

Líder en Ciencia y Tecnología

Universidad Nacional de Ingeniería

Recinto Universitario Simón Bolívar

Facultad de Electrotecnia y Computación

Departamento de Sistemas Digitales y

Telecomunicaciones.

**Trabajo Monográfico Para Optar al Título de:
Ingeniero Electrónico.**

Título:

"Interconexión WAN de 3 sucursales de una empresa con casa matriz aplicando MPLS como tecnología de transporte mediante un diseño de red en GNS3"

Autor:

➤ ***Br. Luis Alfredo Cruz Chávez. Carnet: 2008 - 24334.***

Tutor:

➤ ***PhD. Héctor R. Guillen Navarrete.***

Managua, Nicaragua.

Agosto - 2022.

DEDICATORIA.

Quiero dedicar este trabajo primeramente a mi Madre, Paola Chávez, Con esto concluyo el arduo trabajo de muchos años de estudio y esfuerzo. A esto le sumaria la entrega y sacrificio que tuviste por mí a lo largo de años para poder hoy ver este sueño hecho realidad.

Agradezco a Dios por darme una madre como tú, que siempre trabajó y se esforzó para darme lo que necesitaba y lucho sin el apoyo de un esposo para que yo tuviera un mejor futuro.

Una madre que con su ejemplo me ha ensañado a ser una mejor persona, a creer que las cosas son posibles y que no se necesita tener muchos recursos para obtenerlas, basta con esfuerzo y dedicación tal y como tú lo has hecho , porque tú eres mi mayor inspiración.

Hoy finalizo mi carrera y obtengo el título de Ingeniero Electrónico gracias a ti mamá!!!

AGRADECIMIENTOS.

Estoy grandemente agradecido con Dios, por permitirme alcanzar este logro. Realmente en un momento creí que no lo iba a lograr, pero Dios me dio la fortaleza mental y emocional para reenfocar el trabajo luego de perder la mayoría de avances que tenía. Agradezco a Dios por abrirme puertas y proveerme los recursos que necesitaba para finalizar la monografía.

Así mismo agradezco a mi Esposa, Xochilt Herrera, por su apoyo durante todo este tiempo que tomó el titularme. Fue un pilar emocional, el escuchar sus palabras de que si podía lograrlo motivándome a que me esforzara, que era capaz de hacerlo aun cuando era difícil el poder verlo. Gracias Xo, has sido realmente una ayuda idónea en mi vida.

Quiero Agradecer también a personas como Eleazar Trejos y Félix Torres, que durante el trayecto de este logro me brindaron su asistencia. Les agradezco el poder compartir sus conocimientos sin esperar nada a cambio, los cuales he puesto en práctica para llevar a cabo este trabajo. Gracias por estar allí en momentos importantes.

Para Finalizar y sin quitar merito; estoy muy agradecido con mi Tutor, PhD. Hector Guillen, quien tuvo la paciencia y disposición desde el inicio. Gracias por sus consejos y sugerencias, han traído nitidez a mi cerebro. Sobre todo, le agradezco el permanecer conmigo en este camino, que tuvo momentos de espera, pero hoy ya he completado.

A todos y cada una de las personas que aportaron algo, desde lo más profundo de mi corazón, ¡muchas gracias!.

RESUMEN.

La presente tesis monográfica consiste en la interconexión de sucursales remotas de una empresa con su sitio central o casa matriz mediante un diseño de una red MPLS L3 VPN implementada en el software GNS3 que por su característica de emulación de IOS Cisco permite validar y demostrar el correcto funcionamiento del diseño de red obteniendo resultados fiables y similares a los de entornos de red reales. El diseño está dividido en 2 etapas: primero se diseña la infraestructura de red MPLS que permite proveer servicios (esto vendría siendo la red de un ISP). Luego se diseña la parte de los servicios L3 VPN tomando en cuenta los requerimientos de servicios que una empresa/institución brinda al momento de solicitar el servicio al área correspondiente de un ISP.

Este trabajo es teórico-práctico y parte de lo general a lo específico planteando las bases teóricas en los 2 primeros capítulos y en el tercer y último capítulo se plantea el diseño de red con las consideraciones correspondientes, se detalla la implementación en GNS3 y al final se realizan las validaciones respectivas de los servicios VPN. Este proceso de Diseño, Implementación y Validación se ha organizado de forma secuencial de manera que sirve como una guía paso a paso para entender cómo funciona la tecnología MPLS y cómo los ISP proveen los servicios L3 VPN sobre esta infraestructura de red.

Teniendo esto en mente este trabajo puede contribuir al proceso de enseñanza-aprendizaje de los estudiantes que cursan la carrera de Ingeniería Electrónica en la Universidad Nacional de Ingeniería UNI, mediante la aplicación práctica de los conceptos teóricos abordados en la asignatura Redes de Computadoras en un escenario real y de carácter educativo de manera que complemente la formación de los estudiantes.

LISTA DE FIGURAS.

Figura 1.1. Modelo OSI con MPLS.....	10
Figura 1.2. Etiquetado de Paquetes MPLS.	11
Figura 1.3. Etiquetado vs Encapsulación.....	13
Figura 1.4. Tablas de Etiquetas en enrutadores MPLS.	15
Figura 1.5. Operaciones de Etiquetado MPLS.	16
Figura 1.6. Dominio MPLS.	17
Figura 1.7. Dominio MPLS – LER y LSR.	18
Figura 1.8.....	19
Lógica de trabajo de LSR y LER.	19
Figura 1.9. Asignación de FEC a un Paquete.....	20
Figura 1.10. Encabezado MPLS.....	21
Figura 1.11. Establecimiento de un LSP.....	23
Figura 1.12. Intercambio de Etiquetas por LDP.	25
Figura 1.13. Routing en los Bordes y Switching en el Núcleo.....	26
Figura 1.14. Componentes de Control y Envío MPLS.	28
Figura 1.15. Funcionamiento Global MPLS.....	29
Figura 1.16. Ingeniería de tráfico MPLS.....	33
Figura 2.1. Diagrama de una VPN Empresarial.....	40
Figura 2.2. VPN de Acceso Remoto.....	41
Figura 2.3. VPN Sitio a Sitio utilizando IPsec.	42
Figura 2.4. Cifrado de Datos en un Túnel IPsec.	43
Figura 2.5. Tunelizado de Tráfico en IPsec.....	45
Figura 2.6. Proceso de Autenticación AAA.....	46
Figura 2.7. Tecnologías VPN basadas en Cliente o Red.	49
Figura 2.8. Modelo VPN Superpuesto con Túneles IP.....	51
Figura 2.9. Modelo VPN Peer to Peer.....	52
Figura 2.10. Modelo VPN Peer to Peer con MPLS VPN.	53
Figura 2.11. Modelo Superpuesto de VPN Tradicionales.....	56
Figura 2.12. Modelo MPLS Acoplado para VPN.....	57
Figura 2.13. Red P en una Red MPLS VPN.....	61

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

Figura 2.15. Interacción CE - PE - P en una Red MPLS VPN.....	62
Figura 2.16. MPLS L3 VPN tipo Full Mesh.	63
Figura 2.17. MPLS L3 VPN Hub and Spoke.	63
Figura 2.18. Diagrama de VPN´s Traslapadas.....	64
Figura 2.19. Creación de VRF por cada VPN en PE.....	65
Figura 2.20. Uso de RD y RT en MPLS VPN.	66
Figura 2.21. Trafico VRF a VRF en una red MPLS L3 VPN.	67
Figura 2.22. Funcionamiento Paso a Paso de MPLS L3 VPN.	69
Figura 2.23. Posible ataque en redes MPLS VPN.	69
Figura 3.1. Equipos Emulados y Simulados en GNS3.....	75
Figura 3.2. Topología de Red en GNS3.....	76
Figura 3.3. GNS3 VM 2.2.31 basada en VMware Workstation.....	77
Figura 3.4. Equipo Cisco 3725.....	82
Figura 3.5. Equipo Cisco Serie 7000.	82
Figura 3.6. Creación de Plantilla para Router Cisco en GNS3.....	83
Figura 3.7. Ajustes de la GNS3 VMware.	84
Figura 3.8. Esquema de la red MPLS L3 VPN.....	86
Figura 3.9. Asignación de Direcciones IP a Redes LAN y a Link L3 MPLS.	90
Figura 3.10. Habilitación de OSPF como Protocolo IGP de la Red.	92
Figura 3.11. Configuración de Link L3 entre los Routers.	92
Figura 3.12. Configuración de OSPF como Protocolo IGP.	93
Figura 3.13. Adyacencias OSPF Activas en los Routers.....	93
Figura 3.14. Habilitación de MPLS y LDP en la Red.	94
Figura 3.15. Configuración Global y de Interfaces de MPLS.	94
Figura 3.16. Verificación de CEF, MPLS y LDP habilitados.	95
Figura 3.17. Peer MPLS LDP luego de Habilitar el IGP.....	95
Figura 3.18. Habilitación de MP-iBGP utilizando RR.	96
Figura 3.19. Configuración de MP-iBGP entre PE y RR.	96
Figura 3.20. Peer iBGP Establecidos en el RR.....	97
Figura 3.21. Configuración de Costo de OSPF en Interfaces.	98
Figura 3.22. Mejor Ruta Escogida por OSPF Aplicando Costo a Interfaces.....	98

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

Figura 3.23. Red de Acceso del Cliente.....	99
Figura 3.24. Configuración y Verificación de VRF a Nivel Global e Interfaces.....	99
Figura 3.25. Configuración de Ruta Estática y Anuncio de la VRF en BGP.	100
Figura 3.26. Redes Recibidas por MP-iBGP para la VRF MPLS_IDAI.	100
Figura 3.27. Configuración de MQC como mecanismo de Calidad de Servicio.....	101
Figura 3.28. Configuración WAN y LAN en CE.	102
Figura 3.29. WAN-LAN de Sucursales ya son alcanzables desde la Red MPLS.....	102
Figura 3.30. Configuración de Interfaces para los Enlaces de Casa Matriz.	103
Figura 3.31. Configuración del Peer eBGP Primario y Secundario.....	103
Figura 3.32. Selección de la Mejor Ruta BGP usando Weight y As-Path Prepend.	104
Figura 3.33. Configuración de Interfaces y Peer eBGP en los PE´s.....	104
Figura 3.34. Configuración de QoS para el BW de Casa Matriz.	105
Figura 3.35. Peers eBGP de Casa Matriz hacia el ISP.	105
Figura 3.36. Configuración de Políticas de Ruteo en el Peer eBGP.....	106
Fuente Propia con Datos Obtenidos de Cartilla de Comandos BGP.	106
Figura 3.37. Antes y Después de Redes Aprendidas por eBGP en CE_CM.	106
Figura 3.38. Resultados de Pruebas ICMP de LAN a LAN.	107
Figura 3.39. Resultados de Pruebas Telnet a Routers CE.	108
Figura 3.40. Habilitación de Usuario y Telnet en los CE´s.....	108
Figura 3.41. Validación de Políticas QoS Aplicadas a los Sitios de la VPN.	109
Figura 3.42. Verificación del Flujo de Tráfico Enlace de Datos.	110
Figura 3.43. Prueba de Redundancia Enlace de Datos	110

LISTA DE TABLAS.

Tabla 1.1. Enrutamiento MPLS vs Enrutamiento IP.....	12
Tabla 1.2. MPLS en Acción.	30
Tabla 2.1. Protocolos según Modelo OSI para establecer una VPN.	48
Tabla 2.2. Comparación en cuanto a Servicios de Tecnologías VPN.	58
Tabla 3.1. Requisitos Mínimos de Instalación GNS3.....	78
Tabla 3.2. Requisitos Recomendados de Instalación GNS3.....	79
Tabla 3.3. Requisitos Óptimos de Instalación GNS3.....	79
Tabla 3.4. Asignación de Recurso de BW para Enlaces del Cliente.	81
Tabla 3.5. Rango de IP para las LAN de Cada Sitio.....	88
Tabla 3.6. Rango de IP para los Enlaces WAN.....	88
Tabla 3.7. Rango de IP para los Enlaces Red MPLS.....	89
Tabla 3.8. Direccionamiento para Loopback 0 de Equipos MPLS.....	90

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

LISTADO DE TERMINOS.

ACL: Access Control List – Lista de Control de Acceso.

ADSL: Asymmetric Digital Subscriber Line – Línea de Abonado Digital Asimétrica.

AMD: Advanced Micro Devices -

AS: Autonomous System – Sistema Autónomo.

ASA: Adaptive Security Appliance - Dispositivo de Seguridad Adaptable.

AS-Path: es el mecanismo usado por BGP para evitar bucles entre diferentes AS.

ATM: Asynchronous Transfer Mode - Modo de Transferencia Asíncrona.

AToM: Any Transport over MPLS – Cualquier Transporte sobre MPLS.

Backbone: Núcleo o Troncal de Red.

BGP: Border Gateway Protocol – Protocolo de Puerta de Enlace Exterior.

BW: Bandwidth - Ancho de banda.

CE: Customer Edge - Router Cliente

CEF: Cisco Express Forwarding – Envío Express de Cisco.

CoS: Class of Service – Clase de Servicio.

CPE: Customer Provided Equipment - Equipos Arrendados a un Cliente.

CHAP: Challenge Handshake Authentication Protocol - Protocolo de autenticación por desafío mutuo.

CPU: Central Processing Unit – Unidad Central de Procesamiento.

DES: Data Encryption Estándar – Cifrado estándar de datos.

DiffServ: Differentiated Services - Servicios Diferenciados.

DNS: Domain Name Service – Servicio de Nombre de Dominios.

DoS: Denial of Service – Negación de Servicio.

eBGP/iBGP: BGP externo e interno.

EGP: Exterior Gateway Protocol – Protocolo de Gateway Exterior.

EIGRP: Enhanced Interior Gateway Routing Protocol – Protocolo de enrutamiento de Gateway interior mejorado.

ESXi: Hipervisor de VMware antes conocido como ESX.

FEC: Forwarding equivalence Class - Clase de Envío Equivalente.

FIB: Forwarding Information Base - Base de Información de Encaminamiento.

Firewall: Cortafuegos de red.

FO: Fiber Optic – Fibra Optica.

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

Frame Relay: Tecnología WAN.

FTP: File Transfer Protocol – Protocolo de Transferencia de Archivos.

GRE: Generic Routing Encapsulation – Encapsulación de enrutamiento genérico.

GUI: graphical user interface – Interfaz Gráfica de Usuario.

HDLC: High-Level Data Link Control, Control de Enlace de Datos de Alto Nivel

HFC: Hybrid Fiber-Coaxial – Tecnología de banda ancha híbrida.

HTTP: Hypertext Transfer Protocol – Protocolo de Transferencia de Hipertexto.

Hyper-V: software de virtualización de hardware de Microsoft.

IANA: Internet Assigned Numbers Authority – Ente regulador de Internet.

IETF: Internet Engineering Task Force - Grupo de trabajo en Ingeniería de Internet.

IGP: Interior Gateway Protocol – Protocolo de Gateway Interior.

IOL: Cisco IOS on Linux.

IOS: Internetwork Operating System – Sistema Operativo de Red.

IP: Internet Protocol – Protocolo de Internet.

IPSec: Internet Protocol security – Seguridad del Protocolo de Internet.

IOU: Cisco IOS on Unix.

IPv4/IPv6: Protocolo de Internet versión 4 y 6.

ISP: Internet Service Provider - Proveedor de Servicios de Internet.

L2/L3: Capa 2 y 3 del Modelo OSI.

L2F: Layer 2 Forwarding – Encaminamiento de Capa 2.

L2TP: Layer 2 Tunneling Protocol – Protocolo de túnel de Capa 2.

Label Stack: Pila de Etiquetas.

Label: Etiqueta en MPLS.

LAN: Local Area Network – Red de Área Local.

LDP: Label Distribution Protocol - Protocolo de distribución de Etiquetas.

LER: Layer Edge Router - Router frontera entre capas.

LFIB: Label Forwarding Information Base – base de Información de envío de etiquetas.

LIB: Label Information Base - Base de datos de Información de Etiquetas.

Linux: Sistema operativo de Código abierto basado en UNIX.

Loopback: Interfaz de red virtual.

LSP: Label Switched Path - Camino conmutado de etiquetas.

LSR: Label Switch Router - Conmutador de Etiquetas.

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

MacOS: Macintosh Operating System - Sistema Operativo de Macintosh, de Apple.

MD5: Message-Digest Algorithm 5 – Algoritmo de reducción criptográfica 5

MP-BGP: BGP Multiprotocolo.

MPLS: Multiprotocol Label Switching – Conmutación de Etiquetas Multiprotocolo.

MPPE: Microsoft Point to Point Encryption - Cifrado de punto a punto de Microsoft.

MQC: Modular QoS Command Line – Interfaz de línea de comandos CLI para QoS modular.

NX-OSv: Plataforma virtual para simular equipos Cisco Nexus.

OF: Optical Fiber – Fibra Optica.

OSI: Open System Interconnection – Interconexión de Sistemas Abiertos.

OSPF: Open Shortest Path First – Procotolo de Ruta más Corta Primero

P: Provider Router – Router en el Núcleo del Proveedor de Servicios.

Packet Tracer: Herramienta de simulación de Cisco.

PAP: Password Authentication Protocol - Protocolo de Autenticación de Contraseña.

Payload: Carga útil o Mensaje.

PDU: Unidades de datos del Protocolo.

PE: Provider Edge Router - Router de Borde del Proveedor de Servicios.

PHP: Penultimito Hop Popping.

PKI: Public Key Infrastructure - Infraestructura de Llave Pública.

Pop: Desapilar Etiquetas MPLS

PPP: Protocolo Punto a Punto.

PPTP: Point to Point Tunneling Protocol – Protocolo de Túnel Punto a Punto.

Push: Apilar Etiquetas MPLS

PVC: Permanent Virtual Circuit – Circuito Virtual Permanente.

QoS: Quality of Service - Calidad de Servicio.

RADIUS: Remote Authentication Dial In User Service – Protocolo para autenticación y autorización de acceso remoto.

RAM: Random Access Memory – Memoria de acceso aleatorio.

RD: Route Distinguisher – Distinguidor de Prefijos del Cliente.

RFC: Request for Comment – Respuestas a comentarios.

RIB: Routing Information Base – Base de Información de Enrutamiento

RR: Route Reflector – Reflector de Rutas.

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

RSVP: Resource Reservation Protocol - Protocolo de Reserva de Recursos.	VIRL: Virtual Internet Routing Lab – Laboratorio de enrutamiento virtual de Internet.
RT: Route Target – Objetivo de Ruta (Prefijos VPNv4 de Clientes).	VirtualBox: Software de virtualización propietario de Oracle y sin licencia.
SDH: Synchronous Digital Hierarchy - Jerarquía Digital Síncrona.	VLSM: Variable Length Subnet Mask - Máscara de Subred de Longitud Variable
SLA: Service Level Agreement – Acuerdo de Nivel de Servicio.	VM: Virtual Machine – Máquina Virtual.
SP: Service Provider – Proveedor de Servicios.	VMware Workstation: Un tipo de Hipervisor licenciado.
SSD: Solid State Disk - Disco de Estado Sólido.	VoIP: Voice over IP – Voz sobre IP.
SSL: Secure Socket Layer – Capa de Sockets Seguro.	VPCS: Virtual PC Simulator – Simulador de PC Virtual.
Swap: Intercambiar Etiquetas.	VPI: Virtual Path Identifier - Identificador de Ruta Virtual.
TACACS: Terminal Access Controller Access-Control System - sistema de control de acceso mediante control del acceso desde terminales.	VPLS: Virtual Private LAN Service - Servicio de LAN Privada Virtual.
TCP: Transfer Control Protocol – Protocolo de Control de Transmisión.	VPN: Virtual Private Network - Red Privada Virtual.
TDM: Time Division Multiplexing - Multiplexación por División de Tiempo.	VPNv4: Rutas IPv4 del cliente + añadir el RD.
TI: Tecnologías de la Información.	VRF: Virtual Routing and Forwarding – Enrutamiento y encaminamiento virtual basado en VPN.
TTL: Time to Live – Tiempo de Vida.	WAN: Wide Area Network – Red de Area Amplia.
UDP: User Datagram Protocol – Protocolo de Datagramas de Usuario.	X.25: Conexiones Seriales.
VCI: Virtual Channel Identifier - Identificador de Circuito Virtual.	

ESTRUCTURA DE CONTENIDO

Este trabajo monográfico se organiza en 3 capítulos de contenido y 3 secciones de información, va de lo general a lo específico, se describe de la siguiente forma:

En la Sección 1 se inicia con la introducción al trabajo desarrollado, una breve reseña histórica de la evolución de las tecnologías WAN, se establecen los objetivos a cumplir, así como el porqué del trabajo y la importancia de este.

En el Capítulo I se aborda todo lo relacionado a MPLS, que constituye la base del marco teórico, su definición, descripción, elementos que la componen, su funcionamiento, beneficios y los servicios que pueden implementarse con MPLS.

En el Capítulo II, como primer punto, se habla de manera general de las VPN, los tipos, características y beneficios de utilizar redes VPN. Luego se describen las tecnologías para proveer servicios de VPN y se realiza una comparación de las más utilizadas en la actualidad. Al final se aborda a profundidad la tecnología MPLS VPN. Se menciona las topologías, terminología, elementos, características y funcionamiento de las VPN sobre MPLS.

En el Capítulo III se diseña e implementa la Red MPLS L3 VPN tomando en cuenta los requerimientos de servicios y lo referente al software donde se implementará. El diseño se divide en 2 partes: la red MPLS y los servicios L3 VPN que corren por dicha red. Como paso final se realiza la validación del diseño de red mediante la emulación de los IOS Cisco en GNS3. Se realizan pruebas de conectividad de servicios VPN y verificación de políticas de QoS aplicadas.

En la Sección 2 se presentan las conclusiones del trabajo, las recomendaciones como opciones de mejoras y las referencias bibliográficas que respaldan el contenido del mismo.

En la Sección 3 se agregan los Anexos. Se incluyen las especificaciones y configuraciones de Routers, sondeo realizado a egresados/titulados sobre MPLS, detalles de software utilizado y una cotización de servicios MPLS L3 VPN a 2 ISP.

COMENTARIOS FINALES DE LOS CAPITULOS.

CAPITULO I.

En resumen, MPLS es hoy día ampliamente utilizada para diferentes aplicaciones, como los servicios de VPN sobre MPLS. Se le puede considerar como una autopista por la cual pueden circular diferentes "vehículos" o diferentes soluciones de manera eficaz. Su impacto es tal que los ISP han migrado su Backbone, de arquitecturas de red como ATM a MPLS, para gozar de los múltiples beneficios que esta brinda, tanto para los ISP como para los usuarios finales.

CAPITULO II.

Según lo visto en el capítulo se evidencia la importancia de la Redes Privadas Virtuales para las empresas y organizaciones, pues estas les permiten que los sitios que están geográficamente distantes tengan conectividad entre ellos y puedan comunicarse y transmitir información relevante. Aún más importante es MPLS VPN, una de las tecnologías VPN más implementadas en la actualidad, siendo la opción favorita de los ISP para brindar a las empresas y usuarios finales un canal seguro a través de la Internet pública, con flexibilidad y escalabilidad.

CAPITULO III.

El uso de la herramienta informática GNS3 es de suma importancia para profesionales que buscan una de las certificaciones Cisco y para aquellos también que necesitan probar equipos o topologías de red antes de implementarlas en una red en producción ya que con las características que brinda el software se garantizan resultados casi 100% iguales a los esperados de redes reales.

En el capítulo se realizaron las 3 etapas de un proyecto, las cuales son la etapa de diseño en basa a los requerimientos del cliente, luego se llevó a cabo la etapa de implementación mediante el software de emulación de IOS Cisco GNS3 que nos permite prescindir de equipos físicos reales costosos y por último la etapa de validación del diseño con las pruebas de conectividad de los enlaces de datos e internet tanto a nivel WAN como LAN.

INDICE DE CONTENIDO.

DEDICATORIA.....	ii
AGRADECIMIENTOS.....	iii
RESUMEN.....	iv
LISTA DE FIGURAS.....	v
LISTA DE TABLAS.....	viii
LISTADO DE TERMINOS.....	ix
ESTRUCTURA DE CONTENIDO.....	xiii
COMENTARIOS FINALES DE LOS CAPITULOS.....	xiv
INDICE DE CONTENIDO.....	xv
SECCION I. CONSIDERACIONES INICIALES.....	1
I. INTRODUCCION.....	2
II. CONTEXTO HISTÓRICO.....	3
III. OBJETIVOS.....	5
OBJETIVO GENERAL Y ESPECIFICOS.....	5
IV. JUSTIFICACION.....	6
CAPITULO I: ARQUITECTURA DE RED MPLS.....	7
1.1. GENERALIDADES SOBRE MPLS.....	8
1.1.1. VISION GENERAL.....	8
1.1.2. DEFINICION DE MPLS.....	9
1.1.3. DESCRIPCION DE MPLS.....	10
1.2. SOBRE LA ARQUITECTURA MPLS.....	11
1.2.1. MEJORAS EN LA CONMUTACION.....	11
1.2.2. MEJORAS EN EL ENRUTAMIENTO.....	12
1.2.3. ETIQUETADO FRENTE A ENCAPSULACION.....	13
1.2.4. TABLAS DE GESTION DE ETIQUETAS MPLS.....	14
1.2.5. OPERACIONES DE ETIQUETADO MPLS.....	15
1.3. ELEMENTOS DE LA ARQUITECTURA MPLS.....	16
1.3.1. ELEMENTOS FISICOS MPLS.....	16
1.3.2. ELEMENTOS LOGICOS MPLS.....	19
1.4. FUNCIONAMIENTO DE MPLS.....	25

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

1.4.1. ROUTING EN LOS BORDES Y SWITCHING EN EL NUCLEO..	26
1.4.2. COMPONENTES FUNCIONALES DE MPLS.	27
1.4.3. FUNCIONAMIENTO GLOBAL.	28
1.5. BENEFICIOS DE IMPLEMENTAR MPLS.....	31
1.5.1. SOPORTE DE QoS.....	31
1.5.2. INGENIERÍA DE TRÁFICO.....	32
1.5.3. SOPORTE DE REDES PRIVADAS VIRTUALES (VPN).....	34
1.5.4. USO DE UNA INFRAESTRUCTURA DE RED UNIFICADA.	35
COMENTARIOS FINALES CAPITULO I.....	36
CAPITULO II: TECNOLOGIA MPLS VPN.....	37
2.1. INTRODUCCION A LAS MPLS VPN.....	38
2.2. VIRTUAL PRIVATE NETWORK - VPN.....	39
2.2.1. SOBRE LAS VPN´s.....	39
2.2.2. QUE ES UNA VPN.....	40
2.3. TIPOS DE VPN´s.....	40
2.3.1. VPN DE ACCESO REMOTO.	41
2.3.2. VPN SITIO A SITIO.....	41
2.3.3. CARACTERÍSTICAS DE LAS VPN´s.....	42
2.3.4. BENEFICIOS DE UTILIZAR UNA VPN.....	47
2.4. SERVICIOS DE REDES PRIVADAS VIRTUALES VPN.....	47
2.4.1. CLASIFICACION DE SERVICIOS VPN.....	48
2.4.2. MODELOS DE SERVICIOS VPN.....	50
2.4.3. COMPARATIVA DE TECNOLOGIAS VPN.	54
2.5. SERVICIOS MPLS L3 VPN.....	59
2.5.1. TERMINOLOGÍA MPLS L3 VPN.....	60
2.5.2. TOPOLOGIAS MPLS L3 VPN.....	62
2.5.3. COMPONENTES FUNCIONALES L3 VPN.....	64
2.5.4. COMO OPERAN LAS MPLS L3 VPN.	68
COMENTARIOS FINALES CAPITULO II.....	71
CAPITULO III: IMPLEMENTACION DE UNA RED MPLS L3 VPN.	72
3.1. INTRODUCCION A LAS REDES MPLS L3 VPN.....	73

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

3.2. SOFTWARE GNS3.....	74
3.2.1. SOBRE EL PROGRAMA GNS3.....	74
3.2.2. CARACTERISTICAS DE GNS3.....	75
3.2.3. BENEFICIOS Y LIMITACIONES DE GNS3.....	77
3.2.4. REQUISITOS PARA INSTALAR GNS3.....	78
3.3. DISEÑO DE UNA MPLS L3 VPN.....	79
3.3.1. REQUERIMIENTOS DE SERVICIO.....	80
3.3.2. ELECCION DE EQUIPOS/IMAGENES PARA USO EN GNS3...	81
3.3.3. TOPOLOGIA DE RED MPLS L3 VPN.....	84
3.3.4. ASIGNACION DE DIRECCIONES IP – IP PLAN.....	87
3.4. IMPLEMENTACION DEL DISEÑO EN GNS3.....	90
3.4.1. CONFIGURACION DE LA RED MPLS.....	91
3.4.2. CONFIGURACION DE ENLACES DE DATOS SUCURSALES..	98
3.4.3. CONFIGURACION DE ENLACES DE DATOS CASA MATRIZ.	102
3.5. VALIDACION DEL DISEÑO MPLS L3 VPN.....	107
3.5.1. VERIFICACION DE ENLACES DE DATOS.....	107
3.5.2. VERIFICACION DE REDUNDANCIA DE CASA MATRIZ.....	109
COMENTARIOS FINALES CAPITULO III.....	111
SECCION II: CONSIDERACIONES FINALES.....	112
I. CONCLUSIONES.....	113
II. RECOMENDACIONES.....	114
III. REFERENCIAS BIBLIOGRAFICAS.....	115
SECCION III: ANEXOS.....	i
ANEXO I: SONDEO A EGRESADOS Y ENLACES EXTERNOS.....	ii
I.I ENLACES A ARCHIVOS DE CONFIGURACIÓN DE ROUTERS.....	ii
I.II SONDEO A EGRESADOS/TITULADOS SOBRE MPLS.....	ii
ANEXO II: ESPECIFICACIONES DE EQUIPOS DE RED UTILIZADOS.....	iii
II.I ROUTER CISCO SERIE 7200 VXR.....	iii
II.II ROUTER CISCO SERIE 3725.....	v
ANEXO III: COTIZACION DE SERVICIOS DE MPLS VPN A ISP.....	vi
ANEXO IV: DETALLES DE SOFTWARES UTILIZADOS.....	vii

SECCIÓN I: CONSIDERACIONES INICIALES

En esta sección se inicia con la introducción al trabajo desarrollado, una breve reseña histórica de la evolución de las tecnologías WAN, se establecen los objetivos a cumplir, así como el porqué del trabajo y la importancia de este.

I. INTRODUCCION.

El Objeto de Investigación propuesto se sitúa en el campo de conocimiento de las tecnologías de la información TI. Esto debido a que trata del envío de información a través de las redes de datos utilizando tecnologías de transporte de última generación que satisfagan las demandas de los usuarios finales, así como las necesidades de los ISP's. En nuestro caso en particular servicios MPLS VPN.

MPLS VPN es un tipo de VPN basada en la red (Network-based) y no en el cliente, por lo que el trabajo se enfoca en el diseño de la red MPLS de un ISP y cómo se proveen los servicios de VPN sobre esta infraestructura de red. Al ser un servicio Network-based, la implementación de la VPN no requiere un hardware específico ni costoso para ser instalado en las oficinas del cliente. De este modo, empresas que aún mantienen diferentes y costosos servicios para soportar sus necesidades de voz, datos y video; pueden unificar estos requerimientos con un único proveedor de servicios concluyendo en un ahorro significativo.

Este trabajo monográfico es teórico-práctico y su alcance parte de la base teórica necesaria para realizar el diseño de red MPLS L3 VPN para luego implementarlo en el software GNS3, de manera que exista forma de validar la aplicación del diseño de red mediante pruebas de servicios VPN entre sitios remotos obteniendo; gracias a la característica de emulación de GNS3; resultados válidos, confiables y que se asemejan a resultados de entornos de red reales. Esto con el fin de aportar el ingrediente práctico a la investigación llevada a cabo de manera que se profundicen los conocimientos adquiridos.

Teniendo esto en mente este trabajo puede contribuir al proceso de enseñanza-aprendizaje de los estudiantes que cursan las carreras de Ingeniería Electrónica e Ingeniería en Telecomunicaciones en la Universidad Nacional de Ingeniería UNI, mediante la aplicación práctica de los conceptos teóricos abordados en la asignatura Redes de Computadoras en un escenario real y de carácter educativo de manera que complemente la formación de los estudiantes.

II. CONTEXTO HISTÓRICO.

En un mundo en el que día a día las empresas incursionan en nuevos mercados, en busca de más clientes de diferentes países, se hace necesaria la comunicación dentro de sus diferentes sedes para transmitir información sobre ventas o estrategias de negocio, para informar sobre la producción minuto a minuto, o cualquier otro fin; este tipo de crecimiento empresarial ha dado lugar a que se desarrollen tecnologías que satisfagan las necesidades de las empresas, en el sentido de velocidad, disponibilidad y seguridad de su comunicación.

En años anteriores una de las grandes limitantes en las empresas ha sido la comunicación, debido a que, si se deseaba tener diferentes servicios como telefonía, enlace de datos y videoconferencia, era necesario tener un proveedor para cada tipo de servicio, es decir tener en la empresa 3 proveedores diferentes ofreciendo diferentes productos conllevaba a un gasto múltiple y poco rentable.

Cosa contraria se observa hoy en día, ya que los proveedores de servicios están ofreciendo sobre el mismo canal servicios de datos, servicios de voz , conexión a Internet y más reciente ahora servicios en la nube, este paquete de servicios recibe el nombre de Convergencia y donde se tiene como principales característica: Calidad del Servicio, Priorización, Seguridad y Anchos de Banda garantizados para cada uno de los servicios que se presta en la red.

Las empresas hoy en día se preocupan por contar con una infraestructura escalable y de gran flexibilidad, tanto en sus redes empresariales como en los servicios provistos por un ISP, que les permita conectarse con quien deseen (entre empresas, sucursales, clientes y proveedores) con una excelente calidad y disponibilidad. Entre estos servicios requeridos por las empresas encontramos:

- Videoconferencias.
- Transmisión de datos a altas velocidades.
- Telefonía.

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

- Transacciones Electrónicas.
- Comercio Electrónico.
- Conexión a Internet.
- Servicios en la Nube.
- Acceso a sistemas de sedes centrales.

En el momento actual los ISP's tienen ante sí el enorme reto de gestionar redes cada vez más complejas y extensas con una mayor gama de servicios, más aún con la aparición de nuevos servicios y realidades a raíz de la situación global padecida por el Covid-19. Cuando un proveedor desea cumplir con las condiciones técnicas y requerimientos para brindar los servicios antes mencionados se hace necesario que se trabaje sobre redes MPLS basadas en IP que garanticen la seguridad, confiabilidad, escalabilidad, flexibilidad y Calidad de Servicio (QoS).

Tecnologías como FRAME RELAY, ATM y MPLS han sido desarrolladas para hacerle frente a estos requerimientos, Frame Relay y ATM como redes de transporte tradicionales y MPLS como una solución emergente más eficiente a las anteriores. Con MPLS, además de poder hacer ingeniería de tráfico IP, permite mantener clases de servicios para cada tráfico y soporta con gran eficacia la creación de VPN's, tecnología muy usada por las empresas para transportar sus datos de forma segura.

En las últimas décadas MPLS ha sido el estándar adoptado como solución dominante a estos requerimientos de comunicación, aunque actualmente existen nuevas tecnologías WAN enfocada a servicios en la nube como SD-WAN, MPLS aún no ha sido destronada y se mantiene como una solución confiable, robusta y segura para brindar servicios.

III. OBJETIVOS.

OBJETIVO GENERAL.

Interconectar a nivel WAN 3 sucursales de una empresa con casa matriz aplicando MPLS como tecnología de transporte mediante un diseño de red en GNS3.

OBJETIVOS ESPECÍFICOS.

1. Establecer los conceptos fundamentales que abarcan la Conmutación de Etiquetas Multiprotocolo - MPLS, así como los principales componentes de esta arquitectura.
2. Describir las tecnologías que proveen servicios VPN haciendo énfasis en MPLS VPN y a la vez realizar una breve comparación entre las tecnologías más utilizadas.
3. Diseñar la Red MPLS L3 VPN en base a los requerimientos de servicio y necesidades de comunicación de un Cliente.
4. Emular la Interconexión WAN de Casa Matriz con sus Sucursales haciendo uso de la herramienta de software GNS3 para la validación del diseño de red planteado.

IV. JUSTIFICACION.

La elaboración de este trabajo monográfico apunta a cumplir con el requisito que establece la Universidad Nacional de Ingeniería - UNI para la culminación de estudios de la carrera de Ingeniería Electrónica del plan de Estudios 97, de tal manera que obtenga el grado de Ingeniero Electrónico y pueda desarrollar el nivel de conocimiento ingenieril pudiendo optar por estudios de Post-Grado.

Luego de realizar un sondeo tanto a estudiantes egresados como titulados se demuestra que el conocimiento sobre MPLS es teórico, reducido a material extraído del internet y opiniones de maestros que no permiten tener una idea clara y veraz, por tal razón se desarrolla el presente trabajo que permite entender cómo funciona la tecnología MPLS y cómo se proveen servicios sobre la misma.

Este trabajo beneficiará tanto a estudiantes como a maestros y/o personas interesadas, donde podrán encontrar un documento que no sólo establezca los fundamentos teóricos de MPLS, sino que también demuestre su funcionamiento mediante un diseño de red, capaz de ser implementada en un entorno real para cualquier empresa en Nicaragua.

Así mismo podrá ser utilizada como material de consulta para futuros trabajos relacionados al tema, dado que se buscó en la biblioteca de la Universidad Nacional de Ingeniería documentos con objetivos similares a los establecidos en este proyecto y se encontraron un par, los cuales no profundizan en el tema.

En este trabajo se implementa un ejemplo práctico del funcionamiento y operación de MPLS, se aplica la solución MPLS L3 VPN para la interconexión de sitios de una empresa utilizando GNS3 para validar el diseño de red propuesto a nivel de conectividad WAN y LAN. Esto aporta un mayor peso a la monografía debido a que se demuestra el funcionamiento de la tecnología de una manera práctica, presentando un diseño de red semejante al que utilizan los ISP en Nicaragua dentro de un ambiente emulado como lo es GNS3.

CAPITULO I: ARQUITECTURA DE RED MPLS.

Este capítulo aborda lo relacionado a la teoría de MPLS, que constituye la base del marco teórico, su definición, descripción, elementos que la componen, funcionamiento, beneficios y los servicios que se pueden implementar sobre MPLS.

1.1. GENERALIDADES SOBRE MPLS.

1.1.1. VISION GENERAL.

La Conmutación de Etiquetas Multiprotocolo MPLS existe hace más de dos décadas, fue diseñada como solución emergente para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes.

Desde sus inicios, a mitad de los años 90, la tecnología MPLS fue bien recibida por la comunidad de internet y continuó creciendo rápidamente hasta convertirse en un estándar para las tecnologías WAN, reemplazando a Frame Relay y ATM como la tecnología preferida para llevar voz, video y datos de alta velocidad en una sola conexión al proporcionar una mayor fiabilidad, un mayor rendimiento y reducir los costos mediante una mayor eficiencia de la red. **(Cisco Systems, Inc., 2013, pág. 45)**

MPLS combina el rendimiento y las capacidades de la conmutación de capa 2 (enlace de datos) con la escalabilidad comprobada del enrutamiento de capa 3 (capa de red). MPLS permite a los proveedores de servicios enfrentar los desafíos del crecimiento explosivo en la utilización de la red al tiempo que brinda la oportunidad de diferenciar los servicios sin sacrificar la infraestructura de red. La arquitectura MPLS es flexible y se puede emplear en cualquier combinación de tecnologías de Capa 2. Ofrece compatibilidad para los protocolos de capa 3 y es posible escalar mucho más allá de lo que ofrece las redes actuales.

MPLS permite de manera eficiente la entrega de servicios IP a través de una red conmutada ATM. También admite la creación de diferentes rutas entre un origen y un destino en una red troncal de Internet basada en enrutadores. Al incorporar MPLS en su arquitectura de red, los SP pueden ahorrar dinero, aumentar los ingresos y la productividad, brindar servicios diferenciados y obtener ventajas competitivas. **(Cisco Systems, Inc., 2013, pág. 45)**

1.1.2. DEFINICION DE MPLS.

MPLS quiere decir Conmutación de Etiquetas Multiprotocolo (Multiprotocol Label Switching), es un estándar creado por la IETF (Internet Engineering Task Force - organización dedicada a facilitar los procesos de trabajo a través de Internet) y definido en el RFC 3031.

Según **(Barberá, 2000)** define a MPLS como:

“Un estándar del IETF que surgió para consensuar diferentes soluciones de conmutación multinivel propuesto por diferentes fabricantes a mitad de los años noventa.

Según el énfasis que se tenga a la hora de explicar sus características y utilidad, MPLS se puede presentar como un sustituto de la conocida arquitectura IP sobre ATM, también como un protocolo para hacer túneles, o bien, como una técnica para acelerar el encaminamiento de paquetes”.

Por otro lado, **(Tapasco Garcia, 2008)** nos comparte que:

“MPLS es una tecnología relativamente nueva que se desarrolló para solucionar la mayoría de los problemas que existen en la técnica (ATM, Frame Relay) de reenvío de paquetes de datos para la comunicación entre dispositivos sobre infraestructuras de transmisión mixtas.” **(Pag.7)**.

De lo anterior podemos darnos cuenta que MPLS no es un tipo de servicio, sino una tecnología de transporte de datos, que en sus inicios fue protocolo interoperable para las tecnologías de conmutación en ese entonces pero que ahora es un estándar de arquitectura de red. Sin embargo, MPLS también es capaz de brindar cualquier tipo de servicio en las capas 1 a 4 del modelo OSI, ya sea voz, video, multimedia u otro tipo de servicio de valor agregado. Podemos decir entonces que por MPLS pasa casi prácticamente todo el tráfico de internet.

1.1.3. DESCRIPCION DE MPLS.

Con MPLS los problemas que presentan las comunicaciones sobre redes ATM; tales como la expansión sobre una topología virtual, la complejidad de gestión de dos redes separadas y tecnológicamente diferentes; quedan resueltos al combinar en una sola tecnología la inteligencia del Routing (enrutamiento) con la rapidez del Switching (conmutación de paquetes). (Barberá, 2000)

MPLS opera entre la capa 2 (de enlace de datos) y la capa 3 (de red) del modelo OSI, como se muestra en la **Figura 1.1.** se podría decir que es un protocolo de unión entre la capa de enlace y la capa de red. Puede considerarse como una evolución tecnológica para construir y gestionar redes IP acorde a las necesidades actuales.



Figura 1.1. Modelo OSI con MPLS.

Fuente Propia con datos de MPLS Fundamentals, De Ghein, 2007.

Las características principales del estándar MPLS pueden resumirse como:

- ✚ Interoperabilidad. Funciona sobre cualquier tecnología de transporte.
- ✚ Flexibilidad. Soporta el envío de paquetes tanto Unicast como Multicast.
- ✚ Escalabilidad. Permite el crecimiento constante de Internet.
- ✚ Capacidad de ofrecer QoS e Ingeniería de Tráfico. Al tener mecanismo de clasificación de paquetes. (Infotecs, 2020)

1.2. SOBRE LA ARQUITECTURA MPLS.

1.2.1. MEJORAS EN LA CONMUTACION.

MPLS combina la flexibilidad de las comunicaciones punto a punto o Internet y la fiabilidad, calidad y seguridad de los servicios Private Line, Frame Relay o ATM. De esta manera intenta conseguir las ventajas de ATM, pero sin sus inconvenientes. (Angulo & Hernandez, 2005, pág. 1)

MPLS se basa en el etiquetado de los paquetes en base a criterios de prioridad y/o calidad de servicio (QoS). Asigna a los datagramas de cada flujo una etiqueta única que permite una conmutación rápida en los Routers intermedios (solo se mira la etiqueta, no la dirección de destino). Tal como muestra la **Figura 1.2.**

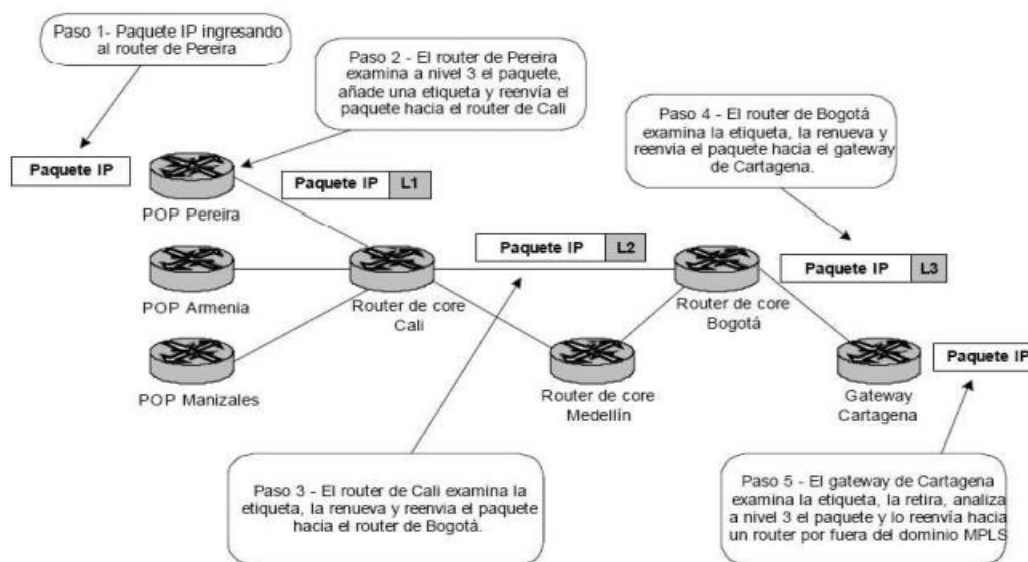


Figura 1.2. Etiquetado de Paquetes MPLS.

Reproducida de MPLS el Presente de las Redes IP, Tapasco Garcia, 2008.

La idea de MPLS es realizar la conmutación de los paquetes o datagramas en función de las etiquetas añadidas en capa 2 y etiquetar dichos paquetes según la clasificación establecida por la QoS. El etiquetado en capa 2 permite ofrecer servicio multiprotocolo y ser portable sobre multitud de tecnologías de capa de enlace: ATM, Frame Relay, líneas dedicadas, LAN's. Pues el funcionamiento de MPLS es independiente de la capa que corra bajo este (Angulo & Hernandez, 2005, pág. 1).

1.2.2. MEJORAS EN EL ENRUTAMIENTO.

En el encaminamiento IP tradicional, la dirección de destino junto a otros parámetros de la cabecera, es examinada cada vez que el paquete atraviesa un Router. La ruta del paquete se adapta en función del estado de las tablas de enrutamiento de cada nodo, pero, como esta no puede predecirse, las búsquedas en tablas de encaminamiento hacen que cada nodo pierda cierto tiempo, que se incrementa en función de la longitud de la tabla, lo que puede influir en la calidad del servicio (QoS). (Infotecs, 2020)

Sin embargo, MPLS permite a cada nodo, ya sea un switch o un Router, asignar una etiqueta a cada uno de los elementos de la tabla de envío y comunicarla a sus nodos vecinos. Esta etiqueta es un valor corto y de tamaño fijo transportado en la cabecera del paquete IP y que establece una correspondencia entre el tráfico y un FEC específico (Clase de Equivalencia de Reenvío). Dicha etiqueta se asigna al paquete IP basándose en su dirección de destino, los parámetros de tipo de servicio, la pertenencia a una VPN o algún otro criterio. De este modo los paquetes se envían en función de las etiquetas. No se examina la cabecera de red. El direccionamiento es más rápido. (Infotecs, 2020)

La **Tabla 1.1.** muestra las diferencias entre ambos enrutamientos.

Tabla 1.1. Enrutamiento MPLS vs Enrutamiento IP.
Adaptada de MPLS el Presente el Presente de las Redes IP, Tapasco Garcia, 2008

	Enrutamiento IP	Enrutamiento MPLS
Análisis Encabezado IP	El análisis se realiza en cada uno de los Routers.	Cuando la etiqueta es asignada en el borde la Red
Soporte de Unicast y Multicast.	Necesaria la aplicación de diferentes algoritmos.	Es necesario sólo un algoritmo de envío.
Decisión de Enrutamiento.	Está basado en direcciones IP.	Se basa en parámetros como QoS.
Base de Datos.	Se define con la tabla de enrutamiento IP.	Con la tabla de Clases Equivalentes de Envío FEC.
Protocolos.	Protocolos de enrutamiento IP.	Protocolos de Control que intercambian los contenidos de la tabla FEC entre LSR.

1.2.3. ETIQUETADO FRENTE A ENCAPSULACION.

MPLS etiqueta los paquetes al momento del ingreso a la red a través de uno de sus Routers de Borde (LER). Sin embargo, hay que diferenciar que este proceso en cómo funciona el etiquetado no es lo mismo a encapsulación, como se hace en cada una de las capas del modelo OSI.

Cuando se encapsula un protocolo en otro se forma las unidades de datos del protocolo (PDU), estas PDU's son contenidas una dentro de otra por cada capa donde el mensaje ha sido encapsulado. Siendo el paquete la PDU de la capa de red, cada capa emisora toma la PDU de la capa superior y lo codifica dentro del área de datos. A medida que se transmite la capa recibe la PDU de su capa par, recupera el área de datos y la transmite a su capa superior que opera igualmente. Por esta razón las PDU tienen encapsuladas en su área de datos otras PDU. **(Morales Dibildox, 2006, pág. 59)**

MPLS toma la PDU de red y la transmite intacta, solo coloca una etiqueta entre el encabezado de red y el de enlace, esto deja integras las tramas pequeñas de tamaño fijo del protocolo de red **(Figura 1.3.)**. Si el protocolo de red es IP, las tramas son variables y grandes, MPLS no modifica esta información y la transmite intactas siendo la longitud de las tramas fija lo que generaliza el proceso.

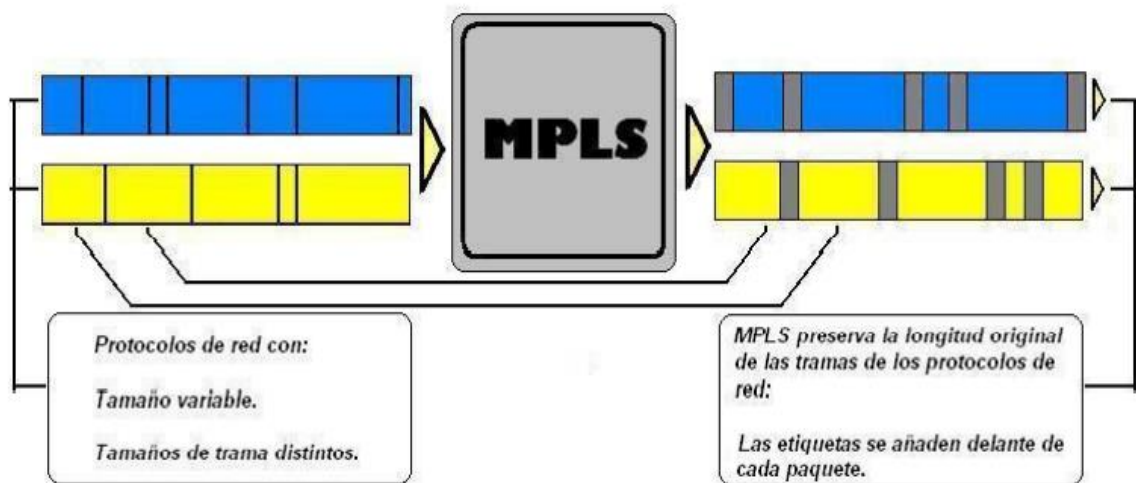


Figura 1.3. Etiquetado vs Encapsulación.

Reproducida de Investigación de Redes VPN con MPLS, Morales Dibildox, 2006.

1.2.4. TABLAS DE GESTION DE ETIQUETAS MPLS.

Para la gestión de los distintos caminos dentro de la red los Routers utilizan tablas de información y reenvío de etiquetas. La base de datos de información de las etiquetas que administra un Router se denomina LIB (Label Information Base). La base de datos de reenvío de etiquetas se denomina LFIB (Label Forwarding Information Base). La tabla de reenvío de paquetes de capa 3 se denomina FIB (Forwarding Information Base), también conocida como RIB (Forwarding Information Base) pues es la tabla de enrutamiento IP tradicional. **(Cruz, Alincaastro, Magnago, & Hernandez, 2013)**

Abajo se describen los 3 tipos de tablas por las cuales un enrutador MPLS toma decisión:

- ❖ LIB: Label Information Base. La tabla LIB gestiona la base de información de las etiquetas que administran los nodos MPLS. Es la encargada de relacionar la pareja (interfaz de entrada - etiqueta de entrada) con (interfaz de salida - etiqueta de salida). En ella solo se observa información de etiquetas MPLS y es utilizada por LDP para la gestión y el envío de etiquetas. Las LIB solo se utilizan en los nodos Frontera (LER).

- ❖ LFIB: Label Forwarding Information Base. O Base de Información para el reenvío de etiquetas. La tabla LFIB es la encargada de asociar las etiquetas con los destinos o rutas de capa 3 y la interfaz de salida del Router. Además, es la encargada de indicar al Router la acción a aplicar al paquete: push, swap o pop. (RFC 5036). Todos los nodos de la red deberán tenerla.

- ❖ FIB: Forwarding Information Base. Esta sería como la tabla de enrutamiento IP convencional. La tabla FIB está basada en rutas de direcciones IP, pero con soporte hardware, para equipos Cisco, utilizando CEF (Cisco Express Forwarding). Esta tabla se actualiza automáticamente con los protocolos de ruteo. **(Cruz, Alincaastro, Magnago, & Hernandez, 2013, pág. 4)**

En la **Figura 1.4.** se muestra un ejemplo del contenido de la tabla LIB y LFIB.

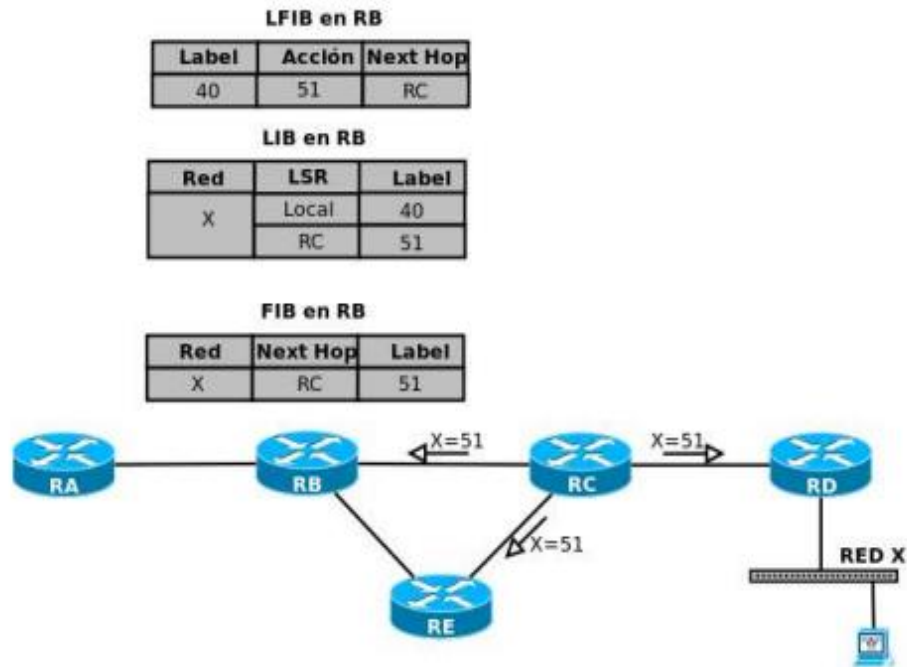


Figura 1.4. Tablas de Etiquetas en enrutadores MPLS.
Reproducida de **Análisis de la Implementación de MPLS en tecnologías de Redes,**
Cruz & Alincastro & Magnago & Hernandez, 2013.

1.2.5. OPERACIONES DE ETIQUETADO MPLS.

Cuando un paquete llega a un enrutador MPLS, este puede realizar una o más operaciones de etiquetado basado en el contenido de su tabla de etiqueta. Estas operaciones son: apilar(PUSH), desapilar(POP), intercambiar(SWAP). **Figura 1.5.**

- ✚ En una operación PUSH una nueva etiqueta es empujada encima de otra (si existe). Si en efecto había otra etiqueta antes de efectuar esta operación, la nueva etiqueta «encapsula» la anterior. Sino solamente se añade la etiqueta.
- ✚ En una operación POP la etiqueta es retirada del paquete lo cual puede revelar una etiqueta interior (si existe). A este proceso se lo llama «desencapsulado» y es usualmente efectuada por el enrutador de egreso.
- ✚ En una operación SWAP la etiqueta es cambiada por otra y el paquete es enviado en el camino asociado a esta nueva etiqueta. Esta operación es realizada por enrutadores en el núcleo del dominio MPLS. **(De Ghein, 2007, pág. 44)**

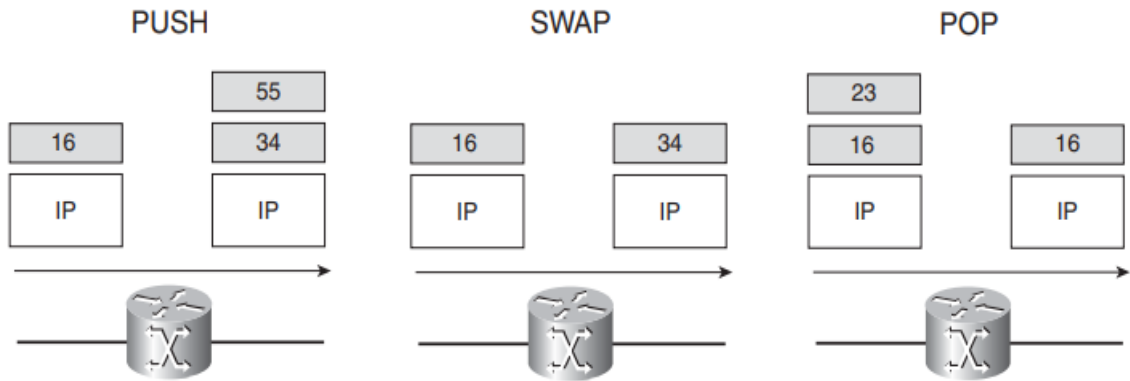


Figura 1.5. Operaciones de Etiquetado MPLS.
Adaptada de MPLS - Fundamentals, De Ghein, 2007.

1.3. ELEMENTOS DE LA ARQUITECTURA MPLS.

La base de MPLS está en la asignación e intercambio de etiquetas que permiten el establecimiento de caminos por los cuales son reenviados los paquetes dentro de la red. Para establecer estos caminos (LSP) participan elementos físicos y lógicos que conforman la arquitectura MPLS. A continuación, se describen.

1.3.1. ELEMENTOS FISICOS MPLS.

Una red MPLS está compuesta por enrutadores MPLS: LSR (Label Switched Router) que están el núcleo de la red o Backbone y los LER (Label Edge Router), que son los Routers de frontera encargados de realizar la interfaz con otras redes. Llamados también LSR de borde. (Silvestre Hernandez, 2008, pág. 2)

Según (De Ghein, 2007), “estos enrutadores son capaces de comprender las etiquetas MPLS, de recibir y transmitir un paquete etiquetado en un enlace de datos y de realizar las 3 operaciones de etiquetado: Pop, Push y Swap” (Pág. 29).

Ambos enrutadores (LER y LSR) constituyen el dominio MPLS, que no es más que un conjunto de Nodos con capacidad de entender etiquetas y que son parte de un mismo dominio de encaminamiento IP, como se muestra en la **Figura 1.6.**

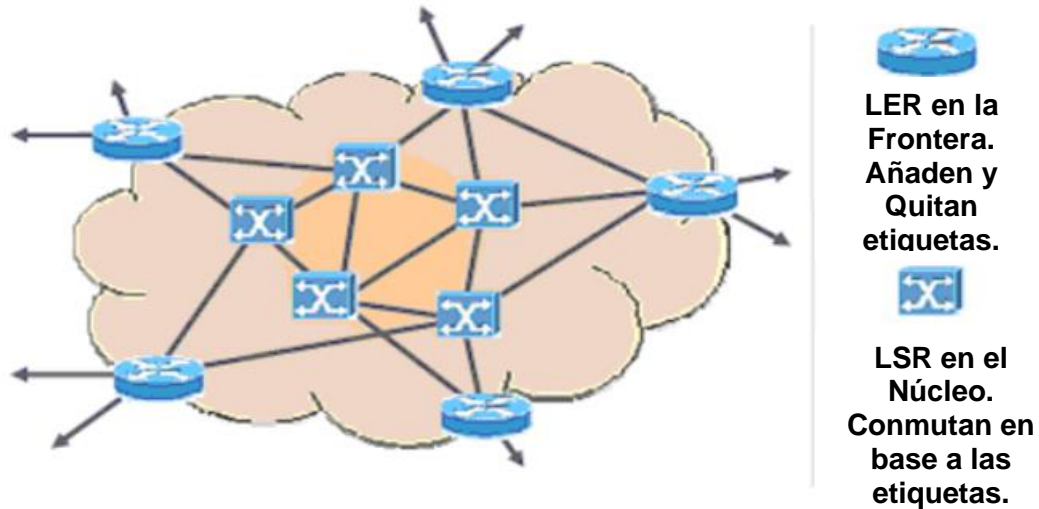


Figura 1.6. Dominio MPLS.
Adaptada de MPLS el Presente de las Redes IP, Tapasco Garcia, 2008.

1.3.1.1. LER - ROUTER DE BORDE DE ETIQUETAS.

De acuerdo a (Tapasco Garcia, 2008),

“Es un dispositivo que opera en el borde de la red de acceso y el dominio MPLS, se encarga de insertar las etiquetas basándose en la información de enrutamiento, así como también de retirar las etiquetas y distribuir el tráfico a las redes de salida. Un LER envía el tráfico a través de la red MPLS después de haber establecido un LSP utilizando un protocolo de distribución de etiquetas” (Pag 44).

Dado que el LER se encuentra en los extremos de un dominio MPLS, comúnmente son llamados LSR de Borde (Edge LSR). Un LER de entrada se conoce como Ingress LSR y un LER de salida como Egress LSR. A continuación, se describen.

- ✚ LER de entrada: reciben un paquete que aún no está etiquetado, insertan una etiqueta delante del paquete y lo envían por un enlace de datos. Estos LSR realizan operaciones PUSH.
- ✚ LER de salida: reciben paquetes etiquetados, eliminan las etiquetas contenidas dentro del paquete y los envían por un enlace de datos. Estos LSR ejecutan operaciones POP.

La **Figura 1.7.** muestra a los LER, que según como sea el flujo del tráfico puede ser de Entrada o de Salida.

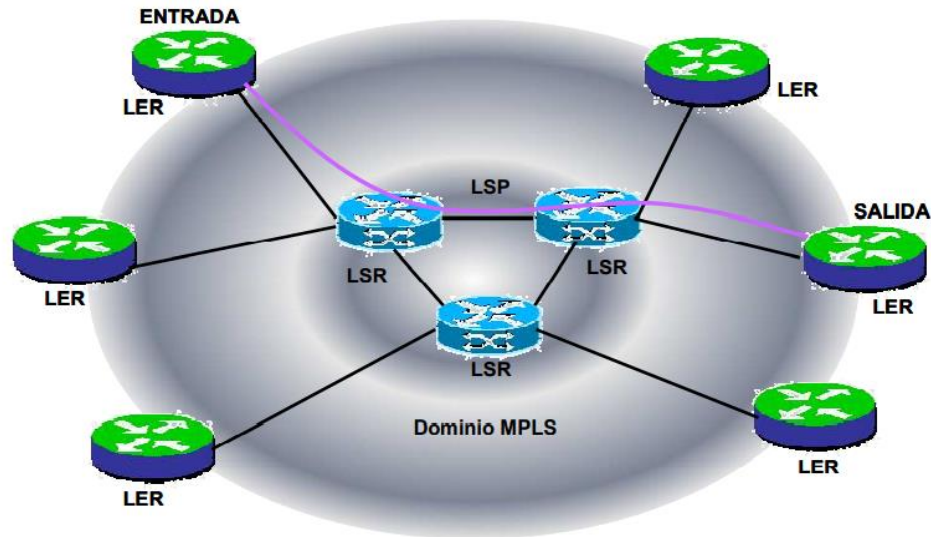


Figura 1.7. Dominio MPLS – LER y LSR.
Reproducida de MPLS el Presente de las Redes IP, Tapasco Garcia, 2008.

1.3.1.2. LSR - ROUTER CONMUTADOR DE ETIQUETAS.

“Un LSR es un enrutador ubicado en el núcleo del dominio MPLS y basa su funcionamiento de envío en el chequeo de la etiqueta que ha sido añadida al paquete IP en la frontera de ingreso al dominio por un LSR Ingreso (LER). No realiza chequeo de capa de red ya que para el envío basta con analizar la etiqueta contenida en el paquete IP etiquetado, la cual le indica el siguiente salto. El LSR remueve la etiqueta y asigna otra para indicar el siguiente salto de la red”.

(Ballesteros, Chiriboga, Villegas, & Moreno, 2007, pág. 2)

De este modo los LSR realizan la conmutación de paquetes a velocidades impresionantes y con gran eficacia debido a que solo leen la etiqueta del encabezado IP y no realizan el proceso de encapsulación y des encapsulación. La diferencia entre estos enrutadores MPLS está en que los LER procesan mucha más información, pues tienen conocimiento tanto de etiquetas como de enrutamiento IP, por lo que son los que realizan el mayor trabajo. Mientras que los LSR se enfocan en el procesamiento de etiquetas dentro del dominio MPLS.

(Morales Dibildox, 2006, pág. 65)

La **Figura 1.8.** muestra la diferencia en como procesan los paquetes los LSR y LER. La principal diferencia está en el plano de datos donde los LSR únicamente manejan información de etiquetas y no de direcciones IP como los LER.



Figura 1.8.
Lógica de trabajo
de LSR y LER.

Adaptada de
Investigación de
Redes VPN con
MPLS, Morales
Dibildox, 2006.

1.3.2. ELEMENTOS LOGICOS MPLS.

Habiendo visto los elementos físicos que constituyen el dominio MPLS, ahora abordaremos los elementos lógicos que permiten el correcto funcionamiento de MPLS dentro de este dominio.

1.3.2.1. FEC - CLASE EQUIVALENTE DE ENVIO.

(Barberá, 2000), describe a la FEC (Forwarding Equivalence Class) como:

“Un Conjunto de paquetes con características similares que pueden reenviarse de la misma manera, es decir, pueden ser enlazado a la misma etiqueta y reenviarse sobre el mismo camino a través de la red, incluso si sus destinos finales son diferentes”.

El término FEC vendría siendo la forma en que un enrutador MPLS (LER Ingreso) clasifique cada paquete entrante por una de sus interfaces. Cada FEC puede representar un requerimiento de servicio para un conjunto de paquetes o para una dirección fija, de este modo se realiza la priorización y segmentación del tráfico.

“En el envío IP, un Router considerará a dos paquetes dentro del mismo FEC si hay algún prefijo de dirección IP en la tabla de Routing el cuál sea la mayor concordancia para la dirección de destino de ambos paquetes. A medida que el paquete sigue circulando por la red, cada Router realiza la misma operación de asignación en un FEC. En MPLS, esta asignación se efectúa solamente cuando el paquete entra en la red. Tras esto, el FEC al que el paquete ha sido asignado se codifica en un valor llamado Etiqueta. Cuando un paquete va a ser enviado al siguiente nodo, se le añade la etiqueta”. (Canalis, 2003, pág. 116)

En la **Figura 1.9.** se observa el proceso de asignación de una FEC a un paquete cuando ingresa a un LER de Borde o Ingress LSR. Esto se realiza una sola vez.

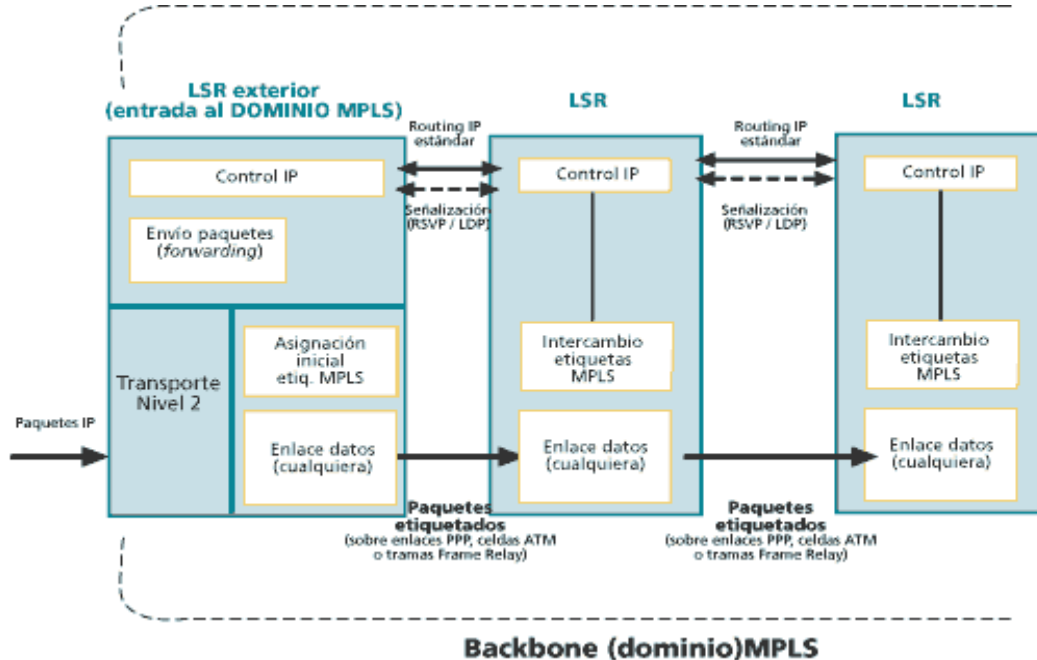


Figura 1.9. Asignación de FEC a un Paquete.
Reproducida de MPLS Una arquitectura para Internet Siglo XXI, Barberá, 2000.

La FEC de los paquetes se puede especificar por varios parámetros, tales como:

- Dirección IP destino o Fuente.
- ID de Protocolo.
- Etiqueta de Flujo IPv6.
- Puerto Destino o Fuente .
- Punto de código de servicios diferenciados.

1.3.2.2. LABEL - ETIQUETA MPLS.

Según (Canalis, 2003), la etiqueta MPLS,

“Es un identificador de valor corto y de tamaño fijo que se emplea para identificar una Clase de Envío Equivalente (FEC). Pues esta establece una correspondencia entre el paquete IP y la FEC asociada. Así mismo, Una etiqueta identifica la trayectoria que un paquete IP etiquetado debe seguir, dentro del dominio MPLS, hasta alcanzar su destino. Dicha etiqueta tiene significado local y es transportado en la cabecera del paquete IP”. (Pag. 104 y 106)

1.3.2.2.1. ENCABEZADO MPLS.

Es el campo que se interpone entre los encabezados de Capa 2 y el encabezado IP (Capa 3). La cabecera MPLS permite que funcione con cualquier tecnología de transporte. La **Figura 1.10.** muestra los campos de la cabecera MPLS, la cual se encuentra en el encabezado de Red y el de Enlace de Datos. .

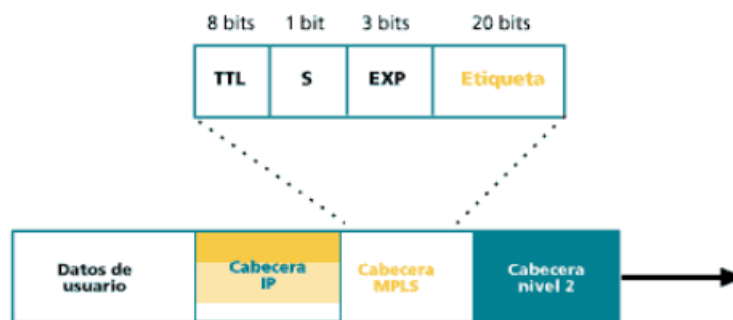


Figura 1.10. Encabezado MPLS.
Reproducida de MPLS - Monografía, Hernandez & Angulo, 2005.

El campo de cabecera MPLS es de 32 bits y se divide de la siguiente manera:

- A. Label:** Es la etiqueta que se le asigna y acompaña a un paquete IP al ingresar al dominio MPLS, este campo consta de 20 bits.
- B. EXP:** Este campo consta de 3 bits, se conoce como CoS (Class of Service) y se usa para identificar la clase de servicio para clasificar el paquete.
- C. S (Bottom of Stack):** Consta de 1 bit y se usa para indicar si existe una pila de etiquetas. 1=Existe Pila de Etiquetas. 0=Si la etiqueta es la única en la pila.

- D. Label Stack (Pila de Etiquetas):** MPLS soporta la colocación de varias etiquetas a un sólo paquete. Estas etiquetas se organizan en una pila de y su principal aplicación es cuando se puede controlar la trayectoria de un paquete sin que sea necesario especificar los enrutadores intermedios. (Tunneling)
- E. TTL (Time To Live):** Consta de 8 bits e indica el número de nodos recorridos por los que el paquete ha pasado hasta llegar hasta su destino. Este valor es tomado del encabezado IP a la entrada del LSP y a la salida de éste mismo. (Tapasco Garcia, 2008, pág. 48)

1.3.2.3. LSP - CAMINO CONMUTADO DE ETIQUETAS.

En relación a esto (Tapasco Garcia, 2008), aporta lo siguiente:

“Se llama así a cada uno de los caminos unidireccionales que un paquete toma para ir desde un LER de entrada a un LER de salida, pasando por uno o varios LSR. Se puede ver como un circuito virtual o túnel de extremo a extremo en el dominio MPLS que siguen todos los paquetes de la misma FEC”. (Pág. 45).

“Los LSP son simplex por naturaleza, se establecen para un sentido del tráfico en cada punto de entrada a la red, para el tráfico dúplex se requieren dos LSP, uno en cada sentido (Silvestre Hernandez, 2008, pág. 3)”.

Recordar que los enrutadores LER se encuentran en el borde del dominio MPLS y conectan con otras Redes, los LSR están en el núcleo MPLS y pueden verse también como enrutadores intermedios. Ver Figura 1.7.

1.3.2.3.1. ESTABLECIMIENTO DE UN LSP.

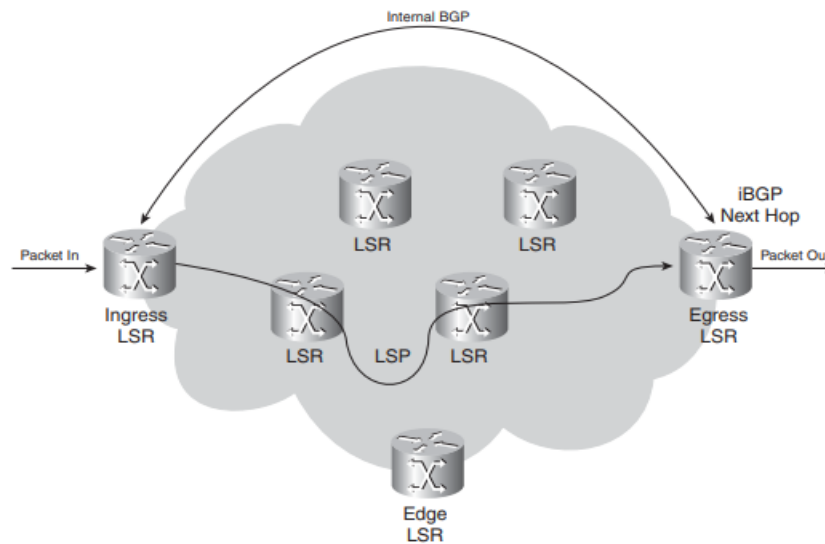
Existen dos mecanismos para establecer un LSP:

- 1) **Encaminamiento salto a salto:** cada LSR selecciona independientemente el próximo salto para un FEC determinado (similar a la lógica utilizada en redes IP). El LSR utiliza cualquier protocolo de enrutamiento como OSPF, iBGP, etc.
- 2) **Encaminamiento explícito:** El LER de entrada determina la secuencia de saltos desde la entrada hasta la salida. Puede que la ruta no esté

completamente especificada, es decir, puede haber un conjunto de nodos representados como un único salto en la ruta. También puede contener un identificador de AS que permita que el LSP sea encaminado a través de un área de la red que está fuera del control administrativo de quien inició el LSP.

Dentro de ambos casos se hará un encaminamiento salto a salto, se establecerán LSP primarios y de respaldo. El establecimiento de estos LSP se realiza usando algoritmos de encaminamiento con QoS que buscan la ruta óptima, tanto desde el punto de vista de la calidad de servicio requerida como desde el punto de vista del uso de los recursos de la red. (Silvestre Hernandez, 2008, pág. 8)

En la **Figura 1.11**, se ve el establecimiento de un LSP, los LSP creados en la red se adaptan al uso real que se esté haciendo de ellos.



**Figura 1.11. Establecimiento de un LSP.
Reproducida de MPLS Fundamentals, Ghein, 2007.**

1.3.2.4. LDP - PROTOCOLO DE DISTRIBUCION DE ETIQUETAS.

Antes se mencionó que la base de MPLS está en que los paquetes son etiquetados y cada enrutador (LER/LSR) debe realizar un intercambio de etiquetas para reenviar el paquete a su destino. Esto significa que la información de las etiquetas debe ser compartida entre enrutadores. De aquí surge LDP, creado por la IETF para establecer el proceso de distribución de etiquetas (RFC 5036).

Según (De Ghein, 2007) LDP,

“Es el conjunto de procedimientos y mensajes mediante los cuales un Router MPLS crea un camino virtual LSP a lo largo de la red, mapeando la información de envío en sus tablas de envío (LIB, LFIB y FIB) y asociando una FEC con cada LSP creado. Los FEC asociados con cierto camino, especifican que paquetes IP van a ir por ese camino”. (Pág. 68)

El protocolo LDP no es el único de los protocolos de distribución de etiquetas, pero es el recomendado por la IETF ya que se ejecuta sobre TCP, lo cual significa que éste asegura la fiabilidad en el envío de mensajes. Entre los otros protocolos están RSVP (usado en Ingeniería de Tráfico), CR-LDP, MP-BGP (aplicado a VPN L3).

1.3.2.4.1. PARES LDP.

Dos LSR que emplean el protocolo LDP para intercambiar información de asociación Etiqueta - FEC son llamados pares LDP, manteniéndose entre ellos una sesión LDP. Esta sesión LDP permite a cada par aprender la información de etiquetas del otro. El protocolo es bidireccional. (Canalis, 2003, pág. 134)

1.3.2.4.2. INTERCAMBIO DE MENSAJES LDP.

Existen cuatro categorías de mensajes:

- ✚ **Mensajes de Descubrimiento:** empleados para anunciar y mantener la presencia de un LSR en la red.
- ✚ **Mensajes de Sesión:** empleados para establecer, mantener y analizar las sesiones entre los pares.
- ✚ **Mensajes de Notificación:** empleados para dar información de aviso o error.
- ✚ **Mensajes de Anuncio:** empleados para crear, cambiar y borrar asociaciones de etiquetas con FEC. (Canalis, 2003, pág. 134)

Los mensajes de descubrimiento anuncian la presencia de un LSR en la red, estos se realizan enviando mensajes Hello periódicamente. Éste es transmitido como un

paquete UDP por el puerto LDP en la dirección Multicast de la Subred del Router. Cuando un LSR desea establecer una sesión con otro LSR, aprendido gracias al mensaje Hello, empleará el procedimiento de inicialización LDP sobre TCP.

Luego de esto los dos LSR son pares LDP y pueden intercambiar mensajes de anuncio. Un LSR pide una etiqueta a su vecino cuando la necesita y la anuncia cuando desea que éste la utilice, ya que es una decisión local de cada LSR. El funcionamiento correcto del protocolo LDP requiere una recepción fiable y ordenada de mensajes. Para ello, se emplea el protocolo TCP para mensajes de sesión, de anuncio y de notificación. Es decir, para todo el proceso, excepto para los mensajes de descubrimiento, que viajan sobre UDP. (Canalis, 2003, pág. 135)

La **Figura 1.12** nos muestra el intercambio de etiquetas MPLS por medio de LDP.

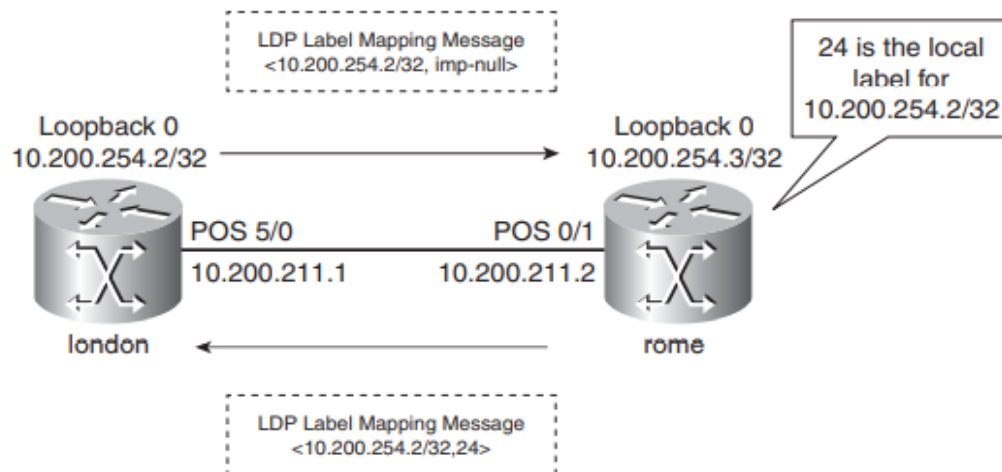


Figura 1.12. Intercambio de Etiquetas por LDP.
Reproducida de MPLS - Fundamentals, Ghein, 2007.

1.4. FUNCIONAMIENTO DE MPLS.

“La tecnología MPLS se despliega en el núcleo de la red del proveedor de servicios, lo que le proporciona a éste un mayor control sobre la calidad del servicio (QoS), la ingeniería de tráfico y la utilización del ancho de banda, y a la vez reduce los requisitos a los equipos de comunicación de los clientes que se conectan a un servicio sobre MPLS. A demás una red MPLS puede transportar múltiples protocolos distintos y de forma simultánea”. (Friedl, 2005)

El modo de funcionamiento de MPLS es similar al de redes de capa 2 (ATM o Frame Relay), con la diferencia que MPLS lo que hace es asignar etiquetas a los paquetes que viajan a través de la red, y esta etiqueta tiene la tarea de informar a cada nodo la forma de procesar y transportar los datos. A continuación, se abordan características y componentes del funcionamiento de la arquitectura de red MPLS.

1.4.1. ROUTING EN LOS BORDES Y SWITCHING EN EL NUCLEO.

La estructura general de un dominio MPLS se basa en el concepto de que los LER del borde del dominio son los que realizan el enrutamiento de paquetes con funciones de decisión del encaminamiento que pueden llegar a ser complicadas y que pueden estar basadas en la interfaz por la que viene el paquete, la red a la que pertenece, los valores de la cabecera de red, etc.

Independientemente de las decisiones de los LER antes de asignar una etiqueta MPLS al paquete, los LRS del núcleo MPLS hacen Switching de los paquetes que han ingresado en el dominio de forma veloz y eficaz sin tener en cuenta nada más que la etiqueta de la cabecera MPLS que los LER han puesto. Por tanto, los paquetes son enrutados en nodos frontera del dominio MPLS y son conmutados rápidamente en los nodos interiores. (Morales Dibildox, 2006, pág. 64)

En la **Figura 1.13.** Podemos observar cómo se da el Routing en los Bordes por los equipos LER y el Switching en el núcleo de la red por los equipos LSR.

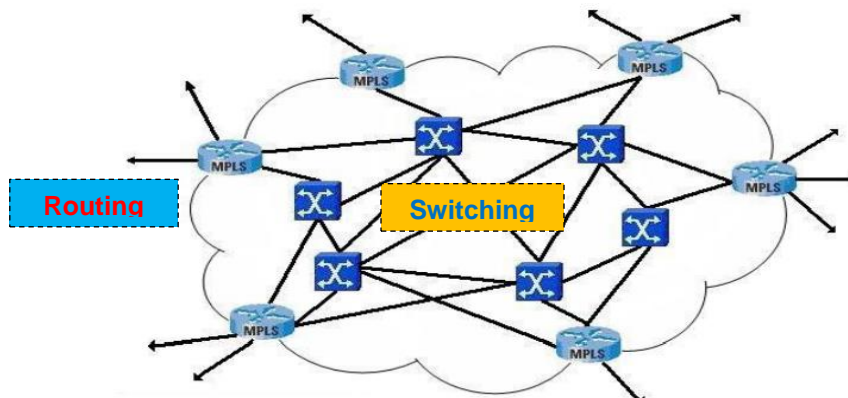


Figura 1.13. Routing en los Bordes y Switching en el Núcleo.
Adaptada de Investigación de Redes VPN con MPLS, Morales Dibildox, 2006.

1.4.2. COMPONENTES FUNCIONALES DE MPLS.

La arquitectura MPLS divide en dos componentes la lógica de operación de cada nodo: El componente de Envío, llamado Plano de Datos y el componente de control, llamado Plano de Control. La idea de separar estos dos componentes es que cada uno se puede implementar y modificar independientemente teniendo en cuenta que la comunicación entre los componentes exista, esto mediante el envío de paquetes y la actualización de información. **(Tapasco Garcia, 2008, pág. 48)**

1.4.2.1. COMPONENTE DE CONTROL.

El componente de Control es el que se encarga de crear y mantener la información de etiquetas asignadas entre los nodos MPLS interconectados realizando un intercambio de información con los enrutadores para la construcción y mantenimiento de las tablas de envío de etiquetas. Para esto se utiliza la información en las tablas de los protocolos de enrutamiento IP (OSPF, BGP o rutas estáticas), Este plano incluye la tabla LIB. Este componente es responsable de configurar los LSP mediante el uso del protocolo de intercambio de etiquetas LDP y de mantener actualizado el sistema cuando existe algún cambio en la topología de la red. **(Tapasco Garcia, 2008, pág. 49)**

1.4.2.2. COMPONENTE DE ENVIO.

El componente de envío es el encargado del transporte de paquetes entre los nodos MPLS. Cuando un paquete llega al componente de envío, éste se encarga de examinar la información que contiene dicho paquete, busca en sus tablas de envío la entrada correspondiente y dirige el paquete desde la interfaz de entrada a la de salida. En el plano de envío se manejan dos tipos de bases de datos de etiquetas para tomar la decisión de encaminamiento: LFIB (Label Forwarding Information Base) y FIB (Forwarding Information Base). La primera se utiliza para el transporte de paquetes que contiene etiquetas y la segunda para transportar paquetes desde o hacia dispositivos que no manejan etiquetas. **(Barberá, 2000)**

En la **Figura 1.14.** se ve el diagrama interno de equipos MPLS operando con estos dos componentes y sus tablas correspondiente de etiquetas.

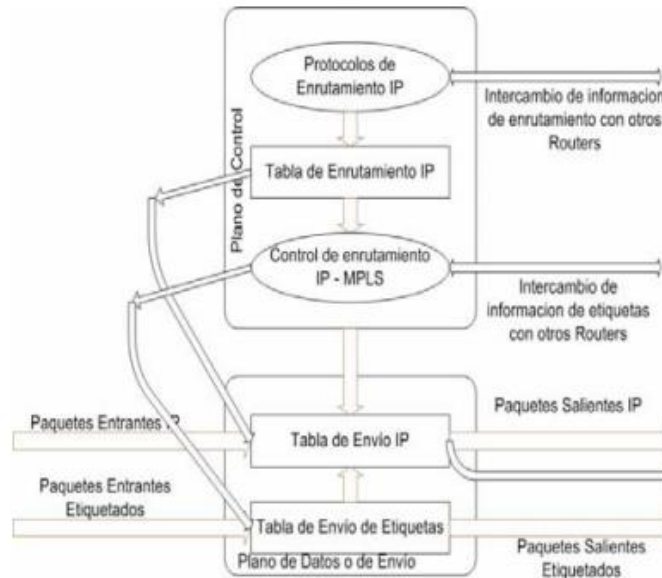


Figura 1.14. Componentes de Control y Envío MPLS.
Reproducida de **Diseño e Implementación de una Red MPLS, Ballesteros, 2007.**

1.4.2.3. OPERACIONES DE AMBOS COMPONENTES.

Una vez que un Nodo MPLS tiene la tabla FIB completa por el protocolo de ruteo dinámico en uso, a cada destino que aparece en dicha tabla, le asocia una etiqueta y la anuncia a sus vecinos utilizando LDP. Dicha asociación queda registrada en la tabla LIB del plano de control. En el plano de envío se mantienen las tablas FIB para enrutar los paquetes de red directamente y la tabla LFIB para conmutar las tramas MPLS utilizando las etiquetas y reenviar la trama a la interfaz de salida correspondiente. (Ballesteros, Chiriboga, Villegas, & Moreno, 2007, pág. 5)

1.4.3. FUNCIONAMIENTO GLOBAL.

Una vez vistos los componentes físicos, lógicos y funcionales, el esquema global de funcionamiento MPLS es el que se muestra en la **Figura 1.15.** donde quedan reflejadas las funciones en cada uno de los elementos que integran la red MPLS. Lo primero que se hace es la creación de caminos LSP mediante el protocolo LDP que utiliza las tablas de etiquetas de los planos de control y envío.

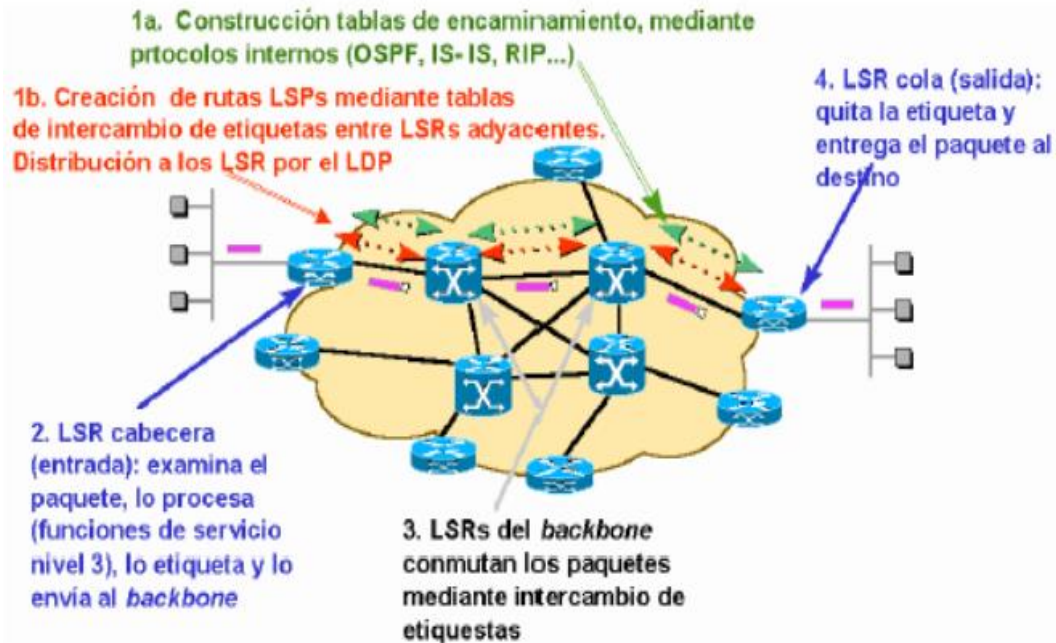


Figura 1.15. Funcionamiento Global MPLS.
Reproducida de MPLS el Presente de las Redes IP, Tapasco Garcia, 2008.

Es importante destacar que en el borde de la nube MPLS tenemos una red convencional de Router IP (LER Ingreso y LER Egreso), el núcleo MPLS (LSR) proporciona una arquitectura de transporte que hace aparecer a cada par de Router (LER Ingreso – LER Egreso) a una distancia de un solo salto. Funcionalmente es como si estuvieran unidos todos en una topología mallada, ahora esa unión a un solo salto se realiza mediante la creación de caminos virtuales LSP establecidos por medio del protocolo de intercambio de etiquetas LDP utilizando la información en las tablas de envío a lo largo del dominio MPLS.

1.4.3.1. MPLS EN ACCION.

A. Cuando un paquete ingresa a una red MPLS a través de un Router de borde (LER de Ingreso), al ingresar el paquete se le asigna un determinado FEC (que puede representar un requerimiento de servicio). A este FEC se le asigna una Etiqueta (se usa como un índice en la tabla que especifica el próximo salto y una nueva etiqueta) y se guarda en la tabla LIB (asociaciones FEC-Etiqueta-interfaz entrada/salida).

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

Luego el LER de ingreso Identifica en la tabla LFIB (Información de envío de etiquetas) el próximo salto correspondiente a la etiqueta asignada. Agrega un encabezado MPLS al paquete con dicha etiqueta y lo envía al siguiente salto dentro del dominio MPLS. **(Tapasco Garcia, 2008, pág. 59)**

B. Una vez adentro de la red MPLS los paquetes van cambiando sus etiquetas al pasar por los diferentes LSR (Nodos intermedios), cada LSR realiza un Label Swap (Remueve y asigna una nueva etiqueta) y decrementa el TTL. Durante estas operaciones el contenido del paquete por debajo de la etiqueta MPLS no es examinado, de hecho, los Router LSR no necesitan examinar la información del encabezado IP. Pues el paquete es enviado basándose en el contenido de su etiqueta, lo cual permite «rutado independiente del protocolo». **(Cruz, Alincaastro, Magnago, & Hernandez, 2013)**

C. Al finalizar el camino el Router de borde (en este caso LER de Egreso) se encarga de quitar la etiqueta MPLS y consultar la tabla FIB (información de rutas IP) reenviando el paquete como IP nativo. El LER de Egreso puede recibir el paquete con etiqueta MPLS o sin ella.

En ciertos casos, es posible que la última etiqueta sea retirada en el penúltimo salto (LSR anterior al LER de Egreso); este procedimiento es llamado «remoción en el penúltimo salto» (PHP). Esto es útil cuando la red MPLS transporta mucho tráfico. En estas condiciones los penúltimos nodos auxiliarán al último en el procesamiento de la última etiqueta de manera que éste no se vea forzado al cumplir con sus tareas de procesamiento. **(Cruz, Alincaastro, Magnago, & Hernandez, 2013)**

En la **Tabla 1.2.** se puede resumir todo lo abordado anteriormente.

Tabla 1.2. MPLS en Acción.
Fuente Propia con datos de Análisis de la Implementación de MPLS en Redes,
Cruz & Alincaastro & Magnago & Hernandez, 2013.

NODO	PASO DE UN PAQUETE POR LA RED MPLS
------	------------------------------------

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

LER Ingreso	Asigna una FEC al paquete recibido. Lo asocia con una etiqueta y guarda la información en la tabla LIB. Crea el camino virtual LSP del paquete en función a la asociación FEC-Etiqueta utilizando LDP. Agrega al paquete IP el encabezado MPLS y lo reenvía al siguiente salto mediante la información en la tabla LFIB.
LSR Intermedio	Examina el encabezado MPLS en busca de etiquetas. No tiene conocimiento IP. Se enfoca en el Switching y no en el Routing. Remueve la Etiqueta y asigna una nueva. Realiza operación SWAP. Reenvía el paquete según la información de la etiqueta contenida en la tabla LFIB.
LER Egreso	Remueve la etiqueta y examina el contenido del paquete IP. Aplica una operación POP. Consulta la Tabla de envío FIB. Para identificar siguiente salto. Reenvía el paquete como IP nativo a una red fuera del dominio MPLS.

1.5. BENEFICIOS DE IMPLEMENTAR MPLS.

Los beneficios que ofrece MPLS al utilizarla como tecnología de transporte de datos son muchos, pero entre los relevantes se tienen: Soporte de Calidad sobre Servicio (QoS), Ingeniería de tráfico, Soporte para Redes Privadas Virtuales (VPN) y Soporte Multiprotocolo lo que permite el uso de una infraestructura de red Unificada. **(De Ghein, 2007, pág. 6)**

1.5.1. SOPORTE DE QoS.

QoS trabaja a lo largo de la red y se encarga de asignar recursos a las aplicaciones que lo requieran, dichos recursos se refieren principalmente al ancho de banda BW. Para asignar estos recursos QoS se basa en prioridades, algunas aplicaciones podrán tener más prioridades que otras, sin embargo, se garantiza que todas las aplicaciones tendrán los recursos necesarios para completar sus transacciones en un periodo de tiempo aceptable.

QoS permite a los administradores de redes el uso eficiente de los recursos de sus redes con la ventaja de garantizar que se asignaran más recursos a aplicaciones que así lo necesiten, sin arriesgar el desempeño de las demás

aplicaciones. En otras palabras, el uso de QoS le da al administrador un mayor control de la red, lo que significa menores costos y mayor satisfacción del cliente.

(Morales Dibildox, 2006, pág. 7)

1.5.1.1. IMPORTANCIA DE QoS.

En los últimos años el tráfico de redes ha aumentado considerablemente, la necesidad de transmitir cada vez más información en menos tiempo, como video y audio en tiempo real (streaming). La solución no es solo aumentar el ancho de banda (BW) cada vez más, ya que en la mayoría de los casos esto no es posible y además es limitado. Es aquí donde la administración efectiva de recursos que provee QoS entra a relucir.

En resumen, QoS otorga mayor control a los administradores sobre sus redes, mejora la interacción del usuario con el sistema y reduce costos al asignar recursos con mayor eficiencia. Mejora el control sobre la latencia para asegurar la capacidad de transmisión de voz sin interrupciones y por último disminuye el porcentaje de paquetes desechados por los enrutadores, brindando confiabilidad.

(Morales Dibildox, 2006, pág. 7)

1.5.2. INGENIERÍA DE TRÁFICO.

MPLS facilita la asignación de recursos en las redes para balancear la carga y proporciona diferentes niveles de soporte dependiendo de las demandas de tráfico de los usuarios. El protocolo IP provee una forma primitiva de Ingeniería de Tráfico al igual que *OSPF*, que permite a los enrutadores cambiar la ruta de los paquetes cuando sea necesario para balancear la carga. Sin embargo, esto no es suficiente ya que puede llevar a congestionar la red y no soporta QoS. **(Canalis, 2003, pág. 140)**

Todo tráfico entre dos puntos finales sigue la misma ruta y puede ser cambiada si ocurriera congestión, pero este cambio solo ocurre solo cuando hay congestión que es algo que siempre se trata de evitar. En MPLS a diferencia de OSPF no se ve paquete por paquete sino flujos de paquetes con su respectivo QoS. Con este

protocolo es posible predecir rutas en base a flujos individuales, pudiendo haber diferentes flujos entre canales similares, pero dirigiéndose a diferentes enrutadores. (Morales Dibildox, 2006, pág. 8)

La **Figura 1.16.** muestra las rutas seleccionadas por un protocolo IGP tradicional en comparación con la ruta optima con ingeniería de tráfico en MPLS. Si llegase a darse congestión en la red, las rutas MPLS pueden ser Re enrutadas inteligentemente, de esta manera se pueden cambiar las rutas de flujo de paquetes dinámicamente conforme a las demandas de tráfico de cada flujo.

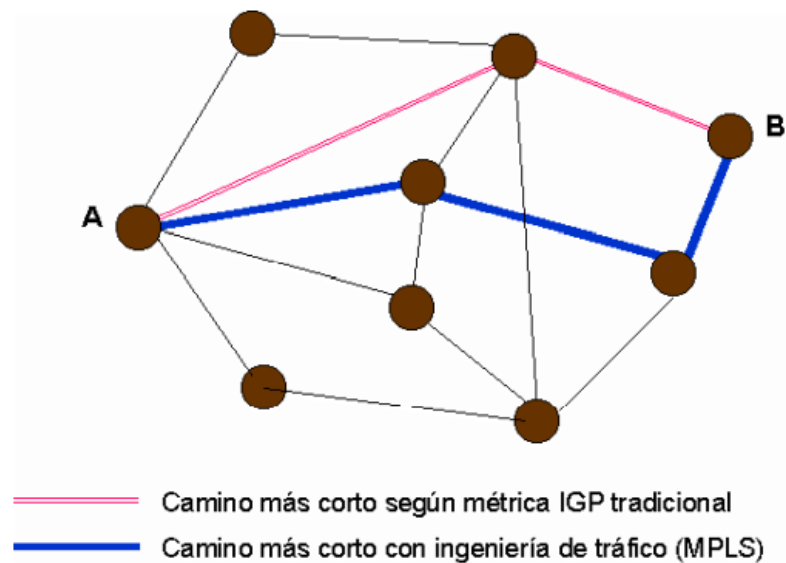


Figura 1.16. Ingeniería de tráfico MPLS.
Reproducida de MPLS una Arquitectura de Red para el Siglo XXI, Canalís, 2003.

1.5.2.1. BENEFICIOS DE LA INGENIERÍA DE TRAFICO.








MPLS permite manejar el tráfico a nuestra conveniencia, de esta manera el flujo de paquetes viaja a través de un túnel de datos en el Backbone creado por el Protocolo de Reserva de Recursos (*RSVP*), la ruta de dicho túnel está dada por los requisitos de recursos del túnel y de la red. El Protocolo de Enrutamiento Interno (*IGP*) rutea el tráfico a dichos túneles. Con un buen manejo del tráfico en las redes se pueden evitar congestionamientos, mejorar el desempeño general y reducir la latencia y el desechado de paquetes. En pocas palabras se maximiza la capacidad de la red y se minimizan los costos. (Barberá, 2000)

La ingeniería de tráfico es esencial para el Backbone de los proveedores de servicios ya que deben soportar un uso elevado de su capacidad de transmisión. Utilizando MPLS las capacidades de ingeniería de tráfico son integradas a la Capa 3, lo que optimiza el ruteo de tráfico IP y las capacidades del Backbone. La ingeniería de tráfico MPLS rutea el flujo de tráfico a lo largo de la red basándose en los recursos que dicho flujo requiere y en los recursos disponibles en toda la red. MPLS emplea la ruta más corta que cumpla con los requisitos del flujo de tráfico, que incluye: requisitos de ancho de banda, de medios y de prioridades sobre otros flujos. **(Canalis, 2003, pág. 142)**

1.5.3. SOPORTE DE REDES PRIVADAS VIRTUALES (VPN)

MPLS provee un mecanismo eficiente para el manejo de redes privadas virtuales. De esta manera el tráfico de una red privada “atraviesa” la Internet eficazmente y de manera transparente para el usuario, eliminando cualquier tráfico externo y protegiendo la información. Las VPN creadas sobre una red MPLS tienen una mayor capacidad de escalabilidad y son más flexibles. MPLS se encarga de reenviar tráfico de la VPN a través de túneles privados utilizando etiquetas que actúan como códigos postales. Dicha etiqueta tiene un identificador que aísla a esa VPN de redes externas. **(Morales Dibildox, 2006, pág. 11)**

Las Ventajas Principales de Implementar VPN en MPLS son:

-  Maximizar la capacidad de ampliación.
-  Actualización transparente para el usuario.
-  Utilización óptima de los recursos de la red.
-  Diferenciación entre servicios.
-  Reducción de costos mediante consolidación de servicios.
-  Seguridad y rapidez de transmisión de información.
-  Uso de tecnología de vanguardia.

1.5.4. USO DE UNA INFRAESTRUCTURA DE RED UNIFICADA.

Con MPLS, la idea es etiquetar los paquetes de ingreso en función de su dirección de destino u otros criterios preconfigurados y conmutar todo el tráfico a través de una infraestructura común. Una de las razones por las que IP se convirtió en el único protocolo que dominó el mundo de las redes es que muchas tecnologías se pueden transportar a través de él. No solo se transportan datos sobre IP, sino también telefonía, Video, etc.

Al usar MPLS con IP, puedes ampliar las posibilidades de lo que puedes transportar. Agregar etiquetas al paquete le permite transportar otros protocolos además de IP a través de una red troncal de IP de capa 3 habilitada para MPLS, de manera similar a lo que anteriormente solo era posible con redes Frame Relay o ATM de capa 2. MPLS puede transportar IPv4, IPv6, Ethernet, control de enlace de datos de alto nivel (HDLC), PPP y otras tecnologías de capa 2. (De Ghein, 2007)

La función mediante la cual cualquier trama de capa 2 se transporta a través de la red troncal MPLS se denomina AnyTransport over MPLS (AToM). Los enrutadores que están cambiando el tráfico AToM no necesitan estar al tanto de la carga útil de MPLS; solo necesitan poder cambiar el tráfico etiquetado mirando la etiqueta que se encuentra encima. En esencia, la conmutación de etiquetas MPLS es un método simple de conmutación de múltiples protocolos en una red.

En resumen, AToM permite que el proveedor de servicios brinde el mismo servicio de capa 2 a los clientes que con cualquier red específica que no sea MPLS. Al mismo tiempo, el proveedor de servicios solo necesita una infraestructura de red unificada para transportar todo tipo de tráfico de cliente. (De Ghein, 2007, pág. 7)

COMENTARIOS FINALES

CAPITULO I.

En resumen, MPLS es hoy día ampliamente utilizada en diferentes aplicaciones, como los servicios MPLS VPN. Se le puede considerar como una autopista por la cual pueden circular diferentes "vehículos" o diferentes soluciones de manera eficaz.

Su impacto es tal que los ISP han migrado su Backbone, de arquitecturas de red como ATM a MPLS, para gozar de los múltiples beneficios que esta brinda, tanto para los ISP como para los usuarios finales.

En el próximo capítulo se hablará de una de las implementaciones de MPLS más utilizadas hoy en día y la más llevada a cabo por los ISP, como lo son los servicios de VPN sobre MPLS.

CAPITULO II: TECNOLOGIA MPLS VPN.

En este capítulo, como primer punto, se habla de manera general de las VPN, los tipos, características y beneficios de utilizar redes VPN. Luego se describen las tecnologías para proveer servicios de redes virtuales y se realiza una comparación de las VPN más utilizadas en la actualidad.

Al final se aborda a profundidad la tecnología MPLS VPN. Se mencionan las topologías, terminología, elementos y características de las VPN sobre MPLS, en específico de una MPLS L3 VPN. En el capítulo III se realiza el diseño de una red VPN de capa 3 sobre MPLS para brindar conectividad a sitios geográficamente separados.

2.1. INTRODUCCION A LAS MPLS VPN.

MPLS VPN, o MPLS Virtual Private Networks, es la implementación más popular y extendida de la tecnología MPLS. Su popularidad ha crecido exponencialmente desde que se inventó, y sigue creciendo de manera constante. Aunque la mayoría de los proveedores de servicios la han implementado como un reemplazo para los servicios Frame Relay y ATM que eran populares antes, MPLS VPN tiene ahora un interés creciente por parte de las grandes empresas que lo ven como un paso necesario en el diseño de su red.

MPLS VPN puede proporcionar escalabilidad y dividir toda la red en redes más pequeñas separadas, lo que a menudo es necesario en las redes empresariales más grandes, donde la infraestructura de TI común tiene que ofrecer redes aisladas a departamentos individuales. **(De Ghein, 2007, pág. 173)**

Debido a la demanda de empresas y organizaciones de permitir que sus sitios remotos y los usuarios finales se conecten a la red central empresarial, los ISP están utilizando la tecnología MPLS (ya que las VPN MPLS pueden operar en redes MPLS como en redes IP puras) para brindar a las empresas un canal seguro a través de la Internet pública, con flexibilidad y escalabilidad y de esta forma satisfacer sus necesidades de comunicación.

MPLS VPN utiliza el poder de la conmutación de etiquetas multiprotocolo para crear redes privadas virtuales o VPN's. Las redes privadas virtuales de capa 3 basadas en MPLS permiten conectar de forma segura diversos, sitios separados geográficamente, a través de una red MPLS. Los servicios MPLS se pueden usar para conectar varios sitios a una red troncal y garantizar un mejor rendimiento para aplicaciones de baja latencia, como voz sobre IP (VoIP) y otras funciones críticas para el negocio. **(Ravi, Dhanumjayulu , Bagubali , & Bagadi , 2017, pág. 1)**

Antes de entrar de lleno con MPLS VPN, se abordará lo referente a las VPN's, así como las tecnologías que proveen servicios de VPN sobre una infraestructura red.

2.2. VIRTUAL PRIVATE NETWORK - VPN.

2.2.1. SOBRE LAS VPN's.

El mundo ha cambiado mucho en las últimas décadas. En lugar de simplemente abordar problemas locales o regionales, las empresas ahora deben tener en cuenta logística y mercados globales. Muchas empresas cuentan con instalaciones en todo el país, incluso en todo el mundo. Esto genera la necesidad de establecer una comunicación con dichas instalaciones que se encuentran separadas geográficamente una de las otras. Y no solo eso, pues las empresas requieren que este tipo de comunicación debe ser rápida, segura y fiable. **(Sclayton, 2008)**

Para establecer esta comunicación, entre redes que no tienen una conexión física entre sí pero que tienen como red común la Internet, las empresas implementan VPN y así transmiten datos entre ellas como si estuvieran físicamente conectadas. La implementación de una VPN permite la transferencia de datos de manera segura utilizando un mecanismo de cifrado de datos que garantice la confidencialidad de la información, así mismo las políticas de seguridad del sistema impedirán que personas no autorizadas tengan acceso a la VPN.

Con una VPN no requieres adquirir canales dedicados excesivamente costosos, por lo que ofrecen la mejor relación costo / beneficio. Los posibles escenarios de red privada virtual basados en la configuración habitual de un servidor VPN son:

- ✚ Acceso remoto de VPN para empleados.
- ✚ Acceso de sucursales a petición.
- ✚ Acceso persistente de las sucursales.
- ✚ Extranet para socios comerciales.
- ✚ VPN y conexión telefónica con autenticación RADIUS. **(Silvestre Hernandez, 2008, pág. 19)**

2.2.2. QUE ES UNA VPN.

Según (De Ghein, 2007) una VPN,

“Es una red que emula una red privada sobre una infraestructura común. La VPN puede proporcionar comunicación en la capa 2 o 3 del modelo OSI. La VPN generalmente pertenece a una empresa y tiene varios sitios interconectados a través de la infraestructura común del proveedor de servicios. La red privada requiere que todos los sitios de los clientes puedan interconectarse y estén completamente separados de otras VPN.” (Pág. 173)

Por otro lado, (Sclayton, 2008) dice que:

“Una VPN es una red privada que utiliza una red pública (Internet) para conectar sitios o usuarios remotos entre sí. En vez de utilizar una conexión real dedicada como línea arrendada, una VPN utiliza conexiones "virtuales" enrutadas a través de Internet desde la red privada de la empresa hacia el empleado o el sitio remoto”.

Entonces, se puede considerar a las VPN (Redes Privadas Virtuales) como redes lógicas que interconectan redes físicas (LAN) por medio de la infraestructura de red del ISP y que proporcionan características específicas. La **Figura 2.1.** muestra como luce la conexión de una VPN entre una empresa y sus sitios remotos.

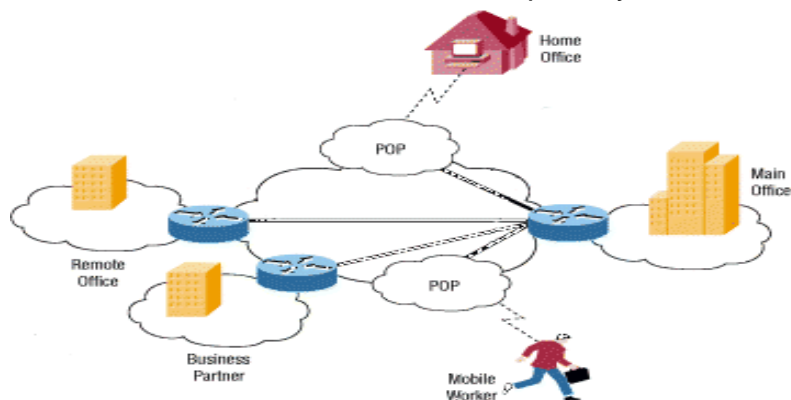


Figura 2.2. Diagrama de una VPN Empresarial.
Reproducida de Como Funcionan las VPN, Sclayton, 2008.

2.3. TIPOS DE VPN´s.

De manera general hay dos tipos de VPN comunes.

2.3.1. VPN DE ACCESO REMOTO.

También denominada Red Telefónica Privada Virtual (VPDN), se trata de una conexión de usuario a LAN utilizada por una empresa que posee empleados que necesitan conectarse a la red privada desde distintas ubicaciones remotas. Normalmente, una empresa que desea configurar una VPN de acceso remoto proporciona algún tipo de cuenta telefónica de Internet a sus usuarios mediante un ISP. Luego, los teletrabajadores pueden marcar un número para conectarse a Internet y usar su software de cliente VPN para acceder a la red corporativa, tal como se observa en la ***Figura 2.2.*** (Sclayton, 2008)

Un buen ejemplo de una empresa que necesita una VPN de acceso remoto sería una firma grande con cientos de miembros del personal de ventas en el campo. Las VPN de acceso remoto permiten conexiones seguras y cifradas entre la red privada de una empresa y los usuarios remotos a través de un SP de terceros.

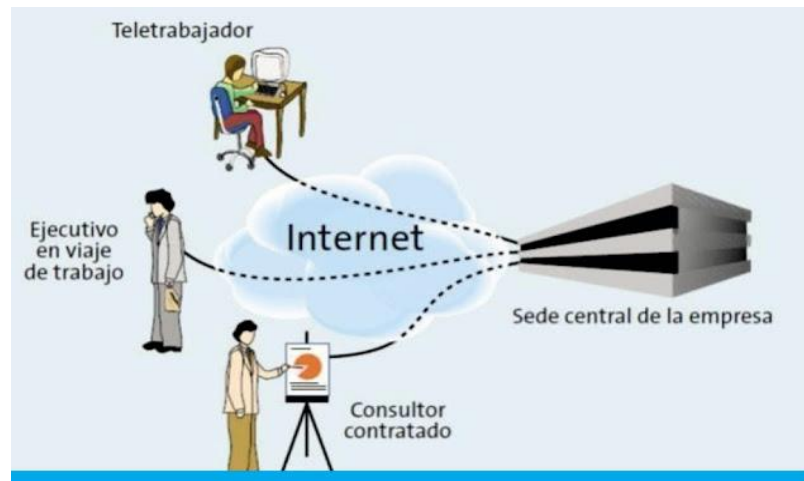


Figura 2.2. VPN de Acceso Remoto.
Reproducida de Diferencias entre VPN, Aragon, syscomblog.com, 2021.

2.3.2. VPN SITIO A SITIO.

Mediante el uso de equipos exclusivos y cifrado a gran escala, una empresa puede conectar varios sitios remotos (sucursales) a través de una red pública como Internet. Cada sitio solo necesita una conexión local a la misma red pública, lo cual ahorra dinero en extensas líneas arrendadas privadas. Las VPN de sitio a sitio

también se pueden clasificar en intranet o extranet. Una VPN de sitio a sitio desarrollada entre oficinas de la misma empresa se denomina VPN intranet, mientras que una VPN desarrollada para conectar la empresa con su socio o cliente se denomina VPN extranet. (Sclayton, 2008)

La **figura 2.3.** muestra un ejemplo de una VPN sitio a sitio, donde sucursales de un banco se comunican con su centro de datos a través del uso de una VPN.

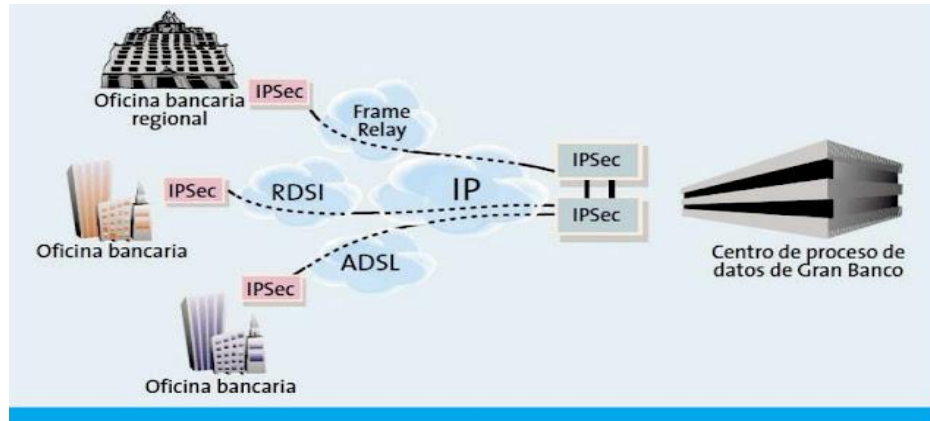


Figura 2.3. VPN Sitio a Sitio utilizando IPSec.
Reproducida de Diferencias entre VPN, Aragon, syscomblog.com, 2021.

En resumen:

VPN Site-to-Site: Sirve para conectar redes LAN completas entre sí, el Router servidor conectara a todos los clientes que están conectados a él, con todos los equipos que están conectados al Router cliente.

VPN Acceso Remoto: Sirve para conectar a un usuario en particular con la red principal del Router servidor.

2.3.3. CARACTERÍSTICAS DE LAS VPN's.

El objetivo de las VPN's es el soporte de aplicaciones intra/extranet, donde se integran aplicaciones multimedia de voz, datos y video sobre infraestructuras de comunicaciones eficientes y rentables. Estas redes se caracterizan por su privacidad (el usuario asume que los enlaces son suyos) y seguridad (los datos no son accesibles a externos), las VPN's son soluciones de comunicación basada en el protocolo de red IP de la Internet. (Tapasco Garcia, 2008, pág. 17)

Una VPN bien diseñada utiliza varios métodos para conservar sus datos y la conexión seguros. A continuación se describen:

2.3.3.1. CONFIDENCIALIDAD DE DATOS.

Este es quizás el servicio más importante de cualquier implementación de VPN. Dado que los datos privados viajan a través de una red pública, la confidencialidad de estos es fundamental y puede lograrse mediante el cifrado de datos. Este es el proceso de tomar los datos que se está enviando y cifrarlos en un formato que solo el destino pueda descifrar. (Sclayton, 2008)

La mayoría de las VPN utiliza uno de estos protocolos para proporcionar cifrado. **IPsec:** el Protocolo de seguridad de IP proporciona funciones de seguridad mejorada como algoritmos de cifrado más potentes y autenticación integral. IPsec tiene dos modos de cifrado: túnel y transporte. El modo de túnel cifra el encabezado y la carga de cada paquete mientras el modo de transporte solo cifra la carga. Los dispositivos deben utilizar una clave o certificado común y deben implementar políticas de seguridad similares. (Morales Dibildox, 2006, pág. 22)

Para los usuarios de VPN de acceso remoto, algún tipo de paquete de software de terceros proporciona la conexión y el cifrado en las PC's de los usuarios. IPsec admite cifrado de 56 bits (DES) o de 168 bits (triple DES). La **Figura 2.4.** nos muestra el mecanismo de cifrado de datos en un túnel IP utilizando el protocolo IPsec, donde vemos los dos modos de funcionamiento.

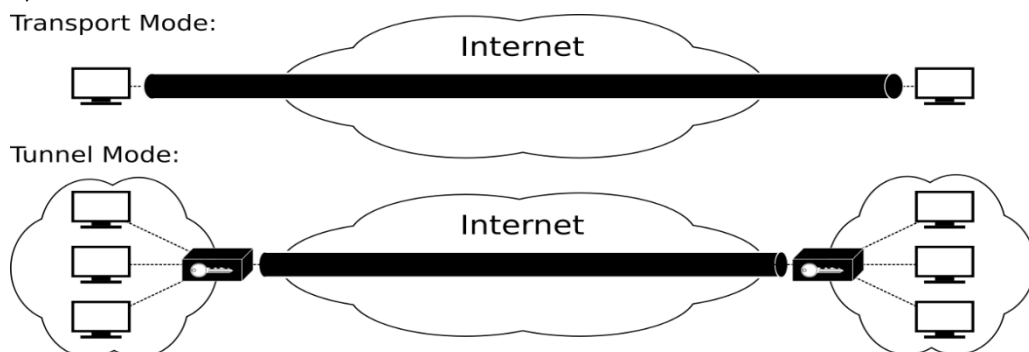


Figura 2.4. Cifrado de Datos en un Túnel IPsec.
Reproducida de Conexiones de Red Seguras con IPsec, www.ionos.es, 2022.

PPTP/MPPE: PPTP fue creado por el foro de PPTP. Admite VPN multiprotocolo, con cifrado de 40 bits y 128 bits mediante un protocolo denominado Cifrado de punto a punto de Microsoft (MPPE). Es importante tener en cuenta que PPTP no proporciona cifrado de datos por su cuenta.

L2TP/IPsec: comúnmente denominado L2TP a través de IPsec, proporciona la seguridad del protocolo de IPsec a través de túneles de capa 2. L2TP es producto de una asociación entre los miembros del foro de PPTP, Cisco y el IETF. Se usa principalmente para VPN de acceso remoto con sistemas operativos Windows. Los ISP también pueden brindar conexiones L2TP para usuarios de acceso telefónico (ADSL) y luego cifrar el tráfico con IPsec entre su punto de acceso y el servidor de red de la oficina remota. **(Morales Dibildox, 2006, pág. 23)**

2.3.3.2. INTEGRIDAD DE LOS DATOS.

Si bien es importante que los datos se cifren a través de una red pública, es igualmente importante verificar que no se hayan modificado mientras están en tránsito. Por ejemplo, IPsec tiene un mecanismo para asegurarse de que no se haya manipulado la parte cifrada del paquete o la parte del encabezado y de los datos. Si se ha detectado manipulación, el paquete se descarta. La integridad de los datos puede implicar la autenticación del par remoto. **(Sclayton, 2008)**

2.3.3.3. AUTENTICACIÓN DE ORIGEN DE DATOS.

Es muy importante verificar la identidad de la fuente de los datos que se envían. Esto es necesario para protegerlos contra un número de ataques que utilizan la suplantación de la identidad del remitente. Una técnica que ayuda a la suplantación de identidad es el Control Antirreproducción, que es la capacidad para detectar y rechazar paquetes reproducidos.

2.3.3.4. CONFIDENCIALIDAD DE TRÁFICO/TUNELIZADO DE DATOS.

El tunelizado es el proceso de encapsular un paquete dentro de otro paquete y enviarlo a través de una red. Es útil cuando se recomienda ocultar la identidad del dispositivo que originó el tráfico. Todos los protocolos de cifrado también usan el tunelado como medio para transferir los datos cifrados a través de la red pública. Es importante tener en cuenta que el tunelado no proporciona seguridad de datos por sí solo. El paquete solo se encapsula dentro de otro protocolo y aún puede visualizarse con un capturador de paquetes si no está cifrado. (Sclayton, 2008)

El tunelado requiere tres protocolos diferentes.

- **Protocolo de Pasajero:** los datos originales que se transportan (IPX, IP).
- **Protocolo de Encapsulación:** el protocolo (GRE, IPsec, L2F, PPTP, L2TP) que envuelve los datos originales.
- **Protocolo de Transporte:** utilizado por la red por la cual viaja la información.

La **Figura 2.5.** muestra este proceso, donde el paquete original se encapsula dentro del protocolo de encapsulación, que, luego, se coloca dentro del encabezado del protocolo IP para la transmisión a través de la red pública. A menudo el protocolo de encapsulación también lleva a cabo el cifrado de los datos.

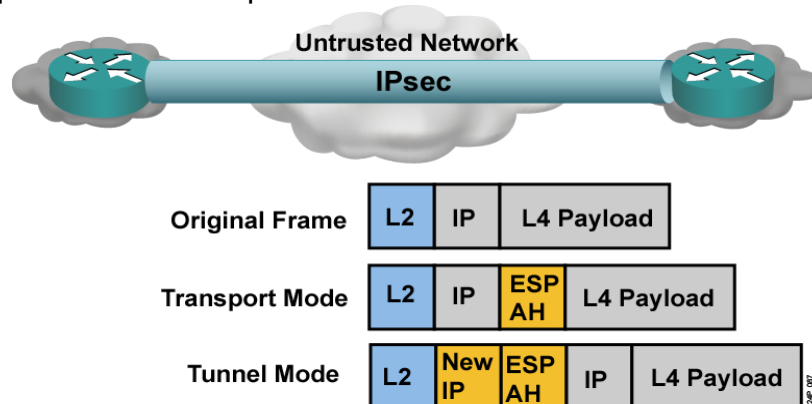


Figura 2.5. Tunelizado de Tráfico en IPsec.
Reproducida de IPsec VPN, byeong9935.tistory.com, 2022.

Para las VPN de sitio a sitio, el protocolo de encapsulación generalmente es IPsec o Encapsulamiento de Routing genérico (GRE). GRE incluye información sobre qué tipo de paquete está encapsulando e información sobre la conexión entre el cliente y el servidor. Para VPN de acceso remoto, el tunelado generalmente se

realiza mediante el Protocolo punto a punto (PPP). Como parte de la pila TCP/IP, PPP es la portadora de otros protocolos IP cuando se comunican a través de la red entre la computadora host y un sistema remoto. El tunelado PPP utilizará uno de los Reenvíos de capa 2: PPTP, L2TP. (Morales Dibildox, 2006, pág. 19)

2.3.3.5. AAA. AUTHENTICATION, AUTHORIZATION, ACCOUNTING.

La autenticación, autorización y contabilización se utiliza para un acceso más seguro en un entorno VPN de acceso remoto. Sin la autenticación del usuario, cualquiera que se encuentra en una computadora portátil con software de cliente VPN bien configurado puede establecer una conexión segura a la red remota. Sin embargo, también se debe introducir un nombre de usuario y contraseña válidos para completar la conexión. Los nombres de usuario y contraseñas se pueden almacenar en el dispositivo VPN o en un servidor AAA externo. (Sclayton, 2008)

Cuando una solicitud para establecer un túnel proviene de un cliente de acceso telefónico, el dispositivo VPN solicita un nombre de usuario y una contraseña, la **Figura 2.6.** refleja este procedimiento. Luego, esto se puede autenticar de forma local o enviarse al servidor AAA externo, que comprueba:

- ✓ Quién es usted (Autenticación)
- ✓ Qué tiene permitido hacer (Autorización)
- ✓ Qué hace realmente (Cuenta) (Sclayton, 2008)

AAA Authentication Process

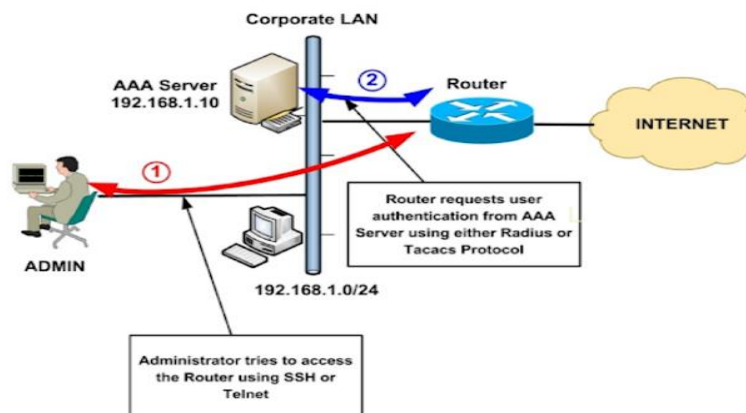


Figura 2.6. Proceso de Autenticación AAA.
Reproducida de Proceso AAA, www.thenetworkdna.com, 2022.

2.3.4. BENEFICIOS DE UTILIZAR UNA VPN.

Los beneficios de las VPN incluyen los siguientes:

- ✚ **Ahorro de Costos:** las VPN permiten a las organizaciones utilizar Internet global para conectar oficinas remotas y usuarios remotos al sitio corporativo principal, esto elimina enlaces WAN dedicados costosos y bancos de módems.
- ✚ **Seguridad:** las VPN proporcionan el mayor nivel de seguridad mediante el uso de protocolos de encriptación y autenticación avanzados que protegen los datos contra el acceso no autorizado. (Casasola, 2015)
- ✚ **Escalabilidad:** como las VPN utilizan la infraestructura de Internet dentro de ISP y de los dispositivos, es sencillo agregar nuevos usuarios. Las corporaciones pueden agregar grandes cantidades de capacidad sin agregar una infraestructura importante.
- ✚ **Compatibilidad con la tecnología de Banda Ancha:** los proveedores de servicios de banda ancha como ADSL – Cable Modem - OF soportan la tecnología VPN, de manera que los trabajadores móviles y los trabajadores a distancia pueden aprovechar el servicio de Internet de alta velocidad que tienen en sus hogares para acceder a sus redes corporativas.
Las conexiones de banda ancha de alta velocidad de nivel empresarial también pueden proporcionar una solución rentable para conectar oficinas remotas. (Casasola, 2015)

2.4. SERVICIOS DE REDES PRIVADAS VIRTUALES VPN.

Desde los primeros días de X.25 y Frame Relay (las dos tecnologías utilizadas inicialmente para implementar los servicios VPN), se han propuesto muchas tecnologías diferentes como base para habilitar una infraestructura VPN. Estas iban desde tecnologías de capa 2 (X.25, Frame Relay y ATM) hasta tecnologías de capa 3 (Túneles IP) o incluso tecnologías de capa 7 (SSL). (Guichard, Pepelnjak, & Apcar, 2003, pág. 21)

2.4.1. CLASIFICACION DE SERVICIOS VPN.

2.4.1.1. SEGÚN EL MODELO OSI.

Según el modelo de referencia OSI, una VPN se puede establecer en la capa de enlace de datos, en la capa de red o incluso en una capa superior. Existen varias VPN's que se usan ampliamente y se pueden dividir según la capa OSI en que se implementan. Estos tipos de VPN's se describen a continuación: (Jimenez, 2019)

- A. **Protocolo de Túnel de Capa 2 (capa enlace de datos):** incluye el Protocolo de túnel de punto a punto (PPTP), el Protocolo de reenvío de capa 2 (L2F), el Protocolo de túnel de capa 2 (L2TP) y MPLS.
- B. **Protocolo de Túnel de Capa 3 (capa de red):** incluye el Protocolo de encapsulación de enrutamiento genérico (GRE), la Seguridad de IP (IPSec) y MPLS. Estos 2 últimos son las VPN de capa 3 más populares
- C. **Protocolo de Tunelización de la Capa de Sesión:** El protocolo Socks4, proporciona un servidor de seguridad que no requiere autenticación para programas cliente-servidor basados en TCP (TELNET,FTP, HTTP, WAIS, GOPHER). Socks4 establece un túnel sin autenticación de cifrado. El protocolo Socks5 se amplía para que sea compatible con UDP, DNS e IPv6.
- D. **Protocolo de túnel de Capa de Aplicación:** Secure Socket Layer (SSL). Es ampliamente utilizado en navegadores web y programas de servidor web. Proporciona autenticación y cifrado de igual a igual de los datos de la aplicación. (Jimenez, 2019)

En la **Tabla 2.1.** se mencionan las características de estos protocolos según la capa OSI a la que pertenece.

Tabla 2.1. Protocolos según Modelo OSI para establecer una VPN.
Fuente Propia con Datos obtenidos de Redes VPN con MPLS, Dibildox, 2006.

Modelo OSI	Protocolo VPN	Características
Capa 2 Enlace de Datos	L2F.	Protocolo inicial de IP VPN. Soporta IP, Frame Relay y ATM. Autenticación TACACS y RADIUS.

	PPTP.	Cifrado por medio de MPPE. Sustituido por L2TP por limitaciones de seguridad.
	L2TP.	Herederero de L2F y PPTP. Autenticación PPP, PAP, CHAP. Cifrado no Robusto.
Capa 3 De Red	GRE.	Carece de Cifrado. Autenticación Sencilla. Necesita de PPP para le Encapsulación.
	IPSec.	Encriptación de Datos. Complejo. Requiere Config. del Cliente Soporta IPV4 y IPv6.
Capa 5 Sesión	Socks4.	Proporciona un Servidor de Seguridad. No requiere autenticación de Cifrado. Soporta TCP e IPv4.
	Sock5.	Proporciona autenticación. Compatible con IPv4 y IPv6. Soporta TCP y UDP.
Capa 7 Aplicación	SSL	Autenticación y Cifrado de Igual a Igual. Utilizado en Navegadores y Servidores Web. Fácil y Sencillo de Usar. Solo requiere

2.4.1.2. BASADOS EN EL CLIENTE O EN LA RED.

Existe otra manera de agrupar las tecnologías VPN's. Según donde se despliegue la VPN se pueden agrupas bajo dos enfoques: VPN's basadas en el cliente y VPN's basadas en la Red del Proveedor (ambas pueden ser de Acceso Remoto y/o Tipo Site to Site). La **Figura 2.7.** muestra las tecnologías VPN's basadas en el cliente o en la red del ISP, abarca también las mencionadas anteriormente.

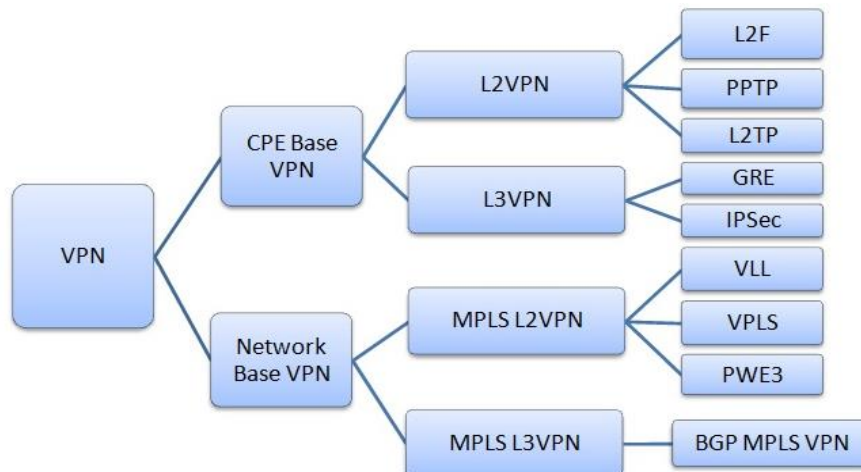


Figura 2.7. Tecnologías VPN basadas en Cliente o Red.
Reproducida de Categorías en que se Clasifican las VPN, Jimenez, 2019.

En este caso se incluye las opciones que ofrece MPLS, las que se implementan en las capa 2 llamadas MPLS L2 VPN y la que se levanta en la capa 3 llamadas BGP/MPLS VPN. Las MPLS VPN se utilizan para establecer la conexión entre los dispositivos de red (Core del ISP) en lugar de las PC remotas. **(Jimenez, 2019)**

Las tecnologías más utilizadas para el manejo de Redes Privadas Virtuales son MPLS y IPSec, en los últimos años se ha incrementado el uso de VPN de acceso remoto de tipo SSL (Capa de aplicación). MPLS por un lado se enfoca principalmente en los Backbone del ISP e IPSec en los clientes. Por esta razón se busca hibridar ambas tecnologías para que IPSec maneje la encriptación de la información y MPLS la provisión de servicios y el enrutamiento del tráfico. **(Morales Dibildox, 2006, pág. 26)**

2.4.2. MODELOS DE SERVICIOS VPN.

Una VPN generalmente pertenece a una empresa y tiene varios sitios interconectados a través de la infraestructura común del proveedor de servicios. Dependiendo de la participación del proveedor de servicios en el enrutamiento del cliente, las implementaciones de VPN a menudo se clasifican en: Modelo Superpuesto y Modelo Punto a Punto **(Nahidha & Alagumani, 2018, pág. 3078)**.

2.4.2.1. MODELO SUPERPUESTO (OVERLAY).

En el modelo superpuesto, el proveedor de servicios proporciona un servicio de enlaces punto a punto o circuitos virtuales a través de su red entre los sitios del cliente. Los enrutadores del cliente forman pares de enrutamiento entre ellos directamente a través de los enlaces o circuitos virtuales del ISP. Los enrutadores o conmutadores del ISP transportan los datos del cliente a través de la red, pero estos enrutadores nunca ven las rutas de los clientes. **(De Ghein, 2007, pág. 10)**

Estos servicios punto a punto pueden ser de Capa 1: enlaces TDM, E1, E3, SONET y SDH. Ejemplos de Capa 2 son los circuitos virtuales creados por X.25,

ATM o Frame Relay. Ejemplos de Capa 3 son los túneles IP como GRE y IPSec. Los sitios del cliente se ven a un salto de distancia entre sí como si no existiese la red del proveedor, el ISP solo brinda el transporte para el túnel virtual y no participa en el enrutamiento de los clientes, y el cliente desconoce la de la Red del ISP. (Nahidha & Alagumani, 2018)

La **Figura 2.8.** nos ayuda a comprender este modelo de VPN. Allí se aprecia como los Router del cliente se ven como pares que estuviesen conectados físicamente.

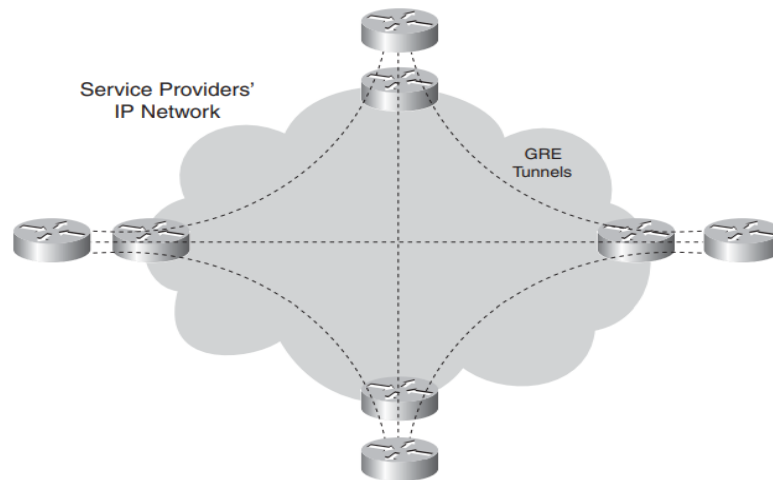


Figura 2.8. Modelo VPN Superpuesto con Túneles IP.
Reproducida de MPLS - Fundamentals, De Ghein, 2007.

2.4.2.2. MODELO PUNTO A PUNTO (PEER TO PEER).

Este modelo se desarrolló para superar los inconvenientes del modelo Overlay y proporcionar a los clientes información óptima de transporte a través de la red troncal del ISP. Por lo tanto, el proveedor de servicios participa activamente en el enrutamiento del cliente. Dentro del modelo peer-to-peer, los datos de enrutamiento se cambian entre los enrutadores del cliente y también los enrutadores del proveedor de servicios, y la información del cliente se transporta a través del núcleo del proveedor de servicios donde se identifican la ruta óptima desde el sitio de un cliente a otro.. (Nahidha & Alagumani, 2018, pág. 3078).

En otras palabras, no necesita la creación de circuitos virtuales, debido a que los enrutadores del proveedor de servicios se emparejan directamente con los

enrutadores del cliente en la capa 3. El resultado es que existe una adyacencia de protocolo de enrutamiento entre el cliente y el enrutador del proveedor de servicios. (De Ghein, 2007, pág. 12)

La **Figura 2.9.** muestra como ahora los pares se establecen entre Router cliente y Router ISP en cada sitio del cliente y para cada VPN que se levante.

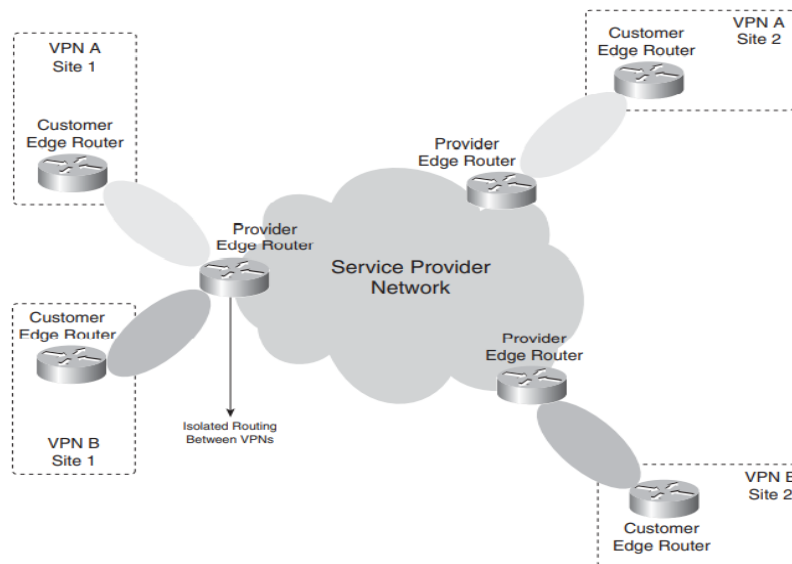


Figura 2.9. Modelo VPN Peer to Peer.
Reproducida de MPLS - Fundamentals, De Ghein, 2007.

Antes de que MPLS surgiera, el modelo de VPN superpuesto se implementaba con más frecuencia que el modelo de VPN punto a punto. El modelo VPN punto a punto demandaba mucho del aprovisionamiento porque agregar un sitio de cliente exigía muchos cambios de configuración en muchos sitios. MPLS VPN es una aplicación de MPLS que hizo que el modelo VPN peer-to-peer fuera mucho más fácil de implementar. Agregar/eliminar un sitio de cliente se hizo más fácil de configurar y exige mucho menos tiempo y esfuerzo. (De Ghein, 2007, pág. 13)

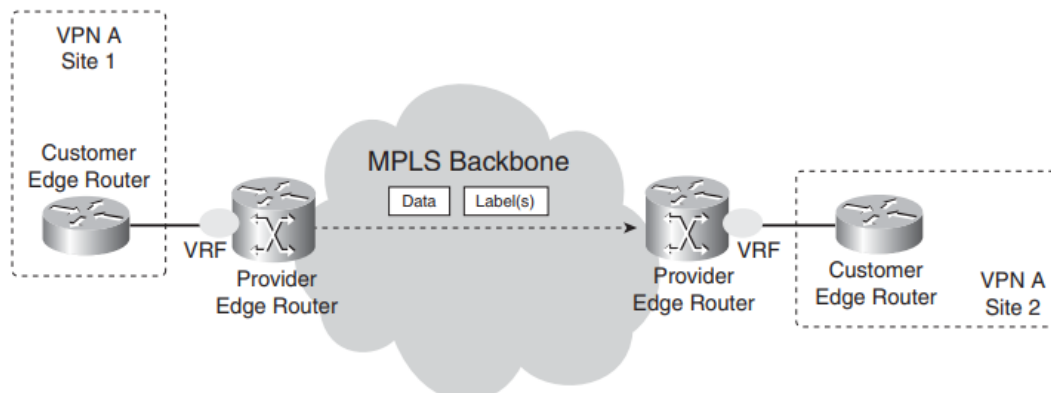
2.4.2.3. MODELO PEER TO PEER CON MPLS.

Antes de que existiera MPLS, el modelo de VPN punto a punto podía lograrse mediante la creación de pares de enrutamiento IP entre los enrutadores del cliente y del proveedor de servicios. El modelo VPN también requiere privacidad o

aislamiento entre los diferentes clientes (es decir las subredes de los sitios de clientes no tiene que ser la misma). Esto se lograba configurando filtros de paquetes (listas de acceso) para controlar los datos hacia y desde los enrutadores del cliente. Otra forma es configurar filtros para anunciar rutas o evitar que las rutas se anuncien a las rutas de los clientes. O bien, ambos métodos al mismo tiempo. (De Ghein, 2007, pág. 14)

La privacidad en las redes MPLS VPN se logra utilizando el concepto de enrutamiento/reenvío virtual (VRF) y el hecho de que los datos se reenvían en la red troncal como paquetes etiquetados. Las VRF garantizan que la información de enrutamiento de los diferentes clientes se mantenga separada, y MPLS en la red troncal garantiza que los paquetes se reenvíen según la información de la etiqueta y no la información del encabezado IP.

La **Figura 2.10.** muestra el concepto de VRF y el reenvío de paquetes etiquetados en la red troncal de una red que ejecuta MPLS VPN.



**Figura 2.10. Modelo VPN Peer to Peer con MPLS VPN.
Reproducida de MPLS - Fundamentals, De Ghein, 2007.**

Agregar un sitio de cliente significa que en el enrutador PE (Provider Edge), solo se debe agregar el emparejamiento con el enrutador CE (Customer Edge). No se necesita la creación de muchos circuitos virtuales como con el modelo de superposición o con la configuración de filtros de paquetes o filtros de ruta con el modelo de VPN punto a punto sobre una red IP. Este es el beneficio de MPLS VPN para el proveedor de servicios. (De Ghein, 2007, pág. 15)

2.4.3. COMPARATIVA DE TECNOLOGIAS VPN.

2.4.3.1. TECNOLOGIAS DE CIRCUITOS VIRTUALES PVC.

Las VPN's tradicionales se han construido sobre infraestructuras de transmisión compartidas con características implícitas de seguridad y respuesta predeterminada. Redes como Frame Relay, que permiten establecer PVC's entre los diversos nodos que conforman la VPN. La seguridad y las garantías las proporcionan la separación de tráfico por PVC y el caudal asegurado CIR.

Algo similar sucede con ATM, con diversas clases de garantía, los inconvenientes de este tipo de solución es que la configuración de las rutas se basa en procedimientos manuales, al tener que establecer cada PVC entre nodos, con la complejidad que esto supone al proveedor en la gestión y los mayores costes asociados, si se quiere tener conectados a todos con todos (topología Full Mesh) añadir un nuevo sitio supone retocar todos los CPE's y restablecer todos los PVC's. **(Tapasco Garcia, 2008, pág. 18)**

2.4.3.2. TECNOLOGIAS DE TUNELES IP.

La búsqueda por conseguir una mayor flexibilidad en el diseño e implementación y unos menores costes de gestión y provisión de servicio llevaron a los ISP a expandir sus redes y a utilizar infraestructuras IP para el soporte de VPN's, La forma de utilizar estas infraestructuras IP para servicio VPN (IP VPN) ha sido la de construir túneles IP. El objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos, de modo que funcionalmente aparezcan conectados, lo que se hace es utilizar una estructura no conectiva como IP para simular esas conexiones: una especie de tuberías privadas por las que no puede entrar nadie a menos que sea miembro de esa IP VPN. **(Canalis, 2003, pág. 143)**

Los túneles IP, vistos anteriormente, se pueden establecer en la Capa 3, mediante IPSec y GRE y en Capa 2 mediante el encapsulamiento sobre IP ya sea L2TP o PPTP.

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

En las VPN's basadas en túneles IPSec, la seguridad requerida se garantiza mediante el cifrado de la información de los datos y de la cabecera de los paquetes IP, que se encapsulan con una nueva cabecera IP para su transporte por la red del proveedor. Es relativamente sencillo de implementar, bien sea en dispositivos especializados como cortafuegos, como en los Routers de acceso del ISP, además, IPSec permite crear VPN's a través de redes de distintos ISP's. El cifrado IPSec oculta las cabeceras de los paquetes originales, con esto las opciones QoS son bastantes limitadas, ya que la red no puede distinguir flujos por aplicaciones para asignarles diferentes niveles de servicio. **(Tapasco Garcia, 2008, pág. 19)**

En los túneles de Capa 2 se encapsulan paquetes multiprotocolo sobre los datagramas IP de la red del ISP, de este modo, la red del proveedor no pierde la visibilidad IP por lo que hay mayores posibilidades de QoS para priorizar el tráfico por tipo de aplicación IP. Los clientes VPN pueden mantener su esquema privado de direcciones, estableciendo grupos cerrados de usuarios (además de encapsular los paquetes, se puede cifrar la información por mayor seguridad, pero en esto limita las opciones QoS). A diferencia de los túneles IP, los túneles decapa 2 están condicionada a un único proveedor. **(Barberá, 2000)**

A pesar de las ventajas de los túneles IP sobre los PVC's, ambos enfoques tienen unas características que las hacen menos eficientes frente a la solución MPLS:

- ✓ Están basadas en conexiones punto a punto (PVC's o túneles).
- ✓ La configuración es manual.
- ✓ La provisión y gestión son complicadas; una nueva conexión supone alterar todas las configuraciones.
- ✓ Plantean problemas de crecimiento al añadir nuevo túneles o circuitos virtuales.
- ✓ La gestión de QoS es posible en cierta medida, no se puede mantener extremo a extremo a lo largo de la red, ya que no existen mecanismos que sustenten los parámetros de calidad durante el transporte. **(Canalis, 2003, pág. 144)**

2.4.3.3. TECNOLOGIA VPN CON MPLS.

El problema que plantean estas IP VPN's, es que están basadas en un modelo superpuesto sobre la topología física existente, basados en túneles IP o Circuitos virtuales entre cada par de Routers en cada VPN. La **Figura 2.11.** ejemplifica este modelo, de ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento al añadir nuevos nodos.

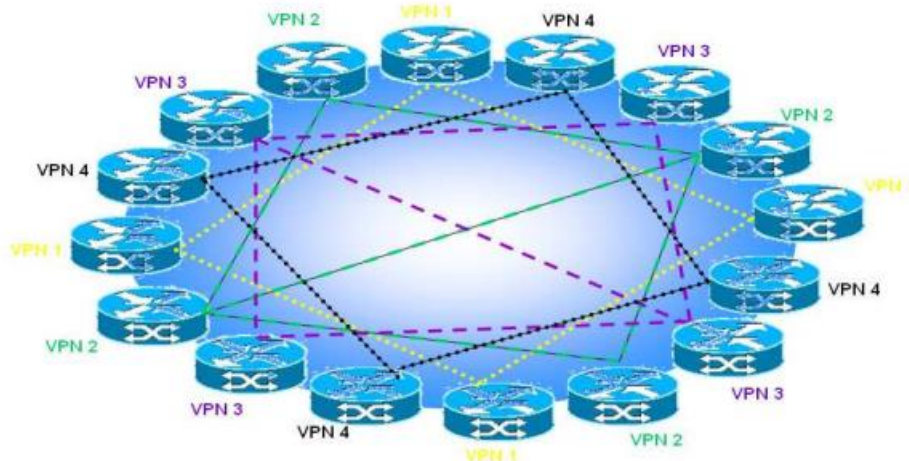


Figura 2.11. Modelo Superpuesto de VPN Tradicionales.
Reproducida de MPLS – El Presente de las Redes IP, Tapasco Garcia, 2008.

Con una arquitectura MPLS se evitan estos inconvenientes ya que el modelo topológico no se superpone sino que se acopla a la red. En el modelo acoplado, en lugar de conexiones extremo a extremo entre los distintos nodos de una VPN, lo que hay son conexiones IP a una “nube común” en la que solamente pueden entrar los miembros de la misma VPN, las “nubes” que representan las distintas VPN's se implementan mediante los caminos LSP's creados por el mecanismo de intercambio de etiquetas MPLS.

En los túneles se utiliza el encaminamiento IP para transportar los datos del usuario, en MPLS estos datos se transporta sobre el mecanismo de intercambio de etiquetas LDP, que no ve el proceso de Routing IP, pero sí se mantiene la visibilidad IP hacia el usuario, que no sabe nada de rutas MPLS sino que ve un internet privado (intranet) entre los miembros de su VPN. (Tapasco Garcia, 2008, pág. 20)

La **Figura 2.12.** expone la diferencia entre el modelo acoplado y el superpuesto. Es más sencillo de aprovisionar y más escalable ya existe una nube en común para cada VPN a la cual solo tienen acceso los sitios que pertenecen a ella.

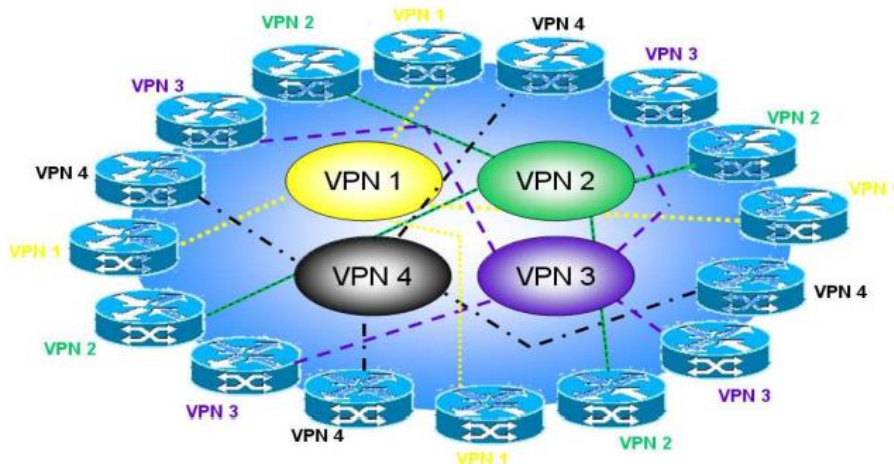


Figura 2.12. Modelo MPLS Acoplado para VPN.
Reproducida de MPLS – El Presente de las Redes IP, Tapasco Garcia, 2008.

Como conclusión, las ventajas que MPLS ofrece para IP VPN's son:

- ❖ Proporcionan un modelo "Acoplado" o "Inteligente", ya que la red MPLS "sabe" de la existencia de VPN's (lo que no ocurre con túneles ni PVC's).
- ❖ Evita la complejidad de los túneles y PVC's.
- ❖ La provisión de servicio es sencilla: una nueva conexión afecta a un solo Router, tiene mayores opciones de crecimiento modular.
- ❖ Permite mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias a las asociaciones de las etiquetas MPLS con las clases definidas FEC a la entrada.
- ❖ Permite aprovechar las posibilidades de Ingeniería de tráfico para poder garantizar los parámetros críticos y la respuesta global de la red, lo que es necesario para un servicio completo VPN. (Canalis, 2003, pág. 145)

2.4.3.4. COMPARACION EN CUANTO A SERVICIOS.

La **Tabla 2.2.** muestra, a modo comparativo, las ventajas y limitaciones de los servicios a manejar en tres opciones de VPN. Se escogió a MPLS VPN e IPSec por ser las más implementadas y a SSL por tener gran auge en los últimos años.

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

**Tabla 2.2. Comparación en cuanto a Servicios de Tecnologías VPN.
Adaptada de Estudio de las Ventajas e Implementación de Servicios IP VPN sobre
MPLS, Silvestre H, 2008.**

ITEMS	VPN BASADAS EN MPLS	VPN BASADAS EN IPSEC	VPN BASADAS EN SSL.
Topología	Sitio-a-Sitio VPN: Hub-and-spoke o full-mesh	Sitio-a-Sitio VPN: principalmente hub-and-spoke	VPN de acceso remoto.
Seguridad y Autenticación de sesión.	Establece una membresía durante el aprovisionamiento, basada en un Puerto lógico y un ID de ruta único. Define el acceso a los servicios VPN de grupos durante la configuración, rechaza todo acceso no autorizado.	Autentica a través de certificados digitales o de claves pre compartidas. Bota los paquetes que no llenen las políticas de seguridad.	Autentica a través de certificados digitales.
Confidencialidad	Separa el tráfico, que alcanzan los mismos resultados que en una red ATM o Frame Relay.	Utiliza Fuentes flexibles de mecanismos de encriptación y Tunneling en la capa de red.	Encripta el tráfico utilizando Infraestructura de Llave Pública (PKI).
QoS and SLA's	Permite SLA's con un mecanismo de QoS escalable y robusto; así como capacidad de ingeniería de tráfico.	No utiliza QoS y SLA's, sin embargo hay algunas aplicaciones que permiten clasificar el tráfico dentro de túnel IP.	No aplicable.
Escalabilidad	Altamente escalable, ya que no requiere un Peering sitio a sitio, es capaz de soportar muchas VPN's a través de la misma red.	Aceptable sobre todo en las configuraciones del tipo hub-and-spoke, la escalabilidad se vuelve un reto para la entrega de VPN IPsec grandes (full Meshed).	No aplicable
Soporte sitio a sitio	Sí.	Sí.	Sí.
Soporte de Acceso Remoto	Sí. sí es usado en conjunto con IPsec.	Sí.	Sí.
Aprovisionamiento	Requiere de una sola vez el	Reduce los costos operacionales a través	No Aplicable.

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

	aprovisionamiento de los equipos del usuario de del lado del proveedor para habilitar el sitio como miembro de un grupo VPN de MPLS.	del aprovisionamiento de redes centralizadas para la oferta de servicios CPE. Utiliza este tipo de aprovisionamiento para ofrecer servicios basados en red.	
Entrega de Servicio	Requiere elementos de red basados en MPLS en la red Core del proveedor de servicio.	Puede ser implementada a través de cualquier red IP existente o a través del Internet.	No Aplicable.
Cliente VPN	No es requerida porque las VPN MPLS es una red basada en el servicio VPN	Es necesario para los clientes IPSec VPN.	No requerido, se usa el buscador Web.
Sitio de la Red	En la red Core del ISP.	Local Loop, Edge, y fuera de la red.	Local Loop, Edge, y fuera de la red.
Transparencia	Reside en la capa de Red, transparente a las aplicaciones.	Reside en la capa de Red, transparente a las aplicaciones.	Reside en la capa de sesión, trabaja solo con aplicaciones codificadas para SSL.

2.5. SERVICIOS MPLS L3 VPN.

Hasta el momento, en este trabajo, se ha ido de lo general (MPLS) a lo específico (Servicios de VPN's). Es momento ahora de abordar la tecnología MPLS L3 VPN que es lo mejor de ambos mundos de las VPN Overlay y VPN Peer to Peer y es en la que se basa el diseño de red Propuesto para la solución del cliente.

En MPLS L3 VPN no se requiere aprovisionamiento estático. Siempre que queramos añadir nuevos sitios podemos añadirlos fácilmente sin reconfigurar otros existentes. En MPLS VPN, el proveedor de servicios mantiene tablas de enrutamiento separadas por cliente dando flexibilidad en el direccionamiento al cliente. En MPLS L3 VPN, la ruta manual y el filtrado ACL no son necesarios en

los ISP. Los clientes pueden usar el enrutamiento predeterminado según sea necesario. **(Ravi, Dhanumjayulu , Bagubali , & Bagadi , 2017, pág. 2)**

MPLS L3 VPN utiliza VRF de capa 3 (Virtual Routing and Forwarding) para segmentar las tablas de enrutamiento para cada "cliente" que utiliza el servicio. El enrutador del cliente (CE) se empareja con el enrutador de borde del proveedor de servicios (PE) y las dos rutas de intercambio, que luego se colocan en una tabla de enrutamiento específica para ese cliente. Se requiere MP-BGP en el borde de la red del SP para intercambiar las rutas VPNv4. **(Ravi, Dhanumjayulu , Bagubali , & Bagadi , 2017)**

2.5.1. TERMINOLOGÍA MPLS L3 VPN.

Para entender el funcionamiento de una red MPLS L3 VPN es necesario conocer los términos relacionados a esta tecnología, pues presentan cierta diferencia respecto a la terminología MPLS vista en el capítulo I. A continuación la descripción de la terminología.

2.5.1.1. RED P - RED DEL PROVEEDOR DE SERVICIOS.

Los componentes P pertenecen a la red del SP y son Routers con capacidad de ejecutar MPLS para poder realizar el reenvío de paquetes etiquetados.

- **Provider Router - P.** Vendrían siendo los LSR-MPLS en el núcleo de la Red. Un enrutador P es un enrutador sin conexión directa a los enrutadores del cliente (CE).
- **Provider Edge Router - PE.** Misma función, diferente nombre al LER-MPLS. Un PE es un enrutador de borde del proveedor. Tiene una conexión directa con el enrutador de borde del cliente (CE) en L3. **(De Ghein, 2007, pág. 174)**

La **Figura 2.13.** refleja los componentes de la red del proveedor (Router con funcionalidades de P y PE).

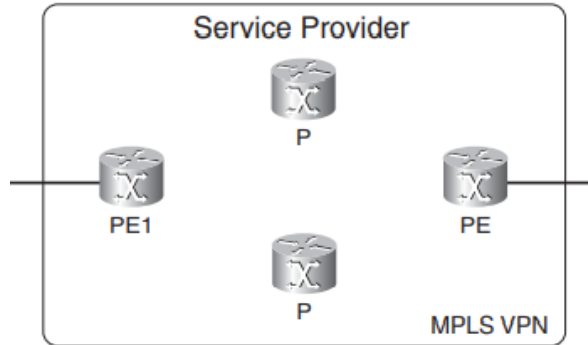


Figura 2.13. Red P en una Red MPLS VPN.
Adaptada de MPLS - Fundamentals, De Ghein, 2007.

2.5.1.2. RED C - RED DEL CLIENTE.

Es una red controlada por el cliente, en la cual no se necesita ejecutar MPLS.

- **Customer - C.** Un enrutador de cliente C es un enrutador sin conexión directa con el enrutador PE de la red del SP.
- **Customer Edge - CE.** Un enrutador CE tiene una conexión directa de capa 3 con el enrutador PE. Los CE's ejecutan enrutamiento IP tradicional.
- **Sitio - S.** Parte de la Red C, vendrían siendo las redes internas del cliente. Un sitio se conecta al Backbone MPLS a través de uno o más enlaces PE-CE.
(Alvez, 2012, págs. 13-16)

La **Figura 2.14.** muestra los elementos del lado del cliente en los 2 extremos o sitios que se establece la conexión.

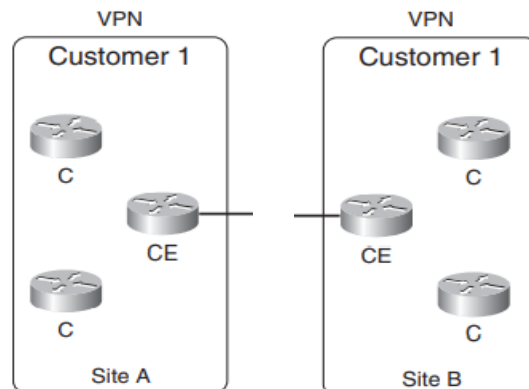


Figura 2.14. Red C en una Red MPLS VPN.
Adaptada de MPLS - Fundamentals, De Ghein, 2007.

2.5.1.3. INTERACCIÓN ENTRE CE - PE - P.

- ✚ Los CE's intercambian rutas con los PE's por medio de enrutamiento IP.
- ✚ Los PE's propagan información de VPN's y sitios conectados con MP-BGP a otros PE's. Los PE's mantienen tablas de rutas separadas.
Las rutas que el PE recibe de los CE's las ubica en una VRF apropiada. Las rutas que el PE recibe de los P's (del IGP) las pone en la tabla IP "tradicional".
- ✚ Los P's no tiene conocimiento de las VPN's ni tampoco corren MP-BGP. Los P's y PE's comparten protocolo de enrutamiento interno IGP (OSPF, iBGP).
- ✚ Un sitio puede ser parte de diferentes VPN's. Los sitios que pertenecen a la misma VPN usan la misma VRF, al igual que las interfaces que conectan a estos sitios. (Alvez, 2012, págs. 15,20)

La **Figura 2.15.** muestra la interacción entre CE, PE y P en una red MPLS L3 VPN.

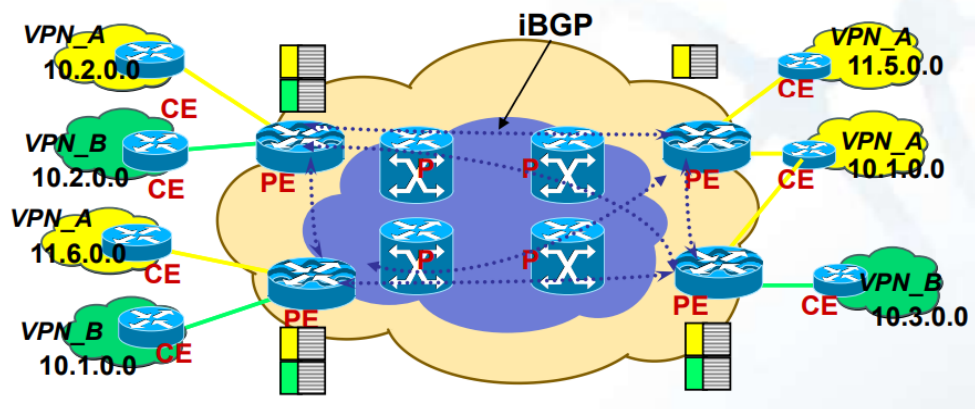


Figura 2.15. Interacción CE - PE - P en una Red MPLS VPN.
Adaptada de Fundamentos de MPLS/VPN, Alvez, 2012.

2.5.2. TOPOLOGIAS MPLS L3 VPN.

2.5.2.1. VPN TIPO FULL MESH - ACOPLAMIENTO COMPLETO.

En este tipo de topología todos los sitios que pertenecen a la misma VPN tienen conexión directa con los demás. Es decir cada CE se puede comunicar directamente con los CE's de otros sitios. Es la más simple de implementar, todas las VRF's que se utilicen para esta topología son configuradas con el mismo Route Target de importación y exportación. (Silvestre Hernandez, 2008, pág. 72)

En la **Figura 2.16**, se aprecia que hay comunicación entre cada CE a través de los equipos PE del proveedor, quienes intercambian información VPN entre ellos.

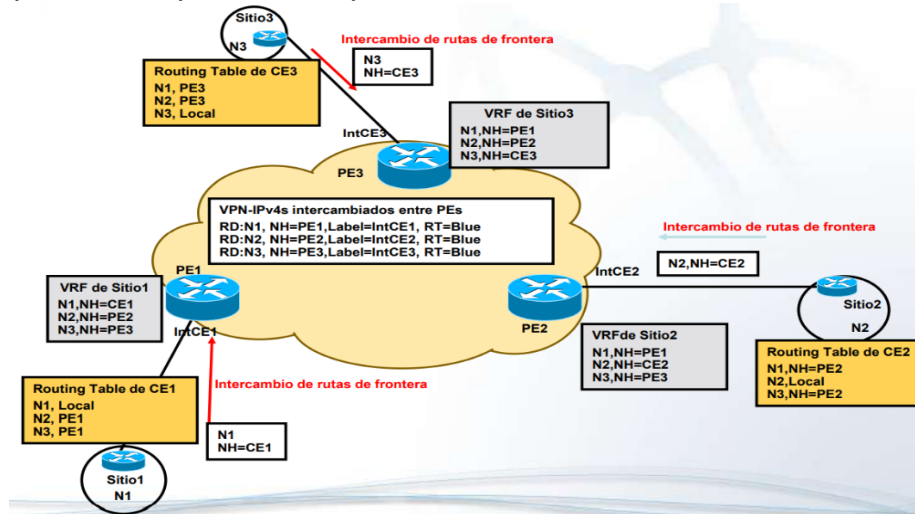


Figura 2.16. MPLS L3 VPN tipo Full Mesh.
Reproducida de Fundamentos de MPLS/VPN, Alvez, 2012.

2.5.2.2. VPN TIPO HUB AND SPOKE – PUNTO TRANSITORIO.

En este tipo de topología, los sitios (spoke) no pueden comunicarse directamente uno con otro, pero lo pueden hacer a través del sitio principal (Hub). Todo el tráfico de los sitios spoke que está destinado para el sitio hub o para un sitio interno, debe de fluir a través del sitio hub. Para que los CE´s se puedan comunicar deben pasar por un CE central definido por el cliente. **(Silvestre Hernandez, 2008, pág. 73)**

La **Figura 2.17**, muestra que CE3 es el Hub-Site (punto de tránsito) para los Spoke Sites CE1 y CE2. Ambos tienen que pasar por CE3 para tener comunicación.

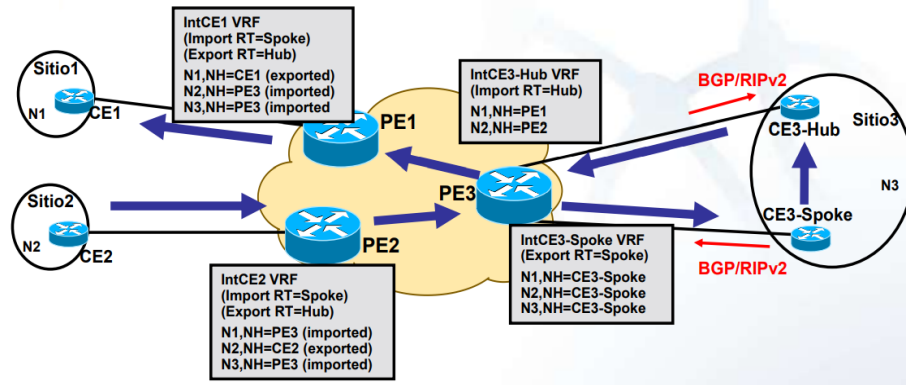


Figura 2.17. MPLS L3 VPN Hub and Spoke.
Reproducida de Fundamentos de MPLS/VPN, Alvez, 2012.

2.5.2.3. VPN TIPO OVERLAPPED O TRASLAPADAS.

En las VPN's traslapadas un sitio puede pertenecer a múltiples VPN's. Este tipo de conectividad IP puede ser utilizada por ejemplo para implementar una Extranet o Servicios Centrales. Se requiere de una dirección de IP única entre las VPN's traslapadas. (Silvestre Hernandez, 2008, pág. 76)

En la **Figura 2.18.** se observa cómo pueden traslaparse varias VPN's. Puede incluir más de un sitio por cada VPN.

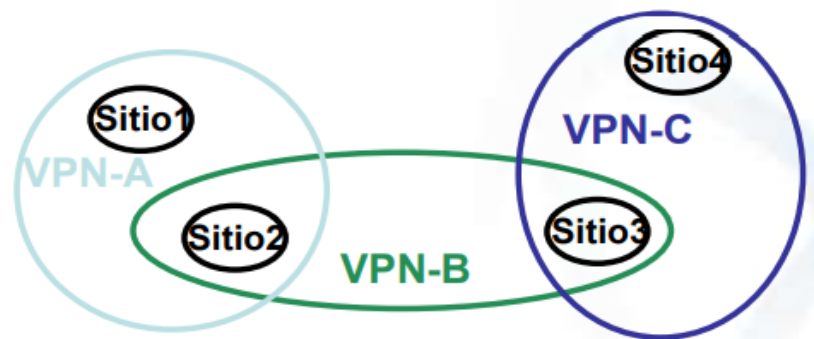


Figura 2.18. Diagrama de VPN's Traslapadas.
Reproducida de Fundamentos de MPLS/VPN, Alvez, 2012.

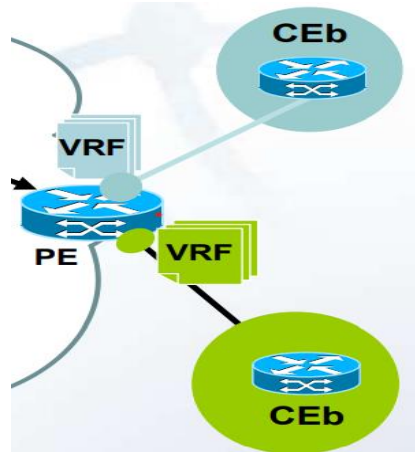
2.5.3. COMPONENTES FUNCIONALES L3 VPN.

Para implementar MPLS L3 VPN, se necesita de algunos componentes básicos en los Routers PE. Estos componentes son: VRF, Route Distinguisher RD, Route Target RT, MP-BGP y reenvío de paquetes etiquetados.

2.5.3.1. VRF - VIRTUAL ROUTING AND FORWARDING.

Una VRF es una instancia de enrutamiento y reenvío de VPN. Es el nombre de la combinación de la tabla de enrutamiento VPN, la tabla VRF Cisco Express Forwarding (CEF) y la tabla de enrutamiento IP en el enrutador PE. Un enrutador PE tiene una instancia de VRF para cada VPN. Esto se puede apreciar en la **Figura 2.19.** donde el Router PE crea una VRF por cada VPN del cliente y el tráfico de cada VPN es privado y lo aloja en tablas de enrutamiento independientes. (De Ghein, 2007, pág. 178)

Al crear VRF se crea un enrutador virtual dentro del IOS del PE que tiene su propia tabla de enrutamiento. Y esta tabla de enrutamiento es diferente a la tabla de enrutamiento global del PE. Cada VPN puede usar el mismo espacio de direcciones IP privadas, pero se diferencian mediante el uso del RT, que es la característica de VRF. Al configurar VRF debemos especificar RD y RT. (Ravi, Dhanumjayulu , Bagubali , & Bagadi , 2017)



**Figura 2.19. Creación de VRF por cada VPN en PE.
Reproducida de Fundamentos de MPLS/VPN, Alvez, 2012.**

2.5.3.2. RD - ROUTE DISTINGUISHER.

Un RD es un campo de 64 bits que se utiliza para hacer que los prefijos VRF sean únicos cuando MP-BGP los transporta. El RD no indica a qué VRF pertenece el prefijo, tampoco es un identificador de VPN. La idea es que cada prefijo de cada cliente reciba un identificador único RD para distinguirse del resto de prefijos.

Cada instancia de VRF en el PE debe tener un RD asignado. El RD tiene el siguiente formato: ASN:nn, donde ASN es el número de sistema autónomo que la IANA asigna al proveedor de servicios y nn es el número que el proveedor de servicios asigna de manera exclusiva a la VRF.

El RD solo se usa para identificar las rutas VPN. Esto es necesario porque las rutas IPv4 de un cliente pueden superponerse con las rutas IPv4 de otro. La combinación de RD con el prefijo IPv4 proporciona un prefijo VPNv4, cuya dirección tiene una longitud de 96 bits. La máscara tiene una longitud de 32 bits, tal como lo es para un prefijo IPv4. (De Ghein, 2007, pág. 179)

2.5.3.3. ROUTE TARGET - RT.

Con el uso únicamente del RD no se garantiza que exista una comunicación óptima entre VPN's, pues en algún momento los RD pueden no coincidir. De aquí que se utilizan los RT. Un RT es una comunidad extendida de BGP que indica qué rutas deben importarse desde el MP-BGP a la VRF. Exportar un RT significa que la ruta VPNv4 exportada recibe una comunidad extendida de BGP adicional configurada en el PE, cuando la ruta se redistribuye desde la tabla de enrutamiento VRF a MP-BGP.

Importar un RT significa que la ruta VPNv4 recibida de MP-BGP se verifica si coincide con una comunidad extendida existente. Si el resultado es una coincidencia, el prefijo se coloca en la tabla de enrutamiento VRF como una ruta IPv4. Si no se produce una coincidencia, se rechaza el prefijo. Se puede adjuntar más de un RT a la ruta VPNv4. (De Ghein, 2007, pág. 180)

La **Figura 2.20.** muestra que los RT controlan qué rutas se importan a qué VRF y con qué RT se exportan las rutas VPNv4 hacia los PE remotos. Por ejemplo la VRF de la VPN B exporta sus redes mediante el RT export 1:2 e importa las de otra VRF mediante el RT import 1:100.

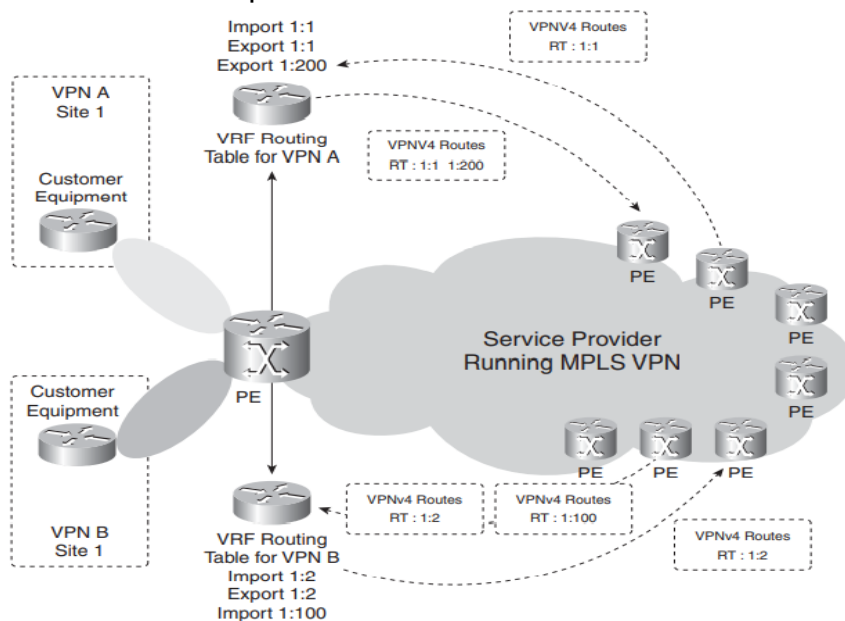


Figura 2.20. Uso de RD y RT en MPLS VPN.
Reproducida de MPLS - Fundamentals, De Ghein, 2007.

2.5.3.4. REENVIO DE PAQUETES ETIQUETADOS.

Los paquetes, en una red MPLS VPN, no se pueden reenviar como paquetes IP entre sitios debido a que los Routers P no tienen la información de VRF de cada sitio. Para esto MPLS utiliza etiquetas para el reenvío de los paquetes. Esto se logra configurando el protocolo LDP entre todos los enrutadores P y PE para que todo el tráfico IP se cambie por etiqueta entre ellos.

Los paquetes de clientes se reenvían con dos etiquetas: la etiqueta IGP como etiqueta superior y la etiqueta VPN como etiqueta inferior. La etiqueta VPN se anuncia por MP-iBGP entre los PE's e indica al PE de salida a qué VRF pertenece el paquete. La etiqueta IGP se distribuye por LDP entre P's y PE's y se intercambia en cada Router P que atraviesa el paquete. (De Ghein, 2007, pág. 187)

La **Figura 2.21.** muestra el reenvío de paquetes en una red VPN MPLS. El paquete ingresa al PE en la interfaz VRF como un paquete IPv4. Se reenvía a través de la red con dos etiquetas. Los enrutadores P reenvían el paquete mirando la etiqueta superior IGP. Las etiquetas se eliminan en el PE de salida y el paquete se reenvía como un paquete IPv4 a la interfaz VRF hacia el CE correcto mirando la etiqueta

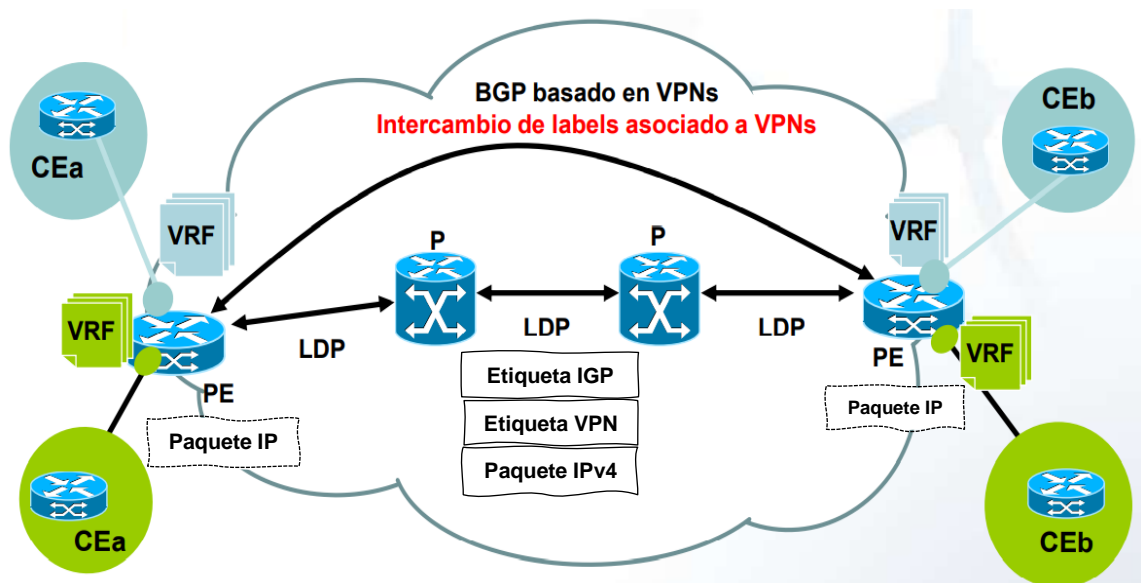


Figura 2.21. Trafico VRF a VRF en una red MPLS L3 VPN.
Adaptada de Fundamentos de MPLS/VPN, Alvez, 2012.

2.5.3.5. MP-BGP - BGP MULTIPROTOCOLO.

BGPv4 es el protocolo que ha hecho que Internet funcione hasta hoy día. Los SP que conforman Internet ejecutan BGP entre ellos. Se emparejan con otros SP a través de eBGP y ejecutan iBGP en sus propias redes. BGP tiene el concepto de familias de direcciones. Entre ellas están: IPv4, IPv6, VPNv4 (VPN-IPv4), VPNv6 (VPN-IPv6) y VRF. (De Ghein, 2007, págs. 189,191)

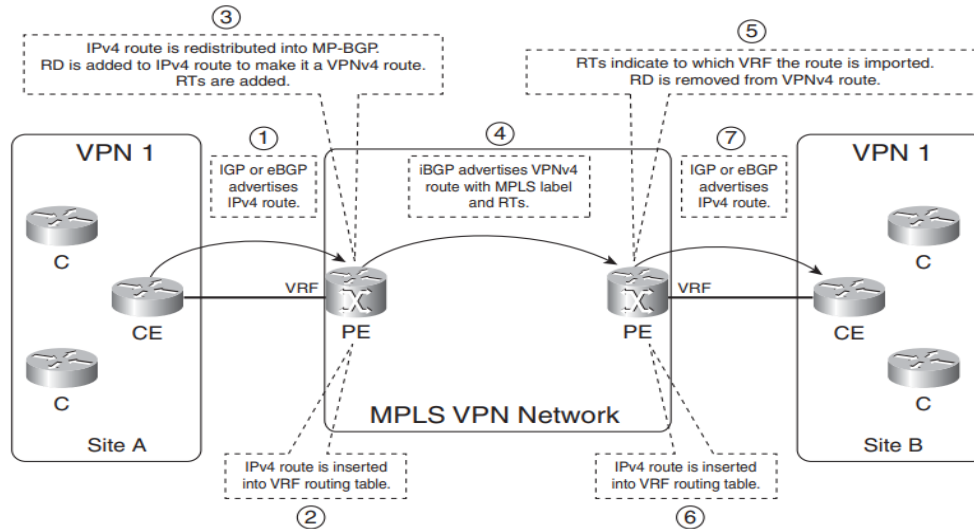
Se utiliza el termino MP-BGP porque BGP se usa para distribuir entre los PE's información de enrutamiento de los prefijos VPNv4 y porque MPLS se usa para reenviar el tráfico etiquetado de un sitio VPN a otro a través de la red troncal del proveedor de servicios. Se habla de MP-iBGP cuando se utiliza BGP como protocolo IGP entre los equipos P y PE de la red MPLS del SP.

2.5.4. COMO OPERAN LAS MPLS L3 VPN.

El PE de ingreso recibe rutas IPv4 del enrutador CE a través de un Protocolo IGP o eBGP. Estas rutas IPv4 del sitio VPN se colocan en la tabla de enrutamiento VRF. Las VRF separan las rutas de los clientes creando para cada VPN una VRF. Las VPN's del cliente se vuelven únicas al agregar el RD a cada ruta IPv4, convirtiéndolas en rutas VPNv4 asignadas a un VRF. A estas rutas VPNv4 se les añade el RT y luego son distribuidas por MP-BGP a todos los PE's en la red.

Durante este proceso, las dos etiquetas están en uso, la etiqueta VPN que representa la red de destino y la etiqueta IGP que contiene la información sobre la ruta LSP que conduce al PE de salida a través de los enrutadores P. En el PE de salida, las rutas VPNv4 se eliminan de los RD y se colocan en la tabla de enrutamiento VRF como rutas IPv4. Estas rutas IPv4 luego se anuncian, según los parámetros del RT, al enrutador CE destino a través de un IGP o eBGP que se ejecuta entre PE y CE. (De Ghein, 2007, pág. 185)

La **Figura 2.22** muestra el funcionamiento de MPLS VPN de CE a CE. Cómo opera el vínculo L3 PE-CE y como trabaja MP-BGP entre PE's en la red del ISP.



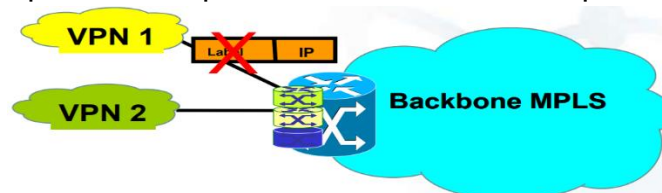
**Figura 2.22. Funcionamiento Paso a Paso de MPLS L3 VPN.
Reproducida de MPLS - Fundamentals, De Ghein, 2007.**

2.5.4.1. PUEDE MPLS L3 VPN SER SUSCEPTIBLE A UN ATAQUE.

Debido a que el borde de la Red MPLS opera como una Red IP haciendo Routing de los paquetes no es posible que un atacante “inyecte” etiquetas, ya que en el borde no existe soporte del protocolo LDP, además el tráfico es clasificado y separado por VPN en VRF independientes. **(Alvez, 2012, pág. 66)**

En el Core, el tráfico VPN se mantiene separado. La suplantación de identidad maliciosa (intento de obtener acceso a un PE) es casi imposible porque los paquetes de los clientes son paquetes IP. Estos paquetes IP deben recibirse en una interfaz o subinterfaz en particular para que se identifiquen de manera única con una etiqueta VPN. **(Cisco System Inc, 2009, pág. 1013)**

La **Figura 2.23.** muestra que en el ingreso a la Red MPLS no se habla de etiquetas sino de paquetes IP. En el borde de la red MPLS se deben tomar las mismas precauciones que para una arquitectura de red IP como spoofing, DoS, etc.



**Figura 2.23. Posible ataque en redes MPLS VPN.
Reproducida de Fundamentos de MPLS/VPN, Alvez, 2012.**

2.5.4.2. CÓMO PROTEGER EL BACKBONE MPLS.

A. Proteger el intercambio de rutas en la frontera PE/CE:

Optar por rutas estáticas si es posible. Filtrar lo que no haga falta. Aprovechar la presencia de autenticación MD5 en el intercambio. Usar las herramientas que proporciona el protocolo BGP (dampening, filtering, maximum-prefix).

B. Protección de los PE's:

Limitar el número de rutas aprendidas por VRF y por interfaz – Impedir tráfico de control innecesario en la frontera – Eventualmente, activar políticas de QoS para dejar pasar tráfico de control en momentos de congestión lícita o provocada por DoS (Alvez, 2012, pág. 67).

2.5.4.3. RESUMEN DEL FUNCIONAMIENTO DE UNA MPLS L3 VPN.

Recopilando de los puntos abordados se puede mencionar los siguientes:

- A. Los enrutadores P están presentes en el núcleo de la red MPLS; ejecutan protocolos MPLS y no tienen conexión directa con los CE del cliente. Tampoco tienen conocimientos de VPN o VRF.
- B. Los enrutadores PE están en el Borde de la nube MPLS y tienen a un P en un extremo y a un CE del cliente en el otro extremo. Todos los servicios VPN están configurados en los PE. Manejan tablas de enrutamiento separadas. Tabla de enrutamiento de VRF y la tabla de enrutamiento IP Global.
- C. El enrutador CE se coloca en el límite de la red del cliente y no ejecuta MPLS.
- D. Un protocolo IGP (OSPF, EIGRP, IS-IS) se ejecuta entre P y PE, lo que también ayuda en las adyacencias LDP y BGP dentro de la red MPLS VPN.
- E. MP-iBGP se ejecuta solo entre PE's y no en el Core de la Red.
- F. En la conexión entre PE & CE se ejecuta un protocolo IGP como OSPF, EIGRP o un EGP como eBGP.
- G. El RD solo se usa para identificar las rutas VPNv4. Tiene el siguiente formato RD = ASN: No de VRF.
- H. Un RT es una comunidad extendida de BGP que indica qué rutas deben importarse o exportarse desde MP-BGP a la VRF.

- I. Se crea una instancia de VRF para cada VPN del cliente.
- J. Los paquetes se reenvían con dos etiquetas, la etiqueta VPN que indica la red de destino y la etiqueta IGP que contiene la ruta LSP hacia el PE de destino.
- K. El reenvío de paquetes etiquetados y el establecimiento de la ruta LSP se realiza mediante el protocolo LDP.

COMENTARIO FINALES

CAPITULO II.

Según lo visto en el capítulo se evidencia la importancia de la Redes Privadas Virtuales para las empresas y organizaciones, pues estas les permiten que los sitios que están geográficamente distantes tengan conectividad entre ellos y puedan comunicarse y transmitir información relevante.

Aún más importante es MPLS VPN, una de las tecnologías VPN más implementadas en la actualidad, siendo la opción favorita de los ISP para brindar a las empresas y usuarios finales un canal seguro a través de la Internet pública, con flexibilidad y escalabilidad. Con múltiples beneficios no solo para los clientes sino también para los proveedores de servicios.

En el capítulo que sigue se ve a detalle la aplicación práctica de los conceptos abarcados en este capítulo. Se diseñará e implementará en GNS3 una red MPLS L3 VPN para interconectar sitios de una empresa con su sede central.

CAPITULO III: IMPLEMENTACIÓN DE UNA RED MPLS L3 VPN.

Este Capítulo trata del diseño e Implementación de la red MPLS L3 VPN. El diseño toma en consideración los requerimientos de Servicios así como lo relacionado al software donde se implementará. El diseño se divide en 2 partes: lo referente a una infraestructura de red MPLS y el establecimiento de los servicios de L3 VPN sobre esta infraestructura de red.

Como paso final se realiza la validación del diseño de red mediante la emulación de los IOS Cisco en GNS3. Se realizan pruebas de conectividad de servicios VPN, Acceso telnet a los sitios pertenecientes a la VPN y verificación de políticas de QoS aplicadas.

3.1. INTRODUCCION A LAS REDES MPLS L3 VPN.

Las Redes VPN implementadas sobre una arquitectura de red MPLS se pueden llevar a cabo de dos formas: VPN's de Capa 2 y VPN's de Capa 3. Ambos tipos basadas en la red del Proveedor, lo que supone menor trabajo y complejidad para el cliente. Entre ellas encontramos 2 tipos más utilizadas hoy en día por los ISP para brindar servicios de redes privadas virtuales a empresas y/o organizaciones.

- ❖ MPLS L2 VPN. Servicios VPLS (Virtual Private LAN Service). De manera general es una VPN punto a multipunto que conecta en L2 redes LAN remotas.
- ❖ MPLS L3 VPN. Conocida como BGP/MPLS VPN por el uso del protocolo BGP para anunciar rutas VPNv4 entre PE's y MPLS para el envío de paquetes en el Backbone del ISP. **(Semeria, 2001, pág. 6)**

Este trabajo aborda MPLS L3 VPN debido a que simplifica las operaciones de red para los clientes y al mismo tiempo permite que los ISP ofrezcan servicios escalables, flexibles y de valor agregado. Entre los múltiples beneficios que brinda MPLS L3 VPN, tanto para el cliente como para los ISP, están los siguientes:

- + No hay restricciones en el plan de direcciones IP utilizado por cada cliente de VPN. Diferentes clientes pueden tener rango de direcciones superpuestos.
- + El enrutador CE en cada sitio no intercambia directamente información de enrutamiento con otro CE. Esto permite a los clientes no lidiar con problemas de enrutamiento entre sitios pues estos son responsabilidad del ISP.
- + Los clientes no necesitan acceso a los enrutadores PE o P y los ISP no requieren administración de CE. Cada parte se encarga de su propio trabajo.
- + Se puede brindar diferentes opciones de QoS según las necesidades tanto en la red del ISP como al cliente en específico
- + Los proveedores de servicios pueden usar una infraestructura común para brindar servicios de conectividad VPN e Internet. **(Semeria, 2001, pág. 11)**

El diseño de red de este trabajo se centra en los servicios VPN entre sitios.

3.2. SOFTWARE GNS3.

Para poder implementar el diseño de red MPLS L3 VPN se hará uso de la herramienta GNS3, que permite emular dispositivos de redes a partir de IOS Cisco y por ende topologías completas sin la implementación de hardware que suele ser complicado y/o costoso de obtener. De esta forma se logran resultados y pruebas similares a los que se obtendrían en una topología de red real.

GNS3 es utilizado por cientos de miles de ingenieros de redes en todo el mundo para emular, configurar, probar y solucionar problemas de redes virtuales y reales. GNS3 le permite ejecutar una pequeña topología que consta de pocos dispositivos a topologías grandes con muchos dispositivos alojados en múltiples servidores o incluso alojados en la nube. (SolarWinds Worldwide, 2022)

3.2.1. SOBRE EL PROGRAMA GNS3.

GNS3 es un software gratuito de código abierto que puede descargarse libremente. Ha existido por más de 10 años y se desarrolla activamente por una comunidad creciente de más de 800,000 miembros. Originalmente solo emulaba dispositivos Cisco, pero ahora ha evolucionado y admite muchos dispositivos de múltiples proveedores de redes. (Telectronika, 2022)

GNS3 admite dispositivos emulados y simulados, términos que no significan lo mismo, como se explica a continuación:

- **Emulación:** GNS3 imita o emula el hardware de un dispositivo y ejecuta imágenes reales en el dispositivo virtual. Por ejemplo, puede copiar el Cisco IOS de un Router Cisco real y ejecutarlo en un Router Cisco virtual en GNS3.
- **Simulación:** GNS3 simula las características y funcionalidades de un dispositivo como un Switch Cisco. No ejecuta el sistema operativo real, sino un dispositivo que simula el funcionamiento de un Switch L2 o L3 real el cual viene incorporado en GNS3. (SolarWinds Worldwide, 2022)

En nuestro caso lo que haremos es emular los Routers cisco ejecutando IOS reales con la ayuda de GNS3 para configurar los equipos y así poder implementar los servicios de L3 VPN tal como lo estuviésemos haciendo con equipos físicos.

En la **Figura 3.1.** se observan los diferentes equipos utilizados en GNS3 para crear topologías de red. Entre ellos están los Routers (parte superior) los cuales emulan los IOS Cisco de equipos reales y los Switches (parte Intermedia) que vienen por defectos para simular el funcionamiento de Switches Cisco. Luego están (parte inferior) dispositivos de uso específico como PC o nube para Internet.

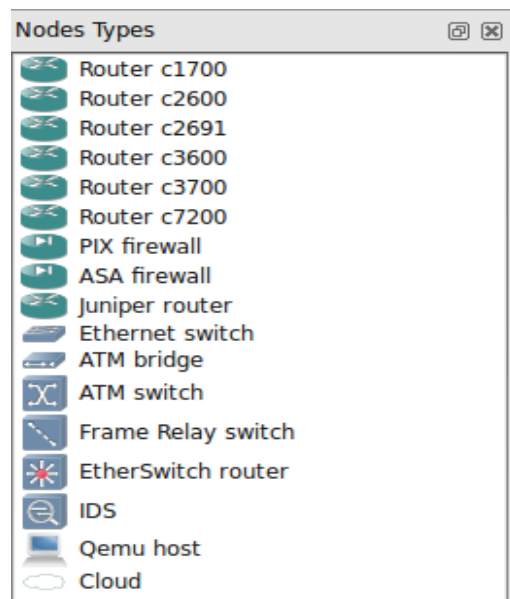


Figura 3.1. Equipos Emulados y Simulados en GNS3.
Fuente Propia con Datos Obtenidos de Software GNS3 2.2.31, www.gns3.com.

3.2.2. CARACTERISTICAS DE GNS3.

GNS3 consta de dos componentes de software:

3.2.2.1. GNS3 ALL IN ONE (TODO EN UNO).

Es el software cliente de GNS3 que se instala en la PC. Es la interfaz gráfica de usuario (GUI) donde se crean y emulan/simulan las topologías de red. Es un programa que requiere de otros programas, pero estos ya vienen integrados en un paquete listos para ser instalados en una sola ocasión. **(Telectronika, 2022)**

Un ejemplo de las topologías de redes que se crean en GNS3 es el que aparece en la **Figura 3.2.** que muestra una topología de red que puede ser emulada o simulada dependiendo del uso de equipos específicos. En ella se aprecian Router (Emulan) Switches L2 y L3 (Simulan) y dispositivos específicos para usos varios como pueden ser una PC, una Máquina Virtual y hasta conectar a internet la red.

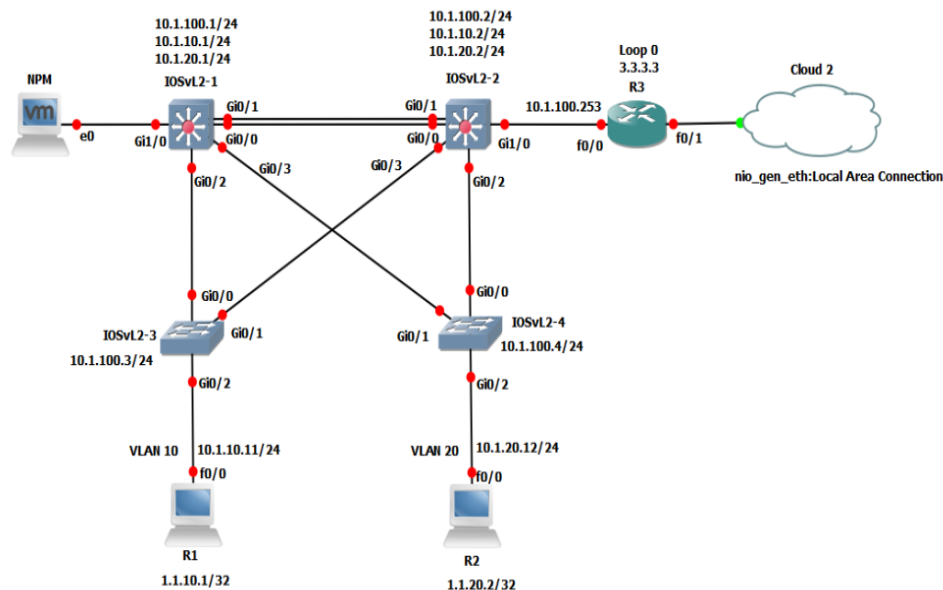


Figura 3.2. Topología de Red en GNS3.
Reproducida de GNS3 Getting Started, docs.gns3.com/docs, 2022.

3.2.2.2. MAQUINA VIRTUAL (VM) GNS3.

Cuando se crean topologías en GNS3 los dispositivos creados deben estar alojados y ejecutados en un servidor. Las opciones para este servidor son:

- ✓ **Servidor GNS3 local.** Se ejecuta localmente en el mismo PC donde se instaló el software All-in-One GNS3.
- ✓ **Máquina Virtual GNS3 local.** Se ejecuta localmente en la PC mediante software de virtualización como VMware Workstation, VirtualBox o Hyper-V.
- ✓ **Máquina Virtual GNS3 remota.** Haciendo uso de un servidor mediante VMware ESXi o incluso en la nube. (SolarWinds Worldwide, 2022)

La **Figura 3.3.** muestra una Máquina Virtual GNS3 (GNS3 VM). En este caso en particular una basada en VMware Workstation, que es la opción recomendada en el sitio web oficial gns3.com, y que aloja el servidor GNS3 (que no es más que un

Ubuntu Linux) donde se corren todos los dispositivos. En ella se aprecian los datos para acceder remotamente y vía web si así se desea.

```
GNS3 server version: 2.2.31
Release channel: 2.2
VM version: 0.13.0
Ubuntu version: focal
Qemu version: 4.2.1
Virtualization: vmware
KVM support available: True
Uptime: up 0 minutes

IP: 192.168.142.128 PORT: 80

To log in using SSH: ssh gns3@192.168.142.128
Password: gns3

To launch the Web-Ui: http://192.168.142.128

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

**Figura 3.3. GNS3 VM 2.2.31 basada en VMware Workstation.
Fuente Propia con Datos Obtenidos de Software VMware Workstation 16.**

3.2.3. BENEFICIOS Y LIMITACIONES DE GNS3.

GNS3 no es el único software para emular/simular equipos de red (Packet Tracer, Cisco VIRL, EVE, etc.) pero es el que más funcionalidades y opciones ofrece, además es gratuito, está en constante actualización y es fácil de instalar ya que viene en formato All-in-One por lo que no se necesita de otro software para ejecutarlo. Entre los beneficios y limitaciones de GNS3 están los siguientes:

3.2.3.1. VENTAJAS.

- ✚ Software libre y de código abierto.
- ✚ Sin tarifas de licencia mensuales o anuales.
- ✚ No hay limitación en el número de dispositivos compatibles (la única limitación es su hardware: CPU y memoria).
- ✚ Soporta múltiples opciones de Switches. (módulo NM-ESW16 Etherswitch, imágenes IOU/IOL Layer 2, VIRL IOSvL2).
- ✚ Soporta todas las imágenes VIRL (IOSv, IOSvL2, IOS-XRv, CSR1000v, NX-OSv, ASA).

- ✚ Soporta entornos de múltiples proveedores. Se ejecuta con o sin hipervisores.
- ✚ Soporta hipervisores gratuitos y de pago (VirtualBox, VMware Workstation, VMware player, ESXi, Fusion).
- ✚ Comunidad grande y activa (más de 800,000 miembros).
- ✚ Soporte nativo para Linux sin necesidad de software de virtualización adicional. **(Telectronika, 2022)**

3.2.3.2. DESVENTAJAS.

- ✚ Las imágenes de Cisco deben ser suministradas por el usuario (descarga de cisco.com u otro sitio web, comprar licencia VIRT, o copiar desde el dispositivo físico).
- ✚ No es un paquete autónomo, pero requiere una instalación local de software (GUI) por parte del usuario.
- ✚ GNS3 puede verse afectado por la configuración y las limitaciones de la PC debido a la instalación local (firewall y configuración de seguridad, políticas de la empresa, etc.). **(SolarWinds Worldwide, 2022)**

3.2.4. REQUISITOS PARA INSTALAR GNS3.

Según el sitio web oficial del fabricante (gns3.com), GNS3 es compatible con los sistemas operativos Windows, MacOS y Linux. Las **Tablas 3.1. - 3.3.** muestran los requisitos de instalación de GNS3 en Windows con un breve comentario.

**Tabla 3.1. Requisitos Mínimos de Instalación GNS3.
Adaptada de GNS3 - Guía Introductoria, telectronika, 2022.**

Ítems	Requisitos Mínimos.
Sistema Operativo	Windows 7 (64 bit) o Superior.
Procesador	2 o Más núcleos lógicos.
Virtualización	Se requieren que tenga habilitada la virtualización en su PC.
Memoria	4 GB RAM
Espacio en Disco	1GB de espacio disponible (la instalación es < 200MB).
Comentarios	Es posible que necesite almacenamiento adicional para las imágenes de los equipos de red.

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

**Tabla 3.2. Requisitos Recomendados de Instalación GNS3.
Adaptada de GNS3 - Guía Introductoria, telectronika, 2022.**

Ítems	Requisitos Recomendados.
Sistema Operativo	Windows 7 (64 bit) o Superior.
Procesador	4 o más núcleos lógicos – AMD-V/RVI Series o Intel VT-X/EPT
Virtualización	Se requieren que tenga habilitada la virtualización en su PC.
Memoria	16 GB RAM
Espacio en Disco	Disco de Estado Sólido (SDD). 35 GB de espacio disponible
Comentarios	La virtualización de dispositivos consume mucho procesador y memoria, por lo tanto, mas es mejor. Tener en cuenta si el dispositivo configurado correctamente supera la RAM y la potencia de procesamiento.

**Tabla 3.3. Requisitos Óptimos de Instalación GNS3.
Adaptada de GNS3 - Guía Introductoria, telectronika, 2022.**

Ítems	Requisitos Óptimos.
Sistema Operativo	Windows 7 (64 bit) o Superior.
Procesador	Core i7 o i9 Intel CPU. R7 o R9 AMD CPU. 8 o más núcleos lógicos – AMD-V/RVI Series o Intel VT-X/EPT
Virtualización	Se requieren que tenga habilitada la virtualización en su PC.
Memoria	32 GB RAM
Espacio en Disco	Disco de Estado Sólido (SDD). 80 GB de espacio disponible
Comentarios	La virtualización de dispositivos consume mucho procesador y memoria, por lo tanto, mas es mejor. Tener en cuenta si el dispositivo configurado correctamente supera la RAM y la potencia de procesamiento.

3.3. DISEÑO DE UNA MPLS L3 VPN.

El diseño de la VPN de capa 3 sobre MPLS parte de los requerimientos de servicio que el cliente brinda al personal correspondiente de un ISP (no se tiene a un cliente específico pero el diseño aplica para cualquier cliente que necesite un L3 VPN). Luego se eligen las imágenes y equipos de red necesarios para implementar el diseño en GNS3. Después se plantea un ejemplo de una infraestructura de red MPLS de un ISP que brinde servicios de VPN. Por último se realiza una asignación de direcciones IP para la topología de red L3 VPN que se llevará a cabo.

3.3.1. REQUERIMIENTOS DE SERVICIO.

3.3.1.1. NECESIDADES DEL CLIENTE.

El cliente (IDAI, por asignar un nombre) cuenta una Casa Matriz y con 3 sucursales geográficamente separadas entre sí, quiere que las sucursales tengan conectividad con su Casa Matriz y a la misma vez entre ellas mediante una VPN L3 que le brinde privacidad y seguridad a sus comunicaciones y transacciones. Los detalles de los requerimientos de servicio se enumeran a continuación:

- ✚ Para cada Sucursal necesita un ancho de banda de 20Mbps para el tráfico interno. Esto según los datos de consumo de la LAN en horas pico.
- ✚ Desea que a Casa Matriz se le brinde enlaces de datos redundantes mediante Fibra Optica.
- ✚ Para el enlace principal de Datos de Casa Matriz requiere un BW de 80Mbps, (BW de las sucursales + CM 20Mbps), y 60Mbps para el enlace de respaldo.

3.3.1.2. CONSIDERACIONES INICIALES.

El tipo de tráfico entre las sucursales y casa matriz puede ser diverso desde voz, datos, video, acceso a sistemas de la empresa e inclusive de internet. Por lo que el implementar la VPN sobre una infraestructura de red eficiente como MPLS es de suma importancia, ya que permite mantener clases de servicio para cada tipo de tráfico y soporta con gran eficacia la creación de VPN.

Los datos de BW planteados anteriormente se dan por sentado y se asume que están basados en un cálculo de ancho de banda de acuerdo al consumo de red de cada sucursal. La parte del cálculo de BW de la red no se considera en este diseño, ya que el objetivo del mismo es la interconexión de las sitios remotos por medio de una MPLS L3 VPN y no abarca el diseño de una red LAN.

De los requerimientos de servicio se tienen los siguientes puntos a considerar:

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

- ❖ La VPN será site to site con topología Full Mesh para que las sucursales se comuniquen entre ellas sin pasar por un Hub Site. (como se vio en capítulo II).
- ❖ La última milla para los enlaces de datos de cada sitio (sucursal y casa matriz) se realizará por conexión directa entre PE-CE en GNS3.
En un ambiente real la última milla puede pasar por una red de varios equipos y podría ser entregada por RADIO/FO dependiendo de la cobertura del ISP.
- ❖ Para la redundancia de los enlaces de datos de Casa Matriz la última milla se conectará de diferentes PE´s para garantizar correctamente la redundancia.
- ❖ El servicio de Datos (VPN) será entregado en un Router (CE) que servirá como Gateway para la red interna de cada sucursal.

La **Tabla 3.4.** nos resume la asignación de recursos de BW para los enlaces de Datos tanto para Casa Matriz como para las sucursales.

**Tabla 3.4. Asignación de Recurso de BW para Enlaces del Cliente.
Fuente Propia con Datos Propios.**

Ítems	Casa Matriz	Sucursales
Datos Principal	80 Mbps	20 Mbps
Datos Respaldo	60 Mbps	N/A

3.3.2. ELECCION DE EQUIPOS E IMAGENES PARA USO EN GNS3.

Visto en el Capítulo II, una Red MPLS L3 VPN está compuesta por 2 partes: la red C del Cliente y la Red P del Proveedor de Servicios. En base a esto se realizará la elección de equipos de red y Cisco IOS a utilizar en GNS3 para cada parte.

3.3.2.1. RED C DEL CLIENTE.

Debido a que en la red del cliente no es necesario de equipos con funcionalidades MPLS, se utilizaran los Routers Cisco de la serie 3700 para las sucursales y casa matriz. El IOS a utilizar es la imagen tipo Mainline c3725-adventerprisek9-mz.124-25d.image, la cual es una de las imágenes estables y recomendadas por el sitio gns3.com para usarse en GNS3. **(SolarWinds Worldwide, 2022)**

La **Figura 3.4.** muestra la apariencia de un Router Cisco 3725, donde se aprecia la parte frontal y trasera del equipo. Este tipo de Router puede ser utilizado para redes pequeñas a medianas brindando buen rendimiento.



Figura 3.4. Equipo Cisco 3725.

Reproducida de www.ricardo.ch/de/a/cisco-3725-3700-series-with-nm-pri-1ce1b-1094348522/, 2022.

3.3.2.2. RED P DEL PROVEEDOR.

Para los equipos de la red MPLS se han escogido Routers cisco de la serie 7000 los cuales soportan el reenvío de paquetes etiquetados y son robustos para ser parte del Core MPLS ya que este Router 7200 tendrá funcionalidades de PE y P, así como de Route Reflector RR. Se utilizará la imagen tipo Mainline c7200-advipservicesk9-mz.152-4.S5.image en su versión 15.

La **Figura 3.5.** muestra un ejemplo del Router Cisco 7200 a utilizarse como equipo Borde/Core en la Red MPLS. Este Router se usa en redes en producción de ISP.



Figura 3.5. Equipo Cisco Serie 7000.

Reproducida de Cisco 7200 Series Routers - Cisco, 2022.

3.3.2.3. SERVIDOR GNS3 VM PARA CORRER LOS IOS.

Como se vio en el inciso [3.1.2.2](#) de este capítulo es necesario correr los IOS de los Routers en un servidor; ya sea local, remoto o en una máquina virtual de GNS3. La opción recomendada es esta última (Máquina Virtual) utilizando VMware como software de virtualización pues brinda mejor rendimiento que la opción de VirtualBox. (SolarWinds Worldwide, 2022)

Esta máquina virtual (GNS3 VM) se ha descargado desde el sitio [Software | GNS3](#) según la versión de GNS3 y se ejecuta sobre VMware Workstation 16. La configuración de la GNS3 VM se setea en base a la cantidad de Routers a utilizar y la memoria RAM que estos demandan. Se tienen 9 Routers 7200 que consumen 512MB de RAM + 4 Routers 3725 que consumen 128MB de RAM, la suma de estos da alrededor de 5GB de RAM a máximo consumo de los Routers. Pudiendo asignarlos con un computadora que cuenta con 8GB mínimo de RAM.

Los datos mencionados en el párrafo anterior los brinda GNS3 al momento de crear las plantillas para los Routers y cargar los IOS Cisco, por defecto GNS3 no provee las imágenes de los equipos y es necesario realizar esto para poder utilizar dispositivos de capa 3. La **Figura 3.6.** muestra los datos una vez son creadas las plantillas de Routers en GNS3. Para cada imagen cisco se crea un perfil con los datos de consumo de RAM, tipo de imagen y las interfaces ethernet que tiene.

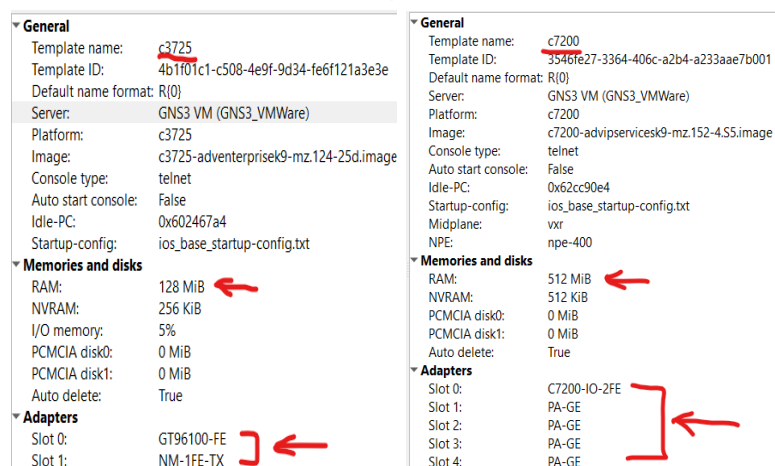


Figura 3.6. Creación de Plantilla para Router Cisco en GNS3.
Fuente propia con datos obtenidos del Software GNS3 versión 2.2.31.

En el inciso [3.1.4](#) de este capítulo se mencionan los requisitos recomendados para instalar GNS3 en Windows, de allí se asigna de los recursos físicos de la computadora (Core e Hilos del procesador) la cantidad de 6 procesadores para la GNS3 VM para que no haya problemas de rendimiento (importante utilizar una PC con suficiente hardware). Los datos de la GNS3 VM se muestran en la ***Figura 3.7.*** el espacio utilizado en disco y los otros datos son asignados automáticamente.

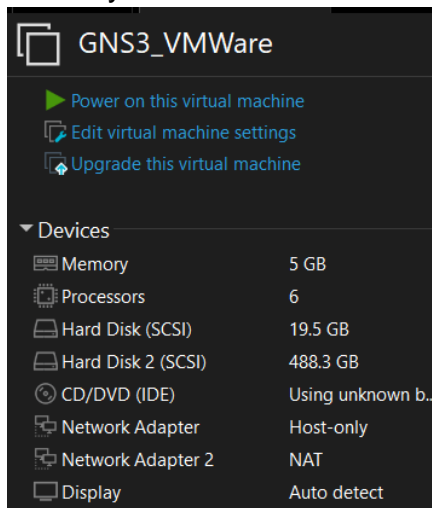


Figura 3.7. Ajustes de la GNS3 VMware.

Fuente propia con datos obtenidos del Software VMware Workstation 16.

3.3.3. TOPOLOGIA DE RED MPLS L3 VPN.

Luego de haber elegido los equipos de red a utilizar en GNS3 se establecerán las bases de diseño para la red MPLS L3 VPN. Primero se abordarán los puntos necesarios para que una infraestructura de red MPLS brinde servicios y luego lo referente a los enlaces de datos de cada sitio que pertenecen a la VPN del cliente.

3.3.3.1. RED MPLS PE y P.

En el capítulo II se vio que una red MPLS L3 VPN se construye a base de Router P (Core) y Router PE (Borde). Esta topología de red consta de 4P's, 4PE's y 1RR (Reflector de Rutas). Para que una red MPLS pueda brindar servicios es necesario de: un protocolo IGP de la red (Borde y Core), protocolos MPLS-LDP en los Routers (Borde y Core) y del protocolo MP-iBGP que correrán los PE's (Borde).

El protocolo IGP no puede ser BGP, pues en una Red MPLS lo que se busca es que el Core sea libre de BGP por la gran cantidad de rutas que este protocolo maneja y la carga que esto supone para los equipos. Además los P's conmutan paquetes basados en etiquetas y no en IP-destino por lo que no se necesita específicamente de BGP para alcanzar redes remotas. **(De Ghein, 2007, pág. 8)**

Se utiliza OSPF (puede usarse otro) porque es un protocolo no patentado que es compatible con VLSM, opera muy bien en topología de malla semicompleta como la que se creará en el Core de la red (que une a los 4P) y permite aplicar costos a interfaces que se utilizará para balancear el tráfico en el Core, de tal forma que el tráfico fluya en el sentido que los costos OSPF lo establezcan. **(sshaim, 2022).**

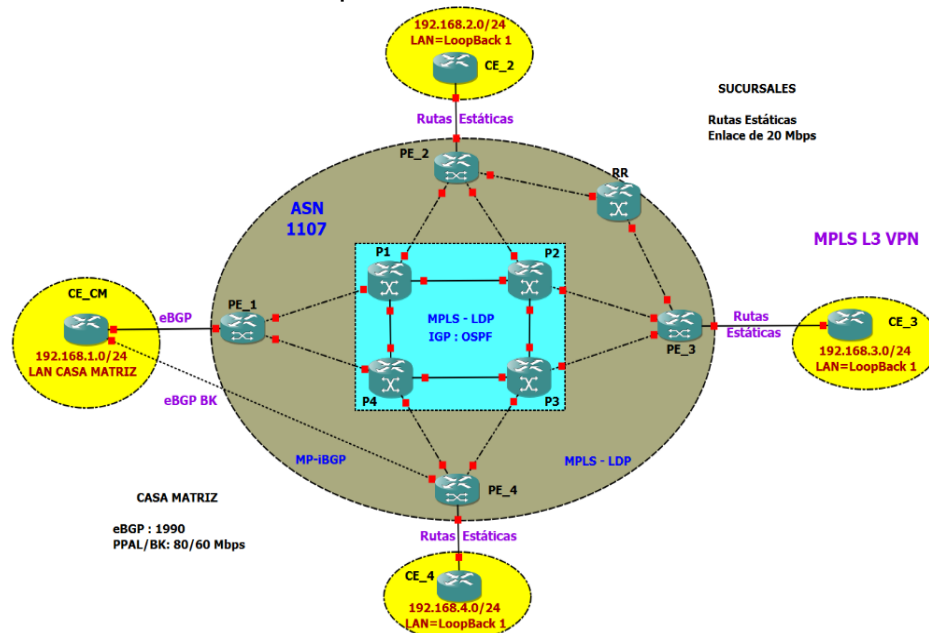
MPLS se habilitará en los P y PE así como en las interfaces que sean parte de la red. Se utilizará LDP para el intercambio de etiquetas entre Routers y el establecimiento del camino virtual LSP. Cada PE tendrá redundancia en su conexión con el P correspondiente, de modo que exista redundancia y así se garantice que el diseño de red sea tolerante a fallas. **(De Ghein, 2007, pág. 32)**

Los PE's levantarán sesiones MP-iBGP hacia los RR para el intercambio de prefijos VPNv4. Un RR es necesario ya que elimina el hecho que cada PE establezca un Full Mesh iBGP hacia los PE's que sean parte de la red (mismo AS), es decir la creación de una malla completa de conexiones lógicas por cada PE. Pues para cumplir con el mecanismo de prevención de Loops del protocolo BGP cada PE debe levantar una sesión iBGP con los demás PE's. **(De Ghein, 2007, pág. 197)**

Con el uso de RR todas estas sesiones iBGP se reducen disminuyendo la carga en los equipos ya que cada PE solo levanta una sesión iBGP con el RR para crear el Full Mesh MP-iBGP. Por ejemplo, si se tiene una red con n PE's, cada PE tiene $n-1$ peer iBGP y existen $n*(n-1)/2$ sesiones iBGP en total. En este caso, con 4 PE's cada PE tendrá 3 peer iBGP y existirán 6 sesiones iBGP en total, no

parecería necesario utilizar RR ya que con él se tienen 4 sesiones iBGP (diferencia de 2). Pero en redes de ISP este no es el caso (4 PE´s) por tal razón se toma en cuenta el RR. (De Ghein, 2007, pág. 198)

La **Figura 3.8.** plantea el diseño de Red MPLS L3 VPN que interconecta las 3 sucursales del cliente IDAI con su Casa Matriz. Las sucursales levantan una VPN de capa 3 con Casa Matriz a través de la Red MPLS del ISP. La figura muestra los requerimientos de BW del cliente para cada sitio VPN, así como los tipos de enrutamientos a llevar a cabo para los enlaces PE-CE.



**Figura 3.8. Esquema de la red MPLS L3 VPN.
Fuente Propia con Datos Obtenidos de Software GNS3 2.2.31.**

3.3.3.2. LINK PE - CE.

Para levantar el link entre la red del cliente y la red del ISP se escogerá el enrutamiento estático para la conexión PE-CE de las sucursales. Las razones de esto son las siguiente: los enlaces no cuentan con redundancia y son redes relativamente pequeñas con solo una ruta de salida hacia el ISP por lo que no es necesario un protocolo de enrutamiento dinámico, de este modo se realizan buenas prácticas de administración de red haciendo un buen uso de los recursos. (De Ghein, 2007, pág. 207)

Para los link entre el CE de Casa Matriz y sus PE´s correspondientes se utilizará enrutamiento dinámico debido a que existe redundancia en los enlaces y la convergencia ante cualquier cambio en la red debe ser lo más rápida posible. Se levantará una sesión eBGP para el enlace de datos principal y respaldo, cada uno hacia un PE diferente. Se usa BGP porque cuenta con atributos que pueden ser aplicados a los peer para establecer la redundancia, además es adaptable para enrutar prefijos dentro y fuera del mismo AS. (Wallace, 2015, pág. 549)

Se simularán las redes LAN de los sitios (sucursales y casa matriz) levantando interfaces Loopback en los Router CE de cada sitio. Esto para evitar añadir más equipos a la topología que conlleve en más consumo de recursos, no obstante los resultados con el uso de loopback serán los mismos que agregando un Switch y PC´s que representen la LAN de cada sitio.

3.3.4. ASIGNACION DE DIRECCIONES IP – IP PLAN.

Esta parte consiste en asignar rango de direcciones privadas a la LAN y WAN de cada sitio, así como a los link L3 y loopback de los equipos de red MPLS.

3.3.4.1. LAN DE LOS ENLACES DE DATOS.

Se asignará un rango de direcciones /24 para la red interna de cada sitio. Esto le proporcionará un espacio de direcciones utilizables de hasta 254 IP´s para hosts. Este dato se obtiene de restar a 32 (longitud de Dirección IPv4) el valor de la máscara de red (/24), luego las base 2 se eleva a este resultado y por último a este valor se le resta 2 (dirección de red y máscara que no pueden ser asignadas). (ODOM, 2020, pág. 273) como se muestra a continuación:

Tomando como ejemplo la red **192.168.1.0/24**, el procedimiento sería: $2^{(32-24)} - 2 = 2^8 - 2 = 256 - 2 = 254$ IP´s. Suficientes para una red LAN pequeña a mediana. La asignación de las direcciones IP que se configurarán en las interfaces Loopback de los Router CE se muestra en la **Tabla 3.5.**

**Tabla 3.5. Rango de IP para las LAN de Cada Sitio.
Fuente Propia con Datos Propios.**

Sitio	Direccionamiento LAN
Casa Matriz CM	192.168.1.0/24
Sucursal S1	192.168.2.0/24
Sucursal S2	192.168.3.0/24
Sucursal S3	192.168.4.0/24

3.3.4.2. WAN DE LOS ENLACES DE DATOS.

Estos son los links entre cada PE con su respectivo CE de cada sitio (sucursal y casa matriz). Para esto únicamente necesitamos 2 direcciones IP que se asignan a cada interfaz en los extremos del link, se asignarán subredes /30 que permiten 2 IP-utilizables (siguiendo el procedimiento en el inciso anterior). (ODOM, 2020, pág. 274)

De este modo serian 5 subredes /30, 3 para sucursales más 2 de casa matriz (Enlace de Datos principal y respaldo) tal como se plasman en la **Tabla 3.6.**

**Tabla 3.6. Rango de IP para los Enlaces WAN.
Fuente Propia con Datos Propios.**

Link PE-CE	Direccionamiento WAN
PE_1 – CE_CM Principal	10.10.100.0/30
PE_4 – CE_CM Respaldo	10.10.100.4/30
PE_2 – CE_S2	10.10.100.8/30
PE_3 – CE_S3	10.10.100.12/30
PE_4 – CE_S4	10.10.100.16/30

3.3.4.3. DIRECCIONAMIENTO DE LA RED MPLS.

El Core MPLS está compuesto por una malla semi completa entre los Routers P1-P4. Los PE's se conectan a los P's con enlaces redundantes así como también el RR está en redundancia con 2 PE's ante posible fallo de algún enlace. Para la asignación de IP's a los enlaces L3 en el Core y Borde MPLS se tomará un rango de direcciones /26 y se subneteará aplicando VLSM para sacar las subredes /30 de los 14 enlaces .

- ✚ Teniendo la red 10.10.10.0/26, la cantidad de IP-utilizables es igual a: $2^{(32-26)} - 2 = 2^6 - 2 = 64 - 2 = \underline{62}$. El rango de direcciones IP contando la subred cero sería de la IP de red **10.10.10.0/26** hasta la máscara de red **10.10.10.63/26**.
- ✚ Para saber si de esta red 10.10.10.0/26 se pueden sacar las 14 subredes /30 para los enlaces de los equipos restamos ambas máscaras de las subredes y luego se eleva 2 a esa cantidad, de la siguiente forma: $2^{(30-26)} = 2^4 = \underline{16}$.
- ✚ El resultado de 16 nos funciona ya que es mayor a las 14 subredes /30 que necesitamos, el rango sería de la subred **10.10.10.0/30** a la **10.10.10.52/30**.
(ODOM, 2020, pág. 281)

En la **Tabla 3.7.** se ve la asignación de estas subredes /30 a cada enlace entre los Routers del Core y de Borde de la red MPLS (de un ISP).

**Tabla 3.7. Rango de IP para los Enlaces Red MPLS.
Fuente Propia con Datos Propios.**

Enlace	Subred	Enlace	Subred
P1 – P2	10.10.10.0/30	P2 – PE_3	10.10.10.28/30
P1 – P4	10.10.10.4/30	P3 – PE_3	10.10.10.32/30
P2 – P3	10.10.10.8/30	P3 – PE_4	10.10.10.36/30
P3 – P4	10.10.10.12/30	P4 – PE_4	10.10.10.40/30
P1 – PE_1	10.10.10.16/30	P4 – PE_1	10.10.10.44/30
P1 – PE_2	10.10.10.20/30	PE_2 – RR	10.10.10.48/30
P2 – PE_2	10.10.10.24/30	PE_3 – RR	10.10.10.52/30

3.3.4.4. HABILITACIÓN DE LOOPBACK 0.

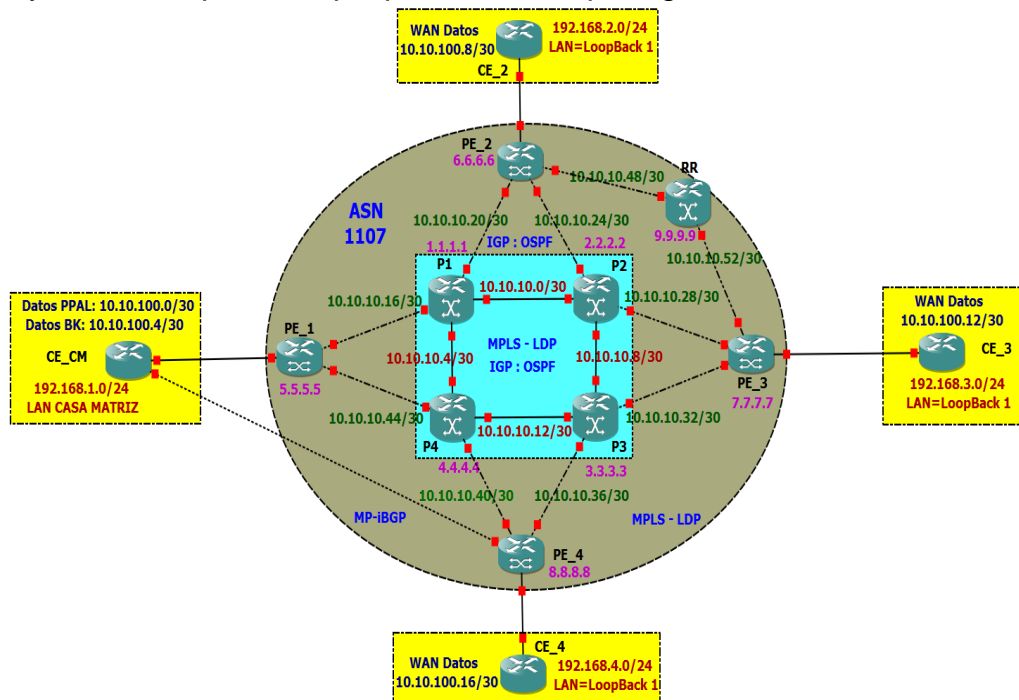
Se habilitará la interface Loopback 0 en los Router PE, P y RR para que sea la interface que los protocolos OSPF, LDP y BGP elijan para intercambiar información con sus Peers, de modo que se evite que cada protocolo escoja una interface del Router (según su algoritmo) que no pueda ser utilizada. Esto dado que los Peers no se levantan con redes directamente conectadas (LDP y BPG).

En la **Tabla 3.8.** se encuentran la direcciones asignadas a la loopback 0 para cada Router. La subredes son /32 pues únicamente se necesita de una IP utilizable.

**Tabla 3.8. Direccionamiento para Loopback 0 de Equipos MPLS.
Fuente Propia con Datos Propios.**

Equipo	Router	Loopback0	Router	Loopback0
Core	P1	1.1.1.1/32	P3	3.3.3.3/32
	P2	2.2.2.2/32	P4	4.4.4.4/32
Borde	PE_1	5.5.5.5/32	PE_3	7.7.7.7/32
	PE_2	6.6.6.6/32	PE_4	8.8.8.8/32
Otro	RR	9.9.9.9/32		

La **Figura 3.9.** muestra la asignación de direcciones IP para los enlaces de datos (LAN y WAN) de cada sitio de la VPN y para los link L3 entre Routers MPLS (incluyendo la loopback 0 que puede usarse para gestión remota de los Routers).



**Figura 3.9. Asignación de Direcciones IP a Redes LAN y a Link L3 MPLS.
Fuente Propia con Datos Obtenidos de Software GNS3 2.2.31.**

3.4. IMPLEMENTACION DEL DISEÑO EN GNS3.

La implementación se lleva a cabo en el software GNS3 en su versión 2.2.31, los IOS Cisco se ejecutan en la máquina virtual VMware - GNS3 VM. Los Router Cisco corren la versión 12 (sucursales) y 15 (Router MPLS P y PE). El software de línea de comando CLI que se utiliza para gestionar los Routers es Secure CRT versión

8.1.4. Las configuraciones que se realizan a continuación parten asumiendo que los ajustes básicos del Router ya están establecidos.

3.4.1. CONFIGURACION DE LA RED MPLS.

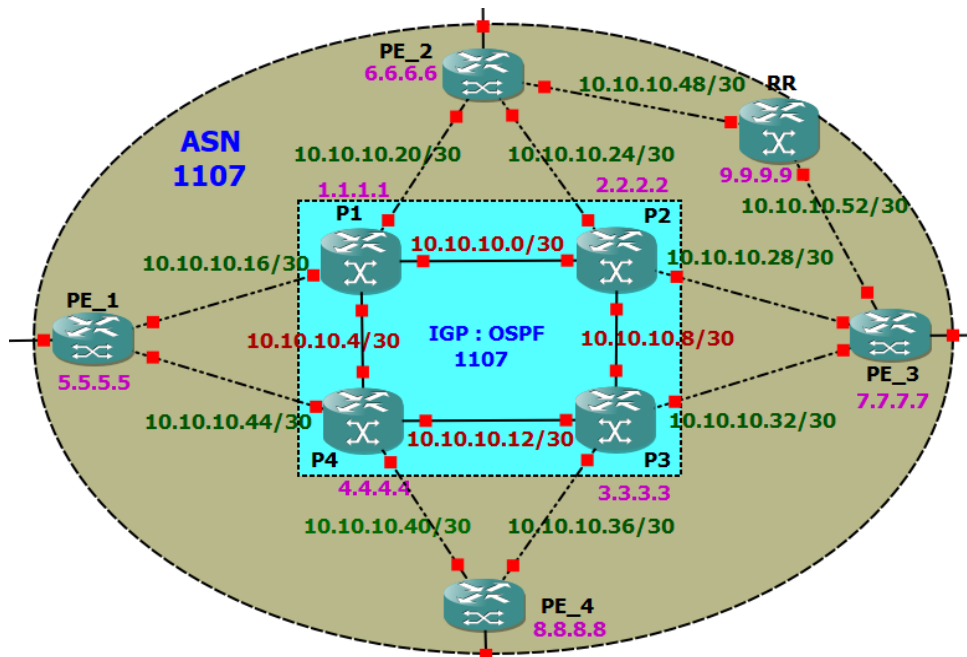
Las configuraciones se dividen en 4 puntos: primero implementar OSPF como protocolo IGP de la red, luego habilitar MPLS - LDP para que los Router puedan reenviar paquetes etiquetados, después establecer el Full Mesh MP-iBGP de los PE's con el RR para que intercambien prefijos VPNv4 y por último balancear la carga en el Core de la red MPLS como medida anti congestión.

3.4.1.1. HABILITACION DE OSPF COMO PROTOCOLO IGP.

La arquitectura MPLS, vista en el capítulo I, permite que en el Core de la red se haga conmutación de paquetes basado en etiquetas y en el Borde enrutamiento tradicional basado en paquetes IP. Esto se conoce como Routing en el Borde y Switching en el Núcleo, funciones híbridas de capa 2 y capa 3 del modelo OSI.

Esta característica de MPLS permite que en el Core de la red no sea necesario implementar BGP (que puede enrutar prefijos y etiquetas a la vez) como protocolo IGP. Esto libera carga y recursos en los Router del Core ya que no tienen que procesar la gran cantidad de rutas de internet que maneja BGP, pudiendo utilizar otro protocolo IGP como EIGRP u OSPF (este caso) que brinde la plataforma de enrutamiento y conectividad de la red que los protocolos LDP y BGP necesitan que exista para el establecimiento de los Peers. **(De Ghein, 2007, págs. 9,33)**

La **Figura 3.10.** muestra los equipos a implementar OSPF (Routers Core y de Borde) como IGP con la IP de la interfaz Loopback 0 como Router-id del proceso OSPF 1107. Este valor (1107) es el ID que se le asigna al proceso OSPF y lo identifica de otros procesos que estén corriendo en el Router, tiene que ser único y puede ser un numero tomado entre 1 – 65535. **(ODOM, 2020, pág. 472)**



**Figura 3.10. Habilitación de OSPF como Protocolo IGP de la Red.
Fuente Propia con Datos Obtenidos de Software GNS3 2.2.31.**

3.4.1.1.1. CONFIGURACION DE OSPF 1107.

Primero se deben levantar los Link L3 entre los Routers y la interfaz loopback0, pues estas serán las redes que se anuncian y se comparten con los vecinos OSPF. La **Figura 3.11.** muestra las configuraciones en P1 para la subred 10.10.10.0/30 y su loopback (1.1.1.1/32), Esta configuración hay que aplicarla en las interfaces de los Router con su correspondiente información de subred y loopback 0.

<pre>interface GigabitEthernet1/0 description HACIA P1_Gi1/0 ip address 10.10.10.2 255.255.255.252 no shutdown</pre>	<pre>interface Loopback0 description MPLS_LABEL ip address 1.1.1.1 255.255.255.255 no Shutdown</pre>
--	--

**Figura 3.11. Configuración de Link L3 entre los Routers.
Fuente Propia con Datos Obtenidos de CCNA 200-301 Cert Guide, 2020.**

Luego se habilita OSPF, la **Figura 3.12.** muestra la configuración necesarias. El valor 1107 es el ID del proceso OSPF y puede ser el mismo que el número de sistema autónomo ASN que la IANA asigna a un ISP. La Figura muestra la configuración para el P1 (Izquierda) y PE_3 (Derecha) donde se anuncian las redes conectadas a los Router. Esta configuración hay que replicarla en todos los Routers con la información de las redes conectadas a ellos. (ver **Figura 3.10.**).

```

router ospf 1107
router-id 1.1.1.1
log-adjacency-changes
network 1.1.1.1 0.0.0.0 area 0
network 10.10.10.0 0.0.0.3 area 0
network 10.10.10.4 0.0.0.3 area 0
network 10.10.10.16 0.0.0.3 area 0
network 10.10.10.20 0.0.0.3 area 0
network 10.10.10.56 0.0.0.3 area 0
!
router ospf 1107
router-id 3.3.3.3
log-adjacency-changes
network 3.3.3.3 0.0.0.0 area 0
network 10.10.10.28 0.0.0.3 area 0
network 10.10.10.32 0.0.0.3 area 0
network 10.10.10.52 0.0.0.3 area 0
!

```

**Figura 3.12. Configuración de OSPF como Protocolo IGP.
Fuente Propia con Datos Obtenidos de CCNA 200-301 Cert Guide, 2020.**

La **Figura 3.13.** muestra las adyacencias OSPF entre los Routers una vez se han aplicados las configuraciones en todos los equipos. En la figura se aprecia la salida del comando *show ip ospf neighbor* en P2 y P4 (Core), PE_1 y PE_3 (Borde). Se ve el estado de la adyacencia ospf, la IP del vecino (la loopback 0 por el comando de Router-id) así como la IP y la interface por medio del cual conoce al vecino.

```

P2(config)#do sh ip ospf neig
Neighbor ID      Pri   State           Dead Time   Address      Interface
7.7.7.7          1     FULL/BDR        00:00:34   10.10.10.30  GigabitEthernet4/0
6.6.6.6          1     FULL/BDR        00:00:33   10.10.10.26  GigabitEthernet3/0
3.3.3.3          1     FULL/DR         00:00:34   10.10.10.10  GigabitEthernet2/0
1.1.1.1          1     FULL/BDR        00:00:32   10.10.10.1   GigabitEthernet1/0
PE_3#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address      Interface
9.9.9.9          1     FULL/BDR        00:00:34   10.10.10.54  GigabitEthernet1/0
3.3.3.3          1     FULL/BDR        00:00:33   10.10.10.33  GigabitEthernet3/0
2.2.2.2          1     FULL/BDR        00:00:37   10.10.10.29  GigabitEthernet4/0
P4(config)#do sh ip ospf neig
Neighbor ID      Pri   State           Dead Time   Address      Interface
5.5.5.5          1     FULL/DR         00:00:34   10.10.10.46  GigabitEthernet4/0
8.8.8.8          1     FULL/BDR        00:00:33   10.10.10.42  GigabitEthernet3/0
3.3.3.3          1     FULL/BDR        00:00:31   10.10.10.13  GigabitEthernet1/0
1.1.1.1          1     FULL/BDR        00:00:32   10.10.10.5   GigabitEthernet2/0
PE_1#show ip ospf neighbor
Neighbor ID      Pri   State           Dead Time   Address      Interface
4.4.4.4          1     FULL/BDR        00:00:35   10.10.10.45  GigabitEthernet4/0
1.1.1.1          1     FULL/BDR        00:00:33   10.10.10.17  GigabitEthernet3/0

```

**Figura 3.13. Adyacencias OSPF Activas en los Routers.
Fuente Propia con Datos Obtenidos de Software Secure CRT versión 8.1.4.**

3.4.1.2. HABILITACION DE MPLS Y LDP.

Para poder implementar MPLS L3 VPN es necesario habilitar antes, Cisco CEF, MPLS y LDP en los Routers de la red. Cisco CEF debe habilitarse primero pues MPLS y LDP requieren que CEF ya este configurado, en IOS recientes CEF ya viene habilitado por defecto. **(Cisco Systems Inc., 2009, pág. 1007)**

Se utiliza la Loopback0 como interfaz Router-id del protocolo LDP para el intercambio de etiquetas entre los Routers, de este modo se evita que el protocolo LDP escoja un Router-id por defecto que no sea utilizable y por ende el protocolo IGP no pueda anunciarlo a los otros Router. (Cisco Systems, 2012, pág. 5)

3.4.1.2.1. CONFIGURACION DE CEF, MPLS Y LDP.

La **Figura 3.14.** muestra la topología (Core y Borde) donde se habilitará CEF, MPLS y LDP, aunque CEF ya viene configurado por defecto en los Router se indican el comando para habilitarlo. Primero se configuran los parámetros globales en los Routers utilizando la interface loopback 0 como el Router-id del protocolo LDP y después se habilita MPLS a nivel de interfaces.

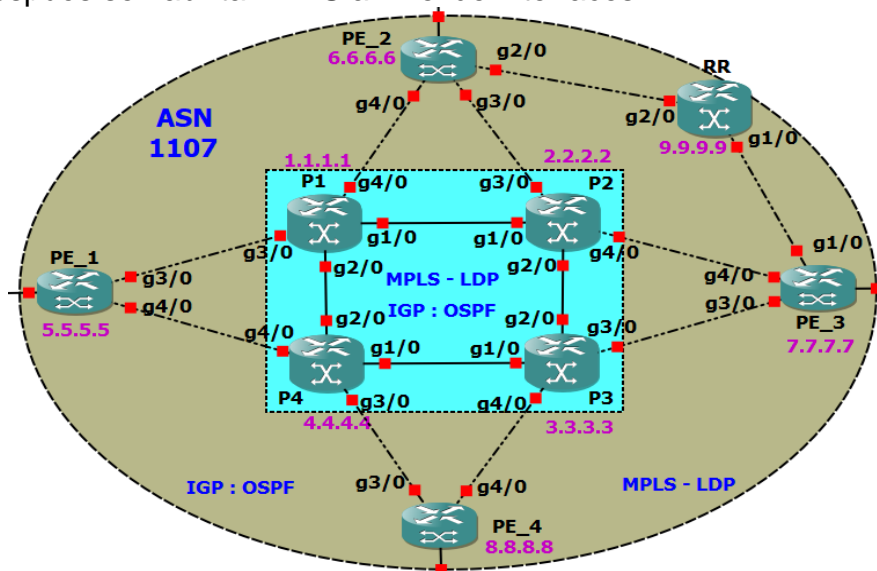


Figura 3.14. Habilitación de MPLS y LDP en la Red.
Fuente Propia con Datos Obtenidos de Software GNS3 2.2.31.

La **Figura 3.15.** muestra las configuraciones a nivel global (Izquierda) y a nivel de interfaces (derecha) a aplicar. Se toma como ejemplo PE_1 y P2 para la configuración de interfaces MPLS. Esto se debe realizar en cada Router.

```
configure terminal
ip cef
mpls ip
mpls label protocol ldp
mpls ldp graceful-restart
mpls ldp router-id loopback0
```

```
P2
interface range gi1/0,gi2/0,gi3/0,gi4/0
mpls ip
```

```
PE_1
interface range gi1/0, gi2/0
mpls ip
```

Figura 3.15. Configuración Global y de Interfaces de MPLS.
Fuente Propia con Datos Obtenidos de MPLS LDP Configuration Guide, 2012.

Luego de aplicar las configuraciones en la **Figura 3.16**, se aprecia que en P1 CEF cuenta con 50 prefijos en su tabla Forwarding, P4 puede descubrir a P1, P3, PE_1 y PE_4 a través de LDP y las interfaces de PE_3 ya participan del protocolo LDP.

```
P1(config-if-range)#do sh ip cef sum
IPv4 CEF is enabled and running
VRF Default
50 prefixes (50/0 fwd/non-fwd)
Table id 0x0
Database epoch: 0 (50 entries)
PE_3#show mpls interface
Interface IP
GigabitEthernet1/0 Yes (ldp)
GigabitEthernet3/0 Yes (ldp)
GigabitEthernet4/0 Yes (ldp)
P4(config)#do sh mpls ldp discovery
Local LDP Identifier:
10.10.10.45:0
Discovery Sources:
Interfaces:
GigabitEthernet1/0 (ldp): xmit/rcv
LDP Id: 3.3.3.3:0
GigabitEthernet2/0 (ldp): xmit/rcv
LDP Id: 1.1.1.1:0
GigabitEthernet3/0 (ldp): xmit/rcv
LDP Id: 8.8.8.8:0
GigabitEthernet4/0 (ldp): xmit/rcv
LDP Id: 5.5.5.5:0
```

Figura 3.16. Verificación de CEF, MPLS y LDP habilitados.
Fuente Propia con Datos Obtenidos de Software Secure CRT versión 8.1.4.

En la **Figura 3.17**, se ve el establecimiento de los Peer LDP. En este caso se muestran los vecinos LDP para PE_4 (P3 y P4), se observa el ID del vecino así como el ID local (IP de la Loopback0). El comando *show mpls ldp neighbor* también indica la interfaz por donde conoce el vecino.

```
PE_4(config)#do show mpls ldp neighbor
Peer LDP Ident: 3.3.3.3:0; Local LDP Ident 8.8.8.8:0
TCP connection: 3.3.3.3.646 - 8.8.8.8.12097
State: Oper; Msgs sent/rcvd: 40/40; Downstream
Up time: 00:11:56
LDP discovery sources:
GigabitEthernet4/0, Src IP addr: 10.10.10.37
Addresses bound to peer LDP Ident:
10.10.10.13 3.3.3.3 10.10.10.10 10.10.10.33
10.10.10.37
Peer LDP Ident: 4.4.4.4:0; Local LDP Ident 8.8.8.8:0
TCP connection: 4.4.4.4.646 - 8.8.8.8.55244
State: Oper; Msgs sent/rcvd: 41/40; Downstream
Up time: 00:11:51
LDP discovery sources:
GigabitEthernet3/0, Src IP addr: 10.10.10.41
Addresses bound to peer LDP Ident:
10.10.10.14 4.4.4.4 10.10.10.6 10.10.10.41
10.10.10.45
```

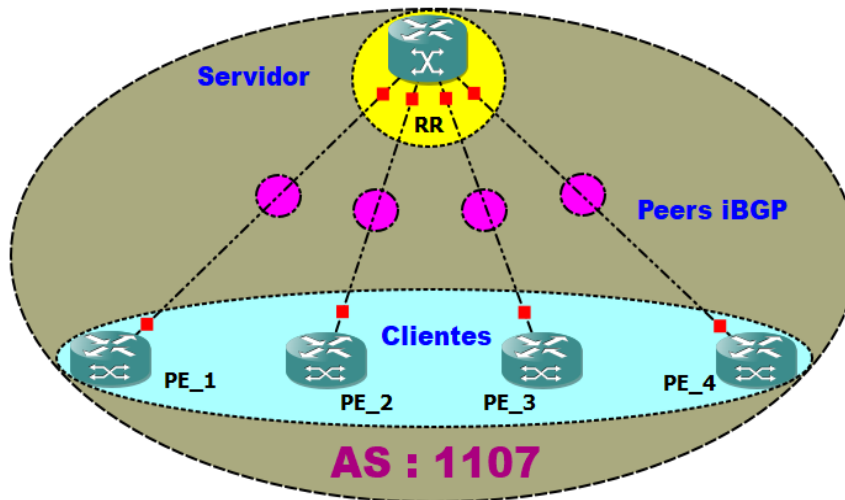
Figura 3.17. Peer MPLS LDP luego de Habilitar el IGP.
Fuente Propia con Datos Obtenidos de Software Secure CRT versión 8.1.4.

3.4.1.3. HABILITACION DE MP-iBGP UTILIZANDO RR.

Una vez habilitado MPLS – LDP y OSPF corriendo como protocolo IGP en la red, es necesario habilitar iBGP en los Router de Borde (PE´s) que conectarán con redes externas ya que BGP es el encargado de anunciar los prefijos VPNv4 de los clientes, luego de esto ya se puede brindar servicios de VPN L3. El RR se conectará en redundancia al PE_2 y PE_3 ya que la topología MP-iBGP quedaría estrella con el RR como Router central iBGP. (Careglio, 2013)

3.4.1.3.1. CONFIGURACION DEL FULL MESH MP-iBGP.

La **Figura 3.18.** muestra que los PE's levantan una sesión iBGP con el RR, cada PE será configurado como cliente iBGP y el RR será el servidor del Peer iBGP. Se utilizará la loopback 0 de los Routers como Router-id del proceso iBGP debido a que se levanta sesión iBGP con Peers que no están directamente conectados.



**Figura 3.18. Habilitación de MP-iBGP utilizando RR.
Fuente Propia con Datos Obtenidos de Software GNS3 2.2.31.**

Las configuraciones para levantar las sesiones iBGP entre los RR y los PE's se muestran en la **Figura 3.19.** La parte derecha de la imagen muestra el ejemplo para el PE_1 utilizando su Loopback 0 (5.5.5.5/32) como Router-id del peer iBGP. La parte izquierda refleja las configuraciones a aplicar en el RR modificando la IP de cada neighbor con la respectiva Loopback 0 de cada PE.

<pre>router bgp 1107 bgp router-id 9.9.9.9 bgp log-neighbor-changes neighbor 5.5.5.5 remote-as 1107 neighbor 5.5.5.5 description iBGP_PE_1 neighbor 5.5.5.5 update-source Loopback0 ! address-family ipv4 neighbor 5.5.5.5 activate neighbor 5.5.5.5 route-reflector-client neighbor 5.5.5.5 soft-reconfiguration inbound exit-address-family ! address-family vpnv4 neighbor 5.5.5.5 activate neighbor 5.5.5.5 send-community both neighbor 5.5.5.5 route-reflector-client exit-address-family</pre>	<pre>router bgp 1107 bgp router-id 5.5.5.5 bgp log-neighbor-changes neighbor 9.9.9.9 remote-as 1107 neighbor 9.9.9.9 description iBGP_RR neighbor 9.9.9.9 update-source Loopback0 ! address-family ipv4 neighbor 9.9.9.9 activate neighbor 9.9.9.9 soft-reconfiguration inbound exit-address-family ! address-family vpnv4 neighbor 9.9.9.9 activate neighbor 9.9.9.9 send-community both exit-address-family</pre>
---	---

**Figura 3.19. Configuración de MP-iBGP entre PE y RR.
Fuente Propia con Datos Obtenidos de Cartilla de Comandos BGP.**

La **Figura 3.20.** muestra el establecimiento de Peers iBGP entre los PE´s y el RR. En el RR se puede ver las sesiones iBGP establecidas hacia los 4 PE´s con la IP de la loopback 0 como IP del neighbor iBGP, así mismo se aprecia el identificador local del proceso BGP para el RR (9.9.9.9) junto con su AS 1107. Cuando ambos peer BGP se crean con el mismo ASN se le llama peer iBGP y cuando tienen diferentes ASN son peer eBGP. El comando utilizado es *show ip bgp summary*.

```
RR(config-router)#do sh ip bgp summ
BGP router identifier 9.9.9.9, local AS number 1107
BGP table version is 1, main routing table version 1
```

Neighbor	V	AS	MsgRcvd	MsgSent	TblVer	InQ	OutQ	Up/Down	State/PfxRcd
5.5.5.5	4	1107	4	2	1	0	0	00:00:22	0
6.6.6.6	4	1107	4	2	1	0	0	00:00:35	0
7.7.7.7	4	1107	4	2	1	0	0	00:00:47	0
8.8.8.8	4	1107	7	7	1	0	0	00:02:57	0

Figura 3.20. Peer iBGP Establecidos en el RR.
Fuente Propia con Datos Obtenidos de Software Secure CRT versión 8.1.4.

3.4.1.4. BALANCEO DE TRAFICO EN EL CORE DE LA RED.

Para finalizar las configuraciones de la red MPLS se balanceará el tráfico que atraviese el Core MPLS (P1-P4), estableciendo una ruta específica para los paquetes etiquetados según su origen (PE_1-PE_4). Sería como una especie de ingeniería de tráfico simple, pero que permite tener una sola ruta en la red para cada tráfico, además se asemeja a la ingeniería de tráfico que se aplica en redes grandes en producción de los ISP, de este modo se balancea el tráfico en el Core.

Se aplican costos de OSPF en los Routers P2 y P4 para que el protocolo OSPF selecciona las rutas para el tráfico que pase por la malla del Core. Para la redundancia del RR, con PE_2 y PE_3, se establece la ruta por PE_3 como la mejor utilizando costos de OSPF de igual manera. En este caso el mismo comando se aplica a las interfaces Gi2/0 de PE_2 y de RR.

La **Figura 3.21.** muestra la configuración a aplicarse en las interfaces Gi1/0 y Gi2/0 de P2 y P4, se modificará el costo por defecto para interfaces Gigabit Ethernet que es de 1 y se cambiará a 3. De este modo el tráfico proveniente de PE_1 pasará por P1-P2, el de PE_3 cursará por el link P2-P3, el tráfico de PE_2 pasará por P1-P4 y el de PE_4 cursará por el link de P3-P4. **(ODOM, 2020, pág. 491)**

P2 y P4 interface range gi1/0, gi2/0 ip ospf cost 3	PE_2 y RR interface gigabitethernet 2/0 ip ospf cost 3
---	--

Figura 3.21. Configuración de Costo de OSPF en Interfaces.
Fuente Propia con Datos Obtenidos de CCNA 200-301 Cert Guide, 2020.

La **Figura 3.22.** muestra la salida del comando `show ip route x`, donde x es la IP de loopback 0 de los Routers. En este caso ya se tiene una sola ruta para alcanzar el destino, habiendo 2 enlaces habilitados por cada PE hacia el Core el protocolo OSPF escoge la mejor ruta en base a los costos que se aplicaron previamente.

```
PE_3#show ip route 5.5.5.5
Routing entry for 5.5.5.5/32
  Known via "ospf 1107", distance 110, metric 4, type intra area
  Last update from 10.10.10.33 on GigabitEthernet3/0, 00:31:08 ago
  Routing Descriptor Blocks:
    * 10.10.10.33, from 5.5.5.5, 00:31:08 ago, via GigabitEthernet3/0
      Route metric is 4, traffic share count is 1
PE_2#show ip route 8.8.8.8
Routing entry for 8.8.8.8/32
  Known via "ospf 1107", distance 110, metric 4, type intra area
  Last update from 10.10.10.21 on GigabitEthernet4/0, 00:31:53 ago
  Routing Descriptor Blocks:
    * 10.10.10.21, from 8.8.8.8, 00:31:53 ago, via GigabitEthernet4/0
      Route metric is 4, traffic share count is 1
PE_4(config)#do show ip route 5.5.5.5
Routing entry for 5.5.5.5/32
  Known via "ospf 1107", distance 110, metric 3, type intra area
  Last update from 10.10.10.41 on GigabitEthernet3/0, 00:31:14 ago
  Routing Descriptor Blocks:
    * 10.10.10.41, from 5.5.5.5, 00:31:14 ago, via GigabitEthernet3/0
      Route metric is 3, traffic share count is 1
PE_1#show ip route 7.7.7.7
Routing entry for 7.7.7.7/32
  Known via "ospf 1107", distance 110, metric 4, type intra area
  Last update from 10.10.10.17 on GigabitEthernet3/0, 00:31:28 ago
  Routing Descriptor Blocks:
    * 10.10.10.17, from 7.7.7.7, 00:31:28 ago, via GigabitEthernet3/0
      Route metric is 4, traffic share count is 1
P4#show ip route 9.9.9.9
Routing entry for 9.9.9.9/32
  Known via "ospf 1107", distance 110, metric 5, type intra area
  Last update from 10.10.10.42 on GigabitEthernet3/0, 00:31:37 ago
  Routing Descriptor Blocks:
    * 10.10.10.42, from 9.9.9.9, 00:31:37 ago, via GigabitEthernet3/0
      Route metric is 5, traffic share count is 1
```

Figura 3.22. Mejor Ruta Escogida por OSPF Aplicando Costo a Interfaces.
Fuente Propia con Datos Obtenidos de Software Secure CRT versión 8.1.4.

3.4.2. CONFIGURACION DE ENLACES DE DATOS DE SUCURSALES.

Ya con las red MPLS lista para brindar servicios de VPN. Lo que sigue ahora es plantear las configuraciones necesarias para llevar a cabo los servicios de L3 VPN sobre MPLS. Para esto se iniciará con los enlaces de Datos de las 3 sucursales.

La **Figura 3.23.** muestra cómo sería el acceso de cada sucursal a la red del ISP representado por una nube. La conexión PE-CE se ve como si cada sitio estuviera a un salto de distancia pero en la realidad esta puede pasar por varios equipos y redes de transmisión que no siempre son IP. Estas opciones pueden ser redes

puramente IP como una Metro Ethernet, una red ADSL, o híbridas con una parte IP y un tramo de radio enlace, inclusive por una red SDH.

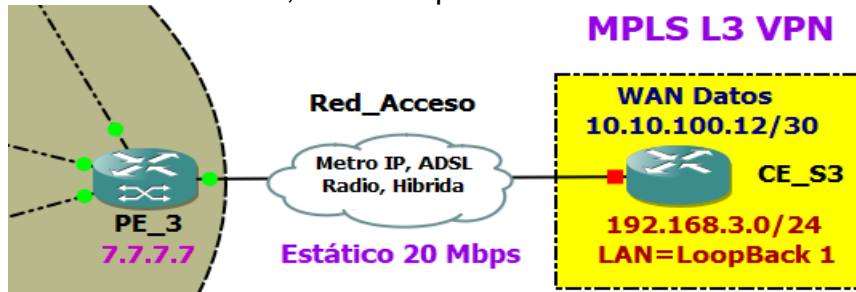


Figura 3.23. Red de Acceso del Cliente.
Fuente Propia con Datos Obtenidos de Software GNS3 2.2.31.

3.4.2.1. CONFIGURACION EN LOS PE.

Los enlaces de las 3 sucursales establecen enrutamiento estático en la conexión PE-CE, las configuraciones en el Borde de la Red (PE) se harán en 3 partes: la creación de la VRF para la VPN del cliente, el anuncio de los prefijos VPNv4 en el MP-iBGP y el establecimiento de QoS para el BW asignado a cada sucursal.

3.4.2.1.1. CREACION DE LA VRF DEL CLIENTE.

En esta parte se aplicarán 3 de los componentes funcionales de una L3 VPN vistos en el Capítulo II como lo son VRF, RD (Route Distinguisher) y RT (Route Target). En la **Figura 3.24.** se observan los comandos a configurarse en el PE correspondiente para cada sucursal (PE_4 de Ejemplo), se nombra la VRF como MPLS_IDAI, se le asigna el RD 1107:10, se importa y exporta el RT y se configura la interfaz que conecta al CE. La figura muestra también la verificación con la salida del comando `show ip vrf brief` en PE_2 como ejemplo.

```

ip vrf MPLS_IDAI
 rd 1107:10
 route-target export 1107:10
 route-target import 1107:10
!
interface FastEthernet0/0
 description HACIA CE_S4_Fa0/0
 ip vrf forwarding MPLS_IDAI
 ip address 10.10.100.17 255.255.255.252
 no shutdown

```

```

PE_2#show ip vrf brief
Name                Default RD          Interfaces
MPLS_IDAI           1107:10             Fa0/0
PE_2#show ip vrf interfaces
Interface            IP-Address          VRF                Protocol
Fa0/0                10.10.100.9        MPLS_IDAI          up

```

Figura 3.24. Configuración y Verificación de VRF a Nivel Global e Interfaces.
Fuente Propia con Datos Obtenidos de Cartilla de Comandos MPLS.

3.4.2.1.2. PROPAGACION DE RUTAS EN EL MP-iBGP.

Se configura la ruta estática que apunte a la LAN de la sucursal, esta ruta estática está dentro de la tabla VRF MPLS_IDAI y no en la tabla global del Router. También se agrega la VRF MPLS_IDAI al address-family ipv4 del MP-iBGP que los PE's levantan con el RR para propagar entre ellos los prefijos VPNv4 de la VPN.

La **Figura 3.25.** muestra la configuraciones necesarias para realizar lo dicho antes. Como ejemplo se observa la ruta estática hacia la LAN de la S3 y el anuncio de los prefijos del cliente (redistribución de rutas estáticas e interfaces configuradas dentro de la vrf MPLS_IDAI) en el iBGP a configurar en el PE_3. La configuración a modificar es la ruta estática con las IP WAN y LAN de cada sucursal.

```
configure terminal
ip route vrf MPLS_IDAI 192.168.3.0 255.255.255.0 10.10.100.14 name LAN_S3

router bgp 1107
address-family ipv4 vrf MPLS_IDAI
redistribute connected
redistribute static
exit-address-family
```

Figura 3.25. Configuración de Ruta Estática y Anuncio de la VRF en BGP.
Fuente Propia con Datos Obtenidos de Cartilla de Comandos BGP Y MPLS.

En la **Figura 3.26.** se aprecia, por medio del comando *show ip route vrf name-vrf*, que en la tabla de enrutamiento de la vrf MPLS_IDAI ya se están recibiendo las redes LAN y WAN de las sucursales. El ejemplo muestra que el PE_3 recibe redes por iBGP (aparece la letra B a la izquierda de las IP).

```
PE_3#show ip route vrf MPLS_IDAI
Routing Table: MPLS_IDAI
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
        D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
        N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
        E1 - OSPF external type 1, E2 - OSPF external type 2
        i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
        ia - IS-IS inter area, * - candidate default, U - per-user static route
        o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
        + - replicated route, % - next hop override

Gateway of last resort is not set

10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
B    10.10.100.8/30 [200/0] via 6.6.6.6, 01:14:25
C    10.10.100.12/30 is directly connected, FastEthernet0/0
L    10.10.100.13/32 is directly connected, FastEthernet0/0
B    10.10.100.16/30 [200/0] via 8.8.8.8, 01:14:06
B    192.168.2.0/24 [200/0] via 6.6.6.6, 01:14:25
S    192.168.3.0/24 [1/0] via 10.10.100.14
B    192.168.4.0/24 [200/0] via 8.8.8.8, 01:14:06
```

Figura 3.26. Redes Recibidas por MP-iBGP para la VRF MPLS_IDAI.
Fuente Propia con Datos Obtenidos de Software Secure CRT versión 8.1.4.

3.4.2.1.3. ESTABLECIMIENTO DE QoS A ENLACES WAN.

Para asignar el BW que cada LAN ocupe de la red se aplicará QoS en los PE's, de manera que se restrinjan los recursos de la red para cada enlace de las sucursales. Para esto se utilizará MQC (Modular QoS Command Line), que es un mecanismo para aplicar QoS bajo el modelo DiffServ (Soft QoS) y permite clasificar tráfico de forma sencilla utilizando clases para tráfico específico. MQC consta de 3 fases: la creación de class-map (clases de servicios), la creación de policy-map (políticas de QoS) y la aplicación del policy-map a una interface en dirección de entrada/salida. (Cisco Systems Inc., 2009, pág. 1013)

La **Figura 3.27.** muestra las configuraciones a aplicarse en cada PE para el BW de 20Mbps. Se toma como ejemplo el PE_4 para el enlace de datos de la sucursal S4. Se crea una lista de acceso que filtre la red LAN, luego un class-map hace match con esta lista de acceso. Después se crea el policy-map que contenga el class-map y se establece el BW requerido mediante un police-cir. Por último, se aplica el policy-map a la interface de acceso en dirección de entrada y salida.

```
ip access-list extended IDAI_DATOS_S4
 permit ip 192.168.4.0 0.0.0.255 any
 permit ip any 192.168.4.0 0.0.0.255
!
class-map match-all IDAI_DATOS_S4
 match access-group name IDAI_DATOS_S4
!
policy-map IDAI_DATOS
 class IDAI_DATOS_S4
  police cir 2048000 conform-action transmit exceed-action drop
!
interface fastethernet 0/0
 service-policy input IDAI_DATOS
 service-policy output IDAI_DATOS
```

Figura 3.27. Configuración de MQC como mecanismo de Calidad de Servicio.
Fuente Propia con Datos Obtenidos de CCNP 300-101 Cert Guide, 2015.

3.4.2.2. CONFIGURACION EN LOS CE.

La configuración del lado del cliente es más sencilla y rápida. Se levanta la Loopback 1 en el Router CE que simula la LAN de la sucursal y se configura una ruta estática por defecto con Gateway a la red del ISP (PE correspondiente).

3.4.2.2.1. CONFIGURACION A NIVEL DE LAN Y WAN.

La **Figura 3.28.** muestra las configuraciones en los Router CE 3725, se activa la loopback 1 y se setea a 100-Full Dúplex el link L3 entre PE-CE para evitar cualquier inconveniente de mis match dúplex en las interface de ambos Routers. La figura muestra el ejemplo en el CE_S3, se debe aplicar estas configuraciones en cada CE con los datos de direccionamiento correspondiente.

```
interface Loopback 1
  description LAN_S3
  ip address 192.168.3.1 255.255.255.0
!
interface FastEthernet0/0
  description WAN_PE_3_Fa0/0
  ip address 10.10.100.14 255.255.255.252
  no shutdown
  speed 100
  full-duplex

ip route 0.0.0.0 0.0.0.0 10.10.100.14 name GW_PE_3
```

Figura 3.28. Configuración WAN y LAN en CE.
Fuente Propia con Datos Obtenidos de IOS 12.4 Command Reference.

En la **Figura 3.29.** se aprecia que desde cualquier PE, en este caso PE_2, se puede alcanzar la WAN y LAN de la sucursal de Granada. Confirmando así el correcto enrutamiento entre PE-CE. Se utiliza el comando *ping vrf vrf-name x.x.x.x.*

```
PE_2#ping vrf MPLS_IDAI 10.10.100.14
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.10.100.14, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 36/46/52 ms
PE_2#ping vrf MPLS_IDAI 192.168.3.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 24/33/48 ms
```

Figura 3.29. WAN-LAN de Sucursales ya son alcanzables desde la Red MPLS.
Fuente Propia con Datos Obtenidos de Software Secure CRT versión 8.1.4.

3.4.3. CONFIGURACION DE ENLACES DE DATOS DE CASA MATRIZ.

Según los requerimientos de servicio, el enlace de Datos (L3 VPN) de Casa Matriz tiene redundancia. Para ambos enlaces (Principal y Respaldo) la conexión PE-CE se realiza por protocolo de enrutamiento dinámico (BGP). En este caso es un eBGP entre la red MPLS (del ISP) y la red del cliente (IDAI). Las configuraciones se han dividido en 2 partes, configuraciones en el CE de Casa Matriz (Datos

Principal y Respaldo) y luego en PE_1 (Enlace Principal) y en PE_4 (Enlace de Respaldo). Para esto se tomarán los datos de direccionamiento de la [Figura 3.9.](#)

3.4.3.1. CONFIGURACION DEL CE DE CASA MATRIZ.

Las configuraciones para el CE de Casa matriz se muestran en las [Figura 3.30. - 3.32.](#) donde se configuran las interfaces y la adyacencia eBGP entre PE-CE. En la [Figura 3.30.](#) se levanta la loopback 1 como LAN de Casa Matriz, se habilitan las interfaces gigabit ethernet 1/0 (principal) y la gigabit 2/0 (Respaldo).

```
interface Loopback 1
description LAN_IDAI_CM
ip address 192.168.1.1 255.255.255.0
no Shutdown
!
```

```
interface GigabitEthernet1/0
description DATOS_PPAL_IDAI_CASA_MATRIZ
ip address 10.10.100.2 255.255.255.252
no shutdown
!
interface GigabitEthernet2/0
description DATOS_BK_IDAI_CASA_MATRIZ
ip address 10.10.100.6 255.255.255.252
no shutdown
```

Figura 3.30. Configuración de Interfaces para los Enlaces de Casa Matriz.
Fuente Propia con Datos Obtenidos de IOS 12.4 Command Reference.

En la [Figura 3.31.](#) aparecen las configuraciones para levantar los Peer eBGP en el CE_CM hacia los PE´s, se utiliza el ASN 1990 del cliente como identificador del proceso BGP y se configura la IP 10.1.1.1 como Router-id para que BGP no escoja la LAN como interface para los intercambios de mensajes. La figura muestra las configuraciones hacia el Peers eBGP primario (PE_1) y secundario (PE_4).

```
router bgp 1990
bgp router-id 10.1.1.1
bgp log-neighbor-changes
neighbor 10.10.100.1 remote-as 1107
neighbor 10.10.100.1 description eBGP_DATOS_PPAL
neighbor 10.10.100.1 update-source GigabitEthernet1/0
neighbor 10.10.100.5 remote-as 1107
neighbor 10.10.100.5 description eBGP_DATOS_BK
neighbor 10.10.100.5 update-source GigabitEthernet2/0
!
address-family ipv4
redistribute conected
neighbor 10.10.100.1 activate
neighbor 10.10.100.1 soft-reconfiguration inbound
neighbor 10.10.100.5 activate
neighbor 10.10.100.5 soft-reconfiguration inbound
```

Figura 3.31. Configuración del Peer eBGP Primario y Secundario.
Fuente Propia con Datos Obtenidos de CCNP 300-101 Cert Guide, 2015.

La redundancia es automática (BGP) y no hay necesidad de desactivar un enlace. Se utiliza el atributo de BGP Weight para establecer un peso al Peer primario para que sea elegido como la mejor ruta para el tráfico saliente y el atributo AS-Path Prepend para aumentar la longitud de ASN en el eBGP secundario y así no sea considerado la mejor ruta del tráfico entrante. De esta forma se tiene comunicación simétrica, necesaria para tráfico sensible como TCP. (Wallace, 2015, pág. 654)

La **Figura 3.32.** muestra las configuraciones a realizarse. Se asigna un peso de 3000 para ambos Peer BGP primarios. Luego se crea un route-map que duplica la longitud del ASN a 2 y este se aplica en dirección de salida al Peer secundario.

```
route-map eBGP_SECUNDARIO permit 5
  set as-path prepend 1990
!
router bgp 1990
  address-family ipv4
  neighbor 10.10.100.1 weight 3000
  neighbor 10.10.100.5 route-map eBGP_SECUNDARIO out
```

Figura 3.32. Selección de la Mejor Ruta BGP usando Weight y As-Path Prepend.
Fuente Propia con Datos Obtenidos de CCNP 300-101 Cert Guide, 2015.

3.4.3.2. CONFIGURACION EN PE_1 Y PE_4.

Dado que la VRF para datos ya está creada (vrf MPLS_IDAI) se habilitan las interfaces que conectan con el CE_CM tanto para el enlace principal (Gi1/0 PE_1) como el de respaldo (Gi2/0 PE_4). El peer eBGP entre PE-CE se levanta con el ASN 1990 del cliente y la red directamente conectada (IP WAN de cada enlace). La **Figura 3.33.** muestra los datos para el Peer eBGP principal en PE_1 (parte derecha), el neighbor eBGP se crea dentro del address-family ipv4 de la vrf.

```
interface GigabitEthernet1/0
  description PPAL_DATOS_IDAI_CASA_MATRIZ
  ip vrf forwarding MPLS_IDAI
  ip address 10.10.100.1 255.255.255.252
!
interface GigabitEthernet2/0
  description BK_DATOS_IDAI_CASA_MATRIZ
  ip vrf forwarding MPLS_IDAI
  ip address 10.10.100.5 255.255.255.252

router bgp 1107
  address-family ipv4 vrf MPLS_IDAI
  redistribute connected
  neighbor 10.10.100.2 remote-as 1990
  neighbor 10.10.100.2 description DATOS_PPAL_IDAI_CASA_MATRIZ
  neighbor 10.10.100.2 activate
  neighbor 10.10.100.2 soft-reconfiguration inbound
  exit-address-family
```

Figura 3.33. Configuración de Interfaces y Peer eBGP en los PE's.
Fuente Propia con Datos Obtenidos de Cartilla de Comandos MPLS y BGP.

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

Para asignar el BW a los enlaces de datos se aplicarán las mismas políticas de QoS que se configuró para las sucursales. En este caso filtrando la red LAN de Casa Matriz. Esto se muestra en la **Figura 3.34.** donde se restringen el BW a 80Mbps y luego se aplica a la interface física. La figura muestra el ejemplo para el enlace principal (PE_1), igual debe realizarse en PE_4 para el enlace de respaldo.

```
ip access-list extended IDAI_DATOS_CASA_MATRIZ
 permit ip 192.168.1.0 0.0.0.255 any
 permit ip any 192.168.1.0 0.0.0.255
!
class-map match-all IDAI_DATOS_PPAL_CASA_MATRIZ
 match access-group name IDAI_DATOS_CASA_MATRIZ
!
policy-map IDAI_DATOS
 class IDAI_DATOS_PPAL_CASA_MATRIZ
  police cir 81920000 conform-action transmit exceed-action drop
!
interface gigabitethernet 1/0
 service-policy input IDAI_DATOS
 service-policy output IDAI_DATOS
```

**Figura 3.34. Configuración de QoS para el BW de Casa Matriz.
Fuente Propia con Datos Obtenidos de CCNP 300-101 Cert Guide, 2015.**

Luego de aplicar las configuraciones, en la **Figura 3.35.** se puede observar el establecimiento del Peer eBGP del CE_CM con el PE_1 y PE_4 (Principal y Respaldo). Con los comandos *show ip bgp summary* en el CE_CM y *show ip bgp vpnv4 vrf MPLS_IDAI summary* en el PE, se ve el tiempo de establecida la sesión bgp (up/down), los prefijos recibidos (PfxRcd), la IP y el número de AS del vecino.

```
CE_CM#sh ip bgp summ
BGP router identifier 10.1.1.1, local AS number 1990
BGP table version is 46, main routing table version 46
9 network entries using 1296 bytes of memory

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.10.100.1   4        1107    21    20     46    0    0 00:09:44    8
10.10.100.5   4        1107    14    14     46    0    0 00:06:47    8
PE_1#sh ip bgp vpnv4 vrf MPLS_IDAI summary
BGP router identifier 5.5.5.5, local AS number 1107
BGP table version is 30, main routing table version 30
9 network entries using 1404 bytes of memory

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.10.100.2   4        1990    33    41     30    0    0 00:20:42    3
PE_4#sh ip bgp vpnv4 vrf MPLS_IDAI summary
BGP router identifier 8.8.8.8, local AS number 1107
BGP table version is 18, main routing table version 18
9 network entries using 1404 bytes of memory

Neighbor      V      AS MsgRcvd MsgSent  TblVer  InQ  OutQ  Up/Down  State/PfxRcd
10.10.100.6   4        1990    32    42     18    0    0 00:23:01    3
```

**Figura 3.35. Peers eBGP de Casa Matriz hacia el ISP.
Fuente Propia con Datos Obtenidos de Software Secure CRT versión 8.1.4.**

Debido a que se están redistribuyendo las redes conectadas hacia los Peer eBGP, es necesario aplicar un filtro en los PE's para seleccionar las subredes que se

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

desean recibir del CE_CM y las que se deben enviar (El cliente solo necesita recibir las redes LAN de las sucursales,). Para esto se aplican políticas de ruteo PBR utilizando prefix-list al Peer eBGP. (Wallace, 2015, pág. 194)

La **Figura 3.36.** muestra la configuración en PE_1 (y PE_4, neighbor 10.10.10.6) para filtrar la LAN de CM de las redes que el CE_CM envía al PE_1 para luego anunciarlas a los demás CE's. De igual forma se inyectan desde el PE_1 al Peer CE_CM solo los segmentos LAN de las sucursales (parte inferior).

```
ip prefix-list PFX_LAN_SUCURSALES seq 10 permit 192.168.2.0/24
ip prefix-list PFX_LAN_SUCURSALES seq 15 permit 192.168.3.0/24
ip prefix-list PFX_LAN_SUCURSALES seq 20 permit 192.168.4.0/24
!
ip prefix-list PFX_LAN_CM_IDAI seq 10 permit 192.168.1.0/24
!
router bgp 1107
 address-family ipv4 vrf MPLS_IDAI
  neighbor 10.10.100.2 prefix-list PFX_DATOS_IDAI in
  neighbor 10.10.100.2 prefix-list PFX_LAN_SUCURSALES out
```

Figura 3.36. Configuración de Políticas de Ruteo en el Peer eBGP. Fuente Propia con Datos Obtenidos de Cartilla de Comandos BGP.

La **Figura 3.37.** muestra el antes (parte superior) y el después (parte inferior) en la tabla de enrutamiento de las redes aprendidas por eBGP en el CE_CM. Luego de aplicar las políticas de ruteo se aprenden únicamente por BGP los segmentos LAN de las sucursales, el comando utilizado para ver esto es *show ip route*.

```
CE_CM#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       10.0.0.0/8 is variably subnetted, 7 subnets, 2 masks
C       10.10.100.0/30 is directly connected, GigabitEthernet1/0
L       10.10.100.2/32 is directly connected, GigabitEthernet1/0
C       10.10.100.4/30 is directly connected, GigabitEthernet2/0
L       10.10.100.6/32 is directly connected, GigabitEthernet2/0
B       10.10.100.8/30 [20/0] via 10.10.100.5, 00:00:19
B       10.10.100.12/30 [20/0] via 10.10.100.5, 00:00:19
B       10.10.100.16/30 [20/0] via 10.10.100.5, 00:00:19
       192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Loopback1
L       192.168.1.1/32 is directly connected, Loopback1
B       192.168.2.0/24 [20/0] via 10.10.100.1, 01:03:37
B       192.168.3.0/24 [20/0] via 10.10.100.1, 01:03:37
B       192.168.4.0/24 [20/0] via 10.10.100.1, 01:00:32
CE_CM#sh ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       10.0.0.0/8 is variably subnetted, 4 subnets, 2 masks
C       10.10.100.0/30 is directly connected, GigabitEthernet1/0
L       10.10.100.2/32 is directly connected, GigabitEthernet1/0
C       10.10.100.4/30 is directly connected, GigabitEthernet2/0
L       10.10.100.6/32 is directly connected, GigabitEthernet2/0
       192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C       192.168.1.0/24 is directly connected, Loopback1
L       192.168.1.1/32 is directly connected, Loopback1
B       192.168.2.0/24 [20/0] via 10.10.100.1, 01:21:44
B       192.168.3.0/24 [20/0] via 10.10.100.1, 01:21:44
B       192.168.4.0/24 [20/0] via 10.10.100.1, 01:18:39
```

Figura 3.37. Antes y Después de Redes Aprendidas por eBGP en CE_CM. Fuente Propia con Datos Obtenidos de Software Secure CRT versión 8.1.4.

3.5. VALIDACION DEL DISEÑO MPLS L3 VPN.

Todo diseño luego de ser implementado debe ser verificado de tal forma que se valide su correcto funcionamiento. En este caso luego de ser implementado en GNS3 se verifica el diseño de la L3 VPN sobre MPLS (cliente IDAI). Para esto se realizan pruebas icmp a la LAN de los sitios de la VPN, acceso telnet a Router CE de las sucursales y pruebas de redundancias para los enlaces de Casa Matriz.

3.5.1. VERIFICACION DE ENLACES DE DATOS.

3.5.1.1. PRUEBA DE PING A LAN DE CADA CE.

Se realizan pruebas icmp desde el CE_CM hacia las sucursales y viceversa para garantizar que la comunicación sea en ambas direcciones. La **Figura 3.38.** muestra el resultado de las pruebas. Se realiza el ping utilizando la LAN de cada sitio como source para demostrar que existe conectividad de LAN a LAN.

```
CE_CM#ping 192.168.2.1 source loopback 1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/62/76 ms
CE_CM#ping 192.168.3.1 source loopback 1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 48/57/72 ms
CE_CM#ping 192.168.4.1 source loopback 1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 52/55/64 ms
CE_S2#ping 192.168.1.1 source loopback 1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/123/152 ms
CE_S2#ping 192.168.3.1 source loopback 1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.3.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.2.1
!!!!

CE_S3#ping 192.168.1.1 source loopback 1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 120/140/180 ms
CE_S3#ping 192.168.4.1 source loopback 1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.4.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
!!!!
CE_S4#ping 192.168.1.1 source loopback 1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.1.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 116/126/152 ms
CE_S4#ping 192.168.2.1 source loopback 1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.2.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.4.1
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 92/144/180 ms
```

Figura 3.38. Resultados de Pruebas ICMP de LAN a LAN.
Fuente Propia con Datos Obtenidos de Software Secure CRT versión 8.1.4.

Las pruebas de LAN a LAN demuestran que la MPLS L3 VPN ha sido implementada con éxito, cada sitio puede conectarse con casa matriz y entre ellos mismos. Las Pruebas a nivel WAN están implícitas ya que para alcanzar las LAN de los sitios primero se pasa por la red MPLS (del ISP).

3.5.1.2. ACCESO TELNET A CADA CE.

Esta prueba es para garantizar que se tenga gestión de los Routers de los sitios en caso que sea necesario algún troubleshooting remoto. De igual forma es parte de las buenas prácticas de la administración de red el poder gestionar los equipos.

La Figura 3.39. muestra (Izquierda) el telnet desde Casa Matriz a las LAN de las sucursales con el comando *telnet x.x.x.x /source loopback 1* y telnet desde los PE´s (Derecha) a la WAN del CE_CM (Datos Principal/Respaldo) con el comando *telnet x.x.x.x /vrf MPLS_IDAI*.

<pre>CE_CM#telnet 192.168.2.1 /source lo1 Trying 192.168.2.1 ... Open User Access Verification Username: admin Password: CE_S2>enable Password: CE_S2# CE_CM#telnet 192.168.3.1 /source lo1 Trying 192.168.3.1 ... Open User Access Verification Username: admin Password: CE_S3>enable Password: CE_S3# CE_CM#telnet 192.168.4.1 /source lo1 Trying 192.168.4.1 ... Open User Access Verification Username: admin Password: CE_S4>enable Password: CE_S4#</pre>	<pre>PE_1#telnet 10.10.100.2 /vrf MPLS_IDAI Trying 10.10.100.2 ... Open CC ----- Este equipo es propiedad privada de IDAI LTD. Si no tiene autorizacion para ingresar al equipo, por favor cancele la conexion inmediatamente. El equipo esta siendo monitoreado y lleva registro de las direcciones IP y usuarios utilizados para la conexion, cualquier anomalia sera reportada a las autoridades correspondientes. ----- User Access Verification Username: admin Password: CE_CM> PE_4#telnet 10.10.100.6 /vrf MPLS_IDAI Trying 10.10.100.6 ... Open CC ----- Este equipo es propiedad privada de IDAI LTD. Si no tiene autorizacion para ingresar al equipo, por favor cancele la conexion inmediatamente. El equipo esta siendo monitoreado y lleva registro de las direcciones IP y usuarios utilizados para la conexion, cualquier anomalia sera reportada a las autoridades correspondientes. ----- User Access Verification Username: admin Password: CE_CM></pre>
--	---

Figura 3.39. Resultados de Pruebas Telnet a Routers CE.
Fuente Propia con Datos Obtenidos de Software Secure CRT versión 8.1.4.

Las pruebas anteriores confirman el acceso remoto a los Routers de cada sitio de la VPN. Pudiendo acceder a los CE con el direccionamiento LAN como con la WAN. Para esto se ha configurado un usuario local y se ha habilitado el acceso telnet en los CE´s con la configuración que muestra las **Figura 3.40.**

```
username admin secret admin
enable secret cisco
!
line vty 0 4
logging synchronous
login local
transport input telnet
transport output telnet
```

Figura 3.40. Habilitación de Usuario y Telnet en los CE´s.
Fuente Propia con Datos Obtenidos de IOS 12.4 Command Reference.

3.5.1.3. PRUEBA DE QoS PARA EL BW DE LOS ENLACES.

Para verificar que las políticas de QoS están restringiendo los recursos de BW que cada sitio ocupa de la red se monitoreará la interfaz de acceso de cada enlace WAN, para esto se usa el comando `show policy-map interface x` (interface que conecta al CE). La **Figura 3.41.** muestra que el policy aplica las políticas según las clases especificadas y filtra el tráfico según los parámetros establecidos. Para observar esto se genera tráfico icmp (ping) desde el CE con source la LAN y con peso de 18,000 en cada uno de los CE, de ejemplo esta la sucursal S3 y CM.

```
PE_1#show policy-map interface gi1/0
GigabitEthernet1/0

Service-policy input: IDAI_DATOS

Class-map: IDAI_DATOS_CASA_MATRIZ (match-all)
 26355 packets, 36867244 bytes
 5 minute offered rate 610000 bps, drop rate 0000 bps
 Match: access-group name IDAI_DATOS_CASA_MATRIZ
  police:
   cir 81920000 bps, bc 2560000 bytes
   conformed 26355 packets, 36867244 bytes; actions:
   transmit
   exceeded 0 packets, 0 bytes; actions:
   drop
   conformed 610000 bps, exceeded 0000 bps

PE_3#show policy-map interface fa0/0
FastEthernet0/0

Service-policy input: IDAI_DATOS

Class-map: IDAI_DATOS_S3 (match-all)
 39104 packets, 55273980 bytes
 5 minute offered rate 574000 bps, drop rate 0000 bps
 Match: access-group name IDAI_DATOS_S3
  police:
   cir 20480000 bps, bc 640000 bytes
   conformed 39104 packets, 55273980 bytes; actions:
   transmit
   exceeded 0 packets, 0 bytes; actions:
   drop
   conformed 574000 bps, exceeded 0000 bps

CE_CM#ping 10.10.100.1 source 101 repeat 1000 size 18000
Type escape sequence to abort.
Sending 1000, 18000-byte ICMP Echos to 10.10.100.1, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
.....
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 12/24/208 ms

CE_S3#ping 10.10.100.13 source 1001 repeat 1000 size 18000
Type escape sequence to abort.
Sending 1000, 18000-byte ICMP Echos to 10.10.100.13, timeout is 2 seconds:
Packet sent with a source address of 192.168.3.1
.....
Success rate is 100 percent (1000/1000), round-trip min/avg/max = 92/145/496 ms
```

**Figura 3.41. Validación de Políticas QoS Aplicadas a los Sitios de la VPN.
Fuente Propia con Datos Obtenidos de Software Secure CRT versión 8.1.4.**

Con estas pruebas se constata que la QoS configurada en los PE's para cada enlace de datos está funcionando adecuadamente. Cuando el tráfico ingresa a la interfaz de acceso del Router procedente de un sitio, éste lo clasifica y le asigna el trato que el tráfico tendrá según la clase configurada.

3.5.2. VERIFICACION DE REDUNDANCIA DE CASA MATRIZ.

Antes de verificar la redundancia es necesario ver la dirección del flujo del tráfico para confirmar que este tome el camino por la 10.10.100.1 (PPAL) y no por la

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

10.10.100.5 (Bk). Para esto hacemos un traceroute a la LAN_CM desde cualquier CE y desde el CE_CM vemos por donde está saliendo el tráfico. La **Figura 3.42.** toma como ejemplo el traceroute desde la LAN de CE_S2 hacia CM con source la LAN local y desde el CE_CM se ve la ruta para el tráfico saliente con el comando *show ip route x.x.x.x*. Ambos comandos confirman que en ambas direcciones el tráfico pasa por la 10.10.100.1

```
CE_S2#traceroute 192.168.1.1 source lo1
Type escape sequence to abort.
Tracing the route to 192.168.1.1
 1 10.10.100.9 128 msec 64 msec 60 msec
 2 10.10.10.21 [MPLS: Labels 28/38 Exp 0] 148 msec 156 msec 148 msec
 3 10.10.100.1 [MPLS: Label 38 Exp 0] 88 msec 116 msec 116 msec
 4 10.10.100.2 116 msec 120 msec 120 msec
CE_CM#sh ip route 192.168.4.1
Routing entry for 192.168.4.0/24
  Known via "bgp 1990", distance 20, metric 0
  Tag 1107, type external
  Last update from 10.10.100.1 01:47:28 ago
  Routing Descriptor Blocks:
  * 10.10.100.1, from 10.10.100.1, 01:47:28 ago
    Route metric is 0, traffic share count is 1
    AS Hops 1
    Route tag 1107
    MPLS label: none
```

**Figura 3.42. Verificación del Flujo de Tráfico Enlace de Datos.
Fuente Propia con Datos Obtenidos de Software Secure CRT versión 8.1.4.**

Sabiendo ya que el tráfico fluye por el enlace principal, ahora se validará que el enlace de respaldo funcione correctamente. Para esto se simulará la caída del enlace principal apagando la interface Gi1/0 en el PE_1. Luego de esto el tráfico deberá conmutar automáticamente y fluir por la 10.10.100.5 (Enlace Respaldo) como lo muestra la **Figura 3.43.** Se toma como ejemplo un traceroute desde la LAN de CE_S3 hacia la LAN CM y otro traceroute en sentido inverso. Se observa que el tráfico conmuta al enlace de respaldo por lo que el resultado de las pruebas de redundancia es exitoso.

```
CE_S3#traceroute 192.168.1.1 source lo1
Type escape sequence to abort.
Tracing the route to 192.168.1.1
 1 10.10.100.13 28 msec 8 msec 8 msec
 2 10.10.10.33 [MPLS: Labels 34/39 Exp 0] 44 msec 40 msec 40 msec
 3 10.10.100.5 [MPLS: Label 39 Exp 0] 40 msec 16 msec 40 msec
 4 10.10.100.6 44 msec 36 msec 44 msec
CE_CM#traceroute 192.168.3.1
Type escape sequence to abort.
Tracing the route to 192.168.3.1
VRF info: (vrf in name/id, vrf out name/id)
 1 10.10.100.5 36 msec 28 msec 8 msec
 2 10.10.10.37 [MPLS: Labels 17/37 Exp 0] 64 msec 64 msec 60 msec
 3 10.10.100.13 [MPLS: Label 37 Exp 0] 60 msec 56 msec 40 msec
 4 10.10.100.14 64 msec 60 msec 60 msec
```

**Figura 3.43. Prueba de Redundancia Enlace de Datos
Fuente Propia con Datos Obtenidos de Software Secure CRT versión 8.1.4.**

COMENTARIO FINALES

CAPITULO III.

El uso de la herramienta informática GNS3 es de suma importancia para profesionales que buscan una de las certificaciones Cisco y para aquellos también que necesitan probar equipos o topologías de red antes de implementarlas en una red en producción ya que con las características que brinda el software garantizan resultados casi 100% iguales a los esperados de redes reales.

En el capítulo se realizaron las 3 etapas de un proyecto, las cuales son la etapa de diseño en basa a los requerimientos de servicio, luego se llevó a cabo la etapa de implementación mediante el software de emulación de IOS Cisco GNS3 que nos permite prescindir de equipos físicos reales costosos y por último la etapa de validación del diseño con las pruebas de conectividad de los enlaces de datos de la VPN tanto a nivel WAN como LAN.

SECCIÓN II: CONSIDERACIONES FINALES.

Esta sección presenta las conclusiones del trabajo, las recomendaciones como opciones de mejoras para futuros trabajos y las referencias bibliográficas que respaldan el contenido del mismo.

I. CONCLUSIONES.

Se concluye el presente trabajo monográfico de manera exitosa ya que se cumplió con los objetivos establecidos al inicio del mismo.

Se establecieron las bases teóricas de la arquitectura MPLS abarcando los conceptos fundamentales, funcionamiento, elementos físicos y lógicos que la componen y los servicios que pueden ser implementados sobre esta arquitectura de red.

Establecidas las bases teóricas se abordó uno de los servicios más implementados de MPLS como lo son las MPLS VPN. Se mencionaron las diferentes tecnologías VPN, tanto tradicionales como emergentes en las últimas décadas.

Luego, dentro de las MPLS VPN, se enfocó en las VPN de capa 3 planteando su terminología, topologías, componentes y la lógica de funcionamiento para poder diseñar una red MPLS L3 VPN que interconecte sitios remotos teniendo en cuenta los requerimientos de servicio de un cliente.

Como punto final se implementó el diseño de red utilizando el programa GNS3, de este modo se prescindió de equipos físicos por la característica de emulación de IOS Cisco del programa, pudiendo validar la topología MPLS L3 VPN y obtener resultados prácticamente exactos al utilizar equipos físicos.

II. RECOMENDACIONES.

Luego de haber finalizado el trabajo monográfico existen opciones de mejora al diseño de red MPLS L3 VPN implementado en GNS3 que pueden ser considerados para futuros trabajos que tomen como punto de partida esta monografía.

- ✚ El diseño de red está enfocado al establecimiento de una L3 VPN sobre MPLS que interconecte los sitios de un solo cliente (empresa o institución). Pero bien se podría ampliar la cantidad de clientes a brindar el servicio de VPN y a la vez proporcionar comunicación entre estos clientes.
- ✚ El alcance del diseño es la red MPLS L3 VPN (mostrando la parte de la red del ISP así como la parte de servicios de VPN's). Igual se podría extender para incluir servicio de Internet Centralizado a las sucursales desde Casa Matriz.
- ✚ Se sugiere implementar el diseño MPLS L3 VPN con direccionamiento IPv6, dado que el actual diseño se realizó utilizando direccionamiento IPv4 en los Routers y Protocolos de Enrutamiento.
- ✚ Así mismo se sugiere utilizar IOS de última generación como XE o XR que sean compatible con plataformas cisco de última generación. En el presente trabajo se utilizó IOS versión 12.4 y 15.

Los puntos anteriores son sugerencias que se consideran importantes e interesantes y le pueden agregar valor a futuros trabajos.

III. REFERENCIAS BIBLIOGRAFICAS.

- Alvez, R. (2012). *www.academia.edu*. Obtenido de *www.academia.edu*:
https://www.academia.edu/9207451/Fundamentos_de_MPLS_VPN
- Angulo, J., & Hernandez, J. (21 de Abril de 2005). *Monografias.com*. Obtenido de *Monografias.com*:
<http://www.monografias.com/trabajos29/informacion-mpls/informacion-mpls.shtml>
- Ballesteros, A., Chiriboga, A., Villegas, L., & Moreno, I. (15 de Mayo de 2007). *www.dspace.espol.edu.ec*. Obtenido de *www.dspace.espol.edu.ec*:
<https://www.dspace.espol.edu.ec/bitstream/123456789/1064/1/1892.pdf>
- Barberá, J. (5 de Febrero de 2000). *Rediris.es*. Obtenido de *Rediris.es*:
<http://www.rediris.es/difusion/publicaciones/boletin/53/enfoque1.html>
- Canalis, M. (2003). *www.urbe.edu/*. Obtenido de *www.urbe.edu/*:
<https://www.urbe.edu/info-consultas/web-profesor/12697883/articulos/Switching/MPLS%202.pdf>
- Careglio, D. (2013). *people.ccaba.upc.edu*. Obtenido de
https://people.ccaba.upc.edu/careglio/wp-content/uploads/2013/10/Lab6-BGP_RR-Confederation.pdf
- Casasola, T. (2015). *sites.google.com*. Obtenido de *sites.google.com*:
<https://sites.google.com/site/redestelematicas2sti/2a-evaluacion/tema-4-wan/4-5-conexion-a-internet/4-5-3-tecnologia-vpn>
- Cisco Systems. (2012). *MPLS Label Distribution Protocol Configuration Guide*. San Jose CA: Cisco Press. Obtenido de
https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_ldp/configuration/12-4t/mp-ldp-12-4t-book.pdf
- Cisco Systems Inc. (2009). *Cisco IOS Multiprotocol Label Switching Configuration Guide*. San Jose CA: Cisco Press. Obtenido de
https://www.cisco.com/c/en/us/td/docs/ios/mppls/configuration/guide/12_2sr/mp_12_2sr_book.pdf
- Cisco Systems, Inc. (2013). *MPLS Basic MPLS Configuration Guide, Cisco IOS XE Release 3S*. San Jose, CA. Obtenido de

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/mp_basic/configuration/xen3s/mp-basic-xe-3s-book.pdf

Cruz, I., Alincaastro, N., Magnago, H., & Hernandez, J. (10 de Mayo de 2013). *cimec.org.ar*. Obtenido de *cimec.org.ar*:

[https://cimec.org.ar/ojs/index.php/mc/article/viewFile/4508/4438#:~:text=La%20base%20de%20datos%20de,LFIB%20\(Forwarding%20Information%20Base\)](https://cimec.org.ar/ojs/index.php/mc/article/viewFile/4508/4438#:~:text=La%20base%20de%20datos%20de,LFIB%20(Forwarding%20Information%20Base)).

De Ghein, L. (2007). *MPLS Fundamentals*. Indianapolis: CISCO PRESS. Obtenido de <https://doc.lagout.org/network/Cisco/CCIE/CCIE%20SP/CiscoPress%20-%20MPLS%20Fundamentals.pdf>

Friedl, A. (Febrero de 2005). *www.acens.com*. Obtenido de *www.acens.com*: <https://www.acens.com/comunicacion/articulos/la-tecnologia-mpls-al-servicio-de-las-redes-privadas/>

Guichard, J., Pepelnjak, I., & Aparcar, J. (Junio de 2003). *MPLS and VPN Architectures Volume II*. Cisco Press. Obtenido de [doc.lagout.org: https://doc.lagout.org/network/Cisco/CCIE/CCIE%20SP/CiscoPress%20-%20MPLS%20and%20VPN%20Architectures%20-%20Volumell.pdf](https://doc.lagout.org/network/Cisco/CCIE/CCIE%20SP/CiscoPress%20-%20MPLS%20and%20VPN%20Architectures%20-%20Volumell.pdf)

Infotecs. (Abril de 2020). *Infotecs.mx*. Recuperado el Mayo de 2022, de *Infotecs.mx*:

<https://infotecs.mx/blog/mppls.html#:~:text=MPLS%20%28Multiprotocol%20Label%20Switching%29%2C%20o%20Conmutaci%C3%B3n%20de%20Etiqueta,comunicaci%C3%B3n%20entre%20dispositivos%20sobre%20infraestructuras%20de%20transmisi%C3%B3n%20mixtas>.

Jimenez, L. (Junio de 2019). *forum.huawei.com*. Obtenido de *forum.huawei.com*: <https://forum.huawei.com/enterprise/es/conociendo-la-categorias-en-que-se-clasifican-las-vpn/thread/542691-100233>

Morales Dibildox, L. (16 de Mayo de 2006). *Catarina.udlap.mx*. Obtenido de *Catarina.udlap.mx*:

http://catarina.udlap.mx/u_dl_a/tales/documentos/lis/morales_d_l/

Nahidha, Z., & Alagumani, S. (2018). IMPLEMENTATION OF MPLS LAYER 3 VPN. *International Journal of Pure and Applied Mathematics*, 3075-3081. Obtenido de <https://acadpubl.eu/hub/2018-119-16/2/318.pdf>

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

- ODOM, W. (2020). *Official Cert Guide CCNA 200-301 Vol 1*. San Jose, CA: Cisco Press.
- Ravi, K., Dhanumjayulu , C., Bagubali , A., & Bagadi , K. (2017). Architecture for MPLS L3 VPN Deployment in Service Provider Network. *Journal of Telecommunications, System & Management.*, págs. 2-4. Obtenido de <https://research.vit.ac.in/publication/architecture-for-mpls-l3-vpn-deployment>
- Sclayton, g. (13 de Octubre de 2008). *www.cisco.com*. Obtenido de [www.cisco.com: https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html](https://www.cisco.com/c/es_mx/support/docs/security-vpn/ipsec-negotiation-ike-protocols/14106-how-vpn-works.html)
- Semeria, C. (2001). *RFC 2547bis: BGP/MPLS VPN Fundamentals*. Sunnyvale: Juniper Networks, Inc. Obtenido de <https://mirror.unpad.ac.id/orari/library/library-ref-eng/ref-eng-3/network/mpls/200012.pdf>
- Silvestre Hernandez, K. (2008). *biblioteca.usac.edu.gt*. Obtenido de [biblioteca.usac.edu.gt: http://biblioteca.usac.edu.gt/tesis/08/08_0221_EO.pdf](http://biblioteca.usac.edu.gt/tesis/08/08_0221_EO.pdf)
- SolarWinds Worldwide, L. (Junio de 2022). *gns3.com*. Obtenido de [gns3.com: https://docs.gns3.com/docs/](https://docs.gns3.com/docs/)
- sshhamim, V. (Marzo de 2022). *cisco.com*. Obtenido de https://www.cisco.com/c/es_mx/support/docs/ip/open-shortest-path-first-ospf/7039-1.html#anc37
- Tapasco Garcia, M. O. (2008). *Repositorio.utp.edu.co*. Obtenido de [Repositorio.utp.edu.co: http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/1311/0046T172.pdf](http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/1311/0046T172.pdf)
- Telectronika. (Junio de 2022). *www.telectronika.com*. Obtenido de <https://www.telectronika.com/articulos/ti/que-es-gns3/>
- Wallace, K. (2015). *CCNP Routing and Switching ROUTE 300-101 Official Cert Guide*. San Francisco: Cisco Press.

SECCIÓN III: ANEXOS.

En este apartado se agrega información complementaria al trabajo monográfico. Se incluyen las especificaciones y configuraciones de equipos de red utilizados, Sondeo a egresados/titulados sobre MPLS, detalles de software que se usaron y una breve cotización a 2 ISP de Nicaragua sobre los enlaces de datos para una MPLS VPN.

ANEXO I: SONDEO A EGRESADOS Y ENLACES EXTERNOS.

I.I ENLACES A ARCHIVOS DE CONFIGURACIÓN DE ROUTERS.

Los archivos que tienen la configuración global de los Routers están alojados en Google Drive. Son 13 archivos de configuración (uno por cada Router) y se pueden abrir como documentos de texto. El link para visualizar/descargar los archivos es:

https://drive.google.com/drive/folders/1G-wQv76oTMcq9a3EVNjbPvQ_bxvUrRcq?usp=sharing

I.II SONDEO A EGRESADOS/TITULADOS SOBRE MPLS.

Se realizó un sondeo a estudiantes egresados/titulados de la UNI y a un par de estudiantes de otras universidades para darse cuenta el grado de conocimiento que se tiene respecto MPLS, en donde la gran mayoría no tiene conocimiento exacto de lo que es MPLS, unos cuantos han leído y/o escuchado sobre MPLS; pocos han recibido información en la universidad.

Esto indica que el conocimiento sobre MPLS en la comunidad estudiantil es bajo y la manera de obtenerlo es principalmente por la web o una vez trabajen para proveedores de servicios, lo que evidencia la importancia del presente trabajo.

A continuación, se presentan las preguntas que fueron parte del sondeo.

- ✚ ¿Has escuchado el termino MPLS? ¿Dónde?
- ✚ ¿Qué entiendes sobre MPLS? ¿Tienes idea de lo que significan las Siglas?
- ✚ ¿Has recibido información por parte de maestros relacionada con MPLS?
- ✚ ¿Con Qué relacionas MPLS?
 - A. Administración de Redes
 - B. Transporte de Datos.
 - C. Tipo de Servicio.
- ✚ ¿Crees que es necesario tener conocimiento de MPLS antes de ingresar al mundo laboral?

ANEXO II: ESPECIFICACIONES DE EQUIPOS DE RED UTILIZADOS.

II.I ROUTER CISCO SERIE 7200 VXR.

Con velocidades de procesamiento de hasta 2 millones de paquetes por segundo, adaptadores de puerto y servicio que van desde NxDS0 a Gigabit Ethernet y OC-3, así como un número incomparable de servicios IP, la serie Cisco 7200 VXR es el dispositivo perimetral WAN/MAN de agregación de servicios ideal para empresas y proveedores de servicios que implementan cualquier tipo de servicios IP.



Aplicaciones.

- ❖ **Servicios VPN:** Con el nuevo módulo de aceleración de servicios VPN (VSA), cisco 7200 VXR proporciona cifrado asistido por hardware de alto rendimiento, generación de claves y servicios de compresión adecuados para aplicaciones VPN de sitio a sitio.
- ❖ **Servicios de Agregación de Suscriptores de Banda Ancha:** para la agregación de densidad pequeña y mediana para operadores de red, operadores de intercambio local (CLEC) competitivos, proveedores de servicios de Internet (ISP), redes de correos, teléfonos y telégrafos (PTT) y empresas de todo el mundo. Las características clave incluyen:
 - Interfaces flexibles y modulares para la agregación de tráfico: OC-3, Gigabit Ethernet, DS3, Fast Ethernet, Ethernet, POS.
 - IP y ATM QoS/clase de servicio (CoS).
 - VPN MPLS y soporte completo L2TP.
 - Servicios IP ricos en funciones y soporte de terminación PPP.

**UNIVERSIDAD NACIONAL DE INGENIERIA
FACULTAD DE ELECTROTECNIA Y COMPUTACION**

- ❖ **Capacidades Multiservicio:** proporciona una solución de puerta de enlace de voz escalable, que va de 2 a 20 T1 y E1. Las características avanzadas de QoS y multiservicio de la serie Cisco 7200 VXR lo convierten en una plataforma ideal en un gran número de implementaciones empresariales y de proveedores de servicios como CPE multiservicio administrado o como puerta de enlace de voz.
- ❖ **Servicios de red gestionados CPE:** El Cisco 7200 VXR es una solución CPE rentable con una plataforma modular actualizable en campo. Las características clave para los servicios generadores de ingresos incluyen QoS, MPLS (MPLS VPN, MPLS QoS, MPLS TE), servicios de borde WAN (soporte VLAN, NetFlow, NBAR), servicios de seguridad (NAT, ACL, cifrado de hardware para VPN) e integración de voz / video / datos.
- ❖ **Agregación de WAN Empresarial:** Proporciona una solución de agregación flexible que se adapta a una amplia gama de opciones de conectividad y servicio, ofrece alta calidad y confiabilidad, y puede escalar para cumplir con los requisitos futuros. La relación de rendimiento por precio del Cisco 7200 VXR en la gama DS0 a OC-3/STM1 lo convierte en la plataforma ideal para agregar múltiples sucursales o ubicaciones remotas.
- ❖ **Compatibilidad con Puertas de Enlace IP a IP:** las interconexiones IP directas entre redes VoIP reducen los costos, reducen la latencia, mejoran la calidad de la voz y ofrecen una mayor flexibilidad para admitir servicios emergentes en comparación con las interconexiones de redes telefónicas conmutadas públicas (PSTN) o multiplexación por división de tiempo (TDM). El servicio de Cisco IP-to-IP Gateway proporciona un punto de interfaz de red a red para:
 - Protocolos de señalización (H.323, SIP).
 - Funcionamiento de medios (DTMF, fax y módem).
 - Traducciones de direcciones y puertos (ocultación de privacidad y topología).
 - Facturación y normalización de CDR.
 - QoS y gestión del ancho de banda (marcado QoS mediante TOS).

II.II ROUTER CISCO SERIE 3725.

Los enrutadores de la serie Cisco 3700 son enrutadores de acceso modular con conexiones LAN y WAN que se pueden configurar mediante módulos de red intercambiables y tarjetas de interfaz.



La serie Cisco 3700 es una familia de enrutadores modulares que permiten la implementación flexible y escalable de nuevas aplicaciones de comercio electrónico en una plataforma integrada de acceso a sucursales. Ofrece una poderosa solución para el acceso a la oficina remota para los clientes que planean migrar servicios de la infraestructura heredada y distribuir nuevas aplicaciones desde el núcleo hasta el perímetro de la empresa. La implementación de Cisco 3700 Series acelera los beneficios de reducción de costos de las aplicaciones de comercio electrónico para los clientes, reduce el costo total de propiedad de la infraestructura de los clientes y mejora el apalancamiento competitivo de la red.

Los enrutadores Cisco 3725 incluyen las siguientes funciones:

- ✓ Procesador de computadora con conjunto de instrucciones reducido (RISC) de 240 MHz de alto rendimiento.
- ✓ Hasta 256 MB SDRAM.
- ✓ Hasta 128 MB de memoria Compact Flash.
- ✓ Dos ranuras para módulos de red, una de las cuales puede acomodar un módulo de red de doble ancho.
- ✓ Tres ranuras para tarjetas de interfaz.
- ✓ Dos ranuras Cisco 3700 Compact Flash (una externa y otra interna).
- ✓ Dos ranuras AIM.
- ✓ Instalación en un rack de 19 o 23 pulgadas o sobre un escritorio.
- ✓ Compatibilidad con el sistema de alimentación redundante de Cisco.
- ✓ Altura del chasis de 2 unidades de rack (RU).

ANEXO III: COTIZACION DE SERVICIOS DE MPLS VPN A ISP.

En este apartado se dan detalles de los costos de un enlace de datos (VPN) según el ancho de banda que se consideró para la implementación de L3 VPN. Se brindan cotizaciones realizadas a 2 ISP de importancia en Nicaragua como los son CLARO e IDEAY. Para tener detalles más exactos de los costos se preguntó por enlaces de datos ubicados en la zona Sur Oriente del País (Masaya, Granada, Rivas para las sucursales y Jinotepe para casa matriz) con FO como medio.

La siguiente tabla muestra los costos para los enlaces de datos tanto de Casa Matriz como de las sucursales, esto con el ISP – Ideay. La tabla muestra el tipo de servicio (Datos=VPN), el tipo de medio de la última milla por la cual se entrega el servicio, el BW requerido y la última columna el costo individual por servicio.

Sucursal	Servicio	Medio	BW	Costo
Casa Matriz Principal	Datos	FO	80 Mbps	\$ 400
Casa Matriz Respaldo	Datos	FO	60 Mbps	\$ 250
Sucursal Masaya	Datos	FO	20 Mbps	\$ 100
Sucursal Granada	Datos	FO	20 Mbps	\$ 100
Sucursal Rivas	Datos	FO	20 Mbps	\$ 100
Costo Total				\$ 950 x Mes.

Los datos mostrados en la tabla a continuación son del ISP – Claro. La tabla refleja los datos con la misma información presentada en la tabla anterior. Según estos datos se observa que con este ISP el costo de un enlace de datos para un sitio central no es tan alto no así para las sucursales pues el precio se eleva considerablemente, pero aun así son poco más bajos que el otro ISP.

Sucursal	Servicio	Medio	BW	Costo
Casa Matriz Principal	Datos	FO	80 Mbps	\$ 200
Casa Matriz Respaldo	Datos	FO	60 Mbps	\$ 100
Sucursal Masaya	Datos	FO	20 Mbps	\$ 200
Sucursal Granada	Datos	FO	20 Mbps	\$ 200
Sucursal Rivas	Datos	FO	20 Mbps	\$ 200
Costo Total				\$ 900 x Mes.

ANEXO IV: DETALLES DE SOFTWARES UTILIZADOS.

Para la Implementación del diseño de red MPLS L3 VPN llevado a cabo en este trabajo monográfico se han utilizado programas informáticos dado que no se tiene al alcance de equipos de red físicos. A continuación se describe el uso de cada uno de estos programas (en caso exista la necesidad de usar GNS3):

✚ **GNS3 2.2.31 all-in-one.** Software de emulación de los IOS Cisco que ejecutan los Routers físicos. Permite prescindir de Equipos físicos para llevar a cabo la implementación de diferentes topologías de red.

Enlace de Descarga: [Software | GNS3](#)

✚ **GNS3 VM.** Máquina Virtual donde GNS3 corre los IOS de los Routers Cisco. La versión de esta máquina debe ser la misma que el programa GNS3.

Enlace de Descarga: [Software | GNS3 VM](#)

✚ **VMware Workstation Pro 16.** Programa tipo Hipervisor para correr en el sistemas operativos o máquinas virtuales. Se utilizó para correr la máquina virtual GNS3 VM.

Enlace de Descarga: [Descargar VMware Workstation Pro | LATAM](#)

✚ **IOS Cisco.** Para emular los Router Cisco en GNS3 se utilizaron imágenes de Routers c3725 y c7200 tipo Mainline (línea principal y no tren tecnológico).

Enlace de Descarga: <https://drive.google.com/drive/folders/18NG5PcKJrEmrKyLcyaaTL6KDIayn4kGA?usp=sharing>

✚ **Secure CRT 8.1.4.** Software de emulación de terminal con acceso remoto seguro. Se utilizó para acceso remoto vía telnet a los Routers de la topología en GNS3. Se tiene que enlazar con GNS3 previamente.

Enlace de Descarga: [VanDyke Software - Download SecureCRT for Windows, Mac, and Linux](#)

✚ **Enlazar GNS3 con Secure CRT.** Por defecto GNS3 viene seteado para que su programa de terminal sea Putty, por lo que hay que enlazar Secure CRT con GNS3 para que sea el programa terminal por defecto.

Enlace a Video Tutorial: [HOW TO USE SECURECRT IN GNS3 - YouTube](#)