

UNIVERSIDAD DE EL SALVADOR  
FACULTAD DE INGENIERÍA Y ARQUITECTURA  
ESCUELA DE INGENIERÍA ELÉCTRICA



**Implementación de protocolos de enrutamiento y servicios para una Red de Área Local mediante software libre.**

PRESENTADO POR:

**LUIS MIGUEL ESCOBAR HERNÁNDEZ**

**MARVIN BALMORE GARCÍA MEJICANO**

**PEDRO ANTONIO SORIANO ARÉVALO**

PARA OPTAR AL TÍTULO DE:

**INGENIERO ELECTRICISTA**

CIUDAD UNIVERSITARIA, AGOSTO 2015

**UNIVERSIDAD DE EL SALVADOR**

**RECTOR :**

**ING. MARIO ROBERTO NIETO LOVO**

**SECRETARIA GENERAL :**

**DRA. ANA LETICIA ZA VALETA DE AMAYA**

**FACULTAD DE INGENIERÍA Y ARQUITECTURA**

**DECANO :**

**ING. FRANCISCO ANTONIO ALARCÓN SANDOVAL**

**SECRETARIO :**

**ING. JULIO ALBERTO PORTILLO**

**ESCUELA DE INGENIERÍA ELÉCTRICA**

**DIRECTOR :**

**MSC. JOSÉ WILBER CALDERÓN URRUTIA**

UNIVERSIDAD DE EL SALVADOR  
FACULTAD DE INGENIERÍA Y ARQUITECTURA  
ESCUELA DE INGENIERÍA ELÉCTRICA

Trabajo de Graduación previo a la opción al Grado de:

**INGENIERO ELECTRICISTA**

Título :

**Implementación de protocolos de enrutamiento y servicios para una Red de Área Local mediante software libre.**

Presentado por :

**LUIS MIGUEL ESCOBAR HERNÁNDEZ**

**MARVIN BALMORE GARCÍA MEJICANO**

**PEDRO ANTONIO SORIANO ARÉVALO**

Trabajo de Graduación Aprobado por :

Docente Asesor :

**MSC. CARLOS OSMÍN POCASANGRE JIMÉNEZ**

San Salvador, Agosto 2015

Trabajo de Graduación Aprobado por:

Docente Asesor :

**MSC. CARLOS OSMÍN POCASANGRE JIMÉNEZ**

## ACTA DE CONSTANCIA DE NOTA Y DEFENSA FINAL

En esta fecha, 17 de julio de 2015, en la Sala de Reuniones de la Escuela de Ingeniería Eléctrica, a las 5:00 horas, en presencia de las siguientes autoridades de la Escuela de Ingeniería Eléctrica de la Universidad de El Salvador:

1. MSc. e Ing. José Wilber Calderón Urrutia  
Director

Firma:

*Wilber Calderón*

2. MSc. e Ing. Salvador de Jesús Germán  
Secretario

Firma:

*Salvador de Jesús Germán*



Y, con el Honorable Jurado de Evaluación integrado por las personas siguientes:

1- MSc. e Ing. Carlos Osmin Pocasangre Jiménez

Firma:

*Carlos Osmin Pocasangre Jiménez*

2- MSc. Hugo Miguel Colato Rodríguez

*Hugo Miguel Colato Rodríguez*

3- Ing. Werner David Meléndez Valle

*Werner David Meléndez Valle*

Se efectuó la defensa final reglamentaria del Trabajo de Graduación:

**Implementación de protocolos de enrutamiento y servicios para una Red de Área Local mediante software libre.**

A cargo de los Bachilleres:

- Escobar Hernández Luís Miguel
- García Mejicano Marvín Balmore
- Soriano Arévalo Pedro Antonio

Habiendo obtenido en el presente Trabajo una nota promedio de la defensa final:

8.9

*(Ocho punto Nueve)*

## AGRADECIMIENTOS

Agradezco principalmente a Dios por darme salud, voluntad y fuerzas para sobrellevar y seguir adelante durante toda la carrera.

A mis padres por darme siempre todos los ánimos necesarios para no decaer y estar siempre pendientes de mi rendimiento apoyándome siempre que lo necesité.

A mis hermanos Lilian, Carlos, Saúl y Mabel por ser un ejemplo para mí, un punto de referencia a mis metas, especialmente agradezco todo el apoyo de mi hermano Carlos que incondicionalmente estuvo conmigo desde el inicio hasta el fin.

A los docentes que me guiaron y transmitieron todo el conocimiento para formarme profesionalmente, especialmente agradezco a nuestro asesor que estuvo siempre dándonos apoyo cuando las cosas se tornaban oscuras.

A mis compañeros de tesis Marvin y Pedro por haber estado a la par, en pie de lucha aportando ideas para solventar las dificultades.

A todos los compañeros con los que inicié la carrera que se transformaron en mis amigos y futuros colegas, en este punto solo se puede decir “valió la pena todo el esfuerzo”

A todas las personas que estuvieron a mi lado dándome ánimos y de alguna manera directa o indirecta me dieron su incondicional apoyo.

Luis Miguel Escobar Hernández

## AGRADECIMIENTOS

Agradezco al creador por darme el coraje y la sabiduría para superar las dificultades y permitirme culminar esta carrera universitaria.

Dedico este trabajo especialmente a la memoria de mi madre Griselda Mejicano quien en vida me brindó su apoyo incondicional, comprensión y consejos para superar cada dificultad durante la mayor parte de mi carrera, quien siempre me animó a continuar a pesar de las dificultades y quien siempre confió en que me convertiría en un profesional.

A mi padre Valmore García por su apoyo, por darme ánimos y por su esfuerzo para que nunca me faltara nada. También a mis hermanas, Claudia, Yesenia y Fátima que de alguna u otra forma siempre me han apoyado, han estado en las buenas y las malas y siempre estarán ahí cuando las necesite.

A mi abuelo Virgilio Mejicano, mi tía Hermilda Mejicano, mi primo Marvin Robles por ser como mi segundo padre, madre y hermano que desde mi infancia me han animado a conseguir mis metas, me han ayudado emocional y económicamente y han estado pendiente de mis logros.

Al Ing. Carlos Osmín Pocasangre Jiménez, por habernos apoyado en la realización de este trabajo, por su confianza, ayuda y consejos que nos ha brindado.

A mis compañeros de tesis por darme la oportunidad de trabajar con ellos, por su esfuerzo, dedicación y aporte a este trabajo de graduación.

A todos mis amigos y compañeros con quienes compartí momentos inolvidables en la Universidad de El Salvador.

Y a todas las personas que de alguna forma me expresaron su apoyo incluso antes que iniciara mi carrera universitaria y me han motivado a terminar esta carrera.

Marvin Balmore García Mejicano

## AGRADECIMIENTOS

Primero agradezco a Dios por permitirme terminar mis estudios, por regalarme fortaleza en el transcurso de ello, y brindarme la oportunidad de conocer a muchos compañeros y amigos ya que con su apoyo el camino ha parecido más corto.

A mis padres ya que con su invaluable apoyo y confianza que depositaron en mí, esta meta ha sido posible. A mi otra familia que me acogió cuando estuve fuera e hizo de su hogar mi segunda casa. Y al resto de mi familia que siempre estuvo conmigo en mi esfuerzo con una palabra de aliento.

A todos docentes de la Escuela de Ingeniería Eléctrica de los cuales tuve el privilegio de aprender tanto aspectos técnicos como aptitudes que me ayudaron a crecer como persona.

A nuestro asesor de trabajo de graduación por toda la orientación durante el desarrollo del mismo, a mis compañeros que me permitieron trabajar junto a ellos.

Pedro Antonio Soriano Arévalo



## ÍNDICE

INTRODUCCIÓN .....	1
OBJETIVOS.....	2
OBJETIVO GENERAL .....	2
OBJETIVOS ESPECÍFICOS.....	2
ALCANCES .....	3
DEFINICIONES Y ABREVIATURAS.....	4
DEFINICIONES .....	4
ABREVIATURAS.....	5
CAPÍTULO I .....	9
REFERENCIA TEÓRICA.....	9
1.1 INTRODUCCIÓN A LAS REDES DE COMPUTADORA .....	10
1.2 MODELO OSI. [1] .....	10
1.2.1 SIETE CAPAS DEL MODELO OSI .....	11
1.2.2 UNIDADES DE DATOS. [1].....	14
1.2.3 MEDIOS FÍSICOS .....	16
1.2.3.1 MEDIOS DE COBRE [2].....	16
1.2.3.2 MEDIOS DE FIBRA ÓPTICA.....	19
1.2.3.3 MEDIOS INALÁMBRICOS .....	20
1.3 MIKROTIK HARDWARE .....	20
1.3.1 ROUTEROS [10].....	21
1.3.2 CARACTERÍSTICAS PRINCIPALES DE ROUTEROS [11] .....	21
1.3.3 FIREWALL .....	22
1.3.4 CALIDAD DE SERVICIO QOS.....	22
1.3.5 ROUTING .....	22
1.3.6 SERVIDOR / CLIENTE.....	22
1.3.8 HERRAMIENTAS DE MANEJO DE RED.....	23
1.3.9 LICENCIAMIENTO [12] .....	23
1.4 SWITCHING .....	27
1.4.1 SWITCH CAPA 2 .....	28
1.4.2 SWITCH CAPA 3 .....	29

1.4.3 SWITCH CAPA 4 .....	30
1.5 REDES VLAN .....	31
1.5.1 IMPLEMENTACIÓN DE VLAN.....	32
1.5.2 CUANDO UTILIZAR REDES VLAN .....	32
1.5.3 LAS VLAN Y LOS NOMBRES PERSONALIZADOS .....	32
1.5.4 TOPOLOGÍA DE VLAN .....	33
1.5.5 TRUNKING (802.1q).....	34
1.5.6 VLAN NATIVA .....	35
1.6 MPLS.....	35
1.6.1 CARACTERÍSTICAS DE MPLS .....	37
1.6.2 APLICACIONES DE MPLS.....	38
1.6.3 OPERACIÓN DE MPLS .....	38
1.6.4 ESTRUCTURA MPLS .....	39
1.6.5 CARACTERÍSTICAS DE LSP.....	40
1.6.6 CARACTERÍSTICAS DE SEÑALIZACIÓN DINÁMICA LDP .....	41
1.6.7 CARACTERÍSTICAS DE SEÑALIZACIÓN DINÁMICA USANDO RSVP .....	42
1.6.8 COMPARACIÓN DE MPLS CON ROUTING y ATM .....	42
1.7 TÉCNICAS DE ENRUTAMIENTO. ....	43
1.7.1 ENRUTAMIENTO ESTÁTICO.....	43
1.7.1.1 ENRUTAMIENTO PREDETERMINADO .....	44
1.7.1.2 RUTAS ESTÁTICAS .....	44
1.7.2 ENRUTAMIENTO DINÁMICO .....	45
1.7.3 PROTOCOLOS DE ENRUTAMIENTO .....	45
1.7.3.1 ROUTING INFORMATION PROTOCOL (RIP) .....	45
1.7.3.2 OPEN SHORT PATH FIRST (OSPF).....	46
1.7.3.3 BORDER GATEWAY PROTOCOL (BGP) .....	47
1.7.4 PROTOCOLOS ENRUTABLES.....	49
1.7.4.1 IP .....	50
1.8 SEGURIDAD .....	50
1.8.1 FIREWALL (CORTAFUEGOS) .....	50
1.8.1.1 FIREWALL DE CAPA DE RED O DE FILTRADO DE PAQUETES.....	51

1.8.2 IPSEC – ARQUITECTURA DE SEGURIDAD PARA IP .....	51
1.8.3 AH y ESP .....	52
1.8.3 NAT .....	53
1.8.4 PORT FORWARDING .....	54
1.8.5 VPN.....	54
1.9 APLICACIONES LAN.....	56
1.9.1 ASIGNACIÓN PARÁMETROS DE RED Y DNS POR DHCP .....	56
1.9.1.1 ¿QUÉ ES EL DHCP? .....	56
1.9.1.2 FUNCIONAMIENTO DE UNA PETICIÓN DHCP .....	57
1.9.2 TELEFONÍA IP .....	58
1.9.2.1 ¿QUÉ ES LA TELEFONÍA IP? .....	58
1.9.2.2 ¿QUÉ ES UNA CENTRAL IP? .....	59
1.9.3 EL PROTOCOLO SIP .....	60
1.9.3.1 FUNCIONES SIP .....	60
1.9.3.2 BENEFICIOS DEL PROTOCOLO SIP .....	61
1.10 PROTOCOLO SNMP .....	62
1.10.1 ¿QUÉ ES SNMP? .....	62
1.10.2 SEGURIDAD EN SNMP .....	64
1.10.3 ¿QUÉ ES EL MIB? .....	64
1.10.4 CACTIEZ.....	67
1.10.5 WEATHERMAP.....	67
1.11 SIMULADOR DE REDES MIKROTIK [39].....	68
1.11.1 HERRAMIENTAS.....	69
1.11.2 PRUEBAS DE RENDIMIENTO .....	70
CAPÍTULO II .....	71
DISEÑO E IMPLEMENTACIÓN.....	71
2.1 SIMULACIÓN DE ROUTEROS EN GNS3 .....	72
2.1.1 INSTALACIÓN Y CONFIGURACIÓN DE MÁQUINAS VIRTUALES EN GNS3.....	73
2.2 ENRUTAMIENTO ESTÁTICO.....	78
2.2.1 EJEMPLO PRÁCTICO.....	79
2.2.2 CONFIGURACIONES.....	79

2.3 ENRUTAMIENTO DINÁMICO RIP V2 .....	80
2.3.1 EJEMPLO PRÁCTICO.....	80
2.3.2 CONFIGURACIONES.....	81
2.4 VLAN Y SERVICIOS DHCP .....	81
2.4.1 EJEMPLO PRÁCTICO.....	82
2.4.2 CONFIGURACIONES.....	83
2.5 ENRUTAMIENTO OSPF Y FIREWALL.....	85
2.5.1 EJEMPLO PRÁCTICO.....	87
2.5.2 CONFIGURACIONES.....	88
2.6 ENRUTAMIENTO DE SISTEMAS AUTÓNOMOS BGP.....	94
2.6.1 EJEMPLO PRÁCTICO.....	94
2.6.2 CONFIGURACIONES.....	95
2.7 SERVICIOS DE VPN .....	97
2.7.1 EJEMPLO PRÁCTICO.....	97
2.7.2 CONFIGURACIONES.....	98
2.8 MPLS Y MONITOREO POR SNMP .....	99
2.8.1 EJEMPLO PRÁCTICO.....	100
2.8.3 CONFIGURACIONES.....	100
2.9 NAT Y PORT FORWARDING .....	108
2.9.1 EJEMPLO PRÁCTICO.....	108
2.9.2 CONFIGURACIONES.....	109
CONCLUSIONES.....	110
RECOMENDACIONES .....	113
BIBIOGRAFÍA .....	115

## ÍNDICE DE FIGURAS

Figura 1. Las siete capas del modelo OSI [3] .....	15
Figura 2. Proceso de encapsulamiento de datos [1] .....	16
Figura 3. Partes del cable coaxial [4] .....	17
Figura 4. Partes del cable de par trenzado sin blindaje (UTP) [5] .....	17
Figura 5. Estándares EIA/TIA T568A y T568B [2].....	18
Figura 6. Tipos de cable estructurado para redes de datos [2] .....	18
Figura 7. Cable para transmisión de luz [6].....	19
Figura 8. Tecnologías inalámbricas y sus estándares [7] .....	20
Figura 9: Dominios de broadcasts .....	28
Figura 10. Red de área local con tres redes VLAN. ....	33
Figura 11. Configuración de conmutadores de una red con VLAN. [16] .....	34
Figura 12. Representación de un puerto trocal. [17] .....	34
Figura 13. Ubicación del protocolo 802.1q en la trama Ethernet. [17] .....	35
Figura 14. Cabecera ATM [18] .....	36
Figura 15. Ilustración de una red MPLS [18] .....	37
Figura 16. Flujo de un paquete MPLS [18] .....	38
Figura 17. Trama y cabecera MPLS [18] .....	39
Figura 18. Ubicación de MPLS en el modelo OSI [18].....	40
Figura 19. Intercambio de mensajes en las interfaces de los LDP [18] .....	41
Figura 20. Ilustración del envío de mensajes entre equipos corriendo MPLS [18].....	42
Figura 21. Ruta por defecto [19].....	44
Figura 22. IBGP y EBGP [24] .....	48
Figura 23. Ilustración de la capa de red en el Modelo OSI [20] .....	50
Figura 24. NAT traduce varias direcciones privadas a una dirección pública [29] .....	53
Figura 25. Conexión de red privada virtual [30].....	55
Figura 26. Peticiones a servidor DHCP [31].....	56
Figura 27. TCP/IP Organizational Tree [36] .....	66
Figura 28. Gráfica de uso de memoria vrs cantidad de router virtuales. ....	70
Figura 29. Sitio de descarga de RouteOS. ....	73
Figura 30. Ejecución de comandos en el Símbolo del Sistema. ....	74

Figura 31. Instalación de RouterOS. ....	74
Figura 32. Instalación de RouteOS exitosa. ....	75
Figura 33. Sistema operativo RouterOS. ....	75
Figura 34. Configuración de máquina virtual QEMU en GNS3.....	76
Figura 35. Configuración de interfaces de red.....	77
Figura 36. Cambio de símbolo de la máquina virtual. ....	77
Figura 37. Simulación de redes en GNS3 con router MikroTik. ....	78
Figura 38. Red a configurar enrutamiento estático.....	79
Figura 39. Red a configurar enrutamiento dinámico RIP. ....	80
Figura 40. Implementación de VLAN y DHCP.....	82
Figura 41. Implementación de OSPF de área única.....	87
Figura 42. Acceso a la interfaz gráfica mediante WinBox. ....	90
Figura 43. Creación de listas de direcciones. ....	91
Figura 44. Lista de direcciones.....	91
Figura 45. Configuración de políticas. ....	92
Figura 46. Reglas creadas para la cadena forward. ....	93
Figura 47. Reglas creadas para la cadena input.....	93
Figura 48. Sistema autónomo único para implementar iBGP.....	95
Figura 49. Muestra la implementación de túneles. ....	98
Figura 50. Ilustración para un Sistema MPLS.....	100
Figura 51. Muestra la opción para direccionar a weathermap desde Cacti.....	102
Figura 52. Muestra la opción para abrir el editor de mapas.....	102
Figura 53. Muestra la opción para agregar un mapa .....	102
Figura 54. Muestra los mapas creados en el editor.....	102
Figura 55. Muestra la opción para agregar un nodo .....	103
Figura 56. Muestra la opción para cambiar la imagen del nodo.....	103
Figura 57. Muestra la opción para cambiar el fondo del mapa .....	104
Figura 58. Muestra la opción para agregar enlaces entre nodos .....	104
Figura 59. Muestra la asignación de una gráfica al enlace entre nodos .....	104
Figura 60. Ventana emergente que muestra la lista de gráficas existente .....	105
Figura 61. Detalle de los nodos con los respectivos enlaces. ....	105

Figura 62. Opción para ir al menú de mapas de Cacti.....	105
Figura 63. Menú de mapas agregas a Cacti.....	105
Figura 64. Opción para agregar a Cacti los mapas creados en el editor .....	106
Figura 65. Mapa final con vista desde Cacti.....	106
Figura 66. Representación para que la red 10.0.0.0/24 tenga salida a internet.....	107
Figura 67. Muestra la implementación NAT y Port Forwarding.....	109

## INDICE DE TABLAS

Tabla 1. Comparación del modelo TCP/IP y el modelo OSI [2] .....	14
Tabla 2. Uso de los cables estructurados [2].....	19
Tabla 3. Licenciamiento RouterOS [12] .....	25
Tabla 4. Características en hardware de MikroTik [14].....	27
Tabla 5: Resumen de las características más relevantes de Routing y Switching. [15] .....	31
Tabla 6. Comparación entre ATM, IP y MPLS.....	43
Tabla 7. Categorías TCP/IP .....	65
Tabla 8. Características del simulador GNS3.....	69
Tabla 9. Características de los entornos de virtualización. [40].....	70



## INTRODUCCIÓN

En el presente documento se detalla el uso de una tecnología en redes de computadoras la cual está basada en el kernel de Linux, el Hardware es conocido como Router Board el cual es fabricado por la empresa MikroTik, del que se tienen diferentes modelos de los cuales se utilizó el RB750, el software que se montó se llama RouterOS y bajo este se realiza una investigación de sus funciones tanto en protocolos como capacidades.

El documento comprende dos capítulos, en el primero se presenta la documentación teórica que hace referencia a los temas específicos seleccionados con el fin de detallar las funciones y características de RouterOS, se presentan detalles físicos del Hardware, limitantes de sus capacidades, se profundiza en temas de enrutamiento estático y protocolos dinámicos, se detalla sobre MPLS como solución de un *backbone* para un proveedor de servicios de internet y se presentan temas relacionados con la seguridad en Networking. Como alternativa a la utilización de RouterOS se presentan métodos para realizar la emulación por computadora, analizando ventajas y desventajas dependiendo de la forma que se seleccione.

En el capítulo dos se desarrollan los temas definidos en el capítulo uno, detallando las configuraciones a realizar para cada tema, se inicia con el proceso de emulación de RouterOS, para dicho proceso se utilizó el entorno de virtualización Qemu ya que permite con una sola imagen emular todos los routers que nuestra computadora pueda soportar, su consumo de memoria es bajo, e interactúa directamente con la interfaz gráfica de GNS3. Posteriormente se detallan los comandos básicos ejemplificados con rutas estáticas y configuración de protocolos dinámicos como RIP y OSPF, luego se explica cómo levantar túneles GRE e IPIP, seguido se detalla como configurar un sistema MPLS, la creación de VPLS y como llevar un monitoreo de red por medio del protocolo SNMP. Finalmente se presentan las conclusiones y observaciones del trabajo realizado y las respectivas referencias bibliográficas en las que se respalda toda la información.

## OBJETIVOS

### OBJETIVO GENERAL

Implementar los protocolos de enrutamiento dinámicos, estáticos, MPLS y aplicaciones LAN mediante software libre para potencializar las habilidades y destrezas de los estudiantes en el área de comunicaciones de la escuela de ingeniería eléctrica.

### OBJETIVOS ESPECÍFICOS

1. Configurar los protocolos de enrutamiento dinámico tales como RIP, BGP, OSPF en una red para establecer comunicación entre los equipos de red.
2. Instalar y configurar el sistema operativo RouterOS trial versión en el entorno virtual GNS3 para simular las prácticas de laboratorio.
3. Realizar una guía de prácticas de laboratorio en las que se implementen los protocolos de enrutamiento y diversos servicios de red LAN utilizando software libre para que los estudiantes fortalezcan y apliquen los conocimientos teóricos adquiridos.
4. Instalar y configurar el software de visualización Cacti y el plugin adicional Weathermap para monitorear en tiempo real cada una de las interfaces de los router haciendo uso del protocolo SNMP.
5. Implementar los servicios básicos de una red LAN tales como servidor DHCP, Port forwarding y NAT para permitir que cualquier dispositivo de red tenga conectividad con la red local e internet.
6. Configurar y administrar redes virtuales (VLAN) en un router Mikrotik para escalar y optimizar la red local.
7. Adquirir los fundamentos de seguridad y establecer políticas de acceso a la red para minimizar los ataques cibernéticos.
8. Configurar redes privadas virtuales con diferentes protocolos de túnel VPN para mantener la privacidad e integridad de los datos de los usuarios.
9. Implementar el protocolo MPLS en una red para optimizar la red y analizar los beneficios obtenidos en cuanto a calidad de servicio y desempeño de la misma.

## ALCANCES

- Configuración de los protocolos de enrutamiento dinámico tales como RIP, BGP, OSPF en una red utilizando tecnología Mikrotik.
- Instalación y configuración del sistema operativo RouterOS trial versión en el entorno virtual GNS3 para la simulación de prácticas de laboratorio.
- Elaboración de una guía de prácticas de laboratorio en las que se implementen los protocolos de enrutamiento y diversos servicios de red LAN utilizando software libre en donde se apliquen los conocimientos teóricos adquiridos.
- Instalación y configuración del software de visualización Cacti y el plugin adicional Weathermap para el monitoreo en tiempo real cada una de las interfaces de los router haciendo uso del protocolo SNMP.
- Implementación de los servicios básicos de una red LAN tales como servidor DHCP, *Port forwarding* y NAT que permita que cualquier dispositivo de red tenga conectividad con la red local e internet.
- Configuración y administración redes virtuales (VLAN) en un equipo con el sistema operativo RouterOS que permita escalar y optimizar la red local.
- Aplicación de los fundamentos de seguridad y establecimiento de políticas de acceso a la red que minimicen los ataques cibernéticos.
- Configuración de redes privadas virtuales con diferentes protocolos de túnel VPN que aseguren la privacidad e integridad de los datos de los usuarios.
- Implementación y construcción física de una red utilizando el protocolo MPLS utilizando la tecnología Mikrotik.

## DEFINICIONES Y ABREVIATURAS

### DEFINICIONES

**DOMINIO DE COLISIÓN:** Es un segmento físico de una red de computadores donde es posible que las tramas puedan "colisionar" (interferir) con otras. Estas colisiones se dan particularmente en el protocolo de red Ethernet.

**DOMINIO DE BROADCAST:** es el área lógica en una red de en la que cualquier computadora conectado puede transmitir directamente a cualquier otro equipo en el dominio sin precisar ningún router, dado que comparten la misma subred.

**VLAN:** acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física

**LAN:** son las siglas de Local Área Network, Red de área local. Una LAN es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada (como una habitación, un edificio, o un conjunto de edificios)

**UDP:** Protocolo del nivel de transporte basado en el intercambio de datagramas (Encapsulado de capa 4 Modelo OSI).

**MULTIDIFUSIÓN:** (inglés multicast) es el envío de la información en múltiples redes a múltiples destinos simultáneamente.

**CRIPTOGRAFÍA:** Una clave, palabra clave o clave criptográfica es una pieza de información que controla la operación de un algoritmo de criptografía. Habitualmente, esta información es una secuencia de números o letras mediante la cual, en criptografía, se especifica la transformación del texto plano en texto cifrado, o viceversa.

## ABREVIATURAS

ACD: *Automatic Call Distributor*

ARP: Address Resolution Protocol, Protocolo de Resolución de Direcciones

ASCII: American Standard Code for Information Interchange.

ASP: Appletalk Session Protocol

BFIFO: Byte limited First In, First Out

BGP: Border Gateway Protocol, Protocolo de gateway fronterizo

BSD: Sistema operativo derivado del sistema Unix.

CDP: Cisco Discovery Protocol, Protocolo de descubrimiento de Cisco

CIDR: Classless Inter-Domain Routing

CPU: Central Processing Unit, Unidad central de proceso

CSMA/CD: Carrier Sense Multiple Access with Collision Detection

CTI: *Computer telephony integration*

DECnet: Digital Equipment Corporation network

DHCP: Dynamic Host Configuration Protocol

DHCP: Dynamic Host Configuration Protocol

DNAT: Destination NAT (por destino)

DNS: Domain Name System - Sistema de nombres de dominio

DSCP: Differentiated Services Code Point

EBCDIC: Extended Binary Coded Decimal Interchange Code

ECMP: Equal-cost multi-path routing

EIA/TIA: Electronic Industries Alliance / Telecommunications Industry Association

ESP: El protocolo proporciona autenticidad de origen, integridad y protección de confidencialidad de un paquete.

ETSI: European Telecommunications Standards Institute

FTP: File Transfer Protocol, Protocolo de Transferencia de Archivos

FTP: Foiled twisted pair, Par trenzado con blindaje global

GPRS: General Packet Radio Service, Servicio general de paquetes vía radio

GSM: Global System for Mobile communications, Sistema global para las comunicaciones móviles

GUI: Graphical user interface, Interfaz gráfica de usuario

HDLC: High-Level Data Link Control, control de enlace de datos de alto nivel

Host: Computadoras conectadas a una red.

HSSI: High-Speed Serial Interface

HTTP: Hypertext Transfer Protocol, Protocolo de Transferencia de Hipertexto

ICMP: Internet Control Message Protocol, Protocolo de Mensajes de Control de Internet

IDE: Integrated development environment, Entorno de desarrollo integrado

IEC: International Electrotechnical Commission, Comisión Electrotécnica Internacional

IEEE: Institute of Electrical and Electronics Engineers, Instituto de Ingenieros

IETF: Internet Engineering Task Force

IGRP: Interior Gateway Routing Protocol, Protocolo de enrutamiento de gateway interior

IKE: Internet key exchange, es un protocolo usado para establecer una Asociación de Seguridad (SA) en el protocolo IPsec

IP: Internet Protocol, Protocolo de Internet

IPX/SPX: Protocolo Novell o simplemente IPX es una familia de protocolos de red desarrollados por Novell.

IPX: Internetwork Packet Exchange, Intercambio de paquetes interred

ISO: International Organization for Standardization, Organización Internacional de Normalización

ISP: Proveedor de servicios de Internet.

IVR: *Interactive Voice Response*

L2TP: Layer 2 Tunneling Protocol

LAN: Local Área Network, Red de Área Local

LAN: Red de área local.

LLC: Logical Link Control, Control Lógico del Enlace

MAC: Media Access Control, Control de Acceso al Medio

MAN: Metropolitan Area Network, Red de Área metropolitana

MD5: Message-Digest Algorithm 5. Es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

MIB: Management Information Base

MIDI: Musical Instrument Digital Interface, Interfaz Digital de Instrumentos Musicales

MPEG: Moving Picture Experts Group

MPLS: Multiprotocol Label Switching

NAT: Network Address Translation, Traducción de direcciones de red

NFS: Network File System, Sistema de archivos de red

OSI: Open System Interconnection, Interconexión de Sistemas Abiertos

OSPF: Open Shortest Path First

PCI: Peripheral Component Interconnect, Interconexión de Componentes Periféricos

PCIe: Peripheral Component Interconnect Express

PCQ: Packet Classification and Queuing

PDU: Protocol Data Unit, Unidad de datos de Protocolo

PFIFO: Packet limited First In, First Out

POP3: Post Office Protocol, Protocolo de Oficina Postal

PPP: Point to Point Protocol, Protocolo Punto a Punto

PPTP: Point to Point Tunneling Protocol

PVC: Polyvinyl chloride, Policloruro de vinilo

QoS: Quality of Service, Calidad de Servicio

RADIUS: Remote Authentication Dial-In User Server, Servidor de Autorización para aplicaciones de acceso remoto a la red

RARP: Reverse Address Resolution Protocol, Protocolo de resolución de direcciones inverso

RDSI: Red Digital de Servicios Integrados (RDSI, en inglés: ISDN)

RED: Random Early Detection

RF: Radiofrecuencia

RFC: *Request for Comments*

RIP: Routing Information Protocol, Protocolo de Información de Enrutamiento

RPC: Remote Procedure Call, Llamada a Procedimiento Remoto

RRDtool: *Round Robin Database Tool*

RS-232: Recommended Standard 232, Estándar Recomendado 232

SFP: Small form-factor pluggable

SHOUTcast: Es una tecnología de streaming auditiva.

SIP: Session Initiation Protocol

SNA: Systems Network Architecture, Sistema de arquitectura de red

SNAT: Source NAT (por origen).

SNMP: Simple Network Management Protocol

SNMP: Simple Network Management Protocol, Protocolo Simple de Administración de Red

SQL: Structured Query Language, Lenguaje de consulta estructurado

SSH: Secure Shell

SSH: Secure SHell, o intérprete de órdenes segura.

STP: Shielded twisted pair, Par trenzado blindado

TCP: Protocolo de Control de Transmisión.

TCP: Transmission Control Protocol, Protocolo de Control de Transmisión

TELNET: Teletype Network

TIFF: Tagged Image File Format, Formato de archivo de imágenes con etiquetas

UDP: User Datagram Protocol

UDP: User Datagram Protocol, Protocolo de Datagrama de Usuario

UMTS: Universal Mobile Telecommunications System, Sistema universal de telecomunicaciones móviles

UTP: Unshielded Twisted Pair, Par trenzado no Apantallado

VLSM: Máscaras de subred de tamaño variable.

VPN: Virtual private network, Red privada virtual

VRF: Virtual routing and forwarding

WAN: Wide Área Network, Red de Área Amplia

WLAN: Wireless Local Area Network, Red de Área Local Inalámbrica



### REFERENCIA TEÓRICA

En el presente capítulo se detalla la información teórica que respalda el tema “Implementación de protocolos de enrutamiento y servicios para una Red de Área Local mediante software libre”, se segmenta en base al modelo OSI el cual se explica brevemente para comprender el orden jerárquico de las capas, se detalla desde los medios físicos e interfaces, niveles de voltaje, características del hardware usado, se explican las capacidades y aplicaciones, manejo de red y modelos de las placas RouterBoard, los cuales están relacionados a la capa uno.

Se definen las características de switching en las que se describe como se direccionan las tramas en capa dos, se detallan las vlan y los puertos troncales o conocidos por el protocolo IEEE 802.1q. Se presentan los conceptos de MPLS desde su estructura, aplicación, características y funcionamiento hasta la comparación de beneficios obtenidos contra redes ATM e IP.

En capa tres se detallan los protocolos de enrutamiento y los protocolos enrutables, se explica el concepto de rutas estáticas y rutas por defecto.

Se tocan también aspectos de seguridad, dentro de Networking este es un tema muy importante ya que constantemente se está investigando y tratando de desarrollar redes lo más confiables en cuanto a protección de la información.

Dentro de aplicaciones para redes de área local se explica la asignación de parámetros de red y DNS por medio de DHCP, se detallan conceptos de telefonía IP, se explica brevemente el protocolo SIP y el funcionamiento de una central telefónica. También se abordan conceptos sobre el protocolo SNMP, agregando detalles sobre el funcionamiento de los árboles mib y el orden jerárquico que llevan, se detalla sobre la herramienta de monitoreo Cacti y se presenta el plugin weathermap.

Finalmente se presenta información sobre la emulación de RouterOS en GNS3, detallando los hipervisores existentes y comparando ventajas y desventajas.

## 1.1 INTRODUCCIÓN A LAS REDES DE COMPUTADORA

Un elemento fundamental para la comprensión de los procesos involucrados en la transmisión de datos sobre medios de *networking* son los modelos teóricos que permiten explicar y comentar la función de cada uno de los elementos que intervienen en la comunicación.

Muchos son los modelos desarrollados hasta el momento: el modelo SNA, el modelo Novell NetWare, el modelo TCP/IP, el modelo OSI, entre otros. La mayoría de ellos son modelos de capas que dividen las diferentes tareas en módulos independientes, lo que facilita la comprensión y por sobre todo el desarrollo.

El modelo de referencia OSI se ha convertido en el modelo principal para la definición de arquitecturas en la interconexión de los sistemas de comunicaciones. Aunque existen otros modelos, la mayoría de los fabricantes de redes relacionan sus productos con el modelo de referencia OSI.

## 1.2 MODELO OSI. [1]

El modelo de interconexión de sistemas abiertos (ISO/IEC 7498-1), más conocido como “modelo OSI” (en inglés, *OpenSystem Interconnection*), es el modelo de red descriptivo, que fue creado en el año 1980 por la Organización Internacional de Normalización (ISO, *International Organization for Standardization*).

Fue creado a partir de los modelos DecNet, SNA y TCP/IP para solucionar los problemas surgidos por el desarrollo de diferentes estándares.

Describe como los datos y la información de la red fluye desde una terminal, a través de los medios de red, hasta otra terminal. Es importante que todos los dispositivos de la red hablen el mismo lenguaje o protocolo. Un protocolo es un conjunto de reglas que hacen que la comunicación en una red sea más eficiente.

Con este objetivo divide el proceso global en grupos lógicos más pequeños de procesos a los que denomina “capas” o “*layers*”. Por este motivo se habla de una “arquitectura de capas”. [2]

### 1.2.1 SIETE CAPAS DEL MODELO OSI

Capa 7: La capa de Aplicación. Su principal función es brindar servicios de red al usuario final. Es función de esta capa establecer la disponibilidad de la otra parte de la comunicación que se intenta lograr, sincronizar las aplicaciones, establecer acuerdos sobre recuperación de errores y control de integridad de los datos, a la vez que determina si hay suficientes recursos para la comunicación que se intenta.

Protocolos que operan en esta capa: http, pop3, snmp, ftp, telnet, etc.

Capa 6: La capa de Presentación. Provee servicios de formateo de datos a la capa de Aplicación. No todas las aplicaciones de red requieren este tipo de servicios.

Algunos servicios de esta capa son la encriptación de datos la compresión y traslación.

Determina la sintaxis de la transferencia de datos.

Protocolos que operan en esta capa: pict, tiff, jpeg, midi, mpeg, quicktime, EBCDIC, ASCII, etc.

Capa 5: La capa de Sesión. Establece, administra y termina las sesiones de comunicación entre aplicaciones en diferentes nodos. Ofrece algunos mecanismos de recuperación y control de datos entre las aplicaciones coordinadas de los nodos.

Protocolos que operan en esta capa: NFS, SQL, RPC, X-Windows, ASP (*Appletalk Session Protocol*).

Capa 4: La capa de transporte. Esta capa requiere de software adicional en la terminal que opera como cliente de red. Este software recibe el flujo de datos generados desde la aplicación y lo divide en pequeños trozos denominados "segmentos". Cada segmento recibe un encabezado que identifica la aplicación de origen utilizando puertos.

Su objetivo es asegurar el transporte y regular el flujo de información entre origen y destino de modo confiable y preciso.

Los protocolos de capa de transporte pueden asegurar comunicaciones *end to end* provistas de control de flujo utilizando el método de ventana deslizante y corrección de

errores. Además asegura la fiabilidad de los datos utilizando números de secuencia y de reconocimiento. TCP utiliza un intercambio de triple vía en el inicio de la transacción entre origen y destino para las pruebas de transporte.

Los servicios de la capa de transporte se pueden sintetizar de la siguiente manera:

- Segmentación del flujo de datos.
- Establecimiento de un circuito virtual extremo a extremo.
- Transporte de segmentos entre extremos.
- Control del flujo de datos a través de la implementación de ventanas deslizantes.
- Confiabilidad de la transmisión por la utilización de números de secuencia y acuses de recibo.

Con el propósito de que múltiples aplicaciones puedan compartir una única conexión de transporte, manteniendo identificado el flujo de datos que corresponde a cada una de ellas, utiliza números de puerto que permiten identificar sesiones de diferentes aplicaciones. El número o ID de puerto es un valor que oscila entre 1 y 65535.

- Los puertos del 1 al 1023 son los "puertos conocidos" o reservados. En términos generales, están reservados para procesos del sistema (daemons) o programas ejecutados por usuarios privilegiados.
- Los puertos del 1024 al 49151 son los "puertos registrados". Son los utilizados por el cliente para iniciar una sesión.
- Los puertos del 49152 al 65535 son los "puertos dinámicos y/o privados"

Ventana deslizante (windowing): Es la técnica que controla la cantidad de información enviada de extremo a extremo expresada en cantidad de bytes sin requerir una confirmación.

Protocolos que operan en esta capa: TCP y UDP.

Capa 3: La capa de Red. Proporciona direccionamiento jerárquico y selección de la mejor ruta. Routing de IP, ICMP, ARP, RARP considerando el direccionamiento lógico.

Para posibilitar la determinación de la ruta, el servicio de routing suministra:

- Inicialización y mantenimiento de tablas de enrutamiento.
- Procesos y protocolos de actualizaciones de enrutamiento.
- Especificaciones de direcciones y dominios de enrutamiento.
- Asignación y control de métricas de ruteo.

Protocolos que operan en esta capa: IP, IPX, Apple Talk, RIP, IGRP.

Dispositivos que operan en esta capa: Routers, Switches capa 3.

Capa 2: La capa de Enlace de Datos. Brinda una interfaz con el medio físico, control de acceso al medio y direccionamiento físico. En esta capa se determina la topología sobre la que operara la red.

En entornos Ethernet, el direccionamiento físico se realiza utilizando direcciones MAC de 48 bits (6 bytes):

- 24 bits identifican al fabricante (3 bytes).
- 24 bits que constituyen el número de serie (3 bytes).

En la operación de Ethernet se divide en dos subcapas: LLC y MAC. La subcapa LLC es responsable de la estructuración de la trama, el direccionamiento y las funciones de control de error. La subcapa MAC es responsable del acceso al medio.

Protocolos que operan en esta capa: CSMA/CD, CDP, Ethernet, 802.3

Dispositivos que operan en esta capa: Bridges, switches LAN.

Capa 1: La capa Física. Es la capa responsable de transmisión de la señal entre puertos. Define las especificaciones eléctricas, mecánicas, de procedimiento y funcionales para activar, mantener y desactivar el enlace físico entre sistemas finales.

Puede tratarse de cables y conectores metálicos, fibra óptica o utilizarse el medio atmosférico (infrarrojo, microondas, etc.)

Cables y conectores: RS-232, RJ-45, v.24, v.35, x.21, g.703, hssi, etc

Dispositivos que operan en esta capa: Repetidores, hubs

El modelo TCP/IP es el estándar histórico y técnico de la Internet creado por el Departamento de Defensa de EE.UU. Aunque algunas de las capas del modelo TCP/IP tienen el mismo nombre que las capas del modelo OSI, las capas de ambos modelos no se corresponden de manera exacta. En la tabla 1 se comparan las capas de ambos modelos y los protocolos que operan en cada capa.

TCP/IP	OSI	Protocolos
Procesos de Aplicación	Aplicación	Telnet, HTTP, SNMP, SMTP
	Presentación	JPG, MP3
	Sesión	NFS, Linux, X-Windows
Transmisión	Transporte	TCP, UDP
Internet	Red	ICMP, ARP, RARP, IP
Acceso a Red	Enlace de datos	Ethernet, PPP, HDLC
	Física	RJ-45, V-35

Tabla 1. Comparación del modelo TCP/IP y el modelo OSI [2]

Ventajas de un modelo de capas:

- Divide la comunicación de red en partes más pequeñas y fáciles de manejar.
- Permite la interoperabilidad de diferentes fabricantes.
- Permite a los distintos tipos de hardware y software de red comunicarse entre sí.
- Evita que los cambios en una capa afecten las otras capas.
- Divide la comunicación de red en partes más pequeñas para simplificar el aprendizaje y la resolución de fallos.

### 1.2.2 UNIDADES DE DATOS. [1]

El intercambio de información entre dos capas OSI consiste en que cada capa en el sistema fuente le agrega información de control a los datos, y cada capa en el sistema de destino analiza y quita la información de control de los datos como sigue:

Si una computadora (A) desea enviar datos a otra (B), en primer término los datos deben empaquetarse a través de un proceso denominado encapsulamiento, es decir, a medida que los datos se desplazan a través de las capas del modelo OSI, reciben encabezados, información final y otros tipos de información. Del mismo modo, el equipo receptor deberá realizar también una serie de tareas que le permitan recuperar los contenidos originales denominada desencapsulamiento.

Durante este proceso, cada protocolo de capa intercambia información, que se conoce como *unidades de datos de protocolo (PDU)*, entre capas iguales. Cada capa de comunicación, en el computador origen, se comunica con un PDU específico de capa y con su capa igual en el computador destino como se ilustra en la figura 1.



Figura 1. Las siete capas del modelo OSI [3]

En la figura 2 se muestra el proceso de encapsulamiento de los datos mencionado anteriormente a través de las diferentes capas hasta llegar al medio físico donde serán transmitidos.

Los nombres que recibe cada agrupamiento de datos en cada capa del modelo OSI son:

- APDU: (capa 7) unidad de datos en la capa de aplicación.
- PDU: (capa 6) unidad de datos en la capa de presentación.
- SPDU: (capa 5) unidad de datos en la capa de sesión.

- Segmento: (capa 4) unidad de datos en la capa de transporte.
- Paquete: (capa 3) unidad de datos en el nivel de red.
- Trama: (capa 2) unidad de datos en la capa de enlace.
- Bit: (capa 1) unidad de datos en la capa física.

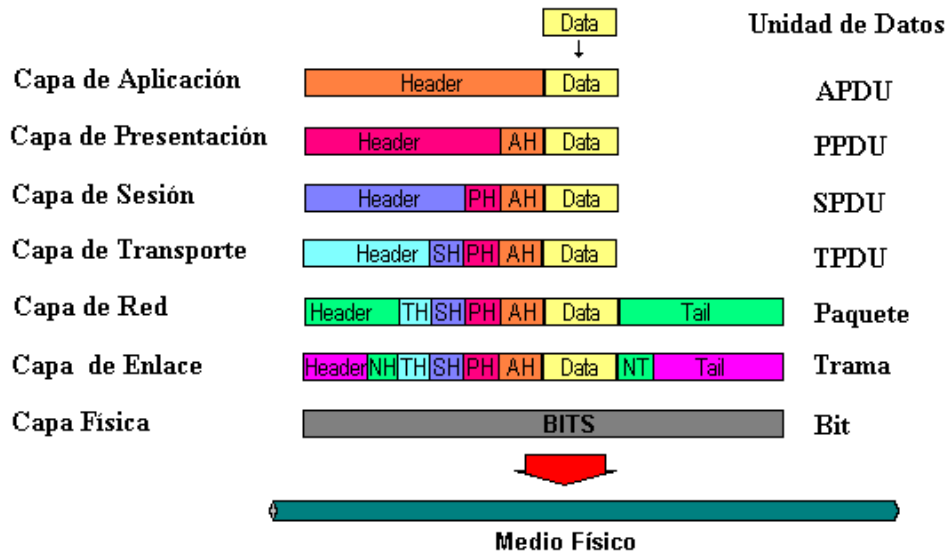


Figura 2. Proceso de encapsulamiento de datos [1]

### 1.2.3 MEDIOS FÍSICOS

En *networking*, un medio es el material a través del cual viajan los paquetes de datos.

Estos se dividen en:

1. Medios de cobre
2. Medios ópticos
3. Medios inalámbricos

#### 1.2.3.1 MEDIOS DE COBRE [2]

Cable coaxial: es un cable utilizado para transportar señales eléctricas de alta frecuencia que posee dos conductores concéntricos, uno interno, llamado núcleo, encargado de llevar la información, y uno exterior, de aspecto tubular, llamado malla, blindaje o trenza, que sirve como referencia de tierra y retorno de las corrientes. Entre ambos se encuentra una capa aislante llamada dieléctrico, de cuyas características dependerá principalmente



la calidad del cable. Hay diferentes tipos de cables coaxiales, los más utilizados en el tendido de redes Ethernet son: Thicknet (cable coaxial grueso) y Thinnet (cable coaxial fino). En la figura 3 se muestran las partes del cable coaxial.

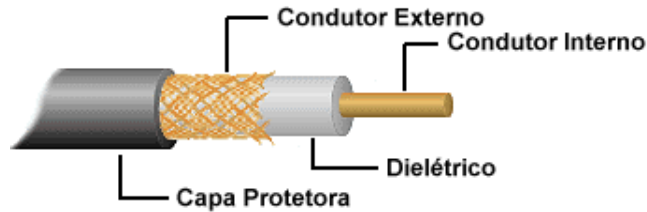


Figura 3. Partes del cable coaxial [4]

Cable de par trenzado de cobre: Este cable está especialmente diseñado para redes de comunicaciones. Se compone de 8 hilos (4 pares) de cobre aislados entre si y trenzados en pares para lograr el efecto de cancelación y blindaje que le permite rechazar interferencias electromagnéticas y de radiofrecuencia. Hay 3 variantes de cable de cobre de par trenzado: UTP, STP y FTP.

En la figura 4 se muestran las partes de uno de los cables más utilizados, el cable de par trenzado sin blindaje (UTP).

### Par trenzado sin blindaje (UTP)

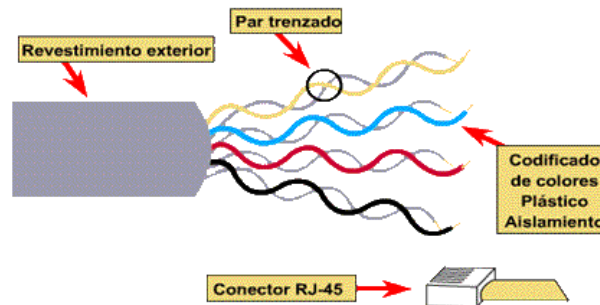


Figura 4. Partes del cable de par trenzado sin blindaje (UTP) [5]

### Normativa para Cableado Estructurado

La EIA/TIA regula la normativa para la instalación de cableado estructurado. Por cableado estructurado entendemos una instalación de cableado de cobre y fibra óptica estándar que asegura una infraestructura de transmisión óptima para cualquier sistema de comunicaciones de voz, video o datos.

El estándar EIA/TIA 568 establece dos formatos básicos para el armado de conectores RJ-45: 568A y 568B. La disposición de los cables para cada formato se muestra en la figura 5.

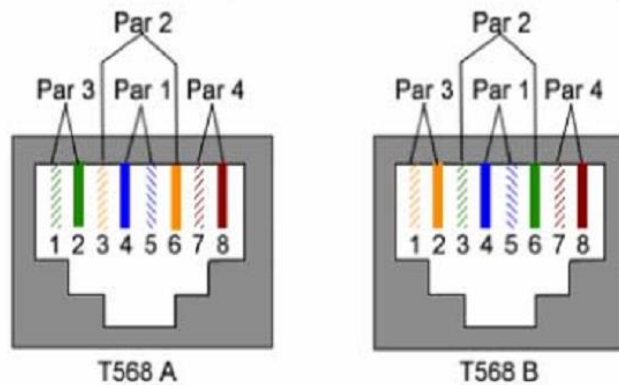


Figura 5. Estándares EIA/TIA T568A y T568B [2]

Estos 2 formatos básicos permiten el armado de diferentes tipos de cable que se muestran en la figura 4, de acuerdo a diferentes necesidades descritas en la tabla 2.

Los diferentes tipos de cable se diferencian por el formato utilizado en cada uno de sus extremos:

- Cable recto: Utiliza el mismo formato en ambos extremos del cable.
- Cable cruzado: Utiliza diferente formato en ambos extremos del cable.
- Cable consola: en este caso el orden de los alambres en un extremo del cable es el espejo exacto del otro extremo.

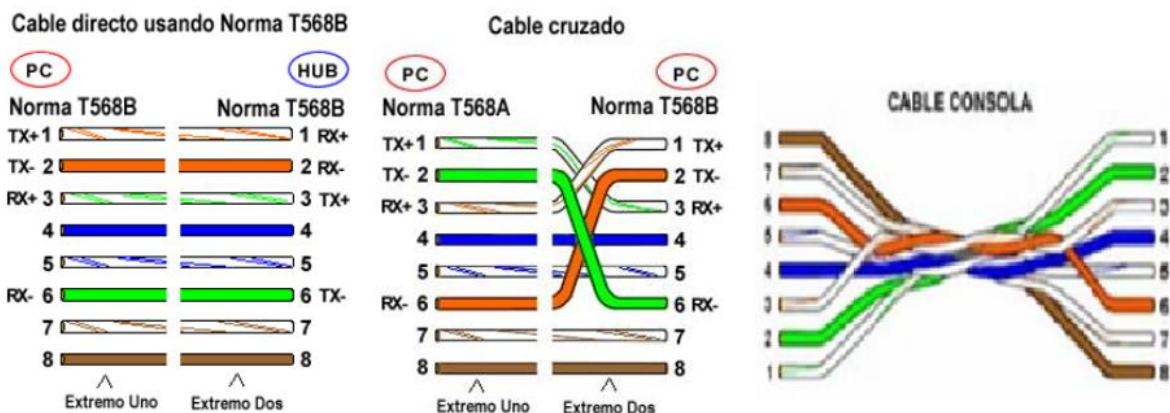


Figura 6. Tipos de cable estructurado para redes de datos [2]

Tipo de cable	Aplicación
<b>Cable Recto</b>	<ul style="list-style-type: none"> <li>▪ Router a hub o switch</li> <li>▪ Servidor a hub o switch</li> <li>▪ Estación de trabajo a hub o switch</li> </ul>
<b>Cable Cruzado</b>	<ul style="list-style-type: none"> <li>▪ Uplinks entre switches</li> <li>▪ Hubs a switches</li> <li>▪ Hub a hub</li> <li>▪ Router a router</li> <li>▪ Conectar dos terminales directamente</li> </ul>
<b>Cable consola</b>	<ul style="list-style-type: none"> <li>▪ Conexión al puerto consola de un dispositivo</li> </ul>

Tabla 2. Uso de los cables estructurados [2]

### 1.2.3.2 MEDIOS DE FIBRA ÓPTICA

La fibra óptica es un medio de transmisión, empleado habitualmente en redes de datos, consistente en un hilo muy fino de material transparente, vidrio o materiales plásticos, por el que se envían pulsos de luz que representan los datos a transmitir. Las partes del cable de fibra óptica se muestran en la figura 7.

Hay 2 tipos básicos de fibra óptica a considerar: fibra monomodo y fibra multimodo.

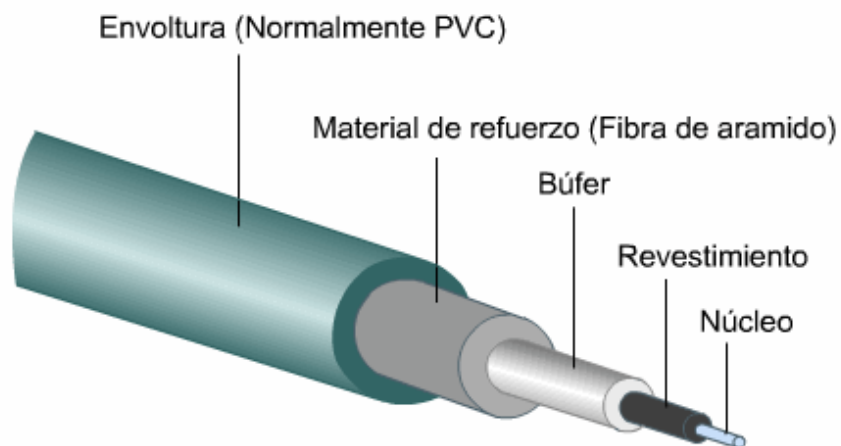


Figura 7. Cable para transmisión de luz [6]

### 1.2.3.3 MEDIOS INALÁMBRICOS

Estos comprenden un conjunto muy amplio de tecnologías inalámbricas, básicamente son aquellos que se encargan de enviar señales electromagnéticas mediante frecuencias de microondas y radiofrecuencias que representan los dígitos binarios de las comunicaciones de datos.

Algunas de las principales tecnologías inalámbricas se muestran en la figura 8 junto con sus estándares.

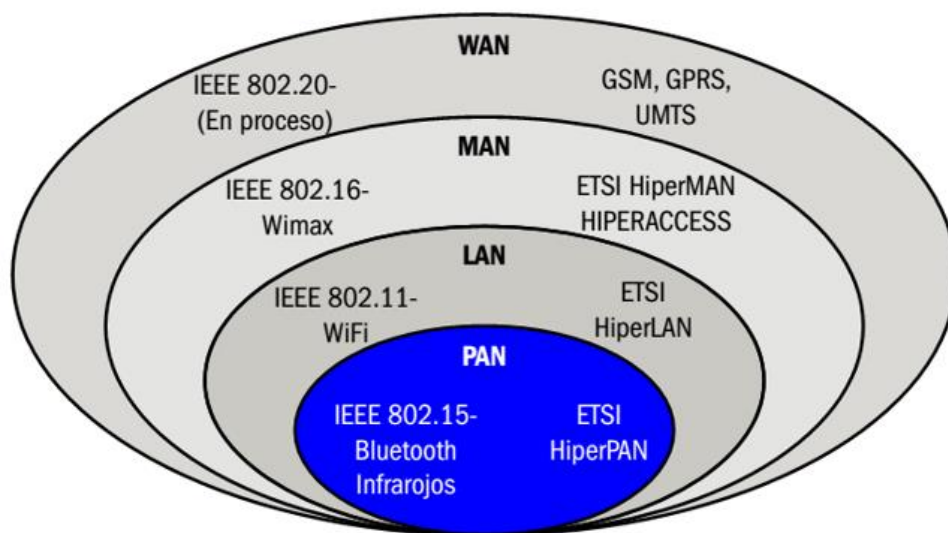


Figura 8. Tecnologías inalámbricas y sus estándares [7]

### 1.3 MIKROTIK HARDWARE

MikroTik Ltd., conocida internacionalmente como MikroTik, es una compañía letona proveedora de tecnología disruptiva de hardware y software para la creación de redes. La compañía fue fundada en el 1995, aprovechando el emergente mercado de la tecnología inalámbrica. Se dedica principalmente a la venta de productos de hardware de red como *routers* denominados *Routerboards* y *switches* también conocidos por el software que lo integra, denominado RouterOS y SwOS. [8]

MikroTik es actualmente considerada como una de las grandes empresas de Networking, compitiendo con grandes fabricantes como Cisco, Juniper, 3Com, D-Link, etc., entre sus clientes y casos de éxito se pueden nombrar a: SIEMENS, IPASS, HP, ERICSSON, Mitsubishi,

RIPE, El Departamento de Estado de los Estados Unidos de América, Motorola, Vodafone, ABB y la NASA. [9]

La principal diferencia de MikroTik frente al resto de marcas en el mercado, es su bajo costo de sus licencias y la amplia capacidad de adaptación a operaciones de networking, con lo cual su uso se ha extendido de forma extraordinaria y rápidamente.

### 1.3.1 ROUTEROS [10]

RouterOS es un sistema operativo de la empresa MikroTik basado en el Kernel de Linux, que permite convertir un equipo x86 común o una placa RouterBOARD en un router dedicado.

El sistema RouterOS fue creado por 2 estudiantes de Latvia como tesis universitaria para diseñar un router basado en Linux que permita equiparar las funcionalidades de otros routers que se encontraban en el mercado. Con el pasar del tiempo se han integrado varias aplicaciones dentro del sistema, como: soluciones de telefonía IP, administración de protocolo BGP, integración de Ipv6, servidor de VPN's, administración de ancho de banda, calidad de servicio (QoS), administración de hotspots, puntos de acceso inalámbrico, backhaul inalámbrico, etc.

### 1.3.2 CARACTERÍSTICAS PRINCIPALES DE ROUTEROS [11]

RouterOS es basado en el Kernel 2.6 de Linux, soporta multi-core (varios núcleos), y computadores multi-CPU (SMP- Symmetric Multiprocessing), la instalación y ejecución puede ser desde discos IDE, HDDs, CF, memorias USB, SSD disk.

Soporta varios métodos de acceso para su configuración: acceso local, con teclado y monitor, por consola mediante puerto serial, Telnet, secure SSH, interface WEB, además de una interface GUI (graphical user interface) propia llamada Winbox; también soporta una conexión a nivel de MAC address llamada Mac-Telnet.

### 1.3.3 FIREWALL

El Firewall implementa filtrado de paquetes que es usado para administrar el flujo de datos desde y a través del router. Junto con el NAT (Network Address Translation) previene el acceso no autorizado a redes internas.

El filtrado puede ser por direcciones IP, rango de direcciones IP, por puerto, rango de puerto, protocolo IP, DSCP (Differentiated Services Code Point) y otros parámetros. Soporta también direccionamiento IP estático y dinámico, además de implementar características de capa 7. Permite detectar ataques por denegación de servicio (DoS)

### 1.3.4 CALIDAD DE SERVICIO QOS

RouterOS puede implementar QoS (802.11Q):

- Tipo de colas: RED (Random Early Detection), BFIFO (Byte limited First In, First Out queue), PFIFO (Packet limited First In, First Out queue), PCQ (Packet Classification and Queuing)
- Colas simples: por origen/destino de red, dirección IP de cliente, por interface
- Árboles de colas: por protocolo, por puerto, por tipo de conexión.

### 1.3.5 ROUTING

RouterOS soporta ruteo estático, y dinámico.

- Para IPv4 soporta RIP v1 y v2, OSPF v2, BGP.
- Para IPv6 soporta RIPng, OSPF v3 y BGP.

RouterOS soporta también Virtual Routing and Forwarding (VRF), ruteo basado en políticas, ruteo basado en interfaces, y ruteo ECMP (Equal-cost multi-path routing). Implementa el protocolo de ruteo MPLS (Multiprotocol Label Switching), el cual trabaja entre la capa 2 y 3 del modelo OSI, y es comúnmente utilizado para manejo y administración de redes de alto rendimiento.

### 1.3.6 SERVIDOR / CLIENTE

RouterOS incorpora varios servicios como servidor o cliente:

- DHCP (Dynamic Host Configuration Protocol)

- Túneles tipo PPPoE (Point to Point Protocol over Ethernet)
- Túneles PPTP (Point to Point Tunneling Protocol)
- Relay de DHCP (Dynamic Host Configuration Protocol)
- Cache web-proxy
- Gateway de Hotspot
- VPN (virtual private network)

### 1.3.7 WIRELESS

RouterOS soporta una variedad de tecnologías inalámbricas, puede trabajar con diferentes configuraciones para diferentes aplicaciones, por ejemplo; Backhaul para enlaces punto a punto, Access Point para enlaces multipunto, Hotspot.

Soporta estándares IEEE802.11a/b/g/n, maneja protocolos propietarios: Nstreme y Nstream2 (dual) que permiten extender el rango de cobertura y velocidad, puede administrar redes Wireless MESH (malla) y HWMP (Hybrid Wireless Mesh Protocol) para incrementar zonas de cobertura de la red inalámbrica.

### 1.3.8 HERRAMIENTAS DE MANEJO DE RED

RouterOS ofrece un buen número de herramientas:

- Ping, traceroute
- Medidor de ancho de banda
- Contabilización de tráfico
- SNMP
- Torch
- Sniffer de Paquetes

### 1.3.9 LICENCIAMIENTO [12]

RouterOS para ser activado requiere una licencia de nivel de aplicaciones, es decir existen varias licencias con limitaciones o características adicionales dependiendo del tipo de aplicación de red que se requiera.

Las licencias de nivel 0 es una licencia demo, habilita todas sus funciones durante un periodo de 24 horas después de ello debe de ser reinstalado. La licencia de nivel 1 es gratuita pero requiere registrarse en [www.mikrotik.com](http://www.mikrotik.com) y tiene limitaciones. La licencia de nivel 2 fue una licencia de transición e investigación, por lo que no se encuentran disponibles.

La licencia de nivel 3 fue una licencia que operaba con características limitadas, y permitía el uso de interfaces inalámbricas solo para trabajar en modo cliente.

La principal diferencia entre las licencias de nivel 4, 5 y 6, son la cantidad de túneles permitidos por nivel, en la tabla 3 se muestra los niveles de licenciamiento y sus características.

Para el uso de BGP sobre x86 es necesario RouterOS v4x.

MikroTik periódicamente revisa y actualiza su sistema operativo, en cada actualización implementa o modifica características de RouterOS, estas actualizaciones son llamadas versiones y existen para cada tipo de licencia.

NIVEL	0 (TRIAL)	1 (DEMO)	3 (WISP CPE)	4 (WISP)	5(WISP)	6 (Controller)
Precio/ Características	No requiere licencia	Requiere registro	Solamente grandes pedidos	\$45	\$95	\$250
Soporte en línea	-	-	-	15 días	30 días	30 días
Wireless AP	24h limite	-	-	si	si	si
Wireles Client y Bridge	24h limite	-	si	si	si	si
Protocolos RIP, OSPF, BGP	24h limite	-	Si(*)	si	si	si
EoIP tuneles	24h limite	1	Ilimitados	Ilimitados	Ilimitados	Ilimitados
PPPoE túneles	24h limite	1	200	200	500	Ilimitados
PPTP túneles	24h limite	1	200	200	500	Ilimitados
L2TP túneles	24h limite	1	200	200	500	Ilimitados
OVPN túneles	24h limite	1	200	200	Ilimitados	Ilimitados
VLAN Interfaces	24h limite	1	Ilimitados	Ilimitados	Ilimitados	Ilimitados



NIVEL	0 (TRIAL)	1 (DEMO)	3 (WISP CPE)	4 (WISP)	5(WISP)	6 (Controller)
Usuarios activos HotSpot	24h limite	1	1	200	500	Ilimitados
Cliente RADIUS	24h limite	-	si	si	si	si
Colas	24h limite	1	Ilimitados	Ilimitados	Ilimitados	Ilimitados
Web proxy	24h limite	-	si	si	si	si
Sesiones activas de administración	24h limite	1	10	20	50	Ilimitados

Tabla 3. Licenciamiento RouterOS [12]

### 1.3.10 MODELOS DE PLACAS ROUTERBOARD (RB) [13]

Se ha fabricado varios modelos de placas MikroTik RouterBoard, los cuales varían entre ellos según la velocidad del procesador, el número de interfaces que admite cada placa, o el tipo de licenciamiento que viene de fábrica, con la posibilidad de cambiar la licencia en cualquier modelo.

En estas placas el nombre del producto describe las capacidades físicas de ésta (con excepciones menores para algunos productos antiguos) de la siguiente manera:

Los primeros 3 dígitos del nombre indican la serie y número de interfaces:

Primer dígito - Es el número de serie

Segundo dígito - Indica el número de interfaces cableadas (Ethernet, SPF, SPF+)

Tercer dígito - Indica el número de interfaces inalámbricas o ranuras PCI

Los siguientes dígitos y letras indican las características de la placa:

U - puerto USB

P - provee POE o alimentación sobre Ethernet

AH - indica mayores capacidades con respecto al CPU y memoria RAM

G - designa capacidad Gigabit para los puertos Ethernet

L - versión de bajo costo

S - puerto SFP

e - tarjeta de expansión PCIe

x<N> - donde N es el número de CPU (x2, x16, x36, etc.)

Tipo de caja

BU - tarjeta sin caja

RM - para montaje en rack

IN - para montaje en interiores

OUT - para montaje en exteriores

SA - alojamiento de antena de sector

HG - alojamiento de antena de alta ganancia

EM - memoria extendida

Otras designaciones para dispositivos con interfaces inalámbricas:

2 - Después del modelo indica banda de operación de 2.4 GHz

5 - Después del modelo indica banda de operación de 5 GHz

n – soporta estándar 802.11n

Potencia de salida RF

H - “High”

HP - “High Power”

SHP - “Super High Power”

D - Indica operación dual chain 802.11n

T - Indica operación triple chain 802.11n

Excepción de nombres – Las tarjetas 600, 800, 1000, 1100, 1200, 2011 son representativas de la serie o tiene más de 9 interfaces cableadas, por lo tanto su nombre fue simplificado a un número entero o el año en que se desarrolló.

En la tabla 4 se muestran algunos ejemplos de RouterBoard y las características que describe el nombre del producto.




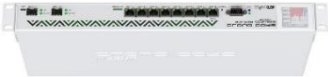
Routers Ethernet	Características	Precio
	RB750 5x Ethernet, Small plastic case, 400MHz CPU, 32MB RAM, Most affordable MPLS router, RouterOS L4	\$39.95
	RB912UAG-2HPnD 600MHz CPU, 64MB RAM, 1xGigabit Ethernet, onboard 1000mW 2.4Ghz wireless, miniPCI-express, USB, SIM slot, RouterOS L4	\$79.00
	RB2011iLS-IN Desktop metal case, 5xEthernet, 5xGigabit Ethernet, SFP cage, PoE out on port 10, 600MHz CPU, 64MB RAM, RouterOS L4	\$119.00
	CCR1036-8G-2S+EM 1U rackmount, 8x Gigabit Ethernet, 2xSFP+ cages, LCD 36 cores x 1.2GHz CPU, 16GB RAM, 41.5mpps fastpath, Up to 28Gbit/s throughput, RouterOS L6	\$1,295.00

Tabla 4. Características en hardware de MikroTik [14]

#### 1.4 SWITCHING

Esta palabra ha ido tomando distintas connotaciones a medida que se plantean nuevos esquemas para mejorar el rendimiento de las redes de área local (Torrent, 1998). Así, cuando hablamos de *switch*, podemos estarnos refiriendo a:

- *Switch* capa 2.
- *Switch* capa 3.
- *Switch* capa 4

### 1.4.1 SWITCH CAPA 2

Este es el tipo de switch de red de área local (LAN) más básico, el cual opera en la capa 2 del modelo OSI. Su antecesor es el bridge, por ello, muchas veces al switch se le refiere como un bridge multipuerto, pero con un costo más bajo, con mayor rendimiento y mayor densidad por puerto.

El switch capa 2 hace sus decisiones de envío de datos en base a la dirección MAC destino contenida en cada *frame*. Estos, al igual que los *bridges*, segmentan la red en dominios de colisión (Ver Figura 9), proporcionando un mayor ancho de banda por cada estación.

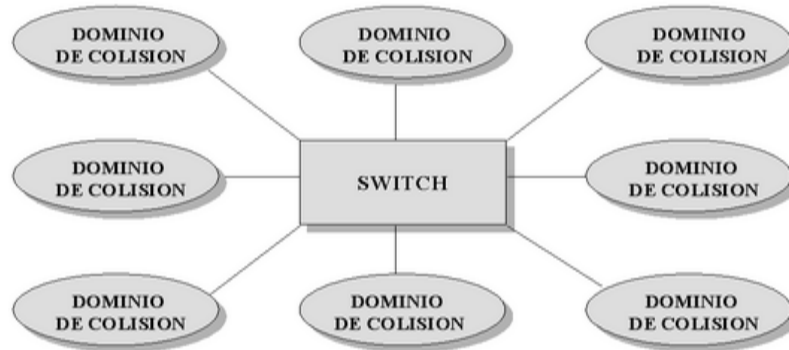


Figura 9: Dominios de broadcasts. [15]

La configuración de los *switches* capa 2 y el soporte de múltiples protocolos es totalmente transparente a las estaciones terminales. Como igual es el soporte de las redes virtuales (VLAN's), las cuales son una forma de segmentación que permite crear dominios de *broadcasts* formando así grupos de trabajo independientes de la ubicación física.

El uso de procesadores especializados (ASIC: *Application Specific Integrated Circuit*) incrementaron la velocidad de conmutación de los switches, en comparación con los bridges, porque pueden enviar los datos a todos los puertos de forma casi simultánea.

Estos *switches* siguen, principalmente, dos esquemas para envío de tráfico, los cuales son:

- *Cut-trough*: comienzan el proceso de envío antes de que el *frame* sea completamente recibido. En estos *switches* la latencia es baja porque sólo basta con leer la dirección MAC destino para comenzar a transferir el *frame*. La desventaja de este esquema, es que los *frames* corruptos (corruptos, enanos, con errores, etc.) son también enviados.
- *Store-and-forward*: lee y valida el paquete completo antes de iniciar el proceso de envío. Esto permite que el *switch* descarte paquetes corruptos y se puedan definir filtros de tráfico. La desventaja de este esquema es que la latencia se incrementa con el tamaño del paquete.

Algunos *switches* implementan otros esquemas (Fragment free) o esquemas híbridos en base a rendimiento y porcentaje de errores, pasando en un momento de modo *Cut-trough* al modo *Store-and-forward* y, viceversa.

#### 1.4.2 SWITCH CAPA 3

Este tipo de *switches* integran *routing* y *switching* para producir altas velocidades (medidas en millones de paquetes por segundo). Esta es una tecnología nueva (Lippis, 1997) a los cuales los vendedores se refieren muchas veces como: Netflow, *tag switching* (Packet, 1998), Fast IP (3Com, 1997), etc.

Este nuevo tipo de dispositivos es el resultado de un proceso de evolución natural de las redes de área local, ya que, combinan las funciones de los *switches* capa 2 con las capacidades de los routers (3Com, 1997).

Existen dos tipos de switches capa 3:

- *Packet-by-packet* (PPL3).
- *Cut-trough* (CTL3).

En ambos tipos de *switches*, se examinan todos los paquetes y se envían a sus destinos. La diferencia real entre ellos es el rendimiento. PPL3 enruta todos los paquetes, en tanto que los *switches* CTL3 efectúan la entrega de paquetes de una forma un poco distinta, estos *switches* investigan el destino del primer paquete en una serie. Una vez que lo

conoce, se establece una conexión y el flujo es conmutado en capa 2 (con el consiguiente, rendimiento del *switching* de capa 2) (Lippis, Jun1997).

Funciones:

- Procesamiento de rutas: esto incluye construcción y mantenimiento de la tabla de enrutamiento usando RIP y OSPF.
- Envío de paquetes: una vez que el camino es determinado, los paquetes son enviados a su dirección destino. El TTL (Time-To-Live) es decrementado, las direcciones MAC son resueltas y el *checksum* IP es calculado.
- Servicios especiales: traslación de paquetes, priorización, autenticación, filtros, etc.

#### 1.4.3 SWITCH CAPA 4

La información en los encabezados de los paquetes comúnmente incluyen direccionamiento de capa 2 y 3, tal como: tipo de protocolo de capa 3, TTL y *checksum*. Hay también información relevante a las capas superiores, como lo es el tipo de protocolo de capa 4 (UDP, TCP, etc.) y el número de puerto (valor numérico que identifica la sesión abierta en el host a la cual pertenece el paquete).

En el caso de los *switches* capa 3, éstos son *switches* capa 2 que utilizan la información del encabezado de capa 3. Lo mismo ocurre con los *switches* capa 4, son *switches* capa 3 que procesan el encabezado de la capa. También son conocidos como switches sin capa (Layerless switches).

La información del encabezado de capa 4 permite clasificar de acuerdo a secuencias de paquetes manejados por aplicación (denominados "flujos"). Ahora bien, dependiendo del diseño del *switch*, éste puede priorizar servicios o garantizar ancho de banda por "flujos". Algunos de los diseños de capa 4 son (Torrent, 1998):

- Arquitectura basada en *Crossbar*: generalmente, sólo proveen priorización por flujos porque tienen un esquema de *buffering* y de planificación muy compleja.

- *Switches* con memoria compartida y cola de salida: son capaces de manejar múltiples niveles de prioridades. Resultando con problemas en proveer servicios cuando el número de flujos excede el número de colas disponibles.
- *Switches* con colas por "flujos": son capaces de garantizar ancho de banda y manejar bien la congestión y pudiendo hacer la clasificación por flujos porque existe una cola por cada uno.

Router	Switch capa 2	Switch capa 3	Switch capa 4
<ul style="list-style-type: none"> <li>• Entrega de tráfico en base a protocolo de capa 3.</li> <li>• Selección óptima de ruta.</li> <li>• Control de tráfico.</li> <li>• No pasa <i>broadcasts</i>.</li> <li>• Soporte de políticas de seguridad, filtros, administración de ancho de banda.</li> <li>• Mayor latencia y menor rendimiento en comparación con los <i>switches</i>.</li> </ul>	<ul style="list-style-type: none"> <li>• Equivalentes a los <i>bridges multipuertos</i>.</li> <li>• Baja latencia y alto rendimiento.</li> <li>• En redes muy grandes (<i>flat networks</i>), éstas son inundadas de "tormentas" de <i>broadcasts</i>, limitaciones de direcciones.</li> <li>• Tipos: <i>Cut-trough</i>, <i>store-and-forward</i>, <i>fragment-free</i>, híbridos.</li> <li>• Segmentar la red en dominios de colisión por puerto y dominios de <i>broadcasts</i> con la configuración de VLAN.</li> <li>• Entrega de tráfico en base a dirección MAC.</li> </ul>	<ul style="list-style-type: none"> <li>• Combinación de la funcionalidad de los <i>switches</i> capa 2 y de las características de los <i>routers</i>.</li> <li>• Alto rendimiento.</li> <li>• Tipos: PPL3 y CTL3.</li> <li>• Entrega tráfico basado en direcciones IP (cuando enruta la primera vez) y en direcciones MAC (cuando conmuta).</li> <li>• Por ahora, la mayoría sólo soporta IP (algunos también IPX) haciendo <i>bridging</i> de los restantes protocolos.</li> </ul>	<ul style="list-style-type: none"> <li>• Combinación de <i>switches</i> capa 3 con utilización de la información del encabezado de capa 4.</li> <li>• Se segmenta por "flujos" de aplicación pudiendo soportar administración de ancho de banda por "flujos" y aplicación de niveles de prioridades.</li> </ul>

Tabla 5: Resumen de las características más relevantes de Routing y Switching. [15]

### 1.5 REDES VLAN

Las LAN virtuales permiten dividir la red en subredes sin tener que agregar nada al entorno de red física. Por lo tanto, las subredes son virtuales y se usan los mismos recursos de la red física. Las VLAN facilitan la administración de la red porque los grupos más pequeños son más fáciles de mantener.

### 1.5.1 IMPLEMENTACIÓN DE VLAN

Una red de área local virtual (VLAN) es una subdivisión de una red de área local en la capa de enlace de datos de la pila de protocolo. Puede crear redes VLAN para redes de área local que utilicen tecnología de nodo. Al asignar los grupos de usuarios en redes VLAN, puede mejorar la administración de red y la seguridad de toda la red local. También puede asignar interfaces del mismo sistema a redes VLAN diferentes.

### 1.5.2 CUANDO UTILIZAR REDES VLAN

Se recomienda dividir una red de área local en redes VLAN si se necesita hacer lo siguiente:

- Crear una división lógica de grupos de trabajo.  
Por ejemplo, suponer que todos los *hosts* de la planta de un edificio están conectados mediante una red de área local con nodos. Puede crear una VLAN para cada grupo de trabajo de la planta.
- Designar diferentes directivas de seguridad para los grupos de trabajo.  
Por ejemplo, las necesidades de seguridad del departamento de finanzas y del departamento de informática son muy diferentes. Si los sistemas de ambos departamentos comparten la misma red local, puede crear una red VLAN independiente para cada departamento. Después, se puede asignar la directiva de seguridad apropiada para cada VLAN.
- Dividir los grupos de trabajo en dominios de emisión administrables.

El uso de redes VLAN reduce el tamaño de los dominios de emisión y mejora la efectividad de la red.

### 1.5.3 LAS VLAN Y LOS NOMBRES PERSONALIZADOS

Las VLAN demuestran la ventaja de utilizar nombres genéricos o personalizados. A una VLAN se le puede asignar, por ejemplo, el nombre *laboratorio-1* o el nombre *sala-lectura*

Los nombres de las VLAN funcionan de manera conjunta con el ID de VLAN. Cada VLAN de una red de área local está identificada por un ID de VLAN, también conocido como etiqueta de VLAN. El ID de VLAN se asigna durante la configuración de la VLAN. Al



configurar los *switches* para que admitan las VLAN, es necesario asignar un ID de VLAN a cada puerto. El ID de VLAN del puerto debe ser el mismo que el ID de VLAN asignado a la interfaz que se conecta al puerto.

#### 1.5.4 TOPOLOGÍA DE VLAN

La tecnología de red LAN con nodos permite organizar los sistemas de una red local en redes VLAN. Para poder dividir una red de área local en redes VLAN, debe tener nodos compatibles con la tecnología VLAN. Puede configurar todos los puertos de un nodo para que transfieran datos para una única VLAN o para varias VLAN, según el diseño de configuración VLAN. Cada fabricante utiliza procedimientos diferentes para configurar los puertos de un *switch*.

En la Figura 10, se muestra una red de área local que se ha dividido en tres VLAN. La LAN tiene la dirección de subred 192.168.84.0. Está subdividida en tres redes VLAN para que se correspondan con tres grupos de trabajo:

- acctg0 con el ID de VLAN 789: grupo de contabilidad. Este grupo posee los hosts D y E.
- humres0 con ID de VLAN 456: grupo de recursos humanos. Este grupo posee los hosts B y F.
- infotech0 con ID de VLAN 123: grupo de informática. Este grupo posee los hosts A y C.

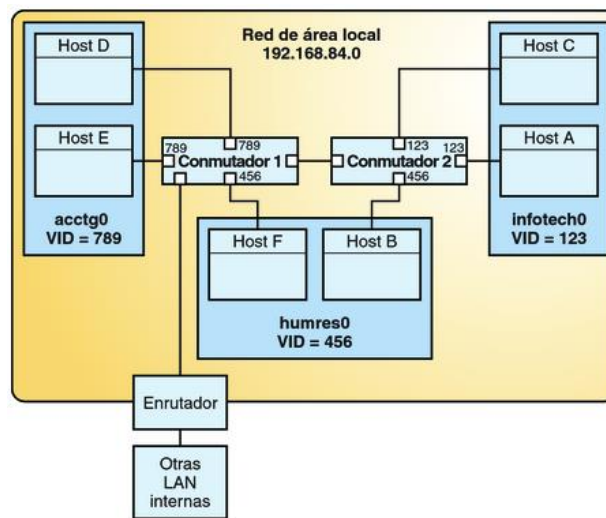


Figura 10. Red de área local con tres redes VLAN. [16]

Una variación de la Figura 10 se muestra en la Figura 11 donde se utiliza un solo *switch*, y varios hosts que pertenecen a diferentes VLAN se conectan a ese mismo *switch*.

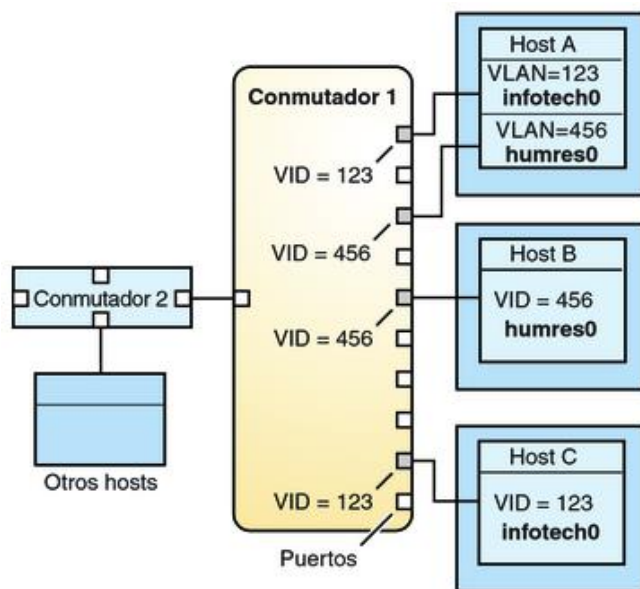


Figura 11. Configuración de conmutadores de una red con VLAN. [16]

### 1.5.5 TRUNKING (802.1q)

Túnel a nivel lógico que permite transportar información de VLANs entre distintos SW, en la figura 12 se ilustra un enlace troncal entre dos switch. [17]

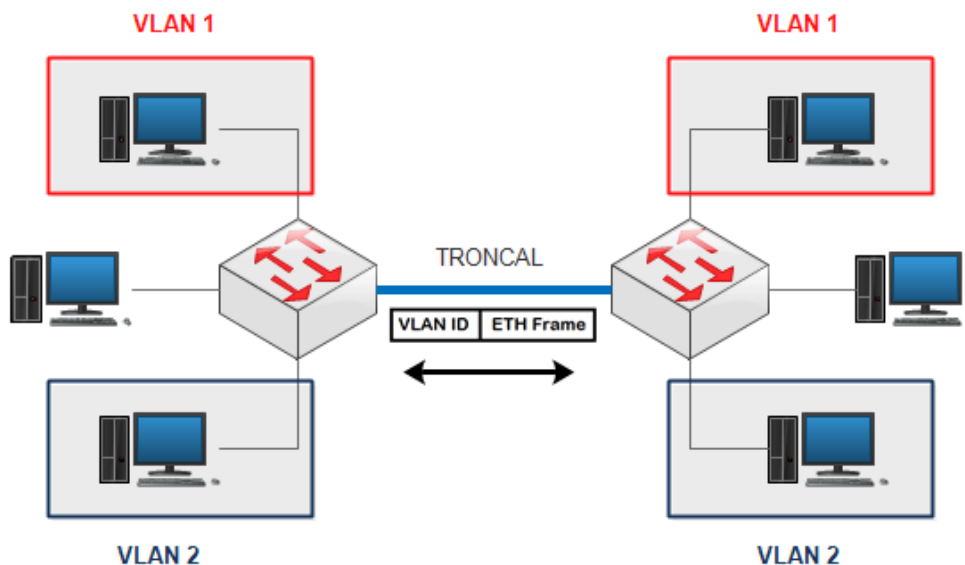


Figura 12. Representación de un puerto troncal. [17]

El 802.1q es el protocolo estándar de la IEEE referido al etiquetado de VLANs en la trama Ethernet, en la figura 13 se detalla la ubicación en trama Ethernet.

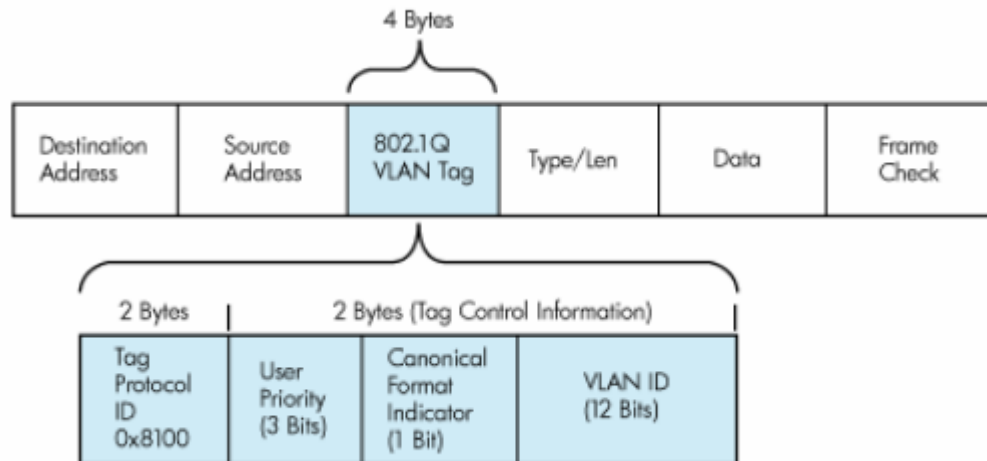


Figura 13. Ubicación del protocolo 802.1q en la trama Ethernet. [17]

### 1.5.6 VLAN NATIVA

El 802.1q define una VLAN nativa por cada *trunk*. No se encapsulan las tramas enviadas por esta VLAN. Cuando un switch recibe una trama y no detecta el *header* de 802.1q reconoce la trama como parte de la VLAN 1 o VLAN nativa.

### 1.6 MPLS

Protocolo de transporte de datos estándar que opera entre la capa de enlace de datos y la capa de red del modelo OSI. [18]

Inicialmente las redes IP enviaban los paquetes por reglas de enrutamiento IGP (Interior Gateway Protocol). En donde cada router decidía el envío de sus paquetes en base a su tabla de enrutamiento.

El problema llegó cuando Internet creció y se hizo difícil optimizar las redes con este modelo. En los noventa se realizó el cambio usando redes transportadas por ATM, sobreponiendo una red de transporte sobre una red IP.

En un inicio se trató de aprovechar el transporte proporcionado por ATM (*Asynchronous Transfer Mode*) de capa dos, en donde se realizó por primera vez la conmutación de paquetes en lugar de circuitos para establecer la comunicación y el cual utilizaba un “marcaje” de paquetes para lograr establecer la comunicación; junto con el enrutamiento de IP en capa tres.

Una red ATM transmite la información utilizando células o etiquetas de 53 bytes de longitud en donde se define el “circuito virtual” (VPI=canal virtual, VCI=circuito virtual) para cada paquete, además de proveer en primera instancia una primitiva diferenciación de servicio (CLP = prioridad de pérdida de celda). Además fue una tecnología diseñada para atender anchos de banda bajo demanda. En la figura 14 se detalla la cabecera ATM.

Sin embargo sobre una red ATM nativa, si bien es cierto la conmutación se establecía de manera eficiente, existían ciertos inconvenientes sobre parámetros utilizados para establecer la comunicación a nivel de capa 3 como por ejemplo soportar *unicast* o *multicast* sobre toda la nube ATM, además de la poca versatilidad para la diferenciación de paquetes circulantes sobre la red, finalmente se perdía alrededor de un 10 a 20% de ancho de banda sobre el tráfico IP.

Por lo que se creó MPLS como una alternativa para optimizar en los *routers* la búsqueda de rutas en las tablas que estaban creciendo en gran manera.

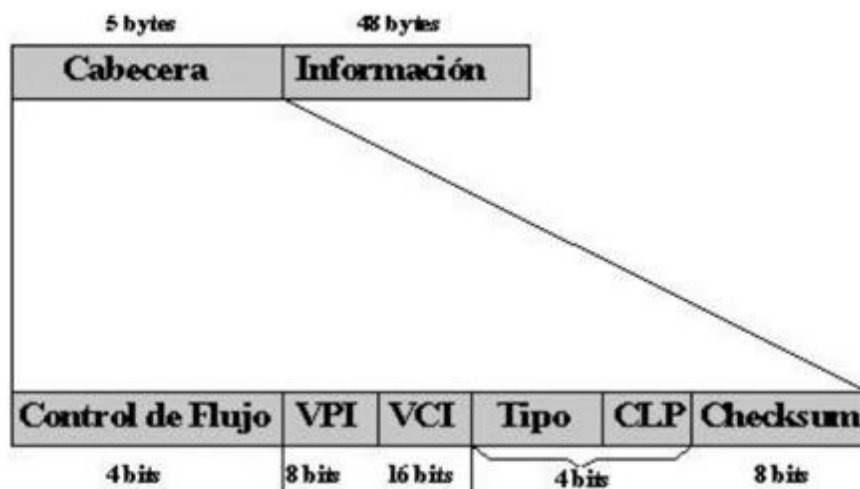


Figura 14. Cabecera ATM [18]

### 1.6.1 CARACTERÍSTICAS DE MPLS

A raíz de las necesidades no solventadas y de la complejidad de una red ATM, surgen las nuevas características que dieron paso MPLS, en la figura 15 se detalla una red *backbone* bajo un sistema MPLS. Entre ellas se tienen:

- Utilización de etiquetas para determinar el camino de los paquetes.
- Las etiquetas se asocian en la entrada de la red MPLS y se eliminan a la salida de la misma.
- El criterio para clasificar los paquetes en etiquetas se puede basar en una decisión local, al entrar en la red MPLS o en base a decisiones preestablecidas.
- Las etiquetas pueden apilarse, es decir un paquete puede tener varias etiquetas.
- Se define la utilización de los LSR (router conmutador de etiquetas).
- MPLS puede ejecutarse sobre cualquier tecnología en la capa de red.

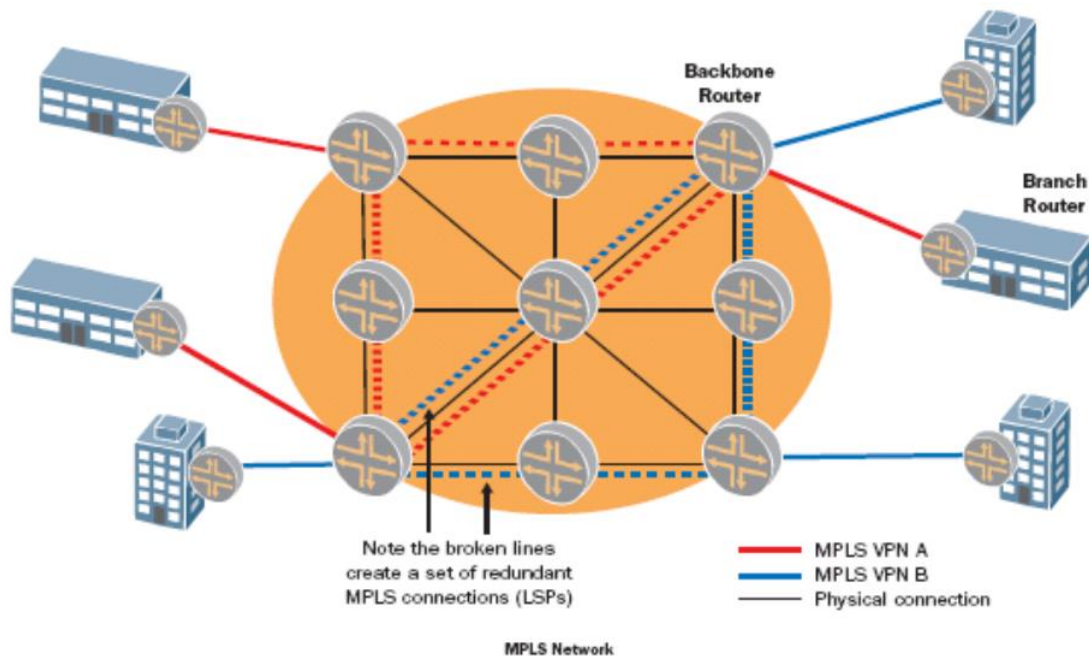


Figura 15. Ilustración de una red MPLS [18]

### 1.6.2 APLICACIONES DE MPLS

Entre las utilidades que MPLS ofrece se pueden mencionar:

- Funciones de ingeniería de tráfico (a los flujos de cada usuario se les asocia una etiqueta diferente)
- Policy Routing
- Servicios de VPN
- Servicios que requieren QoS

### 1.6.3 OPERACIÓN DE MPLS

Una red MPLS consiste de un conjunto de enrutadores de conmutación de etiquetas (LSR) que tiene la capacidad de conmutar y rutear paquetes en base a la etiqueta que se ha añadido a cada paquete. Cada etiqueta define un flujo de paquetes entre dos puntos finales. Cada flujo es diferente y es llamado Clase de Equivalencia de Reenvío (FEC por sus siglas en inglés).

Los routers MPLS no necesitan examinar ni procesar el encabezado IP, solo es necesario reenviar cada paquete dependiendo el valor de su etiqueta. Proporcionando así un reenvío menos complejo que si se examinara el encabezado IP del paquete, disminuyendo de esta forma la latencia de Tx.

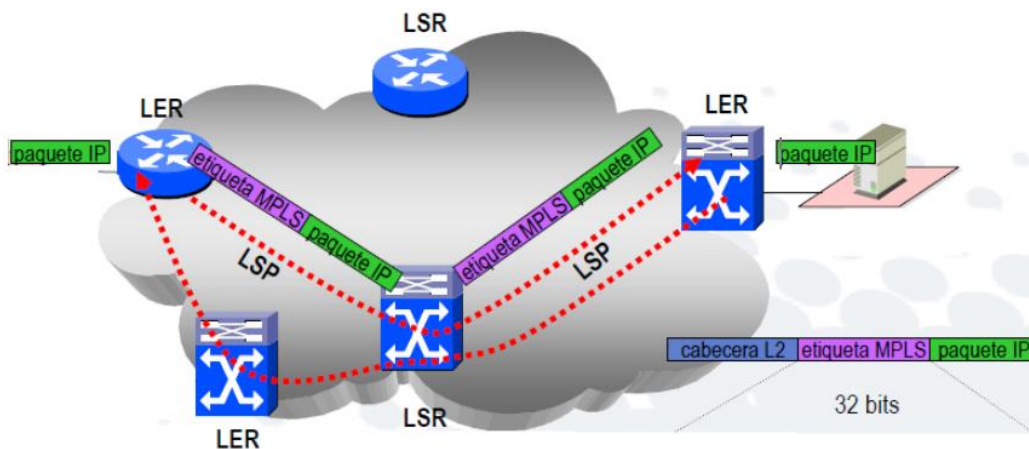


Figura 16. Flujo de un paquete MPLS [18]

Los routers MPLS pueden ser LER (Label Edge Router) o LSR (Label Switching Router); los primeros añaden las etiquetas MPLS al paquete IP al inicio de la ruta y quitan la etiqueta MPLS al final de la misma; mientras que los segundos se encargan de conmutar el tráfico a nivel de capa 2 en función del valor de la etiqueta.

En la figura 16 se presenta brevemente el proceso de flujo de un paquete MPLS:

1. Se establece un camino unidireccional de conmutación de etiquetas (LSP) entre los routers que van a transmitir la FEC, a través de los LER. Estos LSP sirven como túneles de transporte a lo largo de la red MPLS.
2. El paquete entra al dominio MPLS mediante un LSR que asigna el paquete a una FEC y a un LSP particular, lo etiqueta y lo envía.
3. En este punto el paquete ya está dentro del dominio MPLS, y un LSR lo recibe y se reenvía el paquete a otro LSR o se quita la etiqueta de entrada y se le añade la etiqueta de salida.
4. El LER de salida “abre” la etiqueta y lee el encabezado IP para enviarlo al destino final.

#### 1.6.4 ESTRUCTURA MPLS

MPLS comúnmente es llamado protocolo de capa 2.5 ya que este se ubica entre la capa 2 y capa 3 del tradicional modelo OSI. Tal como se presenta en la figura 18.

La trama MPLS está compuesta por 4 campos, agrega encabezados de 32 bits de los cuales 20 son para indicar el ID de la etiqueta. A continuación se presenta la ubicación del encabezado de MPLS.

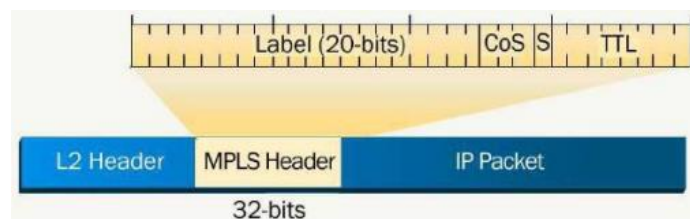


Figura 17. Trama y cabecera MPLS [18]



Figura 18. Ubicación de MPLS en el modelo OSI [18]

Como se observa en la Figura 17, los primeros 20 bits son de la etiqueta MPLS, luego se usan 3 bits para identificar la clase de servicio en el campo CoS o EXP, luego se utiliza un bit para poder apilar etiquetas de forma jerárquica en el campo S, finalmente se reservan 8 bits para indicar el TTL.

Para establecer la comunicación en una red MPLS, las etiquetas pueden ser definidas manualmente o de forma automática para determinar la trayectoria LSP. Para el primer caso se puede utilizar LDP (Label Distribution Protocol), mientras que para el segundo caso se puede usar RSVP (Protocolo de reserva de recursos).

#### 1.6.5 CARACTERÍSTICAS DE LSP

- Entidad unidireccional que existe en un dominio.
- Para cada LSP existe un único router de ingreso.
- Cada LSP pasa luego por los LSR cuya función es hacer intercambio de etiquetas según la tabla MPLS de envío de paquetes (no usa encabezados IP).



- El router penúltimo remueve la etiqueta efectuando una operación de quitar las etiquetas utilizadas para *forwardear* los paquetes en la red MPLS.
- El router de salida efectúa una consulta de ruta y finaliza el LSP.

### 1.6.6 CARACTERÍSTICAS DE SEÑALIZACIÓN DINÁMICA LDP

Es utilizada para proporcionar los mecanismos adecuados para que los equipos de conmutación de etiquetas puedan localizar a sus homólogos y establecer comunicación con ellos. En la figura 19 se detalla el intercambio de mensajes entre los LDP.

- Para sus decisiones usa un protocolo IGP (por lo general ISIS u OSPF).
- LDP envía *keepalives* para mantener activa la conexión TCP
- LDP no tiene mecanismos para hacer ingeniería de tráfico.
- LDP para localizar a sus vecinos usa la dirección de multicast 224.0.0.2:646, luego de localizado usa paquetes TCP para intercambio de tablas y rutas de etiquetas
- FEC (*Forwarding Equivalent Class*)
- Cada router LDP envía sus direcciones vía etiquetas MPLS sobre LDP, de modo que cada router puede ser un router en ingreso para los otros routers.
- LDP establece una ruta LSP del mismo modo como lo haría un protocolo de enrutamiento.
- LDP intercambia mensajes en la interface que ha sido definida con los cuales se establecen mapas para los paquetes.

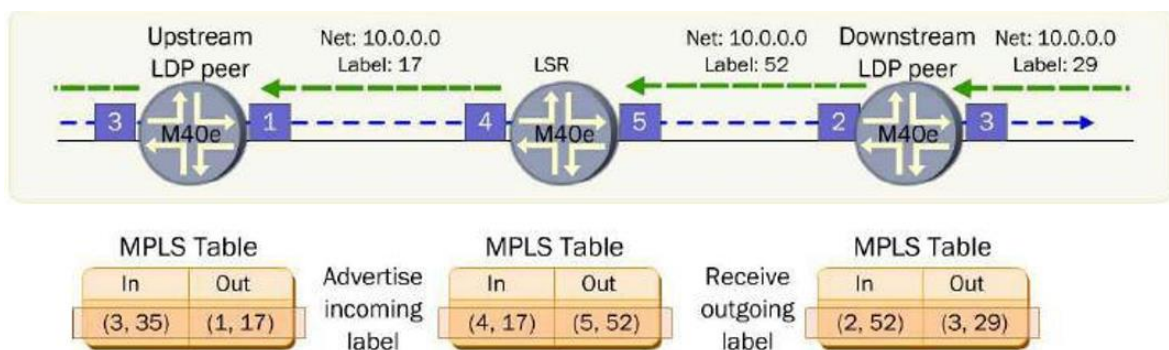


Figura 19. Intercambio de mensajes en las interfaces de los LDP [18]

### 1.6.7 CARACTERÍSTICAS DE SEÑALIZACIÓN DINÁMICA USANDO RSVP

Está orientado al control de la red, permitiendo que se aplique la calidad de servicio en la misma, procesando las sesiones de manera independiente. En la figura 20 se ilustra el envío de mensajes entre equipos que están bajo un sistema MPLS.

- Utiliza flujos unidireccionales para pasar por la red.
- El router de ingreso inicia un mensaje de trayectoria RSVP y lo envía hacia el router de egreso.
- Cuando el mensaje de path, llega al router de egreso, inicia el proceso de reservación de path.
- El router de egreso envía hacia arriba en dirección del router de ingreso mensajes de reservación Resv.

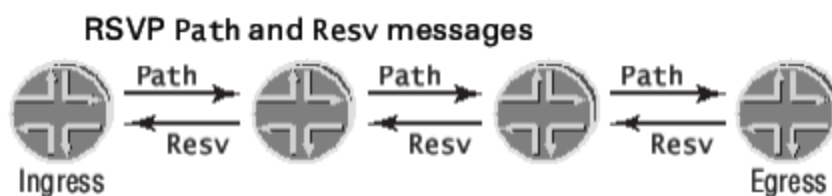


Figura 20. Ilustración del envío de mensajes entre equipos corriendo MPLS [18]

### 1.6.8 COMPARACIÓN DE MPLS CON ROUTING y ATM

MPLS acelera el transporte de paquetes IP, reemplazando el enrutamiento clásico de los mismos, basado en direcciones destino de capa 3, por una conmutación basada en etiquetas.

En la tabla 6 se presenta una comparación entre protocolos usados para construir backbone de los ISP, hay que notar que MPLS solo ofrece ventajas en todos los aspectos y que es la preparación para el futuro. Uno de los principales beneficios de los servicios basados en MPLS reside en su capacidad para aplicar calidades de servicio (QoS) mediante la priorización del tráfico en tiempo real, una prestación clave cuando se quiere introducir voz y vídeo en las redes de datos.

Backbone Frame Relay/ATM	Backbone IP	Backbone MPLS
+ Conmutación veloz de tramas en el backbone (capa 2).	- Velocidad de conmutación de paquetes depende de plataforma (tabla en memoria).	+ Conmutación veloz de paquetes usando etiquetas y no direcciones IP.
+ Total independencia entre redes de clientes (VPN en capa 2).	- Redes de clientes sujetas a compartir una misma tabla de rutas.	+ Total independencia entre redes de clientes (MPLS VPN).
+ Puede transportar cualquier protocolo de capa 3.	- Cualquier otro protocolo a transportar debe pasar encapsulado en paquetes IP	Es multiprotocolo tanto hacia arriba (L3) como hacia abajo (PWE3).
- Esquema de QoS limitado, versatilidad adicional depende del protocolo de capa 3 utilizado.	+ Esquema de QoS para aplicaciones basado en marcación de paquetes (DiffServ) o reserva de ancho de banda (RSVP)	+ Esquema de QoS para aplicaciones basado en marcación de paquetes (MPLS EXP bits).
- Cada cliente nuevo implica la creación de circuitos nuevos (PVCs en el backbone).	+ Cada cliente nuevo sólo implica la creación del circuito de acceso y del enrutamiento.	+ Cada cliente nuevo sólo implica la creación del circuito de acceso y del enrutamiento.
- Utilización no óptima de troncales Frame Relay/ATM	+ Troncales IP con dimensionamiento óptimo.	+ Troncales MPLS con dimensionamiento óptimo.
- Utilización no óptima de acceso central en esquemas hub & spoke	+ Utilización óptima del ancho de banda en accesos (full-mesh virtual)	+ Utilización óptima del ancho de banda en accesos (full-mesh virtual)
- Acceso de cliente a servicios en el proveedor implica nuevos circuitos en capa 2.	+ Fácil acceso a servicios en el proveedor (datacenter) a través de troncales IP existentes.	+ Fácil acceso a servicios en el proveedor (datacenter) a través de troncales existentes.
- Elección de mejor ruta hecha en capa 3.	- Elección de mejor ruta según protocolo de enrutamiento basado sólo en métricas fijas.	+ Elección más inteligente del camino que el tráfico utilizará (MPLS-TE)

Tabla 6. Comparación entre ATM, IP y MPLS

## 1.7 TÉCNICAS DE ENRUTAMIENTO.

### 1.7.1 ENRUTAMIENTO ESTÁTICO

El principal problema que plantea mantener tablas de enrutamiento estáticas, además de tener que introducir manualmente en los *routers* toda la información que contienen, es que el *router* no puede adaptarse por sí solo a los cambios que puedan producirse en la

topología de la red. Sin embargo, este método de enrutamiento resulta ventajoso en las siguientes situaciones:

- Un circuito poco fiable que deja de funcionar constantemente. Un protocolo de enrutamiento dinámico podría producir demasiada inestabilidad, mientras que las rutas estáticas no cambian.
- Se puede acceder a una red a través de una conexión de acceso telefónico. Dicha red no puede proporcionar las actualizaciones constantes que requiere un protocolo de enrutamiento dinámico.
- Existe una sola conexión con un solo ISP. En lugar de conocer todas las rutas globales, se utiliza una única ruta estática.
- Un cliente no desea intercambiar información de enrutamiento dinámico.

#### 1.7.1.1 ENRUTAMIENTO PREDETERMINADO

Es una ruta estática (también conocida como ruta por defecto) que se refiere a una conexión de salida o Gateway de “último recurso”. El tráfico hacia destinos desconocidos por el router se envía a dicha conexión de salida. Es la forma más fácil de enrutamiento para un dominio conectado a un único punto de salida. Esta ruta se indica como la red de destino 0.0.0.0/0. En la figura 21 se ilustra una ruta por defecto hacia el ISP.

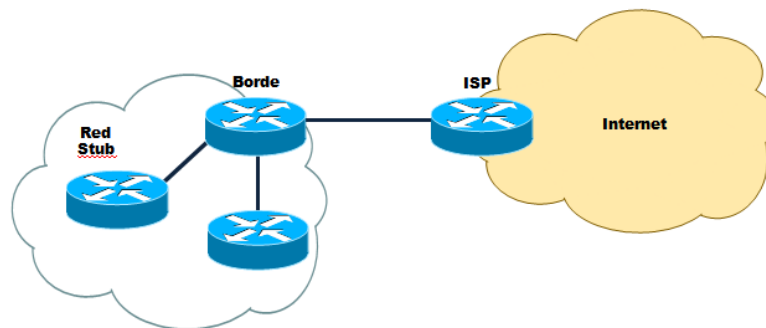


Figura 21. Ruta por defecto [19]

#### 1.7.1.2 RUTAS ESTÁTICAS

Las rutas estáticas se definen administrativamente y establecen rutas específicas que han de seguir los paquetes para pasar de un puerto de origen hasta un puerto de destino. Se establece un control preciso del enrutamiento según los parámetros del administrador.

Las rutas estáticas por defecto especifican un *gateway* (puerta de enlace) de último recurso, a la que el router debe enviar un paquete destinado a una red que no aparece en su tabla de enrutamiento, es decir que desconoce.

Las rutas estáticas se utilizan habitualmente en enrutamientos desde una red hasta una red de conexión única, ya que no existe más que una ruta de entrada y salida en una red de conexión única, evitando de este modo la sobrecarga de tráfico que genera un protocolo de enrutamiento. La ruta estática se configura para conseguir conectividad con un enlace de datos que no esté directamente conectado al router. Para conectividad de extremo a extremo, es necesario configurar la ruta en ambas direcciones. Las rutas estáticas permiten la construcción manual de la tabla de enrutamiento.

### 1.7.2 ENRUTAMIENTO DINÁMICO

Los protocolos de enrutamiento mantienen tablas de enrutamiento dinámicas por medio de mensajes de actualización del enrutamiento, que contiene información acerca de los cambios sufridos en la red, y que indican al software del router que actualice la tabla de enrutamiento en consecuencia. Intentar utilizar el enrutamiento dinámico sobre situaciones que no lo requieren es una pérdida de ancho de banda, esfuerzo, y en consecuencia de dinero.

### 1.7.3 PROTOCOLOS DE ENRUTAMIENTO

Los protocolos de enrutamiento proporcionan mecanismos distintos para elaborar y mantener las tablas de enrutamiento de los diferentes routers de la red, así como determinar la mejor ruta para llegar a cualquier host remoto [20]. En un mismo router pueden ejecutarse protocolos de enrutamiento independientes, construyendo y actualizando tablas de enrutamiento para distintos protocolos encaminados.

#### 1.7.3.1 ROUTING INFORMATION PROTOCOL (RIP)

RIP es un protocolo universal de enrutamiento por vector de distancia que utiliza el número de saltos como único sistema métrico. Un salto es el paso de los paquetes de una red a otra. Si existen dos rutas posibles para alcanzar el mismo destino, RIP elegirá la ruta

que presente un menor número de saltos. No tiene en cuenta la velocidad ni la fiabilidad de las líneas a la hora de seleccionar la mejor ruta. Envía un mensaje de actualización del enrutamiento cada 30 segundos (tiempo predeterminado en routers Cisco), en el que se incluye toda la tabla de enrutamiento del router, utilizando el protocolo UDP para el envío de los avisos. RIP-1 está limitado a un número máximo de saltos de 15, no soporta VLSM y CIDR, y no soporta actualizaciones desencadenadas. RIP-1 puede realizar equilibrado de la carga en un máximo de seis rutas de igual coste. RIP-2 es un protocolo sin clase que admite CIDR, VLSM, resumen de rutas y seguridad mediante texto simple y autenticación MD5. RIP publica sus rutas sólo a los routers vecinos.

#### 1.7.3.2 OPEN SHORT PATH FIRST (OSPF).

OSPF es un protocolo universal basado en el algoritmo de estado de enlace, desarrollado por el IETF para sustituir a RIP. Básicamente, OSPF utiliza un algoritmo que le permite calcular la distancia más corta entre la fuente y el destino al determinar la ruta para un grupo específico de paquetes. Soporta VLSM, ofrece convergencia rápida, autenticación de origen de ruta, y publicación de ruta mediante *multicast*. OSPF publica sus rutas a todos los routers de la misma área. En la RFC 2328 [21] se describe el concepto y operatividad del estado de enlace, mientras que la implementación de OSPF versión 2 se muestra en la RFC 1583 [22]. OSPF toma las decisiones en función del corte de la ruta, disponiendo de una métrica máxima de 65535.

Funciona dividiendo una intranet o un sistema autónomo en unidades jerárquicas de menor tamaño. Cada una de estas áreas se enlaza con un área *backbone* mediante un router fronterizo. Así, todos los paquetes direccionados desde un área a otra diferente, atraviesan el área backbone. OSPF envía Publicaciones del Estado de Enlace (*Link-State Advertisement – LSA*) a todos los routers pertenecientes a la misma área jerárquica mediante multidifusión IP. Los routers vecinos intercambian mensajes *Hello* para determinar qué otros routers existen en una determinada interfaz y sirven como mensajes de actividad que indican la accesibilidad de dichos routers. Cuando se detecta un router vecino, se intercambia información de topología OSPF. La información de la LSA

se transporta en paquetes mediante la capa de transporte OSPF (con acuse de recibo) para garantizar que la información se distribuye adecuadamente.

### 1.7.3.3 BORDER GATEWAY PROTOCOL (BGP)

Es un protocolo de enrutamiento por vector de distancia usado comúnmente para enrutar paquetes entre dominios, estándar en Internet. BGP gestiona el enrutamiento entre dos o más routers que sirven como frontera para determinados Sistemas Autónomos. BGP versión 4 (BGP-4), es el protocolo de enrutamiento entre dominios elegido en Internet, en parte porque administra eficientemente la agregación y la propagación de rutas entre dominios. Aunque BGP-4 es un protocolo de enrutamiento exterior, también puede utilizarse dentro de un SA como un conducto para intercambiar actualizaciones BGP. Las conexiones BGP dentro de un SA son denominadas BGP interno (IBGP), mientras que las conexiones BGP entre routers fronterizos (distintos SA) son denominadas BGP externo (EBGP). BGP-1, 2 y 3 están obsoletos. Para la configuración de OSPF se requiere un número de Sistema Autónomo, ya que se pueden ejecutar distintos procesos OSPF en el mismo routers. BGP se especifica en las RFC 1163, 1267 y 1771 [23], que definen las versiones 2, 3 y 4 de BGP, respectivamente.

Los routers BGP se configuran con la información del vecino a fin de que puedan formar una conexión TCP fiable sobre la que transportar información de la ruta de acceso del sistema autónomo y la ruta de la red. Tras establecer una sesión BGP entre vecinos, ésta sigue abierta a menos que se cierre específicamente o que haya un fallo en el enlace. Si dos routers vecinos intercambian información de ruta y sesiones BGP, se dice que son iguales BGP. En principio, los iguales BGP intercambian todo el contenido de las tablas de enrutamiento BGP. Posteriormente, sólo se envían actualizaciones incrementales entre los iguales para avisarles de las rutas nuevas o eliminadas.

Todas las rutas BGP guardan el último número de versión de la tabla que se ha publicado a sus iguales, así como su propia versión interna de la tabla. Cuando se recibe un cambio en un igual, la versión interna se incrementa y se compara con las versiones de los iguales, para asegurar que todos los iguales se mantienen sincronizados. BGP también guarda una

tabla de rutas BGP independiente que contiene todas las rutas de acceso posibles a las redes publicadas.

Los iguales BGP se dividen en dos categorías: Los iguales BGP de distintos sistemas autónomos que intercambian información de enrutamiento son iguales BGP externos (EBGP). Los iguales BGP del mismo sistema autónomo que intercambian información de enrutamiento son iguales BGP internos (IBGP).

La selección de ruta óptima BGP se basa en la longitud de la ruta de acceso del sistema autónomo para una ruta de red. La longitud se define como el número de sistemas autónomos distintos necesarios para acceder a la red. Cuanto menor sea la distancia, más apetecible será la ruta de acceso. A través del uso de controles administrativos, BGP es uno de los protocolos de enrutamiento más flexibles y totalmente configurables disponibles.

Un uso típico de BGP, para una red conectada a Internet a través de varios ISP, es el uso de EBGP con los ISP, así como el uso de IBGP en la red interna, para así ofrecer una óptima selección de rutas. Las redes conocidas de otros sistemas autónomos a través de EBGP se intercambiarán entre los iguales IBGP. Si sólo hubiera un ISP, valdría con utilizar una ruta resumen o predeterminada para la salida a internet.

En la figura 22 se puede observar una representación para IBGP y EBGP.

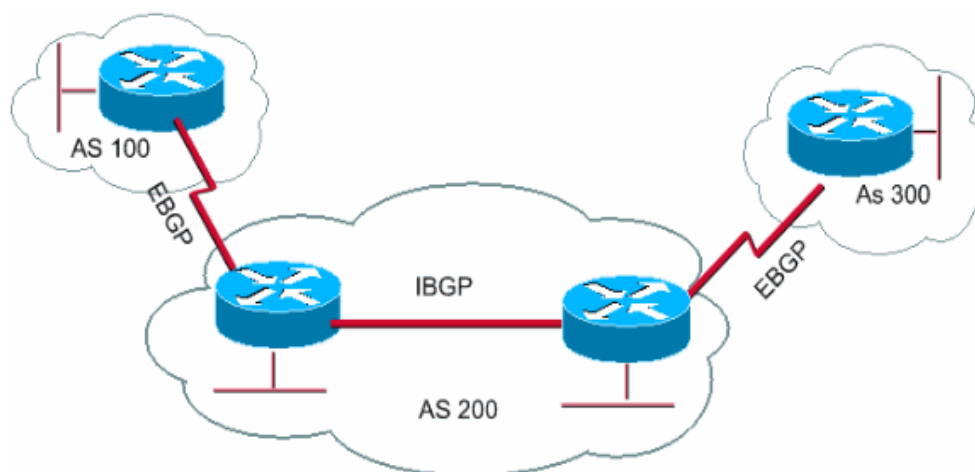


Figura 22. IBGP y EBGP [24]



Se debe considerar que los routers BGP publican las rutas conocidas de un igual BGP a todos sus otros iguales BGP. Por ejemplo, las rutas conocidas a través de EBGp con un ISP se volverán a publicar a los iguales IBGP, que a su vez volverán a publicarlos a otros ISP a través de EBGp. Mediante la publicación reiterada de rutas, la red puede pasar a ser una red de tránsito entre los proveedores con los que se conecte. BGP puede parametrizarse tanto para que la red interna actúe como una red de tránsito, como para que no.

#### 1.7.4 PROTOCOLOS ENRUTABLES.

Los protocolos enrutables soportan la comunicación entre LANs o segmentos de red que pueden estar repartidos por un edificio, en una pequeña área geográfica, como el campus de una universidad, o por todo el mundo, como Internet. Los protocolos enrutables soportan la transmisión de datos desde un segmento de red a otro por cualquiera de las diversas rutas que conectan ambos segmentos. Ejemplos de protocolos enrutables son TCP/IP e IPX/SPX.

Para que un protocolo sea enrutable debe tener la capacidad de asignar un número de red y un número de equipo a cada dispositivo (debemos distinguir el equipo y la red). Algunos protocolos como el protocolo IPX (el que utilizaba las redes Novell, un sistema muy extendido antes), sólo necesitan que se le asigne un número de red; estos protocolos utilizan una dirección MAC de host como el número de host. Otros protocolos como IP, requieren que se suministre una dirección completa y la máscara de red. (La dirección de red se obtiene mediante una operación AND de la dirección con la máscara de subred)

Los protocolos de enrutamiento (no confundir con los protocolos enrutables) determinan las rutas que siguen los protocolos enrutados hacia los destinos. Entre los ejemplos de protocolos de enrutamiento se tienen:

- Protocolo de Información de Enrutamiento (RIP por sus siglas en inglés)
- Protocolo de enrutamiento de gateway (BGP por sus siglas en inglés)
- Protocolo de primero la ruta libre más corta (OSPF por sus siglas en inglés).

Los protocolos de enrutamiento permiten que los routers conectados creen un mapa interno de los demás routers de la red o de Internet. Esto permite que se produzca el

enrutamiento y la selección de la mejor ruta. Estos mapas forman parte de la tabla de enrutamiento de cada router.

#### 1.7.4.1 IP

El protocolo Internet (IP) es un protocolo de capa de red, y como tal se puede enrutar a través de una red. Los protocolos que suministran soporte para la capa de red se denominan protocolos enrutados o enrutables. El enrutamiento es la capacidad de los protocolos de red para localizar redes que están en otros segmentos. En la figura 23 se ilustra la ubicación de la capa de red dentro del modelo OSI.



Figura 23. Ilustración de la capa de red en el Modelo OSI [20]

### 1.8 SEGURIDAD

#### 1.8.1 FIREWALL (CORTAFUEGOS)

Un cortafuegos (o *firewall* en inglés) es un elemento de hardware o software que se utiliza en una red de computadoras para controlar las comunicaciones, permitiéndoles o prohibiéndoles según las políticas de red que haya definido la organización responsable de la red. Su modo de funcionar es indicado por la recomendación RFC 2979 [25], que define las características de comportamiento y requerimientos de interoperabilidad [26]. La ubicación habitual de un cortafuegos es el punto de conexión de la red interna de la

organización con la red exterior, que normalmente es Internet; de este modo se protege la red interna de intentos de acceso no autorizados desde Internet, que puedan aprovechar vulnerabilidades de los sistemas de la red interna.

También es frecuente conectar al *firewall* a una tercera red, llamada zona desmilitarizada o DMZ, en la que se ubican los servidores de la organización que deben permanecer accesibles desde la red exterior.

Un *firewall* correctamente configurado añade protección a una instalación informática, pero en ningún caso debe considerarse suficiente. La seguridad informática abarca más ámbitos y más niveles de trabajo y protección.

#### 1.8.1.1 FIREWALL DE CAPA DE RED O DE FILTRADO DE PAQUETES.

Funciona a nivel de red (capa 3 del modelo OSI, capa 2 del stack de protocolos TCP/IP) como filtro de paquetes IP. A este nivel se pueden realizar filtros según los distintos campos de los paquetes IP: dirección IP origen, dirección IP destino. A menudo en este tipo de cortafuegos se permiten filtrados según campos de nivel de transporte (capa 3 TCP/IP, capa 4 Modelo OSI), como el puerto origen y destino, o a nivel de enlace de datos (no existe en TCP/IP, capa 2 Modelo OSI) como la dirección MAC.

#### 1.8.2 IPSEC – ARQUITECTURA DE SEGURIDAD PARA IP

IPsec está diseñado para proveer seguridad basada en criptografía, de alta calidad e interoperable para Ipv4 e Ipv6. Los servicios de seguridad ofrecidos incluyen control de acceso, integridad en comunicaciones sin conexión, autenticación del origen de datos, protección contra ataques de repetición, confidencialidad mediante encriptado, entre otros. Estos servicios son provistos en la capa IP ofreciendo protección para ésta y las capas superiores.

Para ofrecer tales servicios, IPsec utiliza dos protocolos de seguridad de tráfico, AH (*Authentication Header*) y ESP (*Encapsulating Security Payload*) además del uso de protocolos y procedimientos de administración de claves criptográficas. El protocolo de administración automática de claves por defecto es IKE. IKE es usado para establecer una

política de seguridad compartida y claves autenticadas para servicios que las requieran (como IPsec). Antes del envío de tráfico IPsec, cada router/firewall/host debe ser capaz de verificar la identidad de su par. Esto puede ser hecho manualmente entregando claves pre-compartidas en ambos hosts.

El conjunto de protocolos de seguridad utilizados y la forma en que son empleados estará determinado por requerimientos del sistema y de seguridad de los usuarios y aplicaciones. Los mecanismos utilizados por IPsec están diseñados para ser independientes de los algoritmos empleados. Esta modularidad permite la selección de diferentes conjuntos de algoritmos sin afectar las otras partes del sistema.

IPsec propone un conjunto de algoritmos por defecto para ser usados y proveer interoperabilidad en Internet.

### 1.8.3 AH y ESP

El Encabezado de Autenticación (*Authentication Header - AH*) de IP provee integridad para comunicación sin conexión y autenticación del origen de datos para datagramas IP y para proveer protección ante ataques de repetición.

AH [27] provee autenticación para la mayor parte de la información del encabezado IP y para los protocolos del nivel superior. No todos los campos del encabezado IP son protegidos ya que son modificados en tránsito.

AH puede ser aplicado sólo, en combinación con ESP (*Encapsulating Security Payload*), o de forma anidada a través del uso del modo túnel. Los servicios de seguridad pueden establecerse entre un par de sistemas finales, entre un par de gateways de seguridad o entre un gateway o un sistema final.

ESP [28] puede ser usado para proveer los mismos servicios de seguridad, y también provee un servicio de encriptación. La principal diferencia entre la seguridad provista por ESP y AH es el alcance de la protección. Específicamente, ESP no protege ningún campo del encabezado IP (excepto en modo túnel, donde los datos encriptados por ESP corresponden a otro paquete IP).

### 1.8.3 NAT

La traducción de direcciones de red (NAT) está diseñado para la conservación de la dirección IP. Permite que las redes IP privadas que utilizan direcciones IP no registradas puedan conectarse a Internet. NAT opera en un router, por lo general que conecta dos redes entre sí, y traduce las direcciones privadas (no únicos globales) en la red interna en direcciones legales, antes que los paquetes se reenvían a otra red.

Como parte de esta capacidad, NAT se puede configurar para anunciar una única dirección para toda la red al mundo exterior. Esto proporciona seguridad adicional al ocultar eficazmente toda la red interna detrás de esa dirección. NAT ofrece la doble función de conservación de la seguridad y la dirección y se implementa normalmente en entornos de acceso remoto.

Básicamente, NAT permite que un único dispositivo, tal como un router, para actuar como un agente entre el Internet (o red pública) y una red local (o red privada), lo que significa que sólo se requiere una única dirección IP para representar a todo un grupo de computadoras fuera de su red. En la figura 24 se ilustra la traducción de varias direcciones IP a una sola.

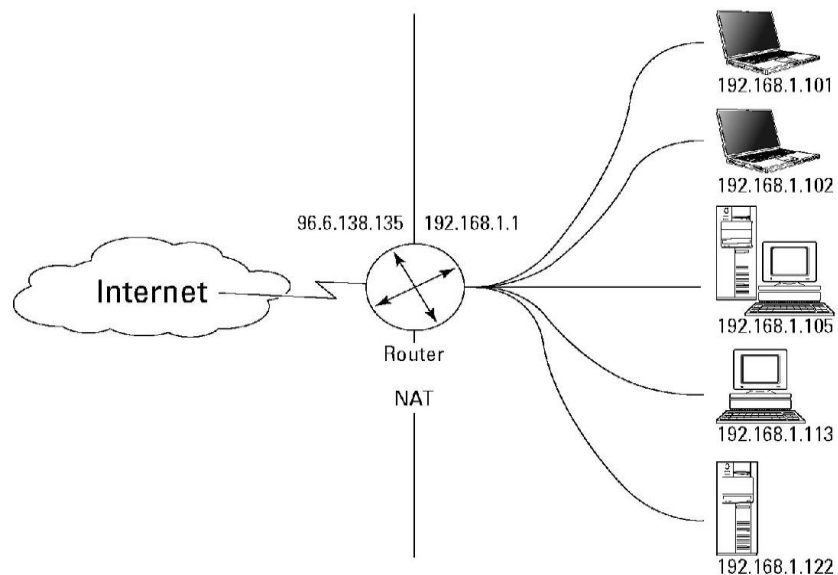


Figura 24. NAT traduce varias direcciones privadas a una dirección pública [29]

#### 1.8.4 PORT FORWARDING

La redirección de puertos, a veces llamado *tunelado* de puertos, es la acción de redirigir un puerto de red de un nodo de red a otro. Esta técnica puede permitir que un usuario externo tenga acceso a un puerto en una dirección IP privada (dentro de una LAN) desde el exterior vía un router con NAT activado.

La redirección de puertos permite que computadoras remotas (por ejemplo, máquinas públicas en Internet) se conecten a una computadora en concreto dentro de una LAN privada.

Por ejemplo:

- la redirección del puerto 8000 en el router a la máquina de otro usuario permite *streaming SHOUTcast*
- la redirección de los puertos 5000 a 6000 a la máquina de un usuario permite el uso de *Unreal Tournament*

Las máquinas con Linux modernos consiguen esto añadiendo reglas de *iptables* a la tabla *nat*: con el destino DNAT a la cadena de PREROUTING y/o con el destino SNAT en la cadena de POSTROUTING.

Las máquinas BSD y Mac OS X usan una herramienta similar llamada *ipfw*. La herramienta *ipfw* corre probablemente como una parte ya integrada del núcleo del sistema operativo.

#### 1.8.5 VPN

Una red privada virtual (VPN) es la extensión de una red privada que incluye vínculos de redes compartidas o públicas como Internet. Una VPN permite enviar datos entre dos ordenadores a través de una red interna compartida o pública de forma que emula las propiedades de un vínculo privado punto a punto. El acto de la configuración y la creación de una red privada virtual se conocen como redes privadas virtuales.

Para emular un vínculo punto a punto, los datos se encapsulan o empaquetan con un encabezado que proporciona información sobre lo que le permite recorrer la *internetwork* tránsito compartido o público para llegar a su punto final de enrutamiento. Para emular un vínculo privado, los datos enviados se cifran para la confidencialidad. Los paquetes

interceptados en la red compartida o pública no se pueden descifrar sin las claves de cifrado. La porción de la conexión en la que se encapsula los datos privados se conoce como *túnel*. La porción de la conexión en la que los datos privados se cifra que se conoce como la conexión de red privada virtual (VPN).

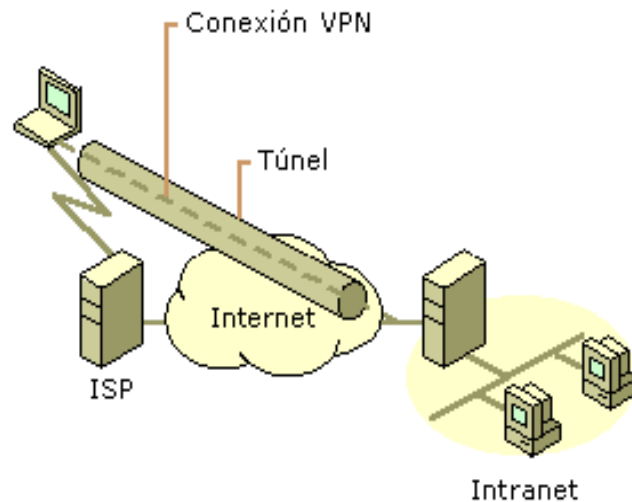


Figura 25. Conexión de red privada virtual [30]

Conexiones VPN permiten a los usuarios que trabajan en casa o en la carretera para conectar de forma segura a un servidor corporativo remoto utilizando la infraestructura de enrutamiento proporcionada por una *internetwork* pública (como Internet). Desde la perspectiva del usuario, la conexión VPN es una conexión punto a punto entre el ordenador del usuario y un servidor corporativo. La naturaleza de la *internetwork* intermedio es irrelevante para el usuario, ya que parece como si los datos se envían a través de un vínculo privado dedicado.

La tecnología VPN también permite a una empresa conectar a las sucursales con otras empresas a través de una interconexión de redes públicas (como Internet), mientras que el mantenimiento de las comunicaciones seguras. La conexión VPN a través de Internet funciona lógicamente como un enlace de red de área amplia (WAN) entre los sitios.

En ambos casos, la conexión segura a través de la red interna aparece al usuario como una red privada de comunicación, a pesar del hecho de que esta comunicación se produce a través de una interconexión de redes públicas, de ahí el nombre de la red privada virtual.

## 1.9 APLICACIONES LAN

### 1.9.1 ASIGNACIÓN PARÁMETROS DE RED Y DNS POR DHCP

#### 1.9.1.1 ¿QUÉ ES EL DHCP?

El protocolo de configuración dinámica de host DHCP (por sus siglas del inglés) es un estándar TCP/IP diseñado para simplificar la administración de la configuración IP de los equipos de nuestra red.

Si disponemos de un servidor DHCP, la configuración IP de las computadoras o de cualquier dispositivo de red en capa tres, puede hacerse de forma automática, evitando así la necesidad de tener que realizar manualmente uno por uno la configuración TCP/IP de cada equipo.

Un servidor DHCP es uno que recibe peticiones de clientes solicitando una configuración de red IP como se muestra en la figura 26. El servidor responderá a dichas peticiones proporcionando los parámetros de red que el cliente solicite. Para que una computadora solicite la configuración a un servidor, en los parámetros de red hay que seleccionar que la asignación sea dinámicamente.

El servidor proporcionará al cliente al menos los siguientes parámetros: Dirección IP, máscara de subred. Opcionalmente, el servidor DHCP podrá proporcionar otros parámetros de configuración tales como: Puerta de enlace y Servidores DNS.

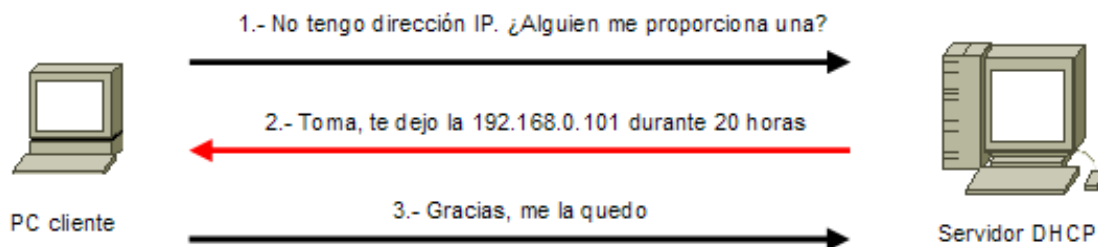


Figura 26. Peticiones a servidor DHCP [31]

El servidor DHCP proporciona una configuración de red TCP/IP segura y evita conflictos de direcciones repetidas. Utiliza un modelo cliente-servidor en el que el servidor DHCP



mantiene una administración centralizada de las direcciones IP utilizadas en la red. Los clientes podrán solicitar al servidor una dirección IP y así poder integrarse en la red.

#### 1.9.1.2 FUNCIONAMIENTO DE UNA PETICIÓN DHCP

El servidor solo asigna direcciones dentro de un rango prefijado. Si por error hemos configurado manualmente una IP estática perteneciente al rango gestionado por nuestro servidor DHCP, podría ocurrir que dicha dirección sea asignada dinámicamente a otro PC, provocándose un conflicto de IP. En ese caso el cliente solicitará y comprobará, otra dirección IP, hasta que obtenga una dirección IP que no esté asignada actualmente a ningún otro equipo de nuestra red.

La primera vez que seleccionamos en una computadora que su configuración IP se determine por DHCP, éste pasará a convertirse en un cliente DHCP e intentará localizar un servidor DHCP para obtener una configuración desde el mismo. Si no encuentra ningún servidor DHCP, el cliente no podrá disponer de dirección IP y por lo tanto no podrá comunicarse con la red. Si el cliente encuentra un servidor DHCP, éste le proporcionará, para un periodo predeterminado, una configuración IP que le permitirá comunicarse con la red. Cuando haya transcurrido el 50% del periodo, el cliente solicitará una renovación del mismo.

Si reiniciamos el equipo cuya configuración IP se determina por DHCP, pueden darse dos situaciones:

- Si la concesión de alquiler de licencia ha caducado, el cliente solicitará una nueva licencia al servidor DHCP (la asignación del servidor podría o no, coincidir con la anterior).
- Si la concesión de alquiler no ha caducado en el momento del inicio, el cliente intentará renovar su concesión en el servidor DHCP, es decir, que le sea asignada la misma dirección IP.

A continuación se definen algunos términos útiles para la instalación y configuración de un servidor DHCP.

Ámbito servidor DHCP: Un ámbito es un agrupamiento administrativo de equipos o clientes de una subred que utilizan el servicio DHCP.

Rango servidor DHCP: Un rango de DHCP está definido por un grupo de direcciones IP en una subred determinada, como por ejemplo de 192.168.0.1 a 192.168.0.254, que el servidor DHCP puede conceder a los clientes.

Concesión o alquiler de direcciones: es un período de tiempo que los servidores DHCP especifican, durante el cual un equipo cliente puede utilizar una dirección IP asignada.

Reserva de direcciones IP: Consiste en reservar algunas direcciones IP para asignárselas siempre a los mismos PCs clientes de forma que cada uno siempre reciba la misma dirección IP. Se suele utilizar para asignar a servidores o equipos concretos la misma dirección siempre. Es similar a configurar una dirección IP estática pero de forma automática desde el servidor DHCP. En el servidor se asocian direcciones MAC a direcciones IP. Es una opción muy interesante para asignar a ciertos equipos (servidores, impresoras de red, computadoras especiales) siempre la misma IP.

## 1.9.2 TELEFONÍA IP

### 1.9.2.1 ¿QUÉ ES LA TELEFONÍA IP?

La telefonía IP es una tecnología que permite integrar en una misma red - basada en protocolo IP - las comunicaciones de voz y datos. Muchas veces se utiliza el término de redes convergentes o convergencia IP, aludiendo a un concepto un poco más amplio de integración en la misma red de todas las comunicaciones (voz, datos, video, etc.).

Esta tecnología hace ya muchos años que está en el mercado (desde finales de los 90) pero no ha sido hasta hace poco que se ha generalizado gracias, principalmente, a la

mejora y estandarización de los sistemas de control de la calidad de la voz (QoS) y a la universalización del servicio Internet.

Cuando hablamos de un sistema de telefonía IP estamos hablando de un conjunto de elementos que debidamente integrados permiten suministrar un servicio de telefonía (basado en VoIP) a la empresa. Los elementos básicos que forman este sistema son: la centralita IP, el Gateway IP y los diferentes teléfonos IP.

Las principales ventajas de la telefonía IP son la simplificación de la infraestructura de comunicaciones en la empresa, la integración de las diferentes sedes y trabajadores móviles de la organización en un sistema unificado de telefonía - con gestión centralizada, llamadas internas gratuitas, plan de numeración integrado y optimización de las líneas de comunicación - la movilidad y el acceso a funcionalidades avanzadas (buzones de voz, IVR, ACD, CTI, etc.)

#### 1.9.2.2 ¿QUÉ ES UNA CENTRAL IP?

Una Centralita Telefónica (o PBX para *Private Branch Exchange* y PABX para *Private Automatic Branch Exchange* en inglés) es un equipo privado que permite gestionar llamadas telefónicas internas en una empresa, y compartir las líneas de acceso a la red pública entre varios usuarios, para permitir que estos realicen y reciban llamadas desde y hacia el exterior. De alguna manera actúa como una ramificación de la red pública de teléfono.

Una centralita IP o una IP-PBX es una centralita telefónica que trabaja internamente con el protocolo IP. De esta manera, utiliza la infraestructura de comunicaciones de datos (LAN y WAN) para realizar sus funciones. Las centralitas IP pueden por tanto conectarse a servicios públicos VoIP, pero también tienen la capacidad de trabajar con líneas convencionales de teléfono analógico o digitales (RDSI).

Estas características les aportan ventajas a nivel funcional y también a nivel de costes, tanto de inversión como de mantenimiento.

Avanvox es una centralita IP que utiliza la tecnología opensource Asterisk. Incorpora además un servidor de fax basado en Hylafax.

### 1.9.3 EL PROTOCOLO SIP

Es un protocolo de control y señalización usado mayoritariamente en los sistemas de Telefonía IP, fue desarrollado por el IETF (RFC 3261) [32]. Dicho protocolo permite crear, modificar y finalizar sesiones multimedia con uno o más participantes y sus mayores ventajas recaen en su simplicidad y consistencia.

Hasta la fecha, existían múltiples protocolos de señalización tales como el H.323 de la ITU, el SCCP de Cisco, o el MGCP, pero poco a poco SIP está ganando la batalla del estándar: Cisco está progresivamente adoptando SIP como protocolo en sus sistemas de telefonía IP en decremento de H.323 y SCCP, Microsoft ha elegido SIP como protocolo para su nuevo OCS (*Office Communication Server*), y los operadores (de móvil y fijo) también están implantando SIP dentro de su estrategia de convergencia, aprovechando de este modo la escalabilidad que nos proporciona el protocolo SIP.

#### 1.9.3.1 FUNCIONES SIP

El protocolo SIP actúa de forma transparente, permitiendo el mapeo de nombres y la redirección de servicios ofreciendo así la implementación de la IN (Intelligent Network) de la PSTN o RTC.

Para conseguir los servicios de la IN el protocolo SIP dispone de distintas funciones. A continuación se enumeran las más importantes:

- *Localización de usuarios* (SIP proporciona soporte para la movilidad).
- *Capacidades de usuario* (SIP permite la negociación de parámetros).
- *Disponibilidad del usuario*
- *Establecimiento y mantenimiento* de una sesión.

En definitiva, el protocolo SIP permite la interacción entre dispositivos, cosa que se consigue con distintos tipos de mensajes propios del protocolo. Dichos mensajes proporcionan capacidades para registrar y/o invitar un usuario a una sesión, negociar los

parámetros de una sesión, establecer una comunicación entre dos a más dispositivos y, por último, finalizar sesiones.

#### 1.9.3.2 BENEFICIOS DEL PROTOCOLO SIP

En la actualidad, los protocolos más usados en Telefonía sobre IP (ToIP por sus siglas en inglés) son tres: SIP, H.323 e IAX2. Entre las características de cada uno se tiene.

H.323 es un estándar de la ITU que provee especificaciones para ordenadores, sistemas y servicios multimedia por redes que no proveen QoS (calidad de servicio).

Como principales características de H.323 tenemos:

- Implementa QoS de forma interna.
- Control de conferencias

IAX2 (Inter Asterisk eXchange) es un protocolo creado y estandarizado por Asterisk. Unas de sus principales características son: Media y señalización viajan en el mismo flujo de datos.

- *Trunking*
- *Cifrado de datos*

Una de las ventajas de este protocolo es que al enviar el “*streaming*” y la señalización por el mismo flujo de datos, se evitan problemas derivados del NAT. Así pues, no es necesario abrir rangos de puertos para el tráfico RTP. Por último, IAX2 nos permite hacer *trunking* de forma que podemos enviar varias conversaciones por el mismo flujo, lo cual supone un importante ahorro de ancho de banda.

Finalmente SIP un protocolo cada día más sólido. Aspectos importantes referentes a dicho protocolo se enumeran:

- El control de llamadas es *stateless* o sin estado, y proporciona escalabilidad entre los dispositivos telefónicos y los servidores.
- SIP necesita menos ciclos de CPU para generar mensajes de señalización de forma que un servidor podrá manejar más transacciones.

- Una llamada SIP es independiente de la existencia de una conexión en la capa de transporte.
- SIP soporta autenticación de llamante y llamado mediante mecanismos HTTP.
- Autenticación, criptográfica y encriptación son soportados salto a salto por SSL/TSL pero SIP puede usar cualquier capa de transporte o cualquier mecanismo de seguridad de HTTP, como SSH o S-HTTP.
- Un proxy SIP puede controlar la señalización de la llamada y puede bifurcar a cualquier número de dispositivos simultáneamente.

En definitiva, vemos que SIP es un protocolo con una gran escalabilidad, modular y muy apto para convertirse en el futuro inmediato de la ToIP.

## 1.10 PROTOCOLO SNMP

### 1.10.1 ¿QUÉ ES SNMP?

El crecimiento constante de las redes de datos, tanto LANs como WANs, y la conexión entre ellas hace que los aspectos relativos a su control, gestión y monitoreo sea esencial, convirtiéndose en algo a lo que todos los responsables de redes han de prestar una gran atención.

Dado que la tendencia natural de una red cualquiera es a crecer, conforme se añaden nuevas aplicaciones y más y más usuarios hacen uso de la misma, los sistemas de gestión empleados han de ser lo suficientemente flexibles para poder soportar los nuevos elementos que se van añadiendo, sin necesidad de realizar cambios drásticos en la misma.

SNMP fue diseñado en los años 80, su principal objetivo fue el integrar la gestión de diferentes tipos de redes mediante un diseño sencillo y que produjera poca sobrecarga en la red.

Opera en el nivel de aplicación, utilizando el protocolo de transporte TCP/IP, por lo que ignora los aspectos específicos del hardware sobre el que funciona. La gestión se lleva a cabo al nivel de IP, por lo que se pueden controlar dispositivos que estén conectados en

cualquier red accesible desde la Internet, y no únicamente aquellos localizados en la propia red local.

El protocolo SNMP está compuesto por dos elementos: el agente (*agent*), y el gestor (*manager*). Es una arquitectura cliente-servidor, en la cual el agente desempeña el papel de servidor y el gestor hace el de cliente.

El agente es un programa que ha de ejecutarse en cada nodo de red que se desea gestionar o monitorizar. Ofrece un interfaz de todos los elementos que se pueden configurar. Estos elementos se almacenan en unas estructuras de datos llamadas MIB. Representa la parte del servidor, en la medida que tiene la información que se desea gestionar y espera comandos por parte del cliente.

El gestor es el software que se ejecuta en la estación encargada de monitorizar la red, y su tarea consiste en consultar los diferentes agentes que se encuentran en los nodos de la red los datos que estos han ido obteniendo.

Hay un comando especial en SNMP, llamado trap, que permite a un agente enviar datos que no han sido solicitados de forma explícita al gestor, para informar de eventos tales como: errores, fallos en la alimentación eléctrica, etc.

En esencia, el SNMP es un protocolo muy sencillo puesto que todas las operaciones se realizan bajo el paradigma de carga-y-almacenamiento (*load-and-store*), lo que permite un juego de comandos reducido. Un gestor puede realizar sólo dos tipos diferentes de operaciones sobre un agente: leer o escribir un valor de una variable en el MIB del agente. Estas dos operaciones se conocen como petición-de-lectura (*get-request*) y petición-de-escritura (*set-request*). Hay un comando para responder a una petición-de-lectura llamado respuesta-de-lectura (*get-response*), que es utilizado únicamente por el agente.

La posibilidad de ampliación del protocolo está directamente relacionado con la capacidad del MIB de almacenar nuevos elementos. Si un fabricante quiere añadir un nuevo comando a un dispositivo, como puede ser un router, tan sólo tiene que añadir las variables correspondientes a su base de datos (MIB).

### 1.10.2 SEGURIDAD EN SNMP

SNMP ofrece muy poco soporte para la autenticación. Tan sólo ofrece el esquema de dos palabras clave (two-passwords). La clave pública permite a los gestores realizar peticiones de valores de variables, mientras que la clave privada permite realizar peticiones de escritura. A estas palabras clave se les llama en SNMP *communities*. Cada dispositivo conectado con una red gestionada con SNMP, ha de tener configuradas estas dos *communities*.

Es muy común tener asignando por defecto el valor "*public*" al *community* público, y "*private*" al privado. Por lo que es muy importante cambiar estos valores para proteger la seguridad de tu red.

### 1.10.3 ¿QUÉ ES EL MIB?

SNMP define un estándar separado para los datos gestionados por el protocolo. Este estándar define los datos mantenidos por un dispositivo de red, así como las operaciones que están permitidas. Los datos están estructurados en forma de árbol; en el que sólo hay un camino desde la raíz hasta cada variable. Esta estructura en árbol se llama *Management Information Base* (MIB) y se puede encontrar información sobre ella en varios RFC's.

La versión actual de TCP/IP MIB es la 2 (MIB-II) y se encuentra definida en el RFC-1213 [35]. En ella se divide la información que un dispositivo debe mantener en ocho categorías (ver Tabla 7). Cualquier variable ha de estar en una de estas categorías.

La definición de un elemento concreto MIB implica la especificación del tipo de dato que puede contener. Normalmente, los elementos de un MIB son enteros, pero también pueden almacenar cadenas de caracteres o estructuras más complejas como tablas. A los elementos de un MIB se les llama "objetos". Los objetos son los nodos hoja del árbol MIB, si bien, un objeto puede tener más de una instancia, como por ejemplo un objeto tabla. Para referirse al valor contenido en un objeto, se ha de añadir el número de la instancia. Cuando sólo exista una instancia del objeto, está es la instancia cero.



Categoría	Información
system	Información del host del sistema de encaminamiento
interfaces	Información de los interfaces de red
addr-translation	Información de traducción de direcciones
ip	Información sobre el protocolo IP
icmp	Información sobre el protocolo ICMP
tcp	Información sobre el protocolo TCP
udp	Información sobre el protocolo UDP
egp	Información sobre el protocolo (Exterior Gateway)

Tabla 7. Categorías TCP/IP

Por ejemplo, el objeto ifNumber de la categoría "interfaces" es un entero que representa el número de interfaces presentes en el dispositivo; mientras el objeto ipRoutingTable de la categoría "ip" contiene la tabla de enrutamiento del dispositivo.

Hay que acordarse de utilizar el número de la instancia para leer el valor de un objeto. En este caso, el número de interfaces presentes en un router puede ser observado mediante la instancia ifNumber.0.

En el caso de ser un objeto tabla, se ha de utilizar el índice a la tabla como último número para especificar la instancia (fila de la tabla).

Existe otro estándar que define e identifica las variables MIB, llamado "*Structure of Management Information*" (SMI). SMI especifica las variables MIB, éstas se declaran empleando un lenguaje formal ISO llamado ASN.1, que hace que tanto la forma como los contenidos de estas variables sean no ambiguos.

El espacio de nombres ISO (árbol) está situado dentro de un espacio de nombres junto con otros árboles de otros estándares de otras organizaciones. Dentro del espacio de nombres ISO hay una rama específica para la información MIB. Dentro de esta rama MIB,

los objetos están a su vez jerarquizados en subárboles para los distintos protocolos y aplicaciones, de forma que esta información puede representarse unívocamente.

La Figura 27 muestra el espacio de nombres del MIB del TCP/IP, éste está situado justo bajo el espacio del IAB "mgmt". La jerarquía también especifica el número para cada nivel.

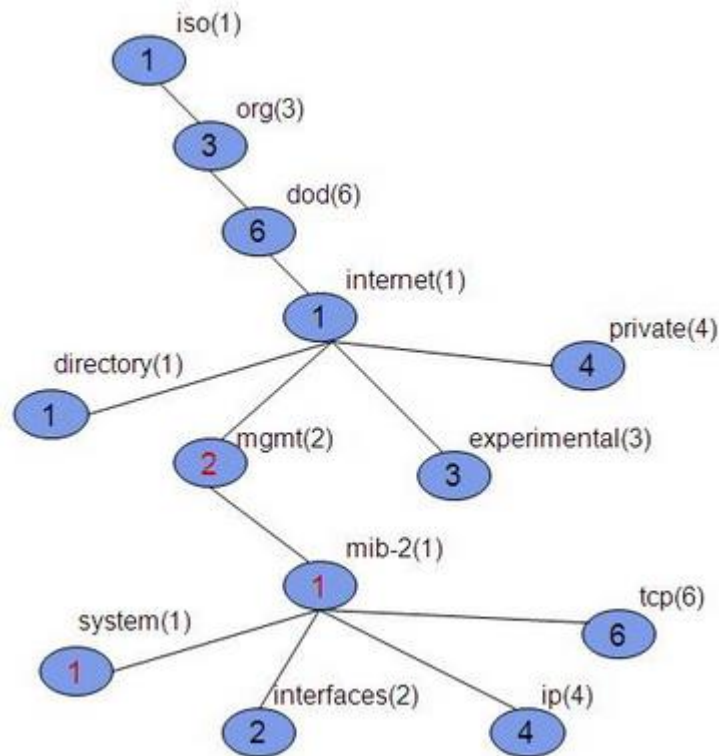


Figura 27. TCP/IP Organizational Tree [36]

Es importante constatar que la mayor parte del software necesita el punto raíz (.) para localizar el objeto en el MIB. Si no se incluye el punto raíz, se asume que el path es relativo desde .iso.org.dod.internet.mgmt.mib-2.

De esta forma, el objeto ifNumber de la categoría "interfaces" se puede llamar:

.iso.org.dod.internet.mgmt.mib-2.interfaces.ifnumber

o el equivalente numérico: .1.3.6.1.2.1.2.1

y la instancia es: .iso.org.dod.internet.mgmt.mib-2.interfaces.ifnumber.0

o el equivalente numérico: .1.3.6.1.2.1.2.1.0

#### 1.10.4 CACTIEZ

CactiEZ [37] es una completa solución de software libre para la generación de gráficos en red, diseñada para aprovechar el poder de almacenamiento y la funcionalidad para gráficas que tienen las aplicaciones RRDtool.

CactiEZ es una distribución Linux (basada en Centos 6.3) que se instala sólo en 5 minutos y tiene ya integrado todo los paquetes necesarios (Cacti y otros) para monitorizar el tráfico de las interfaces de red: Firewall, swiches, routers y servidores Unix/Linux y Windows.

Tiene una interfaz de usuario fácil de usar, que resulta conveniente para instalaciones del tamaño de una LAN, así como también para redes complejas con cientos de dispositivos.

Con Cacti no solo visualizamos el tráfico de red en forma de gráficas a lo largo del tiempo, sino que podemos también configurar alertas (Umbrales) para recibir aviso por correo electrónico cuando sobrepasemos un valor determinado (ancho de banda de entrada o de salida, uso de disco de un servidor, etc).

La versión más reciente de CactiEZ se puede descargar desde el sitio oficial <http://cactiez.cactiusers.org/download/> completamente gratis.

#### 1.10.5 WEATHERMAP

Weathermap es una herramienta de visualización de red, está basada en *open source*, toma los datos que ya tiene y muestra un esquema general en forma de mapa.

Los datos se recogen a través de plugins. Los cuales se suministran para RRDtool, MRTG, archivos de texto delimitados por tabuladores, SNMP, fping, scripts externos, y datos de Cacti específicos. El plugin RRDtool significa que tiene acceso a los datos de una amplia gama de herramientas de monitorización de *open source*, incluyendo Cacti, Cricket, Zenoss, MRTG, Routers2, Munin y muchos más.

La instalación de Weathermap incluye un editor en el que se pueden crear los mapas, y agregar las características como tráfico de cada interfaz, temperatura del equipo y todas los parámetros que pueda controlar SNMP, además de las imágenes e iconos por defecto el editor permite subir imágenes de fondo, iconos específicos para los dispositivos de red que ayudan a personalizar un mapa a conveniencia del usuario.

La versión de Cacti usada en el presente trabajo de graduación es un sistema operativo basado en CentOS y solo se debe habilitar el plugin adicional para weathermap, sin embargo se puede instalar independientemente pero hay que cambiar la arquitectura de Cacti y modificar unos archivos en los directorios, en la siguiente página <http://network-weathermap.com/> [38] se pueden encontrar características y todas las versiones de wathermap, también se puede descargar la versión actual del plugin.

#### 1.11 SIMULADOR DE REDES MIKROTIK [39]

Actualmente existen proveedores de equipos como Cisco y Juniper que tienen la facilidad de poder emular su software de *networking* usando un simulador, lo cual permiten aprender y desarrollar topologías de red, facilitando el aprendizaje y uso de sus dispositivos.

El uso de las simulaciones durante el diseño de redes es importante porque permite estudiar el comportamiento del sistema y de los dispositivos de *networking* antes de su implementación para tener un alto porcentaje de seguridad de que tanto el diseño como los equipos que vamos a utilizar cumplen de manera satisfactoria los objetivos y las funciones para los cuales fueron elegidos.

Además las simulaciones permiten tener un continuo entrenamiento y actualización de los conocimientos, al plantear situaciones muy parecidas a casos reales, a través de las cuales los administradores de red podrán poner a prueba sus conocimientos y experimentar nuevas alternativas en la solución de problemas de red y su posible impacto en el mundo real, impacto relativo a costos de implementación, mantenimiento, escalabilidad y satisfacción de los usuarios.

Mikrotik no posee un simulador de manera oficial, sin embargo, es posible simular su sistema operativo RouterOS mediante herramientas de software libre.

### 1.11.1 HERRAMIENTAS

GNS3 es un simulador gráfico de red que permite diseñar topologías de red complejas y poner en marcha simulaciones sobre ellos, trabaja nativamente con *Dynamips* para emular la plataforma Cisco y Qemu para emular otros sistemas operativos. En la tabla 8 se muestran las características del simulador y el sistema RouterOS de Mikrotik.

GNS3 también es capaz de enlazarse con otros entornos de virtualización como Virtualbox, y VMware. En la Tabla 9 se comparan las características de los entornos de virtualización más utilizados.




		
<ul style="list-style-type: none"> <li>• Simulador grafico de red.</li> <li>• Software de código abierto.</li> <li>• Es multiplataforma.</li> <li>• Permite simular topologías de redes complejas.</li> <li>• Ejecuta varios tipos de dispositivos de red.</li> </ul>	<ul style="list-style-type: none"> <li>• Conocido como Quick EMUlator.</li> <li>• Software de código abierto.</li> <li>• Emula sistemas de forma completa.</li> <li>• Es una alternativa: VMware, Virtualbox, KVM, etc</li> </ul>	<ul style="list-style-type: none"> <li>• Tiene nivel de licencia 0.</li> <li>• Esta desarrollado para la arquitectura x86.</li> <li>• Puede ser instalado desde varios medios, como cd, usb, etc.</li> <li>• Se puede instalar en una PC o Power PC.</li> </ul>

Tabla 8. Características del simulador GNS3. [39]

A partir de esta tabla es posible concluir que Qemu es la mejor opción para emular el sistema RouterOS en GNS3 ya que permite con una sola imagen emular todos los routers que nuestra computadora pueda soportar, su consumo de memoria es bajo, e interactúa directamente con la interfaz gráfica de GNS3.

EMPRESA	POSIBILIDAD DE PONER EN GNS3 (GUI)	LICENCIA	USO DE MEMORIA	OBSERVACIONES
VMWare	Solo conectado	Libre, comercial	Alto	1 imagen por cada router
Virtual Box	Si	Libre	Alto	1 imagen por cada router
Qemu	Si	Libre	Bajo	1 imagen para todos los routers

Tabla 9. Características de los entornos de virtualización. [40]

### 1.11.2 PRUEBAS DE RENDIMIENTO

En la figura 28 se muestra una gráfica de rendimiento que representa la cantidad de memoria RAM utilizada por cada router Mikrotik simulado en GNS3 instalado en una computadora con sistema operativo Windows 7.

Al simular Mikrotik con Qemu solo incrementa principalmente el uso de la memoria RAM, el uso del CPU no es afectado.

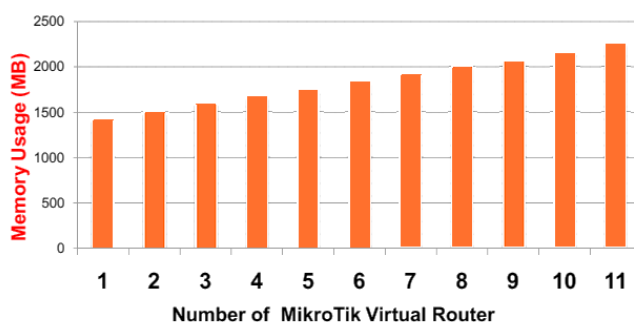


Figura 28. Gráfica de uso de memoria vrs cantidad de router virtuales. [40]

Por cada nuevo router que se agrega al simulador el consumo de memoria RAM incrementa aproximadamente 80MB.

A partir de estos datos podemos hacer un cálculo aproximado de la cantidad máxima de router que podemos simular. Así por ejemplo si tenemos un total de memoria RAM en nuestra computadora de 4GB y un consumo de memoria del sistema operativo Windows 7 de 1.5GB, la cantidad de router vendrá dada por la cantidad de memoria total libre entre la cantidad de memoria utilizada por cada router:  $(4000\text{MB}-1500\text{MB})/80 = 31$  routers).

### DISEÑO E IMPLEMENTACIÓN

En este capítulo se describen mediante ejemplos prácticos los comandos necesarios para configurar diferentes servicios y protocolos tales como RIP, OSPF, SNMP, DHCP, VLAN, NAT, port forwarding y firewall en una *RouterBoard* modelo 750 de la empresa MikroTik.

El primer tema que se aborda es acerca de la emulación de la versión trial de RouterOS utilizando QEMU y GNS3, para preparar un laboratorio virtual que nos permita simular redes con router MikroTik sin necesidad de adquirir un equipo físico.

En el segundo tema se explican los comandos que nos permiten definir IP a una interfaz ethernet, rutas estáticas y rutas por defecto en el sistema operativo RouterOS. Continuamos con la configuración del protocolo RIP version 2, y los comandos que definen las redes que entran en el proceso de enrutamiento y la redistribución de rutas estáticas.

En el siguiente tema se explican los comandos para configurar los servicios de VLAN y DHCP que nos permitan escalar la red mediante el uso de Switch programables y facilitar las configuraciones para que el usuario final pueda tener acceso a internet. Describimos después los comandos para enrutar una red mediante el protocolo OSPF, la utilización de interfaces loopback y la implementación de políticas de acceso a través de un firewall. Se hace una breve reseña del protocolo BGP y su configuración; luego se explican los comandos para la creación de túneles VPN del tipo IPIP y GRE entre router MikroTik y router Cisco.

Una vez que hemos comprendido los fundamentos básicos de enrutamiento estático y dinámico se explica el funcionamiento y configuración del protocolo MPLS, el cual es un protocolo utilizado principalmente en las redes core de los proveedores de internet. También se explica la configuración de un servidor de monitoreo de tráfico utilizando Cacti y el plugin WeatherMap el cual nos permitirá visualizar de forma gráfica el consumo del ancho de banda de cada router.

Para finalizar se muestra un ejemplo práctico de NAT y el reenvío de puertos aplicado a una cámara web, a través de configuraciones de Port Forwarding.

## 2.1 SIMULACIÓN DE ROUTEROS EN GNS3

GNS3 es un simulador gráfico de redes que le permite diseñar fácilmente topologías de red y luego ejecutar simulaciones en él. Soporta el IOS de routers, ATM/Frame Relay/switchs Ethernet, ASA y PIX firewalls de forma nativa ya que incorpora herramientas como Dynamips, QEMU y Dynagen.

Sin embargo también permite enlazar máquinas virtuales de otros entornos de virtualización externos como VirtualBox y QEMU lo cual permite utilizar otros sistemas operativos para dispositivos de red como RouterOS, JunOS y cualquier otro sistema que este soportado por estos entornos de virtualización. Una característica especial de GNS3 es que nos permite conectar las redes virtuales que armemos a redes reales, posee una interfaz gráfica de usuario intuitiva, es de código abierto y multiplataforma [39].

El paquete de instalación para el sistema Windows incluye los siguientes programas:

- Dynamips: es un emulador de routers Cisco escrito por Christophe Fillot. Emula a las plataformas 1700, 2600, 3600, 3700 y 7200, y ejecuta imágenes de IOS estándar.
- QEMU: es una plataforma de emulación y virtualización de hardware basado en la traducción dinámica de binarios (conversión del código binario de la arquitectura fuente en código entendible por la arquitectura huésped). Permite emular un sistema operativo dentro de otro sin tener que reparticionar el disco duro, empleando para su ubicación cualquier directorio dentro de éste.
- WinPcap: es la herramienta estándar utilizada por la Industria para acceder a conexiones entre capas de red funcionando bajo sistema operativo Windows, con esta herramienta podemos capturar-transmitir paquetes de red manipulando la pila de protocolos.
- Wireshark: es un analizador de protocolos basado en las librerías pcap utilizado comúnmente como herramienta de diagnóstico de redes y de desarrollo de aplicaciones de red. Es de código abierto, versátil, multiplataforma y está apoyado en una completa interfaz gráfica que facilita enormemente su uso.
- PuTTY: es un emulador de consola de código abierto y multiplataforma que tiene la capacidad de actuar como un cliente para el SSH, Telnet, rlogin, TCP raw entre otros.



- SolarWinds Standard Toolset: es un conjunto de herramientas de red que facilita las tareas de administración y monitoreo de la red en tiempo real a través de un navegador web. Entre sus funciones se encuentra el monitoreo del CPU, el ancho de banda, diagnóstico de problemas, administración remota, la detección de nuevos dispositivos entre otras.

### 2.1.1 INSTALACIÓN Y CONFIGURACIÓN DE MÁQUINAS VIRTUALES EN GNS3

A continuación se describe el proceso de instalación de RouterOS en una máquina virtual QEMU (previamente instalado) y posteriormente su configuración en GNS3 v1.3.3 para el sistema Windows [40].

- 1) Primero procedemos a realizar la descarga de la imagen ISO de RouterOS desde la página de MikroTik (<http://www.mikrotik.com/download>) y descargamos la versión x86 como se muestra en la figura 29.

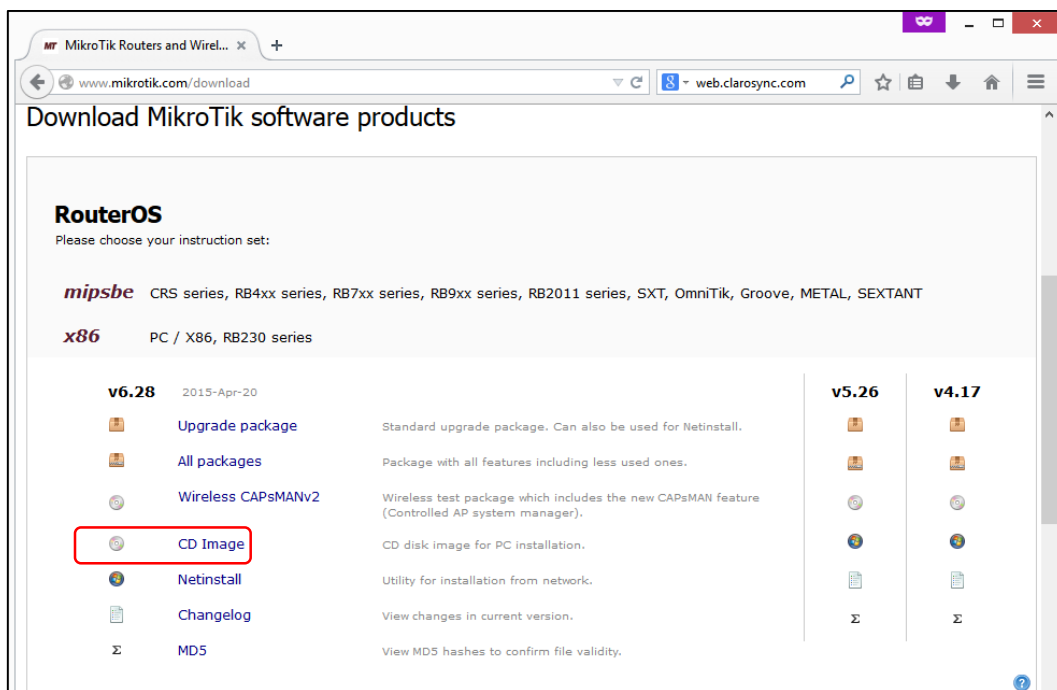


Figura 29. Sitio de descarga de RouteOS.

- 2) Movemos el archivo ISO descargado (mikrotik-6.28.iso) a la carpeta donde se encuentra instalado QEMU (C:\Program Files\GNS3\qemu-2.1.0).

- 3) Abrimos la consola de comandos de Windows con privilegios de administración y nos ubicamos en la carpeta donde está instalado QEMU con el siguiente comando.

```
cd "C:\Program Files\GNS3\qemu-2.1.0"
```

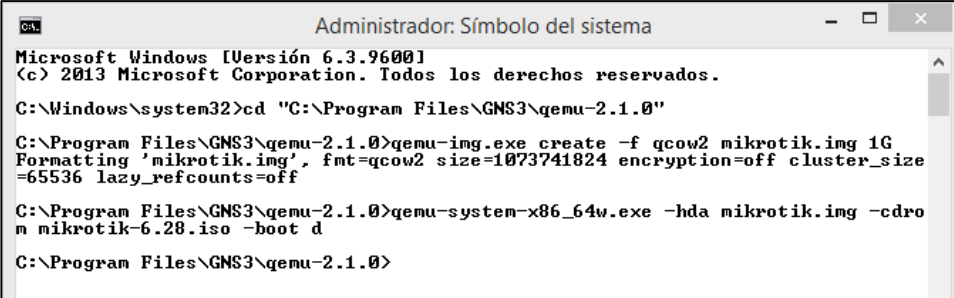
- 4) Ejecutamos el siguiente comando para crear el archivo de imagen de la máquina virtual, con el nombre *mikrotik.img*

```
qemu-img.exe create -f qcow2 mikrotik.img 1G
```

- 5) Arrancamos la máquina virtual con QEMU (en este caso es la versión QEMU de 64 bits) desde la imagen ISO para realizar la instalación de RouterOS.

```
qemu-system-x86_64w.exe -hda mikrotik.img -cdrom mikrotik-6.28.iso -boot d
```

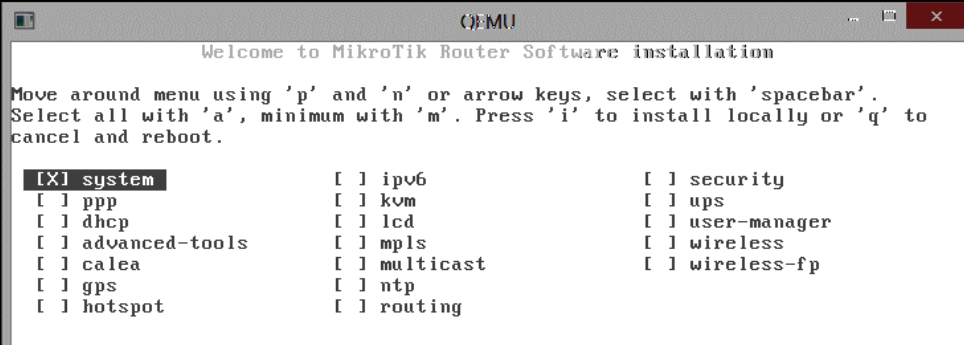
Los resultados se muestran en la figura 30.



```
Administrador: Símbolo del sistema
Microsoft Windows [Versión 6.3.9600]
(c) 2013 Microsoft Corporation. Todos los derechos reservados.
C:\Windows\system32>cd "C:\Program Files\GNS3\qemu-2.1.0"
C:\Program Files\GNS3\qemu-2.1.0>qemu-img.exe create -f qcow2 mikrotik.img 1G
Formatting 'mikrotik.img', fmt=qcow2 size=1073741824 encryption=off cluster_size=65536 lazy_refcounts=off
C:\Program Files\GNS3\qemu-2.1.0>qemu-system-x86_64w.exe -hda mikrotik.img -cdrom mikrotik-6.28.iso -boot d
C:\Program Files\GNS3\qemu-2.1.0>
```

Figura 30. Ejecución de comandos en el Símbolo del Sistema.

Se abrirá una ventana donde se inicia el proceso de instalación similar al que se realiza desde un USB o CD-ROM como se muestra en la figura 31.



```
QEMU
Welcome to MikroTik Router Software installation

Move around menu using 'p' and 'n' or arrow keys, select with 'spacebar'.
Select all with 'a', minimum with 'm'. Press 'i' to install locally or 'q' to
cancel and reboot.

[X] system          [ ] ipv6           [ ] security
[ ] ppp             [ ] kvm            [ ] ups
[ ] dhcp            [ ] lcd            [ ] user-manager
[ ] advanced-tools [ ] mpls           [ ] wireless
[ ] calea           [ ] multicast     [ ] wireless-fp
[ ] gps             [ ] ntp
[ ] hotspot         [ ] routing
```

Figura 31. Instalación de RouterOS.

- 6) Seleccionamos todos los paquetes con la barra espaciadora del teclado y a continuación presionamos la tecla [i] para iniciar la instalación. Al finalizar obtendremos un resultado como el que se muestra en la figura 32.
- 7) Cerramos la ventana y comprobamos la correcta instalación haciendo bootear el sistema operativo desde el disco duro virtual.

```
qemu-system-x86_64w.exe mikrotik.img -boot c
```

Nos solicitará el usuario (admin) y password por defecto (dejar en blanco), luego presionamos "Enter" para continuar. La pantalla inicial es como se muestra en la figura 33. Una vez comprobado que la instalación fue exitosa apagamos la máquina virtual ejecutando: `system shutdown`.

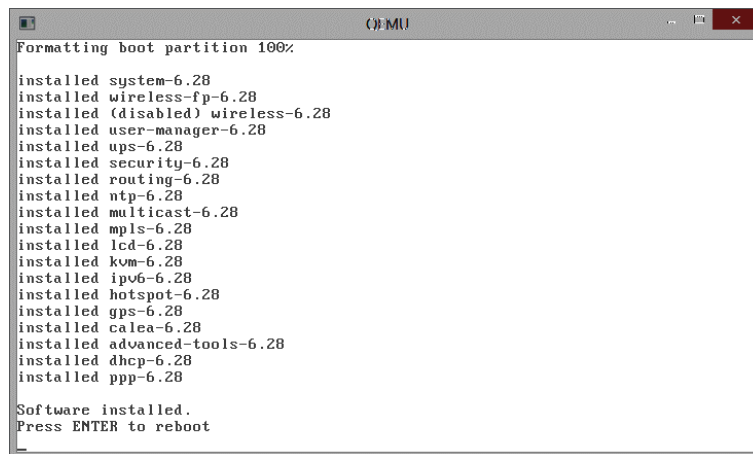


Figura 32. Instalación de RouteOS exitosa.

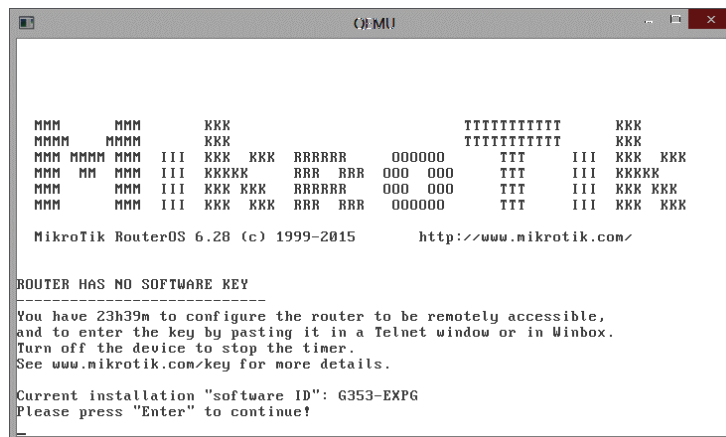


Figura 33. Sistema operativo RouterOS.

Para poder utilizar esta máquina virtual en GNS3 hacemos las siguientes configuraciones:

- 8) Primero abrimos GNS3 y nos dirigimos al menú *Edit > Preferences > Qemu VMs* como se muestra en la figura 34.

Luego presionamos el botón *New* para agregar una máquina virtual, aparecerá un asistente de configuración donde seleccionaremos los siguientes parámetros:

```
Type: Default
Name: Mikrotik
Qemu Binary: C:\Program Files\GNS3\qemu-2.1.0\qemu-system-x86_64w.exe (PARA LA VERSION DE 64BITS)
RAM: 128 MB (hasta un mínimo de 32MB)
Disk image (hda): C:/Program Files/GNS3/qemu-2.1.0/mikrotik.img
```

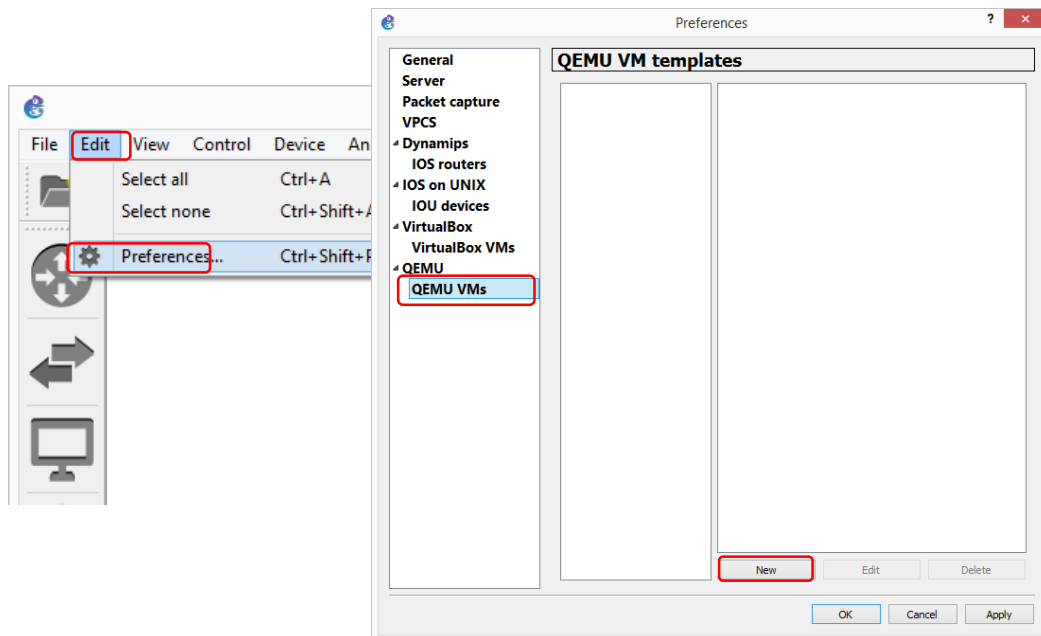


Figura 34. Configuración de máquina virtual QEMU en GNS3.

- 9) En la figura 35 se observa que, por defecto solo tendrá una tarjeta de red; para editar las tarjetas de red hacemos clic en el botón *Edit > Network* y especificamos el número y tipo de tarjetas, en este caso se seleccionaron 5 adaptadores de red tipo Intel Gigabit Ethernet y presionamos OK.

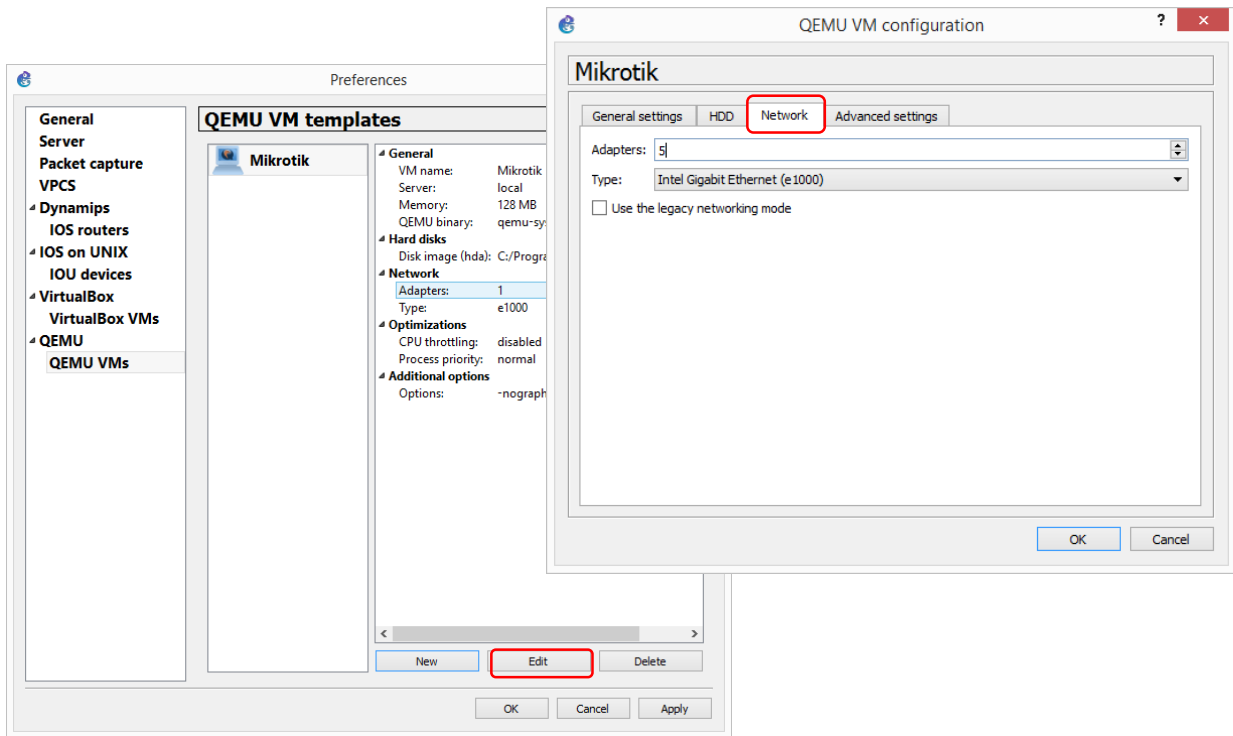


Figura 35. Configuración de interfaces de red.

10) Para modificar el símbolo del router, hacemos clic derecho sobre el ícono actual y en *Change Symbol*; aparecerá una ventana como la de la figura 36 luego seleccionamos un ícono de nuestra preferencia y presionamos OK.

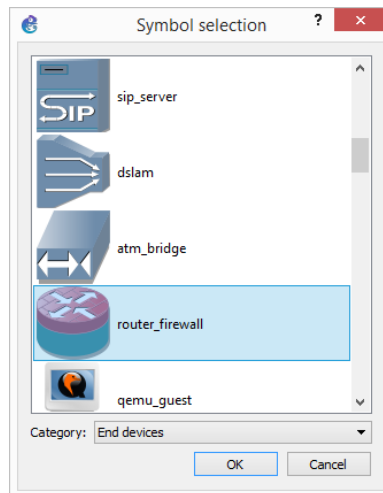


Figura 36. Cambio de símbolo de la máquina virtual.

Finalmente presionamos en OK y ya podemos empezar a construir y simular redes desde la interfaz de GNS3 con router MikroTik, solamente arrastramos el ícono del dispositivo en el área de trabajo y realizamos las conexiones con otros equipos así como se muestra en la figura 37.

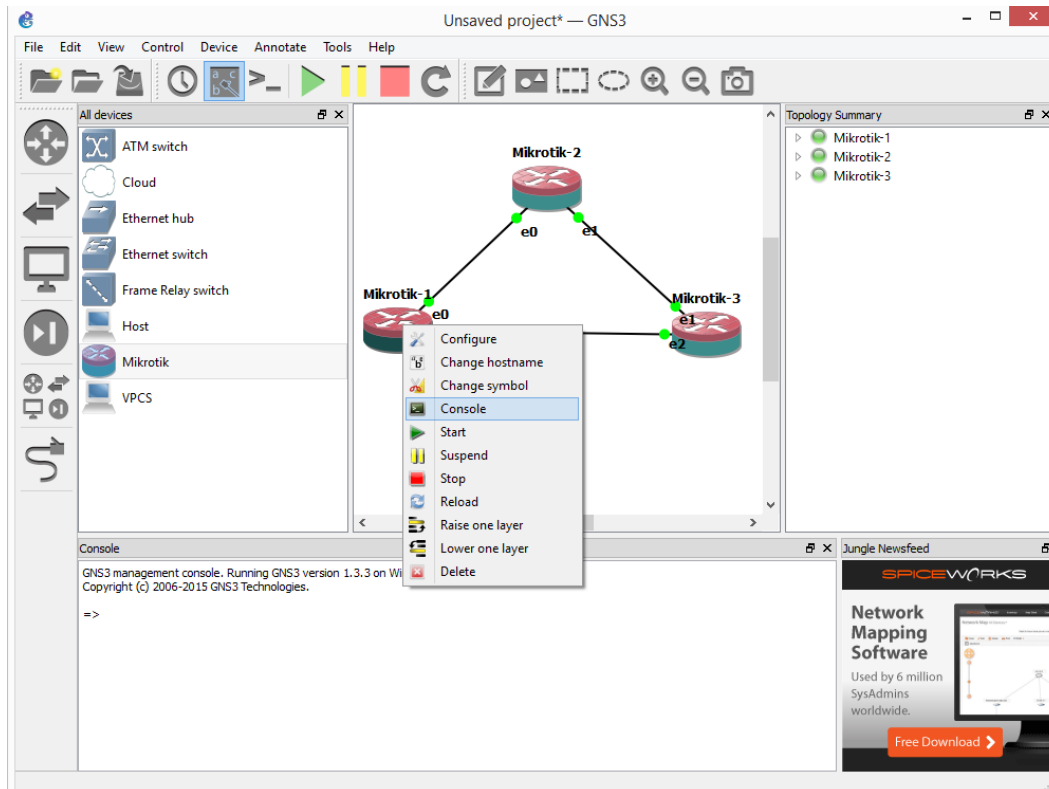


Figura 37. Simulación de redes en GNS3 con router MikroTik.

## 2.2 ENRUTAMIENTO ESTÁTICO

El enrutamiento es fundamental para cualquier red de datos, ya que transfiere información a través de una red de trabajo origen a una red destino.

Las rutas estáticas son definidas manualmente por el administrador para que el router aprenda sobre una red remota. Las rutas estáticas necesitan pocos recursos del sistema, es recomendable utilizarlas cuando nuestra red esté compuesta por un número reducido de routers o que la red se conecte a internet solamente a través de un único ISP [41].

Las rutas estáticas son muy comunes y no requieren la misma cantidad de procesamiento y sobrecarga que generan los protocolos de enrutamiento dinámico [42].

### 2.2.1 EJEMPLO PRÁCTICO

En la figura 38 se presenta el diagrama para la configuración de enrutamiento estático.

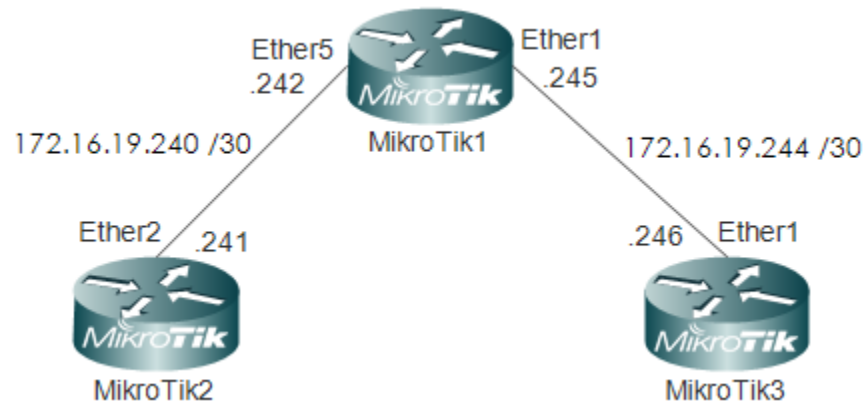


Figura 38. Red a configurar enrutamiento estático.

### 2.2.2 CONFIGURACIONES

Para la configuración de una ruta estática, deben establecerse las ip de cada interfaz involucrada. Para ello se debe ir al directorio `/ip address>` donde podemos agregar una ip con el nemotécnico `add` y especificar la dirección con `address={IP/MASK}`, además de la interfaz a la que se asigna la configuración con `interface= {etherX}`.

Una ruta por defecto para el caso de una sola conexión de salida puede ser establecida mediante la instrucción `add gateway= {IP}` dentro del directorio `/ip route>`, donde también se verifica las rutas disponibles con el comando `print`.

Si existe más de una conexión entre router con diferentes redes será necesario más que una ruta por defecto, es en este caso donde se configura enrutamiento estático especificando la red desconocida mediante `dst-address={IP/MASK}` y su respectiva puerta de salida con `gateway={IP}`.

- 1) Establecer las ip a las interfaces que sea necesario.

Router MikroTik1 (El mismo proceso para los otros MikroTik)

```
/ip address
add address=172.16.19.245/30 interface=ether1
add address=172.16.19.242/30 interface=ether5
```

2) Configurar las rutas estáticas.

Router MikroTik2

```
/ip route
add gateway=172.16.19.242
```

Router MikroTik3

```
/ip route
add dst-address=172.16.19.240/30 gateway=172.16.19.245
```

### 2.3 ENRUTAMIENTO DINÁMICO RIP V2

RIP es un protocolo importante por ser uno de los primeros en implementarse y servir de base para la evolución de los protocolos de enrutamiento dinámico [43]. Entre sus características básicas habría que destacar las siguientes:

- Es un protocolo de enrutamiento vector distancia.
- Utiliza el conteo de saltos como su única métrica o coste para la selección de rutas.
- Las rutas publicadas con conteo de saltos mayores que 15 son inalcanzables.
- Se transmiten mensajes cada 30 segundos.
- Tiene asignada una distancia administrativa de 120.

#### 2.3.1 EJEMPLO PRÁCTICO

En la figura 39 se presenta el diagrama de red para enrutamiento dinámico RIP

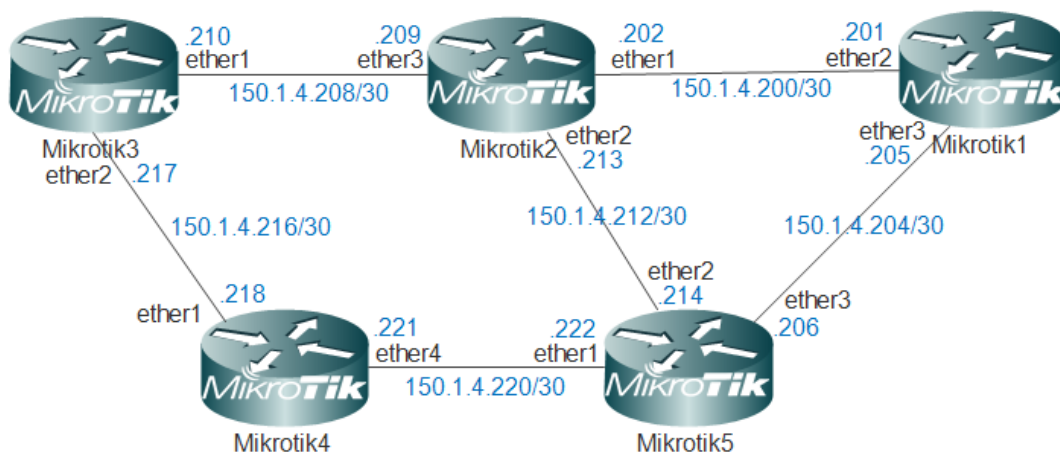


Figura 39. Red a configurar enrutamiento dinámico RIP.



### 2.3.2 CONFIGURACIONES

Para acceder a la configuración general de RIP se debe estar en el submenú `/routing rip` donde se establece con la instrucción `set` las diferentes opciones, entre ellas las más básicas tenemos distribuir rutas por defecto `distribute-default={ always | if-installed | never }`, distribuir redes directamente conectadas `redistribute-connected= yes | no`, distribuir rutas estáticas `redistribute-static=yes`[44]

Ahora solo resta especificar las redes que RIP debe anunciar a sus vecinos, mediante la instrucción `add network={IP/MASK}` en el submenu `/routing rip network>`, a continuación se muestra la configuración para el Router MikroTik1 de la Figura 39, la cual debe repetirse en los demás router con sus respectivas redes.

- 1) Activar y configurar opciones de RIP.

MikroTik1

```
>routing rip set distribute-default=always redistribute-  
connected=yes redistribute-static=yes
```

- 2) Establecer las redes que se anunciarán con RIP.

MikroTik1

```
/routing rip network>add network=150.1.4.204/30  
/routing rip network>add network=150.1.4.200/30
```

Esta configuración es similar para los router que hablarán RIP. Para más detalles sobre rip.

### 2.4 VLAN Y SERVICIOS DHCP

Una red de área local virtual (VLAN) es un método de capa 2 que permite múltiples LANs virtuales en una sola interfaz física [45] (Ethernet, inalámbricos, etc.), dando la posibilidad de separar las redes LAN de manera eficiente mediante el etiquetado de paquetes [46].

Al separar los grupos de usuarios en redes VLAN, se mejora la administración, optimización y seguridad de la red al reducir los dominios de broadcast [47].

En la tecnología de switching, tenemos tres modos de puertos:

1. Acceso: es el que se utiliza sólo con los paquetes sin etiquetar (untagged). Este tipo de puerto es donde se conecta el PC al switch.

2. Troncal: es un puerto capaz de recibir y enviar paquetes de múltiples VLAN's (tagged). Se utiliza para interconectar los switches.
3. Híbrido: es un modo especial que permite paquetes etiquetados y no etiquetados en el mismo puerto.

RouterOS es capaz de realizar las funciones de etiquetado de paquetes a través de la creación de interfaces VLAN y soporta los protocolos 802.1Q y Q-in-Q.

El protocolo de configuración dinámica de host DHCP (por sus siglas del inglés) es un protocolo de red que permite a los clientes de una red IP obtener sus parámetros de configuración automáticamente.

RouterOS soporta un servidor DHCP por cada interface de red brindando las funciones básicas para entregar por cada petición de un cliente una dirección IP, máscara de red, gateway, nombre de dominio, servidor DNS y servidor WINS (para clientes Windows). Para esto se requiere configurar un rango de direcciones IP (sin incluir la IP del servidor DHCP) y las IP de red a las que pertenecen.

#### 2.4.1 EJEMPLO PRÁCTICO

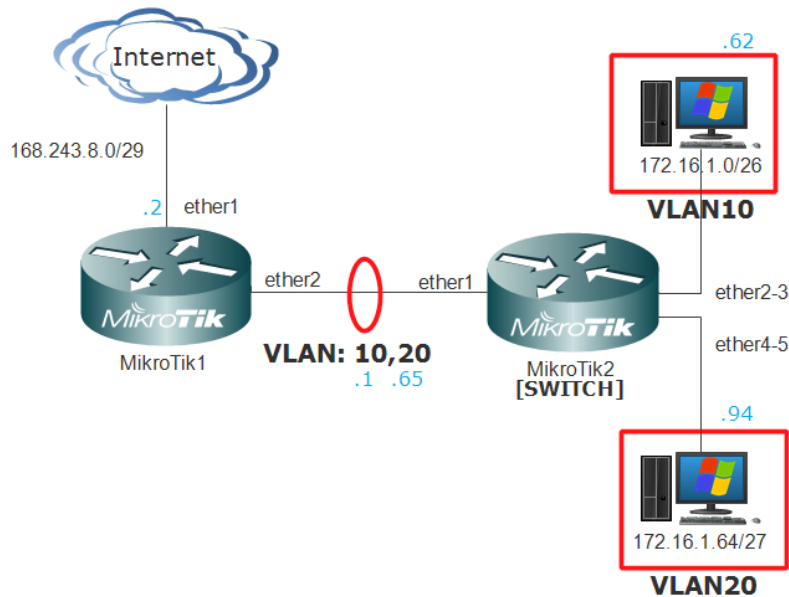


Figura 40. Implementación de VLAN y DHCP.

En la figura 40 se muestra una red con acceso a internet con dos redes locales virtuales conectadas al router principal mediante un único enlace troncal y que proveerá IP's dinámicamente mediante DHCP. El router 2 que se muestra será utilizado solamente como switch para mostrar otros modos de configuración de los puertos.

#### 2.4.2 CONFIGURACIONES

Las configuraciones necesarias para implementar VLAN y DHCP en la red de la figura 40 se muestran a continuación.

- 1) Identificamos el router con un nombre utilizando el siguiente comando:

```
/system identity set name=ROUTER-MIKROTIK
```

- 2) A continuación procedemos a la creación de las interfaces virtuales para cada VLAN asociadas a la interfaz física ether2 (enlace troncal) con su correspondiente nombre y número id.

```
/interface vlan  
add interface=ether2 name=VLAN10 vlan-id=10  
add interface=ether2 name=VLAN20 vlan-id=20
```

- 3) Luego asignamos una dirección IP a cada interfaz virtual.

```
/ip address  
add address=172.16.1.1/26 comment=VLAN10 interface=VLAN10  
add address=172.16.1.65/27 comment=VLAN20 interface=VLAN20
```

- 4) Creamos un servidor DHCP por cada VLAN. Empezamos con un pool indicando un nombre y rango de direcciones.

```
/ip pool  
add name=dhcp_pool1 ranges=172.16.1.2-172.16.1.62  
add name=dhcp_pool2 ranges=172.16.1.66-172.16.1.94
```

- 5) Después habilitamos el servidor DHCP en cada interfaz.

```
/ip dhcp-server  
add address-pool=dhcp_pool1 disabled=no interface=VLAN10  
name=dhcp1  
add address-pool=dhcp_pool2 disabled=no interface=VLAN20  
name=dhcp2
```

- 6) Añadimos la información que se proporcionará a los nuevos hosts: IP de red, servidores DNS locales o públicos y gateway.

```
/ip dhcp-server network
add address=172.16.1.0/26 dns-server=8.8.8.8,172.16.1.10
gateway=172.16.1.1
add address=172.16.1.64/27 dns-server=8.8.8.8,172.16.1.162
```

- 7) Finalmente para brindar acceso a internet desde el router principal configuramos una dirección IP pública, una ruta por defecto (interfaz ether1) y un NAT que enmascare nuestra red local (172.16.1.0/24) para poder comunicarnos con otras redes externas como internet. Para más información sobre NAT ver Sección 2.9.

```
/ip address
add address=168.243.8.2/29 comment=WAN interface=ether1
/ip route add distance=1 gateway=168.243.8.1
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1 src-
address=172.16.1.0/24
```

- 8) El segundo router solo realizará funciones de capa 2 (Switch) por lo tanto solo es necesario configurar el modo de funcionamiento de cada puerto sin asignar ninguna IP. Empezamos identificando el dispositivo.

```
/system identity set name=SW-MIKROTIK
```

- 9) Procedemos a la creación de las interfaces virtuales para cada VLAN asociadas a la interfaz física ether1 (enlace troncal) con su correspondiente nombre y número id.

```
/interface vlan
add interface=ether1 name=VLAN10 vlan-id=10
add interface=ether1 name=VLAN20 vlan-id=20
```

- 10) Creamos un bridge por cada VLAN.

```
/interface bridge
add name=br-vlan10
add name=br-vlan20
```

11) Asignamos puertos a cada bridge que incluyan los puertos no etiquetados donde se conectarán las PC's y la interface VLAN a la que pertenecen.

```
/interface bridge port
add bridge=br-vlan10 comment="interface VLAN10" interface=VLAN10
add bridge=br-vlan10 comment="puerto acceso VLAN10"
interface=ether2
add bridge=br-vlan10 comment="puerto acceso VLAN10"
interface=ether3
```

```
add bridge=br-vlan20 comment="interface VLAN20" interface=VLAN20
add bridge=br-vlan20 comment="puerto acceso VLAN20"
interface=ether4
add bridge=br-vlan20 comment="puerto acceso VLAN20"
interface=ether5
```

Una vez configurado, las computadoras que sean conectadas en los puertos ether2 y ether3 del switch pertenecerán a la VLAN10 y las que se conecten a los puertos ether4 y ether5 pertenecerán a la VLAN20, además cada computadora conectada recibirá desde el router principal una IP (en orden descendente), máscara, gateway y DNS para tener acceso a internet. Para más ejemplos de aplicación sobre VLAN y DHCP.

## 2.5 ENRUTAMIENTO OSPF Y FIREWALL

OSPF es un protocolo de estado de enlace basado en el algoritmo Dijkstra el cual permite calcular la distancia más corta entre la fuente y el destino al determinar la ruta para un grupo específico de paquetes [48]. Entre sus características básicas habría que destacar las siguientes:

- Sus mensajes se encapsulan en un paquete IP con indicador de protocolo 89.
- La dirección de destino se establece para una de dos direcciones multicast: 224.0.0.5 ó 224.0.0.6.
- Tiene asignada una distancia administrativa de 110.
- Su métrica es el costo (función del ancho de banda).
- Soporta autenticación MD5.
- Requiere que se defina un número de área y en cada área un DR y BDR.
- Mantiene y actualiza tres tablas: enrutamiento, adyacencias y topología.

La activación del enrutamiento con OSPF en un router Mikrotik es un proceso bastante sencillo:

- Paso 1: Crear una interface loopback.
- Paso 2: Habilitar una instancia OSPF.
- Paso 3: Añadir las redes que anunciará el router.

Un cortafuegos (o *firewall* en inglés) es un elemento de hardware o software que se utiliza en una red de computadoras para controlar las comunicaciones, permitiéndoles o prohibiéndoles según las políticas de red que haya definido el administrador de la red.

RouterOS permite crear un Firewall Stateful lo que significa que realiza una inspección de estado de paquetes y realiza un seguimiento de estado de conexiones que pasan a través de él.

El filtrado puede ser por direcciones IP, rango de direcciones IP, por puerto, rango de puertos, protocolo IP, DSCP (Differentiated Services Code Point) y otros parámetros. Soporta también direccionamiento IP estático y dinámico, además de implementar características de capa 7 (Layer7).

En un firewall se necesita definir políticas o reglas de filtrado para restringir el tráfico de red; en RouterOS estas reglas son organizadas en cadenas. Hay tres cadenas predefinidas las cuales son:

1. Input: cadena usada para procesar paquetes que entran al router por alguna de sus interfaces cuya dirección IP destino es una de las que posee el router.
2. Forward: cadena usada para procesar paquetes que pasan a través del router.
3. Output: cadena usada para procesar paquetes originados desde el router y que salen a través de alguna de sus interfaces.

Estas reglas se procesan en el orden en que aparecen listadas desde arriba hasta abajo. Si un paquete coincide con los criterios de la regla, entonces la acción especificada se realiza y se deja de procesar las reglas restantes. Por defecto, si un paquete no ha coincidido con ninguna regla de la cadena, entonces se acepta.



## 2.5.2 CONFIGURACIONES

Las configuraciones necesarias para establecer la comunicación entre las tres agencias mostradas en la figura 41 se muestran a continuación.

- 1) Se crea una interfaz loopback en todos los router con el siguiente comando.

```
/interface bridge
add name=Loopback0
```

- 2) Asignamos direcciones IP a cada interfaz física y loopback de cada router.

Configuración en Mejicanos

```
/ip address
add address=10.10.10.1/32 interface=Loopback0
add address=172.16.0.5/30 interface=ether1
add address=172.16.0.2/30 interface=ether2
add address=172.16.1.1/24 interface=ether3
```

Configuración en Ayutuxtepeque

```
/ip address
add address=10.10.10.2/32 interface=Loopback0
add address=172.16.0.6/30 interface=ether1
add address=172.16.2.1/24 interface=ether2
add address=172.16.0.10/30 interface=ether3
```

Configuración en San Salvador

```
/ip address
add address=10.10.10.3/32 interface=Loopback0
add address=172.16.3.1/24 interface=ether1
add address=172.16.0.1/30 interface=ether2
add address=172.16.0.9/30 interface=ether3
```

- 3) Configuramos el enrutamiento OSPF habilitando una instancia OSPF, en este caso habilitamos la que viene por defecto (area backbone) y el router-id definido por la IP de loopback. Luego añadimos las redes que anunciará cada router.



### Configuración en Mejicanos

```
/routing ospf instance
set [ find default=yes ] router-id=10.10.10.1
/routing ospf network
add area=backbone network=172.16.1.0/24
add area=backbone network=172.16.0.0/30
add area=backbone network=172.16.0.4/30
add area=backbone network=10.10.10.1/32
```

### Configuración en Ayutuxtepeque

```
/routing ospf instance
set [ find default=yes ] router-id=10.10.10.2
/routing ospf network
add area=backbone network=172.16.2.0/24
add area=backbone network=172.16.0.4/30
add area=backbone network=172.16.0.8/30
add area=backbone network=10.10.10.2/32
```

### Configuración en San Salvador

```
/routing ospf instance
set [ find default=yes ] router-id=10.10.10.3
/routing ospf network
add area=backbone network=172.16.3.0/24
add area=backbone network=172.16.0.0/30
add area=backbone network=172.16.0.8/30
add area=backbone network=10.10.10.3/32
```

- 4) Finalmente para brindar acceso a internet desde el router SAN SALVADOR configuramos una dirección IP pública, una ruta por defecto (interfaz ether5), un NAT que enmascare nuestra red local (172.16.0.0/22) y distribuimos con OSPF esa ruta hacia internet a todas las redes locales. Para más información sobre NAT ver Sección 2.9.

```
/ip address
add address=168.243.8.2/29 comment=WAN interface=ether5
/ip route add distance=1 gateway=168.243.8.1
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether5 src-
address=172.16.0.0/22
/routing ospf instance
set [ find default=yes ] distribute-default=if-installed-as-type-1
```

Con esto ya tendremos conectividad en toda la red y podemos empezar a configurar el firewall. Para comprender mejor las configuraciones necesarias para establecer las políticas de acceso se utilizará la interfaz gráfica del sistema y la herramienta WinBox en lugar de la consola de comandos.

- 5) Primero accedemos con WinBox al router desde una red que tendrá permitido la administración del router posterior a la aplicación de las políticas de acceso y activamos la casilla `Secure Mode`, para asegurarnos de que si se pierde comunicación con el router por accidente o configuraciones incorrectas se desechen todos los cambios realizados, como se muestra en la figura 42.

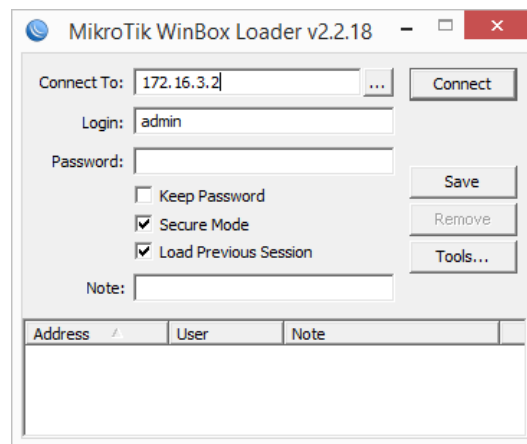


Figura 42. Acceso a la interfaz gráfica mediante WinBox.

- 6) Es conveniente definir listas de direcciones antes de definir las reglas cuando se tienen más de una red. Desde el menú `IP > Firewall` nos dirigimos a la pestaña `Address Lists` y damos clic en el botón añadir. Agregamos un nombre a la lista, definimos la red que pertenecerá a esa lista y presionamos OK como se muestra en la figura 43.

Seguimos añadiendo las redes individuales de cada VLAN hasta completar la lista, en la figura 44 se muestra el resultado final. En este caso hemos creado tres lista llamadas: `all_redes`, `redes_negadas` y `redes_permitidas`. También podemos añadir comentarios para identificar cada elemento de la lista.

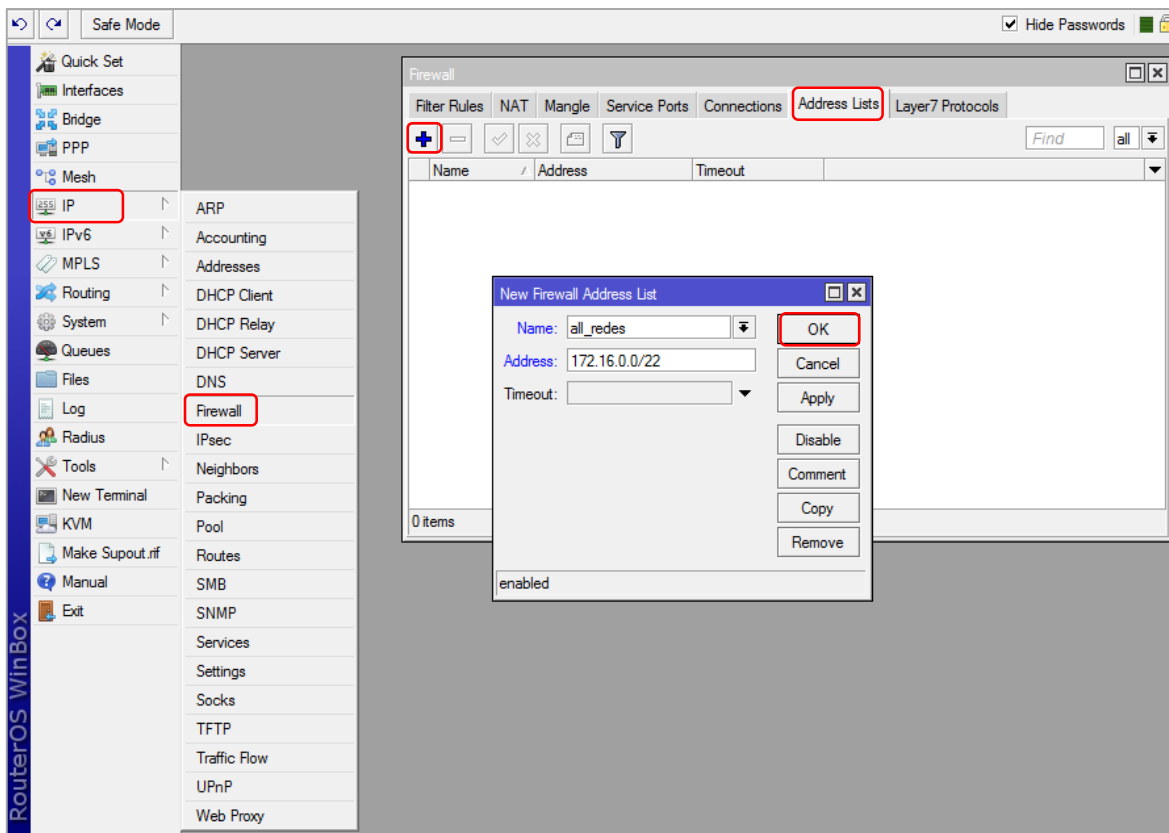


Figura 43. Creación de listas de direcciones.

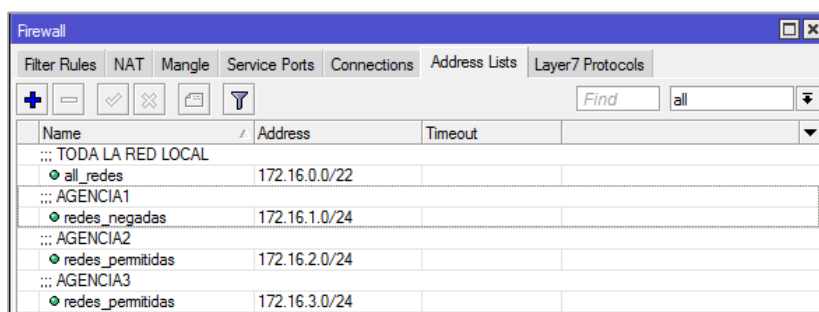


Figura 44. Lista de direcciones.

- 7) Regresamos a la pestaña *Filter Rules* y en el botón añadir nos aparecerá una ventana como la que se muestra en la figura 45. Procedemos a definir las reglas, empezamos aceptando cualquier conexión cuyo origen sea la lista de redes negadas y destino sea únicamente IP's que pertenecen a la red local. Esto se hace

especificando la cadena forward en la pestaña General, lista de direcciones origen y destino que previamente definimos en la pestaña Advanced y en la casilla Action de la pestaña Action seleccionamos accept (aceptar) y presionamos OK.

Luego definimos las reglas para filtrar el contenido de las url's de forma similar, pero en este caso en la pestaña Advanced tendremos como origen la lista de redes permitidas, como destino cualquier IP (0.0.0.0/0) y además añadimos en la casilla Content la palabra porn, facebook o youtube. Finalizamos con la pestaña Action seleccionando la opción Drop (rechazar) en la casilla Action.

Cuando terminemos de especificar todas las reglas, añadimos al final una regla que rechace cualquier otra acción que no haya sido especificada de lo contrario se aceptará por defecto. Todas las reglas creadas para la cadena forward se muestran en la figura 46 y en el modo detallado se observan todos los parámetros que se han configurado.

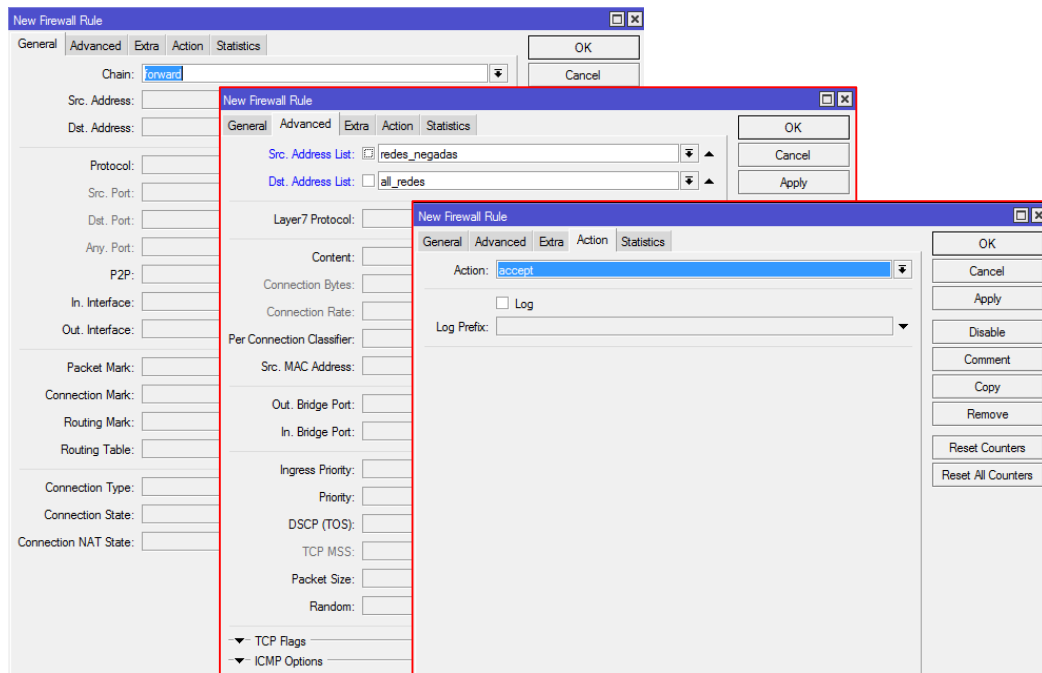


Figura 45. Configuración de políticas.

- 8) Luego agregamos las reglas para la cadena `input` para establecer los host que tendrán permisos para administrar el router como se muestra en la figura 47. Aquí se

han definido reglas de estado de conexión, para ahorrar procesamiento y acelerar las conexiones ya establecidas y relativas (también se pudo haber realizado con la cadena forward anterior).

Definimos la red de administración con mascara /29 para indicar que solo los primeros 6 host válidos de esa red tienen permitido el acceso al router y además se especifica que se podrá acceder desde cualquier interface de red a excepción de la interfaz ether5 (!ether5) ya que ésta se conecta a internet. Para más ejemplos de aplicación sobre OSPF y Firewall.

#	Rule Name	Action	Chain	Log	Bytes	Packets	Rate
0	Permitimos acceso a toda la red local	accept	forward	no	0 B	0	0 bps
1	Rechazamos url que contenga pom	drop	forward	no	0 B	0	0 bps
2	Rechazamos url que contenga facebook	drop	forward	no	0 B	0	0 bps
3	Rechazamos url que contenga youtube	drop	forward	no	0 B	0	0 bps
4	Permitimos todo a las redes permitidas	accept	forward	no	0 B	0	0 bps
5	Rechazamos todo lo demas	drop	forward	no	532 B	13	0 bps

Figura 46. Reglas creadas para la cadena forward.

#	Rule Name	Action	Chain	Log	Bytes	Packets	Rate
6	Permitimos conexiones establecidas	accept	input	no	1712.3 KiB	3	1374 bps
7	Permitimos conexiones relacionadas	accept	input	no	6.2 KiB	0	0 bps
8	Rechazamos conexiones invalidas	drop	input	no	0 B	0	0 bps
9	Permitimos conexiones a 6 host de GERENCIA3	accept	input	no	560 B	4	0 bps
10	Rechazamos todo lo demas	drop	input	no	101.2 KiB	741	0 bps

Figura 47. Reglas creadas para la cadena input.

## 2.6 ENRUTAMIENTO DE SISTEMAS AUTÓNOMOS BGP

Border Gateway Protocol; Protocolo de enrutamiento usado para intercambiar información de enrutamiento entre diferentes redes, pero puede ser usado internamente (iBGP) y externamente (eBGP).

iBGP se usa para transportar:

- Algunos/todos los prefijos de Internet a través del backbone del proveedor (ISP).
- Todos los prefijos pertenecientes a los clientes del ISP.

eBGP se usa para:

- Intercambiar prefijos con otros AS.
- Implementar políticas (reglas) de enrutamiento.

El Sistema Autónomo (AS) es la clave esencial de BGP, identifica de forma única un grupo de redes bajo una administración de enrutamiento común [49]

BGP

- Protocolo de Vector de Trayectoria
- Actualizaciones Incrementales
- Muchas opciones para forzar medidas administrativas (de rutas)
- Soporta Enrutamiento Inter-Dominio Sin Clases
- Muy utilizado en la “espina dorsal” de Internet
- Sistemas Autónomos

### 2.6.1 EJEMPLO PRÁCTICO

BGP o Border Gateway Protocol es un protocolo mediante el cual se intercambia información de encaminamiento entre sistemas autónomos. Por ejemplo, los ISP registrados en Internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP.

En la figura 48 se muestra un diagrama de red bajo el cual se explicará de forma sencilla el concepto de BGP.

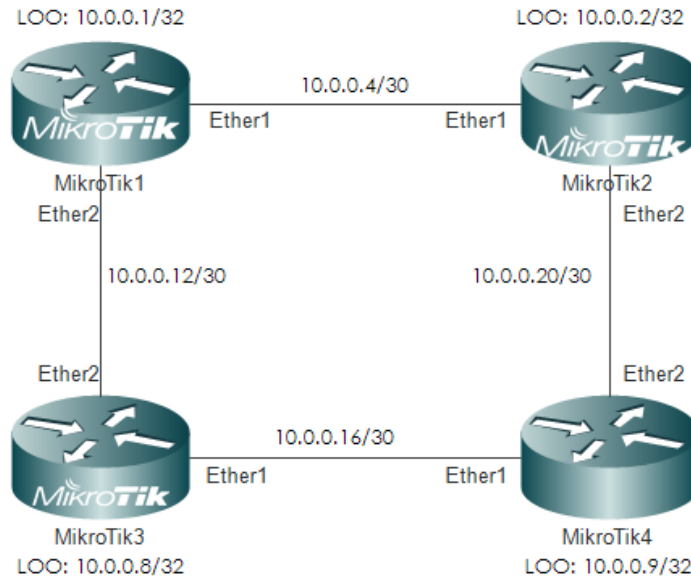


Figura 48. Sistema autónomo único para implementar iBGP.

## 2.6.2 CONFIGURACIONES

Para este ejemplo se implementará BGP sobre la red mostrada en la figura 48, el cual consta de un solo sistema autónomo (iBGP), lo que resulta en un IGP (Protocolo de enlace interior). Dicha configuración requiere de un método de enrutamiento ya sea estático o dinámico, en esta ocasión se usó OSPF.

BGP requiere establecer una sesión con sus vecinos a los cuales se les llama pares, dichos pares necesitan identificarse a través de una IP, esta dirección es altamente recomendado que pertenezca a una interfaz virtual, ya que, supera en estabilidad a una física, además presenta mayor solidez ante posibles ataques.

A continuación se describe la configuración de uno de los routers de la figura 48 primero se creó una interfaz loop para la identificación de los pares `/interface bridge`, posteriormente se procedió a establecer las direcciones IP de cada interfaz involucrada.

Como se mencionó anteriormente para la configuración es esencial un método de ruteo, para lo cual levantó una instancia OSPF `/routing ospf instance` configurado para que distribuya rutas por defecto `distribute-default=if-installed-as-type-1`, así como las rutas estáticas `redistribute-connected=as-type-1`, identificado con su interfaz virtual `router-id=10.0.0.1`. Para completar esta configuración se especifican

las redes conectadas `/routing ospf network add area=backbone network={IP/MASK}`.

Siguiendo el proceso de configuración se activó BGP, con la instrucción siguiente hasta el subdirectorio: `/routing bgp instance`, donde se establece que activa la instancia `default`, se define el sistema autónomo `as=65500` el cual educativos puede ser cualquier número, así como permitir que redistribuya redes conectadas `redistribute-connected=yes`, y por último la identidad de nuestro router `router-id=10.0.0.1`.

Para finalizar se establecen los pares entre los que tendrá lugar la sesión BGP, `/routing bgp peer`, donde se agrega su semejante con nombre "peer1" `add name=peer1`, la identidad `remote-address=10.0.0.2`, el sistema autónomo remoto `remote-as=65500`, así también la fuente de actualizaciones `update-source=loopback`.

- 1) Creación de interfaces virtuales y direccionamiento de éstas, así como las interfaces físicas.

Mickotik1:

```
/interface bridge add name=loopback

/ip address
add address=10.0.0.1/32 interface=loopback
add address=10.0.0.5/30 interface=ether1
add address=10.0.0.14/30 interface=ether2
```

- 2) Levantamiento de un protocolo IGP, OSPF para este ejemplo.

Mickotik1:

```
/routing ospf instance
set [ find default=yes ] distribute-default=if-installed-as-type-1 redistribute-connected=as-type-1 router-id=10.0.0.1

/routing ospf network
add area=backbone network=10.0.0.0/24
```

- 3) A continuación establecemos una instancia BGP.

```
/routing bgp instance
set default as=65500 redistribute-connected=yes router-id=10.0.0.1
```



4) Para finalizar se configuró los pares BGP.

```
/routing bgp peer
add name=peer1 remote-address=10.0.0.2 remote-as=65500 update-
source=loopback
add name=peer2 remote-address=10.0.0.8 remote-as=65500 update-
source=loopback
add name=peer3 remote-address=10.0.0.9 remote-as=65500 update-
source=loopback
```

## 2.7 SERVICIOS DE VPN

Los servicios de VPN se pueden implementar de varias maneras, una forma es usando túneles IPIP [50] o túneles GRE [51], se presenta un ejemplo práctico usando ambos. Un túnel IPIP es un protocolo simple que encapsula los paquetes IP en capa tres para levantar un túnel entre dos routers. En RouterOS las interfaces IPIP aparecen enlistadas junto con las interfaces físicas del router. Muchas tecnologías incluyendo Cisco y MikroTik soportan este protocolo. IPIP permite múltiples esquemas de red que se puede implementar.

GRE es un protocolo para túneles originalmente desarrollado por Cisco, puede encapsular una amplia variedad de protocolos para la creación de un enlace punto a punto.

Al igual que IPIP, GRE originalmente fue desarrollado como túnel sin estado, lo que significa que si el extremo remoto se cae todo el tráfico que se dirige por el túnel se pierde. Para resolver este problema RouterOS ha añadido características de *keepalive* para los túneles GRE.

### 2.7.1 EJEMPLO PRÁCTICO

En la figura 49 se muestra un diagrama de red para una empresa con tres agencias, cuyo router central está en San Salvador, se han levantado dos túneles para establecer los servicios de datos, el túnel 0 es IPIP y el túnel 2 es GRE.

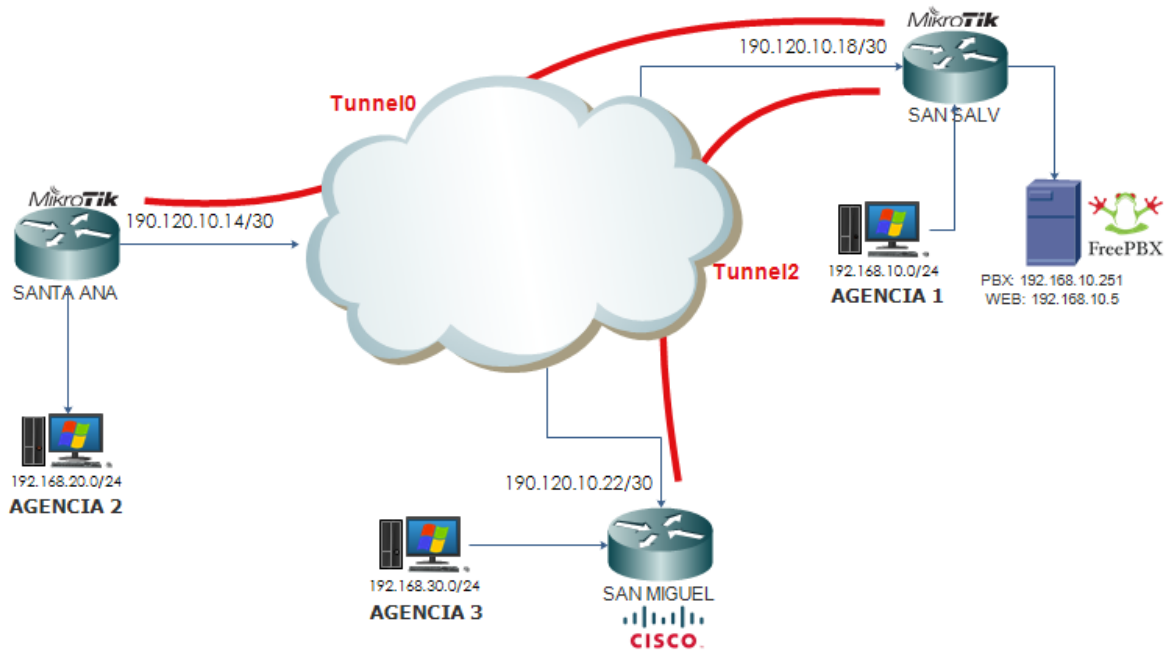


Figura 49. Muestra la implementación de túneles.

## 2.7.2 CONFIGURACIONES

Se detallan las configuraciones para establecer comunicación entre las tres agencias mostradas en la figura 49.

- 1) Se levanta el túnel IP-IP entre Santa Ana y San Salvador, primero se debe crear la interface y luego realizar las configuraciones de la siguiente manera.

### Configuración en Santa Ana

```
/interface ipip
add comment=tunel-hacia-salv local-address=190.120.10.14 \
name=Tunnel0 remote-address=190.120.10.18

/ip address
add address=10.10.10.2/30 interface=Tunnel0
```

### Configuración en San Salvador

```
/interface ipip
add comment=tunel-hacia-sta-ana local-address=190.120.10.18 \
name=Tunnel0 remote-address=190.120.10.14

/ip address
add address=10.10.10.1/30 interface=Tunnel0
```

- 2) Se levanta el túnel GRE entre San Miguel y San Salvador, el router de San Miguel es un Cisco del cual también se detalla como levantar el túnel, en San Salvador primero se debe crear la interface y luego realizar las configuraciones de la siguiente manera.

#### Configuración San Miguel

```
interface Tunnel2
description HACIA-SAN-SALVADOR
ip address 10.10.20.2 255.255.255.252
keepalive 10 5
tunnel source 190.120.10.22
tunnel destination 190.120.10.18
```

#### Configuración San Salvador

```
/interface gre
add comment=tunel-hacia-sn-migu local-address=190.120.10.18 \
name=Tunnel2 remote-address=190.120.10.22

/ip address
add address=10.10.20.1/30 interface=Tunnel2
```

## 2.8 MPLS Y MONITOREO POR SNMP

MPLS es un protocolo que funciona entre la capa de enlace de datos y la capa de red, en cierta forma se reemplaza el enrutamiento IP, la decisión de reenvío de paquetes (interface de salida y puerta de enlace) ya no se basa en los campos de la cabecera IP (normalmente IP de destino) ni en la tabla de enrutamiento. Las decisiones se toman en base a etiquetas, lo cual acelera el proceso de reenvío ya que no es necesario analizar la cabecera IP ni la tabla de rutas [52].

La creación de VPLS permite la simulación de un enorme switch, con lo cual se pueden crear servicios de datos que conecten sitios remotos, sin duda VPLS [53] es una solución muy eficiente para entregar servicios privados, ya que por correr en capa 2 sobre MPLS las velocidades y toma de decisiones para el reenvío son aproximadamente el doble que en una red IP basada en routing. Hay que tener en cuenta que para crear interfaces VPLS se debe tener un sistema MPLS funcionando.

El plugin weathermap para Cacti nos permite personalizar mapas de monitoreo, se crean vistas de la red en las que se pueden llegar control del consumo ancho de banda y rendimiento de los equipos, se puede presentar toda información consultada por SNMP.

### 2.8.1 EJEMPLO PRÁCTICO

En la figura 50 se muestra un sistema MPLS, en los extremos se tienen dos router que hacen la función de LER sobre los cuales se configuran las VPLS [53].

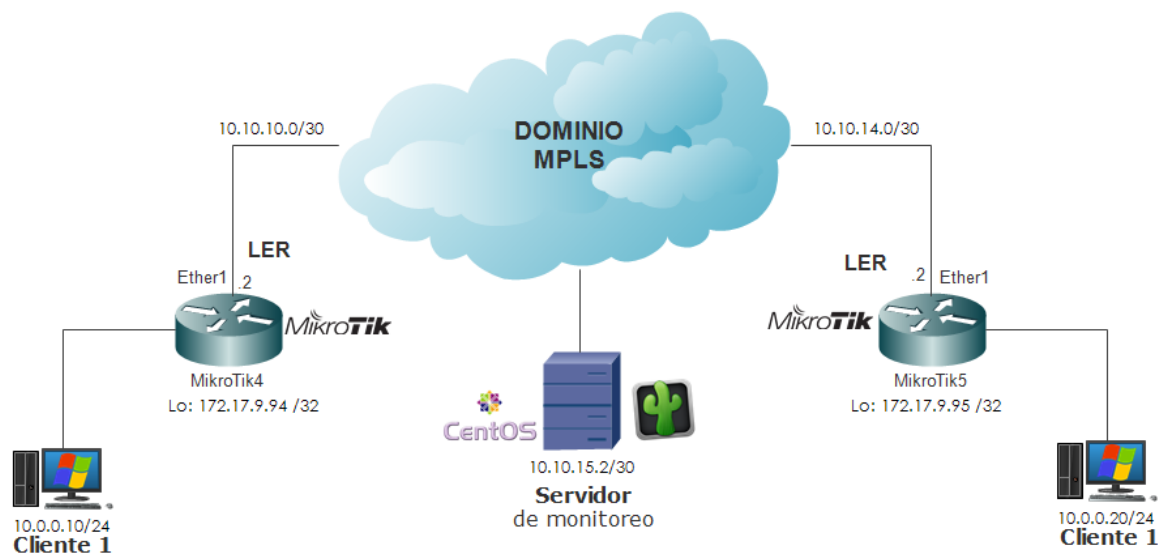


Figura 50. Ilustración para un Sistema MPLS.

### 2.8.3 CONFIGURACIONES

Se detalla el procedimiento para configurar el sistema MPLS de la figura 50, levantar las VPLS y crear la vista en Cacti usando weathermap.

- 1) Se crean las interfaces loopback por medio de un bridge, está misma configuración se aplica en ambos equipos.

```
/interface bridge
add name=loopback
```

- 2) Se realizan las configuraciones IP en las interfaces de los equipos, solo se muestra para el MikroTik 4, se repite lo mismo con diferente IP para el otro extremo.

```
/ip address
add address=10.10.10.2/30 interface=ether1
add address=172.17.9.94/32 comment="LOOPBACK R4" \
interface=loopback
```

- 3) Se configura OSPF para redistribuir dinámicamente las rutas y conocer todos los vecinos dentro de la nube del sistema MPLS.

```
/routing ospf instance
set [ find default=yes ] router-id=172.17.9.94

/routing ospf interface
add interface=ether1

/routing ospf network
add area=backbone network=172.17.9.94/32
add area=backbone network=10.10.10.0/30
```

- 4) Ahora configuramos el sistema MPLS. Para la distribución de etiquetas se activa LDP. Se deben agregar todas las interfaces que participan en MPLS.

```
/mpls interface
set [ find default=yes ] mpls-mtu=1526

/mpls ldp
set enabled=yes lsr-id=172.17.9.94 transport-address=172.17.9.94

/mpls ldp interface
add interface=ether1
```

- 5) Ahora que ya se tiene configurado el sistema MPLS procedemos a crear los servicios de los clientes por medio de las VPLS, se crea un servicio llamado cliente1 el cual está entre el LER MikroTik-4 y el LER MikroTik-5. La misma configuración se realiza en ambos equipos solo cambia el parámetro remote-peer que siempre es la IP de loopback del extremo.

```
/interface vpls
add advertised-l2mtu=1526 cisco-style=yes cisco-style-id=5 \
disabled=no l2mtu=1526 name=vpls1 remote-peer=172.17.9.95

/ interface bridge add name=cliente1
/interface bridge port
add bridge=cliente1 interface=ether2
add bridge=cliente1 interface=vpls1
```

- 6) Se estableció una comunidad SNMP a los equipos para que éstos puedan ser monitoreados.

```
/snmp community
set [ find default=yes ] name=7992@eie.mikroTik

/snmp
set enabled=yes trap-community=7992@eie.mikroTik
```

- 7) Se crear el mapa que llevará el control de tráfico del sistema MPLS, figura 51.



Figura 51. Muestra la opción para direccionar a weathermap desde Cacti

Para abrir el editor de mapas se da clic en la opción Editor, al final de la ventana, como

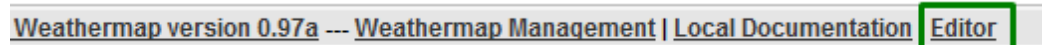


Figura 52. Muestra la opción para abrir el editor de mapas.

Nos apertura una ventana en la que agregamos el nombre del mapa.

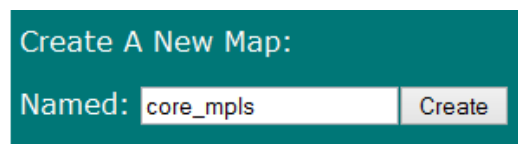


Figura 53. Muestra la opción para agregar un mapa

Al dar clic en Create nos direcciona al editor, también se puede dar clic sobre el enlace para empezar a construir nuestro esquema. La figura 54 muestra los mapas creados.

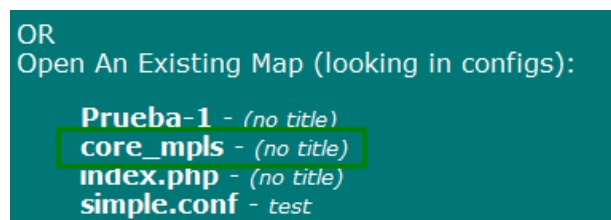


Figura 54. Muestra los mapas creados en el editor

Una vez en el editor agregamos un nodo y le cambiamos nombre, ver la figura 55.

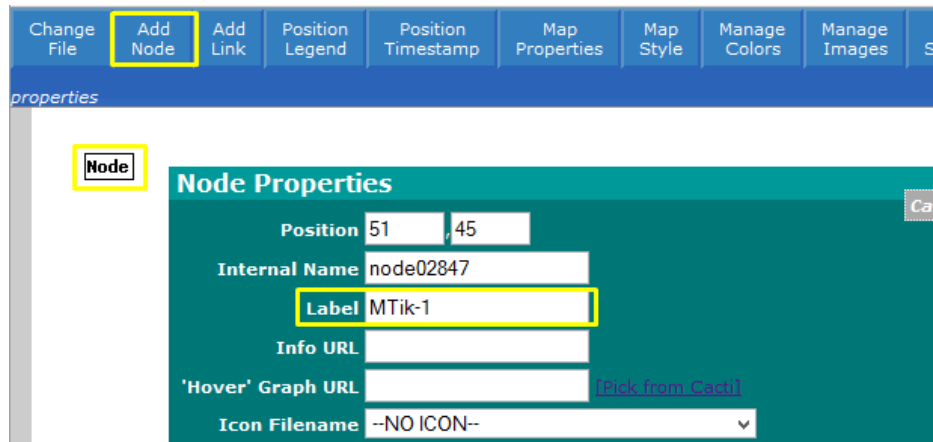


Figura 55. Muestra la opción para agregar un nodo

Creamos un fondo para nuestro mapa y una imagen para nuestros equipos, las cuales se transfieren por FTP a la dirección en el servidor /var/www/html/plugins/weathermap/images/ aquí se encuentran todas las imágenes que podemos usar para personalizar nuestros diagramas. Para cambiar la imagen del nodo desplegamos las opciones del Icon Filename como se muestra en la figura 56 y seleccionamos que la que pasamos vía FTP.

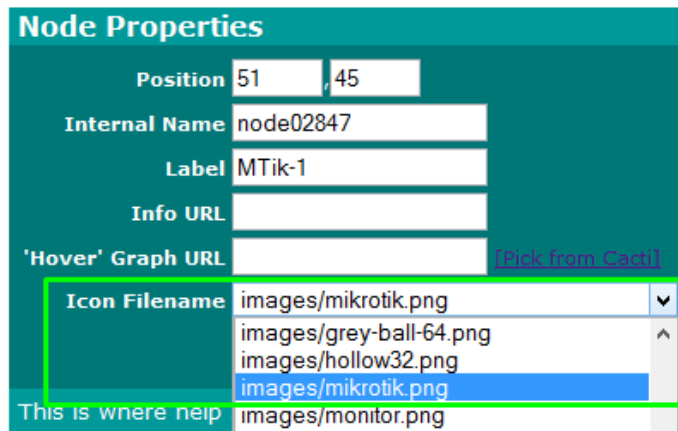


Figura 56. Muestra la opción para cambiar la imagen del nodo

Para cambiar el fondo del mapa editamos las propiedades y luego cambiamos la opción Background Image Filename por el fondo que transferimos al servidor, como se muestra en la figura 57

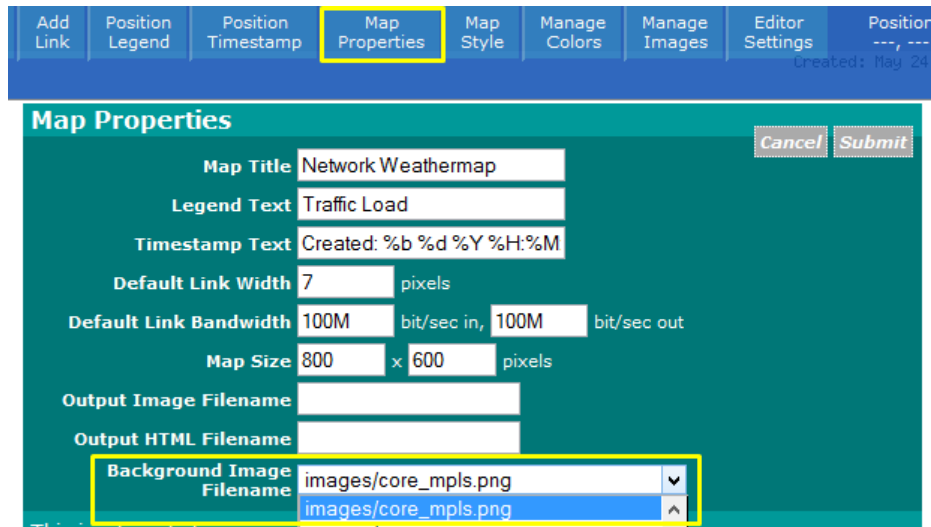


Figura 57. Muestra la opción para cambiar el fondo del mapa

Asignamos los enlaces entre los equipos core, con la opción Add Link que nos permite conectar los nodos, como se detalla en la figura 58

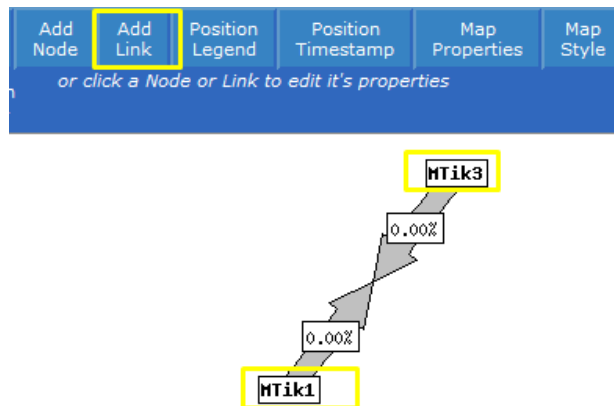


Figura 58. Muestra la opción para agregar enlaces entre nodos

Asignamos a los enlaces entre nodos las gráficas de Cacti, damos clic sobre el enlace y modificamos la opción pick from Cacti, como se muestra en la figura 59.

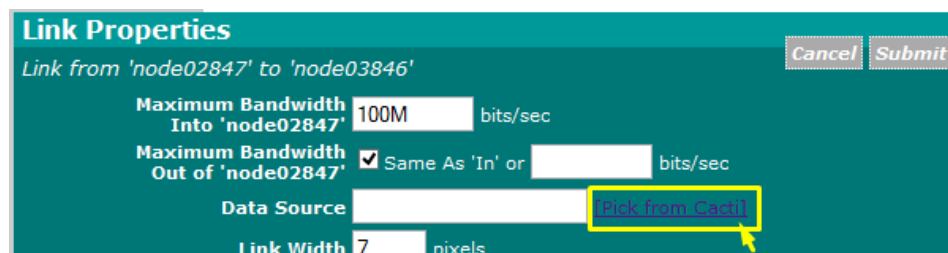


Figura 59. Muestra la asignación de una gráfica al enlace entre nodos



En la ventana emergente se seleccionamos la interfaz que corresponde a la gráfica del enlace que agregaremos. Como se detalla en la figura 60.

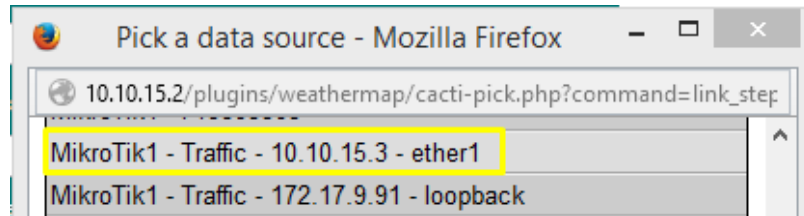


Figura 60. Ventana emergente que muestra la lista de gráficas existente

Una vez agregados todos los nodos y todos los enlaces se obtiene un mapa como el de la figura 61.

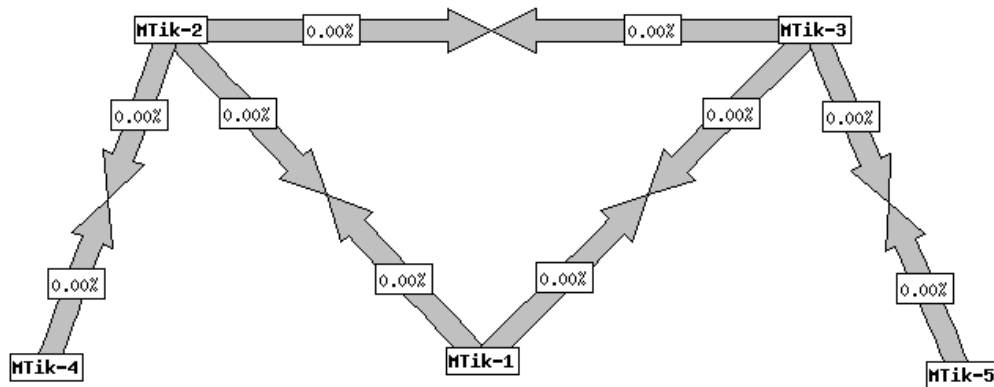


Figura 61. Detalle de los nodos con los respectivos enlaces.

Al tener listo el mapa nos salimos del editor y nos ubicamos en Weather Management para agregar la vista en el cacti, como se muestra en la figura 62.

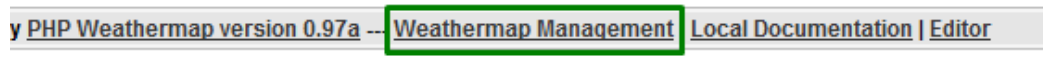


Figura 62. Opción para ir al menú de mapas de Cacti

Agregamos una nueva vista para el mapa que personalizamos en el editor, como detalla la figura 63.

Weathermaps							Add
Config File	Title	Group	Active	Settings	Sort Order	Accessible By	
ALL MAPS	(special settings for all maps)			standard			

Figura 63. Menú de mapas agregas a Cacti

Agregamos la vista dando clic en add como se observa en la figura 64.

Available Weathermap Configuration Files		
		Config File
Add	View	.htaccess
Add	View	Prueba-2
Add	View	core_mpls
Add	View	simple.conf

Figura 64. Opción para agregar a Cacti los mapas creados en el editor

Ya tenemos creado nuestro mapa bajo el cual se tiene monitoreo del sistema MPLS. Para visualizarlo nos vamos a la pestaña Weathermap y aquí nos aparecen todos los mapas que se tengan agregados, como se ilustra en la figura 65.

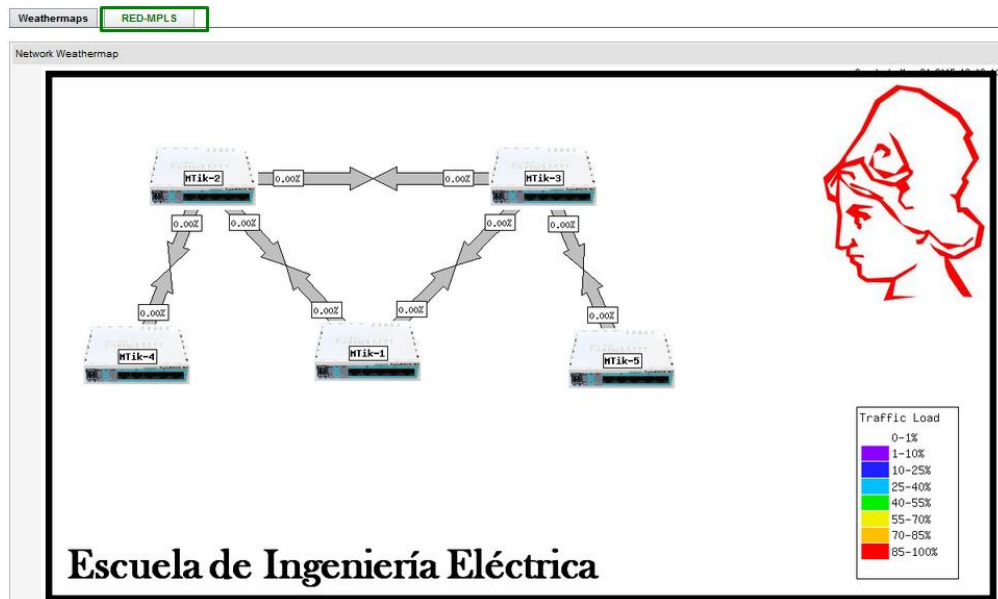


Figura 65. Mapa final con vista desde Cacti

- 8) Si quisiéramos que las redes de los clientes unidas en la VPLS que se muestra en la figura 50 tengan salida a internet es necesario proporcionarles una puerta de enlace ya que el sistema está funcionando como si estuvieran en un switch en capa 2. En la figura 66 se presenta un diagrama en el que se ilustran los cambios a realizar para que la red 10.0.0.0/24 tenga salida a internet, en las configuraciones en el MikroTik debemos hacer un NAT y enviar todo el tráfico por defecto al Gateway de la WAN.

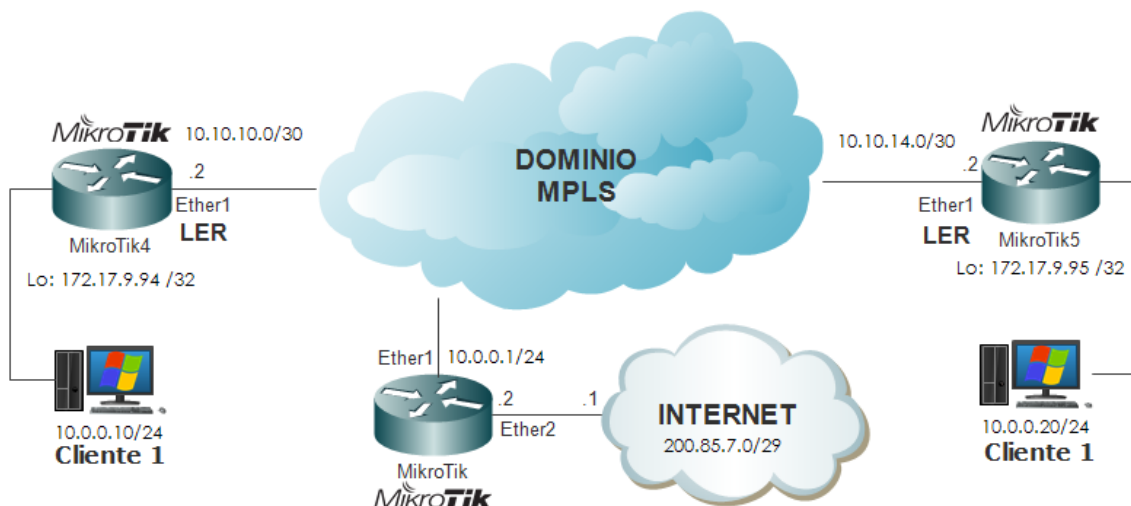


Figura 66. Representación para que la red 10.0.0.0/24 tenga salida a internet

Dentro del sistema MPLS agregamos entre uno de los LSR y el MikroTik4 una VPLS2 la cual asociamos al cliente1, de este equipo depende el router que sirve de puerta de enlace para la salida a internet.

Configuraciones en MikroTik4

```
/interface vpls
add advertised-l2mtu=1526 cisco-style=yes cisco-style-id=5
disabled=no l2mtu=1526 name=vpls2 remote-peer=172.17.9.91

/interface bridge port
add bridge=cliente1 interface=vpls2
```

Configuraciones en el LSR

```
/interface vpls
add advertised-l2mtu=1526 cisco-style=yes cisco-style-id=5
disabled=no l2mtu=1526 name=vpls2 remote-peer=172.17.9.94

/interface bridge add name=cliente1
/interface bridge port
add bridge=cliente1 interface=ether5
add bridge=cliente1 interface=vpls2
```

Se realiza el NAT en el MikroTik que conectaremos a la nube MPLS y se envía todo por defecto a la puerta de enlace en la WAN.

```
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether2 src-
address=10.0.0.0/24 to-addresses=200.85.7.2

/ip route add distance=1 gateway=200.85.7.1
```

## 2.9 NAT Y PORT FORWARDING

NAT es un mecanismo de traducción IP utilizado por routers para intercambiar paquetes entre dos redes (interna y externa) que tienen rangos de direcciones diferentes y por tanto incompatibles. Una LAN que utiliza NAT se conoce como red NATted. Sin duda alguna NAT fue el camino para el escaseamiento de direcciones IPv4, ya que con una sola IP pública se puede dar servicio de internet a una red local.

Port Forwarding es un método que también nos hace una traducción (parecido a NAT) pero la funcionalidad es a la inversa, por ejemplo en el caso que en una red interna se tengan diez cámaras IP, las cuales necesitamos consultar desde cualquier parte del mundo, lo que se pensaría inicialmente es colocarle una IP pública a cada cámara y se resuelve el problema, sin embargo si consideramos el costo de tener una IP pública ya no es tan viable realizar esa configuración, y es ahí donde una configuración Port Forwarding puede ser útil ya que permite hacer traducciones de una IP pública a una IP privada pero con diferente puerto, solo bastaría con establecerle diferente puerto a las cámaras y con una sola IP podríamos controlar las diez.

### 2.9.1 EJEMPLO PRÁCTICO

En la figura 67 se muestra un diagrama de red que ilustra la traducción por medio de NAT [55] y el uso de Port Forwarding [56] para consultar una cámara IP por medio de la IP pública configurada en el router.

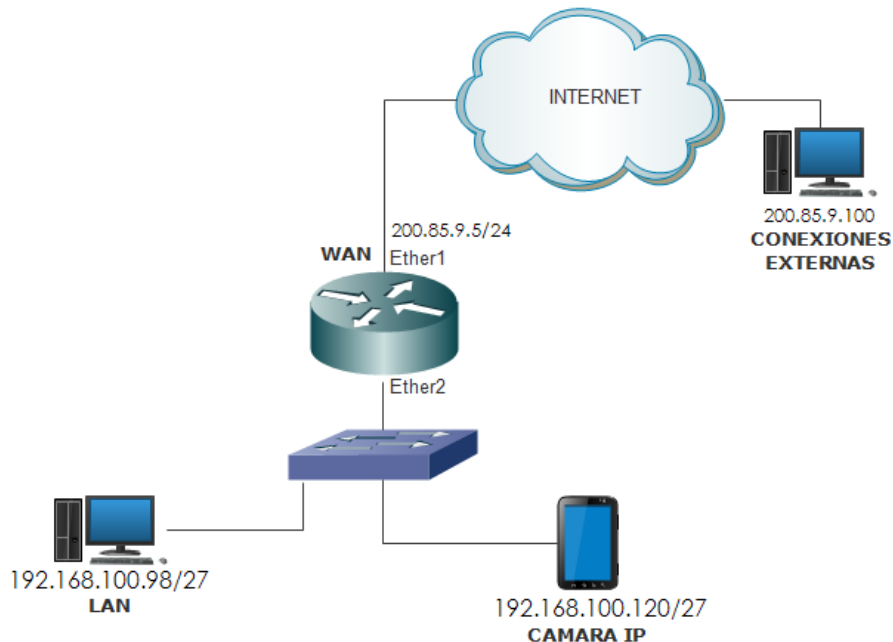


Figura 67. Muestra la implementación NAT y Port Forwarding

## 2.9.2 CONFIGURACIONES

Se detallan las configuraciones para realizar NAT y Port Forwarding para el diagrama presentado en la figura 67.

- 1) Se ingresa en las opciones de ip firewall, ahí se puede encontrar la opción para realizar NAT, se agrega una acción que todo lo que tenga fuente 192.168.100.0/24 lo traduzca a la interface de salida ether1.

```
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1
src-address=192.168.100.0/24
```

- 2) Para realizar el Port Forwarding, siempre en las opciones del ip firewall agregamos una acción que toda consulta que se haga en la interface WAN por el puerto 8080 sea traducido a la IP 192.168.100.120 por el puerto 8080, con esta configuración la cámara IP mostrada en la figura 2.9.1 podrá ser consultada por medio de la IP pública configurada en la WAN.

```
/ip firewall nat
add action=dst-nat chain=dstnat dst-address=200.85.9.5 dst-
port=8080 port=8080 protocol=tcp to-addresses=192.168.100.120
```

## CONCLUSIONES

1. Los router's RB750 utilizados en este trabajo son capaces de implementar los protocolos de enrutamiento RIP, OSPF, BGP, MPLS y servicios LAN como servidor DHCP, DNS, Firewall, aplicación de *Port Forwarding* y servicios de VoIP sin ningún inconveniente; la única limitante debido a su capacidad de procesamiento ya que no soporta más de dieciséis usuarios conectados, sin embargo esto no fue obstáculo para el desarrollo del trabajo de graduación, ya que a lo sumo se llegaron a usar tres usuarios conectados simultáneamente.
2. Se instaló y configuró el sistema operativo RouterOS trial versión 6.28 en el entorno virtual GNS3 en el cual se simularon las prácticas de laboratorio relacionadas con los protocolos RIP, OSPF, BGP, MPLS y los servicios DHCP, DNS, Firewall, Port Forwarding, se concluye que para capacitarse en la tecnología MikroTik no es necesario comprar el equipo físico, ya que el uso de herramientas de software libre como GNS3, QEMU, la versión de prueba de RouterOS y la amplia comunidad de usuarios en línea, permite que cualquier persona pueda obtener el conocimiento de forma autodidacta, gratuita, sin tener físicamente un equipo y sin violar licencias o derechos de autor.
3. Se realizaron nueve guías de laboratorio en las que se implementaron usando el RB750 los protocolos de enrutamiento RIP, OSPF, BGP MPLS y servicios DHCP, DNS, Firewall, y Port Forwarding; para complementar las practicas se hizo uso de herramientas a base software libre como Cacti, FreePBX, Apache y PHP.

GUÍA 1: SIMULACIÓN DE ROUTEROS EN GNS3 V1.3.3

GUÍA 2: ENRUTAMIENTO ESTÁTICO

GUÍA 3: ENRUTAMIENTO DINÁMICO RIP V2

GUÍA 4: CONFIGURACIÓN DE VLAN Y SERVIDORES DHCP

GUÍA 5: ENRUTAMIENTO OSPF Y CONFIGURACIÓN DE FIREWALL

GUÍA 6: ENRUTAMIENTO ENTRE SISTEMAS AUTONOMOS CON BGP

GUÍA 7: CREACIÓN DE SERVICIOS DE VPN POR MEDIO DE TÚNELES

GUÍA 8: MPLS, CREACIÓN DE VPLS Y SISTEMA DE MONITOREO

GUÍA 9: IMPLEMENTACIÓN DE PORT FORWARDING

4. Se Instaló y configuró la distribución de Linux CactiEZ en la cual se habilitaron los plugins *Weathermap* y *realtime* los cuales permitieron personalizar la topología de red usada para la implementación de MPLS y monitorear el consumo de recursos mediante SNMP de forma gráfica y detallada.
5. Se implementaron los servicios básicos de una red LAN tales como servidor DHCP, DNS, Firewall y Port Forwarding, detallando en cada caso la forma configuración, se obtuvieron resultados satisfactorios en cada aplicación, por lo que un MikroTik puede funcionar como CPE (*Customer-Provided Equipment*) sin ninguna limitante respecto a servicios LAN y sustituir a otras tecnologías de mayor costo.
6. Se configuraron y administraron redes virtuales VLAN en un router MikroTik, haciendo uso de interfaces virtuales, puertos en modo acceso y troncal con el protocolo IEEE 802.1Q. Esto permitió optimizar y escalar las redes locales utilizando un Switch modelo Catalyst 2950 de la marca Cisco sin ningún problema de compatibilidad.
7. Se adquirieron los fundamentos de seguridad y se establecieron las políticas de acceso mediante el firewall que incorpora RouterOS el cual es muy versátil porque cuenta con una interfaz gráfica y permite filtrar paquetes por medio de IP's, puertos de origen y destino, tipo de tráfico, interfaces, protocolos y tipo de contenido (capa siete). Esto nos ayuda a tener un control de los paquetes que entran y salen de nuestra red y a evitar accesos no autorizados pero se debe tener en cuenta que la cantidad de reglas, tráfico y usuarios que se filtren requerirá más capacidades de procesamiento para el router.

8. Se configuraron redes privadas virtuales con los protocolos de túnel VPN tales como IPIP y GRE entre router MikroTik y router Cisco sin ningún problema de compatibilidad. Esto nos permitió implementar servicios VoIP mediante el protocolo SIP entre dos sitios remotos con diferentes tecnologías manteniendo la privacidad e integridad de los datos de los usuarios ya que para el resto de la red esta comunicación es transparente.
  
9. Se implementó el protocolo MPLS en una red core formada por cinco router MikroTik y mediante la configuración de VPLS se mejoró el rendimiento de la red ya que al utilizar etiquetas y trabajar en capa 2 la comunicación y la administración de la red es más eficiente y es posible implementa calidad de servicio. Esto permite a los proveedores IP ofrecer nuevos servicios que no son posibles con las técnicas actuales de enrutamiento IP (típicamente limitadas a enrutar por dirección de destino).
  
10. Los *routers* de la empresa MikroTik son una excelente alternativa para el diseño de redes ya que permiten reducir los costos de implementación, soportan los protocolos de enrutamiento estándares, cuenta con amplia documentación, certificaciones oficiales y equipos de diferentes gamas para cada aplicación.



## RECOMENDACIONES

1. El modelo RB750 es un router de gama baja y solo cuenta con las características mínimas, su uso es recomendable solo para pequeñas redes menores a 16 usuarios, sin embargo esta cantidad no es absoluta y varía en función del ancho de banda disponible y la cantidad de servicios configurados en el router por eso es importante mantener un monitoreo continuo con aplicaciones como Cacti.
2. Al momento de emular RouterOS en GNS3 es de considerar los recursos que se consumirán en nuestra computadora tanto en memoria RAM como en procesamiento, es recomendable revisar antes el consumo del sistema operativo bajo el cual se esté trabajando y luego hacer la relación en base a la memoria libre dividirla entre la memoria asignada a cada router y así tener un punto de referencia de cuantos equipos podemos montar.
3. En las guías de laboratorio se trató de cubrir la mayoría de temas respecto al estudio de redes de computadoras, sin embargo hay una serie de temas como QoS, Route Mark, IpSec, interfaces EoIP, entre otros que no se han cubierto por lo que queda abierto el tema a futuras investigaciones.
4. La instalación y configuración de Cacti con todos sus *plugins* es compleja cuando se realiza desde los repositorios de cualquier distribución GNU/Linux por lo que se recomienda la distribución CactiEz en la cual se instalan todos los complementos y solo es necesario activarlos.
5. RouterOS provee de un software gráfico llamado winbox, se recomienda usarlo siempre que sea posible ya que facilita la forma de configuración de las aplicaciones LAN como servicios DHCP, DNS, Firewall, Port Forwarding y los protocolos RIP, OSPF, BGP, MPLS, etc.

6. Aunque la cantidad de interfaces VLAN que se pueden crear en RouterOS con el nivel de licencia 4 en adelante es “ilimitada” como el caso del router RB750 (en realidad el protocolo IEEE 802,1Q solo permite hasta 4095 VLAN-ID), debe tenerse en cuenta que el tráfico y la cantidad de usuarios conectados agotan la cantidad de recursos del router y es posible que se necesite uno con mejores capacidades de procesamiento y además un Switch programable para aumentar la cantidad de puertos disponibles.
7. El firewall es uno de los servicios que puede consumir más CPU en un router ya que debe analizar diferentes capas de los paquetes IP, por eso es recomendable optimizar y reducir la cantidad de reglas tanto como sea posible; para redes con una gran cantidad de tráfico o usuarios se debe utilizar un hardware dedicado como dispositivo firewall.
8. Para poder establecer comunicación entre túneles IPIP es necesario especificar explícitamente el tipo de túnel tanto en los router MikroTik como en Cisco, ya que en el caso de los router Cisco si no se especifica, por defecto asume que se trata de un túnel GRE. El uso de este tipo de túneles se recomienda solo para comunicaciones punto a punto, si se desea comunicar diversos puntos se deben utilizar rutas estáticas hacia cada VPN o utilizar protocolos de VPN que permiten comunicación multipuntos.

## BIBLIOGRAFÍA

- [1] Wikipedia, «Modelo OSI,» [En línea]. Available: [http://es.wikipedia.org/wiki/Modelo\\_OSI](http://es.wikipedia.org/wiki/Modelo_OSI).
- [2] O. Gerometta, Guía de Preparación para el Examen de Certificación CCNA, Buenos Aires: Libronauta, 2006.
- [3] «Definicion de OSI,» [En línea]. Available: <http://www.alegsa.com.ar/Dic/osi.php>.
- [4] «Hardware y Software,» [En línea]. Available: <http://hectorhardwareyssoftware.blogspot.com/>.
- [5] «Medios de transmisión,» [En línea]. Available: <http://carlosenred.galeon.com/medios.html>.
- [6] «Ventajas de las redes inalámbricas y con cableado par tranzado,» [En línea]. Available: <http://seguridadenlainformacion7.bligoo.com.mx/ventajas-de-las-redes-inalambricas-y-con-cableado-par-tranzado#.VSxSgfB3UIM>.
- [7] R. USERS, «Redes Wi-fi en entornos Windows,» *RedUsers*, p. Argentina, 2012.
- [8] MikroTik, «MikroTik,» [En línea]. Available: <http://es.wikipedia.org/wiki/MikroTik>.
- [9] M. customers, MikroTik's customers, [En línea]. Available: <http://www.mikrotik.com/ourcustomers.php>.
- [10] W. S. S. Espinosa, Implementación de enlaces backhaul para backbone de un wisp mediante el uso del sistema operativo RouterOS, 2011.
- [11] «Manual: RouterOS features,» [En línea]. Available: [http://wiki.mikrotik.com/wiki/Manual:RouterOS\\_features](http://wiki.mikrotik.com/wiki/Manual:RouterOS_features).
- [12] «Manual: License,» [En línea]. Available: <http://wiki.mikrotik.com/wiki/Manual:License>.
- [13] «Manual: Product Naming,» [En línea]. Available: [http://wiki.mikrotik.com/wiki/Manual:Product\\_Naming](http://wiki.mikrotik.com/wiki/Manual:Product_Naming).
- [14] RouterBoard, «RouterBoard,» nº <http://routerboard.com/>.
- [15] E. M. Delgado, «SWITCHING VS. ROUTING,» [En línea]. Available: <http://neutron.ing.ucv.ve/revista-e/No4/articulo.htm>.
- [16] Oracle, «Cómo trabajar con redes VLAN,» Oracle, [En línea]. Available: [http://docs.oracle.com/cd/E37929\\_01/html/E36606/fpjve.html#scrolltoc](http://docs.oracle.com/cd/E37929_01/html/E36606/fpjve.html#scrolltoc).
- [17] R. Calero, «Laboratorio de Comunicaciones,» FIUBA, 2008. [En línea]. Available: [http://materias.fi.uba.ar/6679/apuntes/Switching\\_VLAN\\_Abr08.pdf](http://materias.fi.uba.ar/6679/apuntes/Switching_VLAN_Abr08.pdf).
- [18] Navega, «Redes MPLS,» Guatemala.
- [19] L. Networking, «La ruta por defecto,» [En línea]. Available: <http://librosnetworking.blogspot.com/2012/04/la-ruta-por-defecto.html>.
- [20] adrformacion, «Curso de Windows 2008 Server,» adrformacion, [En línea]. Available: <http://www.adrformacion.com/cursos/wserver082/leccion3/tutorial3.html>.
- [21] IETF, «RFC 2328 - OSPF Version 2: interoperate,» IETF, Abril 1998. [En línea]. Available: <https://www.ietf.org/rfc/rfc2328.txt>.
- [22] IETF, «RFC 1583 - OSPF V2: Implementación,» Marzo 1994. [En línea]. Available: <https://www.ietf.org/rfc/rfc1583.txt>.

- [23] IETF, «RFC 1163 - Border Gateway Protocol», IETF, Junio 1990. [En línea]. Available: <https://tools.ietf.org/html/rfc1163>.
- [24] Cisco, «BGP Case Studies», Cisco, 30 Octubre 2008. [En línea]. Available: <http://www.cisco.com/c/en/us/support/docs/ip/border-gateway-protocol-bgp/26634-bgp-toc.html>.
- [25] IETF, «RFC-2979 Behavior of and Requirements for Internet Firewalls», IETF, Octubre 2000. [En línea]. Available: <https://www.ietf.org/rfc/rfc2979.txt>.
- [26] Institute of Electrical and Electronics Engineers, «IEEE Standard Computer Dictionary», New York, 1990.
- [27] IETF, «RFC-2402 IP Authentication Header», IETF, Noviembre 1998. [En línea]. Available: <https://www.ietf.org/rfc/rfc2402.txt>.
- [28] IETF, «RFC-2406 IP Encapsulating Security Payload (ESP)», IETF, Noviembre 1998. [En línea]. Available: <https://tools.ietf.org/html/rfc2406>.
- [29] «Understanding how NAT works», what-when-how, [En línea]. Available: <http://what-when-how.com/tcpip/need-more-addresses-try-subnetting-and-nat-tcpip-part-2/>.
- [30] arayemla, «TECNOLOGIAS», [En línea]. Available: <http://arayemla.blogspot.com/>.
- [31] A. e. red, «Aplicaciones y servicios. Linux: Servidor DHCP», [En línea]. Available: [http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m2/servidor\\_dhcp.html](http://www.ite.educacion.es/formacion/materiales/85/cd/linux/m2/servidor_dhcp.html).
- [32] IETF, «RFC 3261», IETF, [En línea]. Available: <http://www.ietf.org/rfc/rfc3261.txt>.
- [33] IETF, «RFC1213», March 1991. [En línea]. Available: <https://www.ietf.org/rfc/rfc1213.txt>.
- [34] Jitendra Zaa, «Introduction to SNMP», [En línea]. Available: <http://www.jitendrazaa.com/blog/java/snmp/introduction-to-snmp/>.
- [35] CactiEZ, «CactiEZ - Documents», [En línea]. Available: <http://cactiez.cactiusers.org/docs/>.
- [36] N. Weathermap, «PHP Network Weathermap», [En línea]. Available: <http://network-weathermap.com/>.
- [37] «Simulador de red para mikrotik», [En línea]. Available: <http://www.ryohnosuke.com/foros/index.php?threads/15424/>.
- [38] MUM, «MikroTik User Meeting (MUM)», [En línea]. Available: <http://mum.mikrotik.com/presentations/ID13/rofiq.pdf>.
- [39] R. Fauzi, «MikroTik Network Simulator», 2013. [En línea]. Available: <http://mum.mikrotik.com/presentations/ID13/rofiq.pdf>.
- [40] A. Gordon, «Simulador de red para MikroTik», 2014. [En línea]. Available: <http://www.ryohnosuke.com/foros/index.php?threads/15424/>.
- [41] wiki.mikrotik, «Manual: Simple Static Routing», 2014. [En línea]. Available: [http://wiki.mikrotik.com/wiki/Manual:Simple\\_Static\\_Routing](http://wiki.mikrotik.com/wiki/Manual:Simple_Static_Routing).
- [42] V. Navarro, «Instrucciones», 2014. [En línea]. Available: <http://vnc-instrucciones.blogspot.com/2014/02/configuracion-basica-mikrotik.html>.
- [43] MikroTik, «RIP Routing Information Protocol», 2002. [En línea]. Available: [https://www.mikrotik.com/documentation/manual\\_2.5/Routing/RIP.html](https://www.mikrotik.com/documentation/manual_2.5/Routing/RIP.html).

- [44] wiki.mikrotik, «Manual:Routing/RIP,» 2010. [En línea]. Available: <http://wiki.mikrotik.com/wiki/Manual:Routing/RIP>.
- [45] L. D. Tommaso, «Configuración de VLAN con CISCO,» 2009. [En línea]. Available: <http://www.mikroways.net/2009/08/05/configuracion-de-vlans-con-cisco/>.
- [46] wiki.mikrotik, «Manual: IP/DHCP Server,» 2014. [En línea]. Available: [http://wiki.mikrotik.com/wiki/Manual:IP/DHCP\\_Server](http://wiki.mikrotik.com/wiki/Manual:IP/DHCP_Server).
- [47] MikroTik, «Manual Interface/VLAN» 2014,» 2014. [En línea]. Available: <http://wiki.mikrotik.com/wiki/Manual:Interface/VLAN>.
- [48] MikroTik, «Manual IP/Firewall/NAT,» 2015. [En línea]. Available: <http://wiki.mikrotik.com/wiki/Manual:IP/Firewall/NAT>.
- [49] E. Software, «Introducción a BGP,» 2011. [En línea]. Available: [https://nsrc.org/workshops/2011/walc/routing/raw-attachment/wiki/Agenda/Intro\\_BGP.pdf](https://nsrc.org/workshops/2011/walc/routing/raw-attachment/wiki/Agenda/Intro_BGP.pdf).
- [50] MikroTik, «Manual Interface IPIP,» [En línea]. Available: <http://wiki.mikrotik.com/wiki/Manual:Interface/IPIP>.
- [51] MikroTik, «Manual Interface GRE,» [En línea]. Available: <http://wiki.mikrotik.com/wiki/Manual:Interface/Gre>.
- [52] S. g. d. blog, «MPLS and VPLS on Mikrotik,» [En línea]. Available: <http://sysmagazine.com/posts/169103/>.
- [53] MikroTik, «Transparently Bridge two Networks using MPLS,» [En línea]. Available: [http://wiki.mikrotik.com/wiki/Transparently\\_Bridge\\_two\\_Networks\\_using\\_MPLS..](http://wiki.mikrotik.com/wiki/Transparently_Bridge_two_Networks_using_MPLS..)
- [54] M. M. 201, «MPLS/VPLS para ISP,» 05 Septiembre 2014. [En línea]. Available: <http://mum.mikrotik.com/presentations/MX14/alfredo.pdf>.
- [55] MikroTik, «Manual:IP/Firewall/NAT,» [En línea]. Available: <http://wiki.mikrotik.com/wiki/Manual:IP/Firewall/NAT>.
- [56] MikroTik, «Forwarding a port to an internal IP,» [En línea]. Available: [http://wiki.mikrotik.com/wiki/Forwarding\\_a\\_port\\_to\\_an\\_internal\\_IP](http://wiki.mikrotik.com/wiki/Forwarding_a_port_to_an_internal_IP).
- [57] Cisco, «Low Latency Queueing,» Cisco, [En línea]. Available: [http://www.cisco.com/c/en/us/td/docs/ios/12\\_0s/feature/guide/fslq26.html](http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/fslq26.html).
- [58] Cisco, «Configuring Weighted Fair Queueing,» Cisco, [En línea]. Available: [http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos\\_conmgt/configuration/15-mt/qos-conmgt-15-mt-book/qos-conmgt-cfg-wfq.html](http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/qos_conmgt/configuration/15-mt/qos-conmgt-15-mt-book/qos-conmgt-cfg-wfq.html).
- [59] Cisco, «Class-Based Weighted Fair Queueing,» Cisco, [En línea]. Available: [http://www.cisco.com/en/US/docs/ios/12\\_0t/12\\_0t5/feature/guide/cbwfq.html](http://www.cisco.com/en/US/docs/ios/12_0t/12_0t5/feature/guide/cbwfq.html).
- [60] Massive Networks, «Class of Service,» [En línea]. Available: <http://www.massivenetworks.net/index.cfm/ID/98/Massive-MPLS-QOS/-/Class-of-Service/>.