

ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

DESARROLLO DE GUÍAS PRÁCTICAS PARA LA SIMULACIÓN DE REDES CON EQUIPOS MIKROTIK UTILIZANDO GNS3

TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL TÍTULO DE TECNÓLOGO EN ELECTRÓNICA Y TELECOMUNICACIONES

Andrea Elizabeth Cruz Quilca

andrea.cruz@epn.edu.ec

Ricardo David Gordon Pérez

ricardo.gordon@epn.edu.ec

DIRECTOR: ING. GABRIELA KATHERINE CEVALLOS SALAZAR, MSC.

gabriela.cevalloss@epn.edu.ec

CODIRECTOR: ING. FABIO MATÍAS GONZÁLEZ GONZÁLEZ, MSC.

fabio.gonzalez@epn.edu.ec

Quito, junio 2021

CERTIFICACIÓN

Certificamos que el presente trabajo fue desarrollado por la Srta. Cruz Quilca Andrea Elizabeth y el Sr. Gordon Pérez Ricardo David como requerimiento parcial a la obtención del título de TECNÓLOGO EN ELECTRÓNICA Y TELECOMUNICACIONES bajo nuestra supervisión:



**ING. GABRIELA KATHERINE
CEVALLOS SALAZAR, MSC.**

DIRECTORA DEL PROYECTO



**ING. FABIO MATÍAS GONZÁLEZ
GONZÁLEZ, MSC.**

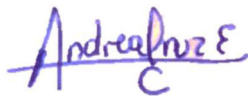
CODIRECTOR DEL PROYECTO

DECLARACIÓN

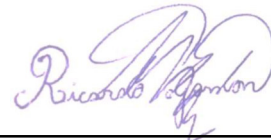
Nosotros Cruz Quilca Andrea Elizabeth con CI: 230027880-7 y Gordon Pérez Ricardo David con CI: 171459122-7 declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y que hemos consultado las referencias bibliográficas que se incluyen en este documento.

Sin perjuicio de los derechos reconocidos en el primer párrafo del artículo 144 del Código Orgánico de la Economía Social de los Conocimientos, Creatividad e Innovación – COESC-, somos titulares de la obra en mención y otorgamos una licencia gratuita, intransferible y no exclusiva de uso con fines académicos a la Escuela Politécnica Nacional.

Entregamos toda la información técnica pertinente, en caso de que hubiese una explotación comercial de la obra por parte de la EPN, se negociará los porcentajes de los beneficios conforme lo establece la normativa nacional vigente.



**Srta. Andrea Elizabeth Cruz
Quilca**



**Sr. Ricardo David Gordon
Pérez**

DEDICATORIA

Dedicado a mi familia y amigos, que estuvieron apoyándome paso a paso y dándome aliento en todo el proceso universitario.

Ricardo David Gordon Pérez

AGRADECIMIENTO

Agradezco a mi familia, especialmente a mis padres y abuelita. Es gracias ellos que he podido culminar esta etapa de mi formación profesional y personal.

A mis hermanos musicales (NOI), por alentarme a seguir creciendo día con día. Demostrando que aquello que vale la pena requiere de esfuerzo y dedicación.

A mi tutora, la ingeniera Gabriela Cevallos por guiarnos de la mejor manera en el desarrollo de la tesis. Además, por demostrar ser alguien excepcional como persona y docente.

A mi compañera de tesis Andrea Cruz, por estar presente ayudando a que nuestra tesis finiquite con éxitos.

Gracias de todo corazón, por confiar y creer en mí.

Ricardo David Gordon Pérez

DEDICATORIA

Dedico este proyecto de titulación y todo el esfuerzo que he realizado en todo el tiempo de carrera a mis padres David Cruz y Gladys Quilca que siempre me apoyaron incondicionalmente en todo sentido para llegar a este momento de ser una profesional más de la Patria.

A mi hermana por todos los consejos y ayuda que me ha brindado todo este tiempo y a mí enamorado por todo el apoyo durante toda mi carrera universitaria.

Andrea Elizabeth Cruz Quilca

AGRADECIMIENTO

Primero que todo quiero agradecer a mis padres porque sin ellos y su apoyo no hubiera podido salir adelante y luchar por lo que ahora estoy a punto de realizarlo. A mi hermana por todas las noches que me ayudaba a aprenderme cada uno de los temas de mis materias sin tener conocimiento alguno de lo que estudiaba, a mis abuelitos que sin su ayuda y acogida nada hubiera sido tan fácil el no sentirme sola en especial a mi abuelito que ya no lo tengo conmigo porque hizo muchos sacrificios por mi durante mi carrera universitaria, a mi familia en general por el apoyo brindado y por último y no menos importante a mi enamorado que desde que llegó a mi vida me inyectó esa fuerza para salir adelante en mi carrera universitaria y ahora sigue apoyándome para dar los últimos pasos y cumplir con tan ansiosa meta propuesta desde el día 1 que llegue a la universidad.

Quiero también agradecer a todos los ingenieros que en toda mi carrera universitaria me enseñaron mucho más que la materia que les correspondía y sobre todo a mi tutora, la Ing. Gabriela Cevallos por toda la paciencia y ayuda que nos brindó durante todo este proceso.

Y para finalizar agradezco a mi compañero de tesis el Sr. Ricardo Gordon por todo este tiempo transcurrido y el trabajo en equipo realizado que pronto se verá reflejado en la meta que nos hemos propuesto.

Muchas gracias a todos por la confianza puesta en mí.

Andrea Elizabeth Cruz Quilca

ÍNDICE DE CONTENIDOS

1	INTRODUCCIÓN.....	22
1.1	Objetivo general	22
1.2	Objetivos específicos.....	22
1.3	Fundamentos.....	23
	<i>Mikrotik</i>	23
	<i>RouterOS</i>	23
	<i>Winbox</i>	23
	<i>Solar Putty</i>	23
	GUI (<i>Graphical User Interface</i>)	23
	RIP (<i>Routing Information Protocol</i>)	23
	NAT (<i>Network Address Traduction</i>)	24
	BGP (<i>Border Gateway Protocol</i>)	24
	Sistema autónomo.....	24
	OSPF (<i>Open Shortest Path First</i>)	24
	PPTP (<i>Point to Point Tunneling Protocol</i>)	24
	VPN (<i>Virtual Private Network</i>).....	24
	<i>Oracle VM VirtualBox</i>	25
	MPLS (<i>Multiprotocol Label Switching</i>).....	25
2	METODOLOGÍA.....	25
2.1	Descripción de la metodología usada	25
3	RESULTADOS Y DISCUSIÓN	26
3.1	Niveles de licencias de los <i>routers Mikrotik</i>	26
3.2	Funcionalidades y herramientas que comprende GNS3	28
	Descarga e instalación de GNS3	28
	Descarga e instalación de <i>Oracle VM VirtualBox</i>	30
	Descarga de la imagen con el sistema operativo del <i>router Mikrotik</i>	30

Creación de un <i>router</i> de <i>Mikrotik</i> en <i>Oracle VM VirtualBox</i>	31
Crear la interfaz de <i>loopback</i> en el ordenador principal	37
Enlazar la máquina virtual a GNS3	41
Comandos básicos e interfaz de GNS3	47
3.3 Análisis y verificación de las topologías de red que se pueden implementar a través de GNS3 con equipos <i>Mikrotik</i>	49
3.4 Elaboración de las hojas guías de prácticas	50
Hojas Guías de Prácticas para Estudiantes	51
Hojas Guías de Prácticas para Docentes.....	63
4 CONCLUSIONES Y RECOMENDACIONES	147
4.1 Conclusiones	147
4.2 Recomendaciones	148
5 REFERENCIAS BIBLIOGRÁFICAS.....	149
6 ANEXOS.....	151

ÍNDICE DE FIGURAS

Figura 3.1 Comparación de niveles de licencias <i>Mikrotik</i>	26
Figura 3.2 Opciones de descargar de GNS3 desde su página oficial	28
Figura 3.3 Ventana para la creación de una cuenta en GNS3	28
Figura 3.4 Ficha de creación de cuenta GNS3	29
Figura 3.5 Pestaña principal para la instalación de GNS3	29
Figura 3.6 Pantalla para instalar <i>Solarwinds</i>	29
Figura 3.7 Sitio oficial de <i>Oracle VM VirtualBox</i>	30
Figura 3.8 Página web para la descarga de la ISO desde el sitio oficial de <i>Mikrotik</i> ..	31
Figura 3.9 Opción “Nueva” para la creación de una máquina virtual	31
Figura 3.10 Interfaz para la creación de una máquina virtual y parámetros	32
Figura 3.12 Configuración General del <i>router Mikrotik</i>	33
Figura 3.13 Configuración Sistema/Placa base.....	33
Figura 3.14 Configuración Sistema/Procesador.....	33
Figura 3.15 Configuración Almacenamiento	34
Figura 3.16 Configuración Red/Adaptadores	34
Figura 3.17 Vista general de los detalles y parámetros configurados en la máquina virtual “ROUTER MIKROTIK” en la pantalla de <i>Oracle VM VirtualBox</i>	35
Figura 3.18 Instalación del sistema operativo de <i>router Mikrotik</i>	35
Figura 3.19 Detalle de instalación del sistema operativo de <i>router Mikrotik</i>	36
Figura 3.20 Cambio del orden de arranque en Sistema/Placa base de la máquina virtual	36
Figura 3.21 Cambios de configuración en Almacenamiento de la máquina virtual	37
Figura 3.22 Pantalla inicial del <i>router Mikrotik</i>	37
Figura 3.23 Pantalla del Administrador de dispositivos	37
Figura 3.24 Pantalla del Administrador de dispositivos/Agregar <i>hardware</i> heredado ..	38
Figura 3.26 Asistente para buscar un <i>hardware</i>	39
Figura 3.27 Lista de los tipos de <i>hardware</i> que pueden ser instalados	39
Figura 3.28 Controlador de dispositivos	40
Figura 3.29 Finalización del Asistente para agregar un <i>hardware</i> heredado	40
Figura 3.31 Pantalla de Preferences en GNS3	41
Figura 3.32 Pestaña de <i>VirtualBox VMs</i>	41
Figura 3.33 Ventana <i>New VirtualBox VM templates</i> y máquina agregada.....	42
Figura 3.34 Configuración General del <i>router Mikrotik</i> en GNS3.....	42

Figura 3.35 Configuración de los adaptadores de red para el <i>router Mikrotik</i> en GNS3	43
Figura 3.36 Pestaña de <i>VirtualBox VM templates</i>	43
Figura 3.37 Pantalla principal de GNS3 con el <i>router Mikrotik</i>	43
Figura 3.38 Pantalla de <i>Browse Switches</i>	44
Figura 3.40 Cableado <i>Router/Switch</i>	44
Figura 3.41 Cableado entre <i>Switch/Cloud</i>	45
Figura 3.42 Configuración de red <i>router Mikrotik</i>	45
Figura 3.43 Configuración de red para el <i>router Mikrotik/Adaptador 1</i>	46
Figura 3.44 Interfaz de conexión de <i>Winbox</i>	46
Figura 3.45 Conexión del <i>router</i> en <i>Winbox</i>	46
Figura 3.46 Licencias de <i>router</i> y actualización de nivel	47
Figura 3.47 Interfaz principal de <i>Winbox</i>	47
Figura 3.48 Diagrama de conexiones Introducción a GNS3	51
Figura 3.49 Diagrama de conexiones Enrutamiento Estático	54
Figura 3.50 Diagrama de conexiones Protocolo de Enrutamiento dinámico IGP (<i>Interior Gateway Protocol</i>) Protocolo Vector Distancia <i>RIP</i>	55
Figura 3.51 Diagrama de conexiones Protocolo de Enrutamiento Dinámico EGP (<i>Exterior Gateway Protocol</i>) Protocolo BGP	57
Figura 3.52 Diagrama de conexiones Red Privada Virtual (VPN) con protocolo PPTP	59
Figura 3.53 Diagrama de conexiones Implementación de red MPLS con OSPF	61
Figura 3.54 Diagrama de conexiones práctica 1	63
Figura 3.55 Ventana del Adaptador de bucle invertido creado	64
Figura 3.56 Pantalla principal del <i>router</i> línea de comandos	64
Figura 3.57 Creación un nuevo proyecto en GNS3	64
Figura 3.58 Asignar un nombre al proyecto	65
Figura 3.59 Aceptar los cambios realizados para el <i>router</i>	65
Figura 3.60 Ícono del <i>Mikrotik</i> creado y vinculado	65
Figura 3.61 Ícono de <i>Ethernet Switch</i>	66
Figura 3.62 Ícono de <i>Cloud</i>	66
Figura 3.63 Elección del puerto en el <i>router</i> para cablearlo con el <i>switch</i>	66
Figura 3.64 Elección del puerto "Bucle invertido" para cablear el <i>switch</i> con <i>cloud</i>	67
Figura 3.65 Cableado de los equipos	67
Figura 3.66 Segundo <i>switch</i> agregado	67
Figura 3.67 Máquinas virtuales cableadas al <i>switch</i>	67
Figura 3.68 Agregar etiquetas a la topología	68

Figura 3.69 Insertar una figura a la topología, cambio de profundidad.....	68
Figura 3.70 Figura insertada para identificar un segmento de la topología	69
Figura 3.71 Segunda figura insertada con los cambios respectivos	69
Figura 3.72 Inicialización del proyecto de GNS3.....	69
Figura 3.73 Proyecto de GNS3 detenido.....	70
Figura 3.74 Cambio de la configuración del adaptador de red del <i>router</i> en <i>VirtualBox</i>	70
Figura 3.75 Interfaces conectadas en GNS3	71
Figura 3.76 Pantalla principal de <i>Winbox</i>	71
Figura 3.77 Conexión con el <i>router</i> mediante <i>Winbox</i>	72
Figura 3.78 Licencia del <i>router Mikrotik</i>	72
Figura 3.79 Pantalla principal de las configuraciones del <i>router</i> en <i>Winbox</i>	72
Figura 3.80 Agregar un nombre mediante línea de comandos	73
Figura 3.81 Asignación de un nombre	73
Figura 3.82 Asignar una dirección IP mediante la interfaz gráfica.....	73
Figura 3.83 Dirección IP agregada.....	74
Figura 3.84 Agregar una dirección IP a la PC1	74
Figura 3.85 Agregar una dirección IP a la PC2	74
Figura 3.86 <i>Ping</i> desde PC1 al <i>Gateway</i>	74
Figura 3.87 <i>Ping</i> desde PC1 a PC2	75
Figura 3.88 <i>Ping</i> desde PC2 al <i>Gateway</i>	75
Figura 3.89 <i>Ping</i> desde PC1 a PC2	75
Figura 3.90 Rutas aprendidas por el <i>router</i>	75
Figura 3.91 Ingreso a la pestaña " <i>Files</i> ".....	76
Figura 3.92 Pantalla principal de los archivos del <i>router</i>	76
Figura 3.93 Creación de un archivo de respaldo.....	76
Figura 3.94 Asignar un nombre y clave.....	76
Figura 3.95 Reiniciar las configuraciones del <i>router</i>	77
Figura 3.96 Selección de opciones para el reinicio del <i>router</i>	77
Figura 3.97 Restauración de las configuraciones.....	77
Figura 3.98 Acceso al archivo con la clave	78
Figura 3.99 Direcciones IP reestablecidas	78
Figura 3.100 Rutas del <i>router</i> reestablecidas.....	78
Figura 3.101 Confirmación para el cambio de clave	78
Figura 3.102 Ingreso mediante <i>Winbox</i> con la clave asignada.....	78
Figura 3.104 Direcciones IP correspondientes al <i>ROUTER1</i>	81

Figura 3.105 Direcciones IP correspondientes al <i>ROUTER2</i>	81
Figura 3.106 Direcciones IP correspondientes al <i>ROUTER3</i>	81
Figura 3.107 Direcciones IP correspondientes al <i>ROUTER4</i>	81
Figura 3.108 Ingreso "Routes" para asignar rutas al <i>ROUTER1</i>	81
Figura 3.109 Tabla de rutas aprendidas por el <i>ROUTER1</i>	82
Figura 3.110 Asignar una nueva ruta al <i>ROUTER1</i>	82
Figura 3.111 Nueva ruta agregada al <i>ROUTER1</i> para llegar a <i>LAN3</i>	82
Figura 3.112 Nueva ruta agregada al <i>ROUTER1</i> enlace 172.16.5.116/30	83
Figura 3.113 Nueva ruta agregada al <i>ROUTER1</i> para llegar a <i>LAN4</i>	83
Figura 3.114 Nueva ruta agregada al <i>ROUTER1</i> enlace 172.16.5.120/30	83
Figura 3.115 Nueva ruta agregada al <i>ROUTER1/LAN5</i>	84
Figura 3.116 Nueva ruta agregada al <i>ROUTER1 /LAN6</i>	84
Figura 3.117 Tabla de enrutamiento aprendida por el <i>ROUTER1</i>	84
Figura 3.118 Tabla de enrutamiento aprendida por el <i>ROUTER2</i>	85
Figura 3.119 Tabla de enrutamiento aprendida por el <i>ROUTER3</i>	85
Figura 3.120 Tabla de rutas aprendidas por el <i>ROUTER4</i>	85
Figura 3. 121 Pantalla de Solar Putty de una <i>VPCS</i> para asignar direcciones IP	86
Figura 3.122 Asignar un dirección IP <i>PC1/LAN1</i>	86
Figura 3.123 Asignar un dirección IP <i>PC2/LAN2</i>	86
Figura 3.124 Asignar un dirección IP <i>PC3/LAN3</i>	86
Figura 3.125 Asignar un dirección IP <i>PC4/LAN5</i>	86
Figura 3.126 Asignar un dirección IP <i>PC5/LAN6</i>	86
Figura 3.127 Asignar un dirección IP <i>PC6/LAN4</i>	86
Figura 3128 Listado de pings exitosos desde la <i>LAN1</i> hacia las otras redes	87
Figura 3.130 Listado de pings exitosos desde la <i>LAN2</i> hacia las otras redes	87
Figura 3.131 Listado de pings exitosos desde la <i>LAN3</i> hacia las otras redes	88
Figura 3.131 Listado de pings exitosos desde la <i>LAN4</i> hacia las otras redes	88
Figura 3.132 Listado de pings exitosos desde la <i>LAN5</i> hacia las otras redes	89
Figura 3.133 Listado de pings exitosos desde la <i>LAN6</i> hacia las otras redes	89
Figura 3.134 Diagrama de conexiones práctica 3	91
Figura 3.135 Direcciones IP aprendidas por el <i>ROUTERA</i>	92
Figura 3.136 Lista de direcciones IP aprendidas por el <i>ROUTERB</i>	92
Figura 3.137 Lista de direcciones IP aprendidas por el <i>ROUTERC</i>	92
Figura 3.138 Ingreso a la pestaña "Routing" para configurar el protocolo RIP en el <i>ROUTERA</i>	92

Figura 3.139 Configuración del puerto por donde se envía y recibe el protocolo RIP en el <i>ROUTERA</i>	93
Figura 3.140 Pestaña donde indica que el puerto ha sido levantado en el <i>ROUTERA</i>	93
Figura 3.141 Opciones de compartición de RIP para el <i>ROUTERA</i>	93
Figura 3.142 Listado de redes que usa el protocolo RIP en el <i>ROUTERB</i>	94
Figura 3.143 Opciones de compartición de RIP para el <i>ROUTERB</i>	94
Figura 3.144 Redes que usa el protocolo RIP en el <i>ROUTERC</i>	94
Figura 3.145 Opciones de compartición de RIP para el <i>ROUTERC</i>	94
Figura 3.146 Listado de rutas aprendidas por el <i>ROUTERA</i>	95
Figura 3.147 Listado de rutas aprendidas por el <i>ROUTERB</i>	95
Figura 3.148 Listado de rutas aprendidas por el <i>ROUTERC</i>	95
Figura 3.149 Designación de una dirección IP 192.168.1.2/24 para la <i>VPCS</i> de la <i>LAN1</i>	96
Figura 3.150 Designación de una dirección IP 192.168.1.3/24 para la <i>VPCS</i> de la <i>LAN2</i>	96
Figura 3.151 Designación de una dirección IP 192.168.2.2/24 para la <i>VPCS</i> de la <i>LAN2</i>	96
Figura 3.152 Designación de una dirección IP 192.168.3.2/24 para la <i>VPCS</i> de la <i>LAN3</i>	96
Figura 3.153 Designación de una dirección IP 192.168.3.3/24 para la <i>VPCS</i> de la <i>LAN3</i>	96
Figura 3.154 <i>Ping</i> realizado desde la <i>LAN1</i> a la <i>LAN2</i> usando una <i>VPCS</i>	96
Figura 3.155 <i>Ping</i> realizado desde la <i>LAN1</i> a la <i>LAN3</i> usando una <i>VPCS</i>	97
Figura 3.156 <i>Ping</i> realizado desde la <i>LAN2</i> a la <i>LAN1</i> usando una <i>VPCS</i>	97
Figura 3.157 <i>Ping</i> realizado desde la <i>LAN2</i> a la <i>LAN3</i> usando una <i>VPCS</i>	97
Figura 3.158 <i>Ping</i> realizado desde la <i>LAN3</i> a la <i>LAN1</i> usando una <i>VPCS</i>	97
Figura 3. 159 <i>Ping</i> realizado desde la <i>LAN3</i> a la <i>LAN2</i> usando una <i>VPCS</i>	97
Figura 3.160 Diagrama de conexiones práctica 4	98
Figura 3.161 Redes aprendidas por el <i>router</i> AS200	99
Figura 3.162 Redes aprendidas por el <i>router</i> AS300	99
Figura 3.163 Redes aprendidas por el <i>router</i> AS400	99
Figura 3.164 Configuración de la interfaz lógica denominada " <i>loop</i> "	99
Figura 3.165 Interfaz lógica " <i>loop</i> " levantada en el <i>router</i>	100
Figura 3.166 Dirección IP agregada a la interfaz lógica " <i>loop</i> " del AS400	100
Figura 3.167 Dirección IP agregada a la interfaz lógica " <i>loop</i> " del AS500	100

Figura 3.168 Configuración y levantamiento de la interfaz lógica “nuestra red” en AS300	101
Figura 3.169 Asignación de una dirección IP a la interfaz lógica “nuestra red”	101
Figura 3.170 Configuración de la dirección IP usada por BGP del <i>router</i> AS200	102
Figura 3.171 Ingreso a “BGP/Peers” en el <i>router</i> AS200	102
Figura 3.172 Configuración de “Peer” para BGP en el <i>router</i> AS200	103
Figura 3.173 Ingreso a la pestaña “BGP/Networks” en el <i>router</i> AS200.....	103
Figura 3.174 Ingreso de la dirección IP de la red a que se conecta el <i>router</i> AS200.	103
Figura 3.175 Configuración de la dirección IP usada por BGP del <i>router</i> AS400	104
Figura 3.176 Configuración de “Peer” para BGP en el <i>router</i> AS400	104
Figura 3.177 Ingreso de la dirección IP de la red a que se conecta el <i>router</i> AS400 en “BGP Network”	105
Figura 3.178 Configuración de la dirección IP usada por BGP del <i>router</i> AS500	105
Figura 3.179 Configuración de “Peer” para BGP en el <i>router</i> AS500	105
Figura 3.180 Ingreso de la dirección IP de la red a la que se conecta el <i>router</i> AS500... 106	106
Figura 3.181 Configuración de “Peer” para BGP en el <i>router</i> AS300 “nuestra red” ...	106
Figura 3.182 Vista general de “Peer1” que une el AS300 con el AS200	106
Figura 3.183 Estado de la interfaz “Peer1” que une el AS300 con el AS200.....	107
Figura 3.184 Vista general de “Peer1” que une el AS300 con el AS400	107
Figura 3.185 Estado de la interfaz “Peer1” que une el AS300 con el AS400.....	107
Figura 3.186 Vista general de “Peer1” que une el AS300 con el AS500	108
Figura 3.187 Vista general de “Peer1” que une el AS300 con el AS500	108
Figura 3.188 Ingreso de la dirección de la red a que se conecta el <i>router</i> AS400 en “BGP Network”	108
Figura 3.189Tabla de rutas aprendidas por el <i>router</i> AS200	109
Figura 3.190 Tabla de rutas aprendidas por el <i>router</i> AS300	109
Figura 3.191 Tabla de rutas aprendidas por el <i>router</i> AS400	109
Figura 3.192 Tabla de rutas aprendidas por el <i>router</i> AS500	110
Figura 3.193 Asignación de una dirección IP a la PC2 que se conecta al <i>router</i> AS200	110
Figura 3.194 Asignación de una dirección IP a la PC1 que se conecta al <i>router</i> AS400	110
Figura 3.195 Asignación de una dirección IP a la PC3 que se conecta al <i>router</i> AS500	110
Figura 3.196 <i>Ping</i> desde la PC2 hacia la dirección IP 192.168.10.1	110

Figura 3.197 <i>Ping</i> desde la PC1 hacia la dirección IP 192.168.10.1	110
Figura 3.198 <i>Ping</i> desde la PC3 hacia la dirección IP 192.168.10.1	111
Figura 3.199 Diagrama de conexiones práctica 5	112
Figura 3.200 Pestaña “Crear máquina virtual” de <i>VirtualBox</i>	113
Figura 3.201 Pestaña “Crear disco duro virtual” de <i>VirtualBox</i>	113
Figura 3.202 Creación de la máquina virtual de <i>Windows 7</i> llamada “Cliente”	114
Figura 3.203 Carga de la imagen con el sistema operativo <i>Windows 7</i>	114
Figura 3.204 Espacio asignado para la máquina virtual.	114
Figura 3.205 Lista de direcciones IP del <i>router</i> REMOTO.....	115
Figura 3.206 Lista de direcciones IP del <i>router</i> BORDE.....	115
Figura 3.207 Lista de rutas aprendidas en el <i>router</i> REMOTO.....	115
Figura 3.208 Lista de rutas que ha aprendido el <i>router</i> BORDE	115
Figura 3.209 Configuración y delimitación del <i>Pool</i> de direcciones IP.....	116
Figura 3.210 <i>Pool</i> de direcciones IP creado.....	116
Figura 3.211 Habilitación de “PPTP <i>Server</i> ”	116
Figura 3.212 Configuración correspondiente a “PPTP <i>Server</i> ”.....	117
Figura 3.213 Creación de una nueva interfaz	117
Figura 3.214 Configuraciones realizadas para crear una interfaz.....	117
Figura 3.215 Interfaz levantada para PPP	117
Figura 3.216 Pestaña para agregar un nuevo perfil	118
Figura 3.217 Configuración del nuevo perfil.....	118
Figura 3.218 Nuevo perfil creado para PPP.....	118
Figura 3.219 Parámetros configurados en “ <i>Secrets</i> ”	119
Figura 3.220 Creación de un nuevo usuario	119
Figura 3.221 Configuración de la regla uno	119
Figura 3.222 Configuración de la regla dos.....	119
Figura 3.223 Reglas creadas para el funcionamiento de PPTP	120
Figura 3.224 Configuración de NAT	120
Figura 3.225 Regla NAT creada	120
Figura 3.226 Pantalla “Centro de redes y recursos compartidos” de <i>Windows 7</i>	121
Figura 3.227 Pantalla “Conexiones de Red”	121
Figura 3.228 Pestaña de “Propiedades de Conexión de área local”.....	121
Figura 3.229 Configuración de la dirección IP del cliente <i>Windows</i>	122
Figura 3.230 <i>Ping</i> realizado hacia el <i>Gateway</i>	122
Figura 3.231 Ingreso para la configuración del servidor PPTP al centro de redes y recursos.....	122

Figura 3.232 Pestaña para configurar una nueva conexión de red	123
Figura 3.233 Selección del tipo de conexión.....	123
Figura 3.234 Configuración de la conexión.....	123
Figura 3.235 Configuración de los parámetros del servidor PPTP en <i>Windows</i>	124
Figura 3.236 Habilitación del adaptador de red PPTP.....	124
Figura 3.237 Configuración de parámetros para PPTP.....	124
Figura 3.238 Selección del tipo de VPN.....	125
Figura 3.239 Unirse al servidor PPTP mediante el adaptador de red.....	125
Figura 3.240 Configuración del usuario y clave para PPTP	125
Figura 3.241 Vista general de los adaptadores de red de <i>Windows</i>	126
Figura 3.242 Configuraciones de la máquina para los adaptadores de red, ingresando a CMD	126
Figura 3.243 Dirección IP asignada a la PC1 según la topología.....	126
Figura 3.244 Dirección IP asignada a la PC2 según la topología.....	126
Figura 3.245 Dirección IP asignada a la PC3 según la topología.....	127
Figura 3.246 Dirección IP asignada a la PC4 según la topología.....	127
Figura 3.247 <i>Ping</i> desde el cliente de <i>Windows</i> hacia la PC1.....	127
Figura 3.248 <i>Ping</i> desde el cliente de <i>Windows</i> hacia la PC2.....	127
Figura 3.249 <i>Ping</i> desde el cliente de <i>Windows</i> hacia la PC3.....	127
Figura 3.250 <i>Ping</i> desde el cliente de <i>Windows</i> hacia la PC4.....	128
Figura 3.251 Traceo realizado desde el cliente hacia la PC1, para comprobar que PPTP se encuentre levantado.....	128
Figura 3.252 Traceo realizado desde el cliente hacia la PC1, para comprobar que PPTP no se encuentra activo una vez que se desactivó el adaptador	128
Figura 3. 253 Diagrama de conexiones práctica 6	130
Figura 3.254 Direcciones IP aprendidas por RA	131
Figura 3.255 Direcciones IP aprendidas por RB	131
Figura 3.256 Direcciones IP aprendidas por RC	131
Figura 3.257 Direcciones IP aprendidas por RD	131
Figura 3.258 Configuración para crear una interfaz lógica en RA	131
Figura 3.259 Interfaz lógica creada en el <i>router</i> RA	131
Figura 3.260 Configuración para crear una interfaz lógica en RB	132
Figura 3.261 Interfaz lógica creada en el <i>router</i> RB	132
Figura 3.262 Configuración para crear una interfaz lógica en RC	132
Figura 3.263 Interfaz lógica creada en el <i>router</i> RC.....	132
Figura 3.264 Configuración para crear una interfaz lógica en RD	133

Figura 3.265 Interfaz lógica creada en el <i>router</i> RD.....	133
Figura 3.266 Asignación de una dirección IP a la interfaz creada para el <i>router</i> RA .	133
Figura 3.267 Asignación de una dirección IP a la interfaz creada para el <i>router</i> RB .	133
Figura 3.268 Asignación de una dirección IP a la interfaz creada para el <i>router</i> RC .	134
Figura 3.269 Asignación de una dirección IP a la interfaz creada para el <i>router</i> RD .	134
Figura 3.270 Agregar y configurar la instancia con la dirección IP asignada a la interfaz lógica para el <i>router</i> RA.....	134
Figura 3.271 Instancia creada en el <i>router</i> RA.....	135
Figura 3.272 Agregar y configurar la instancia con la dirección IP asignada a la interfaz lógica para el <i>router</i> RB.....	135
Figura 3.273 Instancia creada en el <i>router</i> RB.....	135
Figura 3.274 Agregar y configurar la instancia con la dirección IP asignada a la interfaz lógica para el <i>router</i> RC.....	135
Figura 3.275 Instancia creada en el <i>router</i> RC.....	136
Figura 3.276 Agregar y configurar la instancia con la dirección IP asignada a la interfaz lógica para el <i>router</i> RD.....	136
Figura 3.277 Instancia creada en el <i>router</i> RD.....	136
Figura 3.278 Lista de redes agregadas en el <i>router</i> RA para el funcionamiento de OSPF	136
Figura 3.279 Lista de redes agregadas en el <i>router</i> RB para el funcionamiento de OSPF	137
Figura 3.280 Lista de redes agregadas en el <i>router</i> RC para el funcionamiento de OSPF	137
Figura 3.281 Lista de redes agregadas en el <i>router</i> RD para el funcionamiento de OSPF	137
Figura 3.282 Verificación en la pestaña “ <i>Interfaces</i> ” que el protocolo se encuentra levantado en el <i>router</i> RA	137
Figura 3.283 Verificación en la pestaña “ <i>Interfaces</i> ” que el protocolo se encuentra levantado en el <i>router</i> RB	137
Figura 3.284 Verificación en la pestaña “ <i>Interfaces</i> ” que el protocolo se encuentra levantado en el <i>router</i> RC	138
Figura 3.285 Verificación en la pestaña “ <i>Interfaces</i> ” que el protocolo se encuentra levantado en el <i>router</i> RD	138
Figura 3.286 Tabla de rutas aprendidas por el <i>router</i> RA.....	138
Figura 3.287 Tabla de rutas aprendidas por el <i>router</i> RB.....	138
Figura 3.288 Tabla de rutas aprendidas por el <i>router</i> RC	139

Figura 3.289 Tabla de rutas aprendidas por el <i>router</i> RD	139
Figura 3.290 Pestaña principal de “ <i>Traceroute</i> ”	139
Figura 3.291 Traceo con destino a una dirección IP del <i>router</i> RD	140
Figura 3.292 Inicialización y resultados del traceo realizado desde RA a RD	140
Figura 3.293 Pestaña “ <i>LDP Setting</i> ”	140
Figura 3.294 Pestaña “ <i>LDP Setting</i> ” con las opciones configuradas para el <i>router</i> RA	141
Figura 3.295 Pestaña “ <i>LDP Setting</i> ” con las opciones configuradas para el <i>router</i> RB	141
Figura 3.296 Pestaña “ <i>LDP Setting</i> ” con las opciones configuradas para el <i>router</i> RC	141
Figura 3.297 Pestaña “ <i>LDP Setting</i> ” con las opciones configuradas para el <i>router</i> RD	142
Figura 3.298 Agregar la interfaz con la que se une RA con RB	142
Figura 3.299 Interfaz levantada para el <i>router</i> RA, para el funcionamiento de MPLS	142
Figura 3.300 Interfaces levantadas para el <i>router</i> RB, para el funcionamiento de MPLS	142
Figura 3.301 Interfaces levantadas para el <i>router</i> RC, para el funcionamiento de MPLS	143
Figura 3.302 Interfaz levantada para el <i>router</i> RD, para el funcionamiento de MPLS.	143
Figura 3.303 Procolo LDP levantado en el <i>router</i> RA.....	143
Figura 3.304 Procolo LDP levantado en el <i>router</i> RB.....	143
Figura 3.305 Procolo LDP levantado en el <i>router</i> RC.....	143
Figura 3.306 Procolo LDP levantado en el <i>router</i> RD.....	144
Figura 3.307 Tabla de reenvío de datos que se ha llenado en el <i>router</i> RA.....	144
Figura 3.308 Tabla de reenvío de datos que se ha llenado en el <i>router</i> RB.....	144
Figura 3.309 Tabla de reenvío de datos que se ha llenado en el <i>router</i> RC.....	144
Figura 3.310 Tabla de reenvío de datos que se ha llenado en el <i>router</i> RD.....	144
Figura 3.311 Nueva pestaña abierta para realizar un traceo.....	145
Figura 3.312 Inicialización y resultado del traceo, en la pestaña “ <i>Status</i> ”	145
Figura 3.313 Traceo obtenido usando el protocolo OSPF.....	145
Figura 3.314 Traceo obtenido usando la tecnología MPLS.....	146

ÍNDICE DE TABLAS

Tabla 3.1 Línea de Comandos básicos usados en GNS3	48
Tabla 3.2 Íconos de la interfaz de GNS3	48

RESUMEN

Este proyecto tiene como objetivo el estudio del *software* GNS3, para simular diagramas de red utilizando equipos de red de la marca *Mikrotik*.

La finalidad es proporcionar los conocimientos básicos necesarios para que los estudiantes y docentes de la Escuela de Formación de Tecnólogos (ESFOT) puedan familiarizarse con GNS3 y demás programas complementarios, para realizar la simulación, configuración, e implementación de topologías de red usando equipos *Mikrotik*. Afianzando mediante la simulación de diferentes topologías los conocimientos inherentes a la formación educativa de los estudiantes. Los tópicos de las prácticas han sido seleccionados tomando en consideración el PEA de las materias: TCI/IP y Redes de Computadoras, de la Carrera de Tecnología Superior en Redes y Telecomunicaciones de la ESFOT.

Este trabajo cuenta con hojas guías, tanto para docentes como para estudiantes, en las mismas se detallan los procedimientos a seguir de cada una de las prácticas propuestas, configuración de equipos y observaciones importantes, de ser necesarias.

Finalmente se encuentra las conclusiones y recomendaciones obtenidas a lo largo de la realización del proyecto.

PALABRAS CLAVE: GNS3, *Mikrotik*, *Winbox*, *Oracle VM VirtualBox*.

ABSTRACT

This project aims to study GNS3 software, to simulate network diagrams using Mikrotik brand routers.

The objective is to provide the basic knowledge necessary for students and teachers of the Escuela de Formación de Tecnólogos (ESFOT) to become familiar with GNS3 and other complementary programs, in order to simulate, configure and implement network topologies using Mikrotik equipment. Reinforce, by simulating different topologies, the knowledge inherent to the educational training of students. The topics have been selected considering the PEA: TCI/IP and Computer Networks of the Superior Technology in Networks and Telecommunications career of the ESFOT.

This work has guide sheets for both teachers and students. These detail the procedures to be followed for each of the proposed practices, equipment configuration and important observations if necessary.

Finally, there are the conclusions and recommendations obtained throughout the project.

KEYWORDS: GNS3, Mikrotik, Winbox, Oracle VM VirtualBox.

1 INTRODUCCIÓN

En los últimos años la tecnología ha ido avanzando de manera acelerada, lo cual ha hecho que nuevas compañías surjan en el mundo de las telecomunicaciones. Ofreciendo en su catálogo, equipos con características y funciones similares a las que la compañía CISCO brinda. Este es el caso de los equipos *Mikrotik*, que por su accesibilidad económica y prestaciones han empezado a ser adquiridos por las empresas. Siendo esta una de las razones para adquirir los conocimientos relacionados a su manejo y configuración.

La Escuela Politécnica Nacional (EPN) dentro de su plan de estudio ha tenido presente el manejo de redes mediante el simulador *Cisco Packet Tracer*, implementando varios diseños y topologías de red, pero con el uso limitado únicamente a los equipos CISCO.

La Escuela de Formación de Tecnólogos (ESFOT) enfoca la enseñanza al ámbito práctico y aplicativo, concentra sus esfuerzos en que los estudiantes sean capaces de salir al mundo laboral y puedan afrontar el manejo y configuración de equipos de varias marcas.

Por lo antes expuesto este proyecto busca obtener los conocimientos necesarios para que los estudiantes de la ESFOT puedan simular topologías de red con equipos *Mikrotik* mediante el *software* GNS3. Además, brindar al docente una herramienta virtual de enseñanza para la configuración y experimentación con los equipos, previo a la implementación en los equipos físicos.

1.1 Objetivo general

Desarrollar guías prácticas para la simulación de redes con equipos *Mikrotik* utilizando GNS3.

1.2 Objetivos específicos

1. Analizar los niveles de licencias de los *routers MIKROTIK* disponibles en el mercado.
2. Analizar las funcionalidades y herramientas que comprende GNS3.
3. Analizar las topologías de red que se pueden implementar en GNS3 con equipos *MIKROTIK*.
4. Elaborar las hojas guías de prácticas.

1.3 Fundamentos

Mikrotik

Es una empresa fundada en 1996 con el fin de desarrollar enrutadores y sistemas *ISP* inalámbricos. En la actualidad proporciona *hardware* y *software* para la conectividad a Internet en la mayoría de los países del mundo [1].

RouterOS

Es un sistema operativo de un *router Mikrotik*, se lo puede instalar en una PC y lo convertirá en un enrutador con todas las características necesarias: enrutamiento, *firewall*, administración de ancho de banda, punto de acceso inalámbrico, servidor VPN, entre otras [2].

Winbox

Es una aplicación que permite la administración de *Mikrotik RouterOS* usando una GUI (*Graphical User Interface*) rápida y simple. La mayor parte de las funciones de *Winbox* se encuentran en consola, es por esto que no hay secciones de esta aplicación en manuales [3].

Solar Putty

Es una aplicación que permite administrar sesiones remotas y conectarse a cualquier dispositivo en la red. Tiene la capacidad de administrar múltiples sesiones desde una consola, adicional permite que los usuarios puedan guardar sus credenciales o claves privadas facilitando así el inicio de sesión [4].

GUI (Graphical User Interface)

Es un conjunto de componentes gráficos que ayudan a la interacción entre el usuario y la aplicación mediante ventanas, botones, cajas de diálogo, etc. [5].

RIP (Routing Information Protocol)

Protocolo de vector-distancia que utiliza como métrica para la selección de rutas el conteo de saltos, es decir, elige el mejor camino tomando en cuenta el menor número de saltos y así evitar que el paquete enviado caiga en una ruta infinita o inalcanzable, esto sucede cuando se excede el número máximo de saltos, en el caso del protocolo RIP es de 15 saltos. Se tiene RIPv1 realiza encaminamientos *classfull* o con clase y RIPv2 encaminamientos *classless* o sin clase, es decir se puede usar diferentes máscaras, ideal para subredes [6].

NAT (*Network Address Traduction*)

Es la traducción de direcciones de red, se encuentra diseñada para la conservación de direcciones IP. Permite el mapeo uno a uno, es decir, de una dirección IP privada a una dirección IP pública para que los paquetes puedan ser enviados a través del Internet [7].

BGP (*Border Gateway Protocol*)

Trabaja con TCP como protocolo de transporte en el puerto 179, el cual permite la creación de enrutamientos sin bucles usando sistemas autónomos. Los enrutadores BGP intercambian información en cuanto a la accesibilidad de la red principalmente indicaciones de las rutas completas a seguir para llegar hacia algún destino [8].

Sistema autónomo

Es el conjunto de enrutadores que se encuentran bajo una única administración técnica [8].

OSPF (*Open Shortest Path First*)

Es un protocolo de puerta de enlace interior *classless* o sin clase utilizado para la distribución de la información de enrutamiento en un sistema autónomo, permite determinar la red de destino utilizando máscaras diferentes a la máscara por defecto del equipo principal. OSPF recalcula las rutas rápidamente cada cambio de topología es por esto que cada *router* mantiene en su base de datos la topología exacta de la red a la que pertenece además proporciona un balanceo de cargas de rutas de igual peso. [9]

PPTP (*Point to Point Tunneling Protocol*)

Es un protocolo de red utilizado para la implementación de redes virtuales privadas opera con el puerto TCP 1723, fue desarrollado para encapsular al protocolo PPP (Protocolo Punto a Punto) asegurando una buena velocidad y compatibilidad tanto para equipos de cómputo como para dispositivos móviles. Entre las características que posee este protocolo la encriptación y autenticación es la mayor vulnerabilidad de seguridad que posee PPTP. [10]

VPN (*Virtual Private Network*)

Es un túnel seguro entre un dispositivo e internet, en el cual los usuarios pueden proteger su tráfico de internet y ocultar su identidad en línea. Un servidor VPN actúa como un proxy o suplente para su actividad dentro de la *web* ayudando a que el usuario sea anónimo en internet mediante la tunelización y encriptación de la información que viaja entre en el usuario y el servidor, encapsulando el paquete de datos para que terceros no tengan acceso a dicha información. Entre los protocolos que maneja las

VPN los más comunes son PPTP, L2TP y SSTP favoreciendo sea a la velocidad de transmisión de la información o a la seguridad de la información enviada. [11]

Oracle VM VirtualBox

Es un potente programa de virtualización tanto de uso empresarial como doméstico, se encuentra de manera gratuita como *software* de código abierto [12].

MPLS (Multiprotocol Label Switching)

Es un estándar de conmutación de paquetes IP creado para la integración de etiquetas durante el reenvío de paquetes en el sistema de enrutamiento. La ruta de un paquete está en función de las tablas de enrutamiento de cada nodo, permitiendo así que cada nodo asigne una etiqueta a cada uno de los elementos de la tabla de enrutamiento y comunique a los nodos vecinos. [13]

2 METODOLOGÍA

2.1 Descripción de la metodología usada

El presente proyecto busca brindar los conocimientos necesarios para llevar a cabo la configuración y diseño de topologías de red con *routers Mikrotik*, de manera que los estudiantes de la Carrera de Tecnología Superior en Redes y Telecomunicaciones de la ESFOT, evidencien lo aprendido teóricamente mediante simulaciones, siguiendo los procedimientos y pasos de las prácticas aquí descritos. Para esto se han usado principalmente tres programas: GNS3, *Oracle VM VirtualBox* y *Winbox*. Además de la imagen con el sistema operativo de un *router Mikrotik* y de una imagen con *Windows 7* de 32 bits.

En el documento se desarrollan los puntos indicados a continuación:

Análisis de los niveles de las licencias para los *routers MIKROTIK*, tiempo de uso y limitaciones o ventajas en cuanto a los protocolos que se pueden implementar simultáneamente con cada nivel.

Análisis de las funcionalidades y herramientas que comprende GNS3, su instalación, creación de máquinas virtuales con el sistema operativo de un *router Mikrotik*, configuración de las máquinas virtuales, la vinculación de las máquinas virtuales creadas en *Oracle VM VirtualBox* con GNS3, diseño de topologías en GNS3 y comandos básicos utilizados en las diferentes topologías propuestas.

Verificación de las topologías de red que se implementan en GNS3 usando equipos MIKROTIK. Tomando como referencia el PEA de las asignaturas de TCP/IP y Redes de Computadoras de la Carrera de Tecnología Superior en Redes y Telecomunicaciones de la ESFOT.

Y por último la elaboración de hojas guías de las prácticas para los estudiantes y docentes.

3 RESULTADOS Y DISCUSIÓN

3.1 Niveles de licencias de los *routers Mikrotik*

Los dispositivos *RouterBOARD* se encuentran preinstalados con una licencia *RouterOS* de nivel 0. En el caso de adquirir una imagen para sistemas X86, es decir, para dispositivos PC se puede obtener una clave de licencia de nivel 1 o mayor, la cual consta de un bloque de símbolos que se consigue creando una cuenta directamente en el sitio oficial de *Mikrotik*: <https://mikrotik.com/download>. La activación de esta licencia se la puede realizar en la terminal del dispositivo o en el menú de licencias de *Winbox*.

La diferencia entre niveles de licencia se encuentra detallada en la Figura 3.1.

Nivel	0 (Modo prueba)	1 (Demo gratis)	3 (WISP CPE)	4 (WISP)	5 (WISP)	6 (CONTROLADOR)
Precio	Libre (sin clave)	Libre (con clave de registro)	Solo para un volumen alto de suscriptores	\$45	\$95	\$250
Punto de Acceso Inalámbrico	Prueba 24 horas	NO	NO	SI	SI	SI
Cliente inalámbrico y puente	Prueba 24 horas	NO	SI	SI	SI	SI
Protocolos: • RIP • OSPF • BGP	Prueba 24 horas	NO	SI	SI	SI	SI
Protocolo PPTP	Prueba 24 horas	1	200	200	500	ILIMITADO
Protocolo EoIP	Prueba 24 horas	1	ILIMITADO	ILIMITADO	ILIMITADO	ILIMITADO
Protocolo PPPoE	Prueba 24 horas	1	200	200	500	ILIMITADO
Protocolo L2TP	Prueba 24 horas	1	200	200	500	ILIMITADO
Protocolo OVPN	Prueba 24 horas	1	200	200	ILIMITADO	ILIMITADO
Interfaces VLAN	Prueba 24 horas	1	ILIMITADO	ILIMITADO	ILIMITADO	ILIMITADO

Figura 3.1 Comparación de niveles de licencias *Mikrotik* [14]

Licencia nivel cero: es uno de los niveles que no tiene restricción alguna en cuanto a funciones y protocolos que se pueden implementar. El inconveniente de este nivel radica en el tiempo de duración de la licencia, ya que solo tiene 24 horas de uso. Una vez culminado el tiempo se debe volver a crear un *router* e instalar una nueva imagen con

el nuevo sistema operativo. Es decir, el uso del *router* está limitado por un conteo regresivo de 24 horas, que se restan cada vez que el *router* permanece activo o encendido. Ya sea en *Winbox*, en los simuladores GNS3 o *VirtualBox*. Pasado ese tiempo la licencia expira y se debe crear un nuevo *router* para usarlo [14].

Licencia nivel 1: es un nivel de licencia demo en donde el tiempo de uso es ilimitado, adicionalmente no tiene costo, pero presenta restricciones en cuanto a protocolos y funciones que pueden implementarse en los *routers* [14].

Licencia nivel 3: es un nivel de licencia para equipos inalámbricos, este nivel se encuentra disponible únicamente al adquirir más de 100 licencias PCx86 [14].

Licencia nivel 4: este nivel de licencia tiene un valor de \$45 que se cancelan una sola vez para su uso indefinido. No tiene restricción de tiempo para el uso de la licencia. En cuanto a los protocolos que se pueden implementar, este permite trabajar hasta con un máximo de 200 protocolos. Adicionalmente tiene 15 días de asistencia gratuita por correo electrónico [14].

Licencia nivel 5: este nivel de licencia tiene un valor de \$95 que se cancelan una sola vez para su uso indefinido. No tiene restricción de tiempo para el uso de la licencia. En cuanto a los protocolos que se pueden implementar este permite trabajar hasta con un máximo de 500 protocolos. Adicionalmente tiene 30 días de asistencia gratuita por correo electrónico [14].

Licencia nivel 6: este nivel de licencia tiene un valor de \$250 que se cancelan una sola vez para su uso indefinido. No tiene restricción de tiempo para el uso de la licencia o los protocolos que se pueden implementar. Adicionalmente tiene 30 días de asistencia gratuita por correo electrónico [14].

Como se puede observar en la descripción antes realizada, a partir del nivel 4 las licencias dejan de ser gratuitas y su costo varía de acuerdo a la cantidad de interfaces que se pueden ocupar en los protocolos como se evidencia en la Figura 3.1. Las licencias nunca expiran, es decir, se la adquiere una sola vez y no requiere de renovación. A menos que se desee cambiar de nivel, en este caso se debe comprar el nuevo nivel, activarlo y usarlo.

Para el desarrollo de las prácticas del presente documento se ha usado la licencia de nivel 0, debido a que para culminarlas no se sobrepasa el tiempo establecido de uso de 24 horas con el *router* en funcionamiento. Además de brindar todas las herramientas y funciones necesarias, sin que se tenga que adquirir alguna de las licencias pagas.

3.2 Funcionalidades y herramientas que comprende GNS3

Descarga e instalación de GNS3

Como primer paso se debe ingresar al sitio oficial de GNS3, para descargar la aplicación: <https://www.gns3.com/software/download>, ver Figura 3.2.

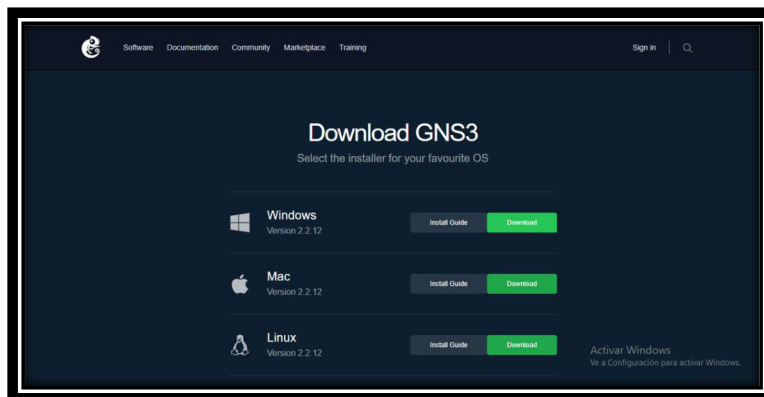


Figura 3.2 Opciones de descargar de GNS3 desde su página oficial [15]

Se descarga el programa GNS3 de acuerdo al sistema operativo del computador. Una vez elegido, aparecerá una ventana que permite la creación de una cuenta para tener acceso a la tienda de GNS3, ver Figura 3.3.

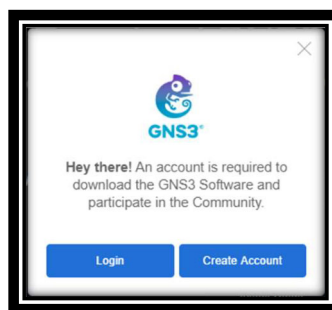


Figura 3.3 Ventana para la creación de una cuenta en GNS3 [14]

Si ya se tiene una cuenta en GNS3 se escoge "login", caso contrario se procede a crear una cuenta nueva, para lo cual se deben llenar los datos que se solicitan en la ficha, ver Figura 3.4. Una vez creada la cuenta ya se puede descargar el programa.

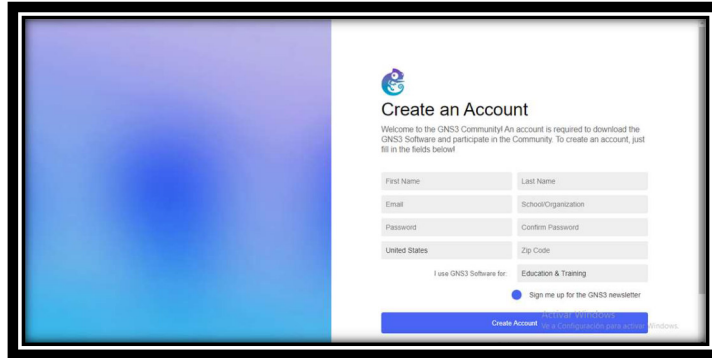


Figura 3.4 Ficha de creación de cuenta GNS3 [16]

Una vez descargado el programa se procede con la instalación del mismo, ver Figura 3.5. Al colocar “Next” aparece la ventana donde se aceptan los términos y condiciones de licencia del programa, se aceptan y continúa.



Figura 3.5 Pestaña principal para la instalación de GNS3

Continuando con la instalación presionar “Next” en todas las ventanas siguientes sin modificar las opciones predeterminadas. Una vez concluida esta sección aparecerá una ventana para la instalación de *Solarwinds* (no es necesario hacerlo, porque además de tener un costo, no tiene uso en el desarrollo de las prácticas), ver Figura 3.6. Presionar “Next” y luego “Finish”. Con eso se concluye la instalación del programa GNS3.

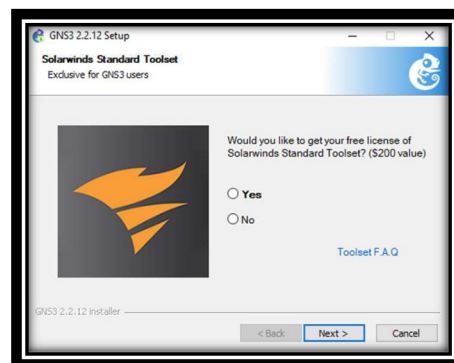


Figura 3.6 Pantalla para instalar *Solarwinds*

Descarga e instalación de *Oracle VM VirtualBox*


Una vez instalado GNS3 se procede con la descarga e instalación de *Oracle VM VirtualBox*, es el programa en el que se crearán las máquinas virtuales para cargar las imágenes del sistema operativo con los *routers Mikrotik*. El programa se lo puede descargar desde el sitio oficial: <https://www.virtualbox.org/wiki/Downloads>, ver la Figura 3.7.



Figura 3.7 Sitio oficial de *Oracle VM VirtualBox* [17]

Se descarga la última versión de *VirtualBox* de forma gratuita y se procede a instalarlo aceptando las configuraciones que el programa lleva predeterminadas de manera automática. Solo se presiona continuar en cada pestaña hasta finalizar la instalación.

Descarga de la imagen con el sistema operativo del *router Mikrotik*

Como siguiente paso se descarga la imagen *ISO* que contiene el sistema operativo del *router Mikrotik*. Para esto, hay que ingresar al sitio oficial de *Mikrotik*: <https://mikrotik.com/download> y hacer clic sobre el ícono , que se encuentra en la fila de "CD Image" para descargar la última versión que se encuentre publicada, ver Figura 3.8.

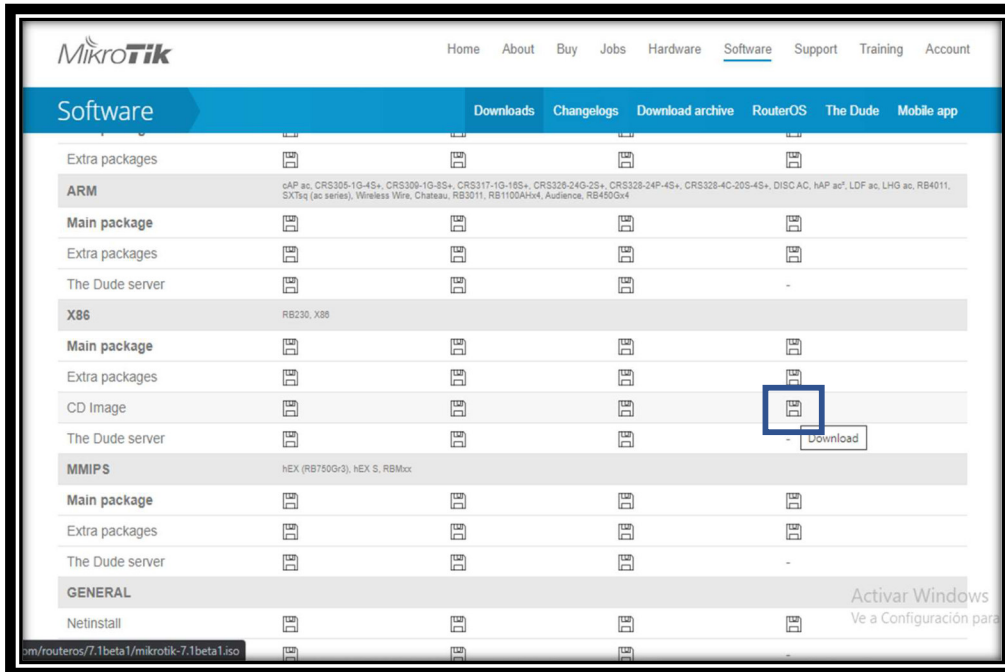


Figura 3.8 Página web para la descarga de la ISO desde el sitio oficial de Mikrotik [18]

En la misma página, en la parte superior, se encuentra una opción de descarga de Winbox, aplicación que también debe ser descargada para su uso posterior.

Creación de un router de Mikrotik en Oracle VM VirtualBox

Una vez instalado Oracle VM VirtualBox se procede a crear una máquina virtual en el programa, en la que se va a cargar la imagen ISO del router Mikrotik para ser vinculada en el programa GNS3 posteriormente.

Para la creación de la máquina virtual se sigue el procedimiento mostrado a continuación:

Ingresar a Oracle VM VirtualBox. Añadir una nueva máquina virtual en la opción "Nueva", como se muestra en la Figura 3.9.



Figura 3.9 Opción "Nueva" para la creación de una máquina virtual

A continuación, se despliega una pestaña donde se coloca el nombre para la nueva máquina virtual, el tipo de sistema operativo y memoria RAM que se le asignará, ver Figura 3.10. Los parámetros a ser configurados son:

- Tipo: *Other*
- Versión: *Other/Unknown*

- Tamaño de memoria: 256 MB
- Disco duro: Crear un disco virtual ahora

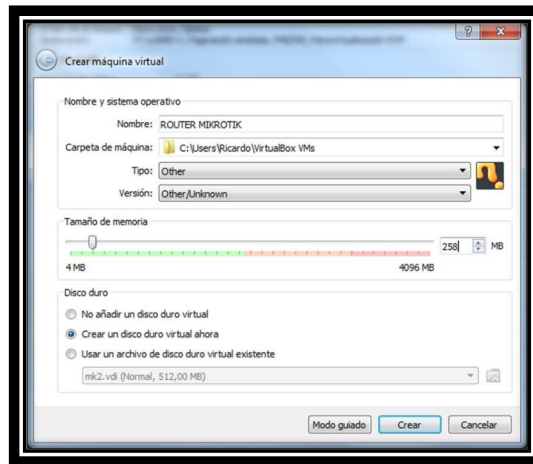


Figura 3.10 Interfaz para la creación de una máquina virtual y parámetros

Se continúa con el proceso designando el tamaño del disco que podrá usar la máquina virtual en el disco duro de nuestro computador, para este caso en concreto se le asignará un espacio de 512 MB. El resto de parámetros quedarán con las opciones predeterminadas por el programa, como se muestra en la Figura 3.11.

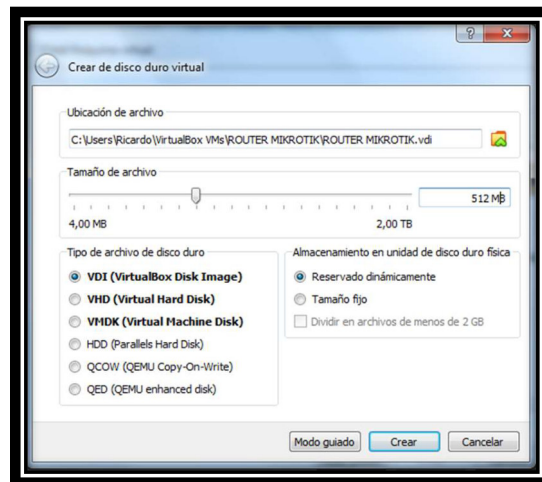


Figura 3.11 Creación del disco duro virtual

Como siguiente paso ingresar a la configuración de la máquina virtual en *Oracle VM VirtualBox*. Seleccionar la máquina creada y hacer clic sobre “Configuración” y se mostrará una nueva pestaña, como indica la Figura 3.12.

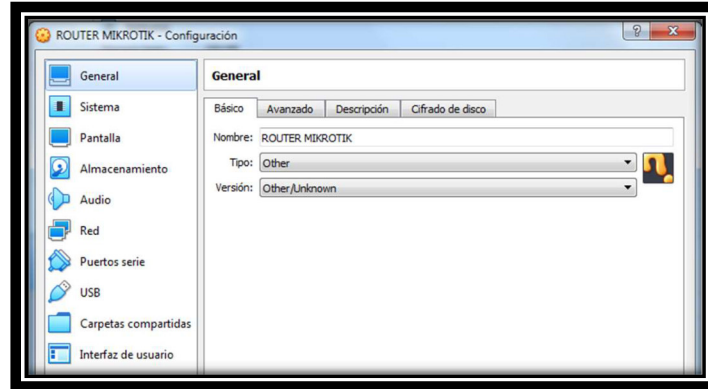


Figura 3.12 Configuración General del router Mikrotik

En la pestaña “Sistema” en “Placa base” de la máquina virtual se debe cambiar la opción “Orden de arranque”, primero colocar “Óptico” y segundo “Disco duro”, ver Figura 3.13..

- Óptico
- Disco duro

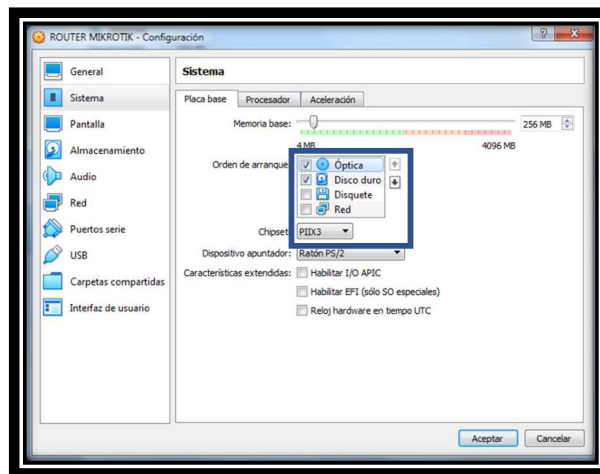


Figura 3.13 Configuración Sistema/Placa base

En la opción “Procesador”: seleccionar “Habilitar PAE/NX”, ver Figura 3.14.

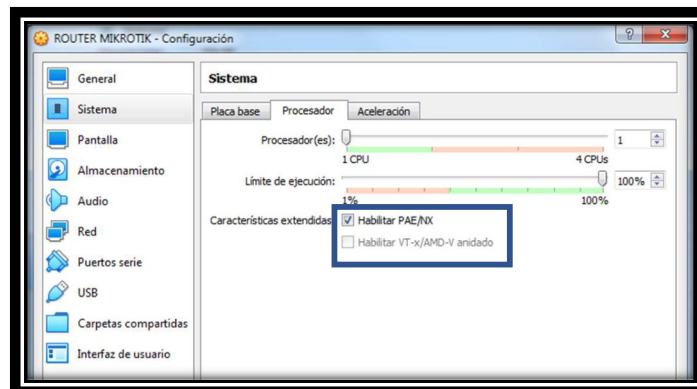



Figura 3.14 Configuración Sistema/Procesador

Al momento de realizar la configuración respectiva en la pestaña de “Almacenamiento”, se necesita agregar un disco para que la máquina virtual arranque, es aquí es donde se va a cargar la imagen ISO con el sistema operativo del *router* previamente descargado. Seleccionar el ícono  y se desplegará una pestaña en donde hay que escoger la opción: “Seleccionar archivo de disco”, como se muestra en la Figura 3.15. Se busca el directorio en donde se encuentra almacenada la ISO y se selecciona.

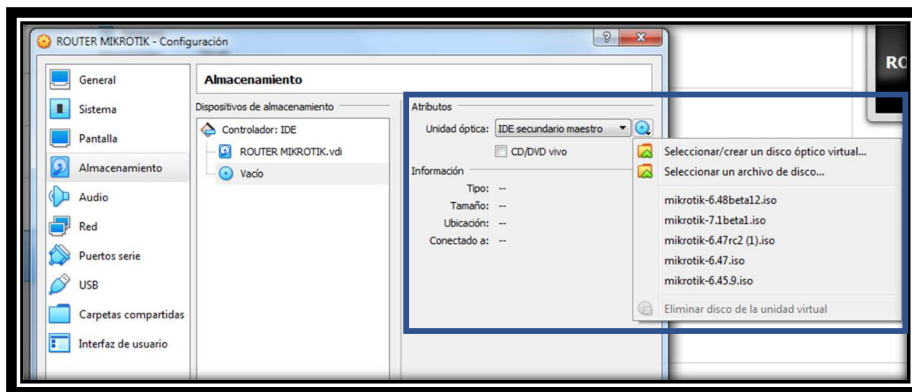


Figura 3.15 Configuración Almacenamiento

Ingresa en la pestaña “Red” y habilitar los 4 adaptadores que posee máquina virtual seleccionando “Habilitar adaptador de red”. Además, todos deben tener seleccionada la opción “Conectado a: No conectado”, ver Figura 3.16.

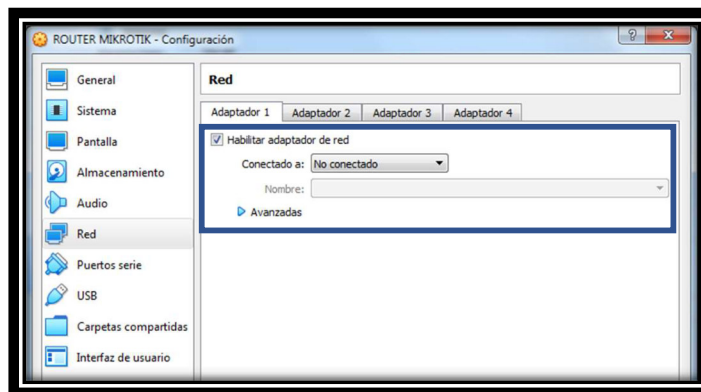


Figura 3.16 Configuración Red/Adaptadores

Con esto se concluye la configuración de la máquina virtual. En la Figura 3.17 se pueden observar los parámetros configurados y características de la máquina virtual creada.

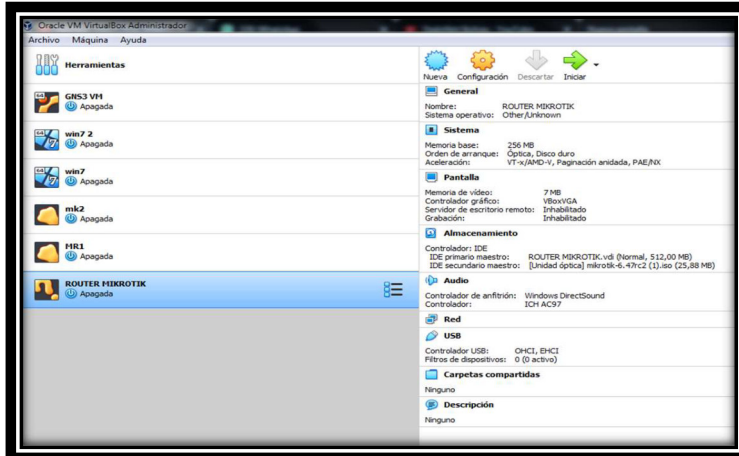



Figura 3.17 Vista general de los detalles y parámetros configurados en la máquina virtual “ROUTER MIKROTIK” en la pantalla de Oracle VM VirtualBox

Se procede con el arranque de la máquina virtual, haciendo clic sobre “Iniciar” . Se presenta una ventana para la instalación del sistema operativo. En la cual se presiona la letra “a”, para seleccionar todas las opciones de instalación propias del sistema operativo del *router*, ver Figura 3.18.

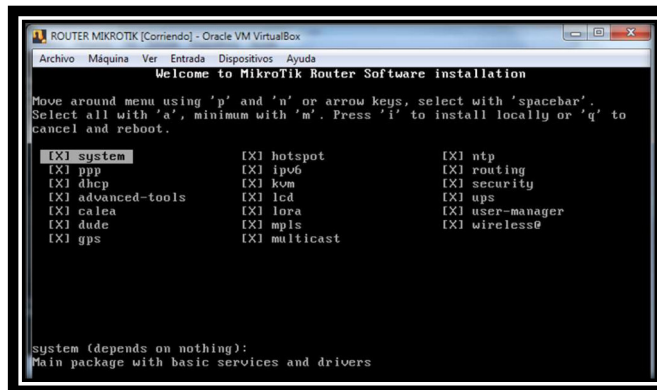


Figura 3.18 Instalación del sistema operativo de *router MikroTik*

Una vez marcado todas las opciones presionar la letra “i” para la instalación. Aparece una pregunta referente a si se desea conservar las configuraciones previas a la instalación. Colocar la letra “n” y luego la letra “y”, en este punto se muestra en detalle la instalación del sistema operativo, ver Figura 3.19. Presionar “ENTER” para continuar y reiniciar la máquina.

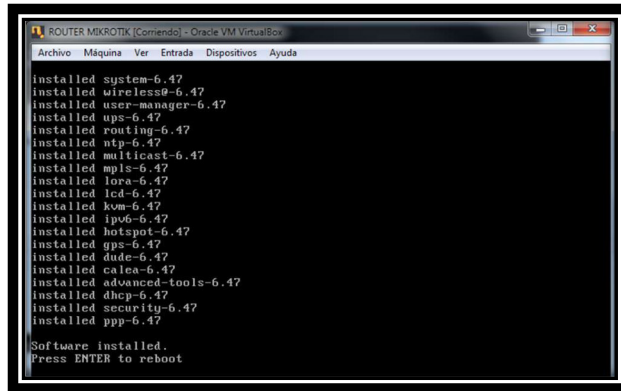


Figura 3.19 Detalle de instalación del sistema operativo de *router Mikrotik*

Una vez reiniciada la máquina virtual, debe ser apagada para realizar un cambio en la configuración. Ingresar a la configuración de la máquina virtual a “Sistema” y en la pestaña “Placa base” cambiar el orden de arranque de la máquina virtual, primero colocar “Disco duro” y segundo “Óptico”, como se muestra en la Figura 3.20.

- Disco duro
- Óptico

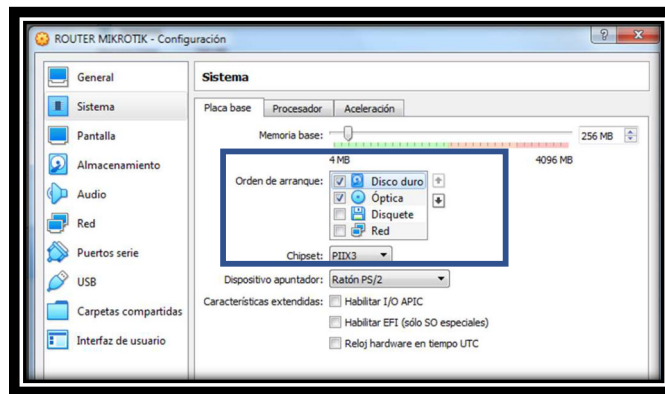



Figura 3.20 Cambio del orden de arranque en Sistema/Placa base de la máquina virtual

Ingresar a “Almacenamiento”, hacer *click* sobre  y en la opción de “Unidad lógica” elegir “Eliminar disco de la unidad virtual”, como se puede observar en la Figura 3.21. Aceptar los cambios y encender la máquina virtual nuevamente.

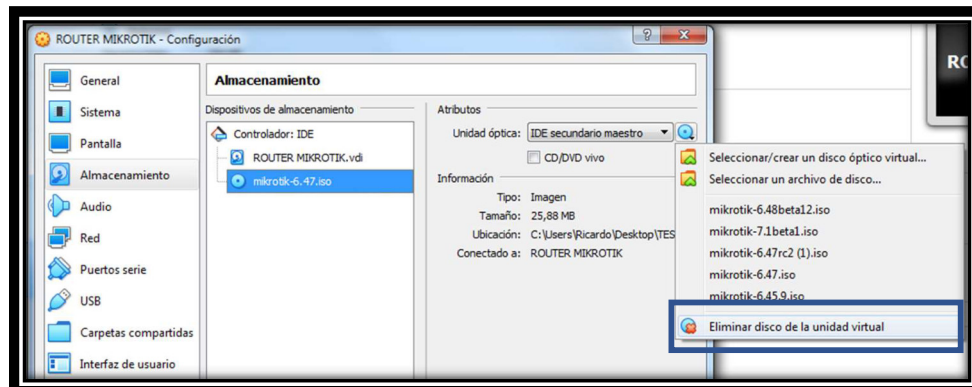


Figura 3.21 Cambios de configuración en Almacenamiento de la máquina virtual

Al arrancar la máquina virtual se pide ingresar un usuario y contraseña, como se muestra en la Figura 3.22. El usuario por defecto es: “admin” y en la contraseña se deja en blanco, presionar “ENTER”.

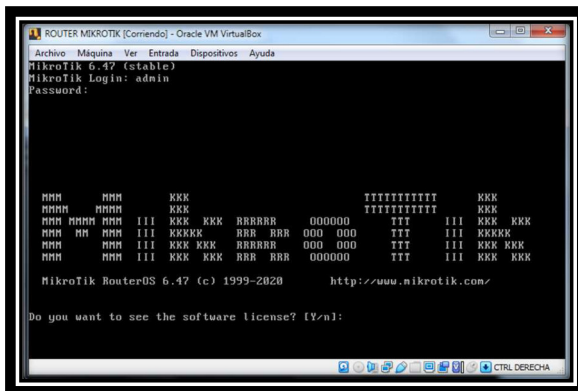


Figura 3.22 Pantalla inicial del router Mikrotik

Se mostrará una pregunta en donde se indica si se desea ver información acerca de la licencia, presionar la letra “n”.

Crear la interfaz de *loopback* en el ordenador principal

Para crear una interfaz de *loopback* en el computador, primero hay que ingresar a “Panel de control” y hacer *clic* en “Administrador de dispositivos”. Aquí se encuentran todos los dispositivos de red, periféricos y de almacenamiento del ordenador, como se muestra en la Figura 3.23.

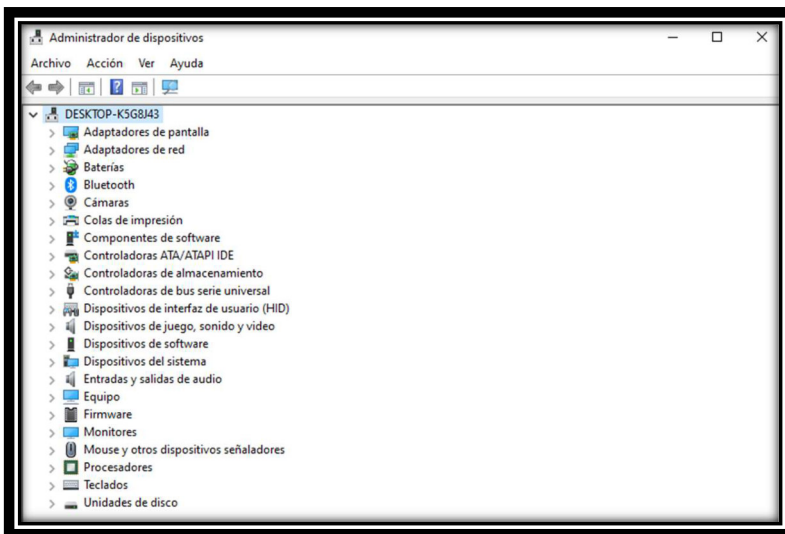


Figura 3.23 Pantalla del Administrador de dispositivos

En la opción “Acción” seleccionar “Agregar *hardware* heredado”, ver Figura 3.24.

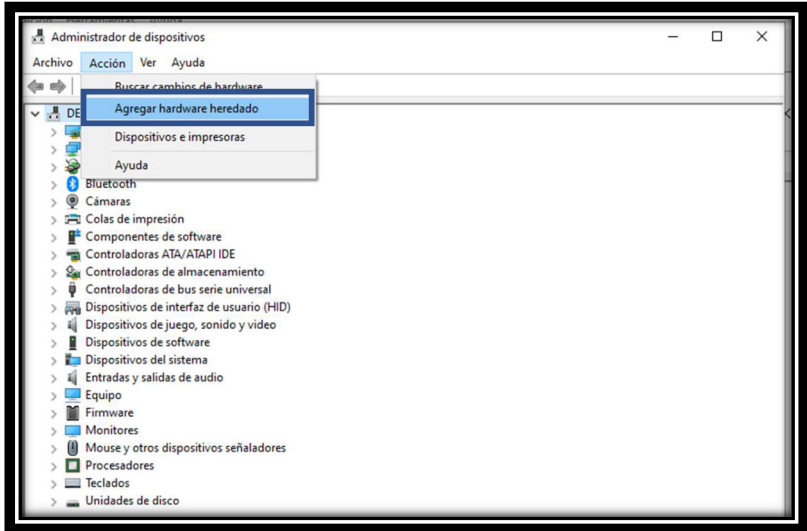


Figura 3.24 Pantalla del Administrador de dispositivos/Agregar *hardware* heredado

Aparecerá una ventana que inicia el proceso de instalación de un nuevo dispositivo en el computador, para este caso específico de agregará una interfaz *loopback* manualmente, como se detalla en los siguientes pasos. Presionar “Siguiente” para continuar, ver Figura 3.25.



Figura 3.25 Asistente para agregar *hardware*

Se muestra una ventana en donde se debe escoger la opción “Instalar el *hardware* seleccionado manualmente de una lista” y presionar “Siguiente”, ver Figura 3.26.

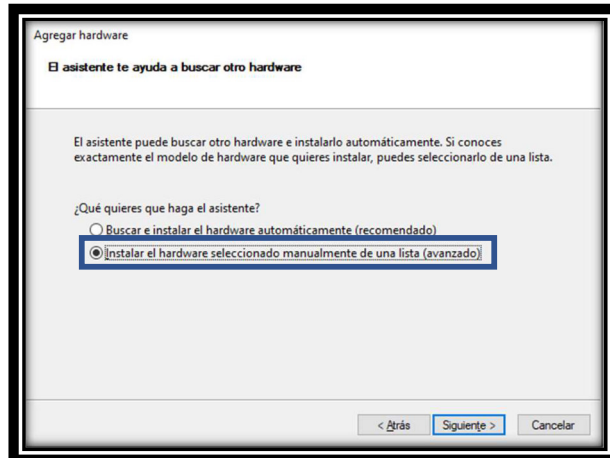


Figura 3.26 Asistente para buscar un *hardware*

De la lista que se despliega seleccionar “Adaptadores de red” y presionar “Siguiente”, ver Figura 3.27.

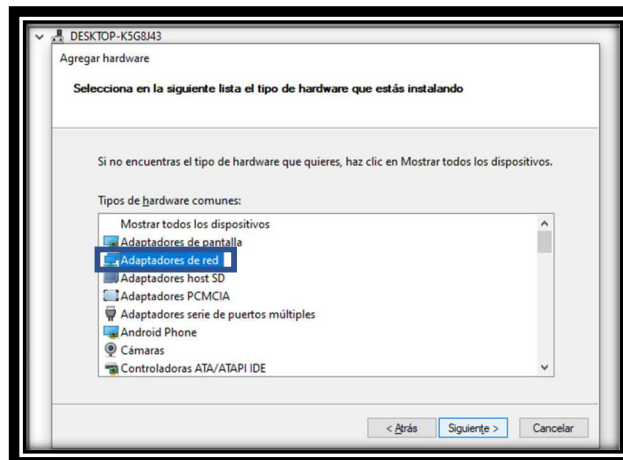


Figura 3.27 Lista de los tipos de *hardware* que pueden ser instalados

En la sección **Fabricante** seleccionar la opción “*Microsoft*” y en la sección **Modelo** escoger la opción “Adaptador de bucle invertido *KM-TEST* de *Microsoft*” y presionar “Siguiente”, ver Figura 3.28.

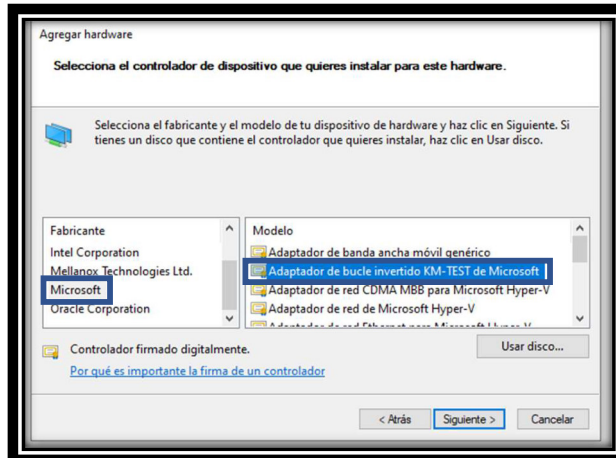


Figura 3.28 Controlador de dispositivos

Una vez instalada la interfaz *loopback*, aparecerá una pestaña que indica la finalización de la instalación para como se observa en la Figura 3.29. Presionar “Finalizar”.

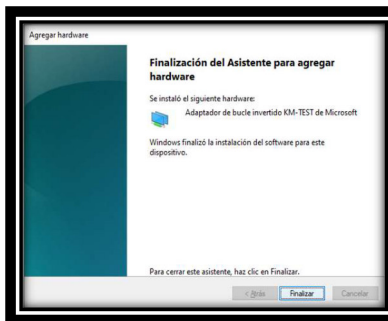


Figura 3.29 Finalización del Asistente para agregar un *hardware* heredado

Se verifica en la pestaña “Administrador de dispositivos” que el “Adaptador de bucle invertido” se ha instalado con normalidad, ver en la Figura 3.30.

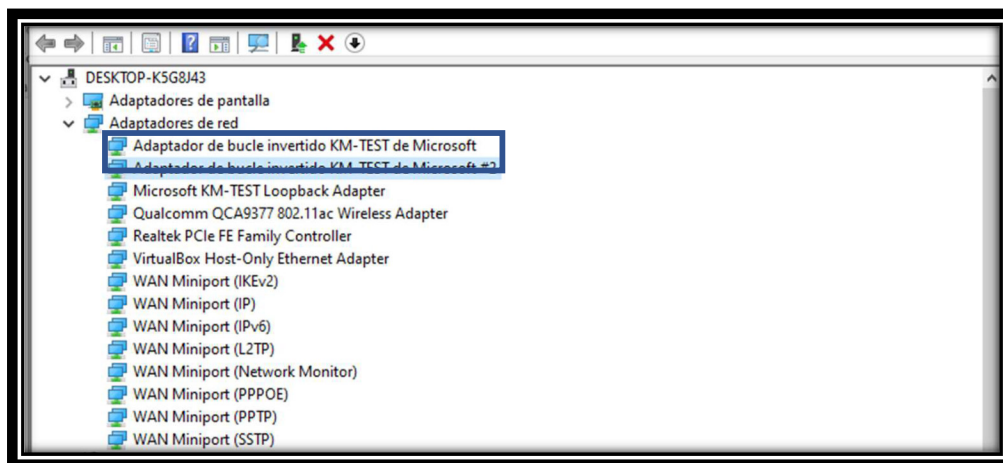


Figura 3.30 Adaptador de bucle invertido creado

Se debe reiniciar el equipo para habilitar las configuraciones del adaptador.

Enlazar la máquina virtual a GNS3

Una vez creada la máquina virtual con el sistema del *router Mikrotik*, se procede a enlazarla con GNS3. Para esto primero se debe iniciar GNS3 haciendo clic sobre el ícono del programa, se iniciará y aparecerá un cuadro de dialogo para asignar un nombre al nuevo proyecto y presionar “OK”. Después seleccionar opción “Edit” ubicada en la parte superior izquierda de la interfaz del programa y seleccionar “Preferences”, allí se procede a vincular la máquina virtual creada en *VirtualBox* con GNS3, ver Figura 3.31.

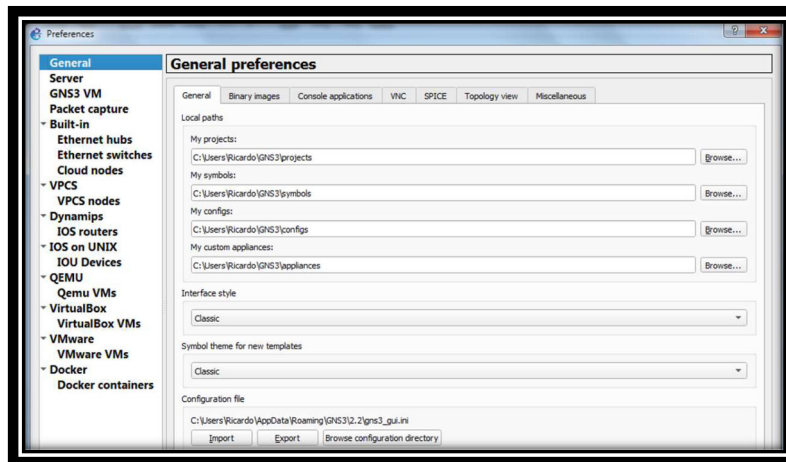


Figura 3.31 Pantalla de *Preferences* en GNS3

Seleccionar la pestaña “*VirtualBox VMs*”. Para agregar la máquina virtual creada en *Oracle VM VirtualBox* a GNS3, se escoge la opción “New”, ver Figura 3.32.

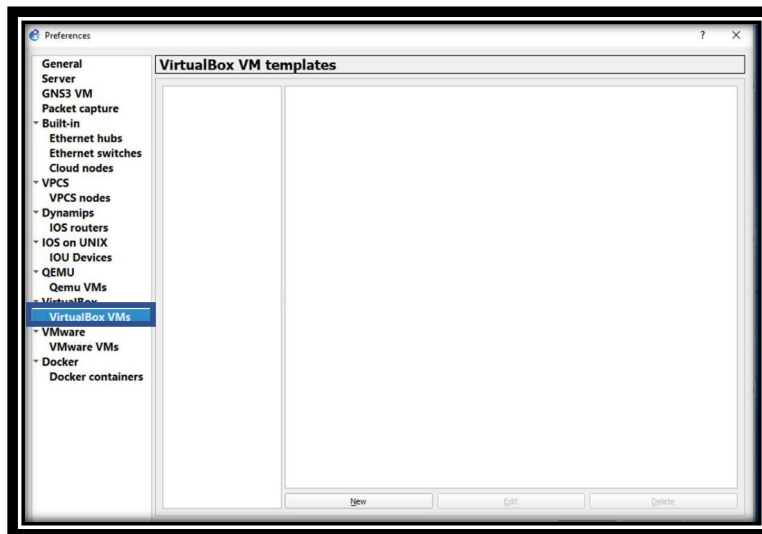


Figura 3.32 Pestaña de *VirtualBox VMs*

Se muestra una ventana y en “VM list:” aparece automáticamente la máquina virtual creada. Hacer *clik* en “Finish” para agregarla a GNS3, como se muestra en la Figura 3.33.

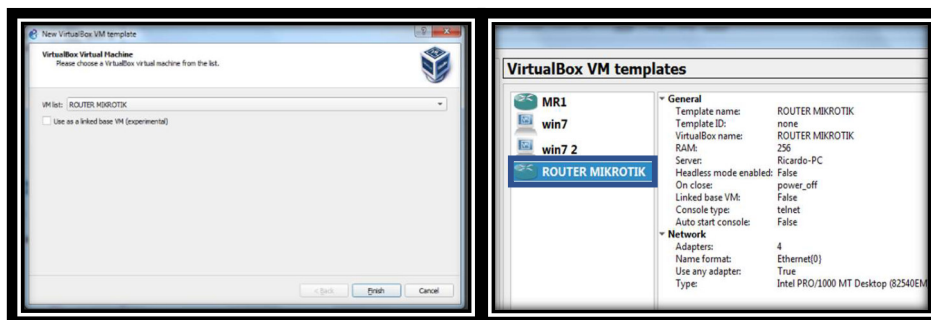


Figura 3.33 Ventana *New VirtualBox VM templates* y máquina agregada.

Una vez añadida se procede a editar ciertos parámetros de la configuración en la máquina virtual para su uso en GNS3, ingresando a “General settings”, ver Figura 3.34. Seleccionar la máquina y hacer *clik* sobre opción “Edit” que mostrará en la parte inferior derecha de la pestaña “VirtualBox VM templates”, los parámetros a editar son los siguientes:

- *Category: Routers*
- *Console Type: Telnet*
- *Symbol: Clic en “Browse...” (aquí se cambia el símbolo del equipo)*

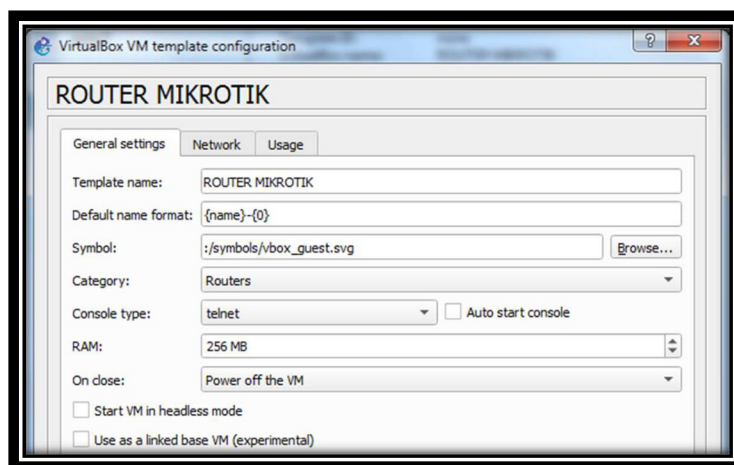


Figura 3.34 Configuración General del *router Mikrotik* en GNS3

Se procede con la configuración de red del *router Mikrotik* seleccionando la pestaña “Network”, como se observa en la Figura 3.35, la información a editar es:

- *Adapters: 4*
- Se habilita la opción “Allow GNS3 to use any configured VirtualBox adapter”. Para permitir que los cambios de configuración de los adaptadores sean validados tanto en *Oracle VM VirtualBox* como en GNS3.

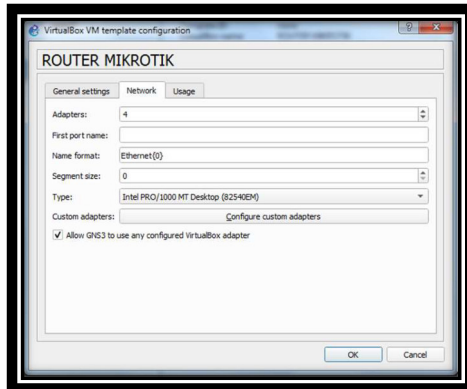


Figura 3.35 Configuración de los adaptadores de red para el *router Mikrotik* en GNS3

Presionar “OK” y luego “Apply”. Aparecerá en la pestaña de *VirtualBox VMs templates* la máquina virtual enlazada a GNS3 (esta se encuentra resaltada con el cuadro de color azul), como se muestra en la Figura 3.36.

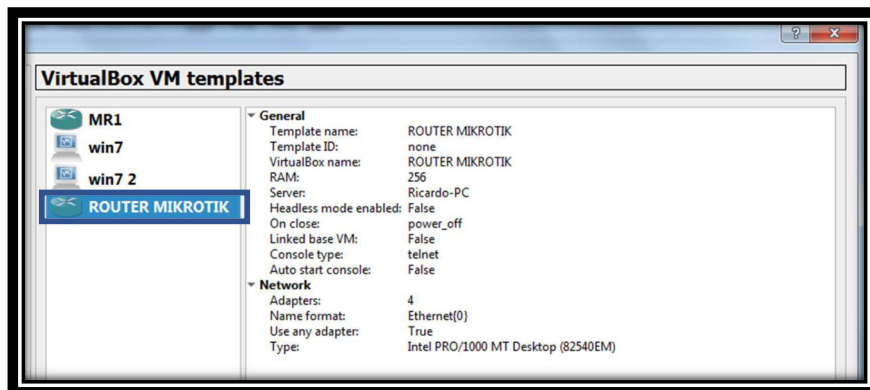



Figura 3.36 Pestaña de *VirtualBox VM templates*

Una vez establecida la vinculación de la máquina entre GNS3 y *VirtualBox*. El *router* aparecerá en la pestaña “*Browse Routers*” , se selecciona y se arrastra hasta la interfaz de GNS3 para usarlo, como se puede observar en la Figura 3.37.

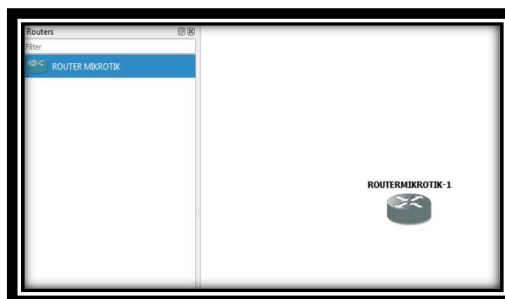



Figura 3.37 Pantalla principal de GNS3 con el *router Mikrotik*

A continuación, se debe agregar un *switch*, para esto se debe ingresar en la opción “*Browse Switches*”  y escoger el dispositivo “*Ethernet Switch*”, ver Figura 3.38. Arrastrarlo hasta la interfaz de GNS3.

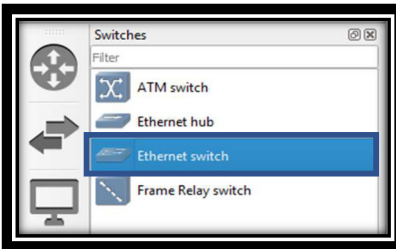


Figura 3.38 Pantalla de *Browse Switches*

Añadir un “*Cloud*” que es usado para vincular la interfaz *loopback* en GNS3. Con la finalidad de establecer un puente entre nuestra tarjeta de red (que usa la interfaz *loopback* como medio virtual para este cometido) y la máquina virtual, utilizando GNS3 como el programa que permite la comunicación entre ambas partes, máquina virtual y tarjeta de red del computador. Se lo encuentra en la opción: “*End devices*” y debe ser arrastrado a la interfaz de GNS3 para su uso, ver Figura 3.39.

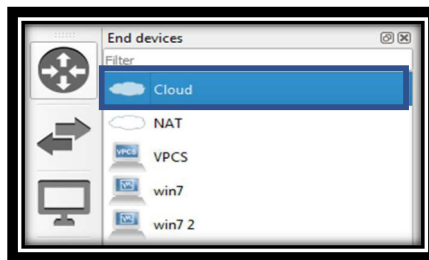



Figura 3.39 Pestaña *End devices* para agregar un *Cloud*

Para agregar los enlaces a la topología se escoge la opción “*Add a link*”  y se une el *router* con el *switch* y de la misma forma el *switch* con *cloud* haciendo *click* sobre el equipo, como se muestra en la Figura 3.40. Se debe tomar en cuenta el puerto *Ethernet* que conecta el *switch* con el *router*, ya que posteriormente este será usado para la vinculación mediante la interfaz *loopback*, en este caso se ha usado el *Ethernet0* (equivalente al Adaptador 1 en *Oracle VM VirtualBox*).

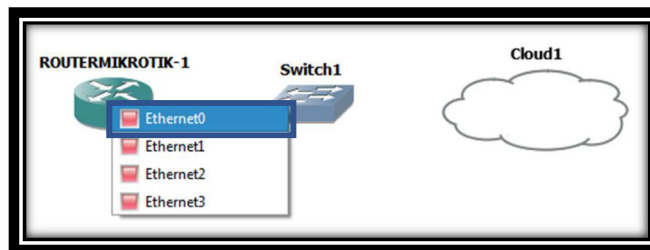


Figura 3.40 Cableado *Router/Switch*

Para el caso del cableado entre el *switch* y *cloud* la conexión se realiza de la misma manera mencionada en el literal anterior. Teniendo en cuenta que se debe seleccionar “*BUCLE INVERTIDO*” para *cloud*. Bucle invertido solo es el nombre que recibe la interfaz

loopback en *Oracle VM VirtualBox* y es denominado así en GNS3, pero viene siendo la misma interfaz para todos los programas, ver Figura 3.41.

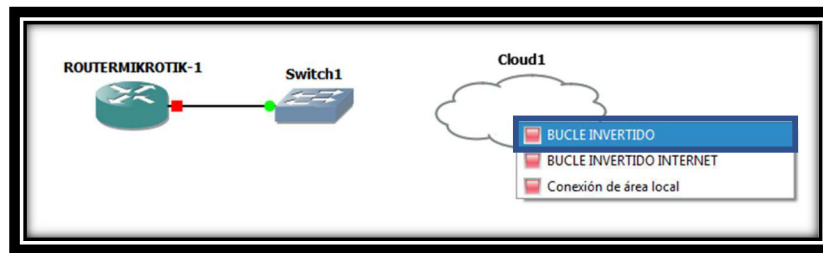


Figura 3.41 Cableado entre *Switch/Cloud*

Otro punto importante es la elección adecuada del adaptador de red de la máquina virtual en *Oracle VM VirtualBox*, para vincularlo con la interfaz de *loopback*. Para realizar este proceso hay que ingresar al programa *Oracle VM VirtualBox* en la sección de configuración de "Red" del *router Mikrotik*, tomar en cuenta que las configuraciones se realizarán en el "Adaptador 1", siendo la misma interfaz que fue conectada al *router* con el *switch* y que es equivalente a "*Ethernet 0*" en GNS3, revisar Figura 3.42.

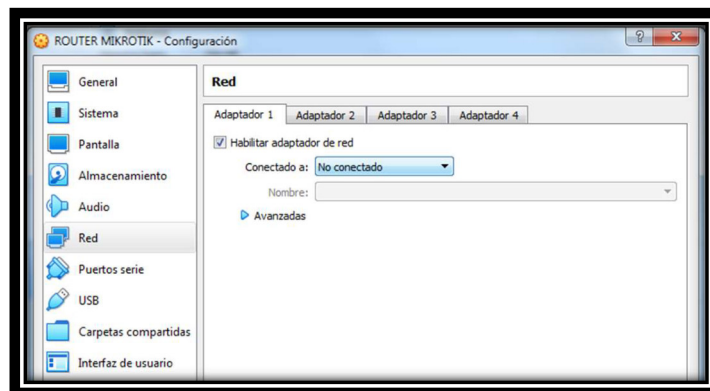


Figura 3.42 Configuración de red *router Mikrotik*

Aquí se debe cambiar la opción "Conectado a:". En la pestaña "Adaptador 1" en la sección "Conectado a:" se pasa de "No conectado" a "Adaptador puente" y en la sección "Nombre:" se escoge "Adaptador de bucle invertido de *Microsoft*", como se muestra en la Figura 3.43. *Clic* en "Aceptar" con ello queda vinculado el adaptador de red a la interfaz *loopback*.

Nota: Como se mencionó anteriormente la interfaz *loopback* recibe diferentes nombres dependiendo del programa en el que se muestre, es decir; En GNS3 se le denomina "BUCLE INVERTIDO" y en *Oracle VM VirtualBox* se le llama "Adaptador de bucle invertido de *Microsoft*".

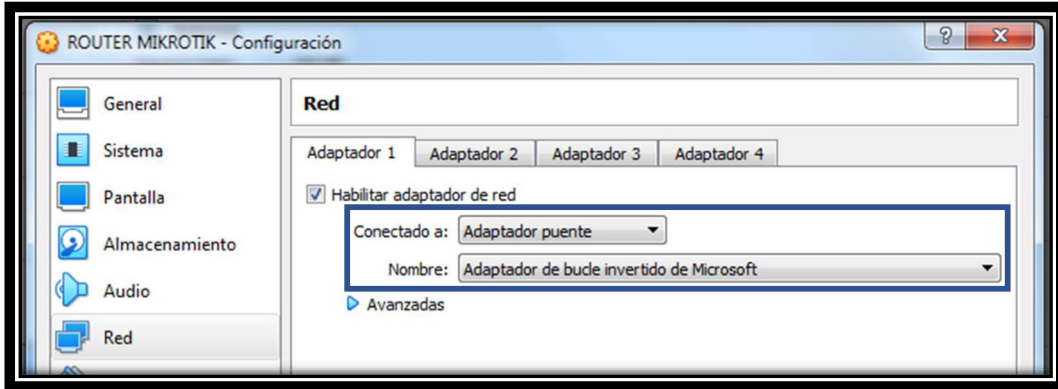



Figura 3.43 Configuración de red para el *router Mikrotik*/Adaptador 1

Inicializar el proyecto creado en GNS3 haciendo *clik* sobre “Iniciar” . Como siguiente punto se debe acceder a la interfaz del *router* mediante *Winbox*. Para ello, abrir la aplicación de *Winbox* haciendo doble *clik* sobre su ícono, se iniciará y mostrará una pantalla. En la parte inferior izquierda se indica la dirección MAC del *router*, como se muestra en la Figura 3.44.

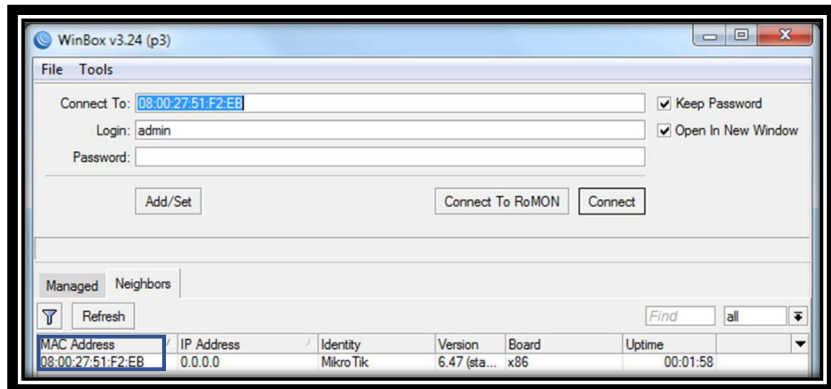


Figura 3.44 Interfaz de conexión de *Winbox*

Seleccionar la dirección *MAC*, hacer *clik* en “*Connect*” y aparecerá una ventana, ver Figura 3.45. En la cual se escoge “*Reconnect*” para establecer la conexión y acceder a las configuraciones del *router* mediante la interfaz de *Winbox*.

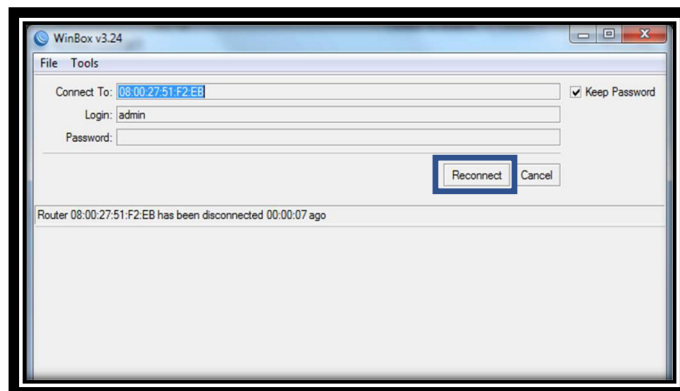


Figura 3.45 Conexión del *router* en *Winbox*

Aparece una pestaña con los términos de la licencia, ver Figura 3.46. Esto es de utilidad cuando se requiere subir el nivel de la licencia, para ese caso solo se coloca "OK". Esto debido a las limitaciones (licencias de nivel 1 y 3) y costos que implican el resto de licencias (licencias de nivel 4, 5 y 6) además de ser usado estrictamente para objetivos prácticos por los estudiantes, se conserva la licencia de nivel 0. Como se explicó anteriormente en la sección 3.1.

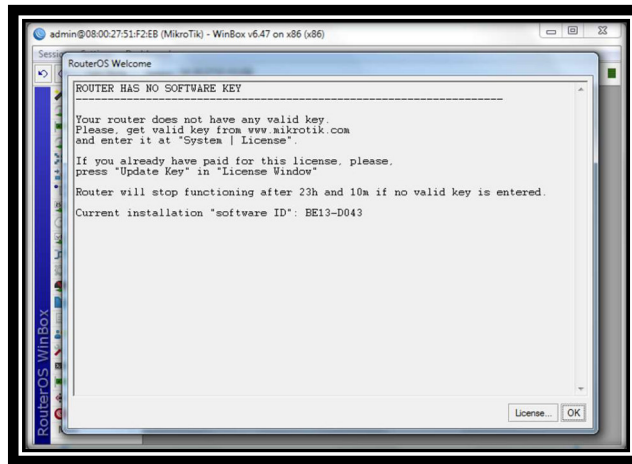


Figura 3.46 Licencias de *router* y actualización de nivel

Se mostrará la interfaz gráfica de *Winbox*, ver Figura 3.47. Interfaz en la que se realizan todas las configuraciones relacionadas al *router*.

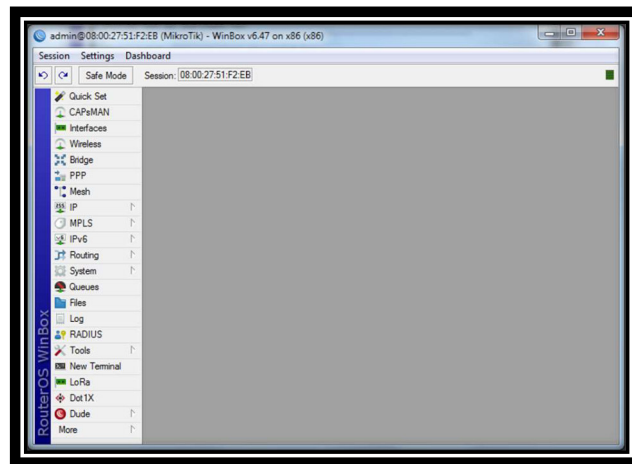


Figura 3.47 Interfaz principal de *Winbox*














Comandos básicos e interfaz de GNS3




En la Tabla 3.1 se encuentran los comandos básicos más usados en las prácticas y en la Tabla 3.2 se describen las herramientas de la interfaz de GNS3 con su funcionamiento e íconos.

Tabla 3.1 Línea de Comandos básicos usados en GNS3

Descripción	Línea de comandos
Asignar un nombre al <i>router</i> .	<code>system identity set name="NOMBRE DEL DISPOSITIVO"</code>
Asignar una dirección IP a una interfaz del <i>router</i> .	<code>ip address add interface=ether# address="Dirección IP/máscara"</code>
Asignar una dirección IP a un VPCS (Telnet).	<code>ip "dirección IP/máscara" "Gateway"</code>

Tabla 3. 2 Íconos de la interfaz de GNS3 [19]

Ícono	Nombre	Descripción
	<i>Manage snapshots</i>	Permite crear una instantánea de los dispositivos, permitiendo crear una versión de guardado de un proyecto.
	<i>Show/Hide Interface labels</i>	Permite mostrar u ocultar las etiquetas de los dispositivos del proyecto en la interfaz de GNS3.
	<i>Console connect to all nodes</i>	Permite abrir las conexiones a cada dispositivo en ejecución.
	<i>Star/Resume all nodes</i>	Permite encender todos los dispositivos dentro del área de trabajo. También puede verificar el estado de los enlaces.
	<i>Suspend all nodes</i>	Permiten suspender los dispositivos dentro del área de trabajo y a la vez pueden someterse a cambios.
	<i>Stop all nodes</i>	Permite detener o apagar todos los dispositivos en el área de trabajo
	<i>Reload all nodes</i>	Permite reiniciar todos los dispositivos dentro del área de trabajo.
	<i>Add a note</i>	Permite agregar notas dentro del área de trabajo con respecto a la topología a diseñar.
	<i>Insert a picture</i>	Permite insertar una imagen de fondo para la topología.
	<i>Draw a rectangle, ellipse, line</i>	Permite agregar y cambiar de manera arbitraria la forma, tamaño y color de las figuras insertadas en el área de trabajo.
	<i>Lock or unlock all items</i>	Permite el bloqueo o desbloqueo de los dispositivos en el área de trabajo.
	<i>Take a screenshot</i>	Permite hacer capturas de los dispositivos en la topología.
	<i>Browse routers</i>	Se encuentran todos los <i>routers</i> instalados por el usuario o por default.

	<i>Browse switches</i>	Se encuentran todos los <i>switches</i> instalados por el usuario o por default.
	<i>End devices</i>	Se encuentran todos los equipos finales instalados por el usuario o por default.
	<i>Add a link</i>	Permite realizar el cableado entre los dispositivos utilizados en el diseño de red.

3.3 Análisis y verificación de las topologías de red que se pueden implementar a través de GNS3 con equipos *Mikrotik*

En este apartado se relacionan los temas del PEA de las asignaturas de TCP/IP y Redes de Computadoras que los estudiantes reciben, para así verificar las topologías de red que se van a implementar en el desarrollo de las prácticas propuestas en el presente documento. La finalidad es que los estudiantes puedan realizar la simulación y comprobación previa a la implementación con los equipos físicos *Mikrotik*.

Se tomó en cuenta los tópicos que los estudiantes reciben en estas materias y se planteó diversas topologías de red afines a las mismas para comprobar su implementación en GNS3. Descartando las que por motivos prácticos no se pudieron concretar, ya sea por errores en el funcionamiento, nivel de dificultad, limitaciones en cuanto a las características que puede brindar un determinado nivel de licencia, capacidad del computador en el que se desarrolló las practicas debido a la alta demanda de memoria RAM que se requería para lograr que todos los dispositivos funcionen simultáneamente, o porque no fueron totalmente acordes al temario que los alumnos reciben. De manera tal, que las prácticas aquí propuestas fueron previamente verificadas e implementadas. Con la finalidad de brindar a los alumnos y docentes una guía útil y comprobada para el desarrollo de las mismas. Por estos motivos se decidió plantear los temas presentados a continuación.

Dentro del PEA de la materia de TCP/IP, se concluyó que las prácticas a realizar son:

CAPÍTULO 3: ENRUTAMIENTO

- Enrutamiento Estático
- Protocolos Vector Distancia (RIP)
- Protocolo BGP

En cuanto al PEA de la materia Redes de Computadoras, se concluyó que la práctica a realizarse es:

CAPÍTULO 5: REDES DE ÁREA EXTENDIDA

- Redes MPLS

Además de la simulación de una VPN con PPTP.

3.4 Elaboración de las hojas guías de prácticas

Teniendo la información sobre las funcionalidades y herramientas de GNS3 y topologías de red que se pueden implementar, se procede a realizar mínimo seis guías prácticas acorde al temario: Introducción a GNS3, Enrutamiento estático, Protocolos de enrutamiento dinámico IGP (*Interior Gateway Protocol*), Protocolo de enrutamiento dinámico EGP (*Exterior Gateway Protocol*), Implementación de red MPLS, Red Privada *Virtual* (VPN).

En las cuales se definirán objetivos, procedimientos y comandos a usar.



ESCUELA POLITÉCNICA NACIONAL
ESCUELA DE FORMACIÓN DE TECNÓLOGOS
HOJA GUÍA
PRÁCTICA 1

1. **TEMA:** Introducción a GNS3

2. **OBJETIVO:**

Familiarizarse con los programas: GNS3, *Oracle VirtualBox Machine* y *Winbox*. Además de las funciones básicas.

3. **TRABAJO PREPARATORIO:**

Cuestionario:

- Definir que es una interfaz de *loopback* (*Windows*), enumerar los pasos para instalarla
- Describir y enumerar las opciones principales de la interfaz de GNS3

4. **DIAGRAMA DE CONEXIONES:**

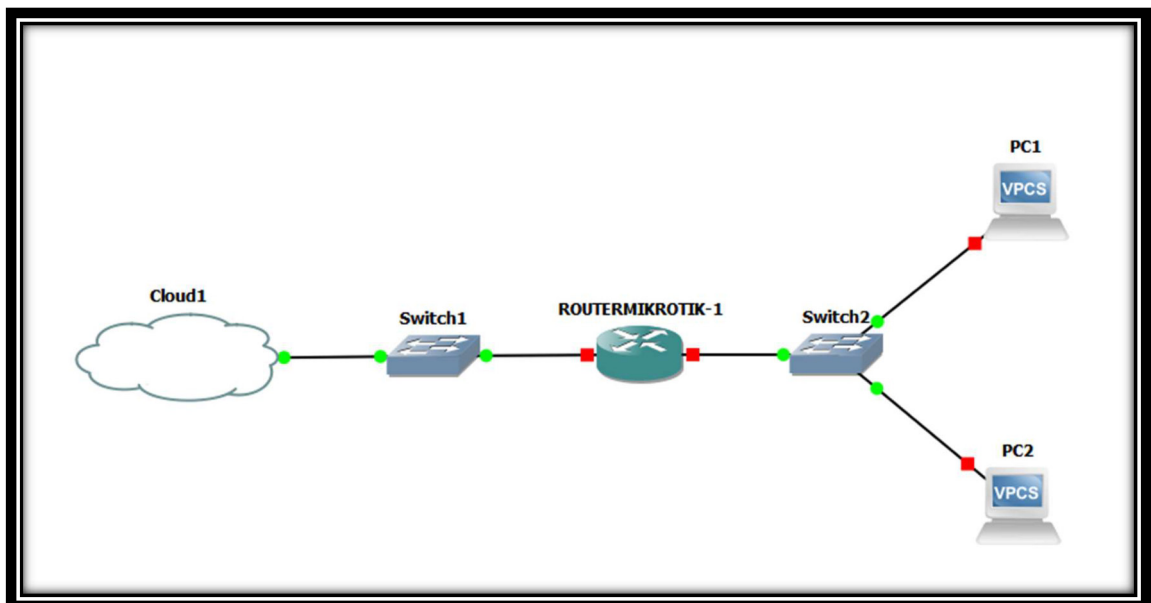


Figura 3.48 Diagrama de conexiones Introducción a GNS3

5. **DESCRIPCIÓN DE LAS ACTIVIDADES Y PROCEDIMIENTO DE LA PRÁCTICA:**

1. Crear interfaz de *loopback*.

2. Crear una máquina virtual en *Oracle VM VirtualBox* y cargar la imagen con el sistema operativo con el *router* Mikrotik e instalar el sistema operativo.
3. Iniciar un nuevo proyecto en GNS3 y vincular el *router Mikrotik* creado previamente en *VirtualBox*.
4. Conectar los dispositivos en base al diagrama de conexiones presentado.
5. Ingresar al *router* mediante la interfaz gráfica *Winbox*, para proceder con la configuración.
6. Asignar un nombre al *router*.
7. Asignar direcciones IP a la interfaz del *router* y a las máquinas virtuales *VPCS*.
8. Familiarizar al estudiante con las opciones básicas que permite implementar la interfaz de GNS3 y *Winbox*:
 - Insertar texto, formas en la pantalla principal de GNS3
 - Verificar tablas de enrutamiento en el *router*
 - Crear copias de seguridad para el *router*
 - Reestablecer el *router* a configuraciones de fábrica
 - Restaurar la configuración de la copia de seguridad
9. Comprobar la conexión de los equipos haciendo *ping* entre las *VPCS* y el *Gateway*.



ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

HOJA GUÍA PRÁCTICA 2

1. **TEMA:** Enrutamiento Estático
2. **OBJETIVO:**

Levantar la conexión de la topología propuesta usando enrutamiento estático.

3. **TRABAJO PREPARATORIO:**

Cuestionario:

- Investigar y realizar un breve resumen de enrutamiento estático y sus características
- Realizar el cálculo para subredes a partir la red principal 172.16.0.0/16 para los siguientes hosts:
 - LAN 1: 500 hosts
 - LAN 2: 60 hosts
 - LAN 3: 300 hosts
 - LAN 4: 150 hosts
 - LAN 5: 10 hosts
 - LAN 6: 30 hosts
 - 3 direcciones IP para enlaces

Requerimiento previo:

- Crear 4 *routers* con el sistema operativo *Mikrotik* en *Oracle VM VirtualBox* y vincularlo con GNS3

4. **DIAGRAMA DE CONEXIONES:**

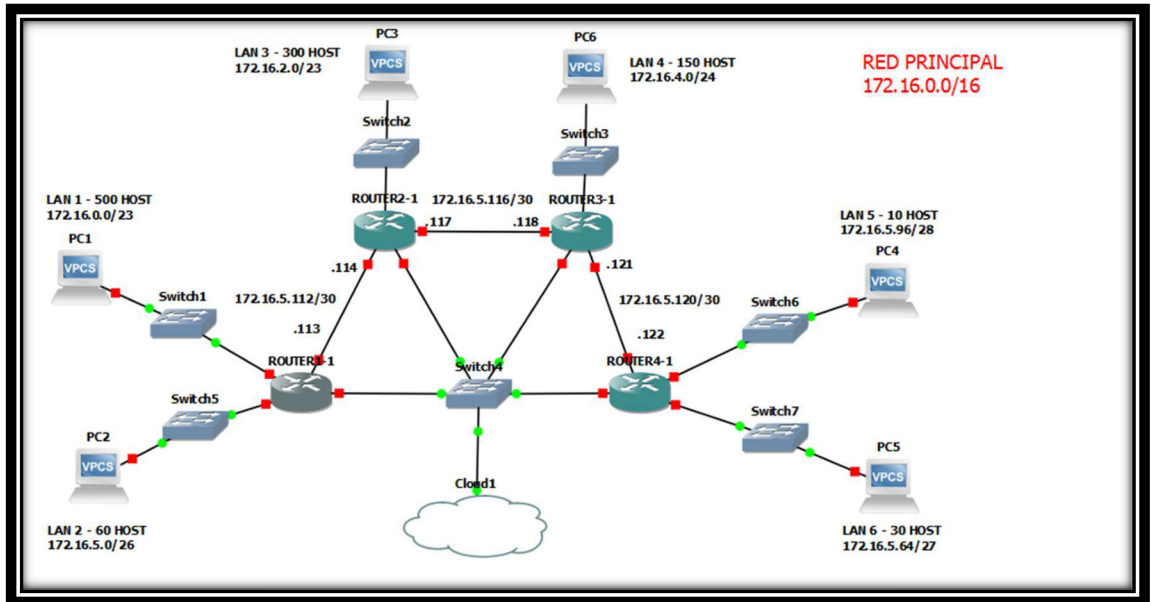


Figura 3.49 Diagrama de conexiones Enrutamiento Estático

5. DESCRIPCIÓN DE LAS ACTIVIDADES Y PROCEDIMIENTO DE LA PRÁCTICA:

1. Conectar los dispositivos en base al diagrama de conexiones presentado.
2. Asignar nombres a los *routers*.
3. Asignar direcciones IP a los *routers* respectivamente según se muestra en el diagrama de conexiones.
4. Crear nuevas rutas en los *routers* mediante la interfaz de *Winbox* en la opción “*routes*” para que se comuniquen todos los equipos del diagrama de conexiones.
5. Revisar tablas de enrutamiento de los *routers* para verificar que se encuentren bien aprendidas las rutas.
6. Asignar direcciones IP a las *VPCS*.
7. Comprobar la conectividad entre las *VPCS*.



ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

HOJA GUÍA PRÁCTICA 3

1. **TEMA:** Protocolo de Enrutamiento dinámico IGP (*Interior Gateway Protocol*)
Protocolo Vector Distancia RIP

2. **OBJETIVO:**

Configurar el protocolo de Enrutamiento RIP en el diagrama de conexiones propuesto.

3. **TRABAJO PREPARATORIO:**

Cuestionario:

- Investigar y realizar un breve resumen del protocolo RIP y sus características

Requerimiento previo:

- Crear 3 *routers* con el sistema operativo *Mikrotik* en *Oracle VM VirtualBox* y vincularlo con GNS3

4. **DIAGRAMA DE CONEXIONES:**

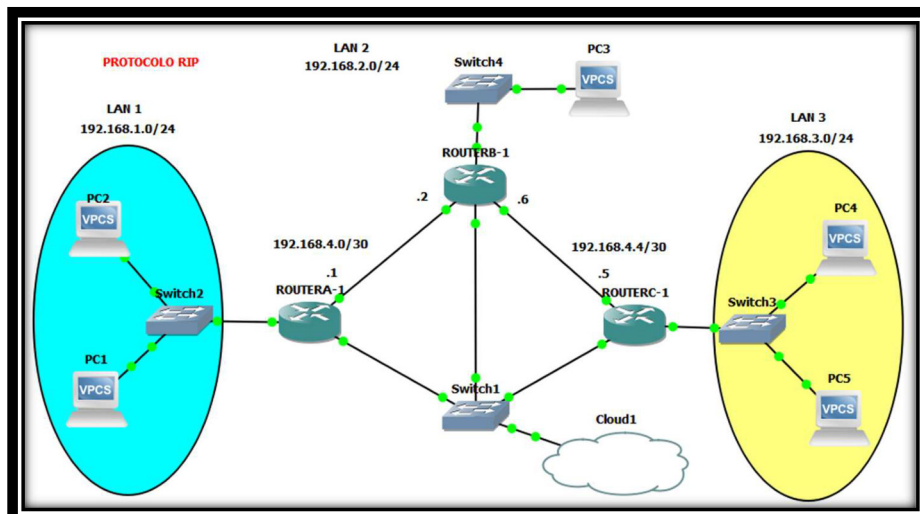


Figura 3.50 Diagrama de conexiones Protocolo de Enrutamiento dinámico IGP (*Interior Gateway Protocol*) Protocolo Vector Distancia RIP

5. **DESCRIPCIÓN DE LAS ACTIVIDADES Y PROCEDIMIENTO DE LA PRÁCTICA:**

1. Conectar los dispositivos en base al diagrama de conexiones presentado.
2. Asignar nombres a los *routers*.
3. Asignar direcciones IP a los *routers* respectivamente según se muestra en el diagrama de conexiones.
4. Ingresar a la interfaz del protocolo RIP en *Winbox* y configurar.

5. Crear una nueva interfaz RIP que trabaje en versión 1 y 2.
6. Crear una red para compartir los paquetes RIP dentro de la pestaña "*Networks*".
7. Habilitar la redistribución de rutas conectadas en la interfaz.



ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

HOJA GUÍA

PRÁCTICA 4

1. **TEMA:** Protocolo de Enrutamiento Dinámico EGP (*Exterior Gateway Protocol*)
Protocolo BGP

2. **OBJETIVO:**

Establecer conexión del protocolo BGP entre equipos *Mikrotik*.

3. **TRABAJO PREPARATORIO:**

Cuestionario:

- Consultar la definición y características del protocolo BGP

Requerimiento previo:

- Crear 4 *routers* con el sistema operativo *Mikrotik* en *Oracle VM VirtualBox* y vincularlo con GNS3

4. **DIAGRAMA DE CONEXIONES:**

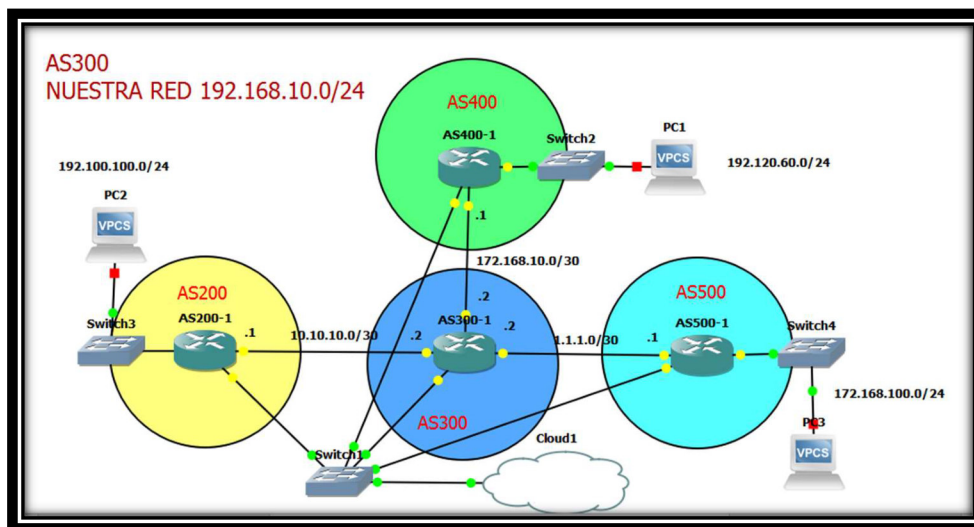


Figura 3.51 Diagrama de conexiones Protocolo de Enrutamiento Dinámico EGP (*Exterior Gateway Protocol*) Protocolo BGP

5. **DESCRIPCIÓN DE LAS ACTIVIDADES Y PROCEDIMIENTO DE LA PRÁCTICA:**

1. Conectar los dispositivos en base al diagrama de conexiones presentado.
2. Asignar nombres a los *routers*.
3. Asignar direcciones IP a los *routers* respectivamente según se muestra en el diagrama de conexiones.
4. Crear una interfaz lógica mediante la interfaz *bridge* de *Winbox*.
5. Asignar una dirección IP a cada interfaz lógica de los *routers*.

6. Levantar el protocolo BGP en cada *router*.
7. Verificar la tabla de enrutamiento de cada *router*.
8. Constatar que las configuraciones realizadas sean correctas haciendo *ping* desde las *VPCS* de una *LAN* a otra.



ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

HOJA GUÍA

PRÁCTICA 5

1. **TEMA:** Red Privada Virtual (VPN) con protocolo PPTP
2. **OBJETIVO:**

Familiarizarse con el funcionamiento del protocolo PPTP.

3. **TRABAJO PREPARATORIO:**

Cuestionario:

- Consultar y definir el protocolo PPTP y sus características
- Realizar un resumen acerca de las rutas por defecto, enumerar los pasos para su configuración en un *router Mikrotik* mediante *Winbox*
- Enumerar los puertos que usa el protocolo PPTP y los pasos que se debe seguir para determinarlos en un *router Mikrotik* mediante *Winbox*
- Investigar y realizar un resumen sobre NAT, enumerar los pasos que se debe seguir para configurarlos en un *router Mikrotik* mediante *Winbox*
- Listar los pasos que se deben seguir para crear un adaptador de red que trabaje con el protocolo PPTP en *Windows 7*

Requerimiento previo:

- Crear 2 *routers* con el sistema operativo *Mikrotik* en *Oracle VM VirtualBox* y vincularlo con GNS3

4. **DIAGRAMA DE CONEXIONES:**

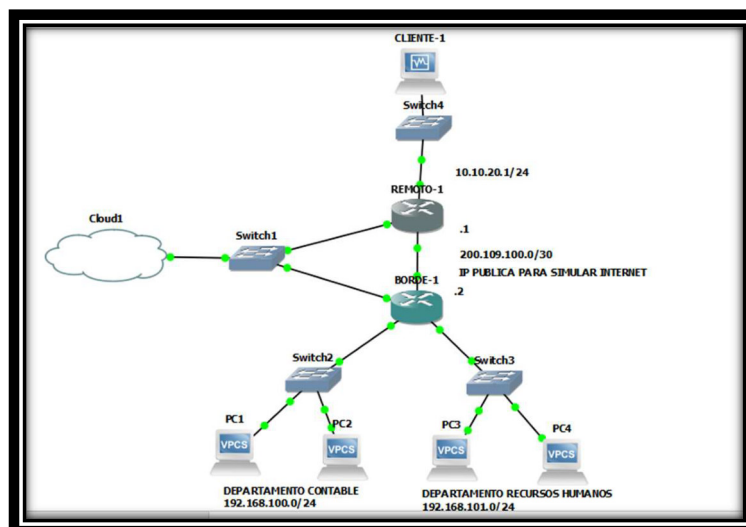


Figura 3.52 Diagrama de conexiones Red Privada Virtual (VPN) con protocolo PPTP

5. DESCRIPCIÓN DE LAS ACTIVIDADES Y PROCEDIMIENTO DE LA PRÁCTICA:

1. Crear una máquina virtual con el sistema operativo *Windows 7* en *Oracle VM VirtualBox* y vincularlo en *GNS3*.
2. Conectar los dispositivos en base al diagrama de conexiones presentado.
3. Asignar nombres a los *routers*.
4. Asignar direcciones IP a los *routers* respectivamente según se muestra en el diagrama de conexiones.
5. Configurar una ruta por defecto en los *routers*.
6. Verificar la tabla de enrutamiento de cada *router*.
7. Asignar un pool de direcciones IP al *router* BORDE
8. Habilitar el protocolo PPTP en el *router* BORDE:
 - Levantar le protocolo
 - Crear un perfil
 - Crear un usuario
9. Configurar las leyes de entrada y salida del Firewall en el *router*, además de habilitar NAT.
10. Asignar una dirección IP al cliente *Windows 7* y verificar que se tenga salida hasta el *Gateway* del *router* REMOTO, mediante un *ping* en CMD.
11. Levantar el protocolo PPTP en el cliente *Windows* y hacer *ping* a las *VPCS* de la topología para verificar las conexiones.
12. Ingresar a CMD y realizar un trazo desde la máquina cliente hacia las *VPCS* para verificar que ruta toma.
13. Desactivar momentáneamente el protocolo PPTP en cliente *Windows* y volver a realizar el trazo hacia las *VPCS*.
14. Comparar los resultados obtenidos.



ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

HOJA GUÍA

PRÁCTICA 6

1. **TEMA:** Implementación de red MPLS con OSPF

2. **OBJETIVO:**

Familiarizarse con la tecnología MPLS y aplicarla junto con OSPF para comprobar su funcionamiento.

3. **TRABAJO PREPARATORIO:**

Cuestionario:

- Realizar un resumen acerca de MPLS
- Enumerar los pasos que se debe seguir para realizar un traceo hacia una dirección IP mediante la interfaz gráfica *Winbox*

Requerimiento previo:

- Crear 4 *routers* con el sistema operativo *Mikrotik* en *Oracle VM VirtualBox* y vincularlo con GNS3

4. **DIAGRAMA DE CONEXIONES:**

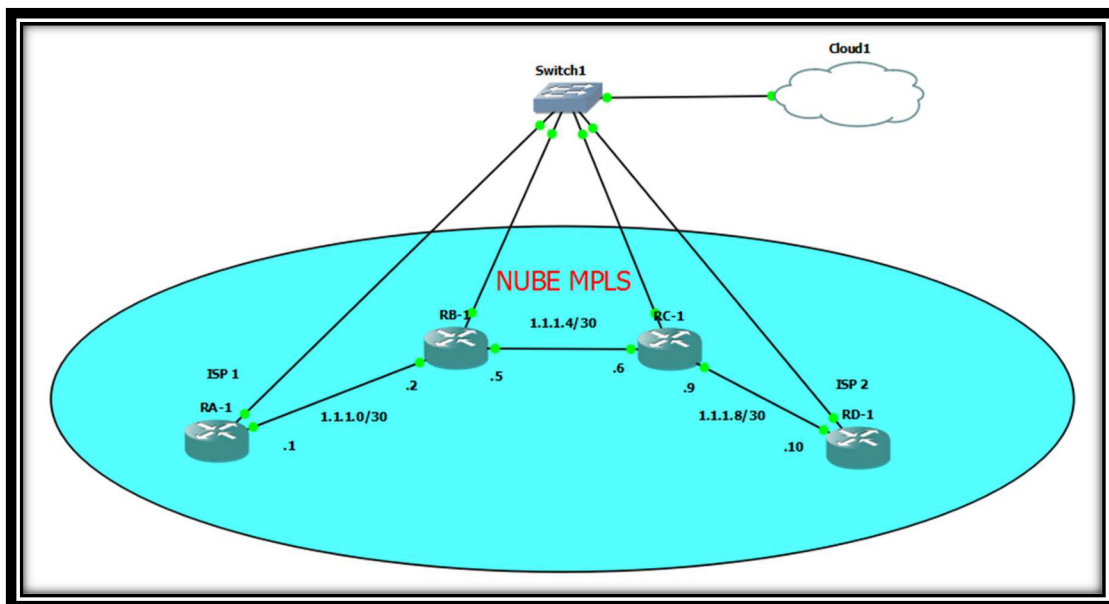


Figura 3.53 Diagrama de conexiones Implementación de red MPLS con OSPF

5. DESCRIPCIÓN DE LAS ACTIVIDADES Y PROCEDIMIENTO DE LA PRÁCTICA:

1. Conectar los dispositivos en base al diagrama de conexiones presentado.
2. Asignar nombres a los *routers*.
3. Asignar direcciones IP a los *routers* respectivamente según se muestra en el diagrama de conexiones.
4. Crear una interfaz lógica mediante la interfaz *bridge* de *Winbox*.
5. Asignar una dirección IP a cada interfaz lógica de los *routers*.
6. Levantar el protocolo OSPF en cada *router*.
7. Verificar la tabla de enrutamiento de cada *router*.
8. Realizar un *trace* a la interfaz *bridge* desde RA a RD y tomar en cuenta la pestaña "*Status*".
9. Levantar la tecnología MPLS en cada *router*.
10. Realizar un *trace* a la interfaz *bridge* desde RA a RD y tomar en cuenta la pestaña "*Status*". Comparar ambos *traces*.



ESCUELA POLITÉCNICA NACIONAL ESCUELA DE FORMACIÓN DE TECNÓLOGOS

HOJA GUÍA PRÁCTICA 1

1. **TEMA:** Introducción a GNS3
2. **OBJETIVO:**

Familiarizarse con los programas: GNS3, *Oracle VirtualBox Machine* y *Winbox*. Además de las funciones básicas.

3. **DIAGRAMA DE CONEXIONES:**

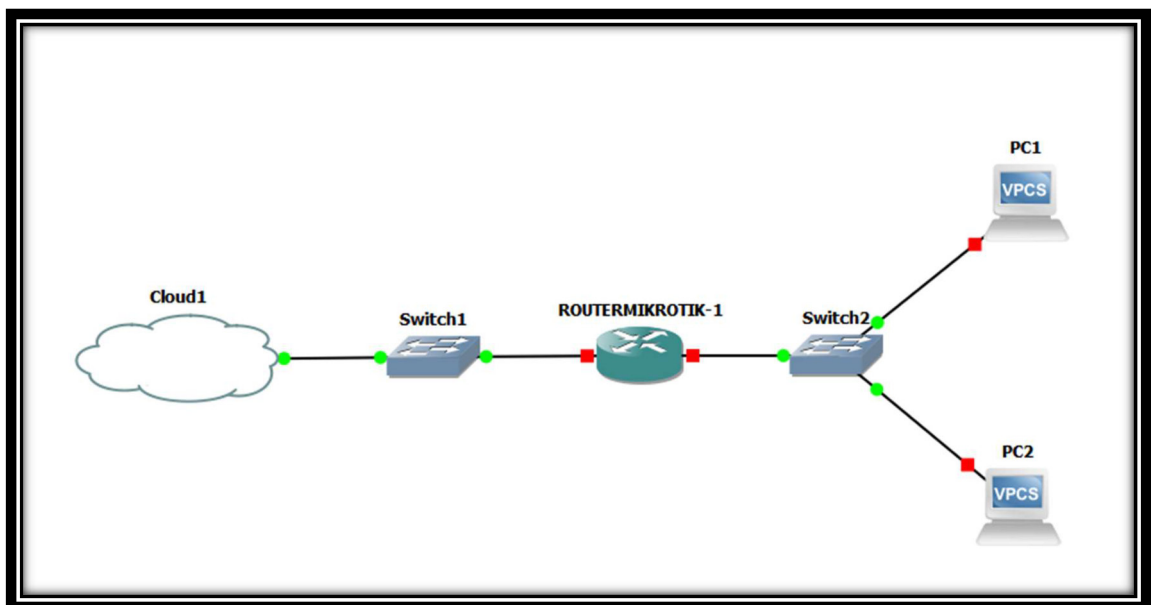


Figura 3.54 Diagrama de conexiones práctica 1

4. **DESARROLLO DE LA PRÁCTICA:**

NOTA: Tiempo estimado para realizar la presente práctica de laboratorio es de una hora.

Paso 1: realizar procedimiento detallado en el numeral 3.2 funcionalidades y herramientas que comprende GNS3

Crear la interfaz de *loopback* en el ordenador principal como se muestra en la Figura 3.55.

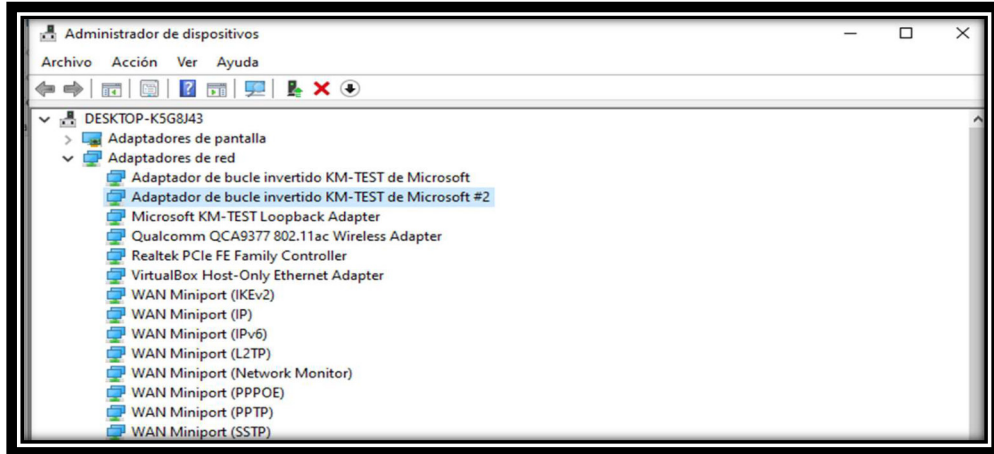


Figura 3.55 Ventana del Adaptador de bucle invertido creado

Reiniciar el equipo para habilitar las configuraciones del adaptador.

VIRTUALBOX

Crear un *router Mikrotik* en *VirtualBox*, como se muestra en la Figura 3.56.

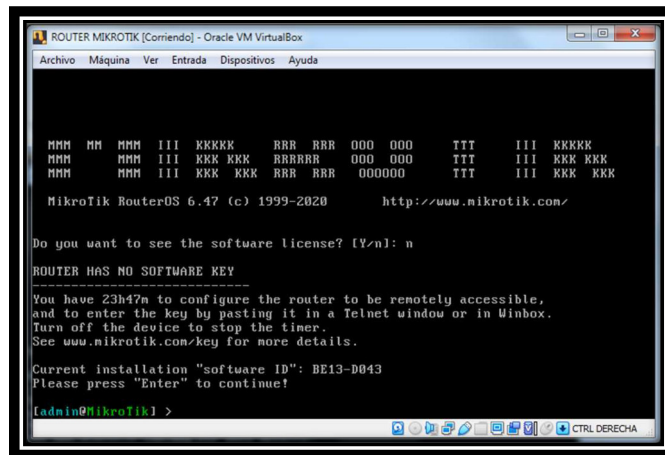


Figura 3.56 Pantalla principal del *router* línea de comandos

GNS3

Crear un nuevo proyecto "INTRODUCCIÓN", ver Figura 3.57 y Figura 3.58.

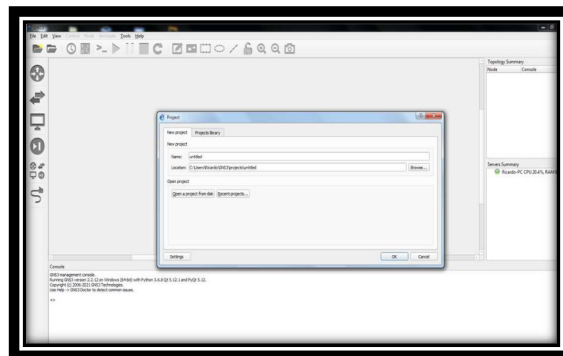


Figura 3.57 Creación un nuevo proyecto en GNS3

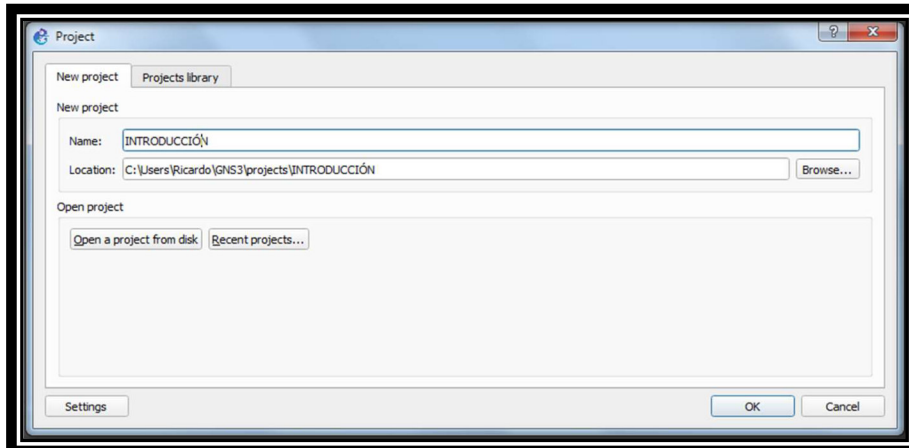


Figura 3.58 Asignar un nombre al proyecto

Vincular el “*ROUTER MIKROTIK*” con GNS3, como se puede observar en la Figura 3.59.

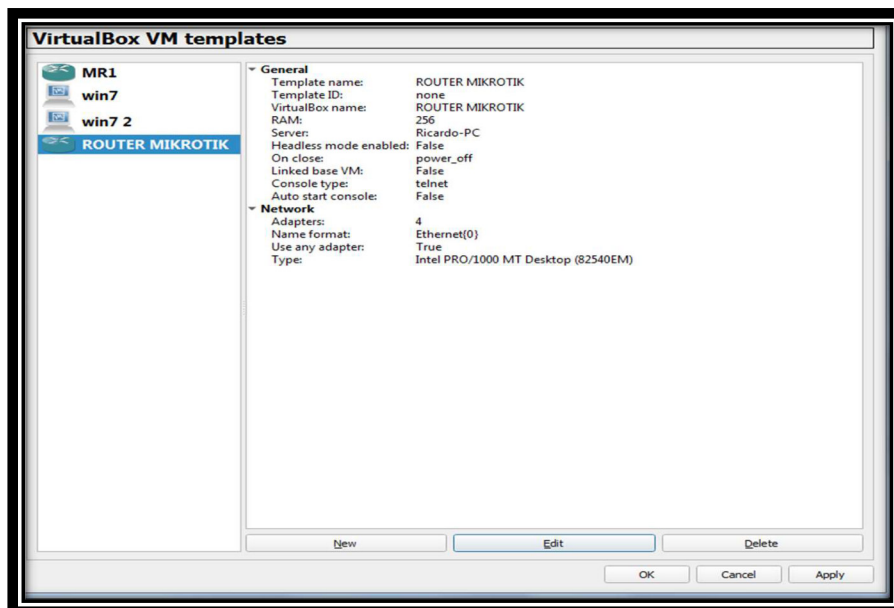


Figura 3.59 Aceptar los cambios realizados para el *router*

Paso 2: comprobación del *router* creado

En la opción “*Routers*” como se muestra en la Figura 3.60, seleccionar el “*ROUTER MIKROTIK*” y arrastrar hasta la pantalla principal de edición.

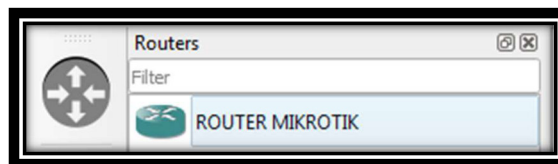


Figura 3.60 Ícono del *Mikrotik* creado y vinculado

De igual manera, de la opción “*Switches*” seleccionar “*Ethernet Switch*”, como se observa en la Figura 3.61 y colocar en la pantalla de edición.

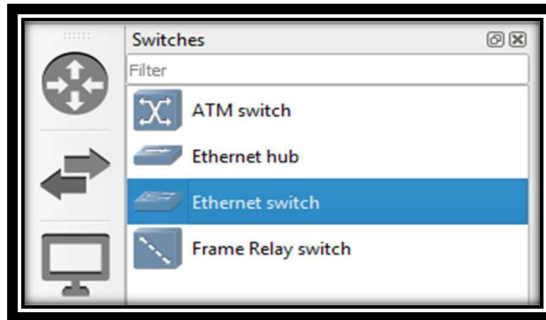


Figura 3.61 Ícono de *Ethernet Switch*

En la opción “*End Devices*” seleccionar “*Cloud*”, como se muestra en la Figura 3.62 y colocar en la pantalla de edición.

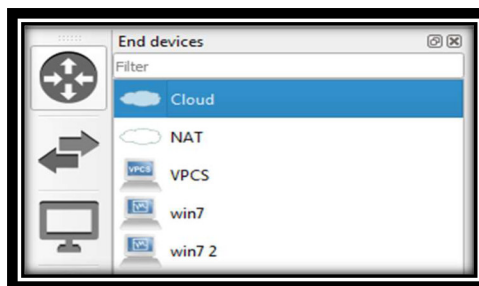


Figura 3.62 Ícono de *Cloud*

Realizar el cableado respectivo de los equipos colocados en la pantalla principal de edición, para esto seleccionar “*Add a link*”, ver Figura 3.63.

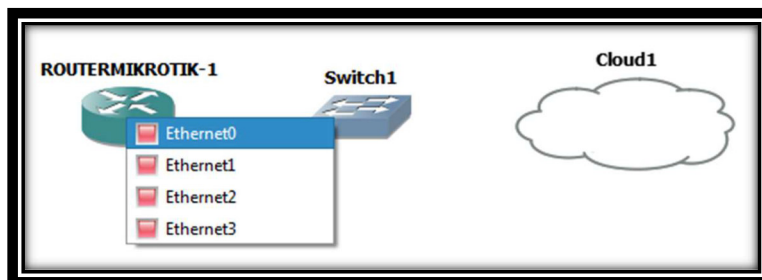


Figura 3.63 Elección del puerto en el *router* para cablearlo con el *switch*

Se debe tomar en cuenta el puerto conectado al *Switch*, ver Figura 3.64.

Puertos equivalentes entre GNS3 y Oracle VM VirtualBox:

- *Ethernet0* equivalente al Adaptador 1
- *Ethernet1* equivalente al Adaptador 2
- *Ethernet2* equivalente al Adaptador 3
- *Ethernet3* equivalente al Adaptador 4

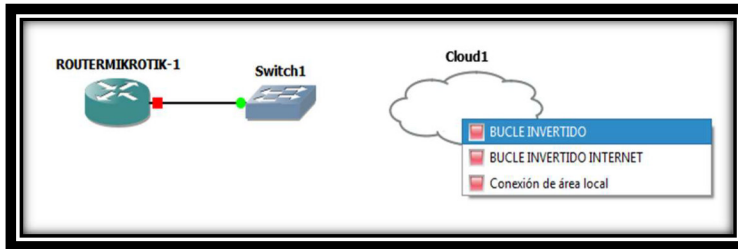


Figura 3.64 Elección del puerto “Bucle invertido” para cablear el switch con cloud

El punto de conexión en *Cloud* va a ser la interfaz de *loopback*, como se muestra en la Figura 3.65.

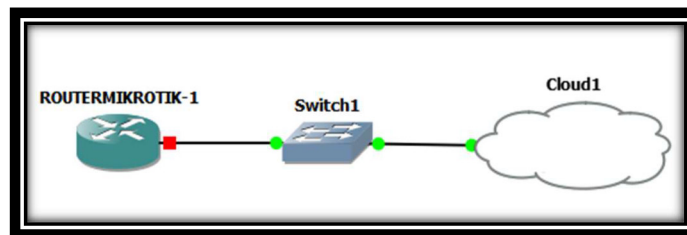


Figura 3.65 Cableado de los equipos

Colocar otro *Ethernet Switch* para conectar a las *VPCS*, ver Figura 3.66.

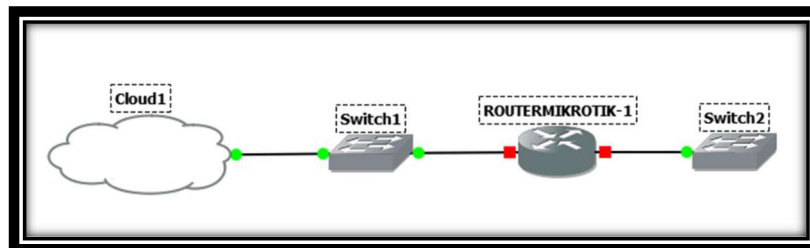


Figura 3.66 Segundo switch agregado

En la pestaña “*End Devices*” seleccionar una *VPCS* (*Virtual PC Simulator*). Las *VPCS* son máquinas virtuales con un sistema operativo con las funciones básicas para la simulación de conectividad, ver Figura 3.67.

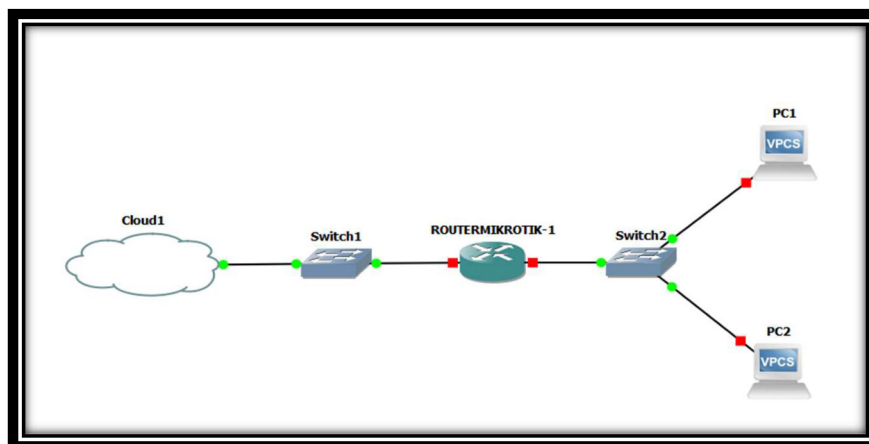



Figura 3.67 Máquinas virtuales cableadas al switch

Escoger la opción  y seleccionar el lugar donde se desea escribir el texto. (Direcciones IP de las VPCS, la dirección de *Gateway* e información general de la red general), ver Figura 3.68.

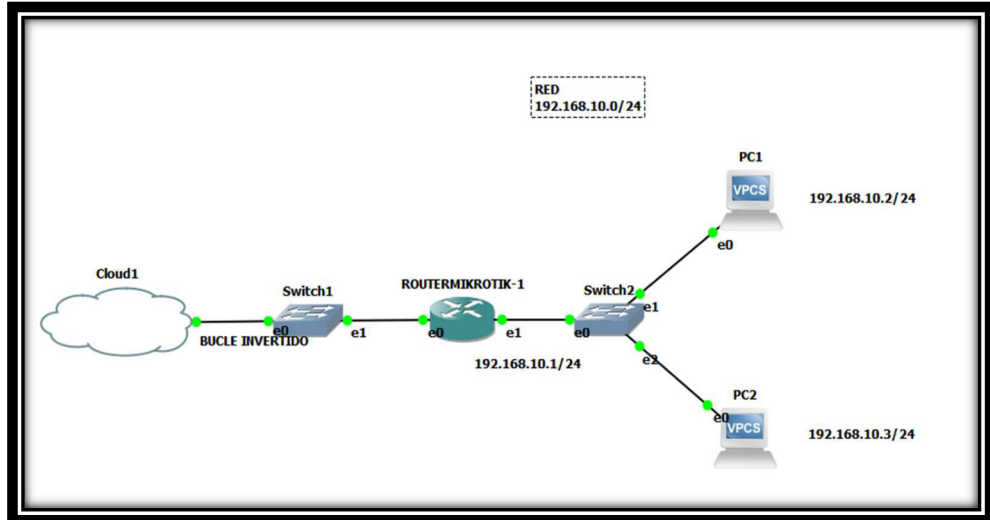




Figura 3.68 Agregar etiquetas a la topología

Si se desea resaltar alguna sección con una forma se lo realiza con la opción  ó  haciendo *click* sobre el símbolo y seleccionando la sección donde se desea colocar, ver Figura 3.69.

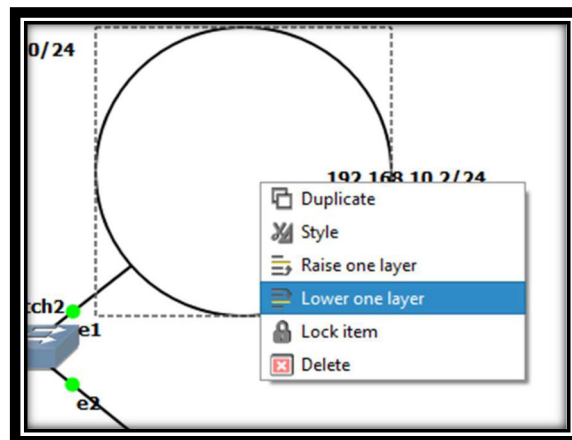


Figura 3.69 Insertar una figura a la topología, cambio de profundidad

Para cambiar la profundidad de la capa, hacer *click* derecho y seleccionar, como se observa en la Figura 3.70:

- *Raise one layer* (subir una capa)
- *Lower one layer* (bajar una capa)

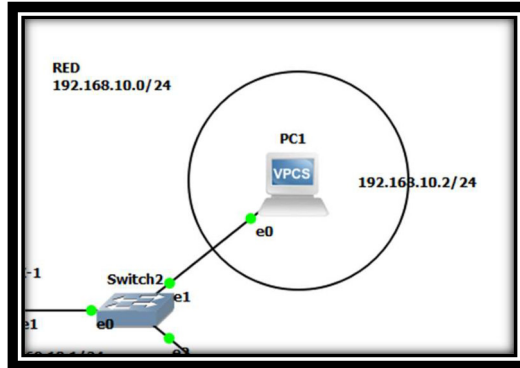


Figura 3.70 Figura insertada para identificar un segmento de la topología

Para cambiar el estilo, dar *clíc* derecho en la figura y seleccionar la opción “*Style*”, como se muestran en las Figura 3.71. Se puede cambiar: relleno, borde y ancho.

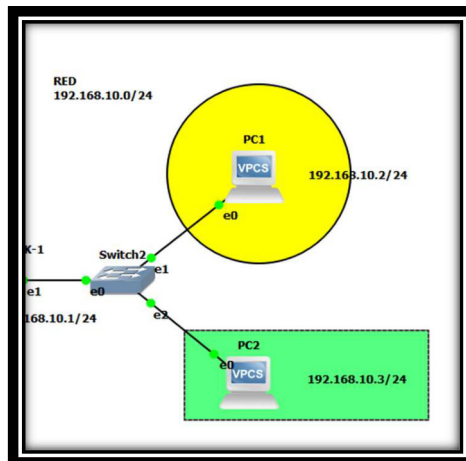



Figura 3.71 Segunda figura insertada con los cambios respectivos

Correr el programa haciendo *clíc* en “Iniciar” , ver figura 3.72.

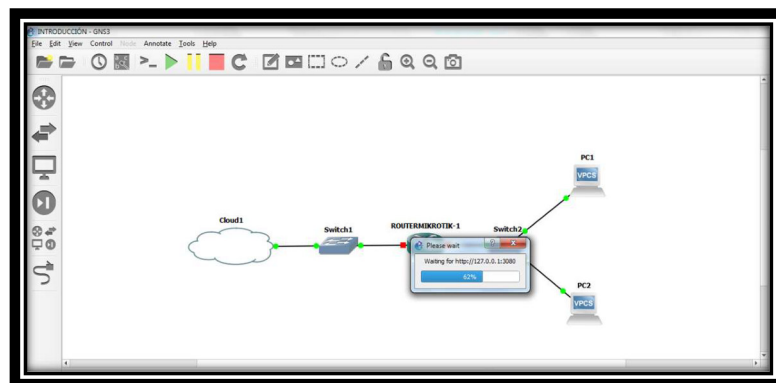


Figura 3.72 Inicialización del proyecto de GNS3

El “*ROUTER MIKROTIK*” se inicia de manera automática en *VirtualBox*, aquí se comprueba que la vinculación: GNS3 a *VirtualBox* fue realizada de manera correcta. Para vincular la interfaz de *loopback* con GNS3 e ingresar a la pantalla de *Winbox* sin que se presenten errores, se selecciona pausa, ver Figura 3.73.

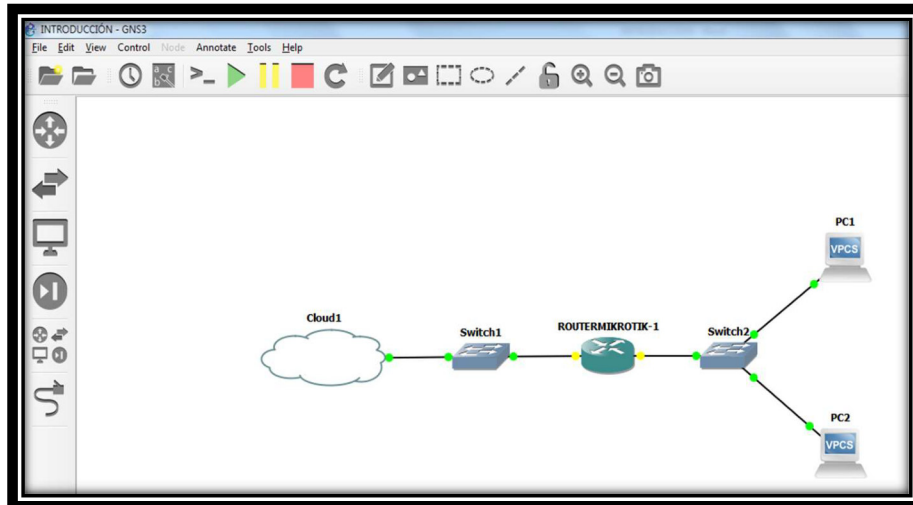


Figura 3.73 Proyecto de GNS3 detenido

Ir a *VirtualBox* a la configuración del “*ROUTER MIKROTIK*”, y en la pestaña “Red” cambiar la configuración del adaptador de red, de acuerdo al puerto que se conectó con el *switch* en GNS3, ver Figura 3.74.

- Conectado a: Adaptador puente.
- Nombre: Adaptador de bucle invertido de Microsoft (Nombre de la interfaz *loopback* creada).

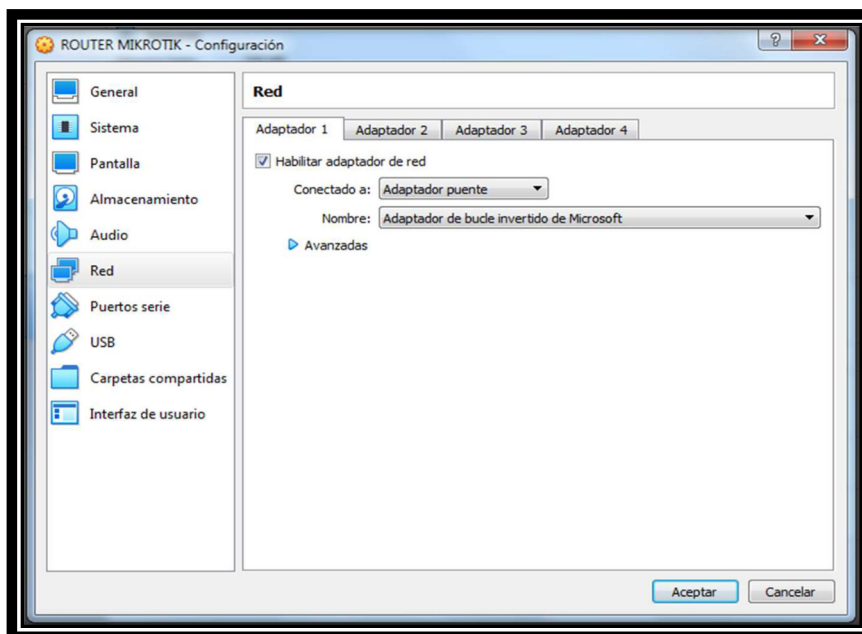



Figura 3.74 Cambio de la configuración del adaptador de red del *router* en *VirtualBox*

En GNS3 para ver las interfaces conectadas hay que seleccionar: *Show/Hide interface labels* . Para confirmar la interfaz que se debe elegir en *VirtualBox*, como se muestra en la Figura 3.75.

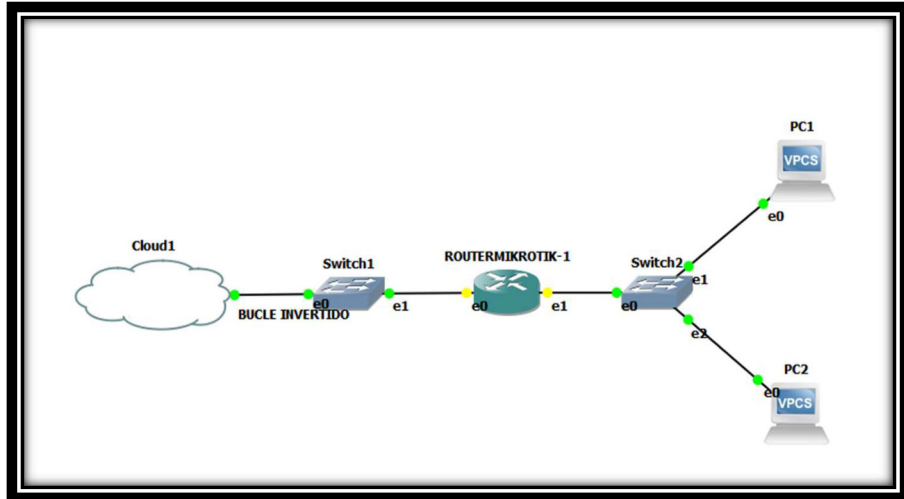


Figura 3.75 Interfaces conectadas en GNS3

Seleccionar “Iniciar” para que se pueda levantar de nuevo de manera correcta los equipos y actualice los cambios realizados.

Paso 3: conexión con Winbox

Abrir Winbox, como se muestra en la Figura 3.76.

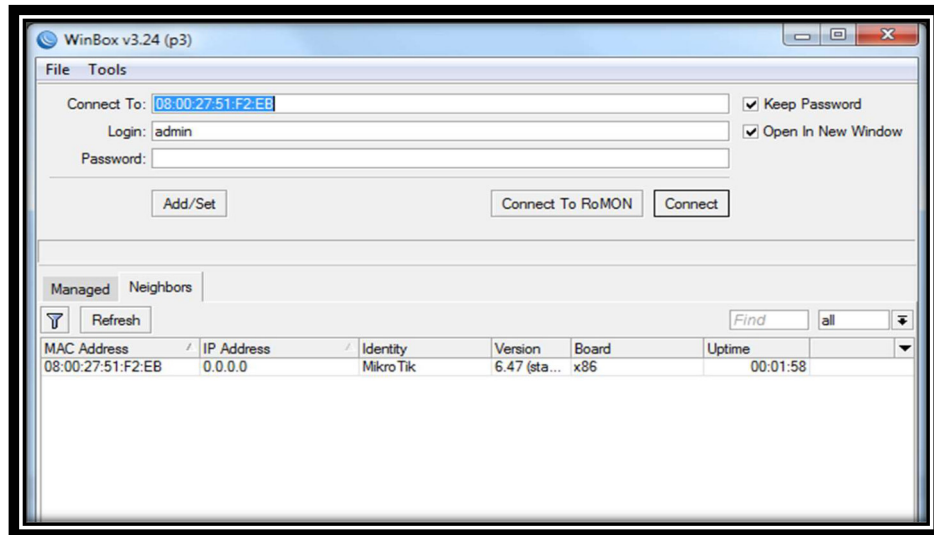


Figura 3.76 Pantalla principal de Winbox

Se muestra el *router* con la dirección MAC respectiva. Seleccionar “Connect”, ver Figura 3.77.

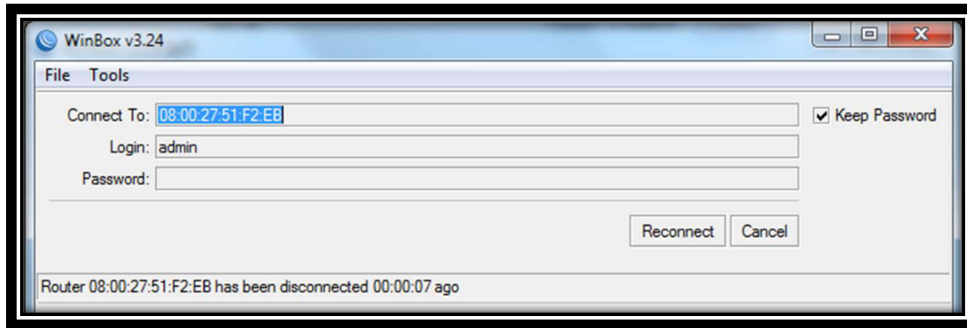


Figura 3.77 Conexión con el *router* mediante *Winbox*

Seleccionar “*Reconnect*” para que empiece a funcionar *Winbox*, ver Figura 3.78 y Figura 3.79.

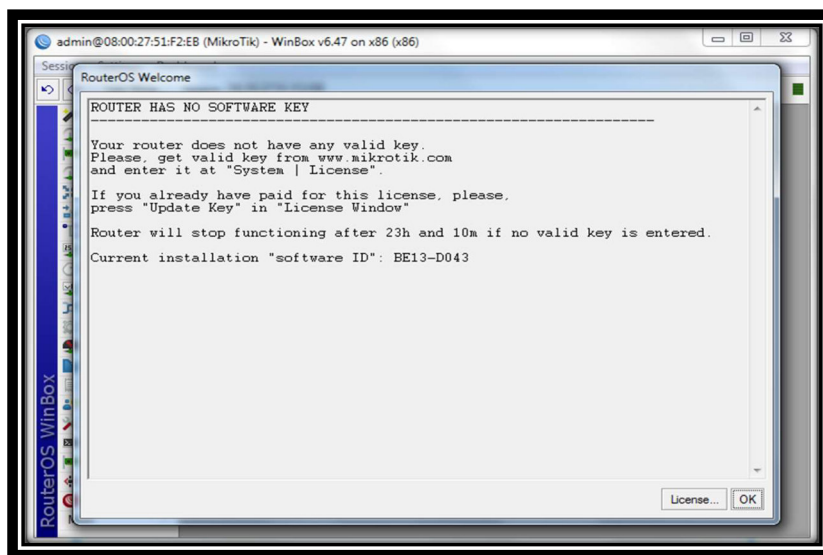


Figura 3.78 Licencia del *router Mikrotik*

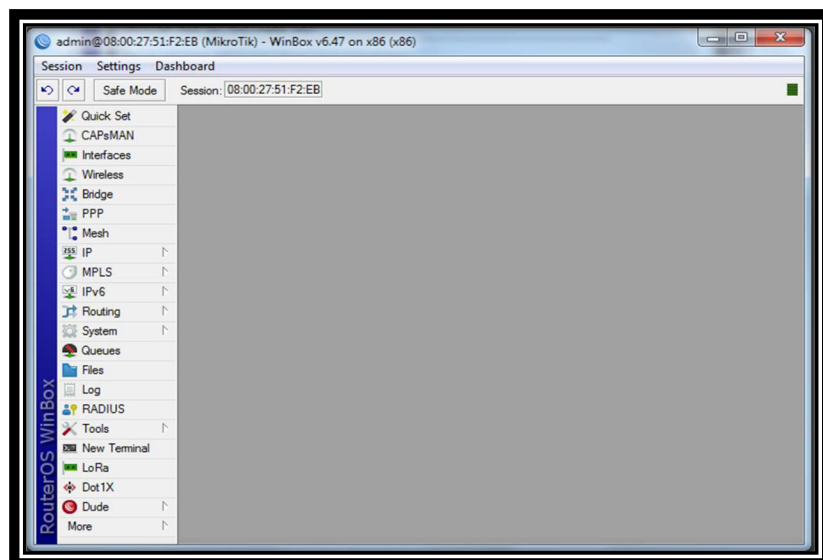


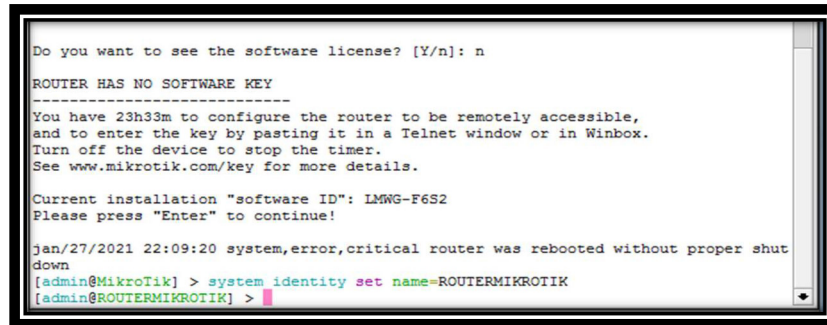
Figura 3.79 Pantalla principal de las configuraciones del *router* en *Winbox*

Paso 4: configuración del “ROUTER MIKROTIK”

El *router* puede ser configurado de dos maneras:

- Línea de comandos

Asignar nombre al *router*, se lo realiza en la pestaña “New Terminal”. En la siguiente línea se escribe el comando: `system identity set name= “ROUTERMIKROTIK”`, ver Figura 3.80.



```
Do you want to see the software license? [Y/n]: n
ROUTER HAS NO SOFTWARE KEY
-----
You have 23h33m to configure the router to be remotely accessible,
and to enter the key by pasting it in a Telnet window or in Winbox.
Turn off the device to stop the timer.
See www.mikrotik.com/key for more details.

Current installation "software ID": LMWG-F6S2
Please press "Enter" to continue!

jan/27/2021 22:09:20 system,error,critical router was rebooted without proper shut
down
[admin@MikroTik] > system identity set name=ROUTERMIKROTIK
[admin@ROUTERMIKROTIK] >
```

Figura 3.80 Agregar un nombre mediante línea de comandos

- Interfaz gráfica Winbox

Asignar nombre al *router* se lo realiza en la pestaña “System” seleccionar “Identity”, como se muestra en la Figura 3.81.

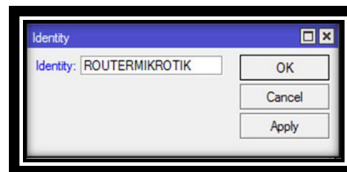


Figura 3.81 Asignación de un nombre

Asignar las direcciones IP respectivas al *router*. En la pestaña “IP” seleccionar la opción “Addresses”, ver Figura 3.82.

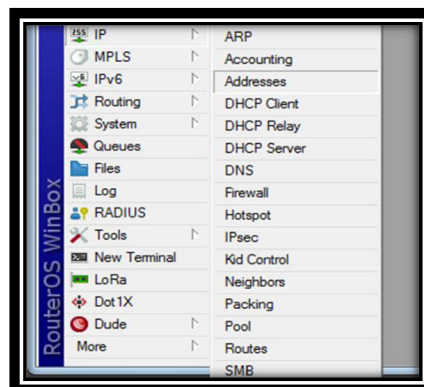


Figura 3.82 Asignar una dirección IP mediante la interfaz gráfica

Agregar la dirección IP del *Gateway* para el *router*, como se muestra en la Figura 3.83, la dirección a usar es: 192.168.10.1/24.

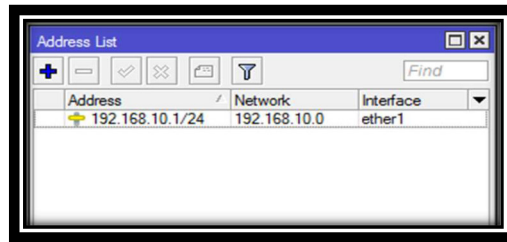


Figura 3.83 Dirección IP agregada

Asignar las direcciones IP a las *VPCS* haciendo doble *clic* en la *VPCS* y en la interfaz de *Solar Putty* escribir: ip “dirección IP/máscara” “*Gateway*”, como se muestra en la Figura 3.84 y Figura 3.85.



Figura 3.84 Agregar una dirección IP a la PC1

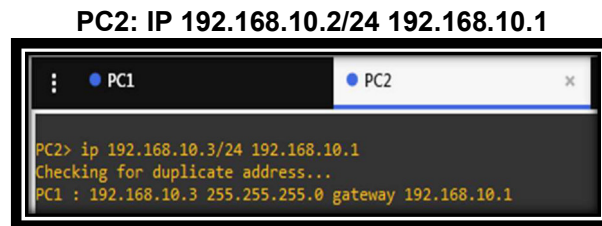


Figura 3.85 Agregar una dirección IP a la PC2

Realizar *ping* a las *VPCS* en la interfaz de *Solar Putty*, se debe escribir: *ping* “dirección IP a la que se quiere hacer *ping*”, como se observa en las Figura 3.86 a la Figura 3.89.

PC1 a GATEWAY (ping 192.168.10.2 a 192.168.10.1)

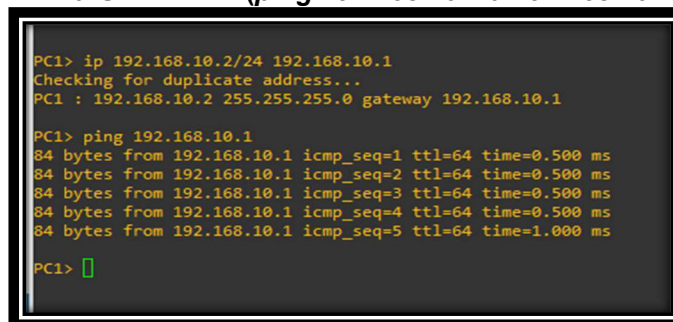


Figura 3.86 Ping desde PC1 al Gateway

PC1 a PC2 (ping 192.168.10.2 a 192.168.10.2)

```
PC1> ping 192.168.10.3
84 bytes from 192.168.10.3 icmp_seq=1 ttl=64 time=0.500 ms
84 bytes from 192.168.10.3 icmp_seq=2 ttl=64 time=0.500 ms
84 bytes from 192.168.10.3 icmp_seq=3 ttl=64 time=0.500 ms
84 bytes from 192.168.10.3 icmp_seq=4 ttl=64 time=0.500 ms
84 bytes from 192.168.10.3 icmp_seq=5 ttl=64 time=0.500 ms
```

Figura 3.87 Ping desde PC1 a PC2

PC2 a GATEWAY (ping 192.168.10.3 a 192.168.10.1)

```
PC2> ip 192.168.10.3/24 192.168.10.1
Checking for duplicate address...
PC1 : 192.168.10.3 255.255.255.0 gateway 192.168.10.1

PC2> ping 192.168.10.1
84 bytes from 192.168.10.1 icmp_seq=1 ttl=64 time=0.500 ms
84 bytes from 192.168.10.1 icmp_seq=2 ttl=64 time=0.500 ms
84 bytes from 192.168.10.1 icmp_seq=3 ttl=64 time=0.500 ms
84 bytes from 192.168.10.1 icmp_seq=4 ttl=64 time=0.500 ms
84 bytes from 192.168.10.1 icmp_seq=5 ttl=64 time=1.001 ms

PC2> █
```

Figura 3.88 Ping desde PC2 al Gateway

PC2 a PC1 (ping 192.168.10.3 a 192.168.10.2)

```
PC2> ping 192.168.10.2
84 bytes from 192.168.10.2 icmp_seq=1 ttl=64 time=0.500 ms
84 bytes from 192.168.10.2 icmp_seq=2 ttl=64 time=0.500 ms
84 bytes from 192.168.10.2 icmp_seq=3 ttl=64 time=0.500 ms
84 bytes from 192.168.10.2 icmp_seq=4 ttl=64 time=0.500 ms
84 bytes from 192.168.10.2 icmp_seq=5 ttl=64 time=0.500 ms

PC2> █
```

Figura 3.89 Ping desde PC1 a PC2

Verificar las tablas de enrutamiento y otras funciones de *Winbox*.

Ingresar a la interfaz *Winbox* y verificar las tablas de enrutamiento. En la pestaña "IP" opción "*Routes*", ver Figura 3.90.

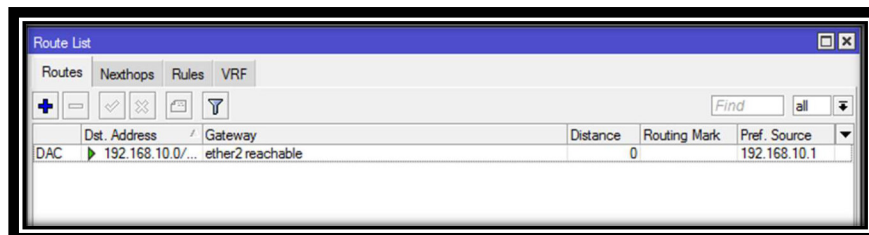


Figura 3.90 Rutas aprendidas por el router

Realizar una copia de seguridad. Ir a la pestaña "*Files*", como se observa en la Figura 3.91 y Figura 3.92.

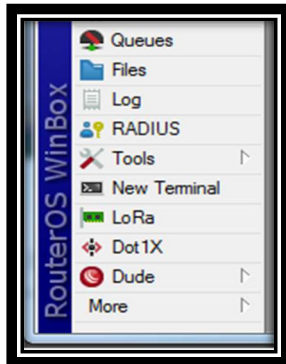


Figura 3.91 Ingreso a la pestaña "Files"

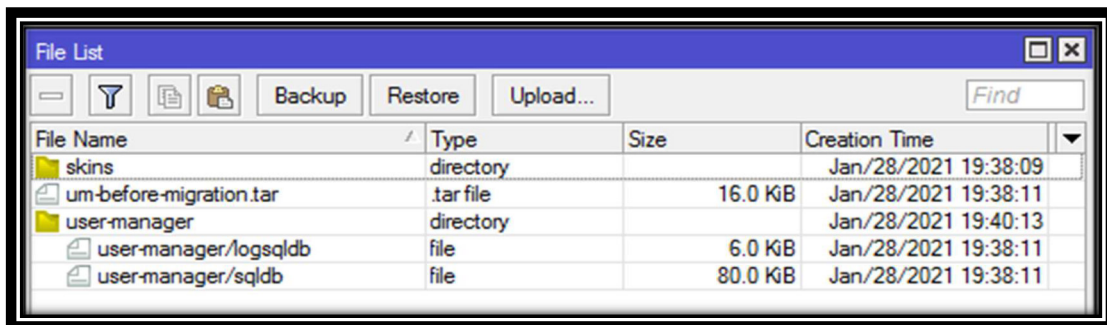


Figura 3.92 Pantalla principal de los archivos del router

Seleccionar la opción "Backup", ver figura 3.93.

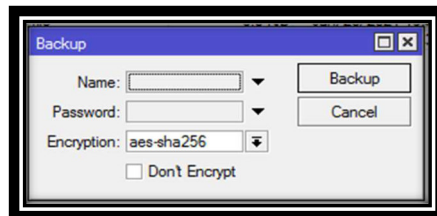


Figura 3.93 Creación de un archivo de respaldo

Se asigna nombre y contraseña para el *backup*, ver Figura 3.94. Contraseña: 123123 (puede ser cualquiera elegida por el usuario).



Figura 3.94 Asignar un nombre y clave

Se genera un archivo (*backup*) una vez concluido el proceso. Para restablecer la configuración del router ir a la pestaña "System" opción "Reset Configuration", ver Figura 3.95.

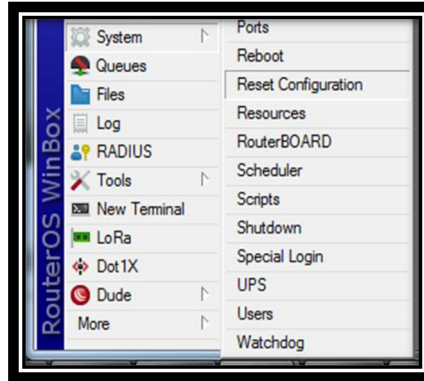


Figura 3.95 Reiniciar las configuraciones del *router*

En la ventana que aparece se tiene las siguientes opciones, ver Figura 3.96:

- *Keep user configuration*: Mantener las configuraciones de usuario (nombres y contraseñas de usuario).
- *No default Configuration*: Configuraciones por defecto (el *router* quedará en blanco).
- *Do not backup*: no generar un *backup* automáticamente.

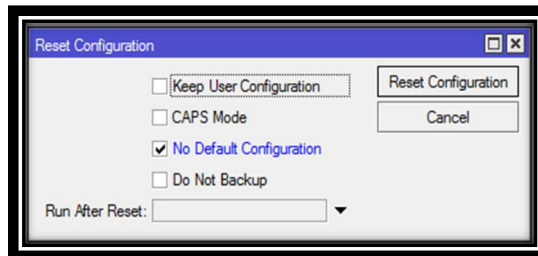


Figura 3.96 Selección de opciones para le reinicio del *router*

Se verifica que se ha reestablecido toda la información (Direcciones IP, nombre del *router* y la tabla de enrutamiento), es decir, todo aparecerá en blanco.

Restaurar las configuraciones de *backup*. Ir a la opción "*Files*", ver Figura 3.97.

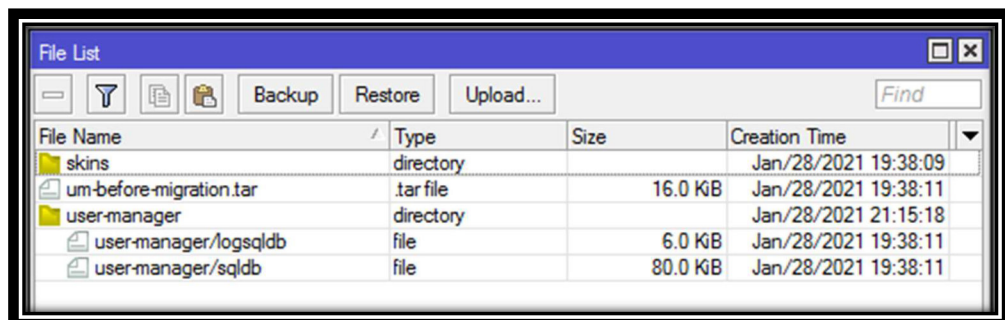


Figura 3.97 Restauración de las configuraciones

Arrastrar el archivo que se creó (*Backup.backup*) y dar clic sobre "*Restore*" e ingresar la contraseña, como se muestra en la Figura 3.98.

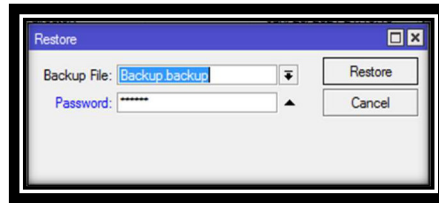


Figura 3.98 Acceso al archivo con la clave

Confirmar las configuraciones previamente establecidas, como se observa en las Figura 3.99 y Figura 3.100.

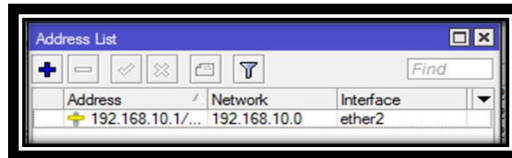


Figura 3.99 Direcciones IP reestablecidas



Figura 3.100 Rutas del *router* reestablecidas

Para establecer una contraseña en el *router* ir a la pestaña “System” en la opción: “Password”.

Escribir una nueva contraseña. Por defecto la contraseña anterior estará en blanco, como se muestra en la Figura 3.101. Se debe tomar en cuenta que esta clave será solicitada al momento de vincular el *router* mediante *Winbox*, ver Figura 3.102.

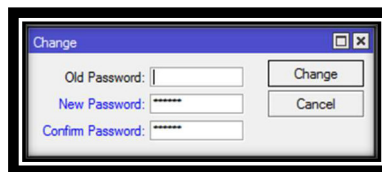


Figura 3.101 Confirmación para el cambio de clave

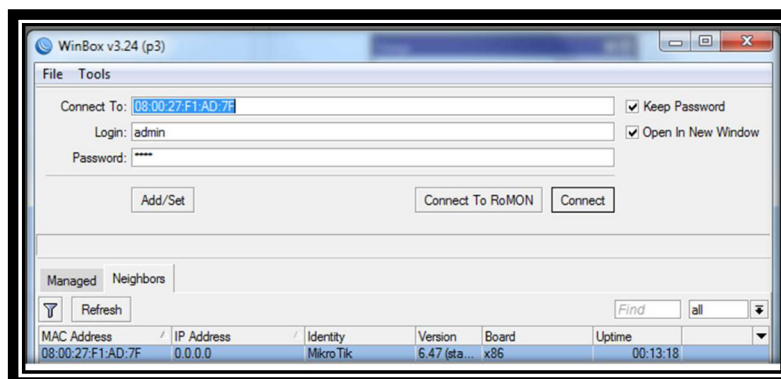




Figura 3.102 Ingreso mediante *Winbox* con la clave asignada

5. RECOMENDACIONES:

- Al escribir las líneas de comandos mediante en *Winbox*, se debe hacerlo en letras minúsculas, de no ser así el programa lo detectará como un comando inválido.
- Para cualquier cambio a realizarse en la configuración de los adaptadores de red de los *routers* simulados, ya sea en GNS o *VirtualBox*, primero se debe pausar el programa presionando el ícono  (pausa), sino GNS3 no permitirá efectuar dichos cambios mientras está corriendo o se presentará un error en el programa que no permitirá acceder a la configuración de los equipos mediante *Winbox*. Una vez efectuadas las modificaciones correspondientes se puede presionar  (iniciar) para continuar con la práctica.
- Una recomendación para con GNS3, es que al momento iniciarlo para crear un nuevo proyecto, hay que esperar a que el programa se vincule con el *host* (nuestro ordenador) y aparezca la ventana para ingresar un nombre al nuevo proyecto. Si no se cumple este proceso de inicialización el programa no funcionará de manera correctamente.



ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

HOJA GUÍA

PRÁCTICA 2

1. **TEMA:** Enrutamiento Estático

2. **OBJETIVO:**

Levantar la conexión de la topología propuesta usando enrutamiento estático.

3. **DIAGRAMA DE CONEXIONES:**

Armaz la siguiente topología:

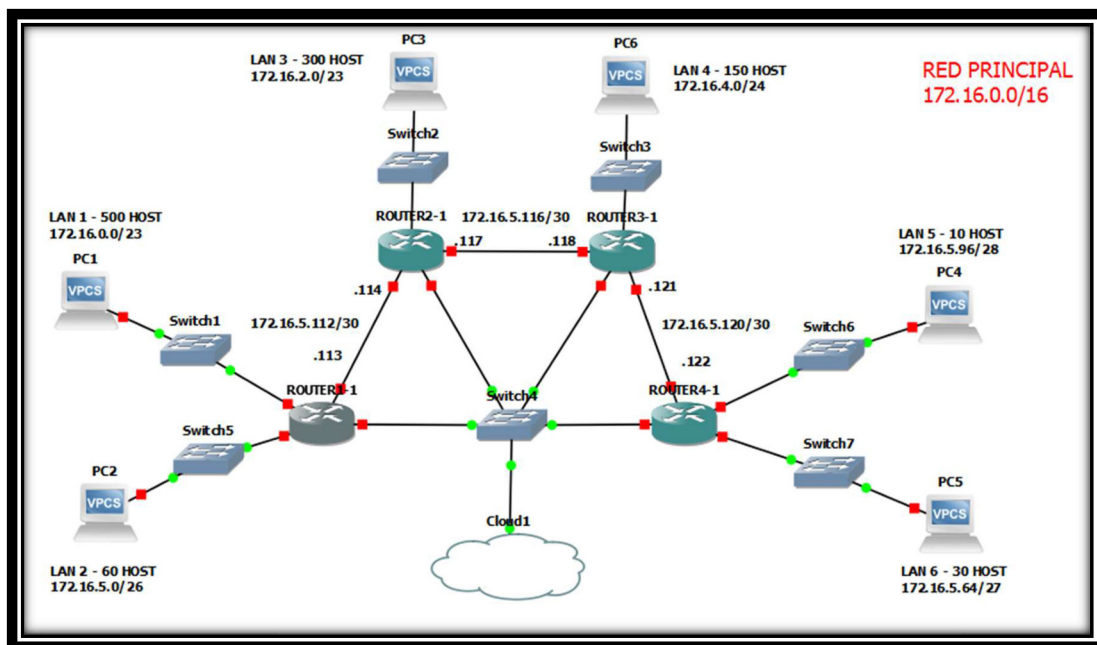


Figura 3.103 Diagrama de conexiones práctica 2

4. **DESARROLLO DE LA PRÁCTICA:**

NOTA: tiempo estimado para realizar la presente práctica de laboratorio es de una hora. Se recomienda que el estudiante tenga creadas 4 máquinas virtuales en *VirtualBox* y vinculadas con *GNS3* para realizar la práctica. Adicional se debe tener creado una interfaz de *loopback* en el computador.

Una vez realizado el diagrama de red correspondiente y todas las configuraciones previas. Se procede con la configuración de direcciones IP que debe conocer cada uno de los *routers*, tomando en cuenta el puerto de conexión y cada dirección de red a conocer, como se puede observar desde la Figura 3.104 a la Figura 3.107.

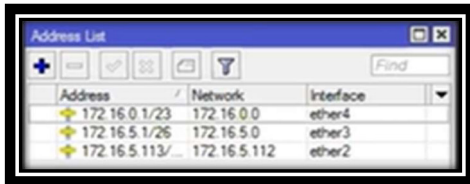


Figura 3.1044 Direcciones IP correspondientes al *ROUTER1*

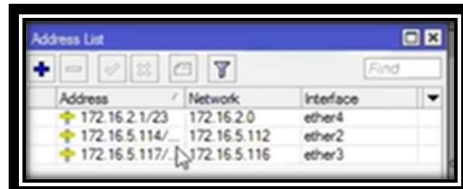


Figura 3.105 Direcciones IP correspondientes al *ROUTER2*

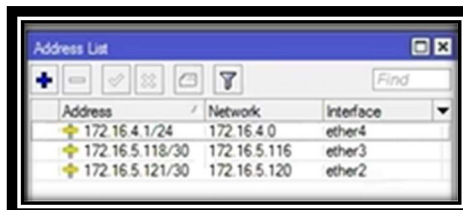


Figura 3.1066 Direcciones IP correspondientes al *ROUTER3*

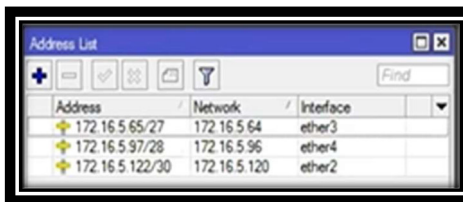


Figura 3.1077 Direcciones IP correspondientes al *ROUTER4*

Paso 1: configuración enrutamiento estático

ROUTER1: En la pestaña "IP" seleccionar "Routes", ver Figura 3.108.

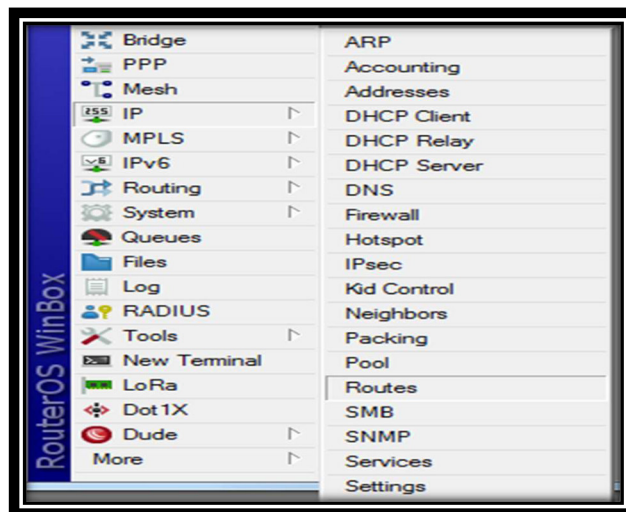


Figura 3.1088 Ingreso "Routes" para asignar rutas al *ROUTER1*

En la ventana que se muestra en la Figura 3.109 seleccionar la opción “Routes” se encuentran todas las direcciones IP que conoce el *ROUTER1*, adicional se encuentra la palabra: “DAC” que indica lo siguiente:

- (D) Ruta Dinámica
- (A) Activa
- (C) Conectada directamente

	Dst. Address	Gateway	Distance	Routing Mark
DAC	172.16.0.0/23	ether4 reachable	0	1
DAC	172.16.5.0/26	ether3 reachable	0	1
DAC	172.16.5.112/...	ether2 reachable	0	1

Figura 3.109 Tabla de rutas aprendidas por el *ROUTER1*

Clic en “+” para crear una nueva ruta en el *router*, ver Figura 3.110.

The 'New Route' dialog box shows the following fields and options:

- General tab:**
 - Dst. Address: 0.0.0.0/0
 - Gateway: (empty)
 - Check Gateway: (checked)
 - Type: unicast
 - Distance: (empty)
 - Scope: 30
 - Target Scope: 10
 - Routing Mark: (empty)
 - Pref. Source: (empty)
- Buttons:** OK, Cancel, Apply, Disable, Comment, Copy, Remove.
- Status:** enabled, active

Figura 3.11010 Asignar una nueva ruta al *ROUTER1*

Para enseñar al *ROUTER1* cómo llegar a la LAN 3 en la sección “Dst. Address” colocar la dirección IP “172.16.2.0/23”. Para el Gateway se escoge la interfaz con la que se une *ROUTER1* y *ROUTER2*, o se escribe la dirección IP “172.16.5.114”. Presionar “OK” para tener la nueva ruta estática creada, ver Figura 3.111.

The 'New Route' dialog box shows the following fields and options:

- General tab:**
 - Dst. Address: 172.16.2.0/23
 - Gateway: 172.16.5.114 reachable ether2
 - Check Gateway: (checked)
 - Type: unicast
 - Distance: 1
 - Scope: 30
 - Target Scope: 10
 - Routing Mark: (empty)
 - Pref. Source: (empty)
- Buttons:** OK, Cancel, Apply, Disable, Comment, Copy, Remove.
- Status:** enabled, active, static

Figura 3.11111 Nueva ruta agregada al *ROUTER1* para llegar a LAN3

Una vez realizado este procedimiento se tiene comunicación entre LAN 1 y 3. Realizar el mismo procedimiento para el *ROUTER1* al resto de LANs de la topología de red diseñada, como se muestran de la Figura 3.112 a la Figura 3.116, tomar en cuenta que para el Gateway se coloca la dirección IP “172.16.5.114”.

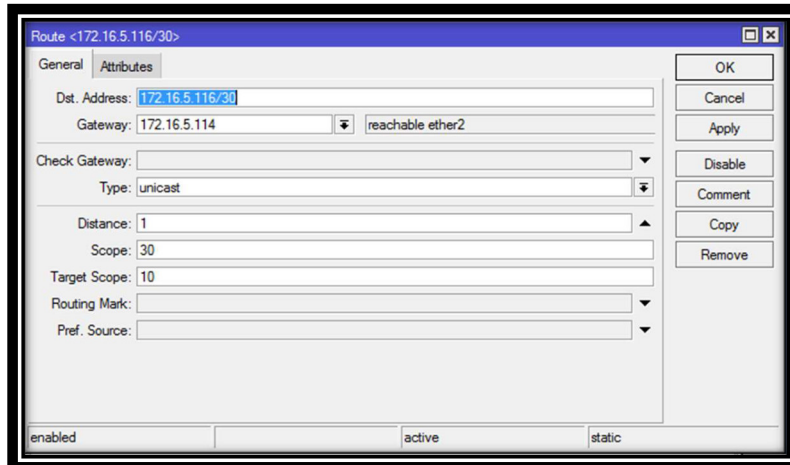


Figura 3.11212 Nueva ruta agregada al *ROUTER1* enlace 172.16.5.116/30

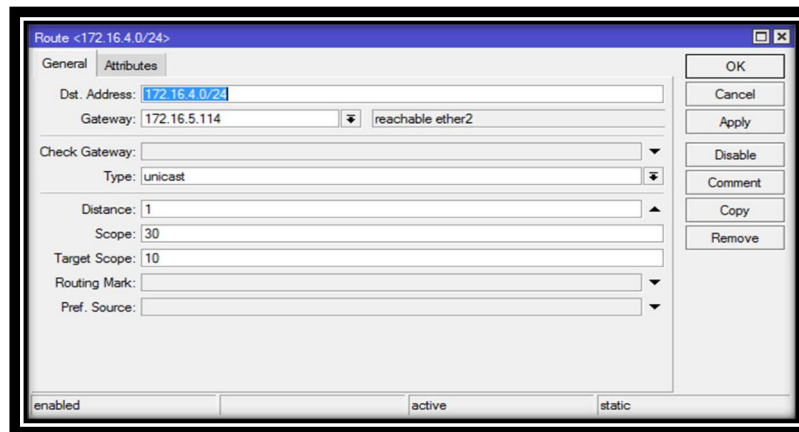


Figura 3.11313 Nueva ruta agregada al *ROUTER1* para llegar a LAN4

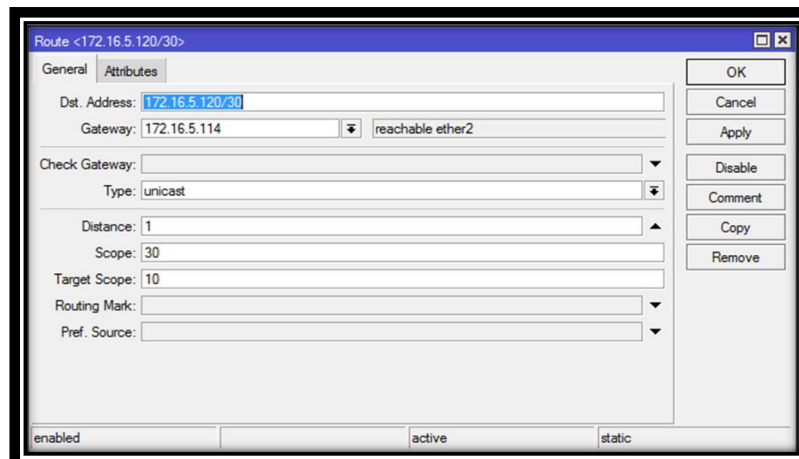


Figura 3.11414 Nueva ruta agregada al *ROUTER1* enlace 172.16.5.120/30

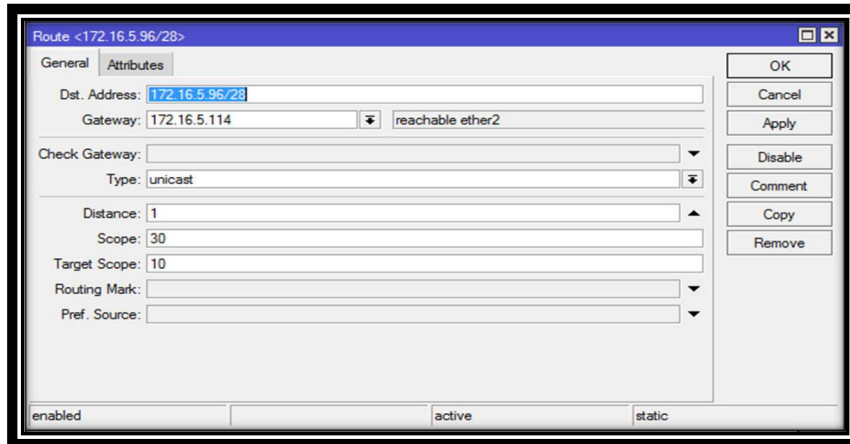


Figura 3.11515 Nueva ruta agregada al *ROUTER1/LAN5*

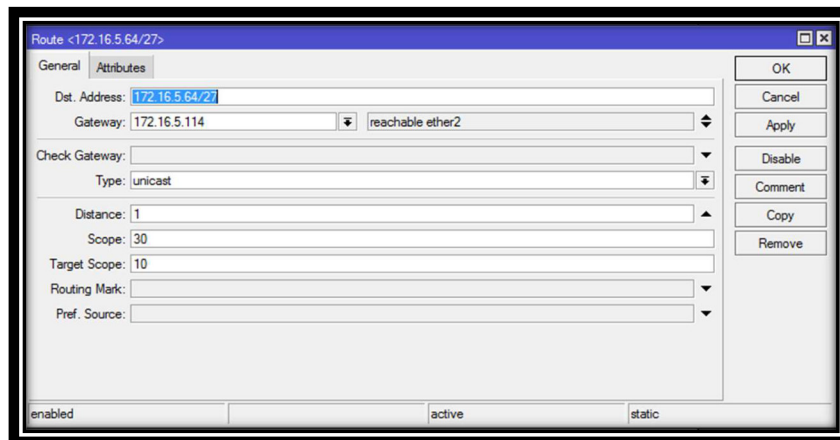


Figura 3.11616 Nueva ruta agregada al *ROUTER1 /LAN6*

La Tabla de Enrutamiento del *ROUTER1* tiene las siguientes siglas, ver Figura 3.117:

El significado de las siglas DAC es:

(D) Ruta dinámica

(A) Activa

(C) Conectada directamente

El significado de las siglas AS es:

(A) Activa

(S) Estática (Aprendida estáticamente)

	Dest. Address	Gateway	Distance	Routing Mark	Pref. Source
DAC	172.16.0.0/23	ether4 reachable	0		172.16.0.1
AS	172.16.2.0/23	172.16.5.114 reachable ether2	1		
AS	172.16.4.0/24	172.16.5.114 reachable ether2	1		
DAC	172.16.5.0/26	ether3 reachable	0		172.16.5.1
AS	172.16.5.64/27	172.16.5.114 reachable ether2	1		
AS	172.16.5.96/28	172.16.5.114 reachable ether2	1		
DAC	172.16.5.112/...	ether2 reachable	0		172.16.5.113
AS	172.16.5.116/...	172.16.5.114 reachable ether2	1		
AS	172.16.5.120/...	172.16.5.114 reachable ether2	1		

Figura 3.11717 Tabla de enrutamiento aprendida por el *ROUTER1*

Repetir el mismo procedimiento para *ROUTER2*, *ROUTER3* y *ROUTER4*.

- *ROUTER2*: dirección IP del *Gateway*: “172.168.5.113” ó “173.168.5.118” dependiendo la ubicación de la *LAN* a la que desea llegar, se puede observar las direcciones aprendidas en la tabla de enrutamiento del *ROUTER2* en la Figura 3.118.

	Dest. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	172.16.0.0/23	172.16.5.113 reachable ether2	1		
DAC	172.16.2.0/23	ether4 reachable	0		172.16.2.1
AS	172.16.4.0/24	172.16.5.118 reachable ether3	1		
AS	172.16.5.0/26	172.16.5.113 reachable ether2	1		
AS	172.16.5.64/27	172.16.5.118 reachable ether3	1		
AS	172.16.5.96/28	172.16.5.118 reachable ether3	1		
DAC	172.16.5.112/30	ether2 reachable	0		172.16.5.114
DAC	172.16.5.116/30	ether3 reachable	0		172.16.5.117
AS	172.16.5.120/30	172.16.5.118 reachable ether3	1		

Figura 3.11818 Tabla de enrutamiento aprendida por el *ROUTER2*

- *ROUTER3*: dirección IP del *Gateway*: “172.168.5.117” ó “173.168.5.122” dependiendo la ubicación de la *LAN* a la que desea llegar, se puede observar las direcciones aprendidas en la tabla de enrutamiento del *ROUTER3* en la Figura 3.119.

	Dest. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	172.16.0.0/23	172.16.5.117 reachable ether3	1		
AS	172.16.2.0/23	172.16.5.117 reachable ether3	1		
DAC	172.16.4.0/24	ether4 reachable	0		172.16.4.1
AS	172.16.5.0/26	172.16.5.117 reachable ether3	1		
AS	172.16.5.64/27	172.16.5.122 reachable ether2	1		
AS	172.16.5.96/28	172.16.5.122 reachable ether2	1		
AS	172.16.5.112/...	172.16.5.117 reachable ether3	1		
DAC	172.16.5.116/...	ether3 reachable	0		172.16.5.118
DAC	172.16.5.120/...	ether2 reachable	0		172.16.5.121

Figura 3.11919 Tabla de enrutamiento aprendida por el *ROUTER3*

- *ROUTER4*: dirección IP del *Gateway*: “172.16.5.121” se puede observar las direcciones aprendidas en la tabla de enrutamiento del *ROUTER4* en la Figura 3.120.

	Dest. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	172.16.0.0/23	172.16.5.121 reachable ether2	1		
AS	172.16.2.0/23	172.16.5.121 reachable ether2	1		
AS	172.16.4.0/24	172.16.5.121 reachable ether2	1		
AS	172.16.5.0/26	172.16.5.121 reachable ether2	1		
DAC	172.16.5.64/27	ether3 reachable	0		1
DAC	172.16.5.96/28	ether4 reachable	0		1
AS	172.16.5.112/...	172.16.5.121 reachable ether2	1		
AS	172.16.5.116/...	172.16.5.121 reachable ether2	1		
DAC	172.16.5.120/...	ether2 reachable	0		1

Figura 3.12020 Tabla de rutas aprendidas por el *ROUTER4*

Paso 2: asignar direcciones IP a las máquinas VPCS

Doble clic a la imagen de cada VPCS y asignar la dirección IP conforme a la LAN que pertenece, ver Figura 3.121.

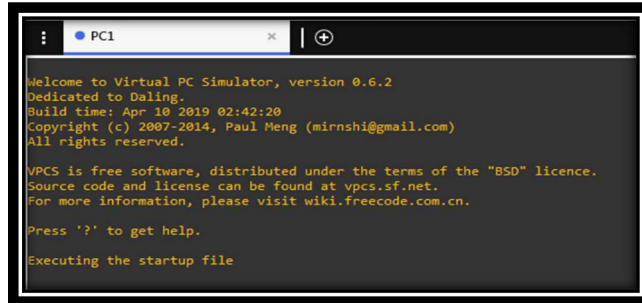


Figura 3. 12121 Pantalla de Solar Putty de una VPCS para asignar direcciones IP

Escribir: ip “dirección IP/máscara” “Gateway”, como se muestra de la Figura 3.122 hasta la Figura 3.127.

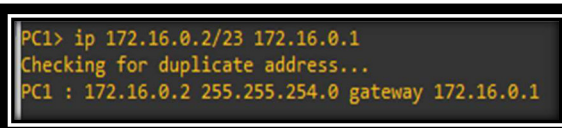


Figura 3.12222 Asignar un dirección IP PC1/LAN1

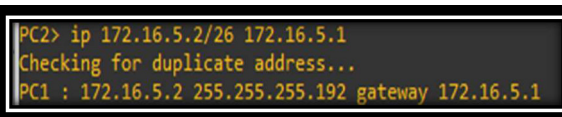


Figura 3.12323 Asignar un dirección IP PC2/LAN2

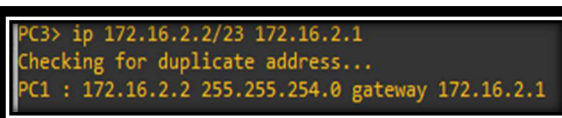


Figura 3.12424 Asignar un dirección IP PC3/LAN3

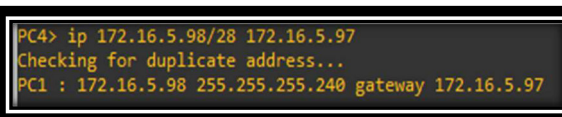


Figura 3.12525 Asignar un dirección IP PC4/LAN5

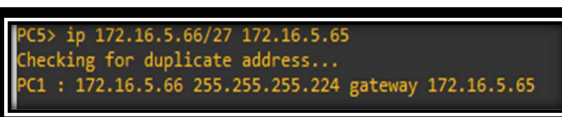


Figura 3.12626 Asignar un dirección IP PC5/LAN6

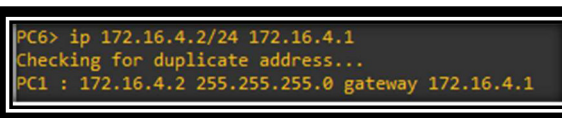


Figura 3.12727 Asignar un dirección IP PC6/LAN4

Paso 3: *ping* entre las LANs de la topología para comprobar conectividad entre las VPCS

Doble *clic* en la VPCS y escribir *ping* "dirección IP a la que se quiere hacer *ping*", ver de la figura 3.128 a la Figura 3.133.

```
PC1> ping 172.16.5.2
84 bytes from 172.16.5.2 icmp_seq=1 ttl=63 time=2.000 ms
84 bytes from 172.16.5.2 icmp_seq=2 ttl=63 time=1.500 ms
84 bytes from 172.16.5.2 icmp_seq=3 ttl=63 time=1.500 ms
84 bytes from 172.16.5.2 icmp_seq=4 ttl=63 time=1.001 ms
84 bytes from 172.16.5.2 icmp_seq=5 ttl=63 time=1.500 ms

PC1> ping 172.16.2.2
84 bytes from 172.16.2.2 icmp_seq=1 ttl=62 time=3.500 ms
84 bytes from 172.16.2.2 icmp_seq=2 ttl=62 time=2.000 ms
84 bytes from 172.16.2.2 icmp_seq=3 ttl=62 time=2.000 ms
84 bytes from 172.16.2.2 icmp_seq=4 ttl=62 time=2.000 ms
84 bytes from 172.16.2.2 icmp_seq=5 ttl=62 time=2.001 ms

PC1> ping 172.16.4.2
84 bytes from 172.16.4.2 icmp_seq=1 ttl=61 time=3.501 ms
84 bytes from 172.16.4.2 icmp_seq=2 ttl=61 time=1.500 ms
84 bytes from 172.16.4.2 icmp_seq=3 ttl=61 time=2.000 ms
84 bytes from 172.16.4.2 icmp_seq=4 ttl=61 time=4.000 ms
84 bytes from 172.16.4.2 icmp_seq=5 ttl=61 time=2.000 ms

PC1> ping 172.16.5.98
84 bytes from 172.16.5.98 icmp_seq=1 ttl=60 time=3.000 ms
84 bytes from 172.16.5.98 icmp_seq=2 ttl=60 time=3.001 ms
84 bytes from 172.16.5.98 icmp_seq=3 ttl=60 time=3.500 ms
84 bytes from 172.16.5.98 icmp_seq=4 ttl=60 time=3.001 ms
84 bytes from 172.16.5.98 icmp_seq=5 ttl=60 time=3.500 ms

PC1> ping 172.16.5.66
84 bytes from 172.16.5.66 icmp_seq=1 ttl=60 time=4.500 ms
84 bytes from 172.16.5.66 icmp_seq=2 ttl=60 time=4.501 ms
84 bytes from 172.16.5.66 icmp_seq=3 ttl=60 time=3.500 ms
84 bytes from 172.16.5.66 icmp_seq=4 ttl=60 time=3.501 ms
84 bytes from 172.16.5.66 icmp_seq=5 ttl=60 time=3.000 ms
```

Figura 312828 Listado de *pings* exitosos desde la LAN1 hacia las otras redes

```
PC2> ping 172.16.0.2
84 bytes from 172.16.0.2 icmp_seq=1 ttl=63 time=1.500 ms
84 bytes from 172.16.0.2 icmp_seq=2 ttl=63 time=1.501 ms
84 bytes from 172.16.0.2 icmp_seq=3 ttl=63 time=1.500 ms
84 bytes from 172.16.0.2 icmp_seq=4 ttl=63 time=3.000 ms
84 bytes from 172.16.0.2 icmp_seq=5 ttl=63 time=1.501 ms

PC2> ping 172.16.2.2
84 bytes from 172.16.2.2 icmp_seq=1 ttl=62 time=2.500 ms
84 bytes from 172.16.2.2 icmp_seq=2 ttl=62 time=1.500 ms
84 bytes from 172.16.2.2 icmp_seq=3 ttl=62 time=1.500 ms
84 bytes from 172.16.2.2 icmp_seq=4 ttl=62 time=1.000 ms
84 bytes from 172.16.2.2 icmp_seq=5 ttl=62 time=1.500 ms

PC2> ping 172.16.4.2
84 bytes from 172.16.4.2 icmp_seq=1 ttl=61 time=2.501 ms
84 bytes from 172.16.4.2 icmp_seq=2 ttl=61 time=3.000 ms
84 bytes from 172.16.4.2 icmp_seq=3 ttl=61 time=3.501 ms
84 bytes from 172.16.4.2 icmp_seq=4 ttl=61 time=2.500 ms
84 bytes from 172.16.4.2 icmp_seq=5 ttl=61 time=3.001 ms

PC2> ping 172.16.5.98
84 bytes from 172.16.5.98 icmp_seq=1 ttl=60 time=3.500 ms
84 bytes from 172.16.5.98 icmp_seq=2 ttl=60 time=2.501 ms
84 bytes from 172.16.5.98 icmp_seq=3 ttl=60 time=2.500 ms
84 bytes from 172.16.5.98 icmp_seq=4 ttl=60 time=2.000 ms
84 bytes from 172.16.5.98 icmp_seq=5 ttl=60 time=2.001 ms

PC2> ping 172.16.5.66
84 bytes from 172.16.5.66 icmp_seq=1 ttl=60 time=2.000 ms
84 bytes from 172.16.5.66 icmp_seq=2 ttl=60 time=2.500 ms
84 bytes from 172.16.5.66 icmp_seq=3 ttl=60 time=2.000 ms
84 bytes from 172.16.5.66 icmp_seq=4 ttl=60 time=4.000 ms
84 bytes from 172.16.5.66 icmp_seq=5 ttl=60 time=3.500 ms
```

Figura 3.12930 Listado de *pings* exitosos desde la LAN2 hacia las otras redes


```
PC3> ping 172.16.5.2
84 bytes from 172.16.5.2 icmp_seq=1 ttl=62 time=2.001 ms
84 bytes from 172.16.5.2 icmp_seq=2 ttl=62 time=2.000 ms
84 bytes from 172.16.5.2 icmp_seq=3 ttl=62 time=1.000 ms
84 bytes from 172.16.5.2 icmp_seq=4 ttl=62 time=1.000 ms
84 bytes from 172.16.5.2 icmp_seq=5 ttl=62 time=1.001 ms

PC3> ping 172.16.4.2
84 bytes from 172.16.4.2 icmp_seq=1 ttl=62 time=2.001 ms
84 bytes from 172.16.4.2 icmp_seq=2 ttl=62 time=2.500 ms
84 bytes from 172.16.4.2 icmp_seq=3 ttl=62 time=3.001 ms
84 bytes from 172.16.4.2 icmp_seq=4 ttl=62 time=4.000 ms

PC3> ping 172.16.5.66
84 bytes from 172.16.5.66 icmp_seq=1 ttl=61 time=4.001 ms
84 bytes from 172.16.5.66 icmp_seq=2 ttl=61 time=2.500 ms
84 bytes from 172.16.5.66 icmp_seq=3 ttl=61 time=2.500 ms
84 bytes from 172.16.5.66 icmp_seq=4 ttl=61 time=2.500 ms
84 bytes from 172.16.5.66 icmp_seq=5 ttl=61 time=2.500 ms

PC3> ping 172.16.5.98
84 bytes from 172.16.5.98 icmp_seq=1 ttl=61 time=2.501 ms
84 bytes from 172.16.5.98 icmp_seq=2 ttl=61 time=3.000 ms
84 bytes from 172.16.5.98 icmp_seq=3 ttl=61 time=2.501 ms
84 bytes from 172.16.5.98 icmp_seq=4 ttl=61 time=2.500 ms
84 bytes from 172.16.5.98 icmp_seq=5 ttl=61 time=3.501 ms

PC3> ping 172.16.0.2
84 bytes from 172.16.0.2 icmp_seq=1 ttl=62 time=2.000 ms
84 bytes from 172.16.0.2 icmp_seq=2 ttl=62 time=2.501 ms
84 bytes from 172.16.0.2 icmp_seq=3 ttl=62 time=1.500 ms
84 bytes from 172.16.0.2 icmp_seq=4 ttl=62 time=2.500 ms
84 bytes from 172.16.0.2 icmp_seq=5 ttl=62 time=2.000 ms
```

Figura 3.13031 Listado de *pings* exitosos desde la LAN3 hacia las otras redes

```
PC6> ping 172.16.5.2
84 bytes from 172.16.5.2 icmp_seq=1 ttl=61 time=3.501 ms
84 bytes from 172.16.5.2 icmp_seq=2 ttl=61 time=3.000 ms
84 bytes from 172.16.5.2 icmp_seq=3 ttl=61 time=2.501 ms
84 bytes from 172.16.5.2 icmp_seq=4 ttl=61 time=3.500 ms
84 bytes from 172.16.5.2 icmp_seq=5 ttl=61 time=2.501 ms

PC6> ping 172.16.2.2
84 bytes from 172.16.2.2 icmp_seq=1 ttl=62 time=2.001 ms
84 bytes from 172.16.2.2 icmp_seq=2 ttl=62 time=1.000 ms
84 bytes from 172.16.2.2 icmp_seq=3 ttl=62 time=1.000 ms
84 bytes from 172.16.2.2 icmp_seq=4 ttl=62 time=1.000 ms
84 bytes from 172.16.2.2 icmp_seq=5 ttl=62 time=1.500 ms

PC6> ping 172.16.5.66
84 bytes from 172.16.5.66 icmp_seq=1 ttl=62 time=2.001 ms
84 bytes from 172.16.5.66 icmp_seq=2 ttl=62 time=2.000 ms
84 bytes from 172.16.5.66 icmp_seq=3 ttl=62 time=1.500 ms
84 bytes from 172.16.5.66 icmp_seq=4 ttl=62 time=2.001 ms
84 bytes from 172.16.5.66 icmp_seq=5 ttl=62 time=1.500 ms

PC6> ping 172.16.5.98
84 bytes from 172.16.5.98 icmp_seq=1 ttl=62 time=2.501 ms
84 bytes from 172.16.5.98 icmp_seq=2 ttl=62 time=2.000 ms
84 bytes from 172.16.5.98 icmp_seq=3 ttl=62 time=1.500 ms
84 bytes from 172.16.5.98 icmp_seq=4 ttl=62 time=2.001 ms
84 bytes from 172.16.5.98 icmp_seq=5 ttl=62 time=1.000 ms

PC6> ping 172.16.0.2
84 bytes from 172.16.0.2 icmp_seq=1 ttl=61 time=3.501 ms
84 bytes from 172.16.0.2 icmp_seq=2 ttl=61 time=3.000 ms
84 bytes from 172.16.0.2 icmp_seq=3 ttl=61 time=3.001 ms
84 bytes from 172.16.0.2 icmp_seq=4 ttl=61 time=3.000 ms
84 bytes from 172.16.0.2 icmp_seq=5 ttl=61 time=2.501 ms
```

Figura 3.13131 Listado de *pings* exitosos desde la LAN4 hacia las otras redes

```
PC4> ping 172.16.5.2
84 bytes from 172.16.5.2 icmp_seq=1 ttl=60 time=5.000 ms
84 bytes from 172.16.5.2 icmp_seq=2 ttl=60 time=3.501 ms
84 bytes from 172.16.5.2 icmp_seq=3 ttl=60 time=3.500 ms
84 bytes from 172.16.5.2 icmp_seq=4 ttl=60 time=2.001 ms
84 bytes from 172.16.5.2 icmp_seq=5 ttl=60 time=2.000 ms

PC4> ping 172.16.2.2
84 bytes from 172.16.2.2 icmp_seq=1 ttl=61 time=3.000 ms
84 bytes from 172.16.2.2 icmp_seq=2 ttl=61 time=3.001 ms
84 bytes from 172.16.2.2 icmp_seq=3 ttl=61 time=2.500 ms
84 bytes from 172.16.2.2 icmp_seq=4 ttl=61 time=3.000 ms
84 bytes from 172.16.2.2 icmp_seq=5 ttl=61 time=3.000 ms

PC4> ping 172.16.4.2
84 bytes from 172.16.4.2 icmp_seq=1 ttl=62 time=1.000 ms
84 bytes from 172.16.4.2 icmp_seq=2 ttl=62 time=1.000 ms
84 bytes from 172.16.4.2 icmp_seq=3 ttl=62 time=2.000 ms
84 bytes from 172.16.4.2 icmp_seq=4 ttl=62 time=2.001 ms
84 bytes from 172.16.4.2 icmp_seq=5 ttl=62 time=2.000 ms

PC4> ping 172.16.5.66
84 bytes from 172.16.5.66 icmp_seq=1 ttl=63 time=1.001 ms
84 bytes from 172.16.5.66 icmp_seq=2 ttl=63 time=1.000 ms
84 bytes from 172.16.5.66 icmp_seq=3 ttl=63 time=1.000 ms
84 bytes from 172.16.5.66 icmp_seq=4 ttl=63 time=1.000 ms
84 bytes from 172.16.5.66 icmp_seq=5 ttl=63 time=0.500 ms

PC4> ping 172.16.0.2
84 bytes from 172.16.0.2 icmp_seq=1 ttl=60 time=3.500 ms
84 bytes from 172.16.0.2 icmp_seq=2 ttl=60 time=3.501 ms
84 bytes from 172.16.0.2 icmp_seq=3 ttl=60 time=3.500 ms
84 bytes from 172.16.0.2 icmp_seq=4 ttl=60 time=4.001 ms
84 bytes from 172.16.0.2 icmp_seq=5 ttl=60 time=3.500 ms
```

Figura 3.13232 Listado de *pings* exitosos desde la LAN5 hacia las otras redes

```
PC5> ping 172.16.5.2
84 bytes from 172.16.5.2 icmp_seq=1 ttl=60 time=3.500 ms
84 bytes from 172.16.5.2 icmp_seq=2 ttl=60 time=2.000 ms
84 bytes from 172.16.5.2 icmp_seq=3 ttl=60 time=2.501 ms
84 bytes from 172.16.5.2 icmp_seq=4 ttl=60 time=1.500 ms
84 bytes from 172.16.5.2 icmp_seq=5 ttl=60 time=1.500 ms

PC5> ping 172.16.2.2
84 bytes from 172.16.2.2 icmp_seq=1 ttl=61 time=3.001 ms
84 bytes from 172.16.2.2 icmp_seq=2 ttl=61 time=2.500 ms
84 bytes from 172.16.2.2 icmp_seq=3 ttl=61 time=3.001 ms
84 bytes from 172.16.2.2 icmp_seq=4 ttl=61 time=2.500 ms
84 bytes from 172.16.2.2 icmp_seq=5 ttl=61 time=3.000 ms



PC5> ping 172.16.5.98
84 bytes from 172.16.5.98 icmp_seq=1 ttl=63 time=1.500 ms
84 bytes from 172.16.5.98 icmp_seq=2 ttl=63 time=1.500 ms
84 bytes from 172.16.5.98 icmp_seq=3 ttl=63 time=1.501 ms
84 bytes from 172.16.5.98 icmp_seq=4 ttl=63 time=0.500 ms
84 bytes from 172.16.5.98 icmp_seq=5 ttl=63 time=0.500 ms

PC5> ping 172.16.4.2
84 bytes from 172.16.4.2 icmp_seq=1 ttl=62 time=2.500 ms
84 bytes from 172.16.4.2 icmp_seq=2 ttl=62 time=2.000 ms
84 bytes from 172.16.4.2 icmp_seq=3 ttl=62 time=2.000 ms
84 bytes from 172.16.4.2 icmp_seq=4 ttl=62 time=2.000 ms
84 bytes from 172.16.4.2 icmp_seq=5 ttl=62 time=2.001 ms

PC5> ping 172.16.0.2
84 bytes from 172.16.0.2 icmp_seq=1 ttl=60 time=5.001 ms
84 bytes from 172.16.0.2 icmp_seq=2 ttl=60 time=3.500 ms
84 bytes from 172.16.0.2 icmp_seq=3 ttl=60 time=3.001 ms
84 bytes from 172.16.0.2 icmp_seq=4 ttl=60 time=3.500 ms
84 bytes from 172.16.0.2 icmp_seq=5 ttl=60 time=4.001 ms
```

Figura 3.13333 Listado de *pings* exitosos desde la LAN6 hacia las otras redes

6. RECOMENDACIONES:

- Para realizar la asignación de direcciones IP a los diferentes *routers*, hay que colocar de manera correcta dirección IP, máscara y *Gateway* que corresponden a cada red y enlaces que unen los *routers*.
- Para cualquier cambio a realizarse en la configuración de los adaptadores de red de los *routers* simulados, ya sea en GNS o *VirtualBox*, primero se debe pausar el programa presionando el ícono  (pausa), sino GNS3 no permitirá efectuar dichos cambios mientras está corriendo o se presentará un error en el programa que no permitirá acceder a la configuración de los equipos mediante *Winbox*. Una vez efectuadas las modificaciones correspondientes se puede presionar  (iniciar) para continuar con la práctica.



ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

HOJA GUÍA

PRÁCTICA 3

1. **TEMA:** Protocolo de Enrutamiento dinámico IGP (*Interior Gateway Protocol*):
Protocolo Vector Distancia RIP
2. **OBJETIVO:**
Configurar el protocolo de Enrutamiento RIP en el diagrama de conexiones propuesto.
3. **DIAGRAMA DE CONEXIONES:**
Armar la siguiente topología:

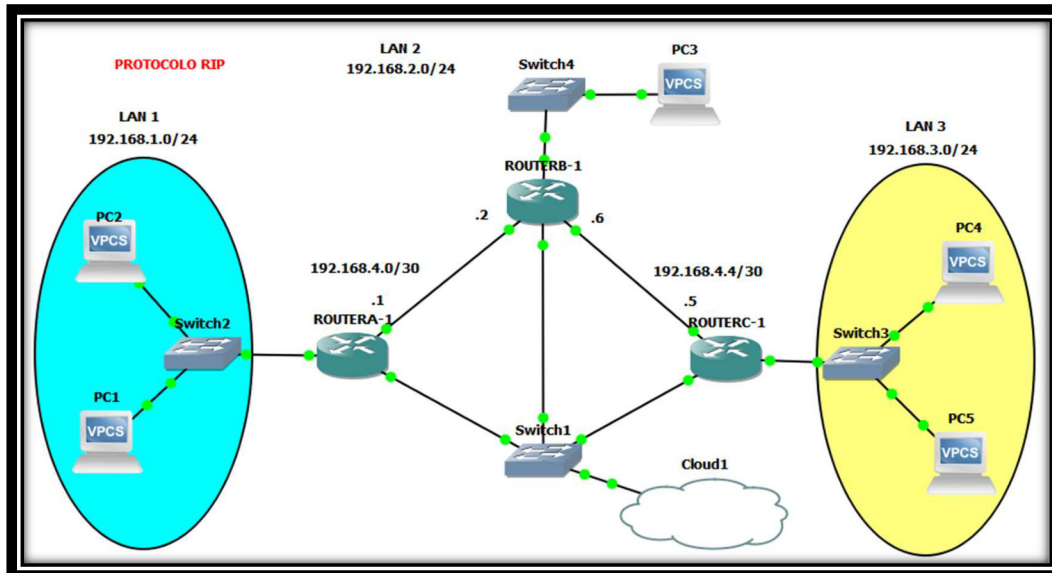


Figura 3.1344 Diagrama de conexiones práctica 3

4. DIAGRAMA DE CONEXIONES DESARROLLO DE LA PRÁCTICA:

NOTA: tiempo estimado para realizar la presente práctica de laboratorio es de una hora. Se recomienda que el estudiante tenga creadas 3 máquinas virtuales en *VirtualBox* y vinculadas con *GNS3* para realizar la práctica. Adicional se debe tener creado una interfaz de *loopback* en el computador.

Una vez realizado el diagrama de red correspondiente y todas las configuraciones previas. Se procede con la configuración de direcciones IP que debe conocer cada uno de los *routers*, tomando en cuenta el puerto de conexión y cada dirección de red a conocer, como se puede observar desde la Figura 3.135 a la Figura 3.137.

Address	Network	Interface
192.168.1.1/24	192.168.1.0	ether3
192.168.4.1/30	192.168.4.0	ether2

Figura 3.1355 Direcciones IP aprendidas por el ROUTERA

Address	Network	Interface
192.168.2.1/24	192.168.2.0	ether3
192.168.4.2/30	192.168.4.0	ether2
192.168.4.6/30	192.168.4.4	ether1

Figura 3.1366 Lista de direcciones IP aprendidas por el ROUTERB

Address	Network	Interface
192.168.3.1/24	192.168.3.0	ether3
192.168.4.5/30	192.168.4.4	ether1

Figura 3.1377 Lista de direcciones IP aprendidas por el ROUTERC

Paso 1: configuración del protocolo RIP

Ingresar a "Routing" y seleccionar "RIP", ver Figura 3.138.

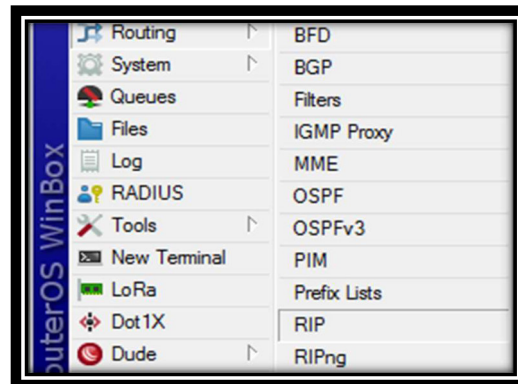


Figura 3.1388 Ingreso a la pestaña "Routing" para configurar el protocolo RIP en el ROUTERA

Clic en (+) y en la sección "Interface" escoger la interfaz que está designada por el enlace. En las secciones "Receive" y "Send" se indica la versión que el protocolo RIP trabajará puede ser V1, V2 o ambas. Presionar OK, como se observa en la Figura 3.139.

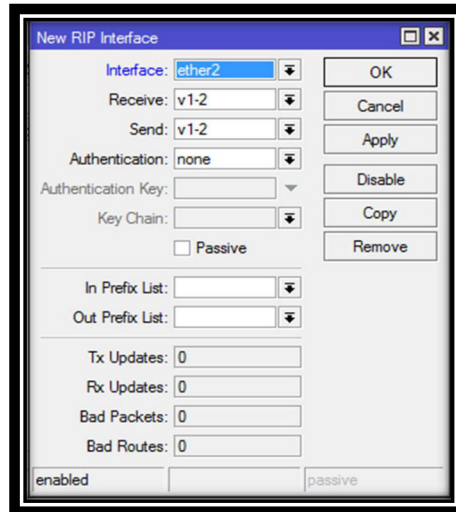


Figura 3.13939 Configuración del puerto por donde se envía y recibe el protocolo RIP en el *ROUTERA*

La pestaña “*Networks*” indica la red de transporte de paquetes RIP. Red de enlace: 192.168.4.0/30, ver Figura 3.140.



Figura 3.14040 Pestaña donde indica que el puerto ha sido levantado en el *ROUTERA*

Clic en (+), en la pestaña “*Interfaces*” seleccionar “*RIP Setting*” para habilitar que el protocolo redistribuya las rutas conectadas, como se observa en la Figura 3.141.

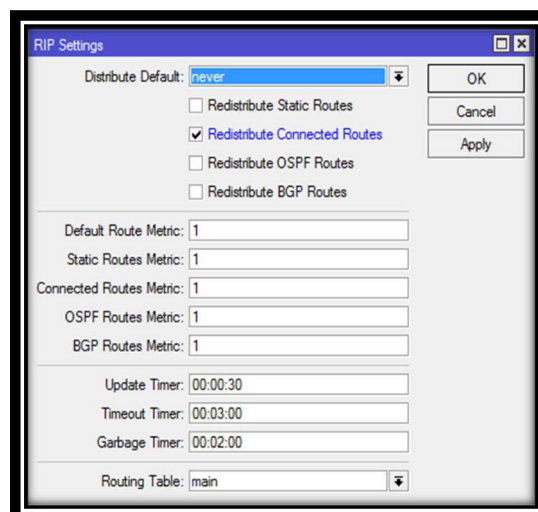


Figura 3.14141 Opciones de compartición de RIP para el *ROUTERA*

Repetir el mismo procedimiento para los *routers*: *ROUTERB* y *ROUTERC*, como se muestra en la Figura 3.142 a la Figura 3.145.

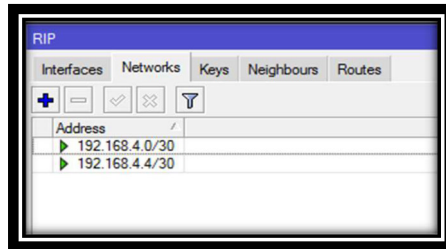


Figura 3.14242 Listado de redes que usa el protocolo RIP en el *ROUTERB*

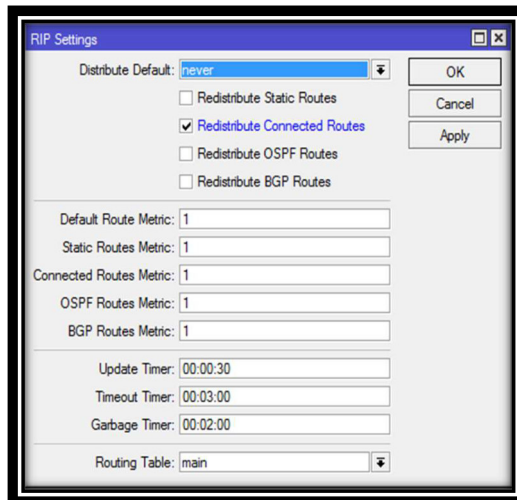


Figura 3.14343 Opciones de compartición de RIP para el *ROUTERB*

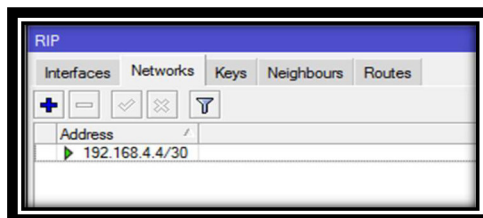


Figura 3.14444 Redes que usa el protocolo RIP en el *ROUTERC*

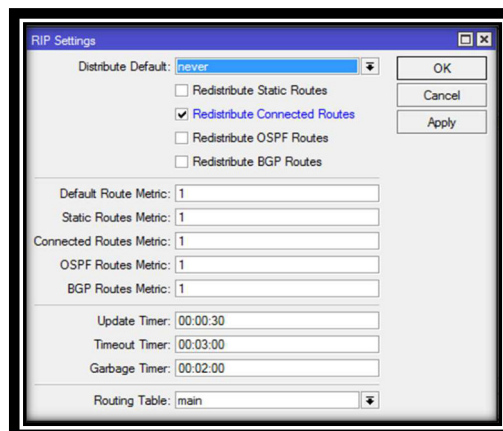


Figura 3.1455 Opciones de compartición de RIP para el *ROUTERC*

Paso 2: comprobación de rutas aprendidas mediante protocolo RIP

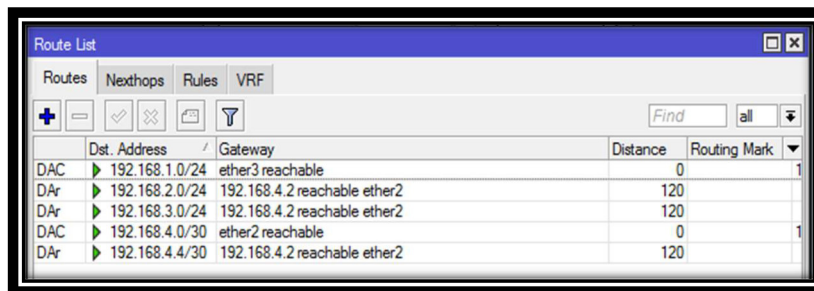
Ver la tabla de Enrutamiento de los *routers*, y verificar las rutas que se han aprendido mediante el protocolo RIP, este procedimiento se lo realiza en la pestaña "IP" opción "Routes". En la Tabla de enrutamiento se encuentra las siguientes siglas, ver desde la Figura 3.146 a la Figura 3.148.

El significado de las siglas DAC es:

- (D) Ruta Dinámica
- (A) Activa
- (C) Conectada directamente

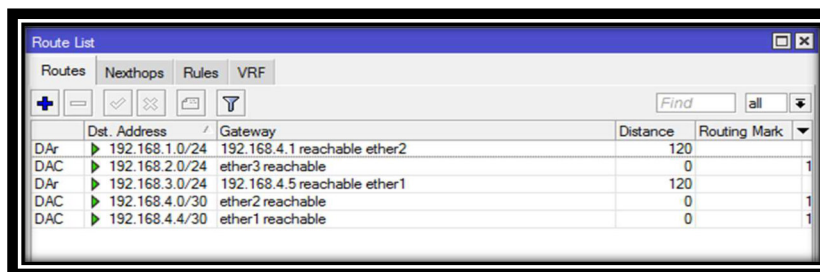
El significado de las siglas DAr es:

- (D) Ruta Dinámica
- (A) Activa
- (r) Aprendida por RIP



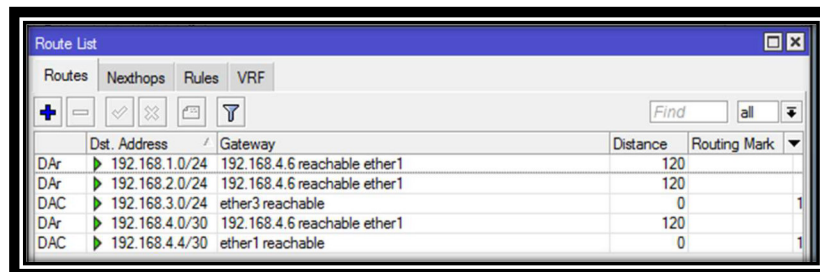
	Dst. Address	Gateway	Distance	Routing Mark
DAC	192.168.1.0/24	ether3 reachable	0	1
DAr	192.168.2.0/24	192.168.4.2 reachable ether2	120	
DAr	192.168.3.0/24	192.168.4.2 reachable ether2	120	
DAC	192.168.4.0/30	ether2 reachable	0	1
DAr	192.168.4.4/30	192.168.4.2 reachable ether2	120	

Figura 3.14646 Listado de rutas aprendidas por el ROUTERA



	Dst. Address	Gateway	Distance	Routing Mark
DAr	192.168.1.0/24	192.168.4.1 reachable ether2	120	
DAC	192.168.2.0/24	ether3 reachable	0	1
DAr	192.168.3.0/24	192.168.4.5 reachable ether1	120	
DAC	192.168.4.0/30	ether2 reachable	0	1
DAC	192.168.4.4/30	ether1 reachable	0	1

Figura 3.14747 Listado de rutas aprendidas por el ROUTERB



	Dst. Address	Gateway	Distance	Routing Mark
DAr	192.168.1.0/24	192.168.4.6 reachable ether1	120	
DAr	192.168.2.0/24	192.168.4.6 reachable ether1	120	
DAC	192.168.3.0/24	ether3 reachable	0	1
DAr	192.168.4.0/30	192.168.4.6 reachable ether1	120	
DAC	192.168.4.4/30	ether1 reachable	0	1

Figura 3.14848 Listado de rutas aprendidas por el ROUTERC

Paso 3: asignar las direcciones IP a las máquinas VPCS

Doble clic en la VPCS: Escribir ip “dirección IP/máscara” “Gateway”. Ejemplo: ip 192.168.1.2/24 192.168.1.1, como se muestra en la Figura 3.149.

```
PC1> ip 192.168.1.2/24 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.2 255.255.255.0 gateway 192.168.1.1
```

Figura 3.14949 Designación de una dirección IP 192.168.1.2/24 para la VPCS de la LAN1

Repetir el proceso para las demás VPCS, tomando en cuenta la LAN en la que se encuentran, como se observa desde la Figura 3.150 a la Figura 3.153.

```
PC2> ip 192.168.1.3/24 192.168.1.1
Checking for duplicate address...
PC1 : 192.168.1.3 255.255.255.0 gateway 192.168.1.1
```

Figura 3.15050 Designación de una dirección IP 192.168.1.3/24 para la VPCS de la LAN2

```
PC3> ip 192.168.2.2/24 192.168.2.1
Checking for duplicate address...
PC1 : 192.168.2.2 255.255.255.0 gateway 192.168.2.1
```

Figura 3.15111 Designación de una dirección IP 192.168.2.2/24 para la VPCS de la LAN2

```
PC4> ip 192.168.3.2/24 192.168.3.1
Checking for duplicate address...
PC1 : 192.168.3.2 255.255.255.0 gateway 192.168.3.1
```

Figura 3.15222 Designación de una dirección IP 192.168.3.2/24 para la VPCS de la LAN3

```
PC5> ip 192.168.3.3/24 192.168.3.1
Checking for duplicate address...
PC1 : 192.168.3.3 255.255.255.0 gateway 192.168.3.1
```

Figura 3.15353 Designación de una dirección IP 192.168.3.3/24 para la VPCS de la LAN3

Paso 4: ping entre LANs de la topología para comprobar conectividad entre VPCS

Clic en la VPCS: Escribir ping “dirección IP a la que se quiere hacer ping”, ver desde Figura 3.154 a la Figura 3.159.

```
PC1> ping 192.168.2.2
84 bytes from 192.168.2.2 icmp_seq=1 ttl=62 time=3.500 ms
84 bytes from 192.168.2.2 icmp_seq=2 ttl=62 time=2.000 ms
84 bytes from 192.168.2.2 icmp_seq=3 ttl=62 time=2.000 ms
84 bytes from 192.168.2.2 icmp_seq=4 ttl=62 time=2.000 ms
84 bytes from 192.168.2.2 icmp_seq=5 ttl=62 time=2.001 ms
```

Figura 3.15454 Ping realizado desde la LAN1 a la LAN2 usando una VPCS

```
PC1> ping 192.168.3.2
84 bytes from 192.168.3.2 icmp_seq=1 ttl=61 time=5.500 ms
84 bytes from 192.168.3.2 icmp_seq=2 ttl=61 time=3.001 ms
84 bytes from 192.168.3.2 icmp_seq=3 ttl=61 time=2.500 ms
84 bytes from 192.168.3.2 icmp_seq=4 ttl=61 time=3.501 ms
84 bytes from 192.168.3.2 icmp_seq=5 ttl=61 time=3.000 ms
```

Figura 3.1555 Ping realizado desde la LAN1 a la LAN3 usando una VPCS

```
PC3> ping 192.168.1.3
84 bytes from 192.168.1.3 icmp_seq=1 ttl=62 time=2.500 ms
84 bytes from 192.168.1.3 icmp_seq=2 ttl=62 time=2.001 ms
84 bytes from 192.168.1.3 icmp_seq=3 ttl=62 time=2.000 ms
84 bytes from 192.168.1.3 icmp_seq=4 ttl=62 time=2.000 ms
84 bytes from 192.168.1.3 icmp_seq=5 ttl=62 time=2.000 ms
```

Figura 3.15656 Ping realizado desde la LAN2 a la LAN1 usando una VPCS

```
PC3> ping 192.168.3.3
84 bytes from 192.168.3.3 icmp_seq=1 ttl=62 time=3.000 ms
84 bytes from 192.168.3.3 icmp_seq=2 ttl=62 time=2.001 ms
84 bytes from 192.168.3.3 icmp_seq=3 ttl=62 time=2.000 ms
84 bytes from 192.168.3.3 icmp_seq=4 ttl=62 time=2.000 ms
84 bytes from 192.168.3.3 icmp_seq=5 ttl=62 time=2.001 ms
```

Figura 3.15757 Ping realizado desde la LAN2 a la LAN3 usando una VPCS



```
PC5> ping 192.168.1.3
84 bytes from 192.168.1.3 icmp_seq=1 ttl=61 time=2.500 ms
84 bytes from 192.168.1.3 icmp_seq=2 ttl=61 time=3.001 ms
84 bytes from 192.168.1.3 icmp_seq=3 ttl=61 time=2.500 ms
84 bytes from 192.168.1.3 icmp_seq=4 ttl=61 time=3.001 ms
84 bytes from 192.168.1.3 icmp_seq=5 ttl=61 time=2.500 ms
```

Figura 3.1588 Ping realizado desde la LAN3 a la LAN1 usando una VPCS

```
PC5> ping 192.168.2.2
84 bytes from 192.168.2.2 icmp_seq=1 ttl=62 time=1.500 ms
84 bytes from 192.168.2.2 icmp_seq=2 ttl=62 time=1.500 ms
84 bytes from 192.168.2.2 icmp_seq=3 ttl=62 time=2.501 ms
84 bytes from 192.168.2.2 icmp_seq=4 ttl=62 time=2.500 ms
84 bytes from 192.168.2.2 icmp_seq=5 ttl=62 time=3.501 ms
```

Figura 3.15959 Ping realizado desde la LAN3 a la LAN2 usando una VPCS

7. RECOMENDACIONES:

- Se debe tener en cuenta que para la correcta implementación de la práctica hay que habilitar la redistribución de rutas conectadas, ya que de esta manera el protocolo RIP podrá ser distribuido y la información de las rutas y redes enviada a los demás *routers*.
- Para cualquier cambio a realizarse en la configuración de los adaptadores de red de los *routers* simulados, ya sea en GNS o *VirtualBox*, primero se debe pausar el programa presionando el ícono  (pausa), sino GNS3 no permitirá efectuar dichos cambios mientras está corriendo o se presentará un error en el programa que no permitirá acceder a la configuración de los equipos mediante *Winbox*. Una vez efectuadas las modificaciones correspondientes se puede presionar  (iniciar) para continuar con la práctica.



ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

HOJA GUÍA PRÁCTICA 4

1. **TEMA:** Protocolo de Enrutamiento Dinámico EGP (*Exterior Gateway Protocol*)
Protocolo BGP
2. **OBJETIVO:**
Establecer conexión del protocolo BGP entre equipos *Mikrotik*.
3. **DESARROLLO DE LA PRÁCTICA DIAGRAMA DE CONEXIONES:**
Armar la siguiente topología:

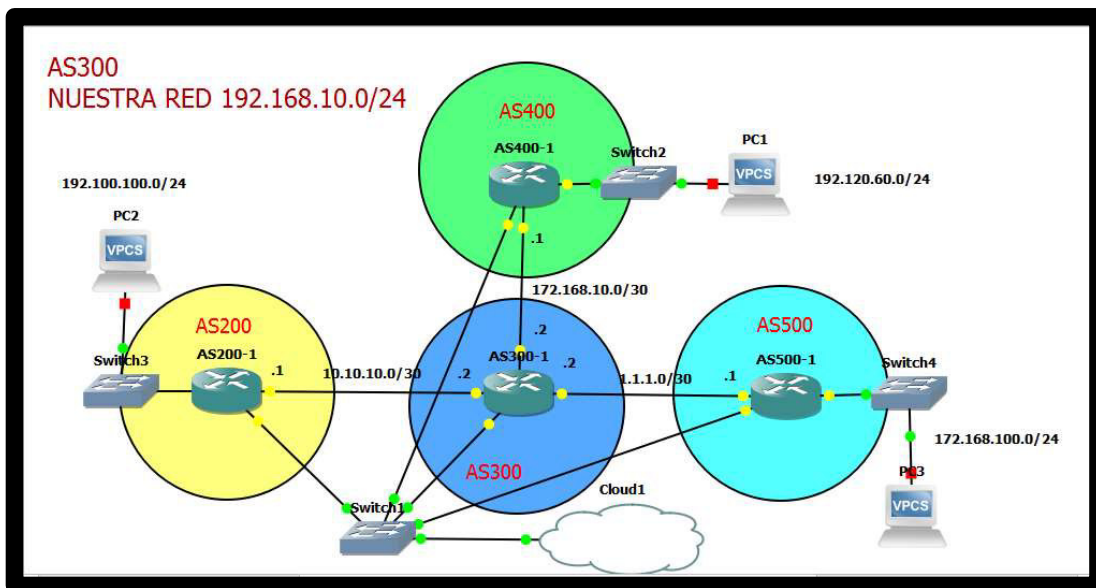


Figura 3.1600 Diagrama de conexiones práctica 4

4. DESARROLLO DE LA PRÁCTICA:

NOTA: tiempo estimado para realizar la presente práctica de laboratorio es de una hora. Se recomienda que el estudiante tenga creadas 4 máquinas virtuales en *VirtualBox* y vinculadas con *GNS3* para realizar la práctica. Adicional se debe tener creado una interfaz de *loopback* en el computador.

Una vez realizado el diagrama de red correspondiente y todas las configuraciones previas. Se procede con la configuración de direcciones IP que debe conocer cada uno de los *routers*, tomando en cuenta el puerto de conexión y cada dirección de red a conocer, como se puede observar desde la Figura 3.161 a la Figura 3.163.

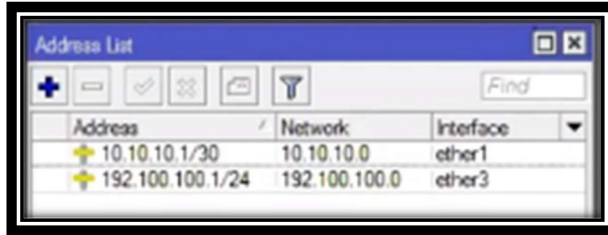


Figura 3.1611 Redes aprendidas por el router AS200

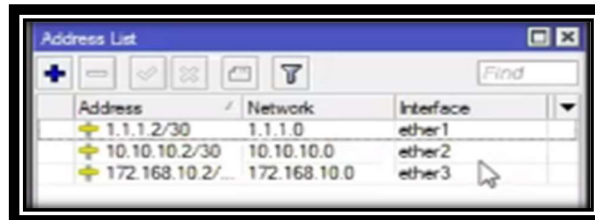


Figura 3.1622 Redes aprendidas por el router AS300

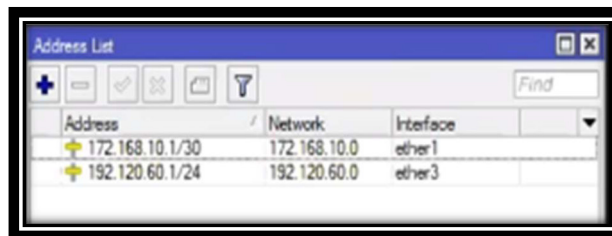


Figura 3.1633 Redes aprendidas por el router AS400

Paso 1: creación de interfaces de *Bridge* en todos los routers para levantar BGP

Configuración ROUTER AS500

En la pestaña “*Bridge*” hacer clic en (+) para crear una interfaz con nombre “*loop*”, ver Figura 3.164 y Figura 3.165.

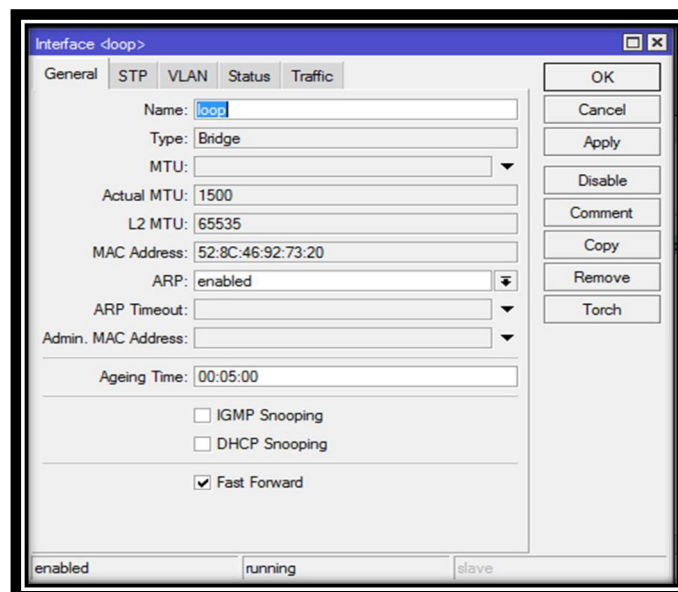


Figura 3.1644 Configuración de la interfaz lógica denominada “*loop*”

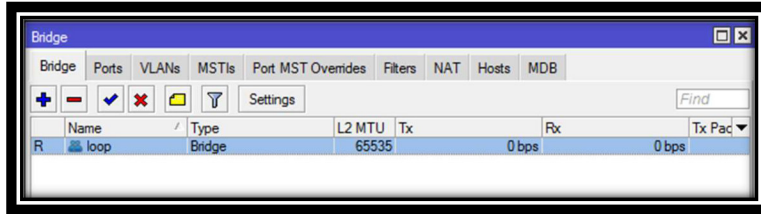


Figura 3.1655 Interfaz lógica “loop” levantada en el router

Repetir el procedimiento antes mencionado para los routers AS300 y AS400.

Paso 2: asignación de direcciones IP a las interfaces “loop”

En la pestaña “IP” opción “Addresses” hacer clic en el símbolo “+” para crear la nueva dirección IP de la interfaz lógica “loop” que será aprendida por los routers, como se muestran desde la Figura 3.166 y Figura 3.167.

AS400

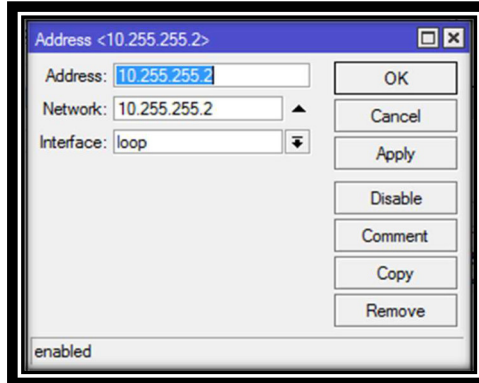


Figura 3.1666 Dirección IP agregada a la interfaz lógica “loop” del AS400

AS500

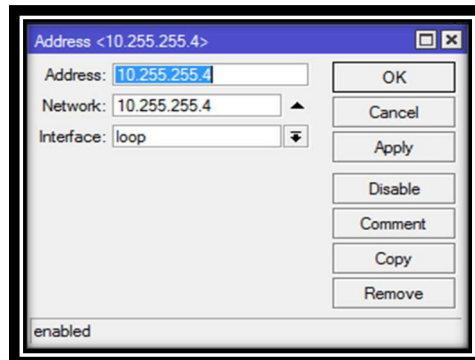


Figura 3.1677 Dirección IP agregada a la interfaz lógica “loop” del AS500

Crear una interfaz *brigde* en el router AS300 con el nombre “nuestra red”, con la finalidad de simular que se encuentra conectado a esta red. Para esto en la pestaña “Bridge” hacer clic en “+”, ver Figura 3.168.

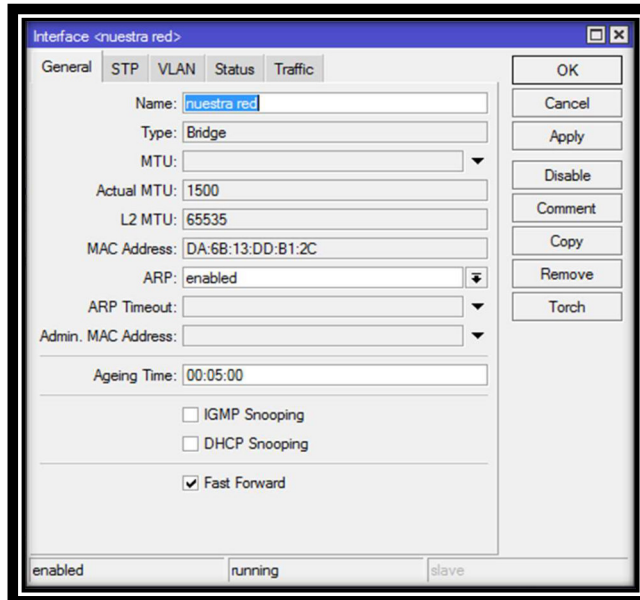


Figura 3.1688 Configuración y levantamiento de la interfaz lógica “nuestra red” en AS300
 Asignar una dirección IP con una de las direcciones de la red en este caso se usará 192.168.10.1/24, ver Figura 3.169.

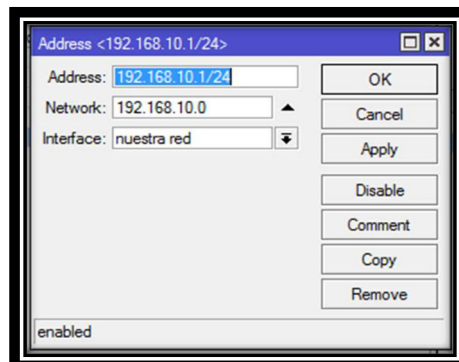


Figura 3.16969 Asignación de una dirección IP a la interfaz lógica “nuestra red”

Paso 3: configurar el protocolo BGP

En la pestaña “Routing” seleccionar BGP.

Cambiar los siguientes parámetros en la Interfaz que se encuentra creada por defecto, ver Figura 3.170:

- AS Sistema Autónomo al que pertenece.
- Router ID Dirección del *bridge* que se creó.

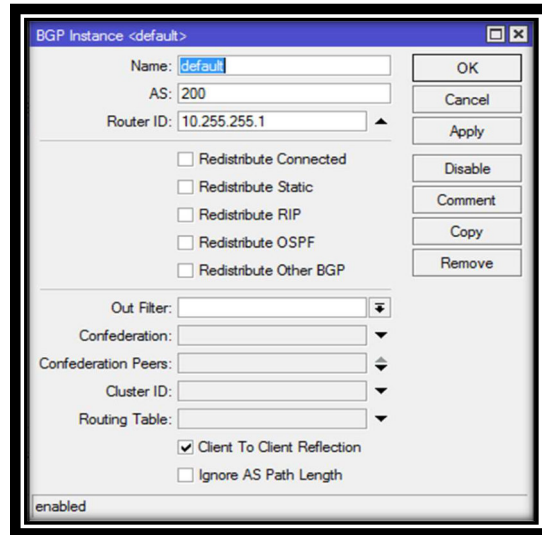


Figura 3.17070 Configuración de la dirección IP usada por BGP del *router* AS200

En la pestaña “PEERS”, se establece una relación con otro *router* mediante *protocolo* BGP, ver Figura 3.171.

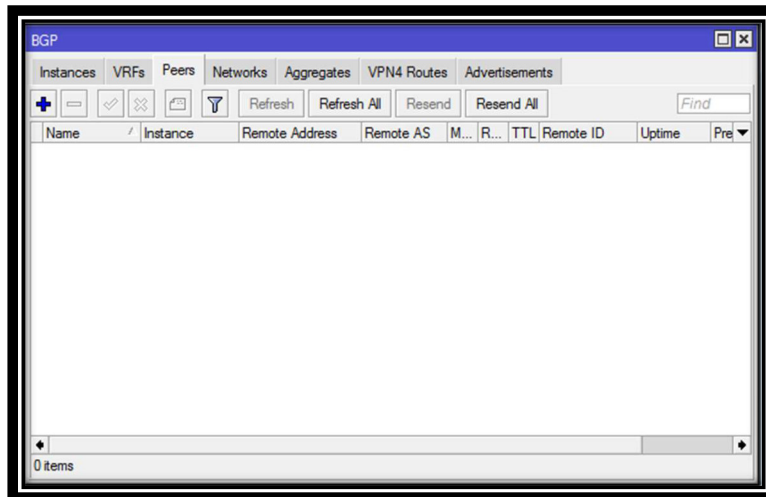


Figura 3.1711 Ingreso a “BGP/Peers” en el *router* AS200

Clic en “+”, como se observa en la Figura 3.172 y modificar los siguientes parámetros:

- *Remote address*: dirección IP del enlace con el otro *ROUTER* (10.10.10.2)
- *Remote AS*: # del sistema autónomo del *ROUTER* al que se une (300)

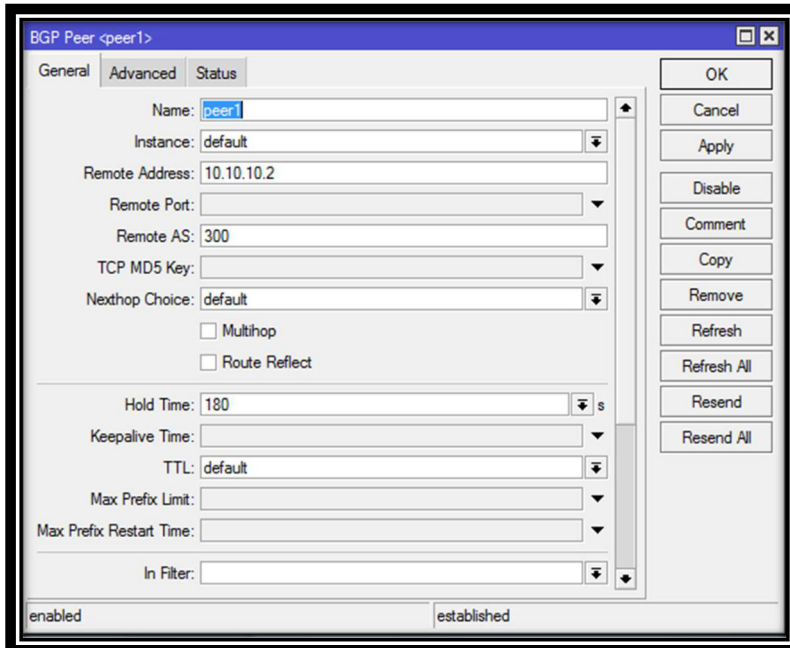


Figura 3.17272 Configuración de “Peer” para BGP en el *router* AS200

En la pestaña “Networks” agregar la dirección de red a la que el *router* se conecta, como se muestra en las Figura 3.173 y Figura 3.174.

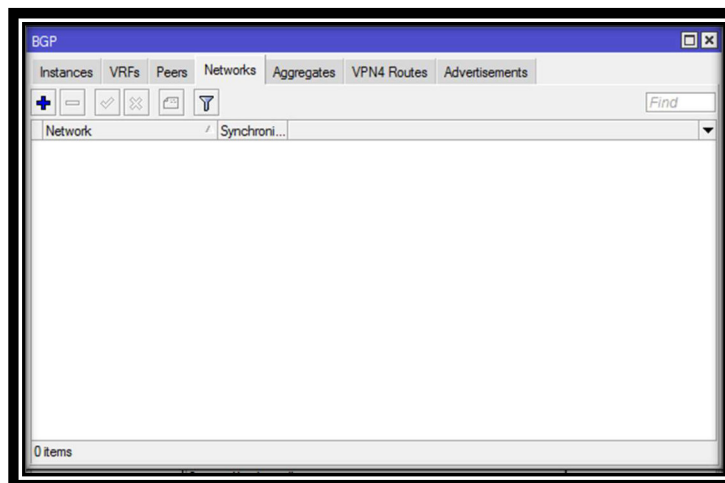


Figura 3.17373 Ingreso a la pestaña “BGP/Networks” en el *router* AS200

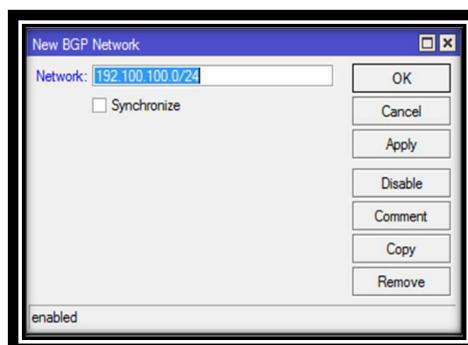


Figura 3.17474 Ingreso de la dirección IP de la red a que se conecta el *router* AS200

Repetir el procedimiento antes expuesto para los demás *routers*. Como se observan desde la Figura 3.175 a la Figura 3.187.

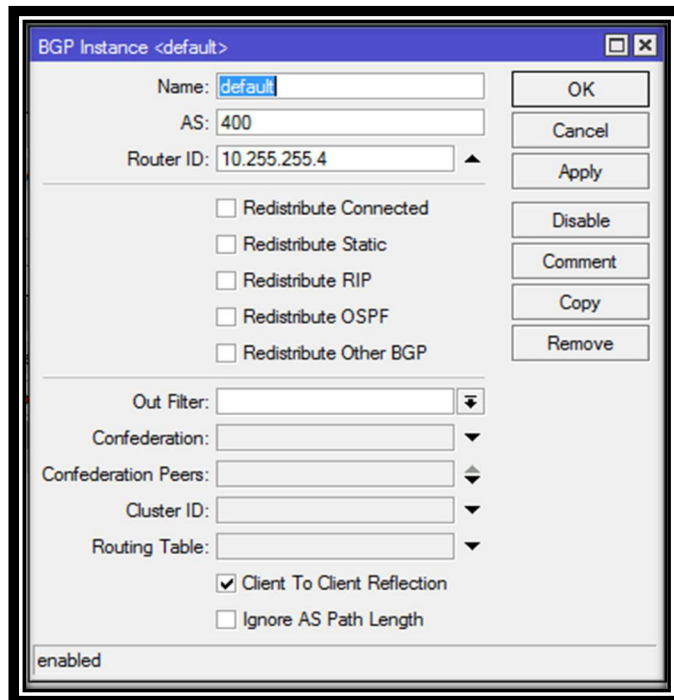


Figura 3.17575 Configuración de la dirección IP usada por BGP del *router* AS400

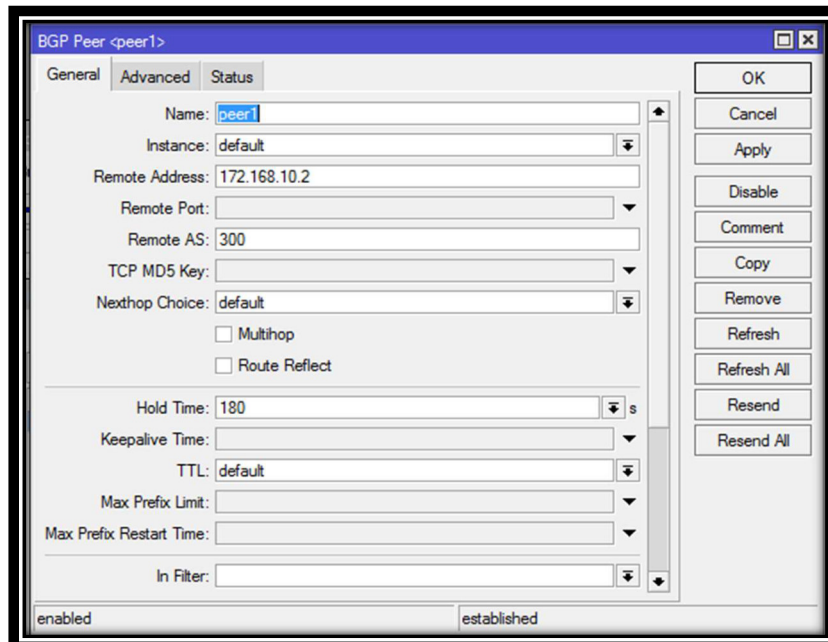


Figura 3.1766 Configuración de "Peer" para BGP en el *router* AS400

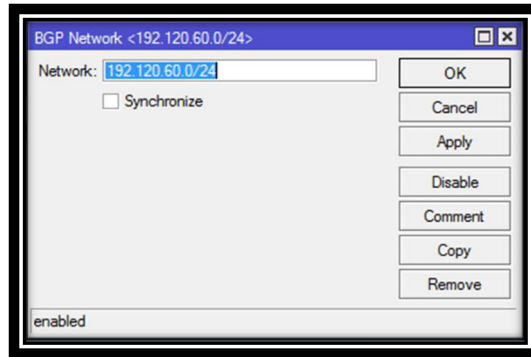


Figura 3.1777 Ingreso de la dirección IP de la red a que se conecta el *router* AS400 en "BGP Network"

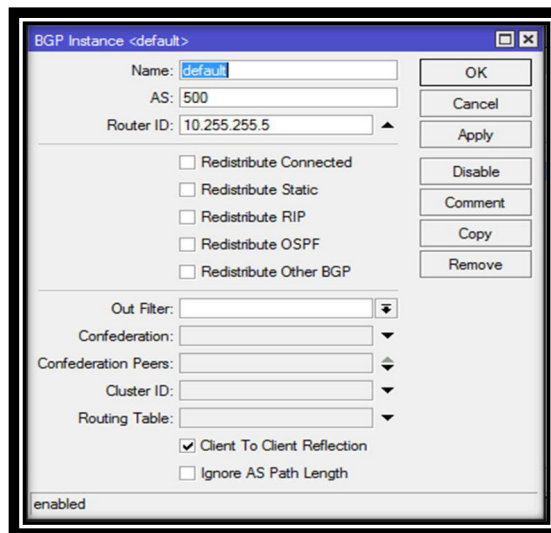


Figura 3.1788 Configuración de la dirección IP usada por BGP del *router* AS500

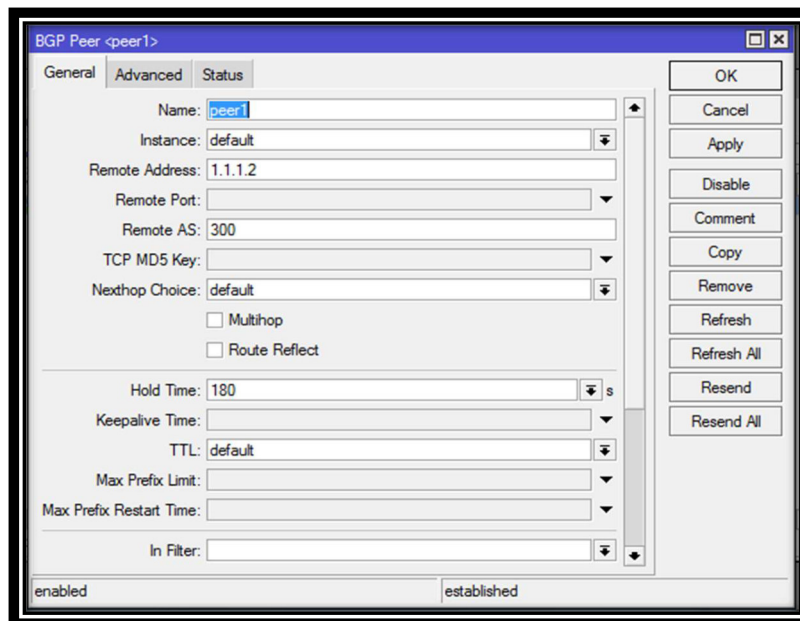


Figura 3.1799 Configuración de "Peer" para BGP en el *router* AS500

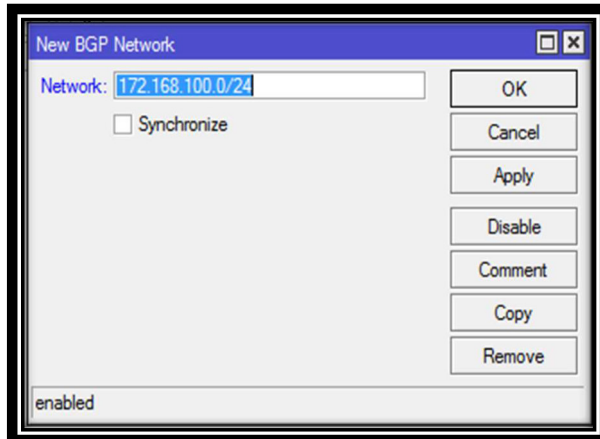


Figura 3.18080 Ingreso de la dirección IP de la red a la que se conecta el *router* AS500

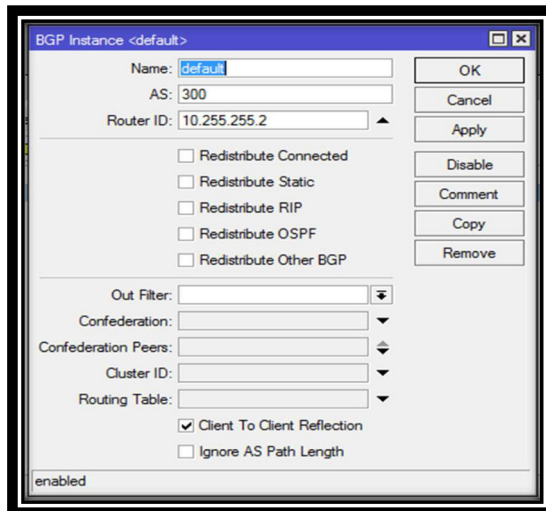


Figura 3.1811 Configuración de "Peer" para BGP en el *router* AS300 "nuestra red"

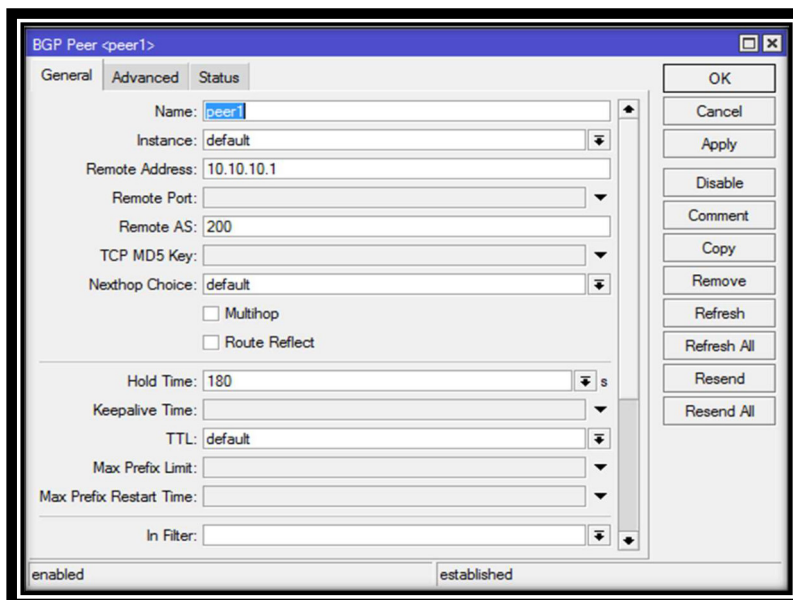


Figura 3.18282 Vista general de "Peer1" que une el AS300 con el AS200

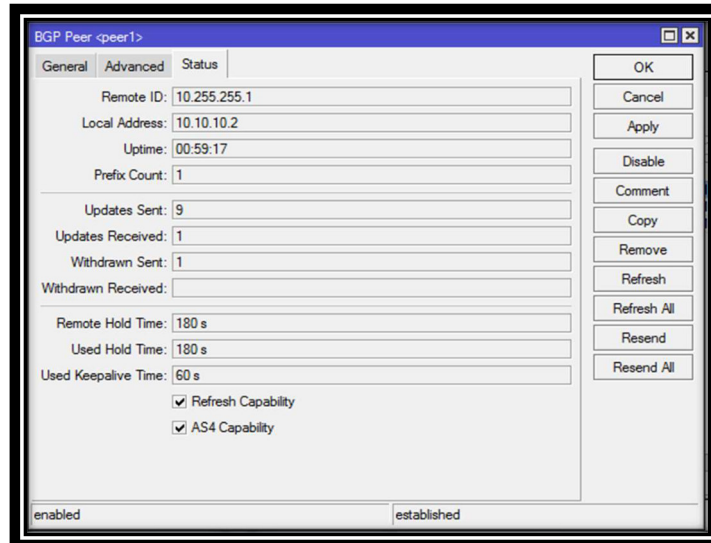


Figura 3.18383 Estado de la interfaz "Peer1" que une el AS300 con el AS200

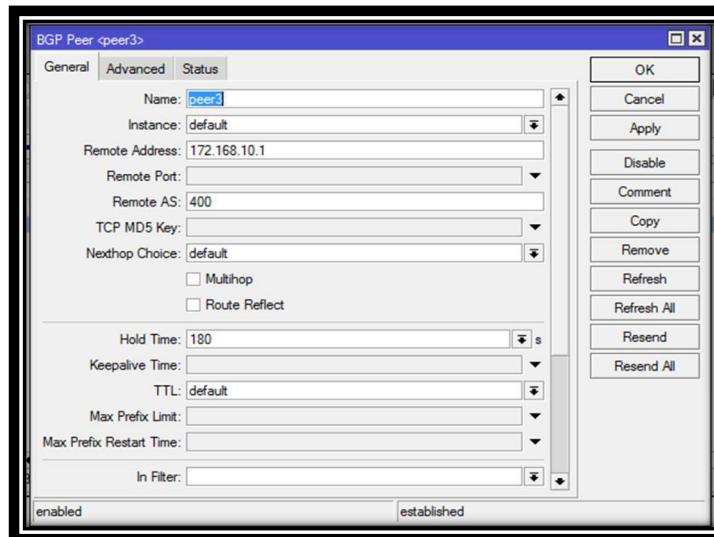


Figura 3.18484 Vista general de "Peer1" que une el AS300 con el AS400

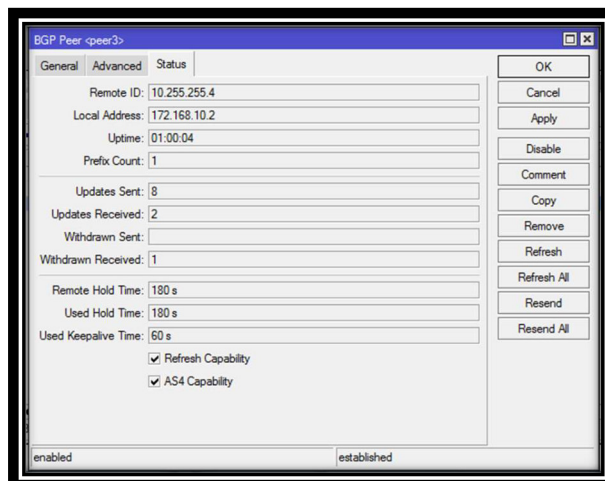


Figura 3.18585 Estado de la interfaz "Peer1" que une el AS300 con el AS400

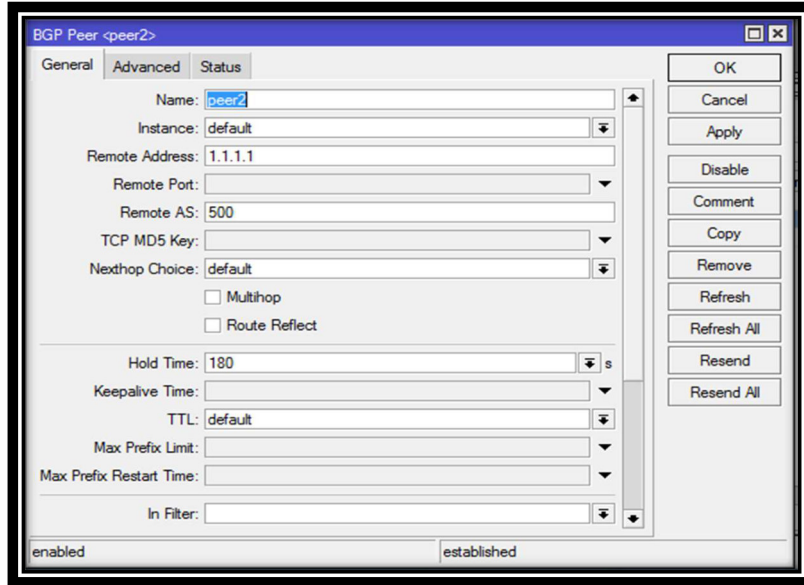


Figura 3.18686 Vista general de "Peer1" que une el AS300 con el AS500

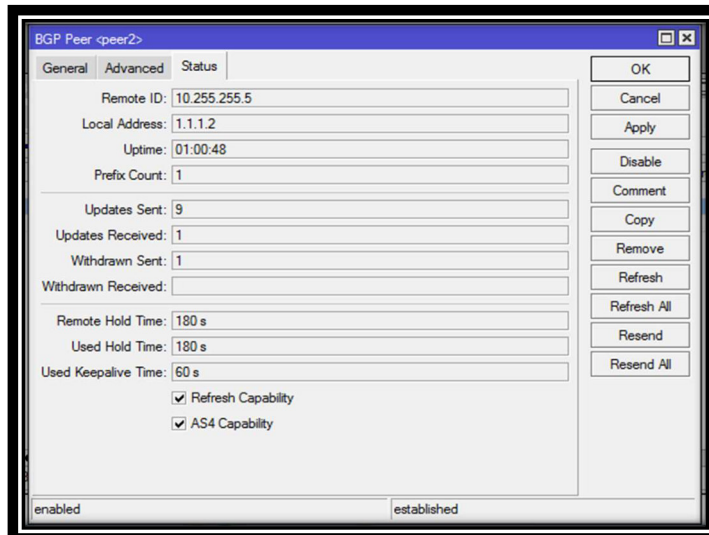


Figura 3.18787 Vista general de "Peer1" que une el AS300 con el AS500

Adicional en *Network* añadir la dirección IP de red perteneciente a "nuestra red", con la finalidad de compartirla mediante el protocolo BGP, ver Figura 3.188.

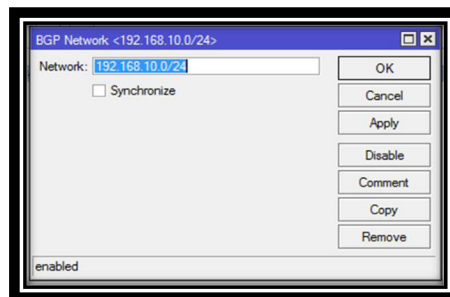


Figura 3.18888 Ingreso de la dirección de la red a que se conecta el *router* AS400 en "BGP *Network*"

Verificar Tabla de enrutamiento de cada *router*, como se muestra en la Figura 3.189 a la Figura 3.192. Se tiene las siguientes siglas:

DAC que significa:

(D) Ruta Dinámica

(A) Activo

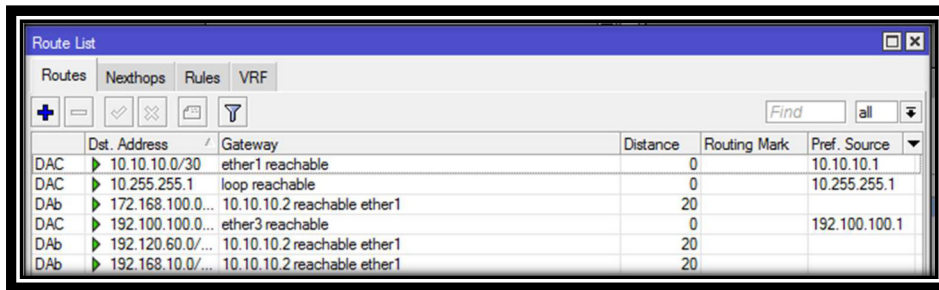
(C) Conectada

DAb que significa:

(D) Ruta Dinámica

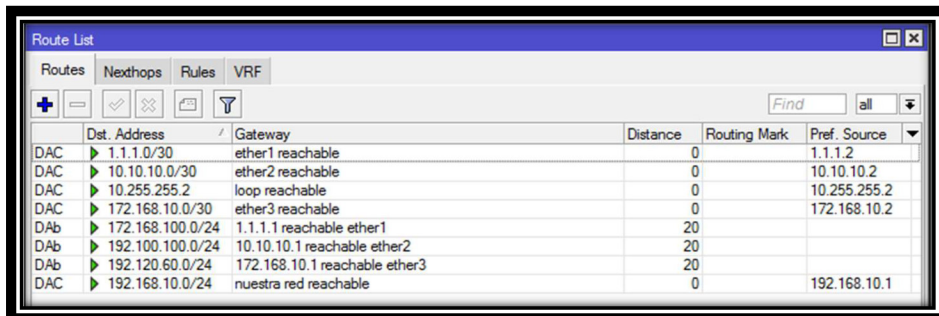
(A) Activo

(b) Aprendida por BGP



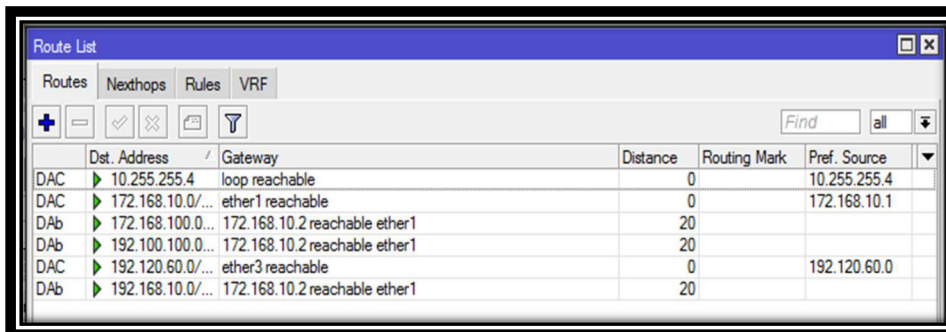
	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAC	10.10.10.0/30	ether1 reachable	0		10.10.10.1
DAC	10.255.255.1	loop reachable	0		10.255.255.1
DAb	172.168.100.0/24	10.10.10.2 reachable ether1	20		
DAC	192.100.100.0/24	ether3 reachable	0		192.100.100.1
DAb	192.120.60.0/24	10.10.10.2 reachable ether1	20		
DAb	192.168.10.0/24	10.10.10.2 reachable ether1	20		

Figura 3.189 Tabla de rutas aprendidas por el *router* AS200



	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAC	1.1.1.0/30	ether1 reachable	0		1.1.1.2
DAC	10.10.10.0/30	ether2 reachable	0		10.10.10.2
DAC	10.255.255.2	loop reachable	0		10.255.255.2
DAC	172.168.10.0/30	ether3 reachable	0		172.168.10.2
DAb	172.168.100.0/24	1.1.1.1 reachable ether1	20		
DAb	192.100.100.0/24	10.10.10.1 reachable ether2	20		
DAb	192.120.60.0/24	172.168.10.1 reachable ether3	20		
DAC	192.168.10.0/24	nuestra red reachable	0		192.168.10.1

Figura 3.1900 Tabla de rutas aprendidas por el *router* AS300



	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAC	10.255.255.4	loop reachable	0		10.255.255.4
DAC	172.168.10.0/24	ether1 reachable	0		172.168.10.1
DAb	172.168.100.0/24	172.168.10.2 reachable ether1	20		
DAb	192.100.100.0/24	172.168.10.2 reachable ether1	20		
DAC	192.120.60.0/24	ether3 reachable	0		192.120.60.0
DAb	192.168.10.0/24	172.168.10.2 reachable ether1	20		

Figura 3.1911 Tabla de rutas aprendidas por el *router* AS400

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAC	1.1.1.0/30	ether1 reachable	0		1.1.1.1
DAC	10.255.255.5	loop reachable	0		10.255.255.5
DAC	172.168.100.0...	ether3 reachable	0		172.168.100.0
DAb	192.100.100.0...	1.1.1.2 reachable ether1	20		
DAb	192.120.60.0/...	1.1.1.2 reachable ether1	20		
DAb	192.168.10.0/...	1.1.1.2 reachable ether1	20		

Figura 3.1922 Tabla de rutas aprendidas por el *router* AS500

Paso 8: asignar direcciones IP a las máquinas VPCS

Doble clic en la VPCS: Escribir ip “dirección IP/máscara” “Gateway”, como se observa desde la Figura 3.193 a la Figura 3.195.

```
PC2> ip 192.100.100.2/24 192.100.100.1
Checking for duplicate address...
PC1 : 192.100.100.2 255.255.255.0 gateway 192.100.100.1
```

Figura 3.1933 Asignación de una dirección IP a la PC2 que se conecta al *router* AS200

```
PC1> ip 192.120.60.2/24 192.120.60.1
Checking for duplicate address...
PC1 : 192.120.60.2 255.255.255.0 gateway 192.120.60.1
```

Figura 3.1944 Asignación de una dirección IP a la PC1 que se conecta al *router* AS400

```
PC3> ip 172.168.100.2/24 172.168.100.1
Checking for duplicate address...
PC1 : 172.168.100.2 255.255.255.0 gateway 172.168.100.1
```

Figura 3.1955 Asignación de una dirección IP a la PC3 que se conecta al *router* AS500

Paso 9: ping entre LANs de la topología para verificar la conectividad entre máquinas VPCS

Escribir: ping “dirección IP a la que se quiere hacer ping”, como se muestra desde la Figura 3.196 a la Figura 3.198.

```
PC2> ping 192.168.10.1
84 bytes from 192.168.10.1 icmp_seq=1 ttl=63 time=1.000 ms
84 bytes from 192.168.10.1 icmp_seq=2 ttl=63 time=2.001 ms
84 bytes from 192.168.10.1 icmp_seq=3 ttl=63 time=1.500 ms
84 bytes from 192.168.10.1 icmp_seq=4 ttl=63 time=1.500 ms
84 bytes from 192.168.10.1 icmp_seq=5 ttl=63 time=1.500 ms
```

Figura 3.1966 Ping desde la PC2 hacia la dirección IP 192.168.10.1



```
PC1> ping 192.168.10.1
84 bytes from 192.168.10.1 icmp_seq=1 ttl=63 time=1.500 ms
84 bytes from 192.168.10.1 icmp_seq=2 ttl=63 time=1.501 ms
84 bytes from 192.168.10.1 icmp_seq=3 ttl=63 time=2.000 ms
84 bytes from 192.168.10.1 icmp_seq=4 ttl=63 time=1.000 ms
84 bytes from 192.168.10.1 icmp_seq=5 ttl=63 time=1.000 ms
```

Figura 3.1977 Ping desde la PC1 hacia la dirección IP 192.168.10.1

```
PC3> ping 192.168.10.1
84 bytes from 192.168.10.1 icmp_seq=1 ttl=63 time=1.500 ms
84 bytes from 192.168.10.1 icmp_seq=2 ttl=63 time=1.500 ms
84 bytes from 192.168.10.1 icmp_seq=3 ttl=63 time=1.501 ms
84 bytes from 192.168.10.1 icmp_seq=4 ttl=63 time=1.500 ms
84 bytes from 192.168.10.1 icmp_seq=5 ttl=63 time=3.000 ms
```

Figura 3.1988 *Ping* desde la PC3 hacia la dirección IP 192.168.10.1

5. RECOMENDACIONES:

- Se debe tener en cuenta las direcciones IP asignadas a la interfaz *bridge* y el sistema autónomo al que pertenece cada *router*, para la compartición de la información mediante la interfaz que los une.
- Para cualquier cambio a realizarse en la configuración de los adaptadores de red de los *routers* simulados, ya sea en GNS o *VirtualBox*, primero se debe pausar el programa presionando el ícono  (pausa), sino GNS3 no permitirá efectuar dichos cambios mientras está corriendo o se presentará un error en el programa que no permitirá acceder a la configuración de los equipos mediante *Winbox*. Una vez efectuadas las modificaciones correspondientes se puede presionar  (iniciar) para continuar con la práctica.



ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

HOJA GUÍA

PRÁCTICA 5

1. **TEMA:** Red Privada *Virtual* (VPN) con protocolo PPTP
2. **OBJETIVO:**
Familiarizarse con el funcionamiento del protocolo PPTP
3. **DIAGRAMA DE CONEXIONES:**
Armar la siguiente topología:

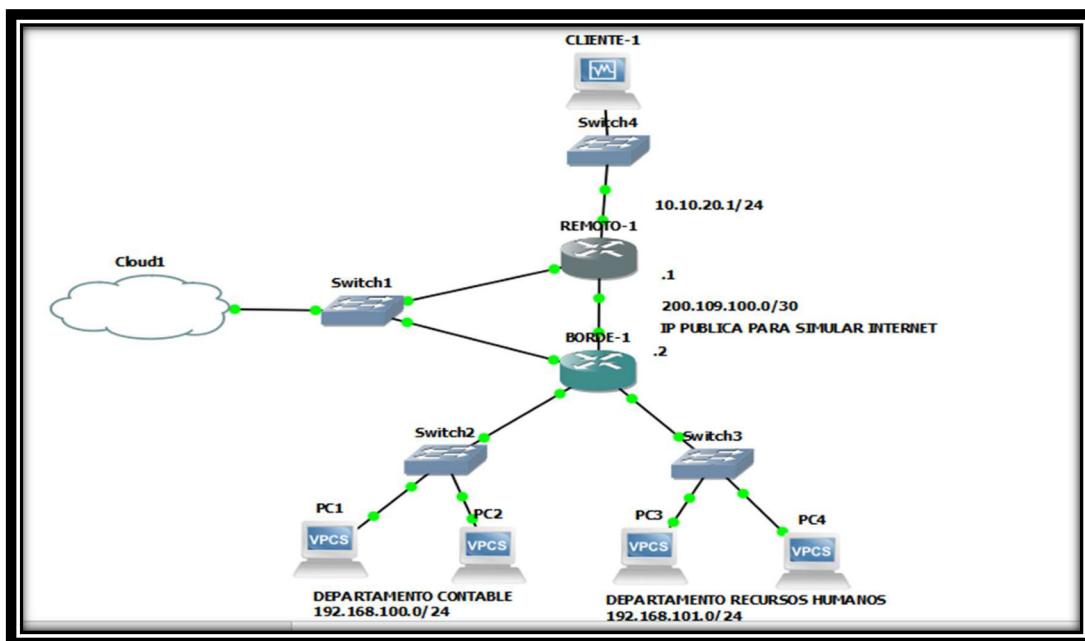


Figura 3.199 Diagrama de conexiones práctica 5

4. DESARROLLO DE LA PRÁCTICA:

NOTA: tiempo estimado para realizar la presente práctica de laboratorio es de una hora. Se recomienda que el estudiante tenga creado en *VirtualBox*, vinculado con *GNS3* y configurado en la interfaz *Winbox* 2 máquinas virtuales para realizar la práctica, adicional se debe tener creado una interfaz de *loopback* y descargado la *ISO* de *Microsoft Windows*.

VIRTUALBOX

Paso 1: crear una máquina virtual con el sistema operativo de *Windows 7 (32 bits)* y 2 *router*

Seleccionar “Nueva” para crear la máquina virtual. Y configurar los siguientes parámetros, ver Figura 3.200:

- Nombre: “CLIENTE”
- Tipo: *Microsoft Windows*
- Versión: *Windows 7 (32 bits)*
- Escoger: “Crear un disco duro virtual ahora”

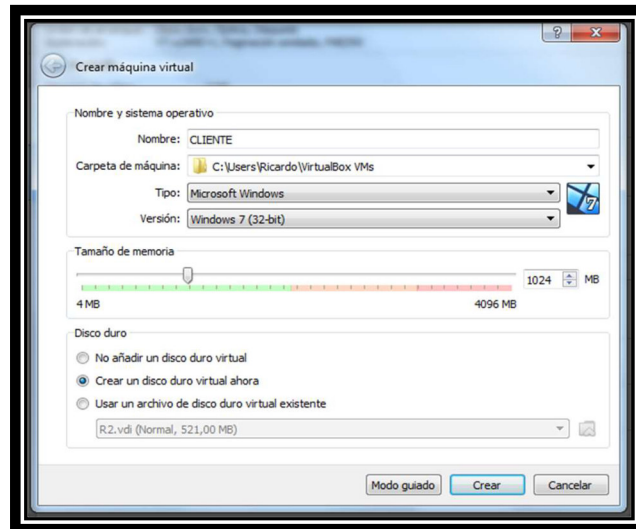


Figura 3.2000 Pestaña “Crear máquina virtual” de *VirtualBox*

Escoger “VDI” y “Reservado dinámicamente”, ver Figura 3.201.

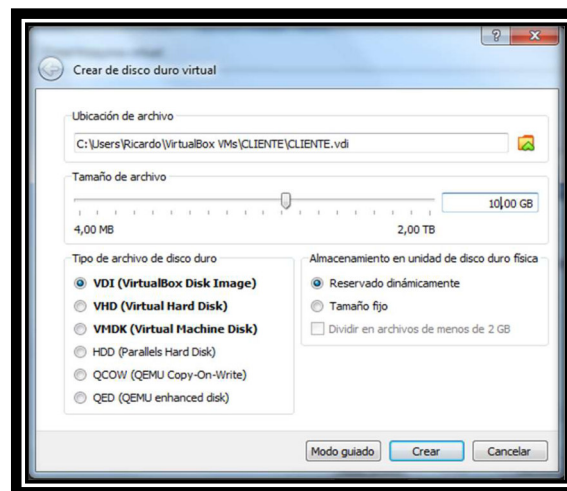


Figura 3.2011 Pestaña “Crear disco duro virtual” de *VirtualBox*

Se observa las 3 máquinas virtuales creadas en la interfaz de *VirtualBox*, ver Figura 3.202.

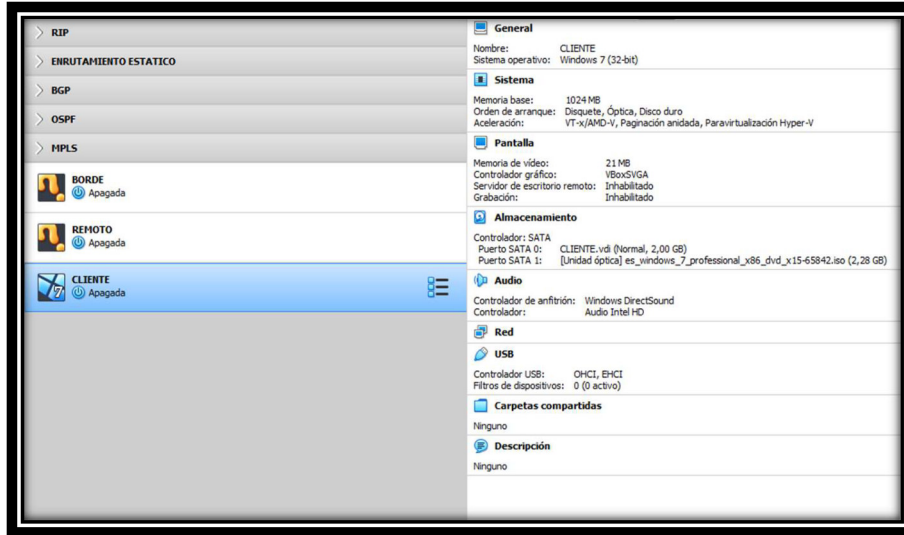


Figura 3.2022 Creación de la máquina virtual de *Windows 7* llamada "Cliente"

Iniciar la máquina virtual creada y escoger la *ISO* de *Windows 7* previamente descargada. Iniciar y continuar, como se muestra en la Figura 3.203.

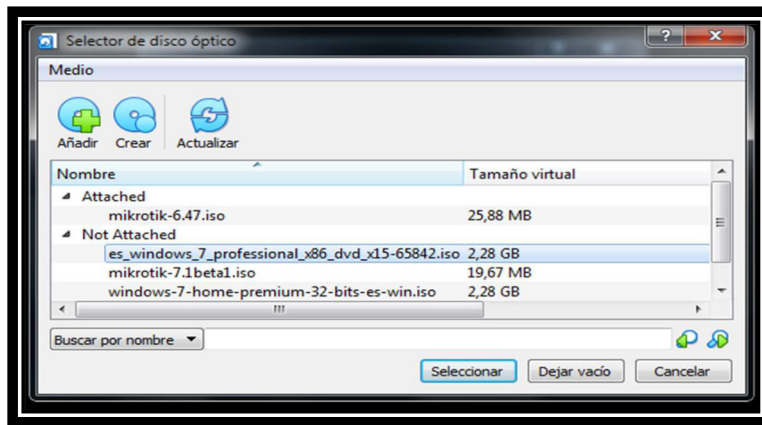


Figura 3.2033 Carga de la imagen con el sistema operativo *Windows 7*.

Escoger idioma del sistema operativo para continuar con la instalación, aceptar términos y condiciones de la licencia, escoger el tipo de Instalación y seleccionar el destino de instalación, se usará el disco virtual asignado, ver Figura 3.204.

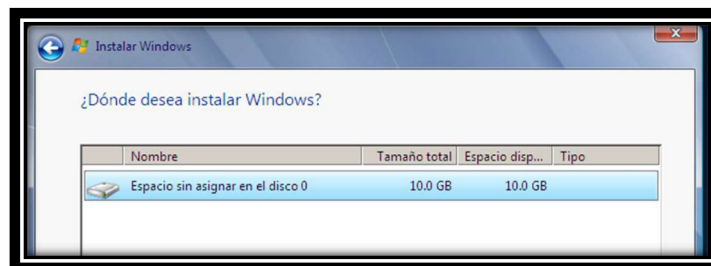


Figura 3.2044 Espacio asignado para la máquina virtual.

Terminar la instalación colocar usuario, nombre del equipo y contraseña y actualizar: Fecha, Hora y Tipo de red.

Una vez realizado el diagrama de red correspondiente y todas las configuraciones previas. Se procede con la configuración de direcciones IP que debe conocer cada uno de los *routers*, tomando en cuenta el puerto de conexión y cada dirección de red a la que desea llegar, como se puede observar desde la Figura 3.205 y Figura 3.206.

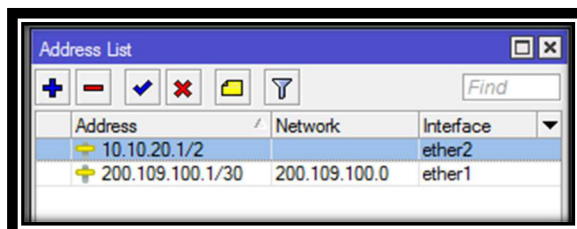


Figura 3.2055 Lista de direcciones IP del *router* REMOTO

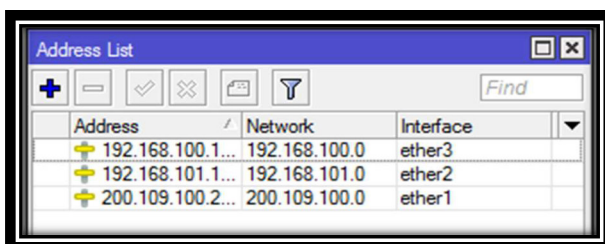


Figura 3.2066 Lista de direcciones IP del *router* BORDE

Paso 2: configurar una ruta por defecto

En la pestaña "IP" opción "*Routes*" seleccionar "+" para crear una nueva ruta. Se ocupa la dirección del *Gateway* del *router* BORDE, como se muestra desde la Figura 3.207 y Figura 3.208.

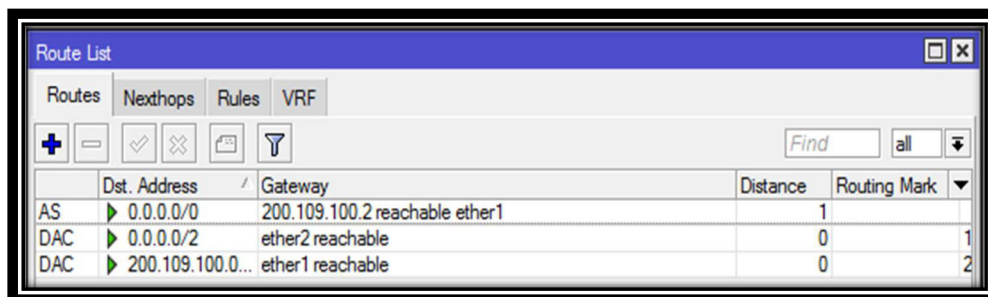


Figura 3.2077 Lista de rutas aprendidas en el *router* REMOTO

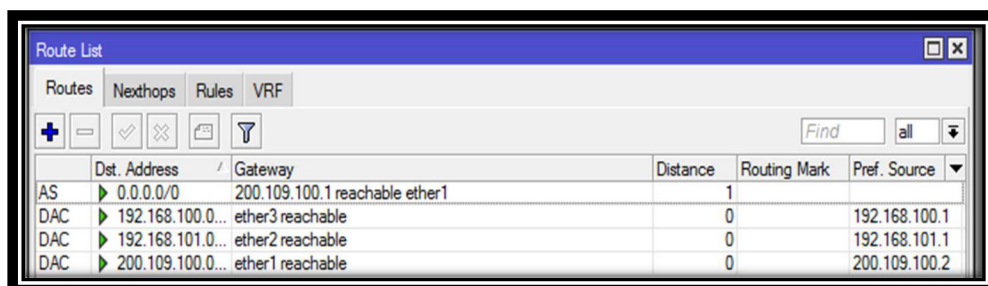


Figura 3.2088 Lista de rutas que ha aprendido el *router* BORDE

Paso 3: asignar un *Pool* de direcciones IP para el funcionamiento del protocolo PPTP

En la pestaña “IP” opción “*Pool*” seleccionar “+” para crear un nuevo *Pool*, como se observa en la Figura 3.209 y Figura 3.210.

- *Name*: asignar un nombre
- *Addresses*: “dirección IP de inicio”-“dirección IP final”

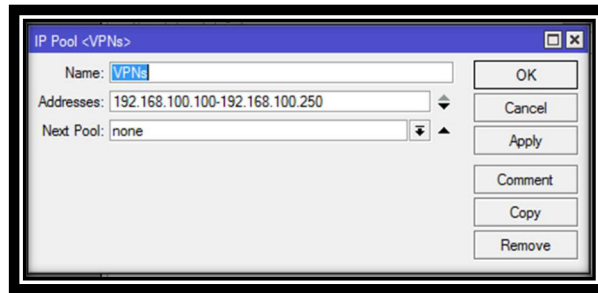


Figura 3.20909 Configuración y delimitación del *Pool* de direcciones IP

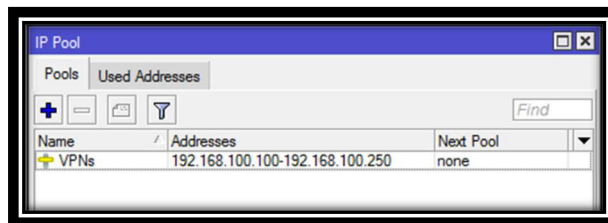


Figura 3.21010 *Pool* de direcciones IP creado

Paso 4: habilitar el protocolo PPTP en el *router* BORDE

Ingresar a la pestaña PPP seleccionar la opción “*PPTP Server*”. Habilitar “*Enable*”, “*chat*” y “*pap*”, como se muestra en la Figura 3.211 y Figura 3.212.

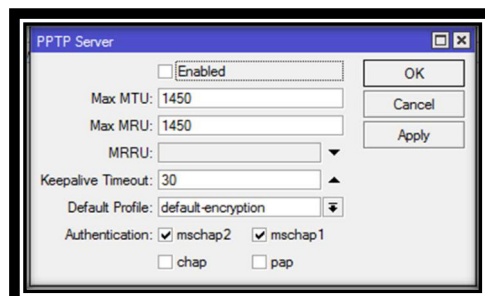


Figura 3.21111 Habilitación de “*PPTP Server*”

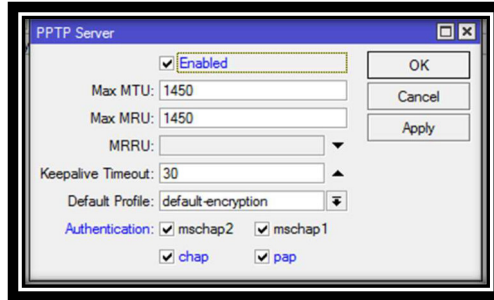


Figura 3.21212 Configuración correspondiente a “PPTP Server”

Seleccionar “+” y escoger “PPTP Server Binding”, como se muestra en la Figura 3.213.

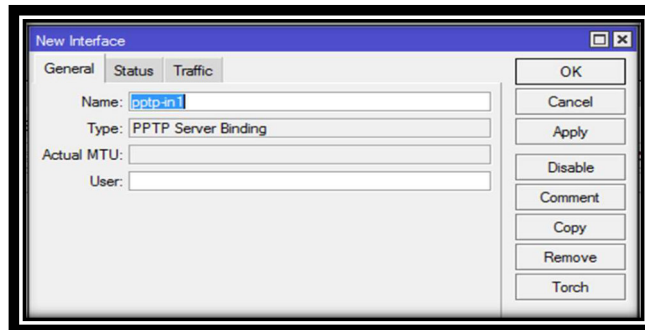


Figura 3.21313 Creación de una nueva interfaz

Editar el nombre del nuevo servidor: “pptp server”, como se muestra en la Figura 3.214 y Figura 3.215.

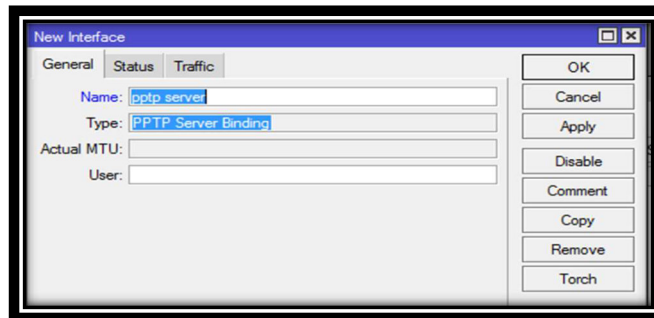


Figura 3.21414 Configuraciones realizadas para crear una interfaz

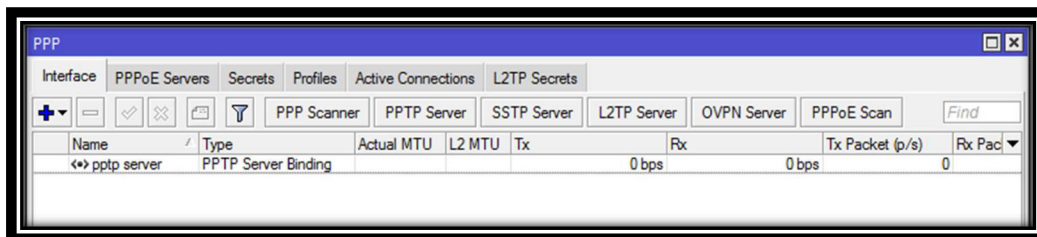


Figura 3.21515 Interfaz levantada para PPP

En la pestaña “Profiles” se crea un nuevo perfil seleccionando “+”, ver Figura 3.216.

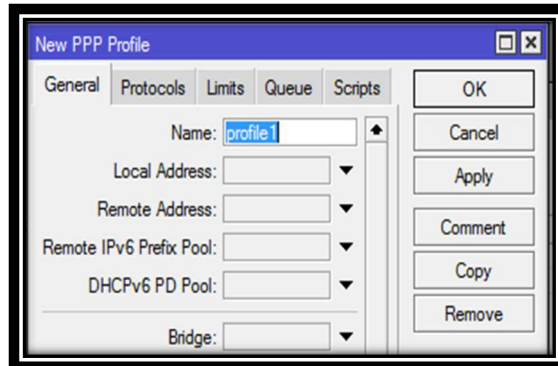


Figura 3.21616 Pestaña para agregar un nuevo perfil

Configurar el nuevo perfil, ver Figura 3.217 y Figura 3.218.

- *Local Address*: “cualquier dirección IP de la red que no esté dentro del rango del *Pool* de direcciones IP creado”.
- *Remote Address*: “VPNs” corresponde al *Pool* de direcciones IP creado

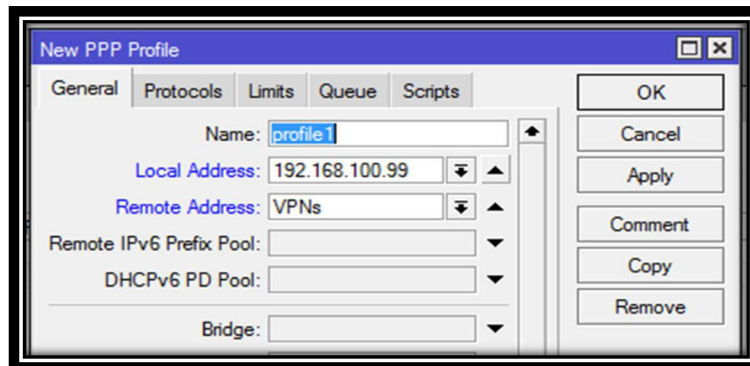


Figura 3.21717 Configuración del nuevo perfil

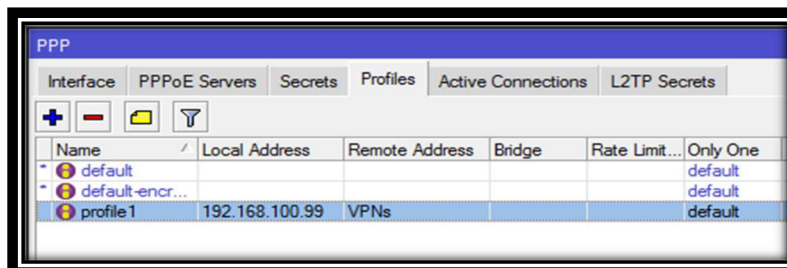


Figura 3.21818 Nuevo perfil creado para PPP

Paso 5: crear cuentas para los clientes

En la pestaña “*Secrets*” seleccionar “+” para editar la configuración del nuevo usuario, como se muestran desde la Figura 3.219 y Figura 3.220.

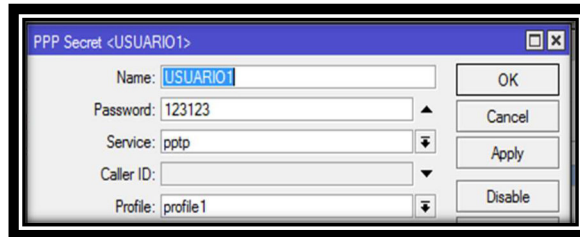


Figura 3.21919 Parámetros configurados en “Secrets”

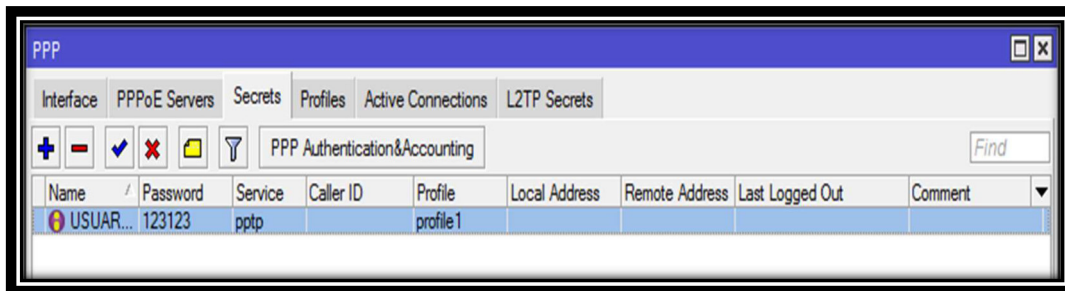


Figura 3.22020 Creación de un nuevo usuario

Paso 6: configurar las reglas de entrada y salida del *router*

En la pestaña “IP” opción “*Firewall*” seleccionar “+” para editar la configuración de la pestaña “General”, como se muestran desde la Figura 3.221 a la Figura 3.223.

- *Chain: input*
- *Protocol: 6 (tcp)*
- *Dst. Port: 1723*

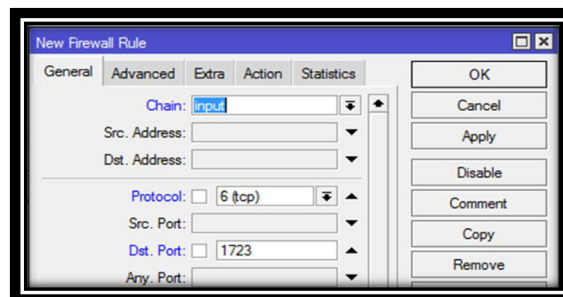


Figura 3.22121 Configuración de la regla uno

- *Chain: input*
- *Protocol: 47 (gre)*

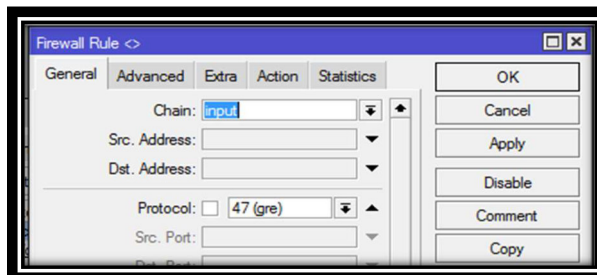


Figura 3.22222 Configuración de la regla dos

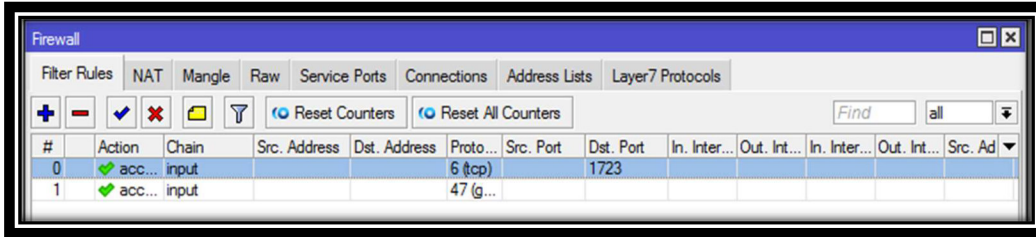


Figura 3.22323 Reglas creadas para el funcionamiento de PPTP

Paso 7: habilitar NAT en el *router* REMOTO

En la pestaña “IP” seleccionar “Firewall” y en la pestaña “NAT” seleccionar “+” para editar la configuración “General”, como se muestra en la Figura 3.224 y Figura 3.225. En la opción “Out Interface” se coloca la interfaz que se une con el *router* de BORDE.

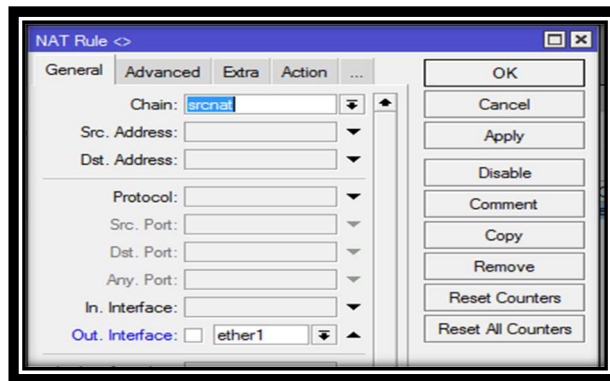


Figura 3.22424 Configuración de NAT

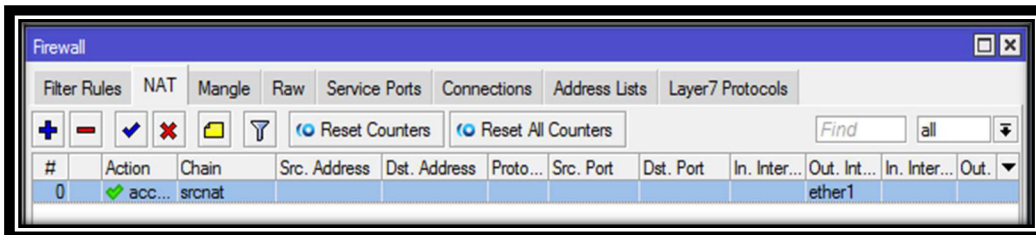


Figura 3.22525 Regla NAT creada

Paso 8: creación de una conexión de red en el cliente *Windows*

Asignar una dirección IP dentro de la red 10.10.20.0/24 con *Gateway* 10.10.20.1 (Según la topología diseñada), como se observa desde la Figura 3.226 a la Figura 3.229.

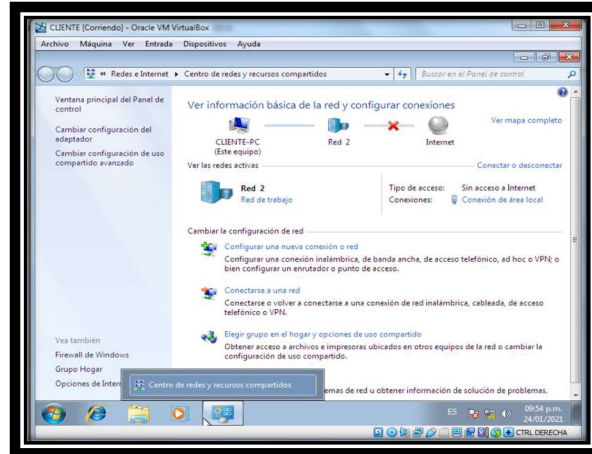


Figura 3.22626 Pantalla “Centro de redes y recursos compartidos” de Windows 7

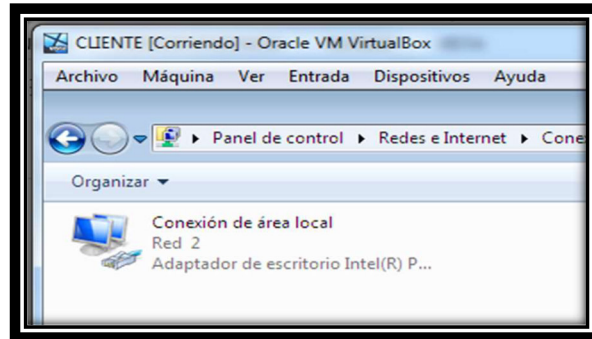


Figura 3.22727 Pantalla “Conexiones de Red”

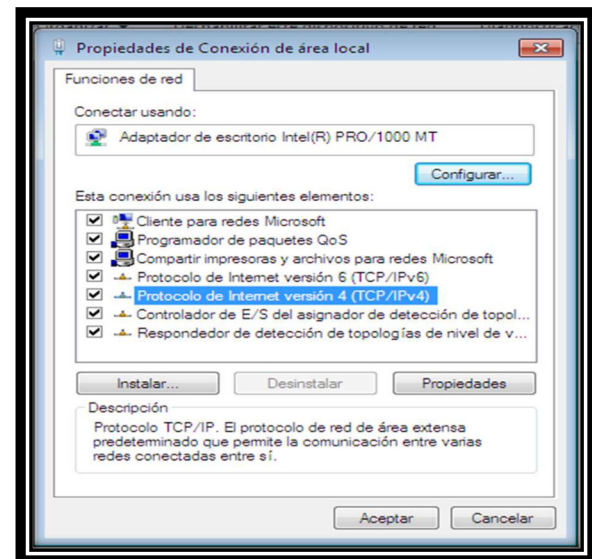


Figura 3.22828 Pestaña de “Propiedades de Conexión de área local”

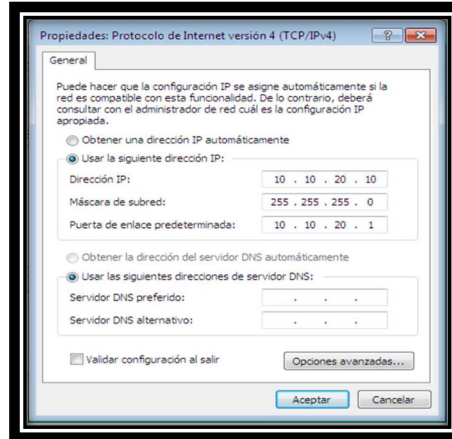


Figura 3.22929 Configuración de la dirección IP del cliente *Windows*

En el CMD se realiza la comprobación de la salida del *Gateway*, haciendo *ping* al mismo (10.10.20.1), ver Figura 3.230.

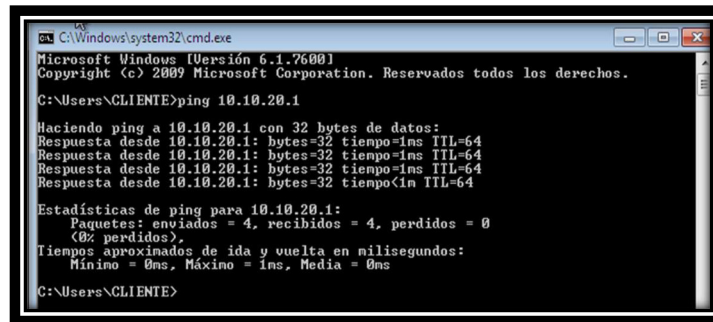


Figura 3.23030 *Ping* realizado hacia el *Gateway*

Levantar el servidor PPTP en el CLIENTE esto se lo realiza en “Centro de redes y recursos compartidos”. Seleccionar “Configurar una nueva conexión o red”, ver Figura 3.231.

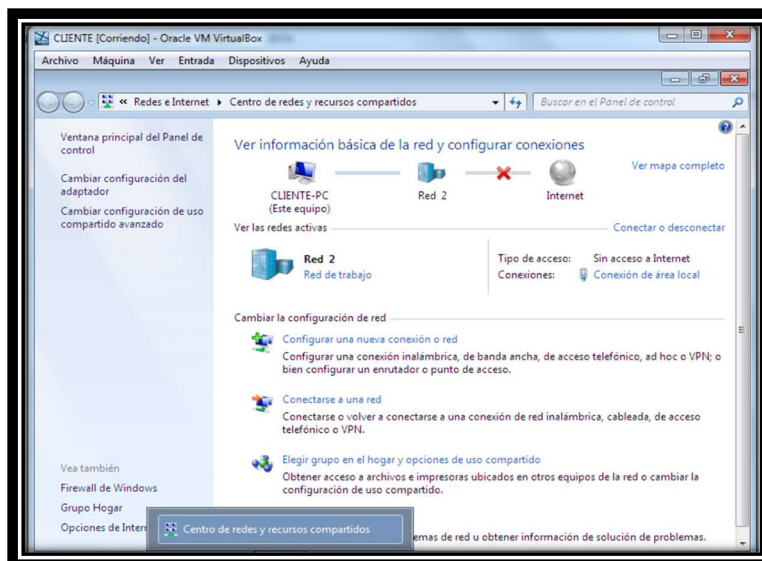


Figura 3.23131 Ingreso para la configuración del servidor PPTP al centro de redes y recursos

Conectar a un área de trabajo. Escoger “Usar mi conexión de Internet (VPN)”, como se muestra en la Figura 3.232 y Figura 3.233.

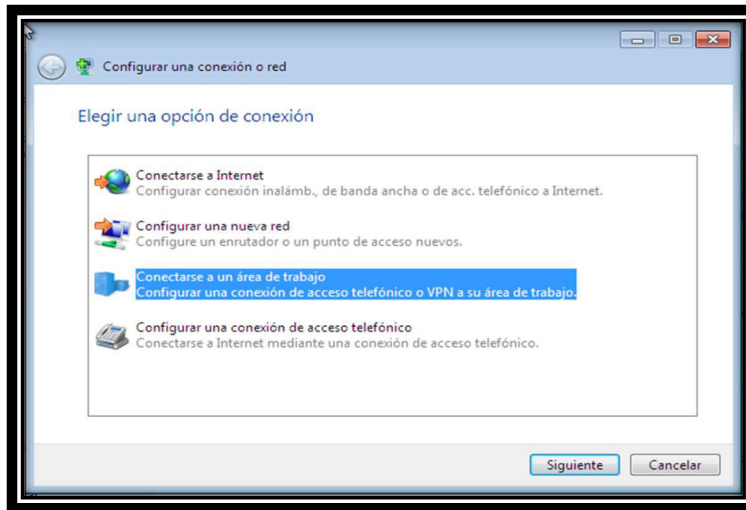


Figura 3.23232 Pestaña para configurar una nueva conexión de red

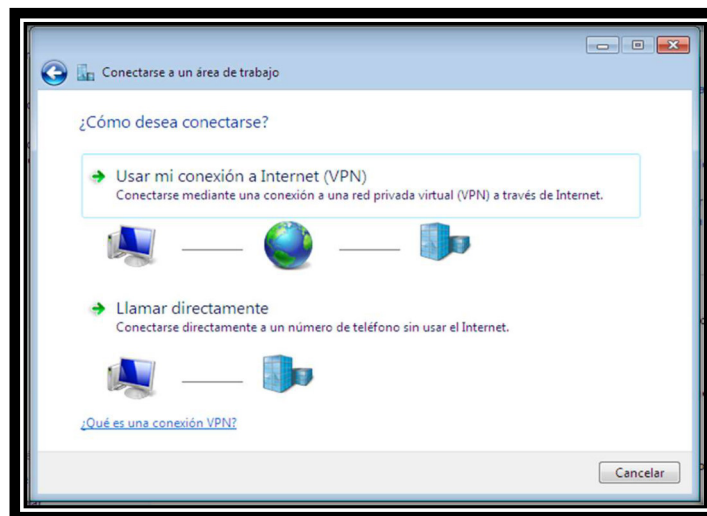


Figura 3.23333 Selección del tipo de conexión

Realizar la conexión a internet VPN, ver Figura 3.234.

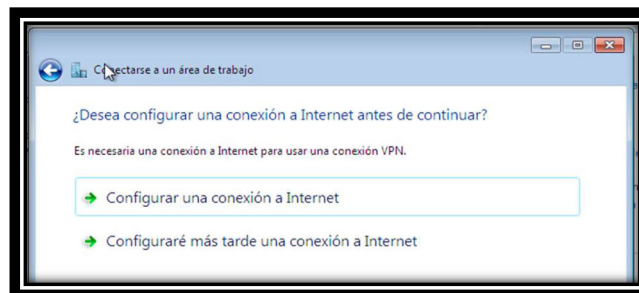


Figura 3.23434 Configuración de la conexión

En la opción “Dirección de Internet” colocar la dirección IP del *router* de BORDE, ver Figura 3.235.

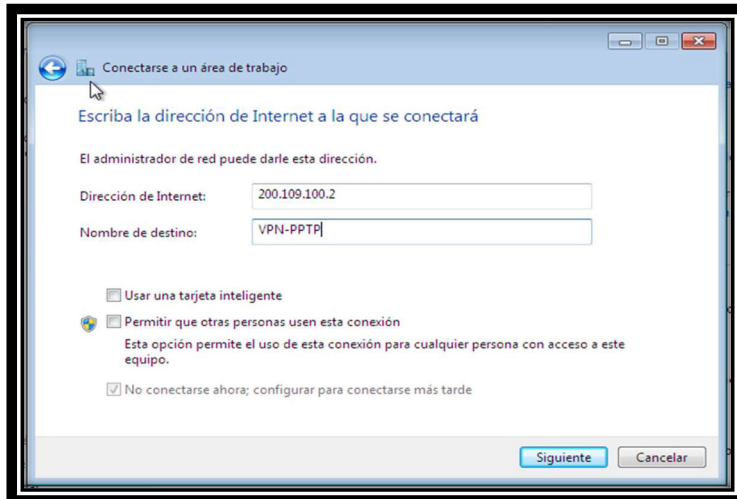


Figura 3.23535 Configuración de los parámetros del servidor PPTP en Windows

En los campos “Nombre de usuario” y “contraseña” completar:

- Nombre de usuario: USUARIO1
- Contraseña: 123123

Una vez realizado todos los cambios aparecerá en “Conexiones de red” la nueva conexión de red creada, como se muestra en la Figura 3.236.

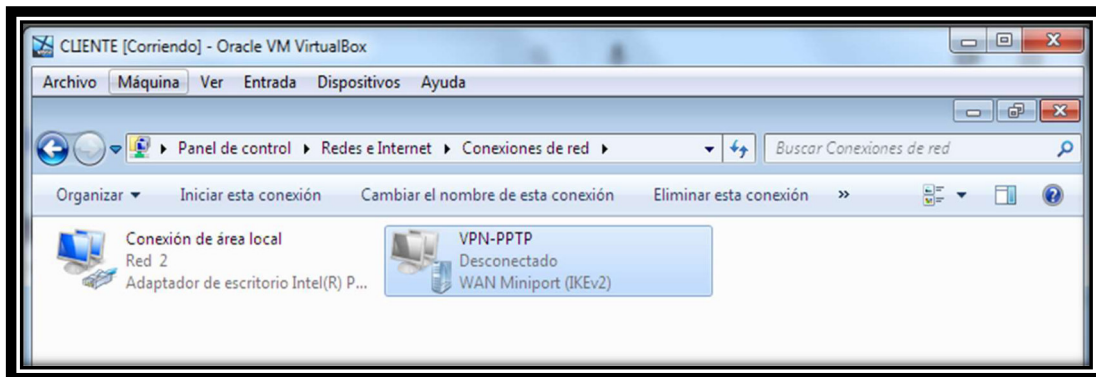


Figura 3.23636 Habilitación del adaptador de red PPTP

Ingresa a las propiedades de la nueva conexión de red, ver Figura 3.237.

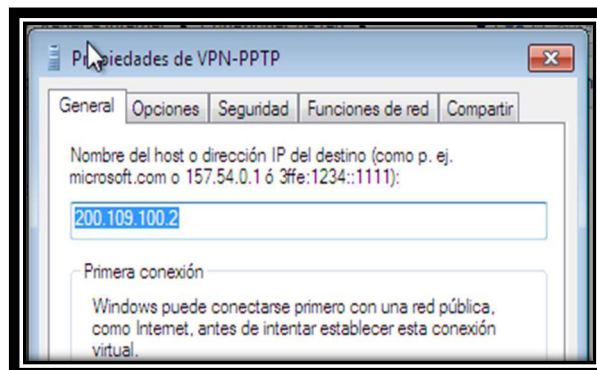


Figura 3.23737 Configuración de parámetros para PPTP

En la pestaña “Seguridad” opción “Tipo de VPN” seleccionar “*Protocolo de túnel punto a punto PPTP*”, ver Figura 3.238.

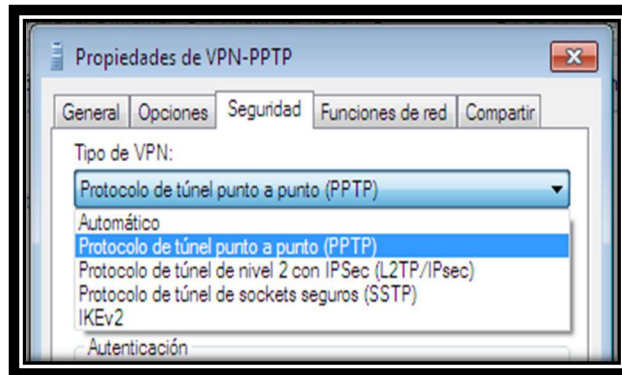


Figura 3.23838 Selección del tipo de VPN

Activar la conexión de red creada. Ver Figura 3.239.

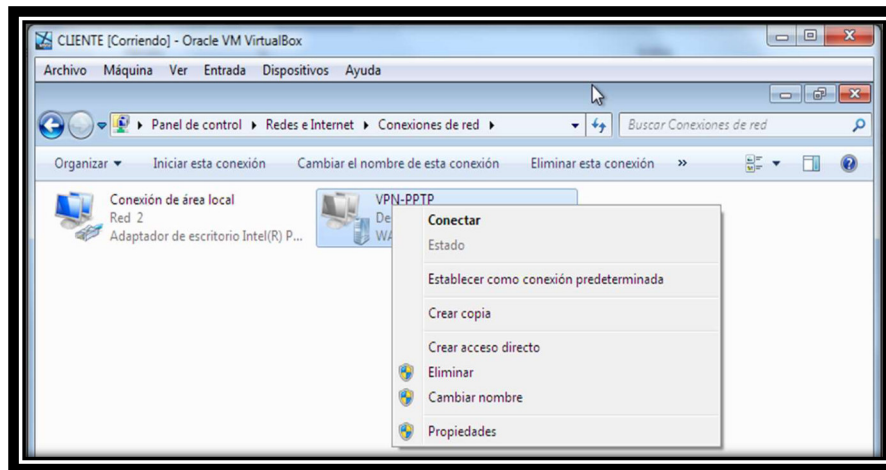


Figura 3.239 Unirse al servidor PPTP mediante el adaptador de red

Colocar la contraseña con la que se creó la nueva red, como se muestra en la Figura 3.240 y Figura 3.241.

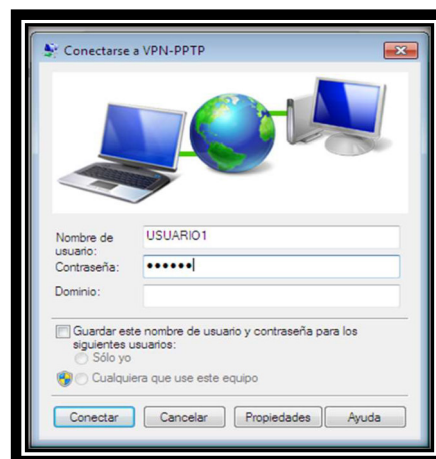


Figura 3.24040 Configuración del usuario y clave para PPTP

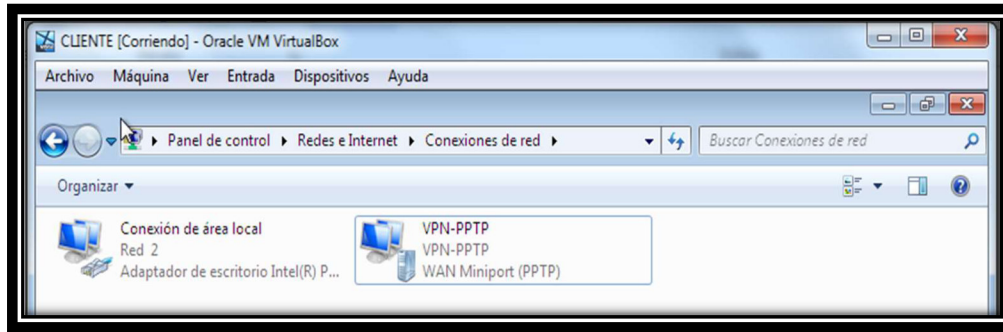


Figura 3.24141 Vista general de los adaptadores de red de *Windows*

En el CMD confirmar que la dirección IP ha sido asignada automáticamente mediante PPTP con el comando: *ipconfig /all*, ver Figura 3.242.



Figura 3.24242 Configuraciones de la máquina para los adaptadores de red, ingresando a CMD Se puede observar que ha sido asignada de manera automática la dirección IP 192.168.100.250.

Paso 9: Asignar direcciones IP a las máquinas VPCS

Doble clic en la VPCS: Escribir ip "dirección IP/máscara" "Gateway", como se muestran desde la Figura 3.243 a la Figura 3.246.



Figura 3.24343 Dirección IP asignada a la PC1 según la topología

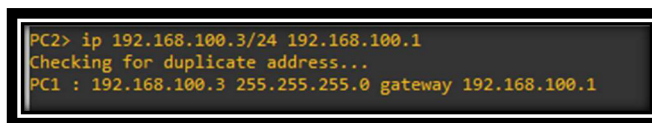


Figura 3.24444 Dirección IP asignada a la PC2 según la topología

```
PC3> ip 192.168.101.2/24 192.168.101.1
Checking for duplicate address...
PC1 : 192.168.101.2 255.255.255.0 gateway 192.168.101.1
```

Figura 3.24545 Dirección IP asignada a la PC3 según la topología

```
PC4> ip 192.168.101.3/24 192.168.101.1
Checking for duplicate address...
PC1 : 192.168.101.3 255.255.255.0 gateway 192.168.101.1
```

Figura 3.24646 Dirección IP asignada a la PC4 según la topología

Comprobar que existe conexión desde la máquina de *Windows* (CLIENTE) hasta las diferentes *VPCS*, que se encuentran ubicadas en el lado del *router* de BORDE, como se observa desde la Figura 3.247 a la Figura 3.250.

```
C:\Users\CLIENTE>ping 192.168.100.2

Haciendo ping a 192.168.100.2 con 32 bytes de datos:
Respuesta desde 192.168.100.2: bytes=32 tiempo=3ms TTL=63
Respuesta desde 192.168.100.2: bytes=32 tiempo=2ms TTL=63
Respuesta desde 192.168.100.2: bytes=32 tiempo=2ms TTL=63
Respuesta desde 192.168.100.2: bytes=32 tiempo=2ms TTL=63

Estadísticas de ping para 192.168.100.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 2ms, Máximo = 3ms, Media = 2ms
```

Figura 3.24747 Ping desde el cliente de *Windows* hacia la PC1

```
C:\Users\CLIENTE>ping 192.168.100.3

Haciendo ping a 192.168.100.3 con 32 bytes de datos:
Respuesta desde 192.168.100.3: bytes=32 tiempo=4ms TTL=63
Respuesta desde 192.168.100.3: bytes=32 tiempo=2ms TTL=63
Respuesta desde 192.168.100.3: bytes=32 tiempo=2ms TTL=63
Respuesta desde 192.168.100.3: bytes=32 tiempo=3ms TTL=63

Estadísticas de ping para 192.168.100.3:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 2ms, Máximo = 4ms, Media = 2ms
```

Figura 3.24848 Ping desde el cliente de *Windows* hacia la PC2

```
C:\Users\CLIENTE>ping 192.168.101.2

Haciendo ping a 192.168.101.2 con 32 bytes de datos:
Respuesta desde 192.168.101.2: bytes=32 tiempo=3ms TTL=63
Respuesta desde 192.168.101.2: bytes=32 tiempo=2ms TTL=63
Respuesta desde 192.168.101.2: bytes=32 tiempo=2ms TTL=63
Respuesta desde 192.168.101.2: bytes=32 tiempo=2ms TTL=63

Estadísticas de ping para 192.168.101.2:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 2ms, Máximo = 3ms, Media = 2ms
```

Figura 3.24949 Ping desde el cliente de *Windows* hacia la PC3


```

C:\Users\CLIENTE>ping 192.168.101.3
Haciendo ping a 192.168.101.3 con 32 bytes de datos:
Respuesta desde 192.168.101.3: bytes=32 tiempo=3ms TTL=63
Respuesta desde 192.168.101.3: bytes=32 tiempo=2ms TTL=63
Respuesta desde 192.168.101.3: bytes=32 tiempo=3ms TTL=63
Respuesta desde 192.168.101.3: bytes=32 tiempo=3ms TTL=63
Estadísticas de ping para 192.168.101.3:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (<0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 2ms, Máximo = 3ms, Media = 2ms

```

Figura 3.25050 Ping desde el cliente de Windows hacia la PC4

Para comprobar que la máquina Windows (CLIENTE) está realizando el enrutamiento mediante NAT, se usa el comando: *tracert* "dirección IP", ver Figura 3.251.

```

C:\Users\CLIENTE>tracert 192.168.100.2
Trazo a la dirección CLIENTE-PC [192.168.100.2]
sobre un máximo de 30 saltos:
  1    3 ms    4 ms    2 ms    192.168.100.99
  2    3 ms    2 ms    3 ms    CLIENTE-PC [192.168.100.2]
Trazo completa.
C:\Users\CLIENTE>

```

Figura 3.25151 Traceo realizado desde el cliente hacia la PC1, para comprobar que PPTP se encuentre levantado

Se observa que la dirección IP del servidor VPN 192.168.100.99. Desactivar momentáneamente el adaptador que se une con el servidor PPTP. Repetir el literal 4, ver Figura 3.252.

```

Trazo a la dirección CLIENTE-PC [192.168.100.2]
sobre un máximo de 30 saltos:
  1    <1 ms   <1 ms   <1 ms   10.10.20.1
  2    1 ms    1 ms    1 ms    200.109.100.2
  3    2 ms    2 ms    2 ms    CLIENTE-PC [192.168.100.2]
Trazo completa.



```

Figura 3.25252 Traceo realizado desde el cliente hacia la PC1, para comprobar que PPTP no se encuentra activo una vez que se desactivó el adaptador

Se observa que los saltos realizados esta vez han sido diferentes (sin tomar la ruta del servidor PPTP).

5. RECOMENDACIONES:

- Para la máquina virtual con el sistema operativo de Windows 7 (32 bits) hay que tener en cuenta los requerimientos básicos para el funcionamiento del mismo, asignar mínimo una memoria RAM de 1024 MB y espacio de disco de 10 GB.
- Tomar en cuenta que la dirección IP de la máquina CLIENTE debe pertenecer a la red que lo une con el Gateway del router REMOTO, para poderse comunicar.

- El nuevo adaptador de red PPTP debe ser configurado correctamente, para que el servidor ubicado en el *router* BORDE pueda asignar la dirección IP automáticamente al CLIENTE y este pueda comunicarse con las *VPCS*.
- Para cualquier cambio a realizarse en la configuración de los adaptadores de red de los *routers* simulados, ya sea en GNS o *VirtualBox*, primero se debe pausar el programa presionando el ícono  (pausa), sino GNS3 no permitirá efectuar dichos cambios mientras está corriendo o se presentará un error en el programa que no permitirá acceder a la configuración de los equipos mediante *Winbox*. Una vez efectuadas las modificaciones correspondientes se puede presionar  (iniciar) para continuar con la práctica.



ESCUELA POLITÉCNICA NACIONAL

ESCUELA DE FORMACIÓN DE TECNÓLOGOS

HOJA GUÍA

PRÁCTICA 6

1. **TEMA:** Implementación de red MPLS con OSPF

2. **OBJETIVO:**

Familiarizarse con la tecnología MPLS y aplicarla junto con OSPF para comprobar su funcionamiento.

3. **DIAGRAMA DE CONEXIONES:**

Armar la siguiente topología:

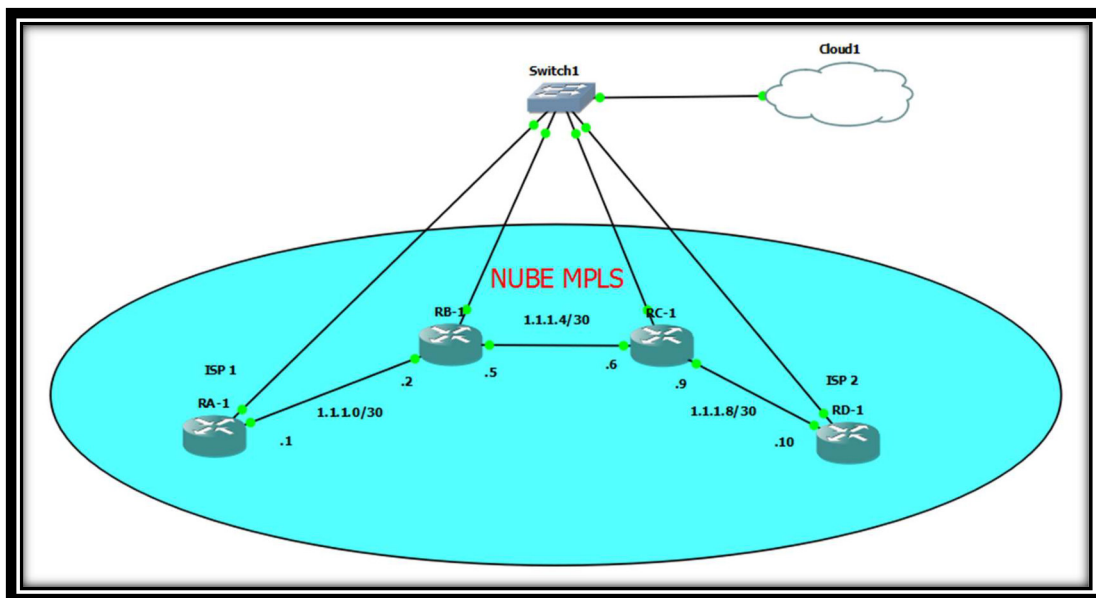


Figura 3. 253 Diagrama de conexiones práctica 6

4. **DESARROLLO DE LA PRÁCTICA:**

NOTA: tiempo estimado para realizar la presente práctica de laboratorio es de una hora.

Se recomienda que el estudiante tenga creado en *VirtualBox*, vinculado con *GNS3* y configurado en la interfaz *Winbox* 4 máquinas virtuales para realizar la práctica, adicional se debe tener creado una interfaz de *loopback*.

Una vez realizado el diagrama de red correspondiente y todas las configuraciones previas. Se procede con la configuración de direcciones IP que debe conocer cada uno de los *routers*, tomando en cuenta el puerto de conexión y cada dirección de red a conocer, como se puede observar desde la Figura 3.254 a la Figura 3.257.



Figura 3.2544 Direcciones IP aprendidas por RA

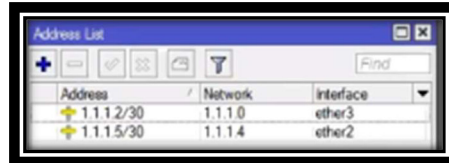


Figura 3.2555 Direcciones IP aprendidas por RB

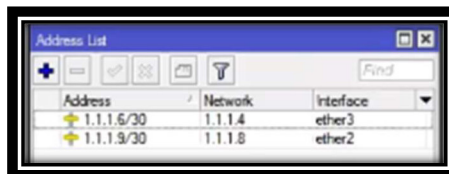


Figura 3.2566 Direcciones IP aprendidas por RC

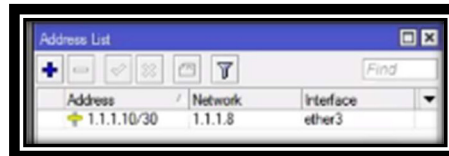


Figura 3.2577 Direcciones IP aprendidas por RD

Paso 1: configuración de OSPF

Crear una interfaz de *loopback* para los 4 *routers*, como se muestra desde la Figura 3.258 a la Figura 3.265.

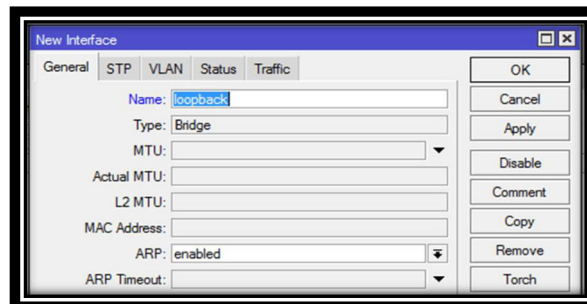


Figura 3.2588 Configuración para crear una interfaz lógica en RA

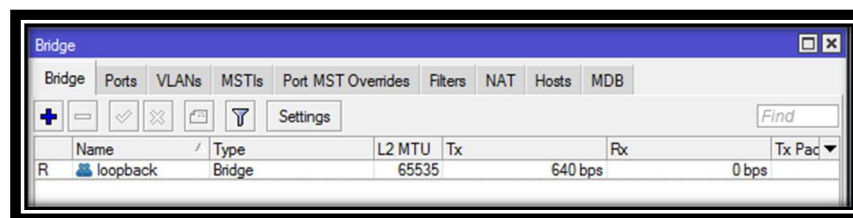


Figura 3.25959 Interfaz lógica creada en el *router* RA

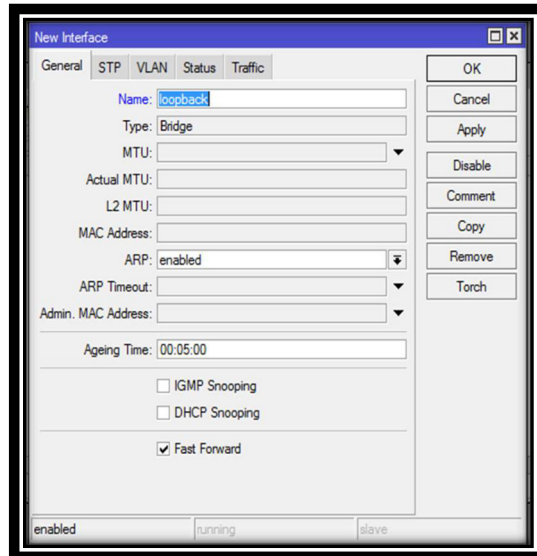


Figura 3.26060 Configuración para crear una interfaz lógica en RB

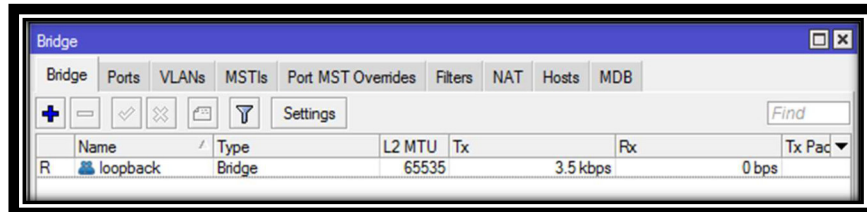


Figura 3.26161 Interfaz lógica creada en el router RB

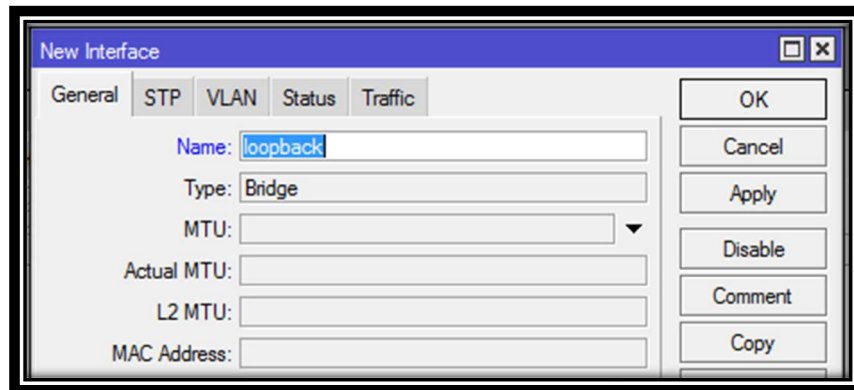


Figura 3.26262 Configuración para crear una interfaz lógica en RC

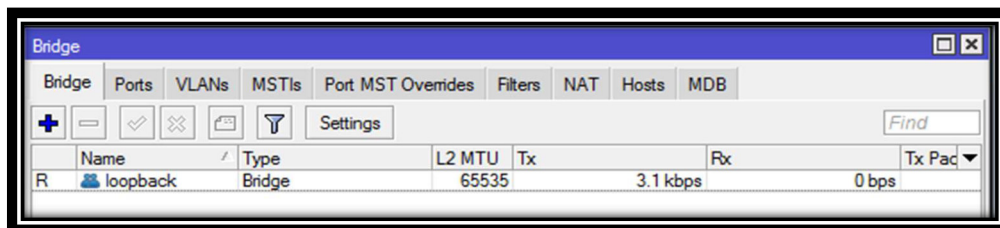


Figura 3.2633 Interfaz lógica creada en el router RC

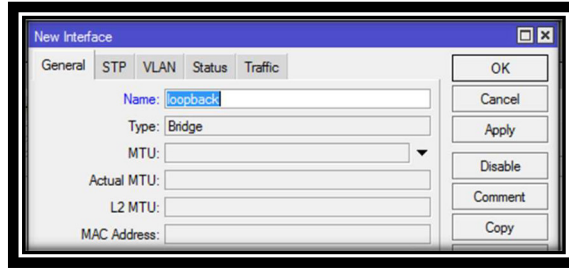


Figura 3.26464 Configuración para crear una interfaz lógica en RD

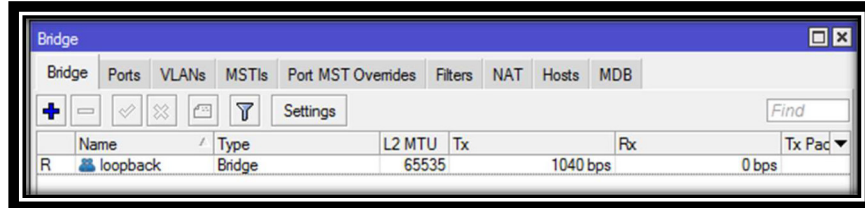


Figura 3.26565 Interfaz lógica creada en el router RD

Asignar una dirección IP para la interfaz creada, como se observa desde la Figura 3.266 a la Figura 3.269.

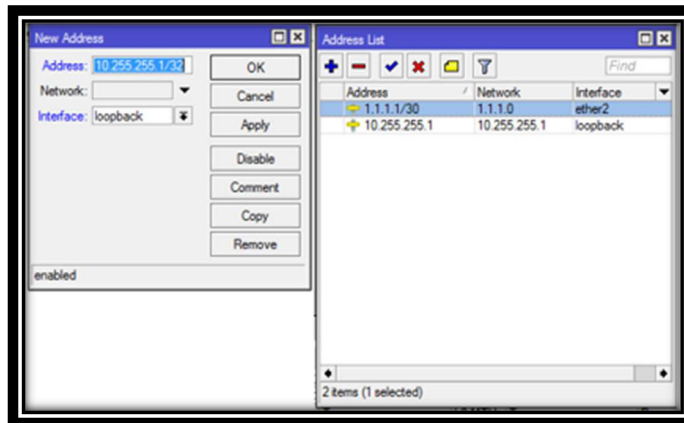


Figura 3.26666 Asignación de una dirección IP a la interfaz creada para el router RA

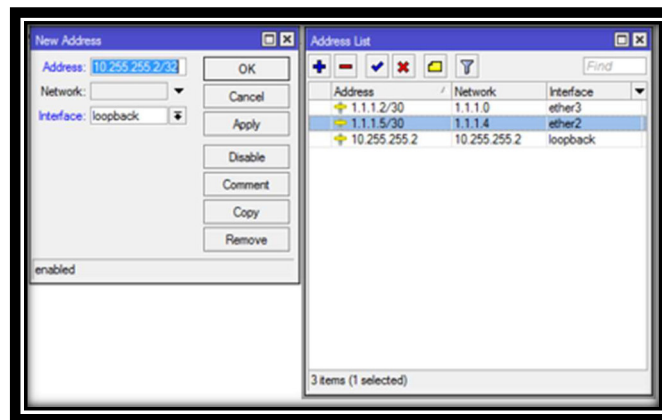


Figura 3.26767 Asignación de una dirección IP a la interfaz creada para el router RB

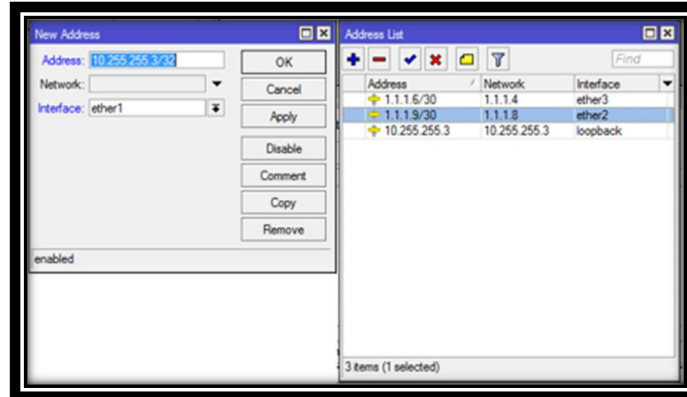


Figura 3.26868 Asignación de una dirección IP a la interfaz creada para el *router* RC

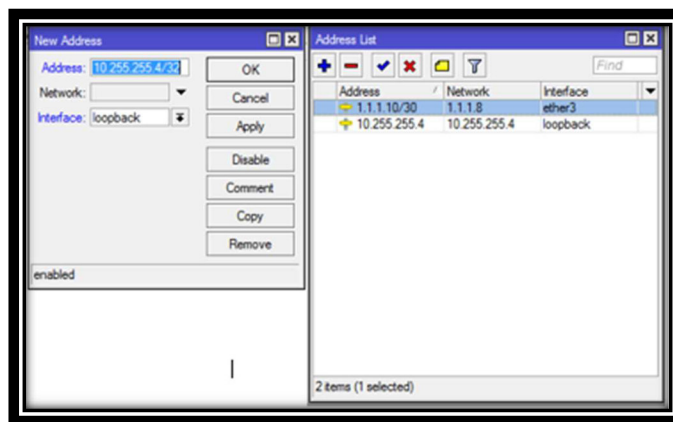


Figura 3.26969 Asignación de una dirección IP a la interfaz creada para el *router* RD

En la pestaña “*Routing*” seleccionar OSPF, en la segunda pestaña “*Interface*” seleccionar la interfaz creada por default para editarla. *Router ID* se configura con la dirección IP que se asignó a la interfaz *loopback*, como se muestra desde la Figura 3.270 a la Figura 3.277.

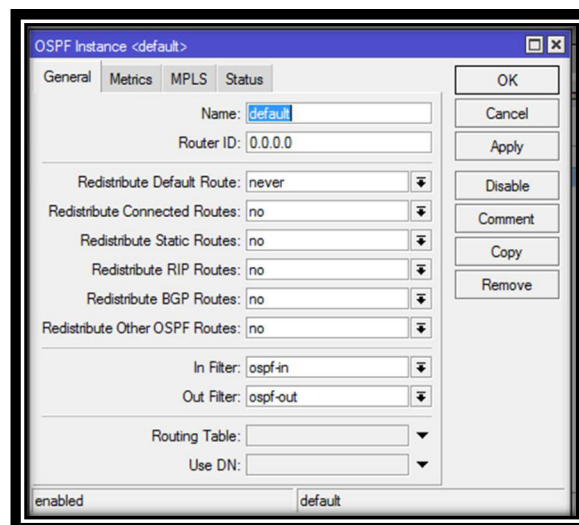


Figura 3.27070 Agregar y configurar la instancia con la dirección IP asignada a la interfaz lógica para el *router* RA

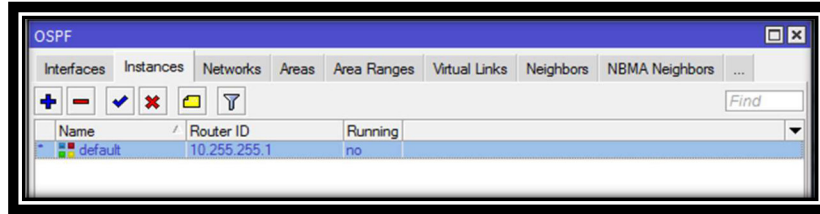


Figura 3.27171 Instancia creada en el router RA

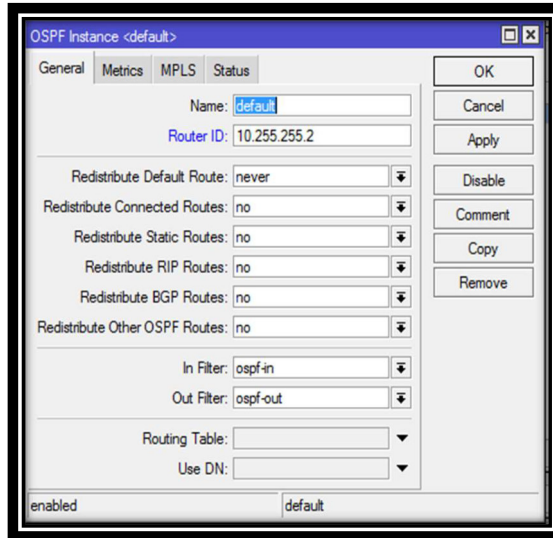


Figura 3.27272 Agregar y configurar la instancia con la dirección IP asignada a la interfaz lógica para el router RB

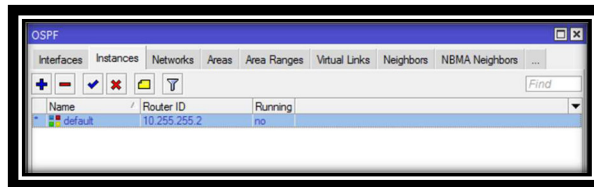


Figura 3.2733 Instancia creada en el router RB

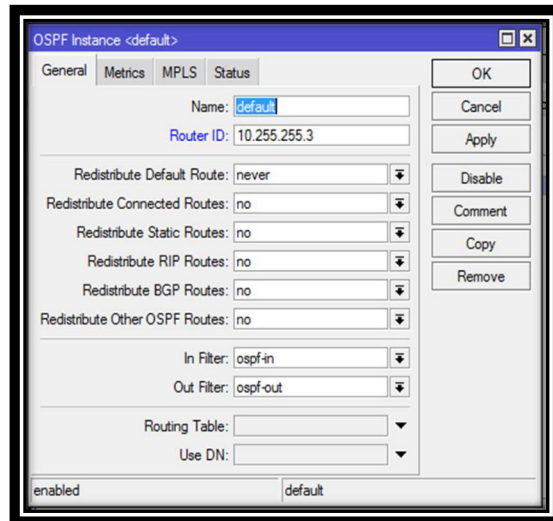


Figura 3.2744 Agregar y configurar la instancia con la dirección IP asignada a la interfaz lógica para el router RC

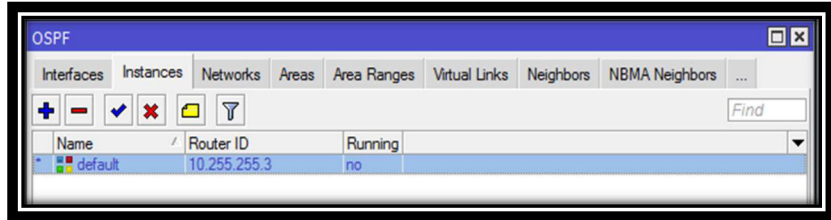


Figura 3.27575 Instancia creada en el *router* RC

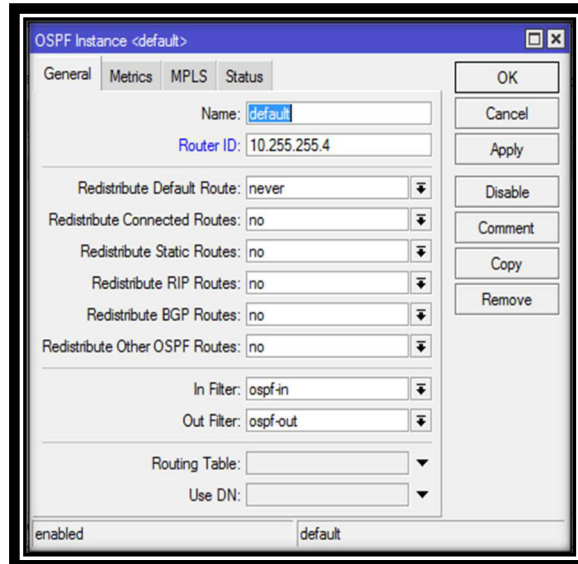


Figura 3.27676 Agregar y configurar la instancia con la dirección IP asignada a la interfaz lógica para el *router* RD

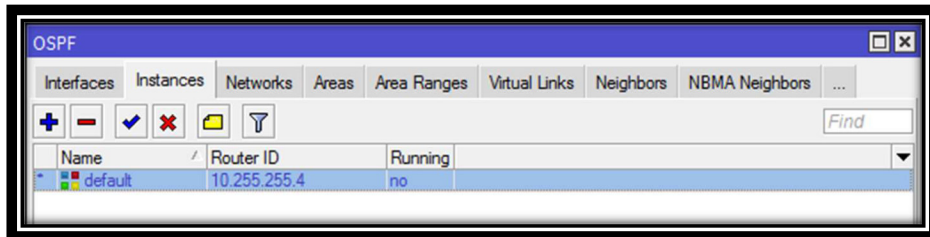


Figura 3.27777 Instancia creada en el *router* RD

En la pestaña “*Networks*” en la opción “+”, crear las direcciones a las que se encuentra conectado cada *router* y de la interfaz de *loopback*, como se observa desde la Figura 3.278 a la Figura 3.281.

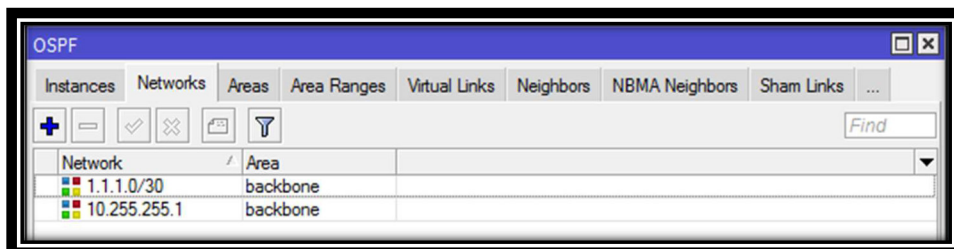


Figura 3.27878 Lista de redes agregadas en el *router* RA para el funcionamiento de OSPF

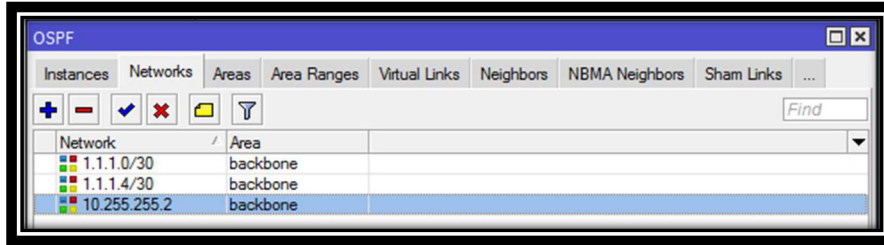


Figura 3.27979 Lista de redes agregadas en el *router* RB para el funcionamiento de OSPF

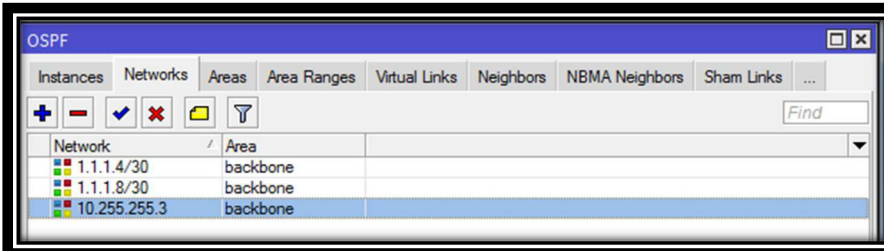


Figura 3.28080 Lista de redes agregadas en el *router* RC para el funcionamiento de OSPF

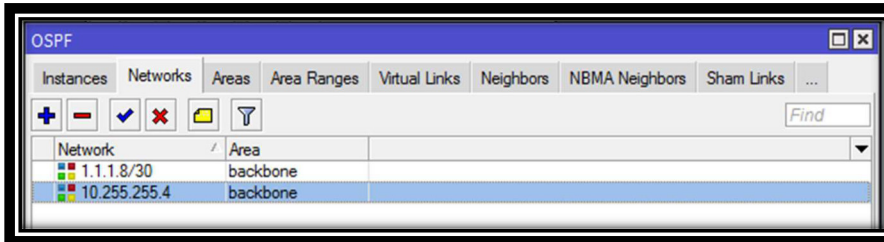


Figura 3.28181 Lista de redes agregadas en el *router* RD para el funcionamiento de OSPF

Verificar que las interfaces creadas en cada *router* se encuentren levantadas, como se muestra en la Figura 3.282 a la Figura 3.285.

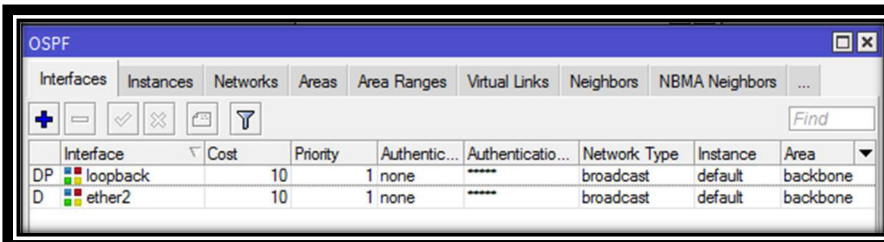


Figura 3.28282 Verificación en la pestaña “*Interfaces*” que el protocolo se encuentra levantado en el *router* RA

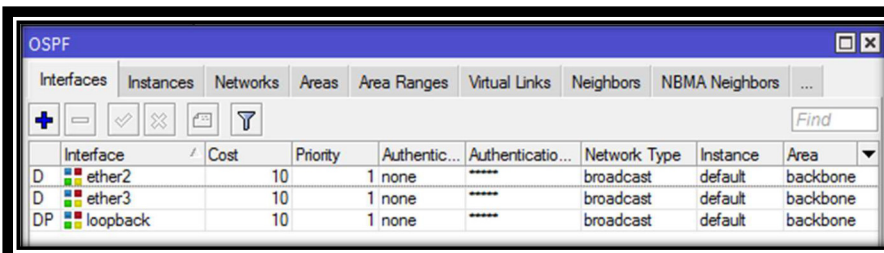


Figura 3.28333 Verificación en la pestaña “*Interfaces*” que el protocolo se encuentra levantado en el *router* RB

Interface	Cost	Priority	Authentic...	Authenticatio...	Network Type	Instance	Area
D ether2	10	1	none	*****	broadcast	default	backbone
D ether3	10	1	none	*****	broadcast	default	backbone
DP loopback	10	1	none	*****	broadcast	default	backbone

Figura 3.2844 Verificación en la pestaña “Interfaces” que el protocolo se encuentra levantado en el router RC

Interface	Cost	Priority	Authentic...	Authenticatio...	Network Type	Instance	Area
D ether3	10	1	none	*****	broadcast	default	backbone
DP loopback	10	1	none	*****	broadcast	default	backbone

Figura 3.28585 Verificación en la pestaña “Interfaces” que el protocolo se encuentra levantado en el router RD

Verificar que la tabla de enrutamiento se haya completado (que se encuentre convergente) en todos los routers, como se muestran desde la Figura 3.286 a la Figura 3.289.

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAC	1.1.1.0/30	ether2 reachable	0		1.1.1.1
DAo	1.1.1.4/30	1.1.1.2 reachable ether2	110		
DAo	1.1.1.8/30	1.1.1.2 reachable ether2	110		
DAC	10.255.255.1	loopback reachable	0		10.255.255.1
DAo	10.255.255.2	1.1.1.2 reachable ether2	110		
DAo	10.255.255.3	1.1.1.2 reachable ether2	110		
DAo	10.255.255.4	1.1.1.2 reachable ether2	110		

Figura 3.28686 Tabla de rutas aprendidas por el router RA

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAC	1.1.1.0/30	ether3 reachable	0		1.1.1.2
DAC	1.1.1.4/30	ether2 reachable	0		1.1.1.5
DAo	1.1.1.8/30	1.1.1.6 reachable ether2	110		
DAo	10.255.255.1	1.1.1.1 reachable ether3	110		
DAC	10.255.255.2	loopback reachable	0		10.255.255.2
DAo	10.255.255.3	1.1.1.6 reachable ether2	110		
DAo	10.255.255.4	1.1.1.6 reachable ether2	110		

Figura 3.28787 Tabla de rutas aprendidas por el router RB

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAo	1.1.1.0/30	1.1.1.5 reachable ether3	110		
DAC	1.1.1.4/30	ether3 reachable	0		1.1.1.6
DAC	1.1.1.8/30	ether2 reachable	0		1.1.1.9
DAo	10.255.255.1	1.1.1.5 reachable ether3	110		
DAo	10.255.255.2	1.1.1.5 reachable ether3	110		
DAC	10.255.255.3	loopback reachable	0		10.255.255.3
DAo	10.255.255.4	1.1.1.10 reachable ether2	110		

Figura 3.28888 Tabla de rutas aprendidas por el *router* RC

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAo	1.1.1.0/30	1.1.1.9 reachable ether3	110		
DAo	1.1.1.4/30	1.1.1.9 reachable ether3	110		
DAC	1.1.1.8/30	ether3 reachable	0		1.1.1.10
DAo	10.255.255.1	1.1.1.9 reachable ether3	110		
DAo	10.255.255.2	1.1.1.9 reachable ether3	110		
DAo	10.255.255.3	1.1.1.9 reachable ether3	110		
DAC	10.255.255.4	loopback reachable	0		10.255.255.4

Figura 3.28989 Tabla de rutas aprendidas por el *router* RD

Paso 3: configuración de MPLS

Se debe verificar como OSPF enruta los paquetes para esto en la pestaña "Tool" seleccionar "traceroute". Desde el *router* RA hacia el RD, ver Figura 3.290.

Figura 3.29090 Pestaña principal de "Traceroute"

Realizar el trazo a la dirección de *loopback* del *router* RD que se encuentra al otro extremo, en la sección "Traceroute To" colocar la dirección: 10.255.255.4, ver Figura 3.291.

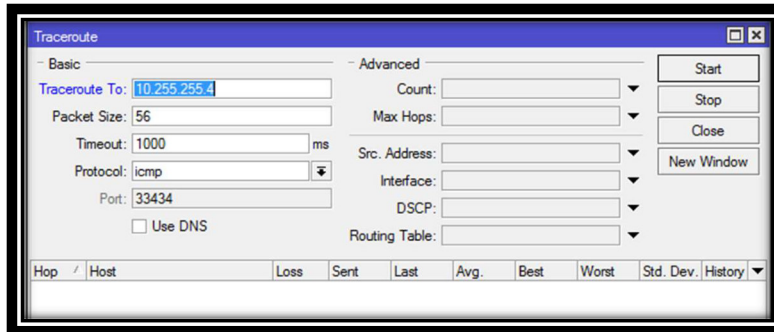


Figura 3.29191 Traceo con destino a una dirección IP del *router* RD

Presionar “*Start*”. Para verificar que se tenga acceso a la dirección de *loopback*. Los saltos son a través de los *routers* RB y RC, ver Figura 3.292.

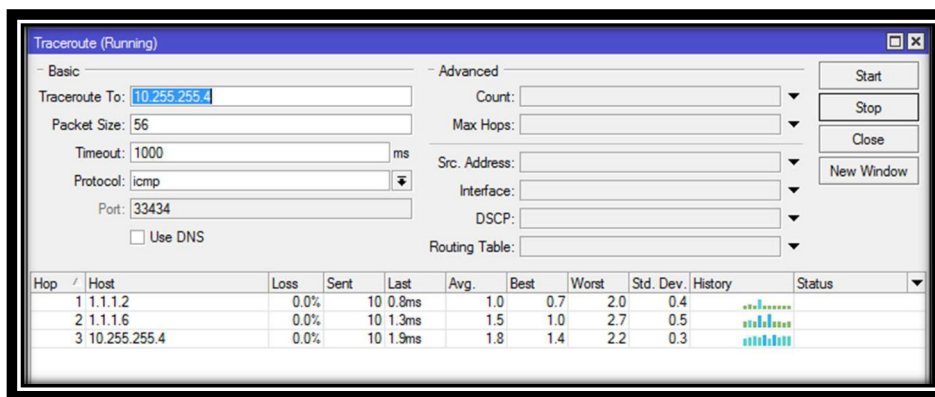


Figura 3.29292 Inicialización y resultados del traceo realizado desde RA a RD

En la pestaña “MPLS” escoger la opción MPLS, en la pestaña “*LDP Interface*” seleccionar la opción “*LDP Setting*”. El protocolo LDP asigna las etiquetas de manera dinámica. Habilitar la opción “*Enable*” y escribir la dirección IP de *loopback* del *router* que se está configurando, ver Figura 3.293.

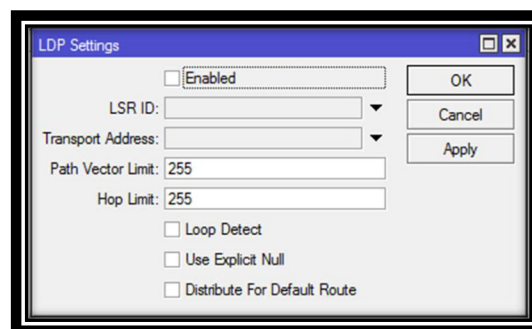


Figura 3.29333 Pestaña “*LDP Setting*”

Configurar “*LSR ID*” y “*Transport address*” de todos los *routers*, como se muestra desde la Figura 3.294 a la Figura 3.297.

RA

- *LSR ID*: 10.255.255.1 (la *ID* no es obligatorio, pero es recomendable)

- *Transport address:* 10.255.255.1

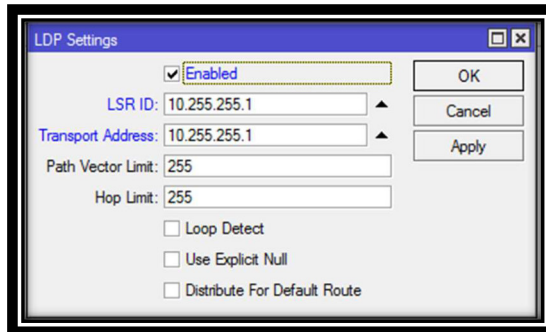


Figura 3.2944 Pestaña “LDP Setting” con las opciones configuradas para el *router* RA

RB

- *LSR ID:* 10.255.255.1 (la *ID* no es obligatorio, pero es recomendable)
- *Transport address:* 10.255.255.2

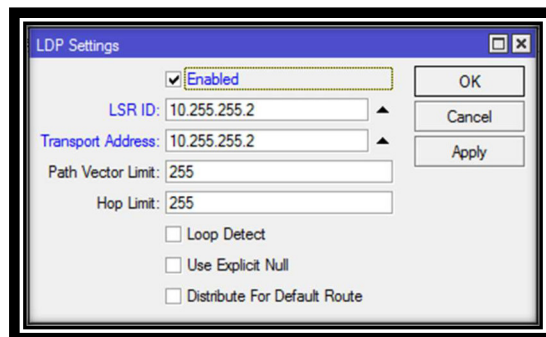


Figura 3.29595 Pestaña “LDP Setting” con las opciones configuradas para el *router* RB

RC

- *LSR ID:* 10.255.255.1 (la *ID* no es obligatorio, pero es recomendable)
- *Transport address:* 10.255.255.3

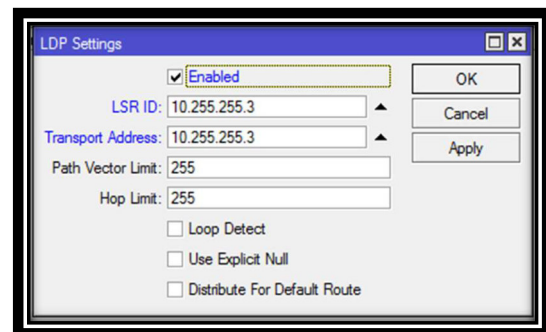


Figura 3.29696 Pestaña “LDP Setting” con las opciones configuradas para el *router* RC

RD

- *LSR ID:* 10.255.255.1 (la *ID* no es obligatorio, pero es recomendable)
- *Transport address:* 10.255.255.4

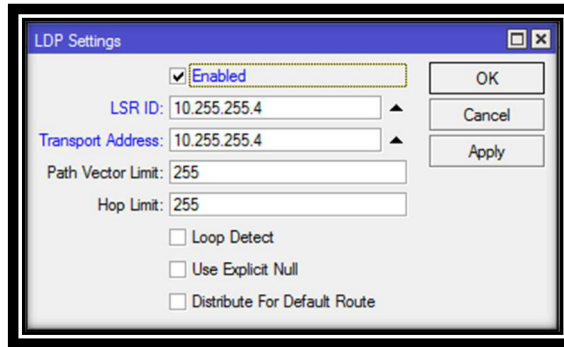


Figura 3.29797 Pestaña “LDP Setting” con las opciones configuradas para el *router* RD

Seleccionar “+” para agregar la interfaz con la que se une los diferentes *routers*. En “LDP Interface”, como se muestra desde la Figura 3.298 a la Figura 3.299.

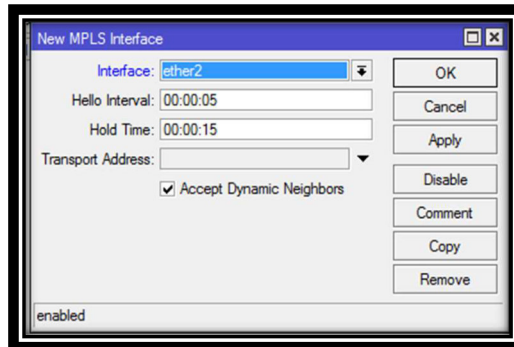


Figura 3.29898 Agregar la interfaz con la que se une RA con RB

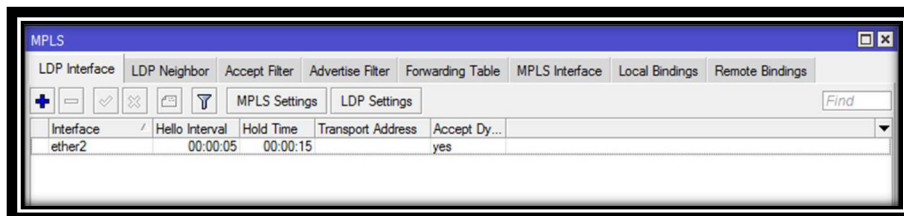


Figura 3.299 Interfaz levantada para el *router* RA, para el funcionamiento de MPLS

Repetir el mismo procedimiento para los demás *router*, como se observa en la Figura 3.300 hasta la Figura 3.302.

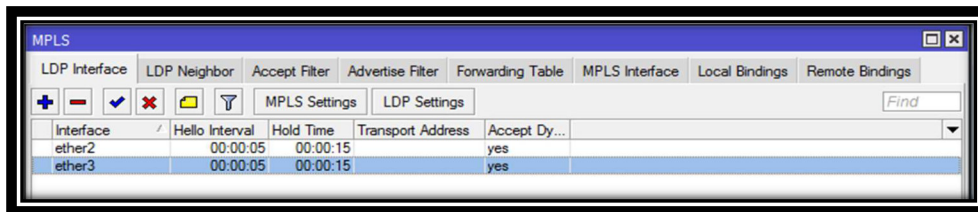


Figura 3.3000 Interfaces levantadas para el *router* RB, para el funcionamiento de MPLS

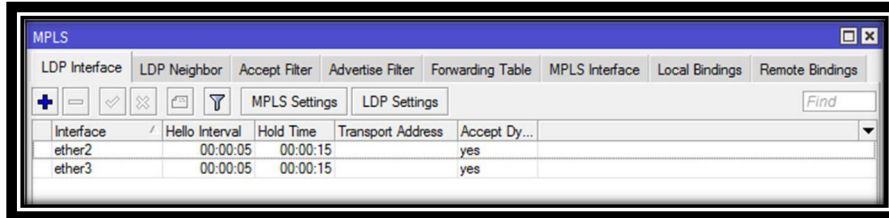


Figura 3.3011 Interfaces levantadas para el *router* RC, para el funcionamiento de MPLS

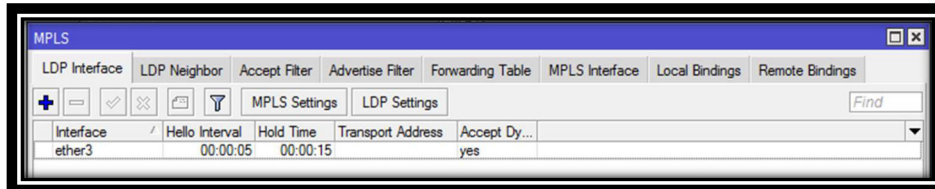


Figura 3.3022 Interfaz levantada para el *router* RD, para el funcionamiento de MPLS

En la pestaña “*LDP Neighbor*”. Se puede observar que los *routers* han aprendido nuevas rutas, debido a que el protocolo LDP de la tecnología MPLS se ha levantado, ver Figura 3.303.

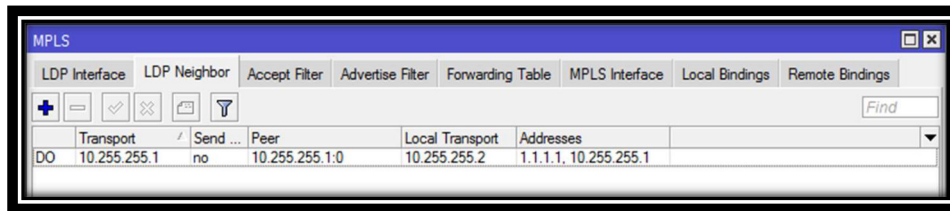


Figura 3.3033 Procolo LDP levantado en el *router* RA

Se verifica que se ha levantado el protocolo en el *router* RA, como se observa desde la Figura 3.304 a la Figura 3.306.

El significado de las siglas DO es:

- (D) dinámica
- (O) operacional

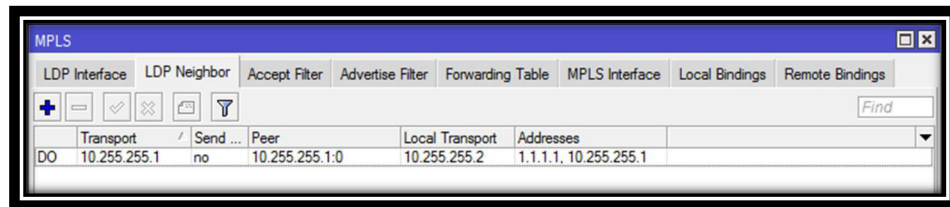


Figura 3.3044 Procolo LDP levantado en el *router* RB

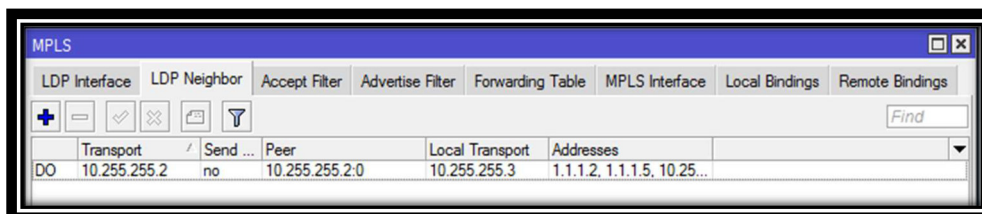


Figura 3.3055 Procolo LDP levantado en el *router* RC

The screenshot shows the 'MPLS' configuration window with the 'LDP Neighbor' tab selected. The table below displays the LDP neighbor configuration for the 'DO' transport address.

Transport	Send ...	Peer	Local Transport	Addresses
DO 10.255.255.3	no	10.255.255.3:0	10.255.255.4	1.1.1.6, 1.1.1.9, 10.25...

Figura 3.3066 Procolo LDP levantado en el *router* RD

En la pestaña “*Forwarding table*” se puede observar las tablas de reenvío de los *routers*, como se muestra desde la Figura 3.307 a la Figura 3.310.

The screenshot shows the 'MPLS' configuration window with the 'Forwarding Table' tab selected for router RA. The table below displays the forwarding entries.

In Label	Out Labels	Interface	Nexthop	Destination	Bytes	Packets	Hw. Bytes	Hw.Pack.
expl-null					0 B	0	0 B	0
L 16	16	ether2	1.1.1.2	1.1.1.8/30	0 B	0	0 B	0
L 17	18	ether2	1.1.1.2	10.255.255.4	0 B	0	0 B	0
L 18	19	ether2	1.1.1.2	10.255.255.3	0 B	0	0 B	0
L 19		ether2	1.1.1.2	1.1.1.4/30	0 B	0	0 B	0
L 20		ether2	1.1.1.2	10.255.255.2	0 B	0	0 B	0

Figura 3.3077 Tabla de reenvío de datos que se ha llenado en el *router* RA

The screenshot shows the 'MPLS' configuration window with the 'Forwarding Table' tab selected for router RB. The table below displays the forwarding entries.

In Label	Out Labels	Interface	Nexthop	Destination	Bytes	Packets	Hw. Bytes	Hw.P.
expl-null					0 B	0	0 B	
L 16		ether2	1.1.1.6	1.1.1.8/30	0 B	0	0 B	
L 17		ether3	1.1.1.1	10.255.255.1	0 B	0	0 B	
L 18	18	ether2	1.1.1.6	10.255.255.4	0 B	0	0 B	
L 19		ether2	1.1.1.6	10.255.255.3	0 B	0	0 B	

Figura 3.3088 Tabla de reenvío de datos que se ha llenado en el *router* RB

The screenshot shows the 'MPLS' configuration window with the 'Forwarding Table' tab selected for router RC. The table below displays the forwarding entries.

In Label	Out Labels	Interface	Nexthop	Destination	Bytes	Packets	Hw. Bytes	H
expl-null					0 B	0	0 B	
L 16		ether3	1.1.1.5	1.1.1.0/30	0 B	0	0 B	
L 17	17	ether3	1.1.1.5	10.255.255.1	0 B	0	0 B	
L 18		ether2	1.1.1.10	10.255.255.4	0 B	0	0 B	
L 19		ether3	1.1.1.5	10.255.255.2	0 B	0	0 B	

Figura 3.3099 Tabla de reenvío de datos que se ha llenado en el *router* RC

The screenshot shows the 'MPLS' configuration window with the 'Forwarding Table' tab selected for router RD. The table below displays the forwarding entries.

In Label	Out Labels	Interface	Nexthop	Destination	Bytes	Packets	Hw. Bytes	Hw.Pack.
expl-null					0 B	0	0 B	0
L 16	16	ether3	1.1.1.9	1.1.1.0/30	0 B	0	0 B	0
L 17	17	ether3	1.1.1.9	10.255.255.1	0 B	0	0 B	0
L 18		ether3	1.1.1.9	10.255.255.3	0 B	0	0 B	0
L 19		ether3	1.1.1.9	1.1.1.4/30	0 B	0	0 B	0
L 20	19	ether3	1.1.1.9	10.255.255.2	0 B	0	0 B	0

Figura 3.31010 Tabla de reenvío de datos que se ha llenado en el *router* RD

Realizar el trazo desde el *router* RA hacia la interfaz de *loopback* de RD. Para esto ingresar a la pestaña “Tools” y escoger “Traceroutes”. Seleccionar la opción: “New window”, ver Figura 3.311.

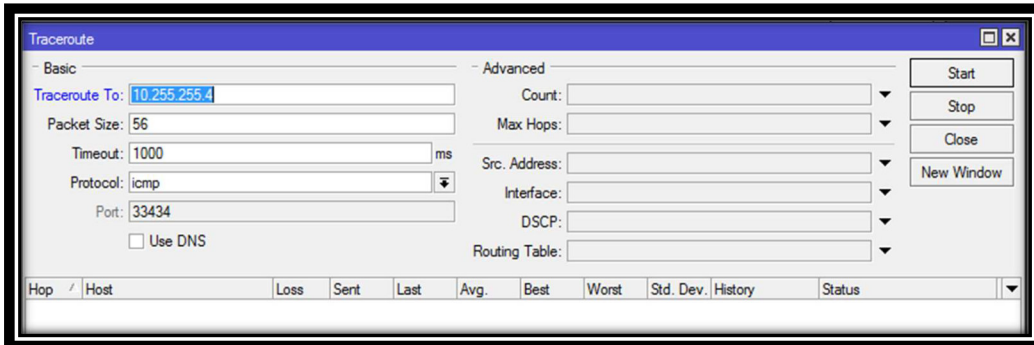


Figura 3.31111 Nueva pestaña abierta para realizar un trazo

Observar el “Status” y la etiqueta que asigna cada *router*, se observa que existen etiquetas asignadas por MPLS ver Figura 3.312.

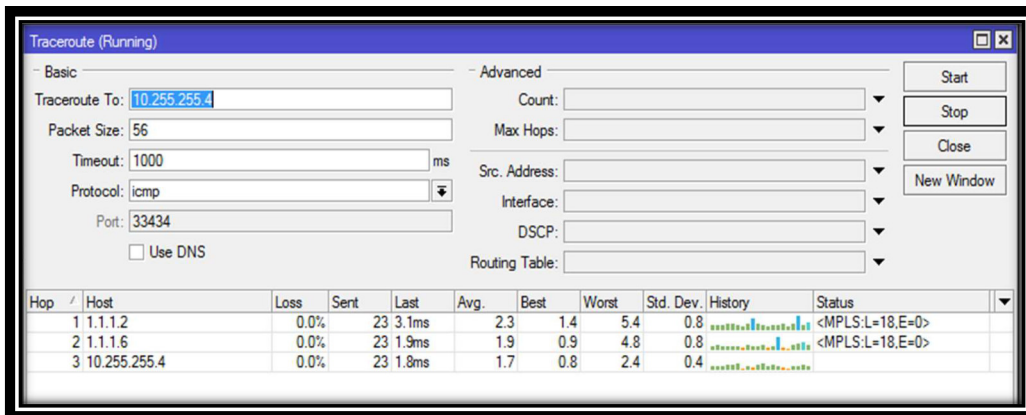


Figura 3.31212 Inicialización y resultado del trazo, en la pestaña “Status”

Se puede observar la diferencia del trazo realizado con OSPF, como se muestra en la Figura 3.313 y MPLS, ver Figura 3.314. Para el trazo con MPLS se han asignado etiquetas.

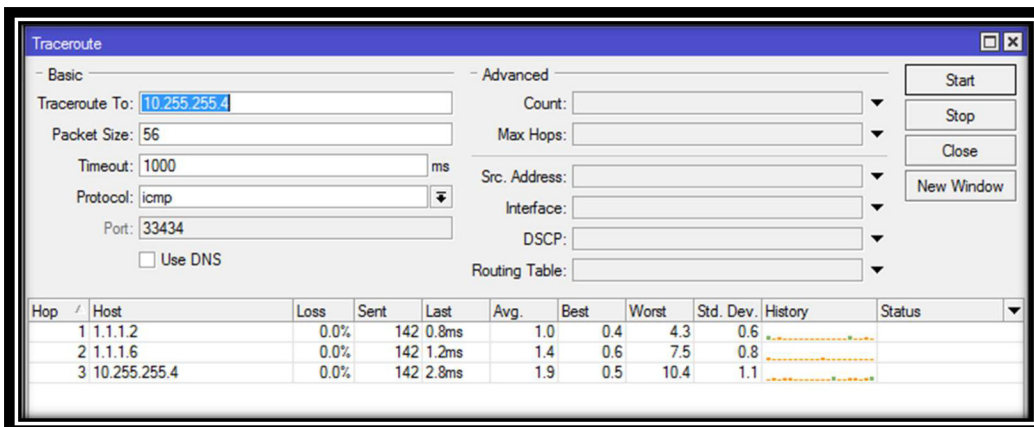


Figura 3.31313 Trazo obtenido usando el protocolo OSPF

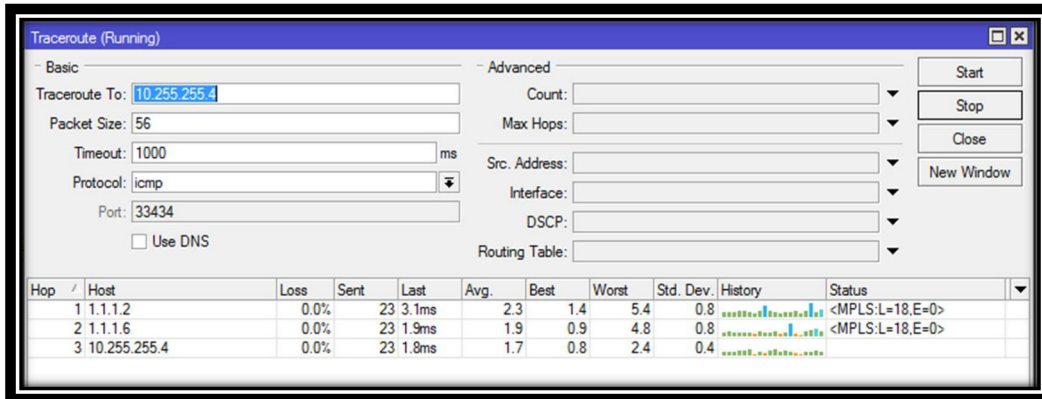




Figura 3.31414 Traceo obtenido usando la tecnología MPLS

5. RECOMENDACIONES:

- Se debe tener en cuenta las direcciones IP asignadas a la interfaz *bridge* que son usadas para el levantamiento del protocolo OSPF.
- Para OSPF tener en cuenta las redes que se deben agregar a cada *router* para que el protocolo las pueda compartir con los demás.
- Tomar en cuenta las interfaces que unen los enlaces de los *routers*, para que MPLS funcione correctamente y agregue las etiquetas propias del protocolo.
- Para cualquier cambio a realizarse en la configuración de los adaptadores de red de los *routers* simulados, ya sea en GNS o *VirtualBox*, primero se debe pausar el programa presionando el ícono  (pausa), sino GNS3 no permitirá efectuar dichos cambios mientras está corriendo o se presentará un error en el programa que no permitirá acceder a la configuración de los equipos mediante *Winbox*. Una vez efectuadas las modificaciones correspondientes se puede presionar  (iniciar) para continuar con la práctica.

4 CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones:

- Se concluye que la licencia de nivel cero es la idónea para ser usada dentro de un ambiente simulado y netamente académico, ya que brinda todas las funcionalidades, protocolos y opciones necesarias para la configuración e introducción al manejo de los *routers Mikrotik*, además de no presentar costo alguno.
- Se concluye que las herramientas y funciones presentes en GNS3 y la interfaz gráfica *Winbox* resultan ser intuitivas y fáciles de usar por el usuario. Además, en este apartado se ha descrito el proceso de: creación de máquinas virtuales en *Oracle VM VirtualBox*, carga de la imagen del *router Mikrotik*, creación de una interfaz *loopback* y vinculación con el programa GNS3. Proporcionando al estudiante y docente un medio de implementación sencillo y práctico para la simulación y configuración de los *routers Mikrotik*.
- Se propuso prácticas relacionadas con el PEA de las materias: TCP/IP y Redes de Computadoras pertenecientes a la Carrera de Tecnología Superior en Redes y Telecomunicaciones de la ESFOT. Con la finalidad de que los estudiantes complementen los conocimientos adquiridos teóricamente, mediante la simulación de diferentes topologías de red. Tratando temas tales como: enrutamiento estático, protocolo vector distancia RIP, BGP, redes MPLS con OSPF y protocolo PPTP (VPN).
- Para un profesional solvente en el área de telecomunicaciones es indispensable adquirir conocimientos correspondientes al manejo y configuración de equipos de redes en diversas marcas. Siendo el caso específico de los *routers Mikrotik*, el alumno podrá ser capaz de familiarizarse con el manejo de estos *routers*, implementar diversas topologías básicas y levantarlas mediante la simulación de las prácticas con la ayuda de las guías del presente documento.
- GNS3 ofrece la opción de implementar diversos sistemas operativos, es decir que en la plataforma de GNS3 se pueden simular diferentes marcas de equipos de red, así como sistemas operativos de PC. Esto debido a que GNS3 es capaz de vincularse con máquinas virtuales, proporcionando de esta manera una mayor gama de equipos con los que se puede trabajar.
- La interfaz gráfica *Winbox*, propietaria de la compañía *Mikrotik* y usada específicamente para estos equipos, es una herramienta indispensable para la

configuración de los *routers*. Puesto que brinda una manera simple e intuitiva para la configuración y manejo, permitiendo al usuario encargado de esta labor un trabajo sencillo y sin tantas complicaciones que implicaría configurar un *router* únicamente mediante línea de comandos.

- Se desarrollaron hojas guías para las docentes, mismas que cuentan con el procedimiento detallado paso a paso, con la respectiva demostración del funcionamiento e implementación correspondiente a cada práctica. Así mismo, se desarrollaron hojas guías para los estudiantes, en donde se detalla de manera resumida los pasos que deben seguir y topología, para ser capaces de implementar las prácticas propuestas.

4.2 Recomendaciones:

- La principal recomendación es la elección del nivel de licencia a utilizar tomando en cuenta todas las ventajas y desventajas que posee cada nivel. La licencia de nivel cero es la indicada para finalidades educativas, mientras que a nivel empresarial es menester adquirir una de las que sean pagadas, por las prestaciones que dan.
- Para cada tópico propuesto en las prácticas es necesario tener claro los conocimientos teóricos, para facilitar y concatenar lo aprendido con la práctica.
- Para el desarrollo e implementación de las prácticas, es recomendable haber creado previamente los *routers* necesarios y vincularlos con GNS3.
- Al usarse varios programas simultáneamente en el computador, estos requieren usar gran capacidad de la memoria RAM, por lo cual es recomendable que el ordenador cuente por lo menos con 4 GB de memoria, para no tener inconveniente alguno con el rendimiento al momento de realizar las prácticas.
- GNS3 al valerse de un programa externo para acoplar y simular máquinas virtuales, tal como *VirtualBox* o *VMware*, permite vincular diversas marcas a la plataforma. Por esta razón se recomienda el uso de este programa para fines educativos y que de esta manera los estudiantes puedan familiarizarse con el uso y configuración de equipos de red.

5 REFERENCIAS BIBLIOGRÁFICAS

- [1] Mikrotik, «Mikrotik,» [En línea]. Available: <https://mikrotik.com/aboutus..> [Último acceso: Agosto 2020].
- [2] Mikrotik, «Mikrotik RouterOS,» [En línea]. Available: <https://mikrotik.com/software..> [Último acceso: Agosto 2020].
- [3] Mikrotik, «Manual: Winbox,» [En línea]. Available: <https://wiki.mikrotik.com/wiki/Manual:Winbox..> [Último acceso: Agosto 2020].
- [4] Corporacion R&CH, «Alternativas al Cliente de sesiones SSH Putty,» [En línea]. Available: <https://electronicarych.com/blog/ssh-6/post/alternativas-al-cliente-de-sesiones-ssh-putty-1#:~:text=Solar%2DPutty.,opciones%20y%20capacidad%20de%20b%C3%BAqueda...> [Último acceso: Agosto 2020].
- [5] GOOGLE, «Programación básica JAVA,» [En línea]. Available: <https://sites.google.com/site/programacionbasicajava/interfaz-grafica-gui..> [Último acceso: Agosto 2020].
- [6] GOOGLE, «Protocolos de enrutamiento Vector-Distancia: RIP,IGRP,» [En línea]. Available: <https://sites.google.com/site/redeslocalesyglobales/6-arquitecturas-de-redes/6-arquitectura-tcp-ip/9-protocolos-tcp-ip/protocolos-de-nivel-de-red/enrutamiento-vector-distancia.> [Último acceso: 16 Junio 2021].
- [7] CISCO, «NAT genérico,» [En línea]. Available: <https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/26704-nat-faq-00.html..> [Último acceso: Agosto 2020].
- [8] CISCO, «Estudios de caso de BGP,» Octubre 2008. [En línea]. Available: <https://www.cisco.com/c/en/us/support/docs/ip/border-Gateway-protocol-bgp/26634-bgp-toc.html.> [Último acceso: Agosto 2020].
- [9] GOOGLE, «Protocolo OSPF,» [En línea]. Available: <https://sites.google.com/site/redeslocalesyglobales/4-configuracion-de-red/2->

configuracion-de-routers/6-configuracion-del-encaminamiento/2-encaminamiento-dinamico/6-protocolo-ospf. [Último acceso: 16 Junio 2021].

- [10] ExpressVPN, «Protocolos VPN: PPTP,» Diciembre 2018. [En línea]. Available: <https://www.expressvpn.com/es/what-is-vpn/protocols/pptp>. [Último acceso: 16 Junio 2021].
- [11] EXPRESSVPN, «VPN,» [En línea]. Available: <https://www.expressvpn.com/es/what-is-vpn>. [Último acceso: 16 Junio 2021].
- [12] VIRTUALBOX, «*VirtualBox*,» [En línea]. Available: <https://www.virtualbox.org/>. [Último acceso: Agosto 2020].
- [13] INFOTECs, «MPLS,» 07 Abril 2020. [En línea]. Available: <https://infotecs.mx/blog/mpls.html>. [Último acceso: 16 Junio 2021].
- [14] SYSCOM, «Niveles de Licencia *Mikrotik*,» [En línea]. Available: <https://soporte.syscom.mx/es/articulos/1867876-mikrotik-niveles-de-licencia..> [Último acceso: Septiembre 2020].
- [15] GNS3, «GNS3,» [En línea]. Available: <https://www.gns3.com/software/download..> [Último acceso: Septiembre 2020].
- [16] GNS3, «GNS3 Created Account,» [En línea]. Available: <https://www.gns3.com/account/register..> [Último acceso: Septiembre 2020].
- [17] Virtual Box, «Oracle VM Virtual Box,» [En línea]. Available: <https://www.virtualbox.org/wiki/Downloads..> [Último acceso: Septiembre 2020].
- [18] *Mikrotik*, «*Mikrotik*: Software,» [En línea]. Available: <https://mikrotik.com/download.> . [Último acceso: Septiembre 2020].
- [19] GNS3, «La GUI de GNS3,» [En línea]. Available: <https://docs.gns3.com/docs/using-gns3/beginners/the-gns3-gui/#manage-snapshot>. [Último acceso: Octubre 2020].

6 ANEXOS

**ANEXO 1: LINK DE REPOSITORIO DE PRÁCTICAS
REALIZADAS.**

<https://drive.google.com/drive/folders/1UnIzvkfhIEAJsxZnmiVgYvxA9JfHdkE?usp=sharing>