorio. Se realizan esquemas y diagramas sobre la estructura del programa y se mencionan las librerías utilizadas para la programación tanto de la ventana gráfica de usuario como para la comunicación con los equipos. Además, se muestran los comandos para la configuración de parámetros básicos para los equipos MikroTik.

Por último, en el capítulo quinto, se verifica el código de la aplicación y su correcto funcionamiento, se presentan los resultados obtenidos en la implementación del programa y se desarrolla una guía básica sobre el uso de la herramienta.

CAPÍTULO 2

ESTADO DEL ARTE

Para poder comprender el desempeño del *software*, es necesario tener bien definido conceptos claves como redes de computadores y virtualización. Dichas definiciones servirán como punto de partida para aclarar lo que la virtualización de redes es y lo que representa; y, de esta manera, diferenciarla del enfoque de la simulación.

Además, con la finalidad de conocer los programas existentes de virtualización de redes, se debe analizar las características primordiales de cada uno de ellos, enfocándose en sus capacidades y en sus limitaciones. Los programas que se listan en el presente capítulo son tanto de licencia gratuita como de licencia pagada y, dentro de sus aplicaciones más comunes, se destaca su uso en laboratorios educativos.

2.1. Conceptos preliminares

2.1.1. Red de computadoras

Red de computadoras es el conjunto de equipos autónomos, capaces de intercambiar información o recursos mediante un medio físico, como cable de par trenzado, cable coaxial o fibra óptica; o medio inalámbrico, como *Wi-Fi*, enlace satelital, entre otros (Newman, 2010).

Los componentes que forman una red son: los nodos de red, correspondientes a cada máquina o servidor; los medios de comunicación, es decir, por donde se dará el intercambio de datos; y, los protocolos, que son las reglas para que dos o más entidades se comuniquen (Alvarado, 2011).

Los equipos de conectividad son los dispositivos que permiten transformar y conducir la información en el funcionamiento de una red de computadores, estos pueden ser: pasivos, ya que no producen amplificación, por ejemplo elementos de conectividad para fibra óptica; o activos, como es el caso de tarjetas PCI (Interconexión de Componentes Periféricos), concentradores, puntos de acceso, módems, enrutadores, *switches* (Garg, 2010).

2.1.2. Simulación

La simulación es una técnica que abarca una extensa colección de métodos y aplicaciones cuyo objetivo es imitar el comportamiento real de un sistema, usualmente se trabaja en un computador digital con *software* apropiado (Vargas Avilés, 2015). La simulación permite que se apliquen diferentes soluciones ante un problema, y así comprobar cuál dio un mejor resultado, sin el riesgo que haya consecuencias reales (Moreno Parra, 2012).

2.1.3. Virtualización

“La virtualización es una técnica que permite encapsular una unidad de proceso para su ejecución dentro de un entorno que emula el entorno real de forma transparente” (Galán, Fernández, Fuertes, Gómez, & de Vergara, 2009). Es decir es la puesta en funcionamiento de recursos de una computadora como máquina virtual en otra máquina física. Ello lleva a la inclusión de dos términos, la “máquina huésped” que se refiere a la máquina virtual, y la “máquina anfitriona” que es la máquina física en donde se lleva a cabo la virtualización (Martín, Marrero, Urbano, Barra, & Moreiro, 2011).

2.1.4. Virtualización de red

“La virtualización de redes es la combinación de los recursos de red del hardware con los recursos de red del *software* en una única unidad administrativa.” (Panchana, y otros, 2011). La virtualización de una red consiste en “unir en una red virtual varios elementos de red heterogéneos, ya sean hardware o *software*, conectados a distintas redes y dispersos topológicamente.” (Martín, Marrero, Urbano, Barra, & Moreiro, 2011). De esta manera, los múltiples elementos de red, tales como: computadoras, impresoras, servidores, enrutadores, etc., de diferentes redes, ubicados en diferentes puntos geográficos, se agrupan formando una sola red virtual (Martín, Marrero, Urbano, Barra, & Moreiro, 2011).

2.2. Herramientas para virtualización y simulación de redes

En la actualidad existen herramientas orientadas a la virtualización de escenarios de redes, tales como VNUML, VNX, NSX, o Ryu; y otras destinadas a la simulación, como son GNS3, Packet Tracer, CADE, PRTG o Dynamips; además de programas de empresas privadas que permiten la visualización topológica y la configuración de sus dispositivos instalados en una red (Ruiz, Marín, Pereñíguez-García, Ruiz, & Gómez, 2010).

Dentro de esta variedad de programas para el diseño de redes podemos encontrar los de licencia gratuita (VNUML, GNS3, CADE,) y los de licencia pagada (PRTG, Packet Tracer).

2.2.1. GNS3



Figura 2.1. Logo del programa GNS3.

Fuente: (Díaz, 2010)

GNS3 (*Graphical Network Simulator*), cuyo logo se muestra en la figura 2.1, es un *software* que permite simular redes de manera gráfica y que emplea como motor de ejecución Dynamips. Este a su vez es una plataforma que emula el entorno de ejecución de equipos Cisco, esto quiere decir que ejecuta el sistema operativo IOS de los dispositivos. Por lo tanto, GNS3 es capaz de emular tanto enrutadores como otros dispositivos: *switches*, PCs, *hubs*, etc., que se basen en el firmware de Cisco (Ruiz, Fernández, Galán, & Bellido, 2008).

La ventana principal del programa, como se puede observar en la figura 2.2, está conformada por cuatro áreas principales: Dispositivos disponibles, Área de construcción de topología, Consola de Dynagen, y Resumen de la topología. Esta interfaz permite el diseño gráfico de la red de una forma dinámica y fácil de realizar.

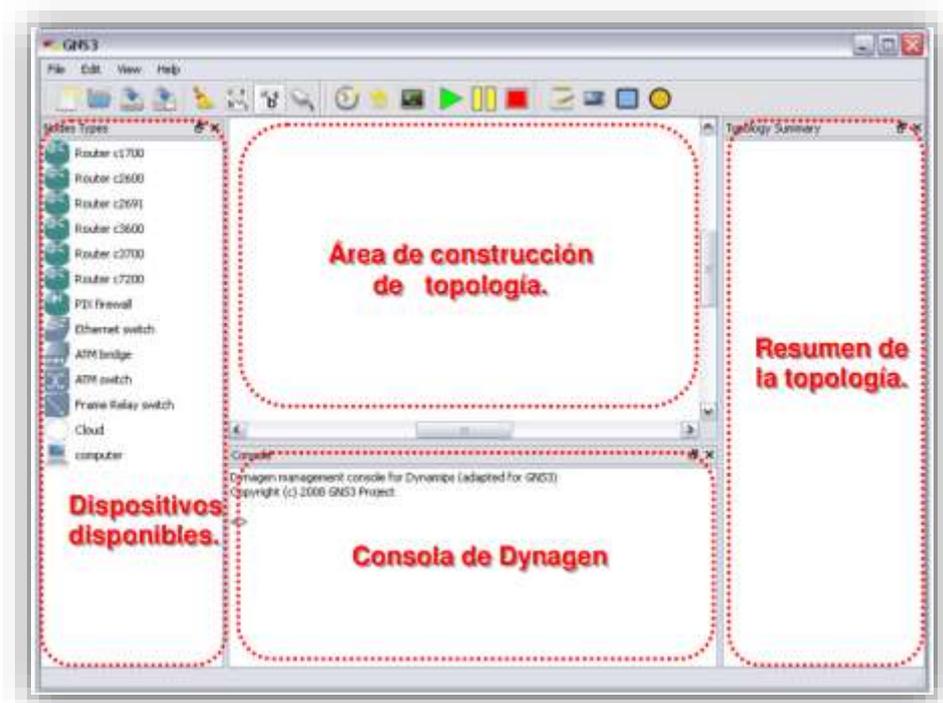


Figura 2.2. Ventana principal del programa GNS3.

Fuente: (Díaz, 2010)

Debido a que GNS3 es un *software* libre y que su entorno es altamente interactivo, ha sido implementado como herramienta para el estudio de redes en varias universidades de todo el mundo. Entre las más importantes destacan la Universidad de Murcia, la Universidad de Alicante y la Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona en España; la Universidad de Costa Rica, y la Universidad Católica Santiago de Guayaquil en Ecuador.

2.2.2. VNUML



Figura 2.3. Virtual Network User Mode Linux (VNUML).
Fuente: (Universidad Politécnica de Madrid, 2012)

VNUML (véase Figura 2.3) son las siglas de *Virtual Network User Mode Linux*, y es un programa basado en UML (*User Mode Linux*). UML es un *software* de virtualización que permite la ejecución de máquinas virtuales en una diferente máquina anfitrión, todas ellas de sistema operativo Linux (Ruiz, Fernández, Galán, & Bellido, 2008).

Por su parte, VNUML automatiza la construcción y gestión de escenarios virtuales, y está compuesta por dos partes principales: el lenguaje VNUML para describir simulaciones (basado en XML), y el intérprete de dicho lenguaje en línea de comandos, que ejecuta el escenario de forma automática (Ruiz, Fernández, Galán, & Bellido, 2008) (Pereñíguez-García, Ruiz, Ros, Marín, & Ruiz, 2012).

VNUML fue desarrollado por el Departamento de Ingeniería de Sistemas Telemáticos (DIT) de la Universidad Politécnica de Madrid (UPM) en España, siendo utilizada ampliamente en la Universidad de Koblenz-Landau (Alemania).

En la actualidad el desarrollo y mantenimiento de VNUML se ha abandonado en favor de la nueva versión de la herramienta que se llama VNX.

2.2.3. VNX

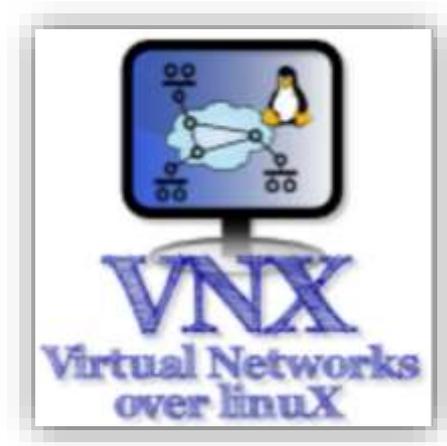


Figura 2.4. Virtual Networks over Linux (VNX).
Fuente: (Universidad Politécnica de Madrid, 2015)

VNX (*Virtual Networks over Linux*) está basado en VNUML e incorpora importantes funcionalidades que superan las limitaciones de la herramienta VNUML (véase Figura 2.4) (Fernández, 2014).

Los aspectos mejorados incluidos en VNX son:

- La integración de las nuevas plataformas de virtualización que permiten la ejecución de máquinas virtuales que utilizan otros sistemas operativos (Windows, FreeBSD, etc.) además de Linux.
- La incorporación de las plataformas de virtualización Dynamips y Olive que permiten la emulación de equipos Cisco y Juniper.
- Implementación de funciones de autoconfiguración y ejecución de comandos para varios sistemas operativos.
- Integración del *switch* virtual Openvswitch con soporte para conexiones de configuración de VLAN, inter-interruptores y la configuración de parámetros SDN (controlador de la dirección IP, el modo, la versión OpenFlow, etc.) (Fernández, 2014).

2.2.4. Packet Tracer



Figura 2.5. Logo de Cisco Packet Tracer.

Fuente: (Netacad, 2015)

Packet Tracer (véase Figura 2.5) es un programa de simulación de redes desarrollado por la empresa Cisco. Es altamente utilizado en la Networking Academy, academia de la misma marca que facilita la enseñanza y el aprendizaje de redes (Netacad, 2015).

Packet Tracer permite experimentar con el comportamiento de la red y ofrece simulación, visualización, creación, y evaluación de redes, facilitando así la enseñanza y el aprendizaje de conceptos tecnológicos complejos (Netacad, 2015).

El programa se encuentra disponible de forma gratuita para los instructores de Networking Academy, estudiantes, ex alumnos y administradores que están registrados en Netspace. Sin embargo no es un *software* libre ya que no se puede acceder a su código de programación. Además, existen dos versiones del programa, una versión completa desarrollada para los instructores, y una, con algunas limitaciones, para los estudiantes (Netacad, 2015).

Aunque en sus inicios solamente fué pensado como un simulador de redes, desde la versión 5.3.3, es posible utilizar el programa en un entorno real utilizando una aplicación externa llamada PTBridge desarrollada en lenguaje Java (Packet-Tracer-Network, 2015).

La ventana principal de Cisco Packet Tracer se puede apreciar en la figura 2.6.

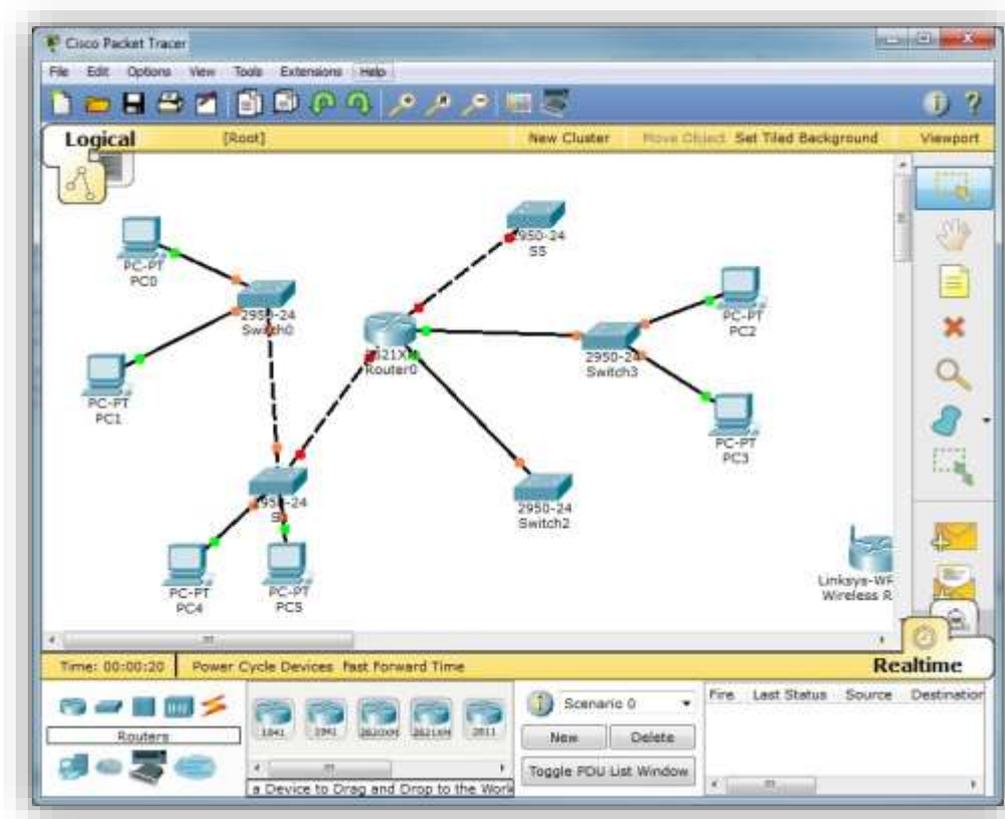


Figura 2.6. Cisco Packet Tracer.
Fuente: (Netacad, 2015).

2.2.5. PRTG



Figura 2.7. PRTG Network Monitor.
Fuente: (Paessler, 2015)

PRTG (véase Figura 2.7) es un *software* creado por la compañía Paessler AG. Es ideal para monitorizar una red de cualquier tamaño, la cual puede ser creada de manera sencilla por su interfaz intuitiva y fácil de usar. Posee abundantes animaciones y gráficos que permiten obtener un vistazo rápido y detallado de los elementos que conforman la red y del tráfico que cursa por ellos.

PRTG asegura la disponibilidad y mide el tráfico y el uso de los componentes de red. Reduce costos evitando interrupciones, optimizando las conexiones, la carga y la calidad.

En base a todas las características que PRTG presenta, el costo para obtenerlo es alto, debido a que está dedicado para grandes empresas. Asimismo, se trata de un *software* comercial, por lo que la modificación de su código fuente es restringida. (Paessler, 2015).

2.2.6. Resumen comparativo

Existen varios programas destinados al diseño de redes de comunicaciones, en la Tabla 2.1 observamos los más conocidos en la actualidad con sus principales características, beneficios y limitaciones.

Tabla 2.1. Herramientas para virtualización de redes de comunicación.

Herramienta	Packet Tracer	GNS3	VNUML	VNX	CADE	PRTG
Licencia	Pagada	Gratuita	Gratuita	Gratuita	Gratuita	Pagada
Última Versión (2015)	6.8.1.3	1.3.13	1.8.9 (2009, reemplazado por VNX)	2.0b.5647	2.20.3	15.4.21.5215
Sistemas Operativos Soportados	Windows Linux MAC OS	Windows Linux MAC OS	Linux	Linux	Windows	Windows
GUI	Sí	Sí	No	Sí	Sí	Sí
IOS Cisco	Sí	Sí	No	No	No	Sí
Comunicación con equipos reales	No	No	Sí	Sí	No	Sí

Entre los más destacados se encuentran: VNUML, herramienta diseñada por la Universidad Técnica de Madrid y utilizada ampliamente en la Universidad de Koblenz-Landau (Alemania); Dynamips, *software* desarrollado para emular enrutadores de las marcas Cisco Systems (IOS) y Juniper (JunOS); y, GNS3, virtualizador de redes gráfico enfocado a la simulación de redes complejas que usa como motor de ejecución la plataforma Dynamips/Dynagen (Britos, Vargas, Arias, Giraudo, & Veneranda, 2013) (Pereñíguez-García, Ruiz, Ros, Marín, & Ruiz, 2012).

Al comparar los programas, de acuerdo a la encuesta llevada a cabo a los estudiantes en la Universidad de Murcia, GNS3 obtiene una mejor valoración en cuanto a usabilidad de la herramienta ya que posibilita al estudiante centrar su esfuerzo en el aprendizaje y no dedicar tiempo a aspectos relacionados con el manejo del entorno. Sin embargo, también destaca que su uso está limitado a la virtualización de escenarios de red fundamentados en enrutadores Cisco o Juniper. Por otra parte, sobre VNUML expone que, si bien no permite trabajar de forma fluida con escenarios de red complejos, virtualiza topologías donde las máquinas son tipo Linux, lo que permite la instalación de nuevo *software* (Pereñíguez-García, Ruiz, Ros, Marín, & Ruiz, 2012).

Cabe destacar que ninguno de los programas mencionados es capaz de configurar equipos físicos por sí solos, únicamente trabajan como simuladores virtuales. Algunos de ellos utilizan aplicaciones externas como interfaces para realizar la comunicación con el entorno real de una red aunque su desempeño es limitado y continúa en desarrollo (Britos, Vargas, Arias, Giraudo, & Veneranda, 2013) (Pereñíguez-García, Ruiz, Ros, Marín, & Ruiz, 2012).

Por otro lado, en investigaciones realizadas por miembros de la IEEE, se ha combinado tecnologías como XEN y VNC (Computación Virtual en Red,) para construir un laboratorio basado en Web (NVLab), siendo adecuado para cursos de TIC donde se requiere trabajar con múltiples dispositivos conectados en red (Dougliis & Krieger, 2013) (Wannous & Nakano, 2010).

CAPÍTULO 3

SITUACIÓN ACTUAL

Al tener una ligera idea de lo que se pretende realizar con el programa, es necesario también conocer el entorno en el que será implementado y la configuración inicial que requieren los equipos antes de la integración del *software*.

La aplicación será instalada en el laboratorio de redes de la Universidad del Azuay, por ello, en el presente capítulo se explica la topología de la red existente; cuáles son los equipos que forman la misma; sus características fundamentales y sus opciones de configuración. Además, se detallan las conexiones externas (físicas) e internas (virtuales) de las interfaces de cada nodo de red.

3.1. Distribución de la red

3.1.1. Esquema de la red

El laboratorio está distribuido de tal manera que tiene dos *racks* idénticos que poseen elementos de red para las capas de núcleo, distribución y acceso.

La capa de núcleo (*core*) cuenta con dos enrutadores interconectados entre sí, colocados cada uno en su *rack* respectivo. En la capa de distribución se dispone de tres enrutadores por *rack* con conexiones directas hacia el *router core* pertinente. De igual forma, cada uno de ellos está conectado a un conmutador (*switch*) de la capa de acceso, que son los que permiten la conexión de los computadores que integran los puestos de prácticas del laboratorio.

El laboratorio, además de los seis ordenadores con los que dispone, permite la utilización de más computadores a través de *patch panels* conectados a los conmutadores de la red. Para esto, los usuarios pueden acceder a la red por medio de cables de cobre (*patch cords*).

Cabe destacar que debido a los equipos utilizados en el laboratorio, los usuarios solamente podrán acceder a la red por un medio de transmisión alámbrico.

Para un mejor entendimiento, en la figura 3.1 se muestra el esquema de la red configurada para el laboratorio:

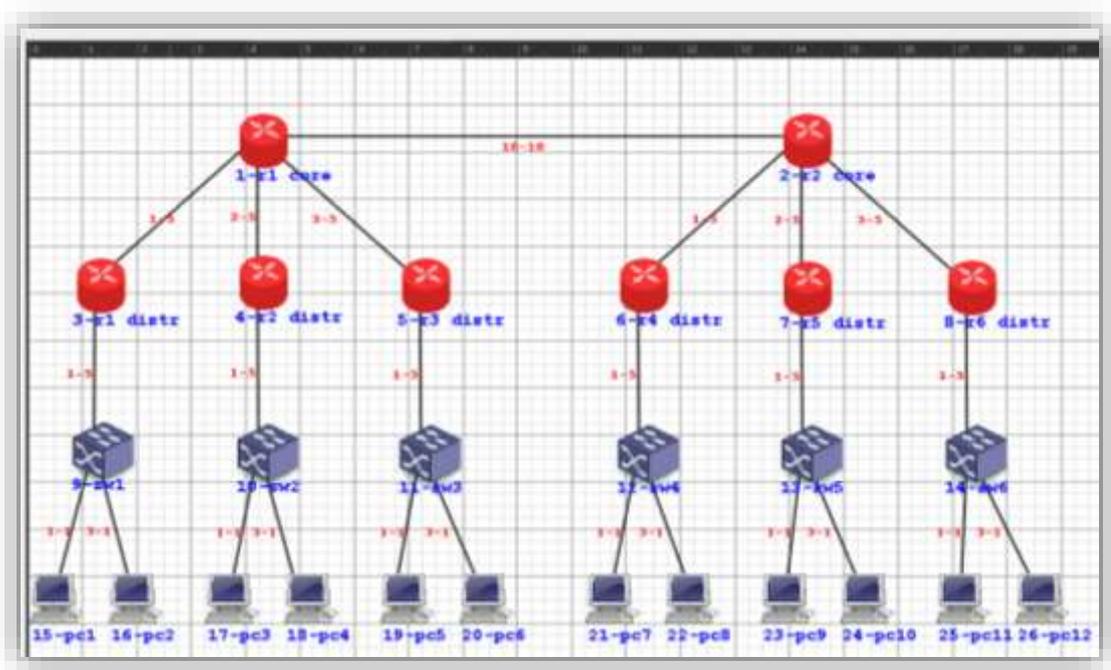


Figura 3.1. Esquema de red del laboratorio de redes de la Universidad del Azuay.

3.1.2. Configuración actual

Para aprovechar al máximo la red del laboratorio, en la capa de acceso está configurado cada *switch* con dos VLANs diferentes, a su vez cada VLAN tiene asignados dos puertos, por lo que hay un total de 12 puntos de acceso: 6 de las interfaces corresponden a los equipos del laboratorio y las restantes permiten la entrada de más dispositivos.

De igual manera, se cuenta con VLANs para la conexión entre cada *switch* y su respectivo *router* de la capa de distribución. Asimismo, VLANs entre las capas de distribución y la capa núcleo permiten comunicar los *switches* con los *routers core* a través del *router* de distribución. Finalmente, los *routers core* se encuentran conectados entre sí, permitiendo comunicar los dos *racks*.

En la figura 3.2 podemos observar las subredes, mientras en la figura 3.3 se ve las VLANs creadas entre cada elemento del laboratorio.

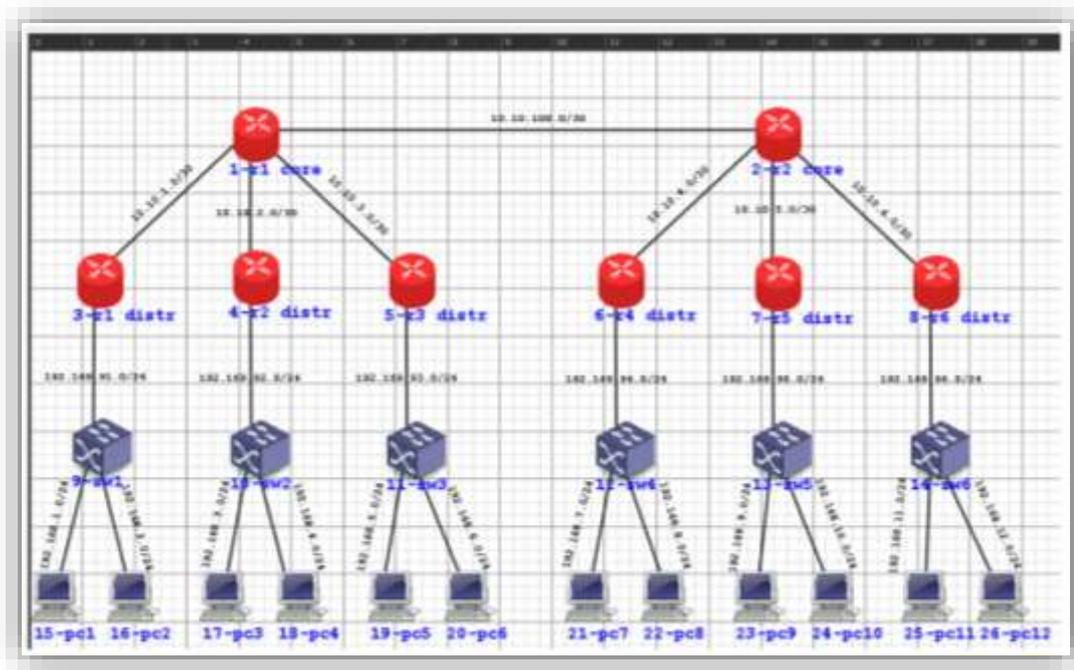


Figura 3.2. Diagrama de direcciones IP de la red actual.

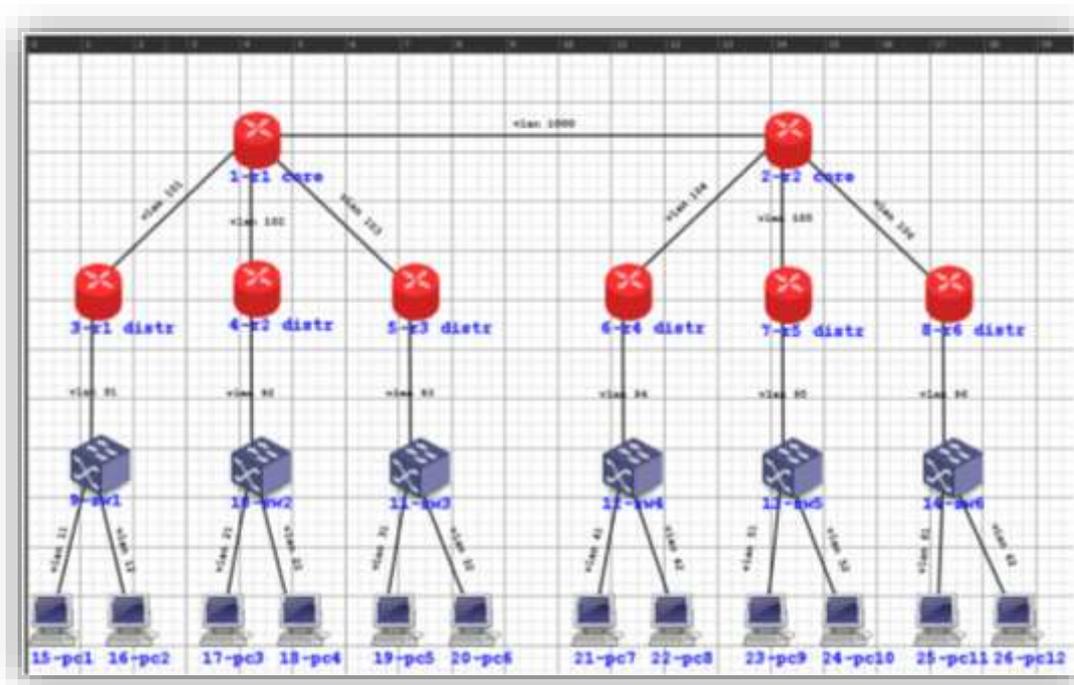


Figura 3.3. Distribución de VLANs de la red actual.

3.1.3. Resumen de direccionamiento

En la tabla 3.1 podemos observar las direcciones IP y las VLANs utilizadas en cada subred.

Tabla 3.1. Tabla de direccionamiento de la red.

Vlan	Dirección	Rango de host utilizables	Broadcast	Gateway
1000	10.10.100.0/30	10.10.100.1-10.10.100.2	10.10.100.3	-
101	10.10.1.0/30	10.10.1.1-10.10.1.2	10.10.1.3	-
102	10.10.2.0/30	10.10.2.1-10.10.2.2	10.10.2.3	-
103	10.10.3.0/30	10.10.3.1-10.10.3.2	10.10.3.3	-
104	10.10.4.0/30	10.10.4.1-10.10.4.2	10.10.4.3	-
105	10.10.5.0/30	10.10.5.1-10.10.5.2	10.10.5.3	-
106	10.10.6.0/30	10.10.6.1-10.10.6.2	10.10.6.3	-
91	192.169.91.0/24	192.169.91.1-192.169.91.254	192.169.91.255	192.169.91.1
92	192.169.92.0/24	192.169.92.1-192.169.92.254	192.169.92.255	192.169.92.1
93	192.169.93.0/24	192.169.93.1-192.169.93.254	192.169.93.255	192.169.93.1
94	192.169.94.0/24	192.169.94.1-192.169.94.254	192.169.94.255	192.169.94.1
95	192.169.95.0/24	192.169.95.1-192.169.95.254	192.169.95.255	192.169.95.1
96	192.169.96.0/24	192.169.96.1-192.169.96.254	192.169.96.255	192.169.96.1
11	192.168.1.0/24	192.168.1.1-192.168.1.254	192.168.1.255	192.168.1.1
12	192.168.2.0/24	192.168.2.1-192.168.2.254	192.168.2.255	192.168.2.1
21	192.168.3.0/24	192.168.3.1-192.168.3.254	192.168.3.255	192.168.3.1
22	192.168.4.0/24	192.168.4.1-192.168.4.254	192.168.4.255	192.168.4.1
31	192.168.5.0/24	192.168.5.1-192.168.5.254	192.168.5.255	192.168.5.1
32	192.168.6.0/24	192.168.6.1-192.168.6.254	192.168.6.255	192.168.6.1
41	192.168.7.0/24	192.168.7.1-192.168.7.254	192.168.7.255	192.168.7.1
42	192.168.8.0/24	192.168.8.1-192.168.8.254	192.168.8.255	192.168.8.1
51	192.168.9.0/24	192.168.9.1-192.168.9.254	192.168.9.255	192.168.9.1
52	192.168.10.0/24	192.168.10.1-192.168.10.254	192.168.10.255	192.168.10.1
61	192.168.11.0/24	192.168.11.1-192.168.11.254	192.168.11.255	192.168.11.1
62	192.168.12.0/24	192.168.12.1-192.168.12.254	192.168.12.255	192.168.12.1

Además en la tabla 3.2 se muestra el rango de direcciones IP fijas y dinámicas asignadas por el servidor DHCP configurado en cada *router*.

Tabla 3.2. Rangos de direccionamiento estático y dinámico de cada subred.

Vlan	Subred	Rangos	
		IPs Fijas	IPs Dinámicas
91	192.169.91.0/24	192.169.91.1-192.169.91.99	192.169.91.100-192.169.91.254
92	192.169.92.0/24	192.169.92.1-192.169.92.99	192.169.92.100-192.169.92.254
93	192.169.93.0/24	192.169.93.1-192.169.93.99	192.169.93.100-192.169.93.254
94	192.169.94.0/24	192.169.94.1-192.169.94.99	192.169.94.100-192.169.94.254
95	192.169.95.0/24	192.169.95.1-192.169.95.99	192.169.95.100-192.169.95.254
96	192.169.96.0/24	192.169.96.1-192.169.96.99	192.169.96.100-192.169.96.254
11	192.168.1.0/24	192.168.1.1-192.168.1.99	192.168.1.100-192.168.1.254
12	192.168.2.0/24	192.168.2.1-192.168.2.99	192.168.2.100-192.168.2.254
21	192.168.3.0/24	192.168.3.1-192.168.3.99	192.168.3.100-192.168.3.254
22	192.168.4.0/24	192.168.4.1-192.168.4.99	192.168.4.100-192.168.4.254
31	192.168.5.0/24	192.168.5.1-192.168.5.99	192.168.5.100-192.168.5.254
32	192.168.6.0/24	192.168.6.1-192.168.6.99	192.168.6.100-192.168.6.254
41	192.168.7.0/24	192.168.7.1-192.168.7.99	192.168.7.100-192.168.7.254
42	192.168.8.0/24	192.168.8.1-192.168.8.99	192.168.8.100-192.168.8.254
51	192.168.9.0/24	192.168.9.1-192.168.9.99	192.168.9.100-192.168.9.254
52	192.168.10.0/24	192.168.10.1-192.168.10.99	192.168.10.100-192.168.10.254
61	192.168.11.0/24	192.168.11.1-192.168.11.99	192.168.11.100-192.168.11.254
62	192.168.12.0/24	192.168.12.1-192.168.12.99	192.168.12.100-192.168.12.254

3.2. Equipos utilizados

3.2.1. Capa de núcleo: *router* RB2011UiAS-RM

La familia de *routers* RB2011L ha estado en el mercado por 15 años y ha sido continuamente mejorada añadiendo características como enrutamiento dinámico, *firewall*, MPLS, VPN, balanceo de cargas, configuración en tiempo real y monitorización.

El *router* RB2011UiAS-RM, diseñado específicamente para montaje en *rack*, tiene 5 puertos Fast Ethernet, 5 puertos Gigabit Ethernet, un puerto serial RJ45, y un puerto micro USB. Tiene una memoria RAM de 128MB y funciona con el sistema operativo RouterOS L5, y además posee una pantalla táctil LCD para su monitorización. El puerto Ethernet 10 incluye la función de salida PoE que permite energizar otros dispositivos con una corriente máxima de salida de 500mA.

La imagen del dispositivo se muestra en la figura 3.4 mientras que la tabla 3.3 se detallan, de una manera resumida, sus características.

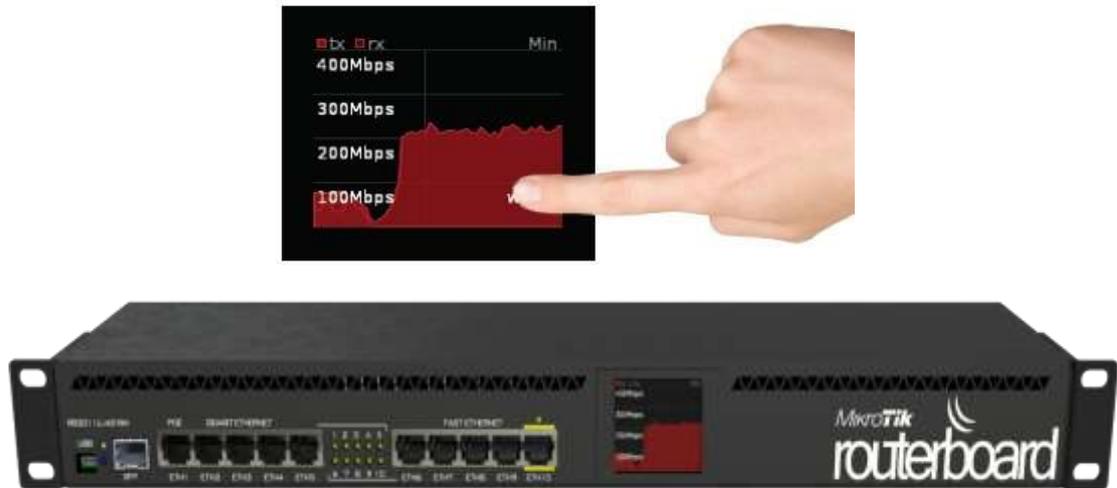


Figura 3.4. Router RB2011UiAS-RM.
Fuente: (MikroTik, s.f.)

Tabla 3.3. Características del router RB2011UiAS-RM.

Tabla de Características	
Router RB2011UiAS-RM	
CPU	Atheros AR9344 600MHz
Memoria	128MB DDR SDRAM
Puertos 10/100 Mbit Fast Ethernet	5
Puertos 10/100/1000 Mbit Gigabit Ethernet con Auto-MDI/X	5
Voltaje de Entrada	8 v - 28 v
PoE Entrada/Salida	Si
Dimension	443x92x44mm
Sistema Operativo	RouterOS
Nivel de licencia	5
Rango de temperatura	-25C a + 65C
Potencia máxima de consumo	15W max
Puerto SFP	1

Fuente: (MikroTik, s.f.)

A continuación, en la figura 3.5 se presenta un esquema del router RB2011UiAS-RM, donde se detalla la configuración interna del equipo.

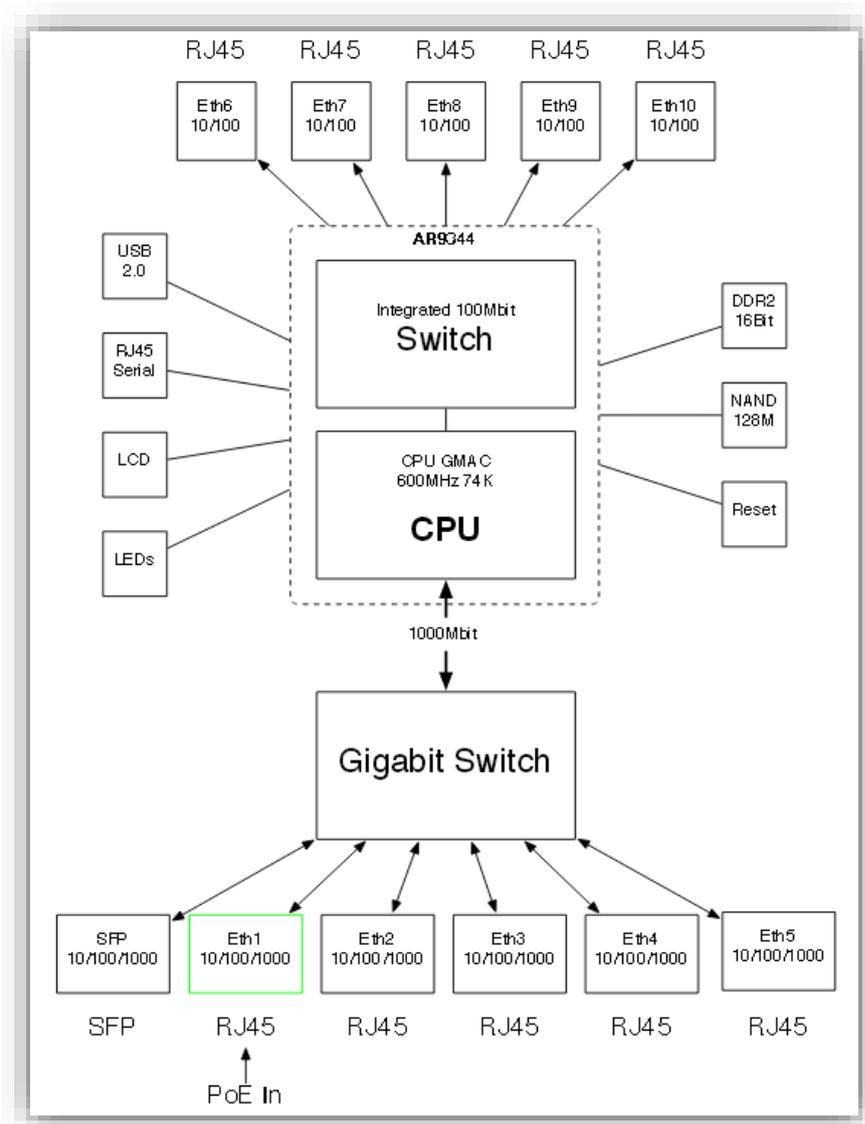


Figura 3.5. Esquema interno del *router* RB2011UiAS-RM.
Fuente: (MikroTik, s.f.)

3.2.2. Capa de distribución: *router* hEX lite

Es un *router* que posee 5 puertos de conexión Ethernet, configurables con velocidades de 10/100 Mbps, siendo el primer puerto Ethernet la entrada para el acceso de Internet y también un puerto PoE de entrada, trabajando con rangos de voltaje entre 6 y 30 voltios. Posee un procesador de un núcleo funcionando a una frecuencia de 850 MHz y su memoria RAM es de 64 Mb. El hEX lite posee memoria interna y trabaja con el sistema operativo RouterOS.

La imagen del *router* se muestra en la figura 3.6 y en la tabla 3.4 se detallan sus características.



Figura 3.6. *Router* hEX lite.

Fuente: (MikroTik, s.f.)

Tabla 3.4: Características del *router* hEX lite.

Tabla de Características	
hEX lite	
Frecuencia nominal del CPU	850 MHz
Nucleos del CPU	1
Memoria RAM	64 MB
Puertos Ethernet 10/100	5
Voltaje de Entrada	6 v - 30 v
PoE	Si
Dimension	113x89x28mm
Peso	129 g
Sistema Operativo	RouterOS
Rango de temperatura	-20C a + 70C
Nivel de licencia	4
CPU	QCA9531
Potencia máxima de consumo	2W
Tipo de almacenamiento	FLASH
Tamaño de almacenamiento	16 MB

Fuente: (MikroTik, s.f.)

3.2.3. Capa de acceso: *switch* RB260GSP

Este modelo corresponde a un *switch* SOHO (*Small Office/Home Office*) que permite conectar varios dispositivos entre sí a una misma red mediante el uso de conmutación de paquetes para recibir, procesar y enviar datos.

Posee 5 puertos Gigabit Ethernet con velocidades de 10/100/1000 Mbps y un puerto SFP, además los puertos Ethernet 2-5 tienen la capacidad de energizar otros dispositivos PoE con el mismo voltaje aplicado al switch. Trabaja con rangos de voltaje entre 8 y 30 voltios. El sistema operativo que se encuentra en el dispositivo es el SwOS. En la figura 3.7 se puede apreciar al equipo mientras que en la figura 3.8 podemos observar el acceso al sistema operativo mediante un navegador.

SwOS es configurable desde el navegador web y contiene las funcionalidades básicas de un switch, además permite la configuración *port forwarding* puerto a puerto, aplicar filtros MAC, crear VLANs, configurar un puerto espejo o *port mirroring*, limitar el ancho de banda e incluso ajustar cabeceras para algunas direcciones MAC e IP.

El resumen de sus especificaciones se muestra en la tabla 3.5 a continuación (MikroTik, s.f.).



Figura 3.7. *Switch* RB260GSP.

Fuente: (MikroTik, s.f.)

	Port1	Port2	Port3	Port4	Port5
Link					
Enabled	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Link Status	link on	link on	no link	no link	link on
Auto Negotiation	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Speed	1000	100			100
Full Duplex	yes	<input checked="" type="checkbox"/>	no	no	yes
Flow Control	<input checked="" type="checkbox"/>				

Figura 3.8. MikroTik SwOS.

Fuente: (MikroTik, s.f.)

Tabla 3.5: Características del *switch* RB260GSP

Tabla de Características	
RB260GSP	
CPU	Taifatech TF470
Memoria	Embebida 96K SRAM
Puertos Ethernet 10/100/1000	5
Voltaje de Entrada	8 v - 30 v
PoE Entrada/Salida	Si
Dimension	113x139x28mm
Peso	212 g
Sistema Operativo	SwitchOS
Rango de temperatura	-25C a + 65C
Nivel de licencia	4
Potencia máxima de consumo	6W
Puerto SFP	1

Fuente: (MikroTik, s.f.)

CAPÍTULO 4

IMPLEMENTACIÓN DEL PROGRAMA DE VIRTUALIZACIÓN

Para desarrollar un *software* es necesario plantear o definir las funciones que va a realizar, la mejor manera de organizar la ideas es la de crear diagramas de flujo y esquemas; éstos permiten que cualquier persona sin tener un alto grado de programación entienda, en un aspecto básico, cómo trabaja el programa.

De igual manera es importante dar a conocer cómo está estructurado el programa, es decir, explicar el entorno en el que se maneja. Esto se lleva a cabo explicando las ventanas y las herramientas del *software*, permitiendo familiarizar al usuario con el mismo.

El programa desarrollado en esta tesis, que desde ahora se llamará ENDS (*Easy Network Designer Software*), trabaja con librerías adicionales de Java y un gestor de base de datos MySQL. El programa de licencia gratuita XAMPP incorpora dicha característica y, debido a su facilidad de manejo e instalación, fue escogido para inicializar el servicio.

4.1. Requisitos de instalación

4.1.1. Java

ENDS se basa en lenguaje de programación Java, por lo que son necesarios dos componentes en el entorno donde se va a ejecutar: una máquina virtual de Java (JVM), y un conjunto de bibliotecas para proporcionar los servicios que pueda necesitar la aplicación. La JVM es proporcionada por Sun Microsystems, y en ella se incluyen las bibliotecas estándar, normalmente se conocen como JRE (*Java Runtime Environment*) o entorno en tiempo de ejecución para Java. El sistema debe contar con JRE que es lo mínimo para poder ejecutar una aplicación Java sobre el mismo. (Oracle, s.f.)

Se debe recalcar que para hacer uso de las librerías adicionales que citaremos a continuación es necesario tener la versión 1.6 de Java, disponible en la página oficial de Oracle. (Oracle, s.f.)

4.1.2. Librerías de Java

4.1.2.1. Apache Commons Net

Para poder establecer la comunicación con los equipos mediante el protocolo Telnet (*Telecommunication Network*), Java requiere de la librería Apache Commons Net. Esta librería, desarrollada por la Fundación de Software Apache, en inglés The Apache Software Foundation, incluye una colección de utilidades de redes y además implementa múltiples protocolos. Su propósito es el de proveer el acceso fundamental a los protocolos de red a través de un cliente. (The Apache Software Foundation, s.f.)

Los protocolos soportados por la librería son:

- FTP/FTPS (File Transfer Protocol / File Transfer Protocol Secure)
- NNTP (Network News Transport Protocol)
- SMTP (Simple Mail Transfer Protocol)
- POP3 (Post Office Protocol)
- IMAP (Internet Message Access Protocol)
- Telnet
- TFTP (Trivial File Transfer Protocol)
- Finger
- Whois
- rexec/rcmd/rlogin (Remote Process Execution / Command Prompt / Login)
- Time (rdate) and Daytime
- Echo
- Discard
- NTP/SNTP (Network Time Protocol / Simple Network Time Protocol)

Para incluir la librería en un proyecto desarrollado en un IDE (entorno de desarrollo interactivo, en inglés *Integrated Development Environment*), como NetBeans, se debe descargar los archivos .jar que contienen la librería. Ésta se encuentra disponible de forma gratuita en la misma página de la fundación.

Una vez agregada al proyecto, el IDE se encarga de incluirla en el programa compilado para su futura distribución, por lo que el usuario no tiene la necesidad de descargarla.

4.1.2.2. MySQL Connector/J

Para la ejecución de operaciones sobre bases de datos desde el lenguaje de programación, Java incluye la API¹ *Java Database Connectivity*, más conocida por sus siglas JDBC, que es independiente del sistema operativo donde se ejecute o de la base de datos a la cual accede y que hace uso del código SQL del modelo de base de datos que se utilice.

Para que el sistema operativo pueda interactuar con JDBC es necesario un controlador de dispositivo o *driver*, en este caso, MySQL Connector/J es el driver oficial para la comunicación con el servicio MySQL que ENDS necesita para su funcionamiento.

De igual manera que con la librería Apache Commons Net, el IDE se encarga de incluir MySQL Connector/J en la carpeta de distribución del programa final.

4.1.3. Xampp

Xampp es un servidor independiente de plataforma, de código libre, que incluye varios sistemas importantes como son: gestión de bases de datos MySQL, Apache, servidores FTP, intérpretes de lenguajes PHP² y Perl, entre otros. Se destaca por su facilidad al momento de inicializar estos servicios y ofrece la posibilidad de realizar configuraciones sobre los mismos de una forma sencilla.

La última versión de Xampp para cada sistema operativo se puede obtener gratuitamente en la página oficial del programa en la sección de descargas.

ENDS requiere del servicio MySQL, por lo que en la instalación de Xampp se debe seleccionar únicamente esta opción tal como se indica en la figura 4.1.

¹ Interfaz de Programación de Aplicaciones, del inglés: *Application Programming Interface*.

² *PHP Hypertext Pre-processor*.

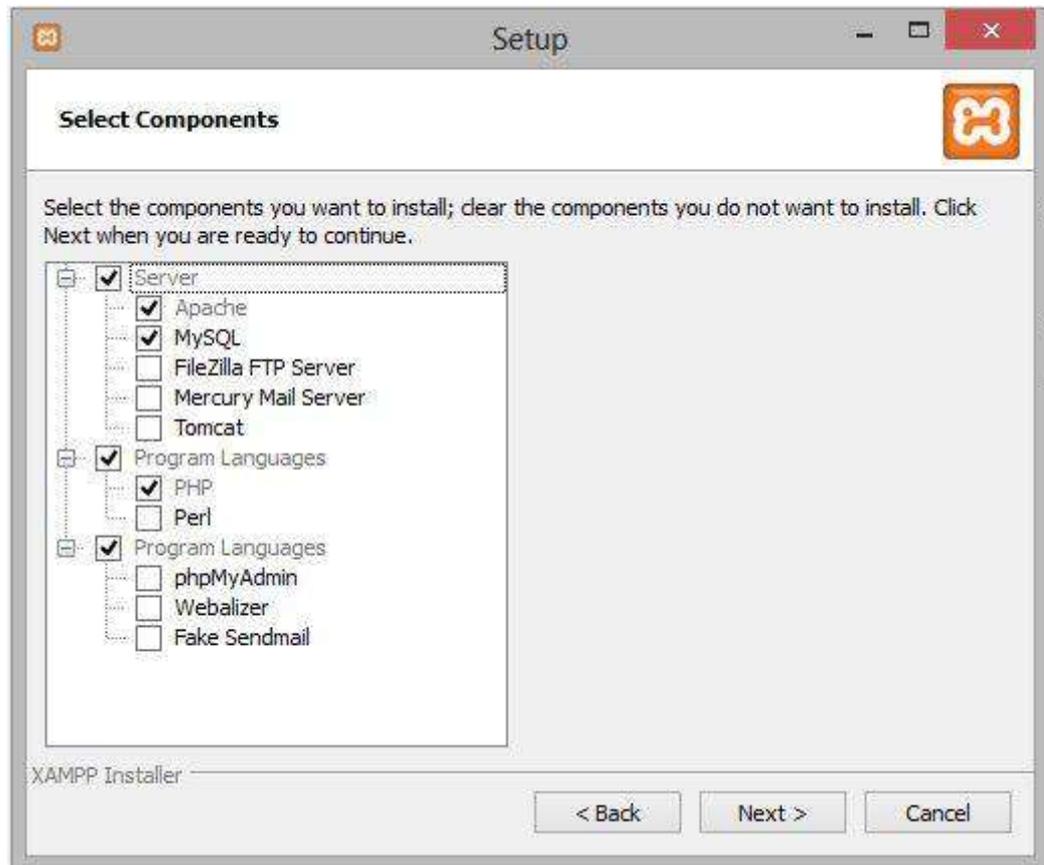


Figura 4.1. Selección de servicios en la instalación de Xampp.

4.2. Explicación del programa

4.2.1. Diagramas de flujo

La ventana gráfica de ENDS trabaja de una forma interactiva con el usuario y permite agregar, modificar y borrar elementos. El diagrama de flujo de la figura 4.2 muestra cómo el programa obtiene los elementos de red de un proyecto almacenado en su base de datos y los presenta en su interfaz. También permite crear o eliminar enlaces entre los nodos y guardarlos en el proyecto.

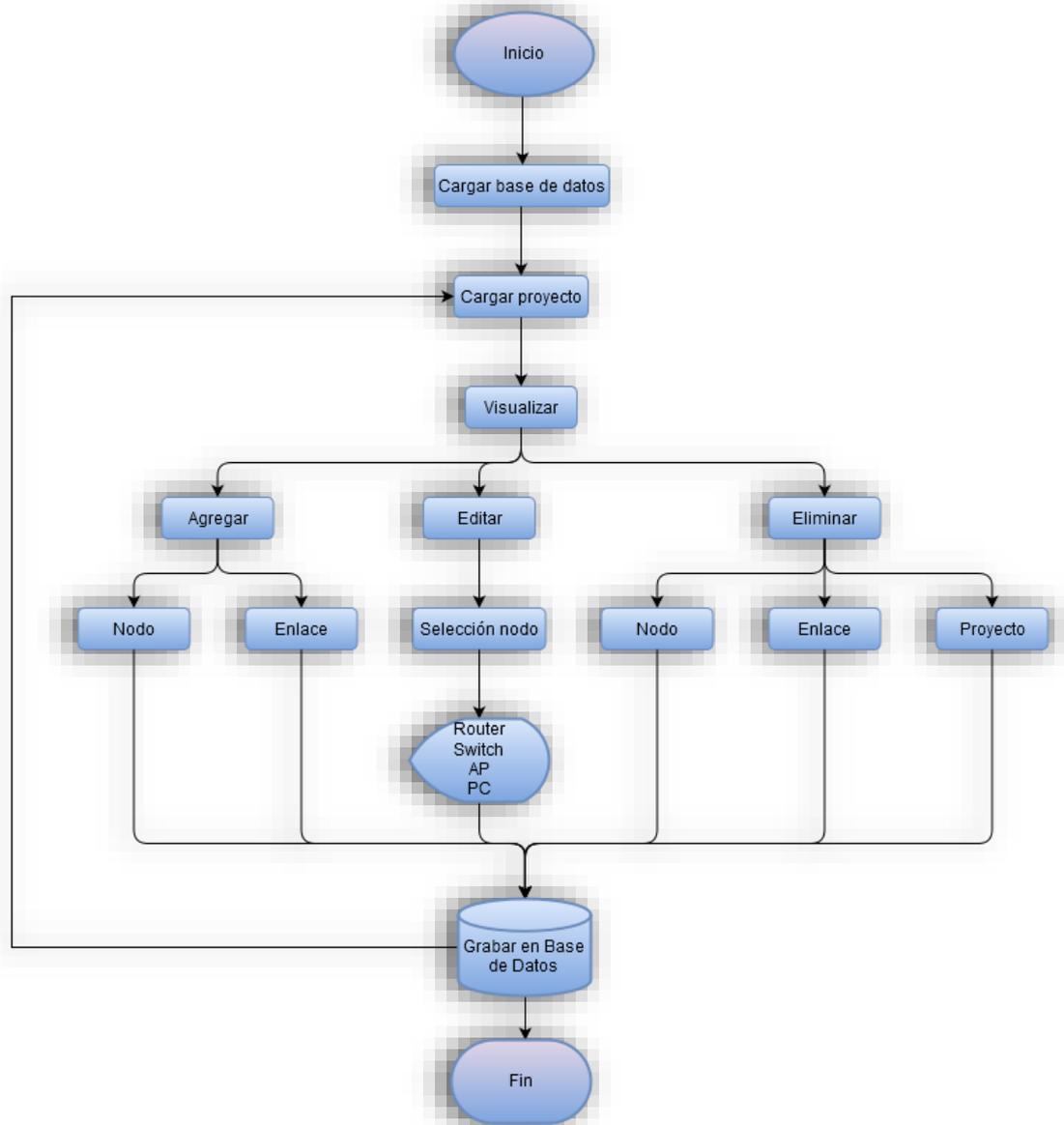


Figura 4.2. Diagrama de flujo de la interfaz gráfica de ENDS.

ENDS además despliega ventanas de configuración adicionales según el nodo de red que sea seleccionado y permite la comunicación con los equipos del laboratorio.

En la figura 4.3 el diagrama de flujo indica el proceso de búsqueda de campos en la base de datos acerca del equipo que se desea configurar y el inicio de comunicación con el mismo. En caso de no encontrar la dirección IP del dispositivo en el proyecto, ENDS solicita el ingreso de usuario y contraseña para permitir el acceso a la unidad. Una vez establecida la comunicación, según la configuración que el usuario desee realizar en el equipo, ENDS enviará los comandos respectivos.

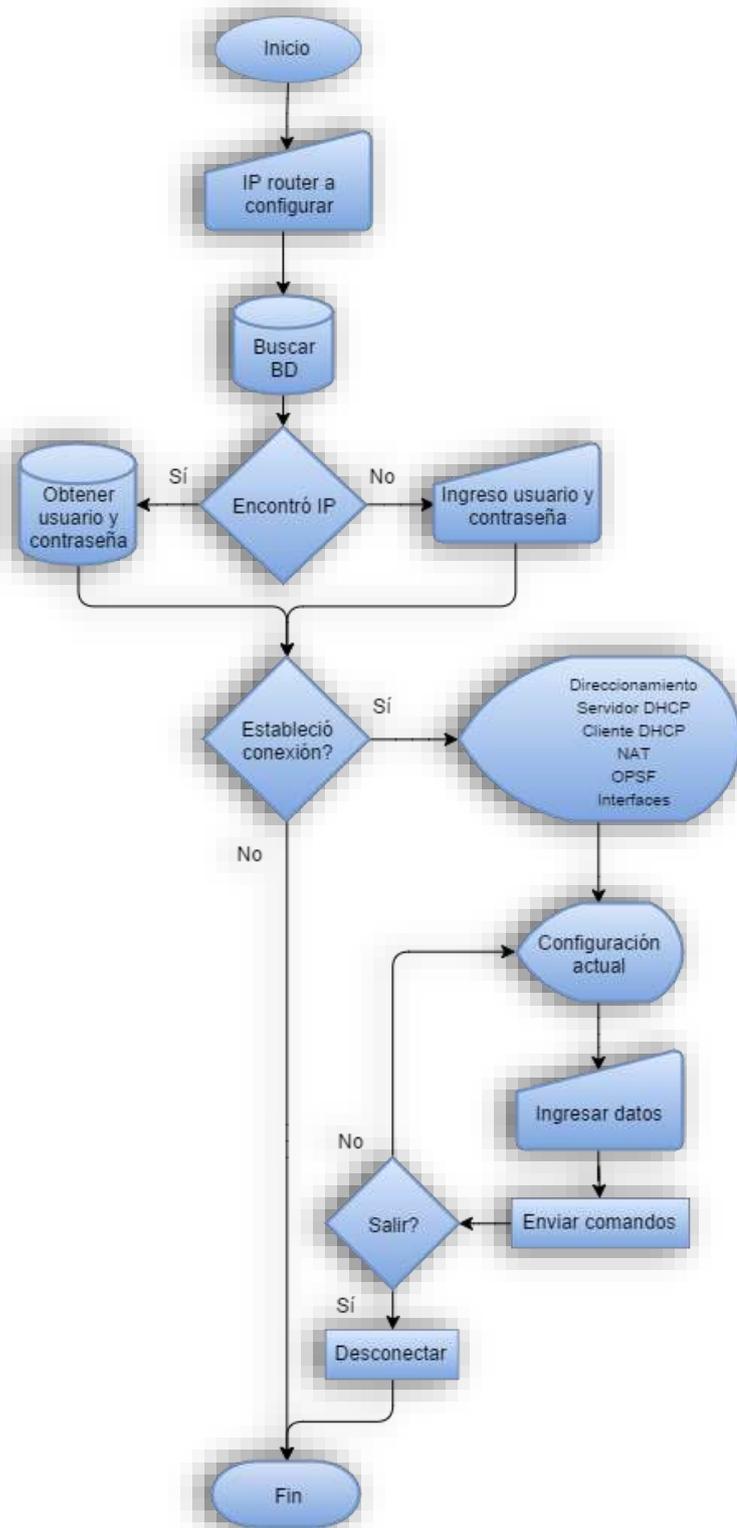


Figura 4.3. Diagrama de flujo para establecer la comunicación con un equipo del laboratorio.

4.2.2. Funcionamiento general

ENDS hace uso de Xampp para establecer la comunicación con la base de datos local a través del servicio MySQL, la cual contiene información de diseños de red realizados y los comandos de equipos MikroTik. Cada vez que ENDS se ejecuta en un ordenador el programa verifica la existencia de la base de datos y en caso de no encontrarla la crea automáticamente.

Desde la ventana principal se cargan los diferentes proyectos almacenados para mostrarlos en la interfaz. En ella, los diseños pueden ser modificados agregando o eliminando elementos de red y también se pueden crear nuevos diseños.

ENDS permite la configuración de los elementos de red de un proyecto a través de ventanas emergentes. Cada una de ellas solicita el ingreso de datos conforme la función que se desee realizar.

En primera instancia, haciendo uso de la dirección IP del dispositivo se establece una comunicación Telnet con el mismo. Para permitir el acceso se utilizan los campos de usuario y contraseña guardados en la base de datos. Una vez autenticado, el usuario ingresa la información que desee configurar y con esto se genera el comando respectivo para enviar al equipo. Finalizado el proceso, ENDS cierra la comunicación y despliega la interfaz principal nuevamente.

4.3. Estructura del programa

4.3.1. Ventana de inicio

Al ejecutar el programa, se muestra la ventana de inicio, la cual presenta el logo de ENDS y una barra de progreso como indicadora de que está cargando la base de datos. Dicha ventana se muestra en la figura 4.4.



Figura 4.4. Ventana de inicio de ENDS.

4.3.2. Ventana principal

La ventana principal de ENDS constituye la interfaz más importante del programa, en ella se muestran los diseños de red y los botones que permiten acceder a los demás paneles. Para un mejor entendimiento, se divide a la ventana en siete secciones como se puede ver en la figura 4.5.

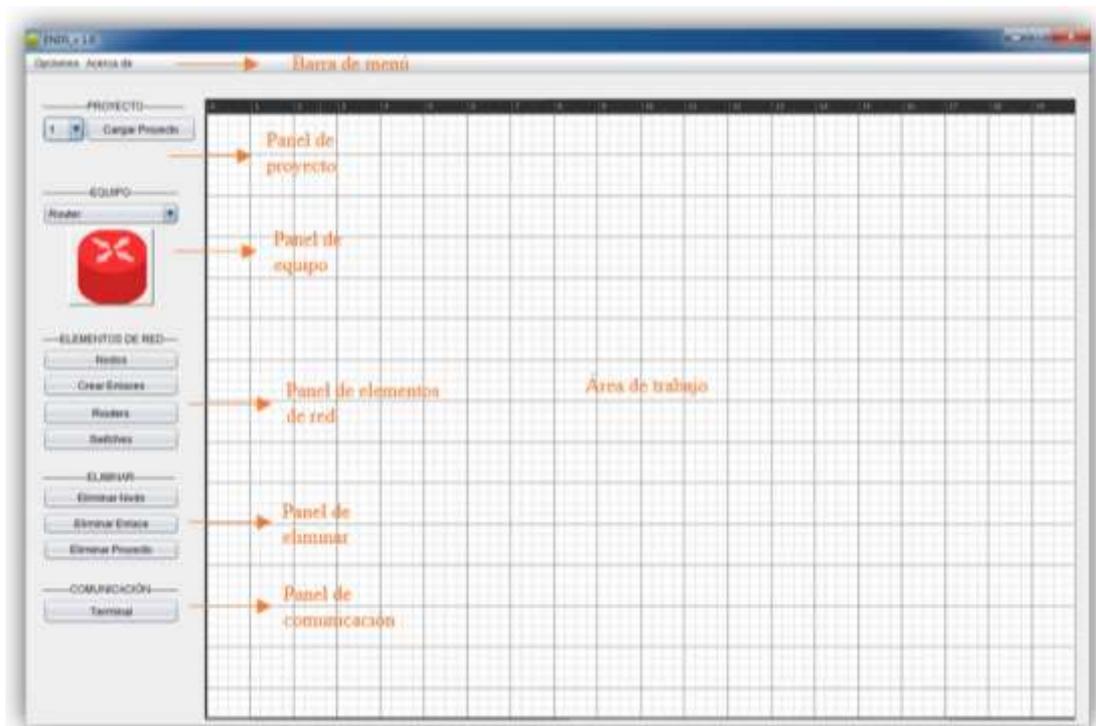


Figura 4.5. Ventana principal de ENDS.

- **Barra de menú:** contiene información general del *software*.
- **Panel de proyecto:** permite seleccionar el proyecto que se desee cargar de una lista desplegable.
- **Panel de equipo:** permite escoger entre los distintos nodos de red que se desee agregar al proyecto: *router*, *PC*, *switch*, o *access point*. Estas opciones se muestran en la figura 4.6.



Figura 4.6. Opciones del panel de equipo de la ventana principal.

- **Panel de elementos de red:** posee botones que permiten desplegar ventanas con información acerca de los nodos.
- **Panel de eliminar:** incluye botones para escoger la opción a eliminar.
- **Panel de comunicación:** muestra el botón para acceder al terminal de comunicaciones.
- **Área de trabajo:** presenta el diseño de red y facilita la adición de nuevos elementos.

Además, el panel de área de trabajo detecta eventos del ratón (*mouse clicked*) para reconocer si se realiza una selección de un nodo existente o si se presiona sobre una zona en blanco. Cada selección despliega una ventana diferente que depende del tipo del nodo escogido; y, en caso de requerir la adición de un nuevo elemento, la aplicación solicita el nombre del mismo a través de una ventana emergente.

4.3.3. Elementos de red

4.3.3.1. Nodos

Esta ventana lista los nodos de red del actual proyecto sin importar su tipo. Para la visualización de cada uno de ellos se cuenta con una tabla que muestra la información; y, al seleccionar un elemento de la tabla, se llenan campos de texto que permiten la modificación de los registros de dicho nodo en la base de datos.

En la figura 4.7 se puede observar la ventana “*Nodos de Red*” dividida en sus secciones más representativas, que son:

- **A:** permite mostrar en la tabla ya sean todos los nodos de red del proyecto o, mediante una indagación personalizada por dirección IP o tipo, el ítem del campo de texto de búsqueda.
- **B:** contiene botones que permiten actualizar o eliminar los registros del proyecto en la base de datos.
- **C:** muestra los campos de texto con la información respectiva. Vale mencionar que los campos X y Y indican la posición del nodo seleccionado en el diseño de red.

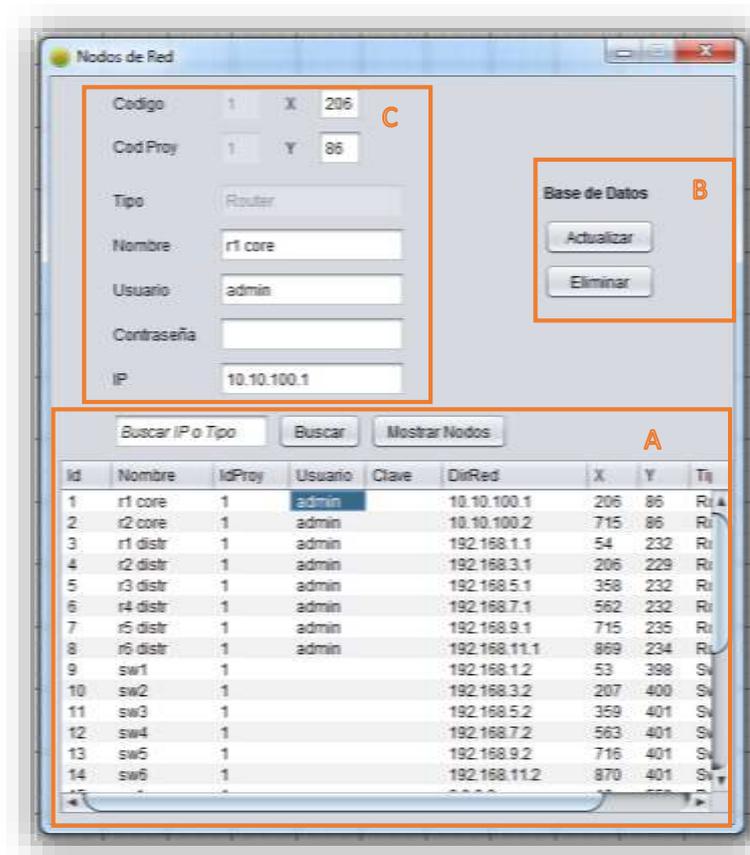


Figura 4.7. Ventana “*Nodos de Red*”.

4.3.3.2. Crear Enlaces

Permite crear un enlace entre dos nodos y además agregar un comentario al mismo. Es necesario digitar los números de identificación de cada nodo para realizar esta acción. La figura 4.8 ilustra el proceso de creación de un enlace.

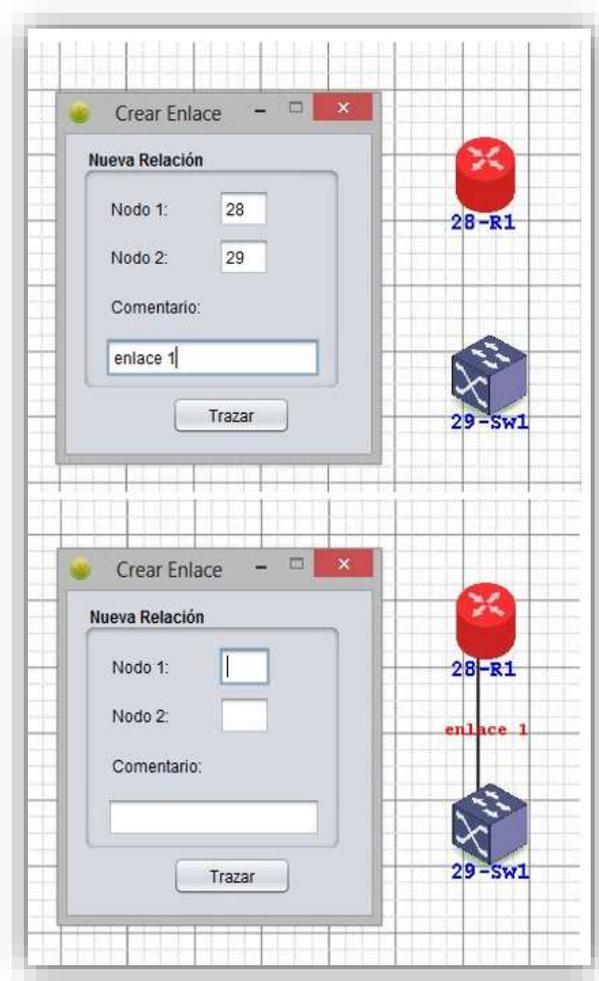


Figura 4.8. Creación de un enlace entre dos nodos.

4.3.3.3. Routers

La ventana “Router”, que se puede observar en la figura 4.9, lista los nodos tipo *router* que contiene el proyecto. Una tabla muestra la información de cada elemento; y, en caso de seleccionar uno de ellos, se llenan campos de texto que permiten la modificación de los registros de dicho *router* en la base de datos de manera similar que en la ventana “Nodos de Red”, con la diferencia que el botón *Agregar*, del panel Base de Datos, se activa para guardar un nuevo dispositivo al proyecto.

Además, en una tabla adicional se muestran los enlaces que involucran al *router* seleccionado. Esta tabla consta de tres columnas: la primera contiene el número de identificación *Id* del primer nodo del enlace, la segunda el número *Id* correspondiente al segundo nodo, y la tercera columna lista los comentarios del enlace.

Id	Nombre	IdProy	Usuario	Clave	DirRed	X	Y	Tipo
1	r1 core	1	admin		10.10.100.1	206	86	Router
2	r2 core	1	admin		10.10.100.2	715	86	Router
3	r1 distr	1	admin		192.168.1.1	54	232	Router
4	r2 distr	1	admin		192.168.3.1	206	229	Router
5	r3 distr	1	admin		192.168.5.1	358	232	Router

Nodo1	Nodo2	Comentario
1	2	10
1	3	1
1	4	2
1	5	3

Figura 4.9. Ventana “Router”.

Los botones *Buscar* y *Mostrar Routers* permiten buscar una dirección IP dentro de la tabla o mostrar todos los *routers* del proyecto respectivamente. Junto a ellos, los botones *Conectar* y *Abrir Navegador*, posibilitan establecer una comunicación con la dirección IP del campo de texto *Dirección IP*, ya sea mediante el terminal o el navegador predeterminado del sistema.

Adicionalmente, el panel *Configuraciones* presenta botones que dirigen a ventanas anexas en las cuales, como su nombre indica, se pueden realizar configuraciones sobre el equipo. Todas ellas trabajan conjuntamente con el terminal de comunicaciones por lo que al presionar cualquier botón se abrirá la ventana correspondiente y también el “*Terminal Telnet*” que se expone más adelante.

A continuación se explican cada una de las interfaces de configuración.

a. Interfaces

Esta opción, que se puede observar en la figura 4.10, ejerce configuraciones sobre un puerto Ethernet o interfaz del dispositivo.

En los campos *Interfaz* y *Gateway* se define sobre qué puerto se desea trabajar y la dirección IP, con su máscara de subred, que se desee asignar. Para ello se requiere pulsar el botón *Agregar*.

El campo de texto seguido de la etiqueta *Maestro* permite definir si el puerto posee a otro como maestro, en caso afirmativo se debe escribir el puerto que cumple las funciones de maestro, caso contrario, se establece la opción predeterminada *none* o ninguno.

Además es posible habilitar o deshabilitar el puerto a partir de la lista de *Estado*, así como también se puede cambiar el nombre de la interfaz en el campo de texto *Nombre*. Estas acciones se llevan a cabo al presionar el botón *Modificar*.

Por último, el botón *Actualizar Tabla* imprime, en el terminal, la tabla que lista los puertos existentes junto con sus configuraciones.



Figura 4.10. Ventana “*Interfaces*”.

b. Direccionamiento estático

Desde esta opción se puede acceder a una nueva ventana “*Dir. Estático*”, la cual facilita definir el *gateway* de una red. La interfaz se puede observar en la figura 4.11.



Figura 4.11. Interfaz de la ventana “*Dir. Estático*”

Para finalizar, se cuenta con una sección que permite al usuario habilitar, deshabilitar o borrar una de las configuraciones. Para ello debe ingresar el número con la cual se identifica a la regla en la tabla.

c. Direccionamiento dinámico

El enrutamiento dinámico OSPF se puede realizar a través de la ventana que se muestra en la figura 4.12, aquí se definen las diferentes redes por medio de áreas. En Mikrotik el área predeterminada y que siempre debe ser utilizada es la *backbone*, sin embargo, se pueden crear nuevas áreas que se comuniquen con ella.



Figura 4.12. Interfaz de la ventana "OSPF"

Los campos que solicita la ventana son la red y el área a la que se desea asignar, por lo que se debe escoger, de una lista desplegable, si se mantiene la *backbone* o se crea una nueva área, para lo que se debe establecer un nombre y un número de identificación *Area-id*.

Como complemento, se cuenta con la posibilidad de habilitar, deshabilitar y borrar las reglas configuradas sobre el equipo tanto de áreas como redes, para ello se tiene que seleccionar de la lista desplegable con etiqueta *Seleccione* cualquiera de las dos opciones.

d. VLANs

La ventana que se observa en la figura 4.13, requiere especificar tres parámetros: el nombre que llevará la VLAN a crear, el número de identificación *VLAN Id* y por último, a cual interfaz pertenecerá. Al igual que en las demás ventanas del programa, una sección permite modificar una regla de la tabla correspondiente.



Figura 4.13. Interfaz de la ventana “VLANs”

e. Servidor DHCP

Esta interfaz muestra los campos requeridos para establecer un servidor DHCP en un router MikroTik y está dividida en tres paneles:

- **DHCP-Server Network:** en él se crea la red y se establece el *gateway* de la misma.
- **Pool:** especifica el rango de direcciones de la red que van a ser asignados automáticamente.
- **DHCP-Server:** establece el servidor DHCP y permite escoger el rango de direcciones IP, según su nombre, para asignarlos a una interfaz. Además, posibilita definir el tiempo que el equipo almacenará los datos de todos los clientes al que el servidor DHCP asignó una IP automáticamente.

En la parte inferior, el botón *Actualizar Tablas* imprime en el terminal las tablas respectivas de cada una de las configuraciones.

Por último, cada panel consta de una sección que facilita habilitar, deshabilitar o borrar un campo de la tabla respectiva. Para ello, se debe escribir el número de la regla a alterar.

En la figura 4.14 se muestra la ventana de la configuración del servidor DHCP.

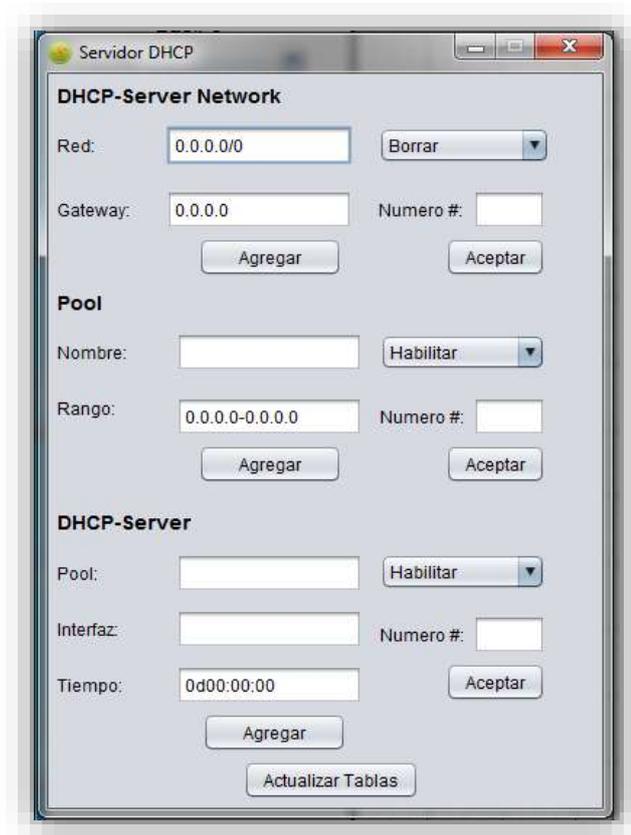


Figura 4.14. Ventana “*Servidor DHCP*”.

f. Cliente DHCP

La configuración de un cliente DHCP en un router MikroTik requiere únicamente la habilitación de esta opción sobre una interfaz, sea esta física (puerto Ethernet) o lógica (VLAN), razón por la cual la ventana “*Cliente DHCP*”, que se puede observar en la figura 4.15, solicita solamente este campo.

Al igual que en las ventanas anteriores, es posible habilitar, deshabilitar o borrar una regla en la sección pertinente.



Figura 4.15. Ventana “*Cliente DHCP*”.

g. NAT

Desde la ventana “*NAT*”, que se muestra en la figura 4.16, se realizan configuraciones que permiten a los anfitriones o *hosts* utilizar un conjunto de direcciones IP privadas para las comunicaciones locales y que éstas sean indiferentes al establecer una comunicación hacia la red de área local LAN. Es decir, la puerta de enlace NAT realiza la reescritura de la dirección IP al transmitir paquetes desde y hacia la LAN.

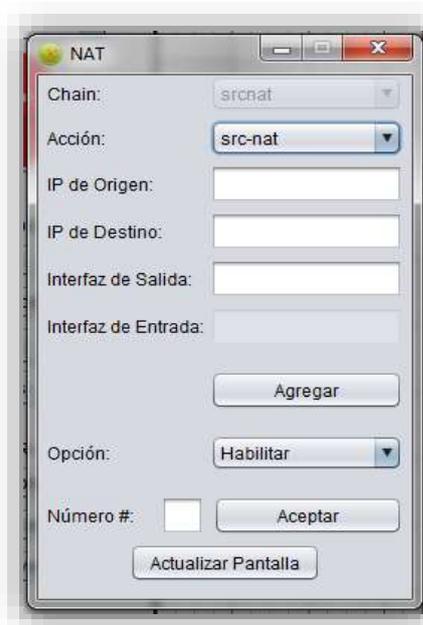


Figura 4.16. Ventana “*NAT*”.

En los equipos MikroTik se debe escoger un tipo de acción para configurar el NAT: src-nat, dst-nat y masquerade.

- **Src-nat:** se aplica a los paquetes que se originan a partir de una red privada, en el campo *IP de Origen* se debe colocar la dirección desde donde partirá la información, mientras en el campo *IP de Destino* se escribe la dirección que se desea alcanzar, por último en el campo *Interfaz de Salida* se coloca la interfaz del equipo donde se realiza la configuración.

- **Dst-nat:** esta acción se relaciona con src-nat ya que aquí su configuración se la puede describir como un espejo, en el campo *IP de Origen* se debe indicar la dirección de llegada de los paquetes, mientras en el campo *IP de Destino* se especifica la dirección IP de origen, por último en el campo *Interfaz de Entrada* se coloca la interfaz del equipo donde se realiza la configuración.

Hay que destacar que en estas configuraciones es imprescindible contar con direcciones IPs fijas.

- **Masquerade:** cuando se requiere de la configuración del NAT sin especificar la dirección IP de destino se utiliza la acción masquerade. En el campo *IP de Origen* se debe escribir la dirección de partida de la información y en el campo *Interfaz de Salida* el puerto a configurar.

4.3.3.4. Switch

Esta ventana, que se puede observar en la figura 4.17, presenta características similares a “Router”, permitiendo mostrar solo los nodos tipo *switch* de un proyecto. La diferencia primordial radica en que estos dispositivos cuentan con el sistema operativo SwOS, que no soporta el protocolo Telnet, por lo que únicamente se puede establecer una comunicación con el equipo vía HTTP haciendo uso del navegador predeterminado del computador.

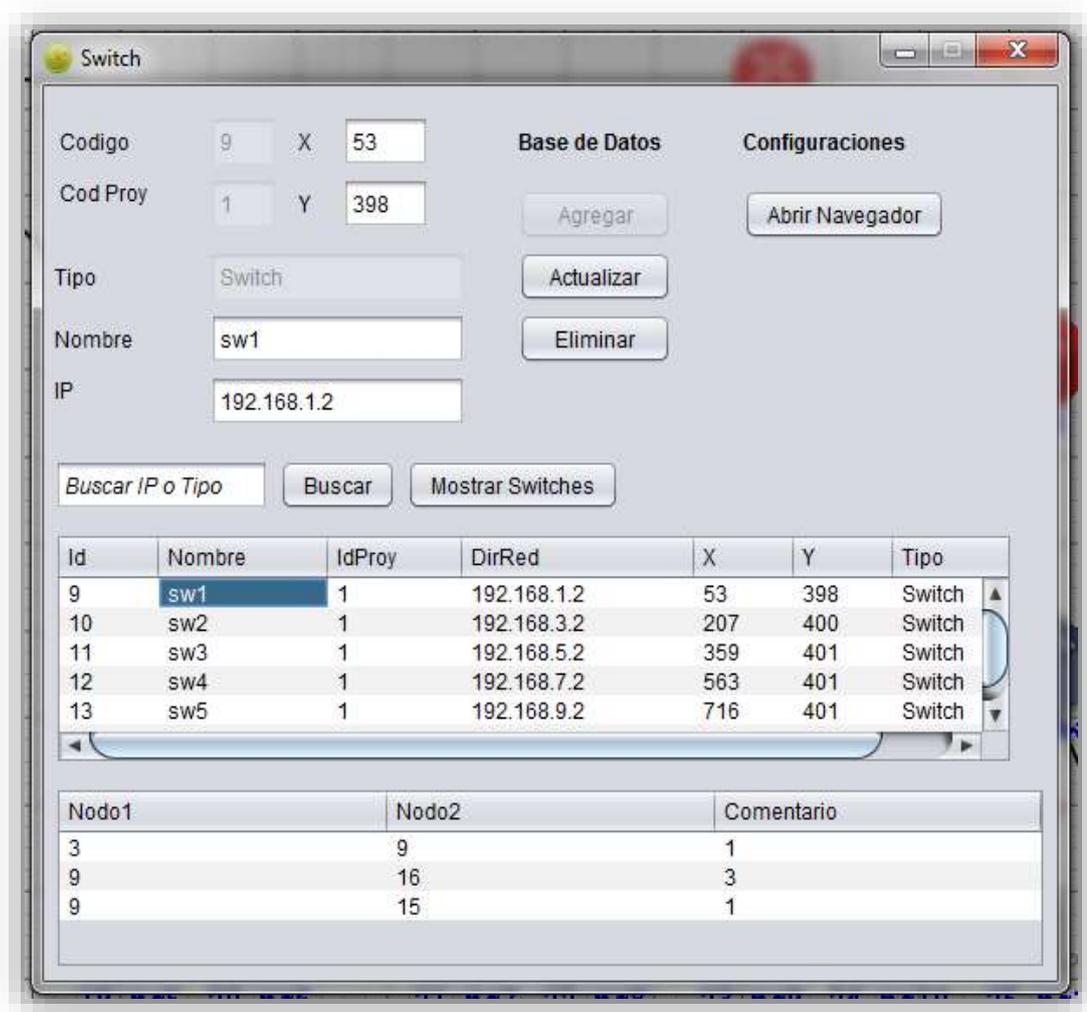


Figura 4.17. Ventana “Switch”.

4.3.3.5. Access point

La ventana “Access Point” emerge cuando el usuario presiona el símbolo del punto de acceso en el área de trabajo de la ventana principal. Esta interfaz funciona de manera parecida a las ventanas “Router” y “Switch”, sin embargo su tabla de información tiene la restricción de enlistar los nodos de tipo *access point* únicamente.

Si bien en el laboratorio no se encuentra implementado ningún punto de acceso y consecuentemente no es posible su configuración real, ENDS incluye este nodo de red para propósitos de diseño topológico; y, si en un futuro se dispone de un equipo de este tipo, es posible acceder a su panel de configuración mediante el botón *Abrir Navegador*.

En la figura 4.18 se exhibe la ventana “Access Point”.

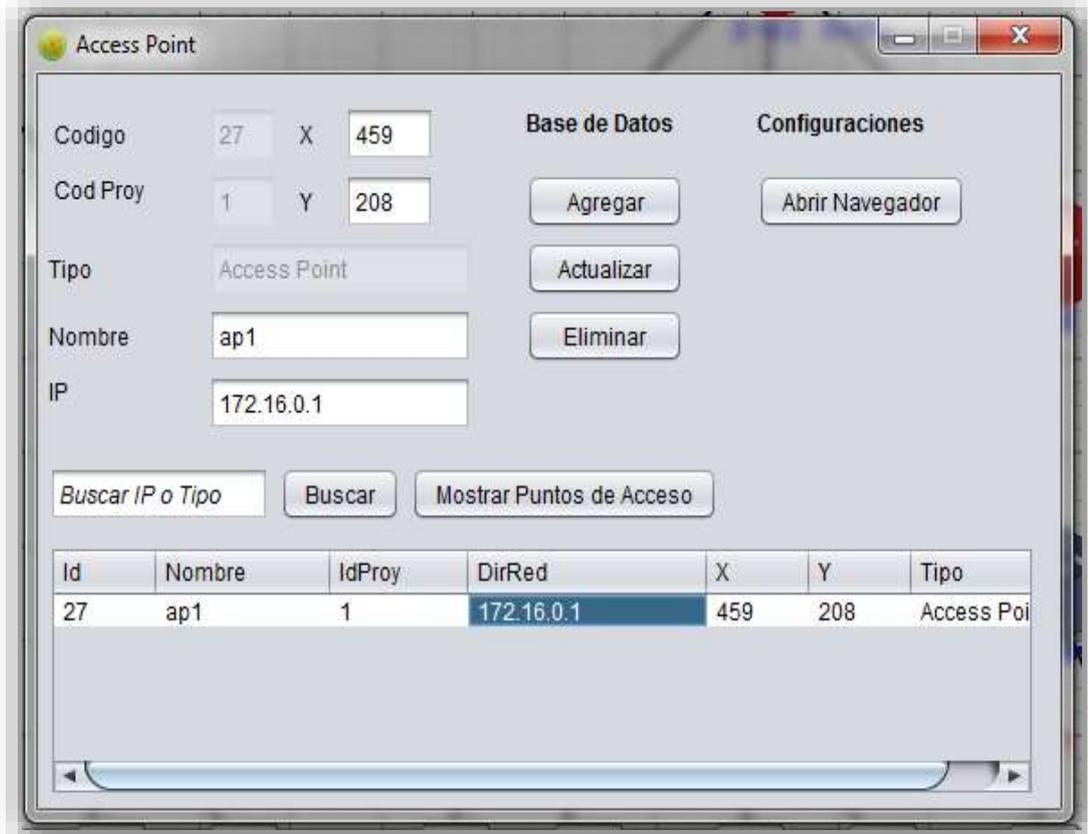


Figura 4.18. Ventana “Access Point”.

4.3.3.6. Computador

Al momento de crear, o presionar, un computador en el área de trabajo, surge la ventana “PC”, que se presenta en la figura 4.19. En ella se expone una interfaz de funcionamiento semejante a las de los demás nodos de red. No obstante, el *software* de virtualización no es capaz de configurar un equipo de esta naturaleza, razón por la cual es posible modificar los campos de diseño únicamente, es decir: su nombre, posición en el área de trabajo y dirección IP.

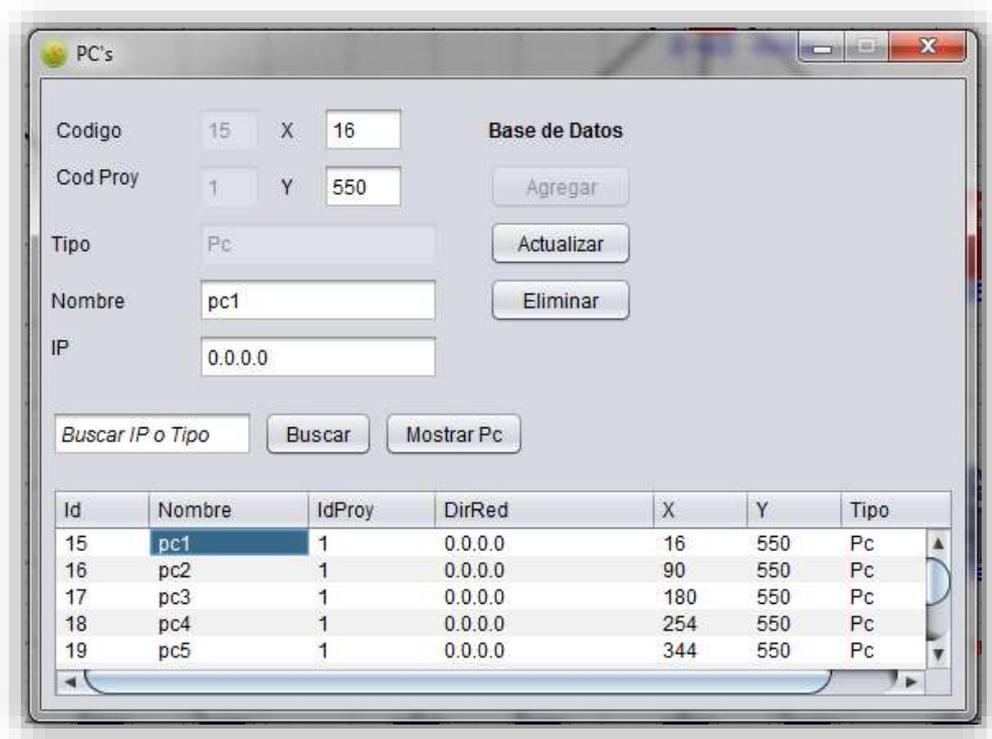


Figura 4.19. Ventana "PC".

4.3.4. Eliminar

4.3.4.1. Eliminar un nodo

Desde esta ventana, que se presenta en la figura 4.20, se solicita al usuario digitar el número de identificación del nodo que se desee eliminar de cualquier proyecto.

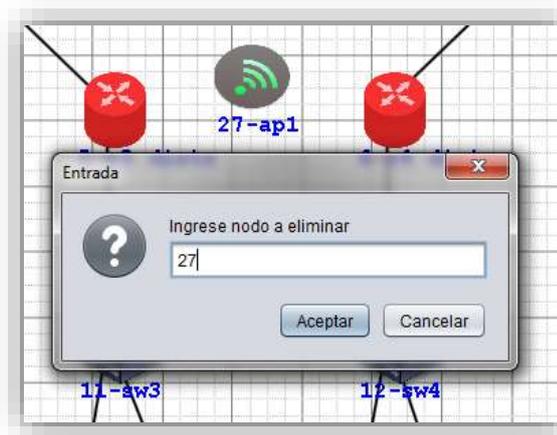


Figura 4.20. Eliminación de un nodo.

4.3.4.2. Eliminar un enlace

La interfaz que se observa en la figura 4.21 permite eliminar un enlace entre dos nodos solicitando el ingreso de los números de identificación de cada uno de ellos en los campos de textos respectivos.



Figura 4.21. Ventana “Eliminar Enlaces”.

4.3.4.3. Eliminar un proyecto

El botón *Eliminar Proyecto* despliega una ventana de diálogo que solicita confirmar si el usuario desea realmente eliminar el proyecto actual en su totalidad. Esta ventana emergente se muestra en la figura 4.22.

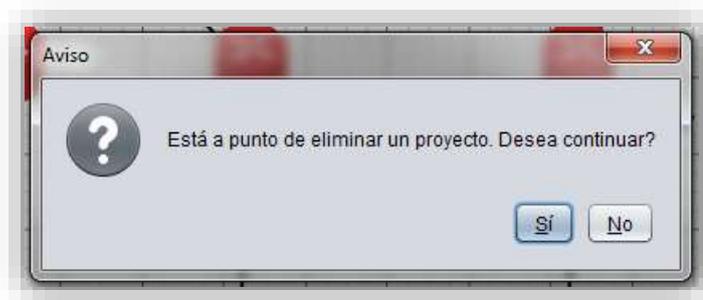


Figura 4.22. Confirmación para eliminar un proyecto.

4.3.5. Comunicación: terminal Telnet

La comunicación de ENDS con los equipos MikroTik que operan el sistema RouterOS se realiza a través del protocolo Telnet utilizando el puerto estandarizado 23. El programa actúa como un cliente de este protocolo y emula un terminal similar al *shell* de los sistemas Unix o al *cmd* (*Command Prompt*) de los sistemas Windows.

El panel de comunicación nos permite acceder a la ventana “*Terminal Telnet*”, desde esta interfaz es posible establecer una comunicación Telnet a cualquier equipo que se encuentre en la red.

En primer lugar se debe ingresar la dirección IP del dispositivo a conectar en el campo respectivo. Al pulsar el botón *Conectar*, previo a comunicarse con el equipo, ENDS busca en la base de datos los campos de *usuario* y *contraseña* correspondientes a la dirección IP ingresada, en caso de que ésta no se encuentre, solicita el ingreso de dicha información para permitir el acceso a la unidad.

Posteriormente, dependiendo si hubo éxito al establecer la comunicación, se activará una etiqueta, junto al botón *Conectar*, que indicará el estado de la misma.

Por otra parte, toda la información, tanto de entrada como de salida, es presentada en un área de texto simple. Esto quiere decir que la presentación del texto no contiene formato, sino que solamente exhibe caracteres.

Por último, en la parte inferior de la interfaz, se encuentra un campo de texto que permite al usuario escribir comandos y enviarlos al dispositivo al presionar la tecla Intro del teclado.

Además, como función adicional, se dispone de una sección que posibilita el ingreso de una dirección IP con la cual se desea probar conectividad mediante el botón *Ping*. Esta sección se habilita sólo después de que el equipo MikroTik haya permitido el acceso remoto.

En la figura 4.23 se puede apreciar la ventana “*Terminal Telnet*”.

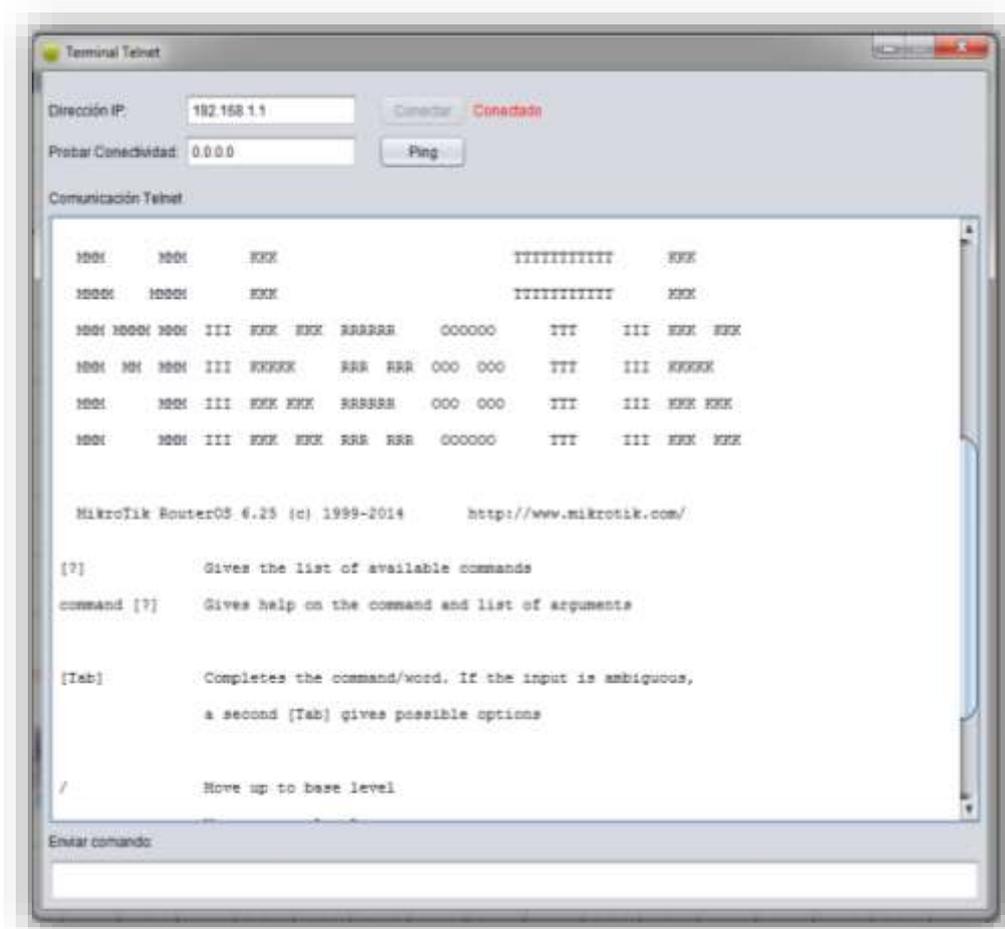


Figura 4.23. Terminal Telnet.

4.3.6. Acerca de

El panel de la figura 4.24 enseña información sobre la versión del *software* y sus programadores.

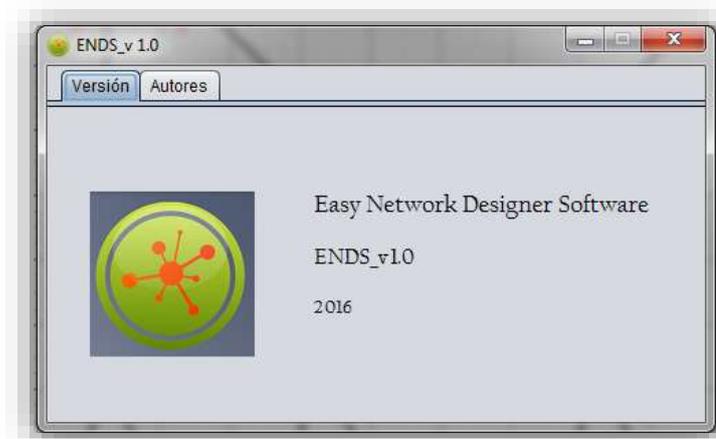


Figura 4.24. Ventana “Acerca De”.

4.3.7. Opciones

En la barra de menú, dentro de *Opciones*, es posible escoger, ya sea desplegar información de ayuda al usuario, o salir del *software*.

4.3.7.1. Ayuda

Al seleccionar la opción *Ayuda* se dará inicio al lector de archivos .pdf del ordenador y se abrirá el manual de usuario.

4.3.7.2. Salir

Antes de cerrar el programa, aparece un panel de diálogo (véase figura 4.25) que solicita confirmar la salida de ENDS.

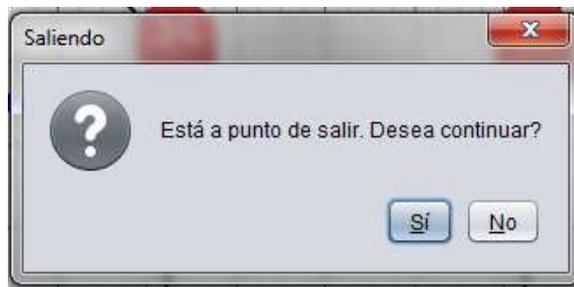


Figura 4.25. Confirmación de salida.

4.4. Comandos MikroTik

4.4.1. Interfaces

Los comandos utilizados para esta configuración son los de la tabla 4.1.

Tabla 4.1. Comandos para la configuración de interfaces de equipos MikroTik.

COMANDO	DESCRIPCIÓN
<code>ip address add address=0.0.0.0/0 interface=etherx</code>	Agrega una dirección IP a una interfaz del equipo.
<code>ip address print</code>	Muestra las direcciones IP agregadas al equipo.
<code>ip address enable</code>	Habilita una dirección IP.
<code>ip address disable</code>	Deshabilita una dirección IP.
<code>ip address remove</code>	Elimina una dirección IP.

4.4.2. Ping

Para comprobar una conexión con otro dispositivo se emplea el comando de la tabla 4.2.

Tabla 4.2. Comando para realizar un ping en equipos MikroTik.

COMANDO	DESCRIPCIÓN
<code>ping 0.0.0.0 count=4</code>	Realiza un ping a una dirección IP.

4.4.3. Enrutamiento estático

Para realizar este tipo de configuración en los equipos Mikrotik, se utilizan los comandos de la tabla 4.3.

Tabla 4.3. Comandos para enrutamiento estático en equipos MikroTik.

COMANDO	DESCRIPCIÓN
<code>ip route add dst-address=0.0.0.0/0 gateway=0.0.0.0</code>	Agrega una ruta de salida a la red especificada.
<code>ip route print</code>	Imprime las rutas de red agregadas.
<code>ip route enable</code>	Habilita una ruta (<i>gateway</i>) de red.
<code>ip route disable</code>	Deshabilita una ruta (<i>gateway</i>) de red.
<code>ip route remove</code>	Elimina una ruta (<i>gateway</i>) de red.

4.4.4. VLANs

En la tabla 4.4 se muestran las líneas usadas para configurar VLANs.

Tabla 4.4. Comandos para crear VLANs en equipos MikroTik.

COMANDO	DESCRIPCIÓN
<code>interface VLAN add name=nombre VLAN-id=numeroID interface=etherx disabled=no</code>	Añade una VLAN al equipo.
<code>interface VLAN print</code>	Muestra las VLANs existentes.
<code>interface VLAN enable</code>	Habilita una VLAN.
<code>interface VLAN disable</code>	Deshabilita una VLAN.
<code>interface VLAN remove</code>	Elimina una VLAN.

4.4.5. Enrutamiento dinámico OSPF

Para la configuración OSPF se emplean los comandos que se listan en la tabla 4.5.

Tabla 4.5. Comandos para enrutamiento dinámico OSPF en equipos MikroTik.

COMANDO	DESCRIPCIÓN
<code>routing ospf area add name=<i>nombre</i> area-id=<i>0.0.0.0</i></code>	Añade un área a la <i>backbone</i> .
<code>routing ospf network add network=<i>0.0.0.0/0</i> area=<i>nombre</i></code>	Agrega una red a un área.
<code>routing ospf lsa print</code>	Imprime las listas OSPF.
<code>routing ospf area print</code>	Imprime las áreas creadas.
<code>routing ospf network print</code>	Imprime las redes creadas.
<code>routing ospf neighbor print</code>	Muestra las áreas vecinas a la <i>backbone</i> .
<code>routing ospf area enable</code> <code>routing ospf area disable</code> <code>routing ospf area remove</code>	Habilita, deshabilita y elimina áreas.
<code>routing ospf network enable</code> <code>routing ospf network disable</code> <code>routing ospf network remove</code>	Habilita, deshabilita y elimina redes creadas.

4.4.6. Cliente DHCP

Para habilitar un cliente DHCP se hace uso de las líneas que se presentan en la tabla 4.6.

Tabla 4.6. Comandos para habilitar un cliente DHCP en equipos MikroTik.

COMANDO	DESCRIPCIÓN
<code>ip dhcp-client add interface=<i>etherx</i> disabled=<i>no</i></code>	Configura una interfaz como un cliente DHCP.
<code>ip dhcp-client print</code>	Muestra los clientes DHCP del equipo.
<code>ip dhcp-client enable</code>	Habilita un cliente DHCP.
<code>ip dhcp-client disable</code>	Deshabilita un cliente DHCP.
<code>ip dhcp-client remove</code>	Elimina un cliente DHCP.

4.4.7. Servidor DHCP

Los comandos que se muestran en la tabla 4.7 permiten configurar un servidor DHCP.

Tabla 4.7. Comandos para configurar un servidor DHCP en equipos MikroTik.

COMANDO	DESCRIPCIÓN
<code>ip dhcp-server network add address=0.0.0.0/0 gateway=0.0.0.0</code>	Agrega una nueva red para la asignación de direcciones.
<code>ip dhcp-server network print</code>	Imprime las direcciones de red añadidas.
<code>ip dhcp-server network enable ip dhcp-server network disable ip dhcp-server network remove</code>	Habilita, deshabilita y elimina redes creadas.
<code>ip pool add name=nombre ranges=0.0.0.0- 0.0.0.0</code>	Configura un rango de direcciones para ser asignadas.
<code>ip pool print</code>	Muestra los rangos de direcciones configurados.
<code>ip pool enable ip pool disable ip pool remove</code>	Habilita, deshabilita y elimina rangos de direcciones.
<code>ip dhcp-server add interface=etherx address-pool=nombrePool lease-time=0d disabled=no</code>	Crea un servidor DHCP.
<code>ip dhcp-server print</code>	Imprime los servidores DHCP existentes.
<code>ip dhcp-server enable ip dhcp-server disable ip dhcp-server remove</code>	Habilita, deshabilita y elimina un servidor DHCP.

4.4.8. NAT

La configuración NAT requiere de los comandos que se muestran en la tabla 4.8.

Tabla 4.8. Comandos para configurar un NAT en equipos MikroTik.

COMANDO	DESCRIPCIÓN
<code>ip firewall nat add chain=srcnat action=src-nat to-address=0.0.0.0 src-address=0.0.0.0 out-interface=etherx</code>	Añade a una interfaz un <i>source</i> NAT o srcnat.
<code>ip firewall nat add chain=dstnat action=dst-nat to-address=0.0.0.0 dst-address=0.0.0.0 in-interface=etherx</code>	Añade a una interfaz un <i>destination</i> NAT o dstnat.
<code>ip firewall nat add chain=srcnat action=masquerade src-address=0.0.0.0 out-interface=etherx</code>	Añade a una interfaz un NAT tipo masquerade.
<code>ip firewall nat print</code>	Muestra las configuraciones NAT creadas en el equipo.
<code>ip firewall nat enable</code>	Habilita una regla NAT.
<code>ip firewall nat disable</code>	Deshabilita una regla NAT.
<code>ip firewall nat remove</code>	Elimina una regla NAT.

CAPÍTULO 5

RESULTADOS

Con razón de explicar cómo trabaja ENDS, el capítulo a seguir detalla una guía paso a paso destinada a orientar, al usuario del programa, el proceso para realizar un diseño de red y posteriormente efectuar la configuración de los equipos que la constituyen.

Este apartado abarca la selección de los distintos elementos de red, su distribución en la interfaz, el almacenamiento del proyecto en la base de datos, la creación de enlaces entre los nodos y la configuración de parámetros en cada equipo, ya sea mediante el uso del navegador web o el terminal de comunicaciones Telnet.

Por último, se presentan imágenes que reflejan el correcto funcionamiento de la red diseñada.

5.1. Planteamiento de la red

Siguiendo un esquema de red del laboratorio similar al presentado en el capítulo 3 anteriormente, la red a diseñar posee: un *router* en la capa de núcleo; enlazados a él, dos *routers* en la capa de distribución; y finalmente, un *switch* para cada *router* de distribución en la capa de acceso.

En las tablas 5.1 y 5.2 a continuación, se especifican las direcciones de todas las subredes, las puertas de enlace de las mismas, y las redes locales virtuales a las que pertenecen.

Tabla 5.1. Tabla de direccionamiento de la red.

VLAN	Dirección	Rango de host utilizables	Broadcast	Gateway
31	10.10.1.0/30	10.10.1.1-10.10.1.2	10.10.1.3	-
32	10.10.2.0/30	10.10.2.1-10.10.2.2	10.10.2.3	-
21	192.168.10.0/24	192.168.10.1- 192.168.10.254	192.169.10.255	192.168.10.1
22	192.168.11.0/24	192.168.11.1- 192.168.11.254	192.169.10.255	192.168.11.1
10	192.168.1.0/24	192.168.1.1-192.168.1.254	192.168.1.255	192.168.1.1
11	192.168.2.0/24	192.168.2.1-192.168.2.254	192.168.2.255	192.168.2.1
10	192.168.3.0/24	192.168.3.1-192.168.3.254	192.168.3.255	192.168.3.1
11	192.168.4.0/24	192.168.4.1-192.168.4.254	192.168.4.255	192.168.4.1

Tabla 5.2. Rangos de direccionamiento fijo y dinámico de cada subred.

VLAN	Subred	Rangos	
		IPs Fijas	IPs Dinámicas
21	192.168.10.0/24	192.168.10.1- 192.168.10.99	192.168.10.100- 192.168.10.254
22	192.168.11.0/24	192.168.11.1- 192.168.11.99	192.168.11.100- 192.168.11.254
10	192.168.1.0/24	192.168.1.1-192.168.1.99	192.168.1.100-192.168.1.254
11	192.168.2.0/24	192.168.2.1-192.168.2.99	192.168.2.100-192.168.2.254
10	192.168.3.0/24	192.168.3.1-192.168.3.99	192.168.3.100-192.168.3.254
11	192.168.4.0/24	192.168.4.1-192.168.4.99	192.168.4.100-192.168.4.254

En la figura 5.1 se muestra la red que va a ser creada en el presente capítulo. Adicionalmente, en la figura 5.2, se pueden observar las redes locales virtuales de la misma red.

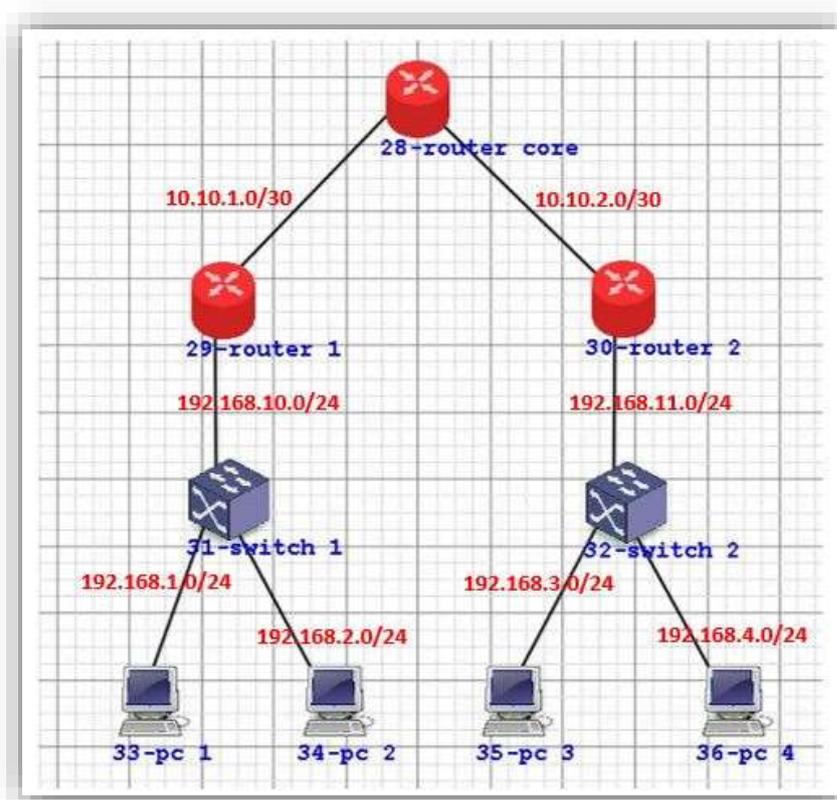


Figura 5.1. Diseño de la red.

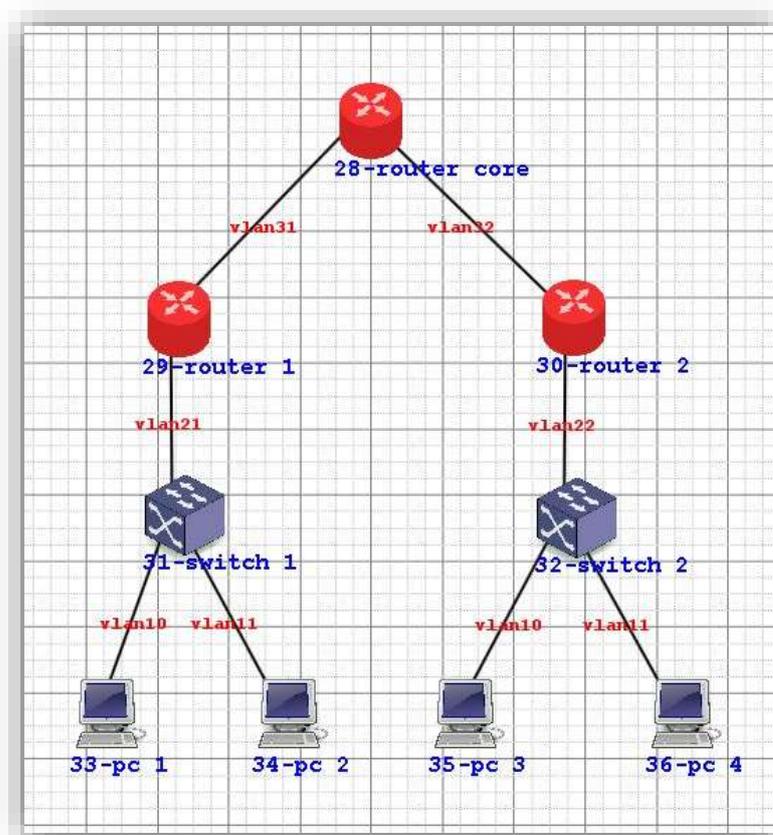


Figura 5.2. Redes locales virtuales de la red.

5.2. Diseño de la red

En primera instancia, se escoge el equipo que va a ser agregado al proyecto. Como se puede observar en la figura 5.3, en el panel *Equipo* se selecciona la opción *Router*, y luego se presiona en el área de trabajo el lugar donde se desea colocar el dispositivo. En la ventana que emerge ingresamos su nombre, en este caso, al ser el *router* de la capa de núcleo lo llamaremos “router core”. Esta última acción se muestra en la figura 5.4.

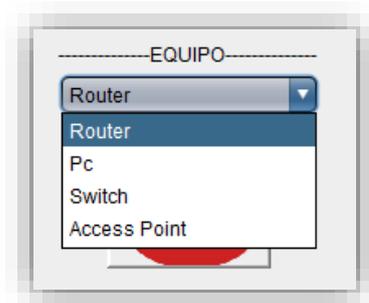


Figura 5.3. Selección del equipo a agregar a la interfaz.



Figura 5.4. Nombramiento del nodo de red.

A continuación, se presenta la ventana “*Router*”. Desde aquí se completa la información general del nodo recién creado; y, en caso de estar todo correcto, se guardan los cambios en la base de datos con el botón *Agregar*, como se observa en la figura 5.5. Luego, se abandona la pantalla y el área de trabajo se verá como la figura 5.6.

Figura 5.5. Ingreso de nuevo elemento en la base de datos.

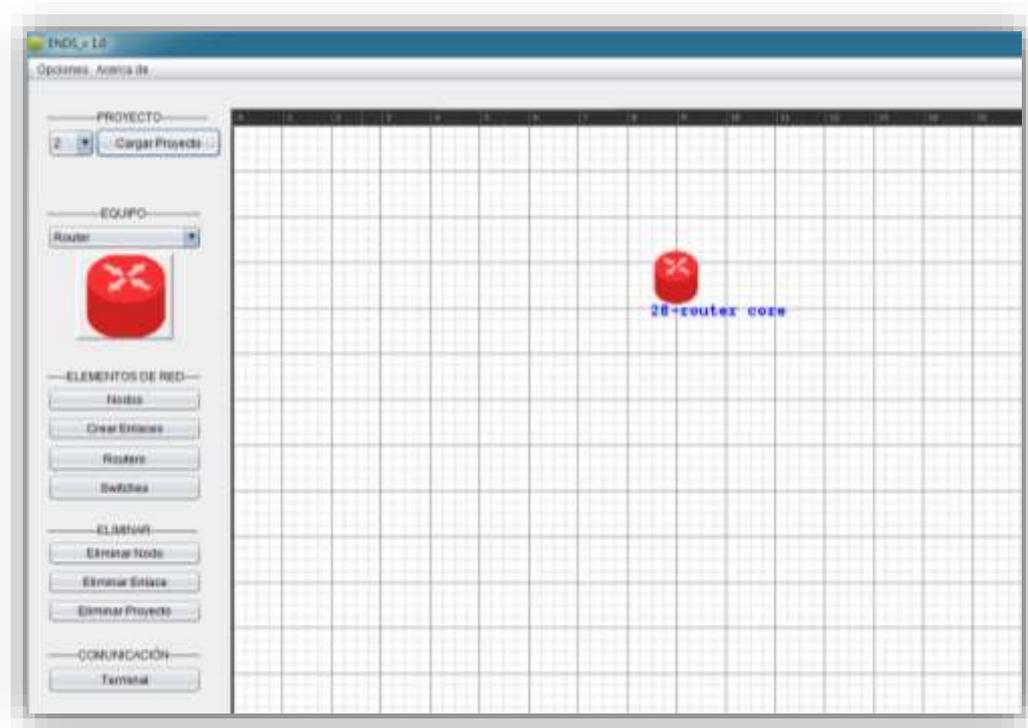


Figura 5.6. Creación de un nuevo nodo.

Se repite el proceso anterior para ingresar los demás *routers* que pertenecen a la red, como se ve en la figura 5.7.

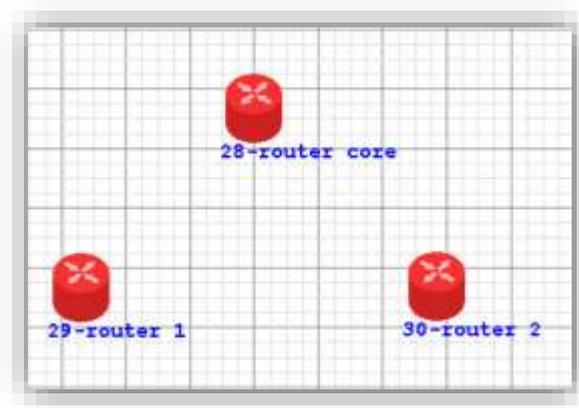


Figura 5.7. Adición de *routers* en el área de trabajo.

A continuación, de acuerdo a las figuras 5.8 y 5.9, se añaden los nodos faltantes tipo *switch* y PC de manera similar.

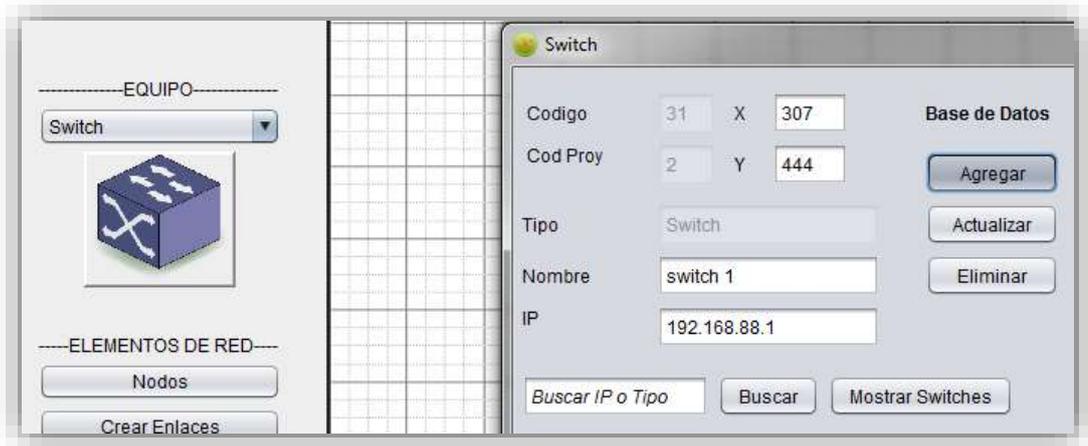


Figura 5.8. Ingreso de un nodo tipo *switch*.

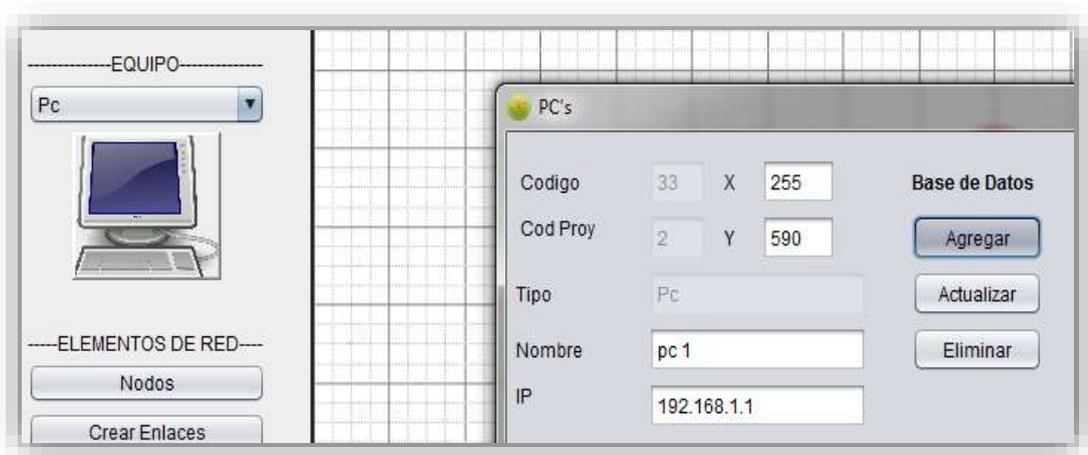


Figura 5.9. Ingreso de un nodo tipo PC.

Una vez completados los pasos anteriores el área de trabajo se dispone como en la figura 5.10.

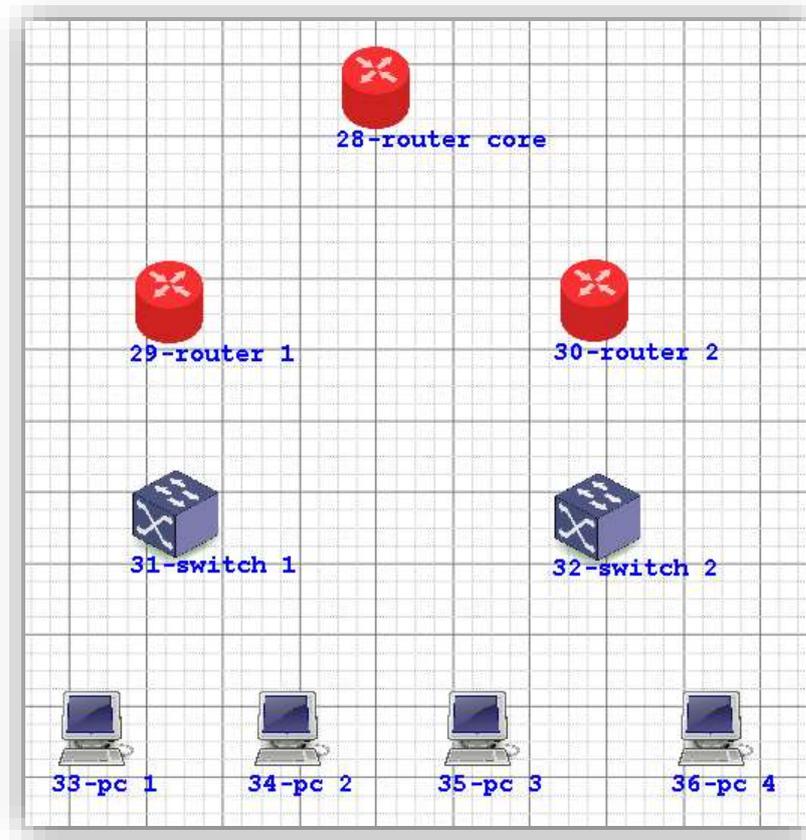


Figura 5.10. Distribución de los nodos de la red en el área de trabajo.

Se prosigue creando los enlaces entre los equipos, para ello, como se observa en la figura 5.11, se presiona el botón *Crear Enlaces* en la parte izquierda de ENDS.



Figura 5.11. Selección del botón *Crear Enlaces*.

Enseguida surgirá la ventana respectiva, en ella se digita el número de identificación de cada nodo a enlazar y opcionalmente, se escribe un comentario. Este proceso se muestra en las figuras 5.12 y 5.13.

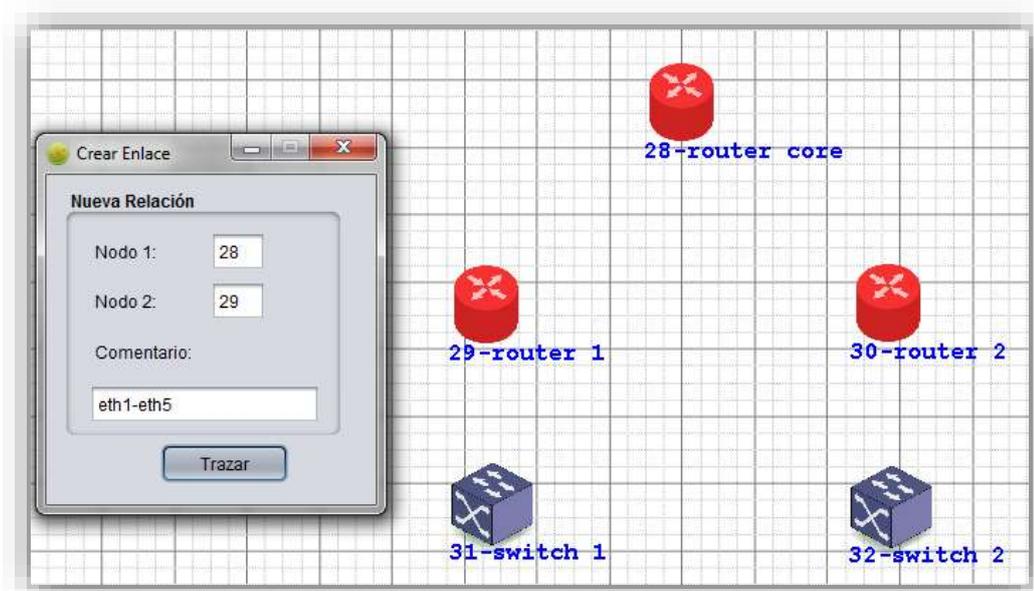


Figura 5.12. Creación de un enlace entre dos nodos.

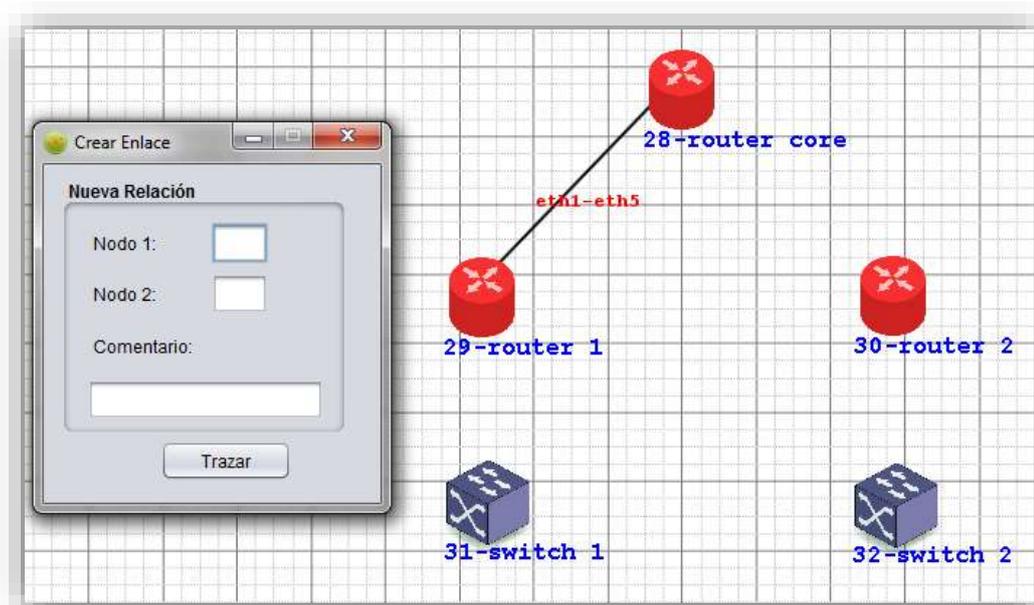


Figura 5.13. Visualización del enlace creado.

Como paso final en el diseño de la red, se crean los enlaces entre cada uno de los dispositivos. El diseño final se visualiza en la figura 5.14.

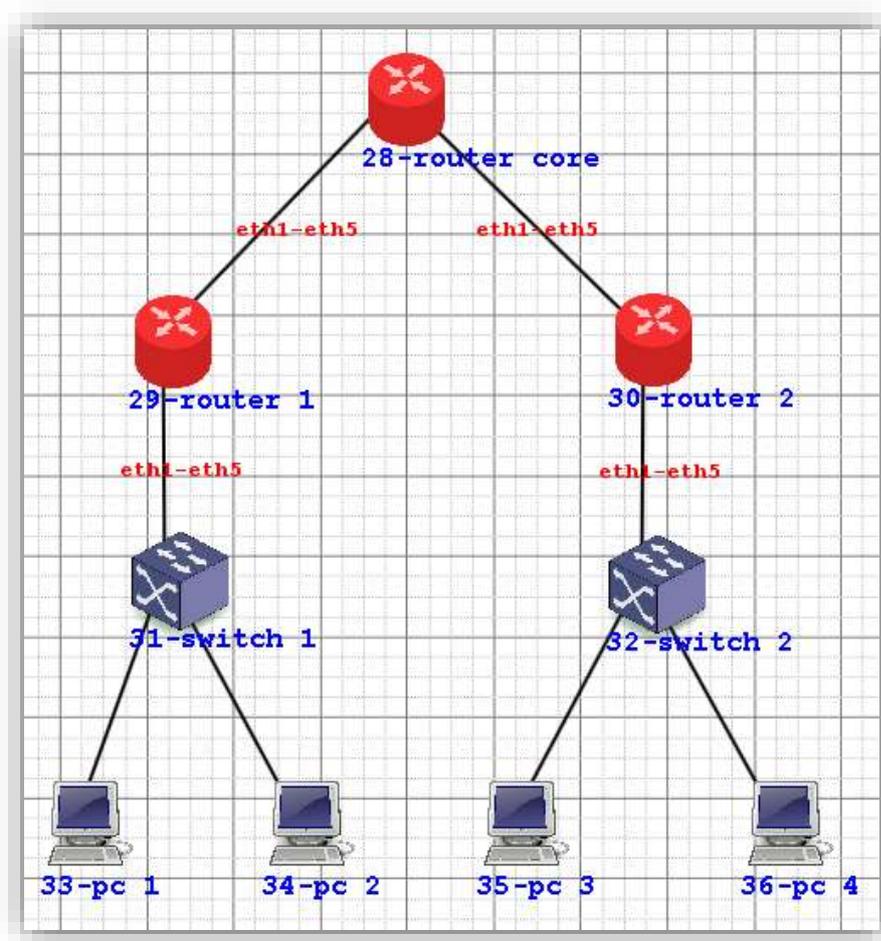


Figura 5.14. Diseño final de la red.

5.3. Configuraciones en los equipos

Al restaurar un equipo MikroTik a su configuración de fábrica, éste es accesible a través de la dirección IP 192.168.88.1, razón por la cual es necesario incluir a nuestro ordenador en la misma red.

En las figuras 5.15 y 5.16 se presenta el proceso de asignación de una dirección IP estática desde la configuración del adaptador de red en la ruta *Panel de control\Redes e Internet\Conexiones de red* de un computador que funciona con el sistema operativo Windows 7.



Figura 5.15. Propiedades de conexión de área local de Windows 7.

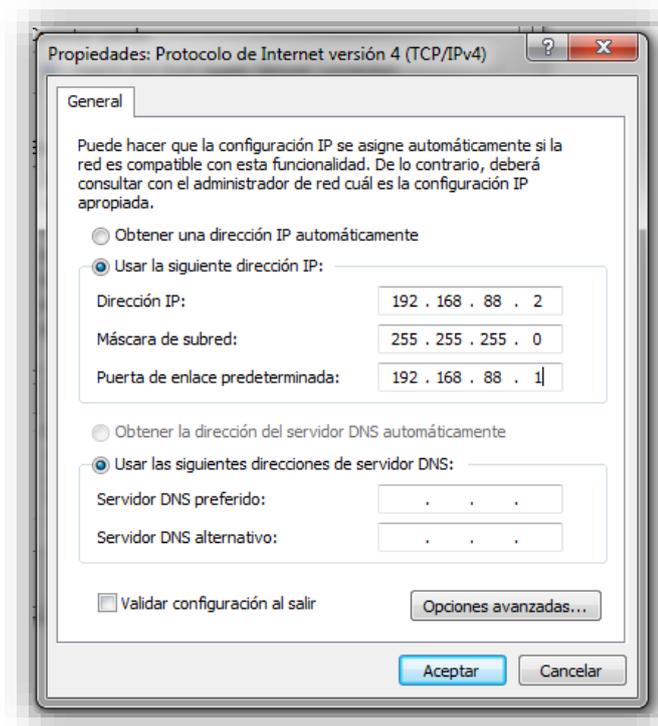


Figura 5.16. Cambio de dirección IP.

Previo a la configuración de los equipos, es necesario mencionar que para comunicarse con cada uno de ellos es primordial conectarse a través de un cable Ethernet a cualquier puerto libre.

5.3.1. Capa de acceso

Para la configuración del *switch*, se presiona el botón *Abrir Navegador*, que se observa en la figura 5.17, para iniciar el navegador predeterminado del computador y establecer una comunicación con el equipo.

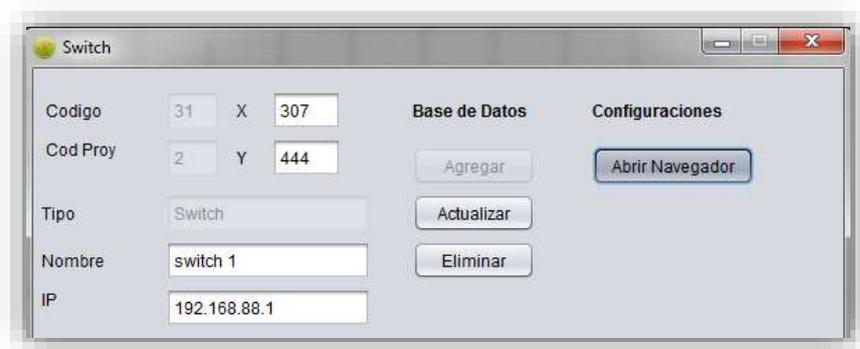


Figura 5.17. Ingreso a la configuración del *switch*.

Una ventana solicita especificar el usuario y contraseña del equipo, por defecto MikroTik establece el nombre de usuario como “admin” y la contraseña no contiene caracteres, es decir “”, como se observa en la figura 5.18

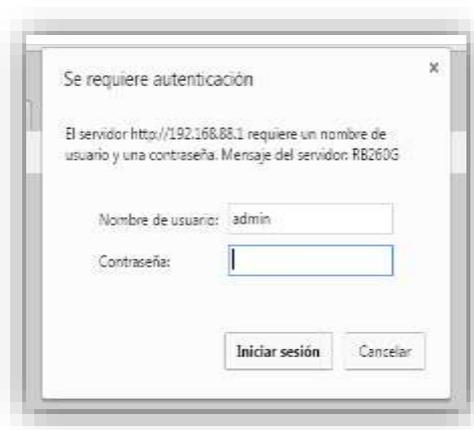


Figura 5.18. Autenticación de ingreso de un usuario.

Una vez autenticado, para crear VLANs en el dispositivo, se escoge la pestaña *VLANs*, y se presiona en *Append*, donde se añaden los parámetros que serán guardados al pulsar el botón *Apply All* como se ve en la figura 5.19. Luego, como muestra la figura 5.20, se selecciona la pestaña *VLAN*, en ella se indica el comportamiento de cada interfaz del *switch* y se presiona *Apply All*.



Figura 5.19. Creación de VLANs en MikroTik SwOS.

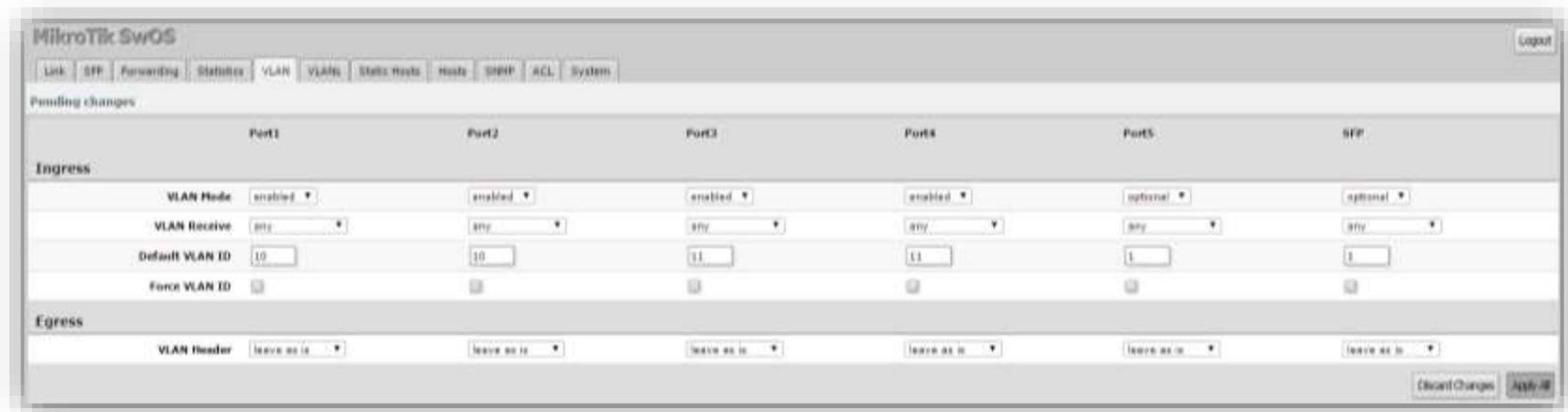


Figura 5.20. Configuración de parámetros en cada puerto.

Por último, desde la pestaña *System*, se cambia la dirección IP a la correspondiente de nuestra red, es decir para el “switch 1” se asigna la dirección 192.168.10.2 como se observa en la figura 5.21. A su vez se actualiza este campo en la base de datos de ENDS como se puede observar en la figura 5.22.

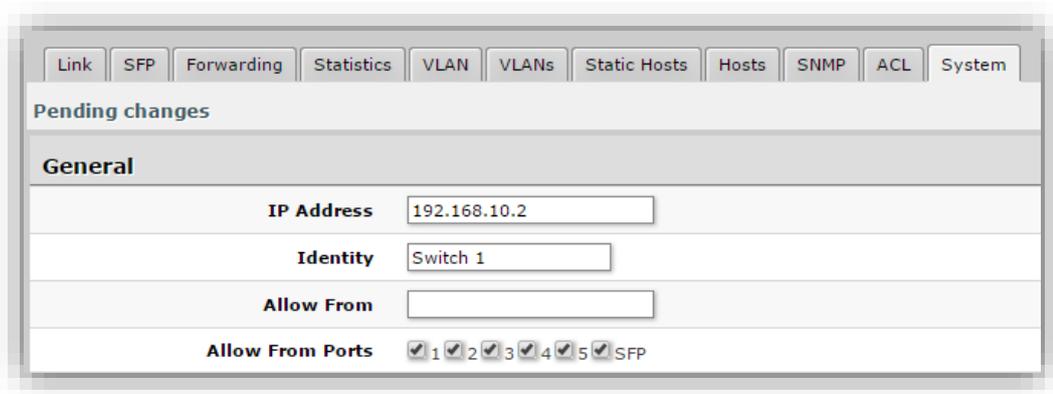


Figura 5.21. Cambio de dirección IP del Switch 1.



Figura 5.22. Actualización del campo IP del Switch 1.

En el caso del “switch 2” se repite la misma configuración anterior de VLANs; y, la dirección IP que se le asigna al equipo es 192.168.11.2, como se ve en las figuras 5.23 y 5.24.

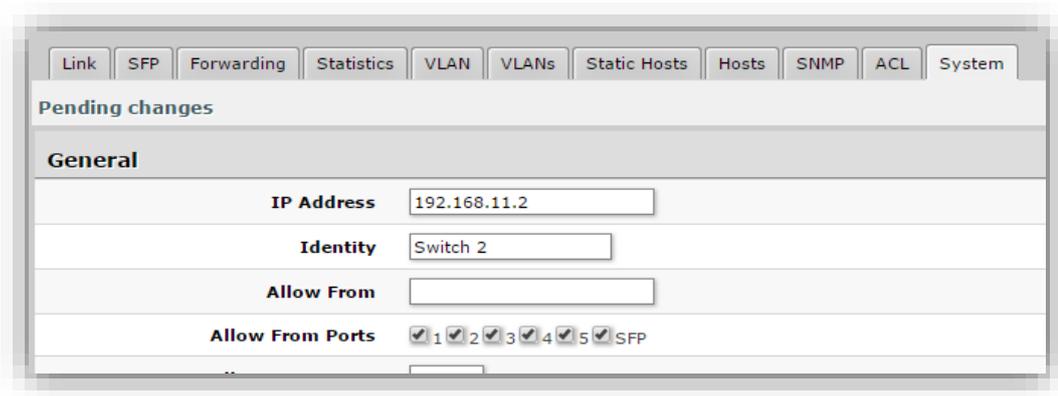


Figura 5.23. Cambio de dirección IP del “switch 2”.



Figura 5.24. Actualización del campo IP del “switch 2”.

5.3.2. Capa de distribución

En primer lugar, desde la ventana “Router” es necesario dirigirse a la configuración *Interfaces*, que mostrará la ventana correspondiente y el terminal Telnet. Ya que el equipo se restauró a su configuración de fábrica, se mostrará un mensaje de confirmación que informa sobre este hecho, como muestra la figura 5.25. Para aceptar se puede enviar cualquier carácter diferente de “r”, o simplemente presionar el botón *Actualizar Tablas*.

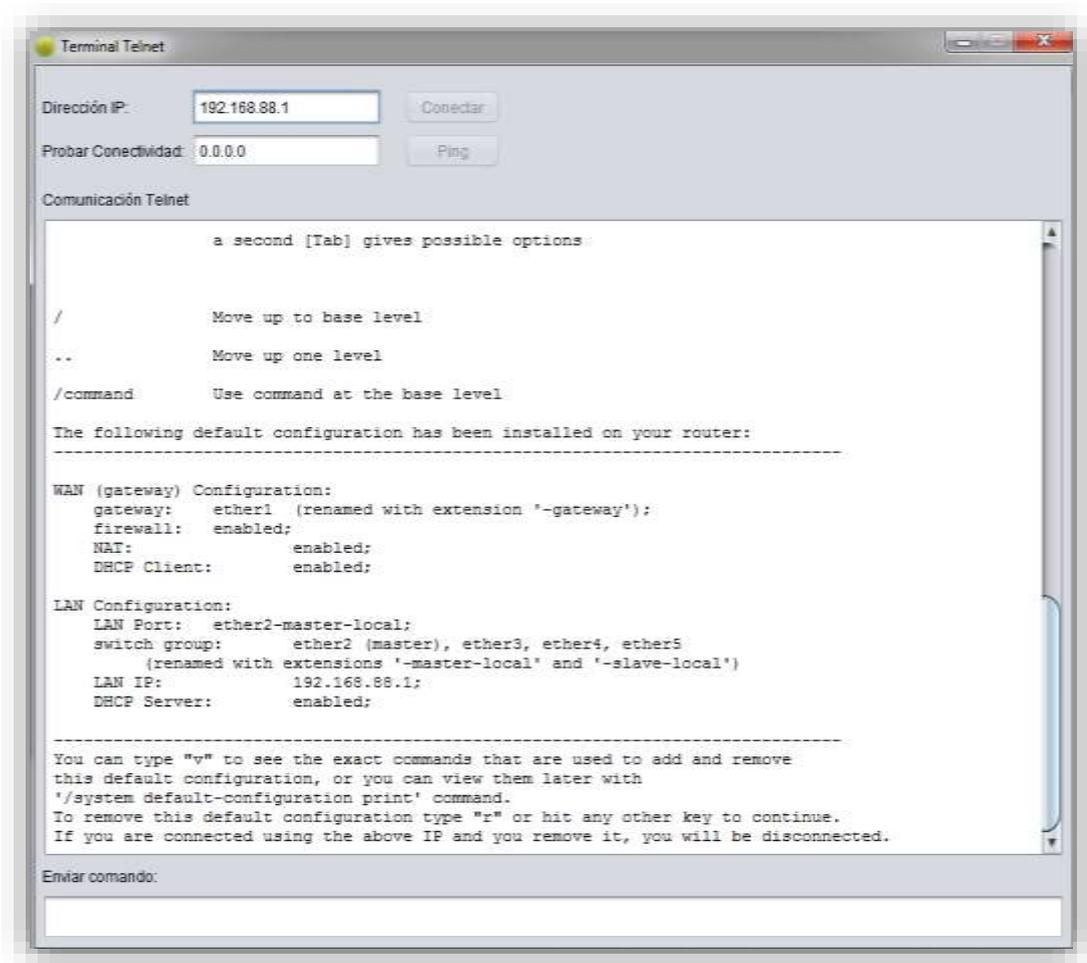


Figura 5.25. Mensaje de configuración de fábrica del *router*.

Ahora bien, en la ventana “*Interfaces*” se realiza el cambio de nombre para cada puerto del equipo. Al mismo tiempo, se especifica que la interfaz seleccionada no posee un puerto maestro. Los cambios ocurren al pulsar el botón *Modificar* como se ve en la figura 5.26.



Figura 5.26. Modificación de parámetros de una interfaz.

Para observar los cambios realizados en la pantalla del terminal, que se observa en la figura 5.27, se presiona el botón *Actualizar Tablas*.

```
[admin@MikroTik] > interface ethernet print
Flags: X - disabled, R - running, S - slave
#  NAME      MTU  MAC-ADDRESS  ARP      MASTER-PORT  SWITCH
0 R  ether1    1500 4C:5E:0C:08:8F:4A enabled    none         switch1
1 R  ether2    1500 4C:5E:0C:08:8F:4B enabled    none         switch1
2   ether3    1500 4C:5E:0C:08:8F:4C enabled    none         switch1
3   ether4    1500 4C:5E:0C:08:8F:4D enabled    none         switch1
4 R  ether5    1500 4C:5E:0C:08:8F:4E enabled    none         switch1
```

Figura 5.27. Visualización de la lista de interfaces Ethernet del router.

Después de haber cambiado los nombres y los estados de las interfaces, se procede a crear las redes virtuales locales de acuerdo a la figura 5.2. En la ventana “Router” se pulsa el botón *VLANs* y en la pantalla aparecerá la venta pertinente. En los campos respectivos, como se puede ver en la figura 5.28, se ingresa la información.

Para la interfaz ether1 se añaden las VLANs con id 10, 11, y 21, mientras que a la interfaz ether5 únicamente la VLAN con id 31. La tabla resultante se muestra en la figura 5.29.

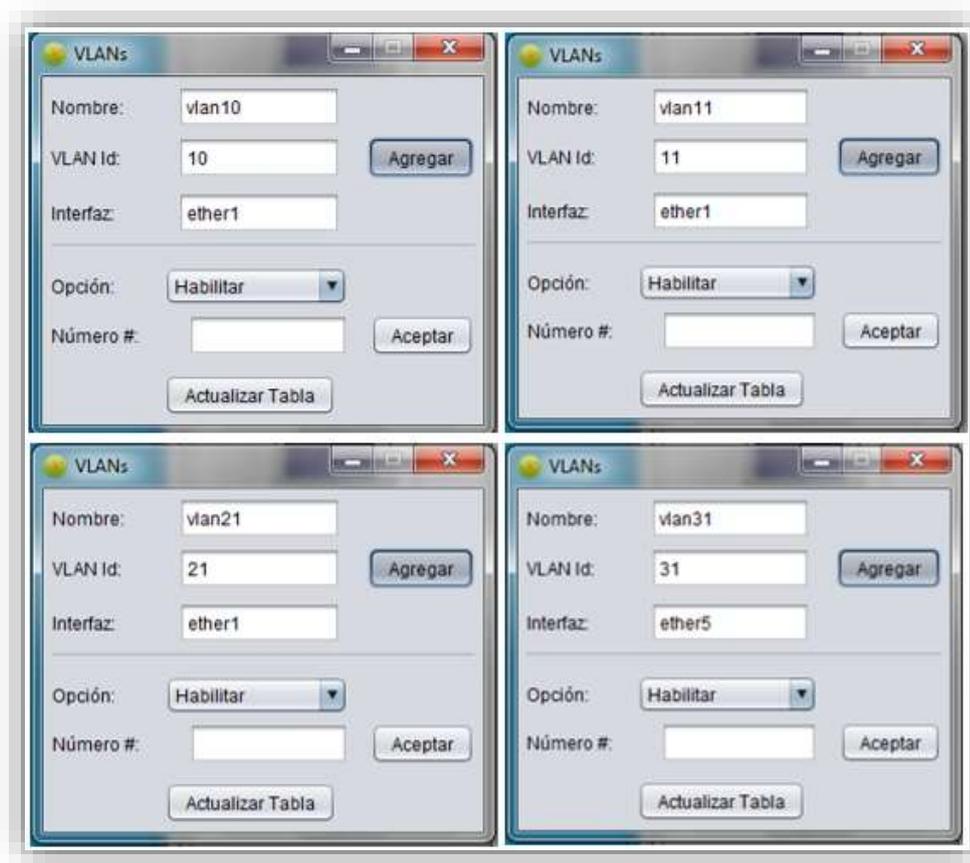


Figura 5.28. Adición de VLANs a las interfaces físicas del equipo.

```
[admin@MikroTik] > interface vlan print
interface vlan print

Flags: X - disabled, R - running, S - slave
#  NAME      MTU ARP  VLAN-ID INTERFACE
0 R  vlan10    1500 enabled  10 ether1
1 R  vlan11    1500 enabled  11 ether1
2 R  vlan21    1500 enabled  21 ether1
3 R  vlan31    1500 enabled  31 ether5
```

Figura 5.29. Listado de VLANs del “router 1”.

Luego de crear las VLANs desde la ventana “Router” se regresa a la configuración *Interfaces*, aquí se define el *gateway* y la máscara de subred que se relaciona a la interfaz física o lógica del equipo. En el caso de la red planteada, por cada VLAN existente en el “router 1” se añadió un *gateway*, como se observa en la figura 5.30.



Figura 5.30. Configuración de *gateway* para cada VLAN.

La presentación de las interfaces con su puerta de enlace se puede apreciar en la pantalla del terminal como muestra la figura 5.31.

```
ip address print

Flags: X - disabled, I - invalid, D - dynamic
#  ADDRESS          NETWORK          INTERFACE
0  ;;; default configuration
1  192.168.88.1/24   192.168.88.0    ether2
2  192.168.1.1/24   192.168.1.0     vlan10
3  192.168.2.1/24   192.168.2.0     vlan11
4  192.168.10.1/24  192.168.10.0    vlan21
5  10.10.1.2/30     10.10.1.0       vlan31
```

Figura 5.31. Presentación de *gateway* configurado para cada interfaz.

A continuación se añade un servidor de configuración dinámica de hosts (DHCP). La configuración de un servidor de esta índole en Mikrotik se realiza en tres secciones.

En primer lugar es necesario establecer las redes con sus puertas de enlace. Este paso lo realizamos en la sección *DHCP-Server Network* de la manera que se presenta en la figura 5.32.



Figura 5.32. Redes para los servidores DHCP.

Se prosigue añadiendo los rangos de direcciones IP, previamente definidos en la tabla 5.2, que van a ser asignados automáticamente. Este paso se lleva a cabo en la sección *Pool* de la misma ventana y se puede ver en la figura 5.33.

Para finalizar la configuración del servidor, se hace uso de la sección *DHCP-Server*. En el primer campo se debe especificar un *pool* creado anteriormente; en el siguiente se debe escribir la interfaz en donde correrá el servidor; por último, se debe definir el tiempo de validez de cada dirección asignada en el campo *Tiempo*. Para una mejor comprensión, la figura 5.34 muestra el proceso de creación de los tres servidores DHCP en el “router 1”.

The screenshot displays three vertically stacked configuration panels for DHCP pools. Each panel includes a 'Nombre' (Name) field, a 'Rango' (Range) field, a 'Numero #' (Number) field, and a 'Habilitar' (Enable) dropdown menu. Below each panel are 'Agregar' (Add) and 'Aceptar' (Accept) buttons.

Nombre	Rango	Numero #	Habilitar
pool1	100-192.168.10.254		Habilitar
pool2	1.100-192.168.1.254		Habilitar
pool3	2.100-192.168.2.254		Habilitar

Figura 5.33. Rangos de direcciones dinámicas para DHCP.

The screenshot displays three vertically stacked configuration panels for DHCP servers. Each panel includes a 'Pool' field, an 'Interfaz' (Interface) field, a 'Tiempo' (Time) field, a 'Numero #' (Number) field, and a 'Habilitar' (Enable) dropdown menu. Below each panel are 'Agregar' (Add) and 'Aceptar' (Accept) buttons.

Pool	Interfaz	Tiempo	Numero #	Habilitar
pool1	vlan21	3d00:00:00		Habilitar
pool2	vlan10	3d00:00:00		Habilitar
pool3	vlan11	3d00:00:00		Habilitar

Figura 5.34. Creación de servidores DHCP.

La impresión de las tablas finales sobre las configuraciones modificadas al crear los servidores DHCP para cada subred se visualizan en la figura 5.35.

```
ip dhcp-server network print

# ADDRESS          GATEWAY          DNS-SERVER        WINS-SERVER        DOMAIN
0 192.168.1.0/24    192.168.1.1
1 192.168.2.0/24    192.168.2.1
2 192.168.10.0/24   192.168.10.1
3 ;;; default configuration
  192.168.88.0/24   192.168.88.1

[admin@MikroTik] > ip pool print

# NAME              RANGES
0 default-dhcp      192.168.88.10-192.168.88.254
1 pool1             192.168.10.100-192.168.10.254
2 pool2             192.168.1.100-192.168.1.254
3 pool3             192.168.2.100-192.168.2.254

[admin@MikroTik] > ip dhcp-server print

Flags: X - disabled, I - invalid
# NAME      INTERFACE  RELAY      ADDRESS-POOL  LEASE-TIME  ADD-ARP
0 default  ether2     default-dhcp  10m
1 dhcp1    vlan21     pool1        3d
2 dhcp2    vlan10     pool2        3d
3 dhcp3    vlan11     pool3        3d
```

Figura 5.35. Configuración de servidores DHCP para cada subred.

La última configuración que se debe realizar en el dispositivo es la de añadir su puerta de salida a la red, es decir la dirección del “router core”. Como se muestra en la figura 5.36, al definir la dirección 0.0.0.0/0 en el campo red, se especifica que la puerta de enlace para todas las subredes es la dirección 10.10.1.1.



Figura 5.36. Designación de la puerta de salida de todas las subredes.

En el caso de las redes definidas en *Interfaces*, la puerta de enlace de cada una de ellas se añade automáticamente a la tabla de rutas del equipo. La figura 5.37 expone la tabla mencionada.

```
[admin@MikroTik] > ip route print
ip route print

Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
# DST-ADDRESS      PREF-SRC  GATEWAY      DISTANCE
0 A S 0.0.0.0/0       10.10.1.1   1
1 ADC 10.10.1.0/30     10.10.1.2   vlan31        0
2 ADC 192.168.1.0/24  192.168.1.1 vlan10         0
3 ADC 192.168.2.0/24  192.168.2.1 vlan11         0
4 ADC 192.168.10.0/24 192.168.10.1 vlan21         0
5 ADC 192.168.88.0/24 192.168.88.1 ether2         0
```

Figura 5.37. Tabla de enrutamiento del “router 1”.

Debido a que la restauración de fábrica del equipo incluye configuraciones preestablecidas es necesario eliminar estas reglas para el óptimo funcionamiento de nuestra red. En ENDS, para suprimir una regla se debe introducir el número identificador de la misma según se liste en la tabla correspondiente. Las figuras 5.38, 5.39 y 5.40 indican este proceso.

The screenshot displays the Mikrotik WinBox interface for DHCP server configuration. On the left, the 'Servidor DHCP' window is open, showing the 'DHCP-Server Network' and 'DHCP-Server' sections. In the 'DHCP-Server Network' section, the 'Numero #' field is set to 3. In the 'DHCP-Server' section, the 'Numero #' field is set to 0. On the right, the command-line interface shows the output of three commands: 'ip dhcp-server network print', 'ip pool print', and 'ip dhcp-server print'. The output of 'ip dhcp-server network print' shows a list of networks with the third entry (ID 3) highlighted in red. The output of 'ip pool print' shows a list of pools with the first entry (ID 0) highlighted in red. The output of 'ip dhcp-server print' shows a list of servers with the first entry (ID 0) highlighted in red.

Figura 5.38. Eliminación de reglas en las tablas de los servidores DHCP.

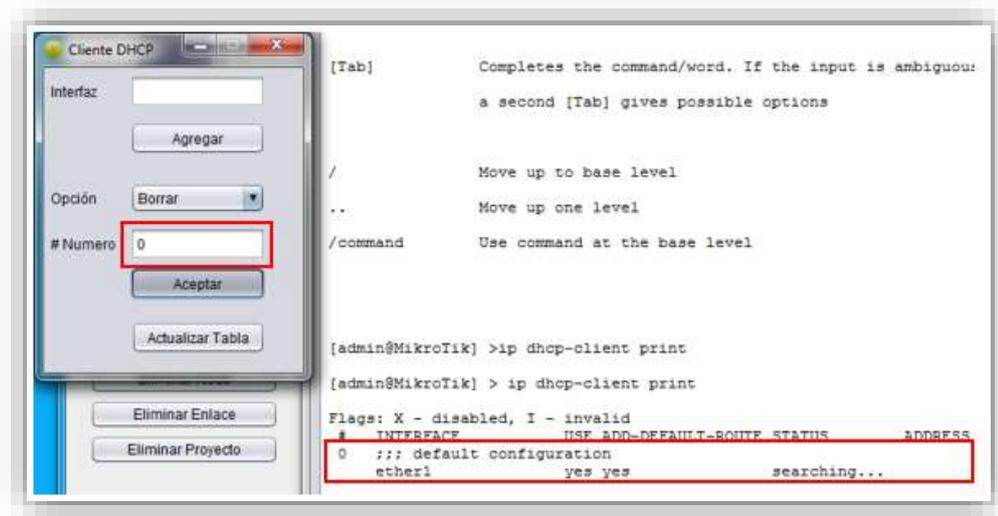


Figura 5.39. Eliminación del cliente DHCP.

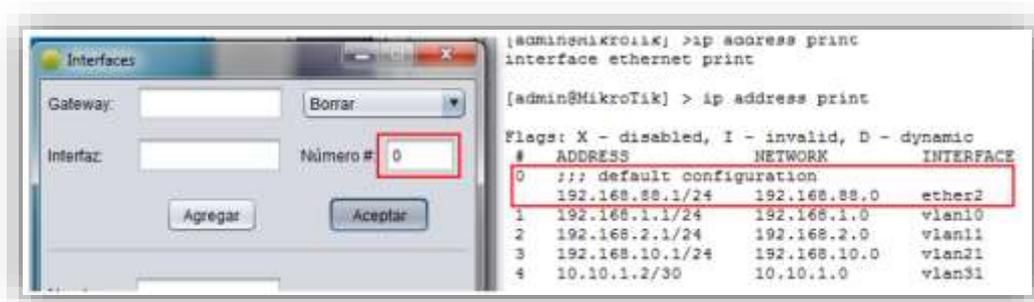


Figura 5.40. Borrado de la dirección 192.168.88.1 predefinida por configuración de fábrica.

Es importante mencionar que una vez suprimidas estas configuraciones se perderá comunicación con el equipo, razón por la cual, como último paso, se debe cambiar la dirección IP en la base de datos de ENDS como se ve en la figura 5.41.



Figura 5.41. Actualización de dirección IP del “router 1”.

De acuerdo a la red planteada, para el “router 2”, las configuraciones se realizan de manera similar al “router 1”, con la diferencia que se debe modificar los parámetros según se expone en las tablas 5.1 y 5.2.

5.3.3. Capa de núcleo

El acceso al “router core” se efectúa a través de la dirección IP 192.168.88.1, aquí también el terminal Telnet muestra el mensaje para aceptar la configuración de fábrica como se ve a continuación en la figura 5.42.

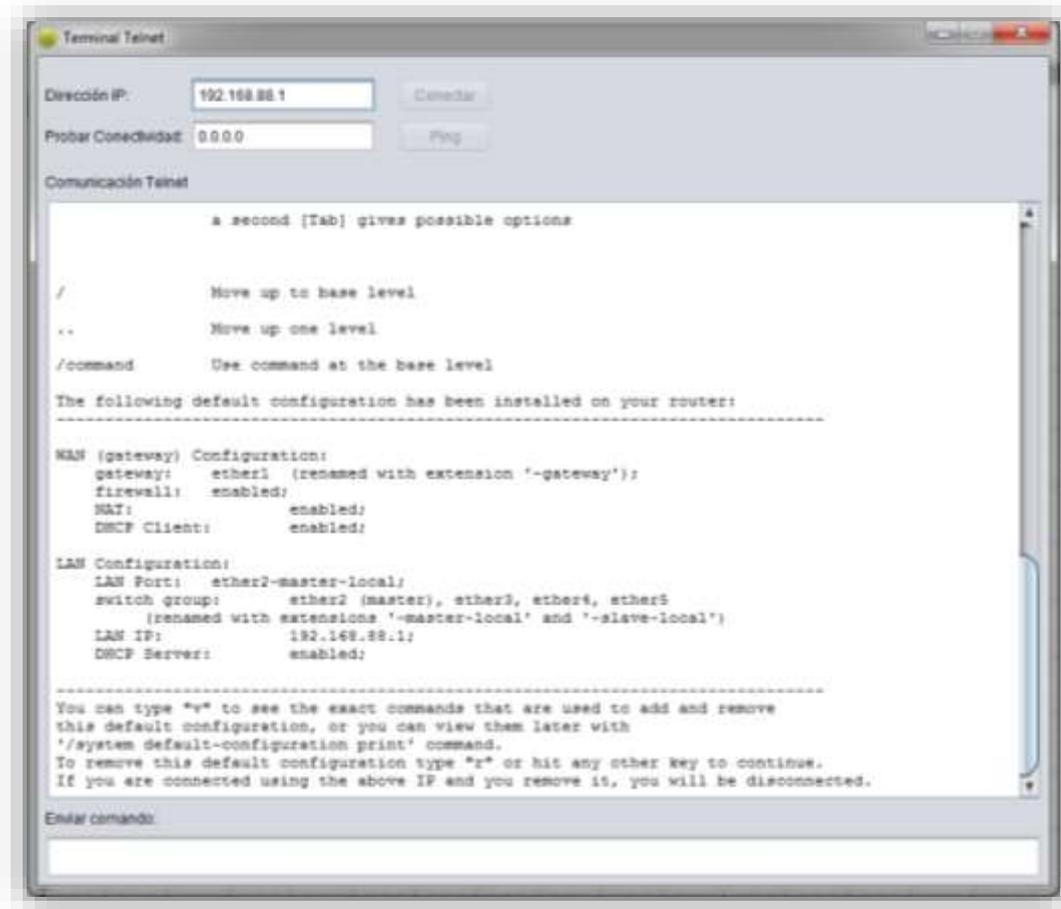


Figura 5.42. Mensaje de configuración de fábrica del “router core”.

En un proceso muy similar al seguido en el “router 1”, se ingresa a la ventana *Interfaces*, aquí se debe modificar el nombre y el estado de todos los puertos del equipo, resultando una tabla como se ve en la figura 5.43.

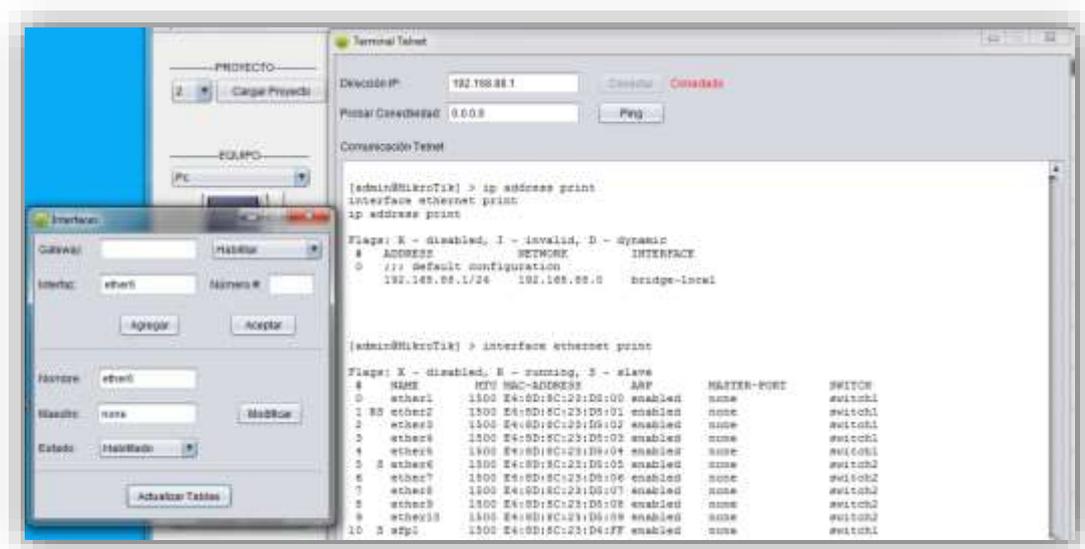


Figura 5.43. Cambio de nombre y estado de las interfaces.

De igual forma, en la figura 5.44 se añaden las VLANs respectivas con los números de identificación VLAN Id 31 y 32.

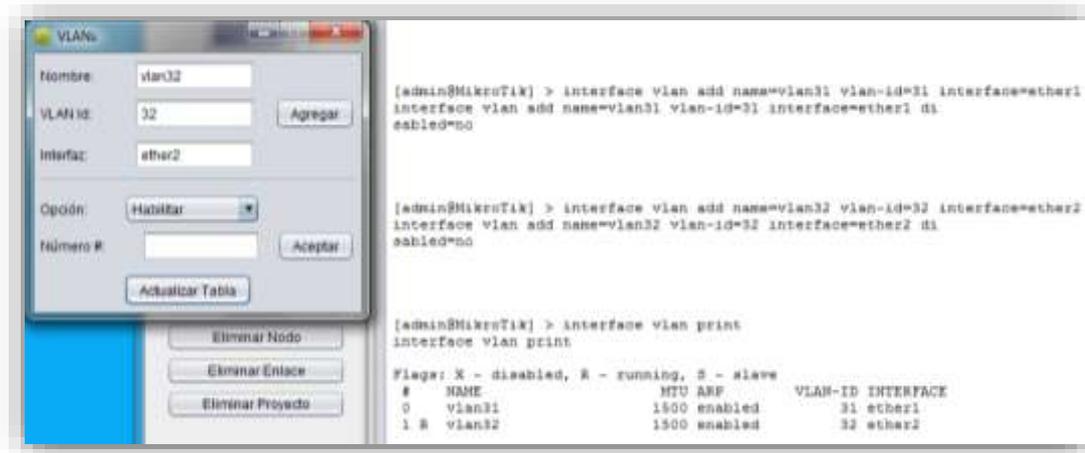


Figura 5.44. Redes virtuales locales del “router core”.

Para este equipo se establece adicionalmente un cliente DHCP para la conexión con una red externa. Se ingresa, a través del botón del mismo nombre en la ventana “Router”, a la ventana en la que, como primer paso, se debe eliminar el cliente configurado de fábrica. Se puede notar además que esta regla lleva el estado *searching* que nos indica que el dispositivo no se encuentra vinculado a otra red. Esta acción se observa en la figura 5.45.

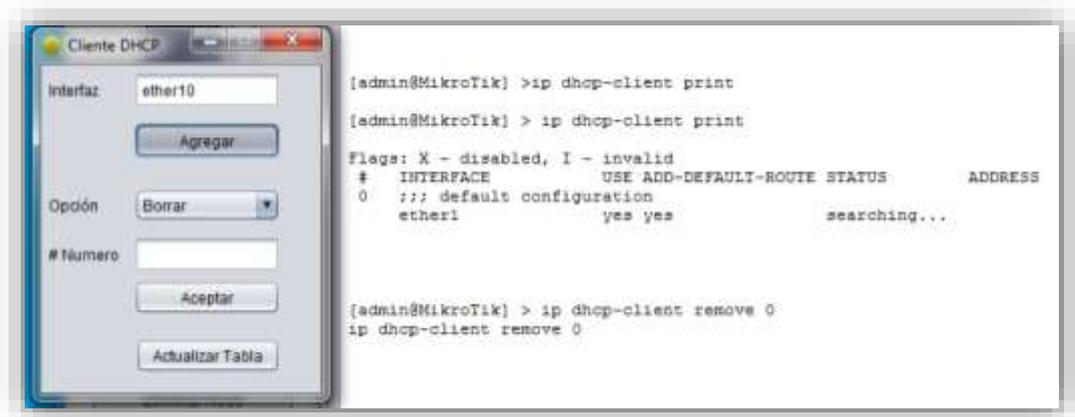


Figura 5.45. Eliminación de parámetros en el apartado cliente DHCP.

Prosiguiendo con la configuración, se añade un cliente DHCP a la interfaz ether10. En esta ocasión, ya que sí existe una conexión con la red del campus universitario, la tabla que se ve en la figura 5.46 indica el estado *bound* y la dirección IP asignada.

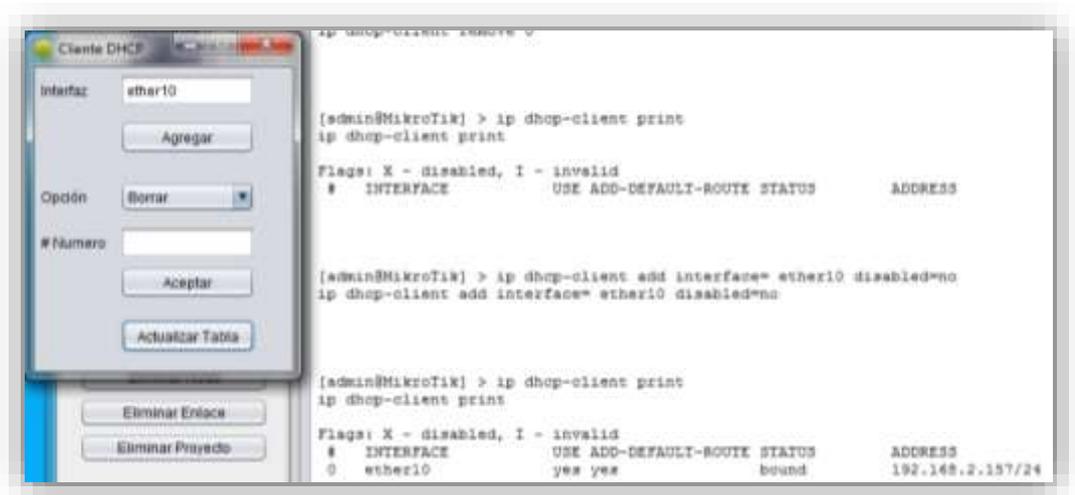


Figura 5.46. Establecimiento de un cliente DHCP.

Al haber configurado el cliente DHCP, se añade una configuración NAT que permite la traducción de direcciones IP privadas cuando éstas requieran salida a la red de área local. Como no se conoce la dirección IP de destino se utiliza la acción *masquerade* que realiza el cambio automáticamente y no solicita este parámetro. Las figuras 5.47 y 5.48 ilustran este proceso.

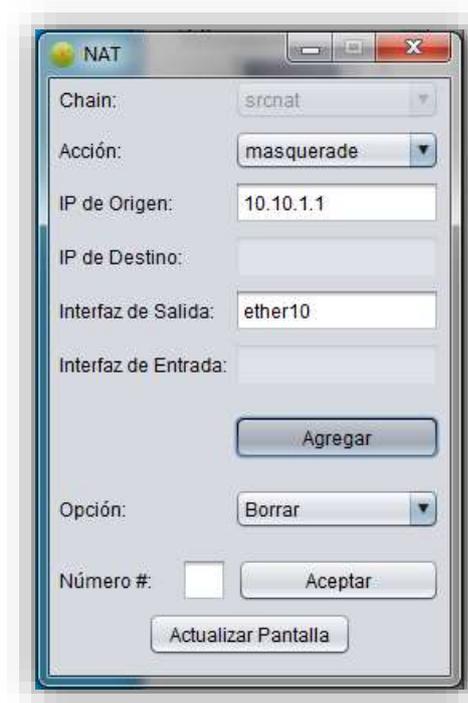


Figura 5.47. Configuración de NAT.

```
[admin@MikroTik] > ip firewall nat print
ip firewall nat print

Flags: X - disabled, I - invalid, D - dynamic
0 chain=srcnat action=masquerade src-address=10.10.1.1
  out-interface=ether10 log=no log-prefix=""
```

Figura 5.48. Visualización de un NAT tipo masquerade.

En el caso de este router no se cuenta con un servidor DHCP, no obstante, se debe eliminar las reglas creadas por la configuración predeterminada de fábrica; esto incluye: eliminar la red, el rango de direcciones y el servidor DHCP, tal como se observa en la figura 5.49.

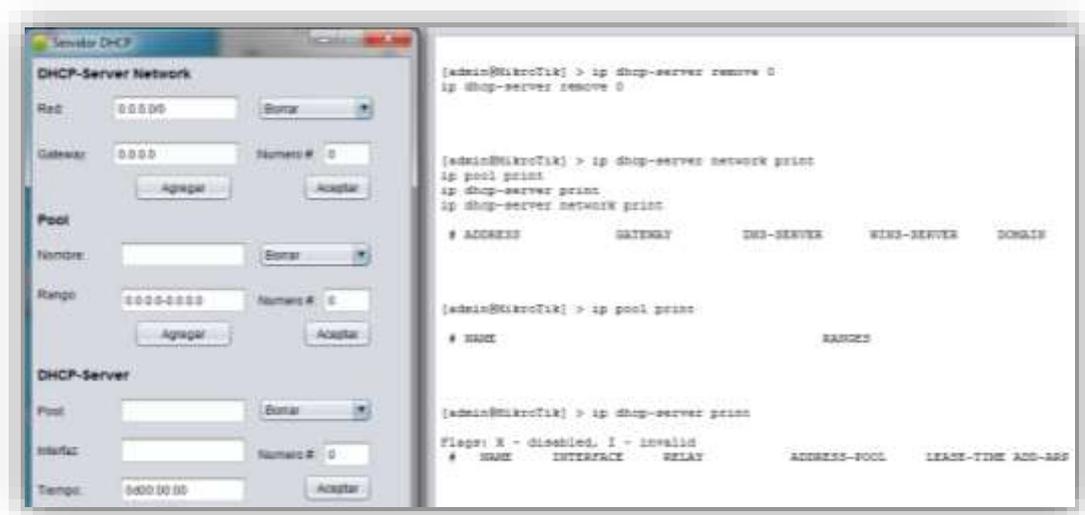


Figura 5.49. Eliminación de reglas en la ventana Servidor DHCP.

En la figura 5.50 se puede observar la tabla que contiene las direcciones de red que se deben agregar a las VLANs creadas previamente.

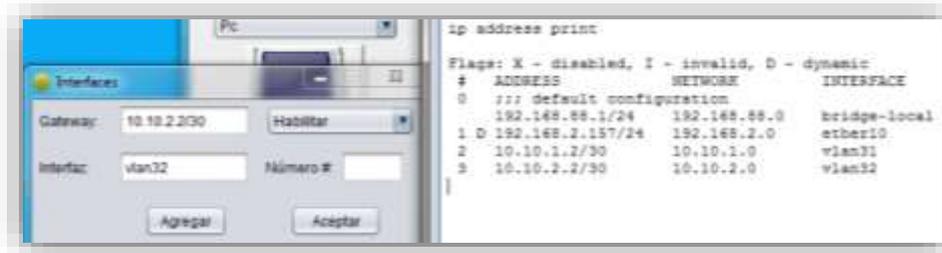


Figura 5.50. Tabla de direcciones de red de las interfaces del “router core”.

Para finalizar, en la ventana “Dir. Estático”, se incluyen las redes faltantes con sus respectivas puertas de enlace tal como se muestra en la figura 5.51.

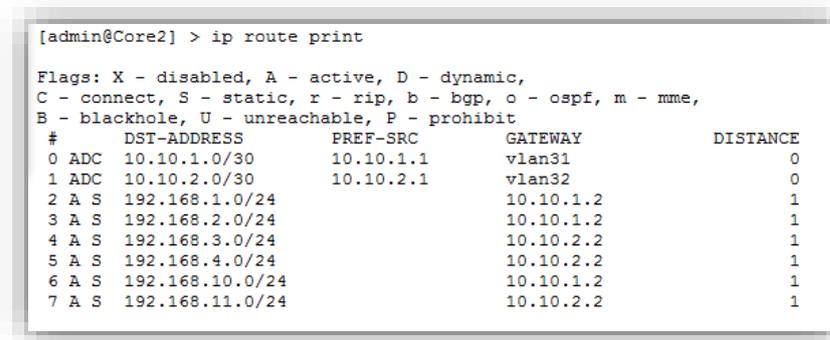


Figura 5.51. Tabla de enrutamiento del “router core”.

Al igual que en los demás equipos, se deben eliminar las configuraciones no utilizadas. También, se debe actualizar la dirección IP en ENDS como se ve en la figura 5.52.

Figura 5.52. Tabla de enrutamiento del “router core”.

Como punto final, en la figura 5.53 se observa la ventana “Nodos”, la misma que contiene la información general de todos los nodos pertenecientes al proyecto.

Id	Nombre	IdProy	Usuario	Clave	DirRed	X	Y	Tipo
28	router core	2	admin		10.10.1.1	443	160	Rout
29	router 1	2	admin		192.168.10.1	306	303	Rout
30	router 2	2	admin		192.168.11.1	588	302	Rout
31	switch 1	2			192.168.10.2	307	444	Swit
32	switch 2	2			192.168.11.2	587	446	Swit
33	pc 1	2			192.168.1.1	255	590	Pc
34	pc 2	2			192.168.2.1	385	590	Pc
35	pc 3	2			192.168.3.1	511	590	Pc
36	pc 4	2			192.168.4.1	666	590	Pc

Figura 5.53. Resumen de los nodos de red del proyecto.

5.4. Pruebas de comunicación

La figura 5.54 permite observar la dirección IP asignada por el servidor DHCP al conectar un ordenador al “switch 1”. Además, mediante el comando *ping*, se comprueba la comunicación con el *router* de la capa núcleo.

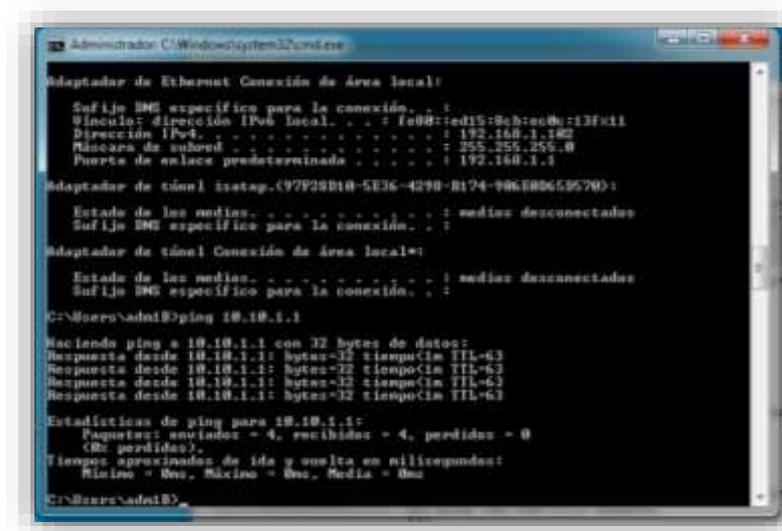


Figura 5.54. Comprobación de funcionamiento de la red.

Dentro del terminal Telnet de ENDS, con motivo de verificar el funcionamiento de la red creada en el apartado anterior, se utiliza el botón *Ping* para comprobar la comunicación, como se presenta en las figuras 5.55 y 5.56, desde el *router* de núcleo hacia los *routers* de distribución y hacia los *switches* de la capa de acceso.

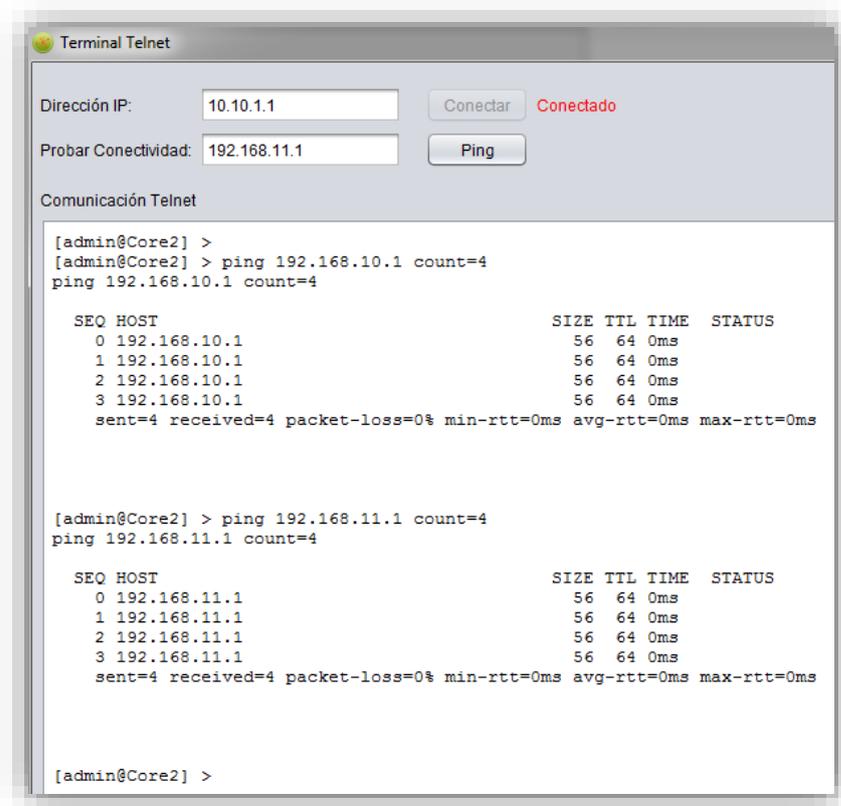


Figura 5.55. Comunicación entre las capas de núcleo y distribución.

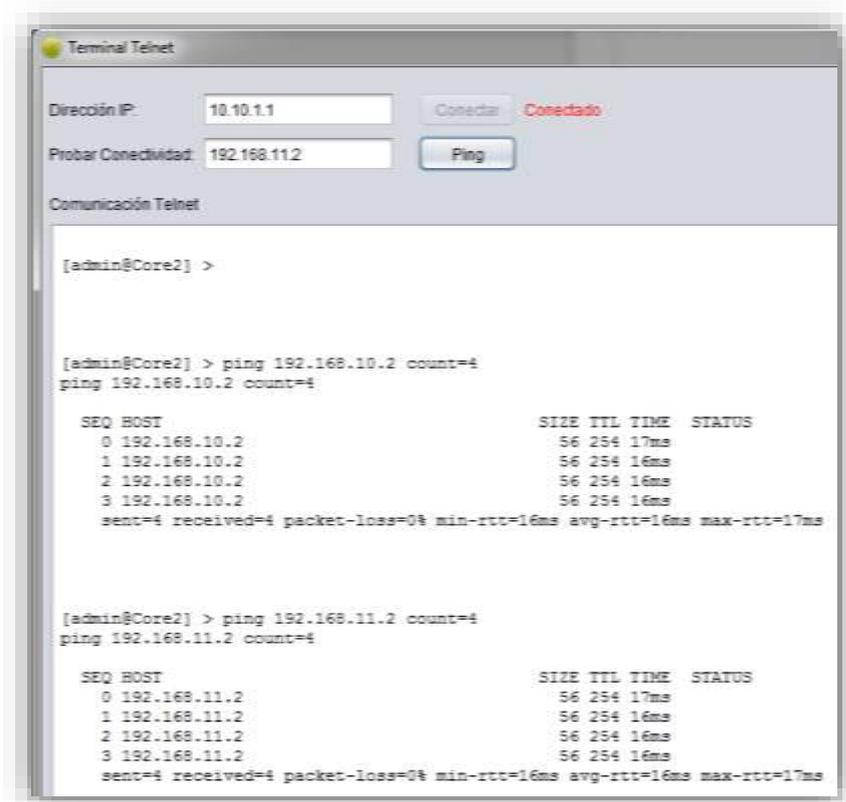


Figura 5.56. Comunicación entre las capas de núcleo y acceso.

CONCLUSIONES Y RECOMENDACIONES

Conclusiones:

- La recopilación de programas similares demostró que existe una gran cantidad de software para el diseño de redes, muchos de ellos presentan una interfaz gráfica de fácil manejo e incluso algunos tienen la posibilidad de establecer comunicación con equipos reales; sin embargo, la mayoría de programas disponibles en la actualidad están enfocados a la simulación de redes más no a la virtualización.
- La investigación realizada por varias universidades internacionales expuso que el uso de herramientas intuitivas para la simulación o la virtualización de redes permite a los estudiantes afianzar los conocimientos teóricos.
- Con la finalidad de que el programa se integre de mejor manera al laboratorio de redes y pueda ser empleado para la virtualización, se describió la situación actual del mismo, el cual cuenta con dos racks idénticos que incluyen equipos de la marca MikroTik para las capas de núcleo, distribución y acceso de la red. Además posee seis ordenadores y posibilita la integración de seis computadores adicionales.
- La utilización de base de datos facilitó el acceso a la información almacenada, y permitió que ENDS trabaje de una forma más rápida y que los cambios sean guardados de una manera más eficiente.
- Se determinó necesario que el servicio MySQL se encuentre activo en el ordenador para que ENDS pueda obtener la información de los proyectos realizados y los comandos de configuración de equipos MikroTik.

- En la implementación del programa en el laboratorio se pudo constatar que, a diferencia del sistema operativo MikroTik RouterOS, el sistema MikroTik SwOS no soporta el protocolo Telnet utilizado para la comunicación. Por esta razón, para los equipos que emplean este sistema, su configuración se realizó a través del navegador web con el protocolo HTTP.

Recomendaciones:

- Para el funcionamiento de ENDS, el computador donde se ejecuta debe tener instalado como mínimo la versión 1.6 de Java y también un gestor de base de datos MySQL. Como recomendación, se sugiere emplear el programa gratuito Xampp para este propósito.
- Para establecer una comunicación con cualquier dispositivo, el programa ENDS requiere únicamente de una dirección IP previamente configurada en el equipo a conectarse. En un dispositivo nuevo, o restaurado a su configuración de fábrica, MikroTik establece ésta dirección como 192.168.88.1.
- El programa ENDS, elaborado con la posibilidad de ser instalado en múltiples plataformas, y con el propósito de llegar a ser una herramienta primordial para la enseñanza de redes de comunicación, invita a los estudiantes a utilizarlo debido a su facilidad de manejo y funcionalidad; y además, incita a continuar mejorándolo, ampliando sus capacidades, poniendo a su disponibilidad el código fuente del proyecto desarrollado en el IDE NetBeans.

BIBLIOGRAFÍA

- Alvarado, L. (2011). *Redes de Computadoras*. Perú: UNASAM.
- Britos, J. D., Vargas, L. M., Arias, S., Giraudo, N., & Veneranda, G. (2013). Laboratorio virtual y remoto para la enseñanza de diseño y administración de redes de computadoras. *In XV Workshop de Investigadores en Ciencias de la Computación*.
- Díaz, L. (2010). *Evaluación de la herramienta GNS3 con conectividad a enrutadores reales*. Barcelona: Escuela Técnica Superior de Ingeniería de Telecomunicación de Barcelona.
- Douglis, F., & Krieger, O. (2013). Virtualization. *Internet Computing*, 6-9.
- Fernández, D. (2014). *Virtual Networks over linux*. Madrid: Center for Open Middleware.
- Galán, F., Fernández, D., Fuertes, W., Gómez, M., & de Vergara, J. E. (2009). Scenario-based virtual network infrastructure management in research and educational testbeds with VNUML. *Annals of telecommunications-Annales des télécommunications*, 305-323.
- Garg, V. (2010). *Wireless Communications & Networking*. Boston: Morgan Kaufmann.
- Martín, D., Marrero, M., Urbano, J., Barra, E., & Moreira, J. A. (2011). Virtualización, una solución para la eficiencia, seguridad y administración de intranets. *El profesional de la información*.
- MikroTik. (s.f.). *RouterBoard*. Obtenido de <http://routerboard.com/>
- Moreno Parra, R. (2012). *Simulación: Conceptos y programación*. Cali: Universidad Libre Cali.
- Netacad. (2015). *Cisco Networking Academy*. Recuperado el 6 de Noviembre de 2015, de Cisco Packet Tracer: <https://www.netacad.com/es/web/about-us/cisco-packet-tracer>
- Newman, M. (2010). *Networks: an introduction*. Oxford : Oxford University Press.
- Oracle. (s.f.). *Oracle Technology Network for Java Developers*. Recuperado el 03 de Marzo de 2016, de <http://www.oracle.com/technetwork/java>
- Packet-Tracer-Network. (2015). *Cisco Packet Tracer 6.2: Download free labs and tutorials for CCNA certification exam preparation*. Recuperado el 6 de Noviembre de 2015, de <http://www.packettracernetwork.com/>
- Paessler. (2015). *PRTG Network Monitor - Intuitive Network Monitoring Software*. Recuperado el 6 de Noviembre de 2015, de <https://www.paessler.com/prtg>

- Panchana, B., Stefania, D., Izurieta, V., Gabriela, N., Espinoza, D., & Stalyn, R. (2011). *Diseño e implementación de un ambiente virtualizado para un sistema de administración de contenidos usando Microsoft Sharepoint*. Guayaquil.
- Pereñíguez-García, F., Ruiz, A., Ros, F. J., Marín, R., & Ruiz, P. M. (2012). VNUML vs GNS3 en el desarrollo de laboratorios de redes virtuales. *Jornadas de Enseñanza de la Informática*.
- Ruiz, A., Marín, R., Pereñíguez-García, F., Ruiz, P. M., & Gómez, A. F. (2010). Experiencia con la herramienta de virtualización VNUML para la enseñanza de redes de computadores. *Jornadas de Enseñanza Universitaria de la Informática*.
- Ruiz, J., Fernández, D., Galán, F., & Bellido, L. (2008). Modelo de Laboratorio Docente de Telemática basado en Virtualización Distribuida. *VII Jornadas de Ingeniería Telemática*.
- Scroxtton, A. (25 de Septiembre de 2014). *Lancaster University supports SDN development with HP Networking*. Recuperado el 10 de Enero de 2016, de Lancaster Uni deploys 40 OpenFlow-enabled HP switches to run SDN research and production environments concurrently: <http://www.computerweekly.com/news/2240231403/Lancaster-University-supports-SDN-development-with-HP-Networking>
- Scroxtton, A. (26 de Mayo de 2015). *City University London moves towards SDN with Avaya Fabric Connect*. Recuperado el 10 de Enero de 2016, de Avaya Fabric Connect helps City University London move towards software-defined infrastructure and streamlines its network deployment: <http://www.computerweekly.com/news/4500246896/City-University-London-moves-towards-SDN-with-Avaya-Fabric-Connect>
- The Apache Software Foundation. (s.f.). *Apache Commons Net*. Recuperado el 01 de Marzo de 2016, de <https://commons.apache.org/proper/commons-net/>
- Universidad Politécnica de Madrid. (13 de Febrero de 2012). *Virtual Network User-Mode-Linux (VNUML)*. Recuperado el 6 de Diciembre de 2015, de http://web.dit.upm.es/vnumlwiki/index.php/Main_Page
- Universidad Politécnica de Madrid. (24 de Julio de 2015). *Virtual Networks over linux (VNX)*. Recuperado el 6 de Diciembre de 2015, de http://web.dit.upm.es/vnxwiki/index.php/Main_Page
- Vargas Avilés, J. (2015). Introducción a la Modelación y Simulación de Sistemas. *Universidad de Managua*.
- Wannous, M., & Nakano, H. (2010). NVLab, a networking virtual web-based laboratory that implements virtualization and virtual network computing technologies. *Learning Technologies*, 129-138.