Protocolo Multiprotocol Label Switching (MPLS)

Ana María López Echeverry

Miller Ramírez Giraldo

Edward Fabián Penagos Granada

Protocolo Multiprotocol Label Switching (MPLS) Revisión Teórica

**Ana María López Echeverry
Miller Ramírez Giraldo
Edward Fabián Penagos Granada**

Colección Estado del Arte para Todos
Centro de Innovación y Desarrollo Tecnológico (CIDT)
2018

López Echeverry, Ana María
Protocolo Multiprotocol Label Switching (MPLS). Revisión
teórica / Ana María López Echeverry, Miller Ramírez Giraldo y
Edward Fabián Penagos Granada. -- Pereira : Universidad
Tecnológica de Pereira, 2018.

183 páginas. -- (Colección Estado del arte para todos)

ISBN: 978-958-722-314-9

eISBN:978-958-722-356-9

1. Ingeniería de tráfico 2. Redes de telecomunicaciones 3.
Enrutamiento 4. Procesamiento electrónico de datos 5. Redes
de información 6. Sistemas de transmisión de datos.

CDD 004.66

©Ana María López Echeverry, 2018

©Miller Ramírez Giraldo, 2018

©Edward Facián Penagos, 2018

©Universidad Tecnológica de Pereira, 2018

Primera edición

Universidad Tecnológica de Pereira

Pereira, Colombia

ISBN: 978-958-722-314-9

eISBN:978-958-722-356-9

“Protocolo Multiprotocol Label Switching (MPLS)”.

Esta publicación ha sido realizada por el Grupo de Investigación Nyquist, en el marco del Proyecto Plataforma de Emulación de Servicios Sobre Redes Inteligentes, en el marco del proyecto Centro de Innovación y Desarrollo Tecnológico CIDT en su I Fase de implementación (2014-2017), financiada con recursos provenientes del Fondo de Ciencia, Tecnología e Innovación del Sistema General de Regalías, en asocio con la Gobernación de Risaralda, la Universidad Tecnológica de Pereira, la Alcaldía de Pereira, la Universidad Católica de Pereira, Parquesoft Pereira e Incubar Eje Cafetero.

Universidad Tecnológica de Pereira

Vicerrectoría de Investigaciones, Innovación y Extensión

Editorial Universidad Tecnológica de Pereira

Coordinador editorial:

Luis Miguel Vargas Valencia

luismvargas@utp.edu.co

Tel: 3137381

Edificio 9 Biblioteca central “Jorge Roa Martínez” 9/N1/110

Cra 27 No. 10-02 Los Álamos

Pereira, Colombia

www.utp.edu.co

Montaje y producción:

Universidad Tecnológica de Pereira

Centro de Recursos Informáticos y Educativos CRIE

Impresión y acabados:

Publprint S.A.S.

Pereira

Pereira

Reservados todos los derechos

Autores

Ana María López Echeverry
Miller Ramírez Giraldo
Edward Fabián Penagos Granada

Transcripciones

Lorena Sandoval

Edición

Sello Editorial Universidad Tecnológica de Pereira

SISTEMA GENERAL DE REGALÍAS

Luis Fernando Mejía, Director General, Departamento Nacional de Planeación (DNP)
Mauricio Cárdenas Santamaría, Ministro, Ministerio de Hacienda y Crédito Público
Germán Arce Zapata, Ministro, Ministerio de Minas y Energía
César Ocampo Rodríguez, Director, Departamento Administrativo de Ciencia, Tecnología e Innovación (Colciencias)
Luis Fernando Gaviria Trujillo, Presidente, Órgano Colegiado de Administración y Decisión (OCAD) – Fondo de Ciencia, Tecnología e Innovación, Risaralda

GOBERNACIÓN DE RISARALDA

Sigifredo Salazar Osorio, Gobernador de Risaralda
Diana Yaneth Osorio Bernal, Secretaria de Desarrollo Económico y Competitividad
Adrián Cardona Alzate, Asesor Secretaria de Desarrollo Económico y Competitividad

ALCALDÍA DE PEREIRA

Juan Pablo Gallo Maya, Alcalde de Pereira
Daniel Perdomo Gamboa, Secretario de Educación
Claudia Patricia Velásquez Lopera, Secretaria de Planeación

UNIVERSIDAD TECNOLÓGICA DE PEREIRA

Luis Fernando Gaviria Trujillo, Rector
Martha Leonor Marulanda Ángel, Vicerrectora de Investigaciones, Innovación y Extensión.
Francisco Uribe Gómez, Jefe Oficina de Planeación
Viviana Barney Palacín, Directora CIDT

UNIVERSIDAD CATÓLICA DE PEREIRA

Ptro. Jhon Fredy Franco Delgado, Rector
María Paulina Giraldo, Directora Proyección Social
Andrés Henao Rosero, Decano Facultad de Ciencias Económicas y Administrativas
Yaffa Nahir Ivette Gómez Barrera, Decana Facultad de Arquitectura y Diseño

PARQUESOFT

Johanna Loaiza Mesa, Directora Ejecutiva Parquesoft Risaralda
Alexander Cadavid Giraldo, Director Parquesoft Colombia

INCUBAR EJE CAFETERO

Carlos Alberto Guevara, Director Ejecutivo Incubar Eje Cafetero

ÍNDICE PARTE I

Introducción.....	15
Módulo 1.....	17
Conceptos de Redes MPLS.....	19
Introducción Básica a los Conceptos de MPLS.....	19
Inconvenientes del Enrutamiento IP Tradicional.....	19
Características Básicas de MPLS.....	21
Red ATM.....	22
Planos del Modelo ATM.....	23
Niveles del Modelo ATM.....	23
IP Sobre ATM Clásico.....	24
Modelo de Red Overlay.....	25
Túnel TE MPLS.....	26
Ingeniería de Tráfico (TE).....	26
Diferencias Entre MPLS e IP Sobre ATM.....	28
Etiquetas MPLS.....	28
Etiquetas MPLS: Modo Trama.....	28
Etiquetas MPLS: Modo Celda.....	29
Componentes de Una Arquitectura MPLS.....	30
LSR (Label Switch Router).....	31
ATM LSR.....	31
Arquitectura de las LSRs.....	32
Arquitectura de ATM LSR.....	32
Arquitectura de Edge LSR.....	32
Introducción a las Etiquetas MPLS y Pila (Stack) de Etiquetas.....	33
Pila de Etiquetas.....	33
Reenvío MPLS.....	34
Identificando Aplicaciones MPLS.....	36
Aplicaciones Usadas con MPLS.....	36
Enrutamiento IP Unicast.....	37
Enrutamiento IP Multicast.....	37
MPLS TE.....	37
Calidad del Servicio (QoS).....	38
Redes Virtuales Privadas (VPN).....	38
Módulo 2.....	39
Asignación y Distribución de Etiquetas.....	41
Introducción a la Distribución Típica de Etiquetas en el Modo Trama de MPLS.....	41
Propagación de Etiquetas a través de Una Red.....	41
Rutas Conmutadas por Etiquetas (LSP).....	44
Propagando Etiquetas Utilizando PHP (Penultimate Hop Popping).....	45
Sumarización en LSP.....	47
Asignación de Etiquetas en Una Red MPLS Modo Trama.....	48
Distribución y Aviso de Etiquetas.....	52
Detección de Bucles en el Modo Trama.....	55

Operación Tradicional del TTL.....	55
Detección de Bucles con el TTL.....	56
Traceroute con la Propagación TTL Deshabilitada.....	56
Impacto de Deshabilitar la Propagación del TTL.....	58
Asignación de Etiquetas.....	58
Asignación de Etiquetas por Plataforma.....	60
Beneficios e Inconvenientes de la Asignación de Etiquetas por Plataforma.....	60
Introducción a la Convergencia en el Modo Trama.....	60
Operación del Estado o Comportamiento Estable (Steady-State).....	60
Fallo de Enlace.....	60
Convergencia del Protocolo de Enrutamiento Después de un Fallo.....	61
Recuperación del Enlace.....	61
Introducción a la distribución tradicional de etiquetas sobre interfaces LC-ATM y	
Combinación de Circuitos Virtuales (VC Merge).....	62
Inconvenientes de las Redes MPLS Modo Celda.....	62
Construyendo la Tabla de Enrutamiento IP.....	63
Interfaz LC-ATM.....	64
Solicitud y Asignación de Etiquetas.....	65
Inconvenientes del Intercalado de Celdas.....	68
Inconvenientes del Intercalado de Celdas : Asignación Adicional de Etiquetas.....	69
Combinación de Circuitos Virtuales (VC Merge).....	69
Beneficios:.....	70
Inconvenientes:.....	70
Detección de Bucles en Modo Celda.....	70
Detección de Bucles en Modo Celda: LDP Hop-Count TLV (Type-Length-Value).....	71
Traceroute a través de ATM LSRs.....	71
Introducción a los Modos de Asignación, Distribución y Retención de Etiquetas MPLS.....	72
Asignación de Etiquetas por Interfaz (Per-Interface Label Allocation).....	72
Parámetros de Distribución de Etiquetas.....	73
Retención de Etiquetas.....	75
Descubriendo Vecinos LDP.....	75
Mensajes Hello LDP.....	76
Estableciendo una Sesión LDP.....	76
Establecimiento de la Conexión de Transporte.....	76
Inicialización de la Sesión.....	77
Negociación en una Sesión LDP.....	77
Negociando el Espacio de Etiquetas.....	77
Descubriendo Vecinos LDP.....	78
Mecanismo Discovery Básico.....	78
Mecanismo Discovery Extendido: Vecinos No Adyacentes.....	78
Módulo 3.....	81
Tecnología MPLS para Redes Virtuales Privadas (VPNs).....	83
Introducción a las Redes Virtuales Privadas (VPNs).....	83
Conectividad de Red Tradicional Basada en Router.....	83
Ventajas de las VPNs.....	85
Elementos de una VPN.....	86
Terminología VPN,.....	87

Switched WANs.....	88
Circuitos Virtuales Usados en Switched WANs.	88
Circuitos virtuales conmutados (SVC)	89
Circuitos Virtuales Permanentes (PVC)	89
Red MetroEthernet.....	89
Red MetroEthernet: Proveedor de Servicios.....	90
E-LINE (punto a punto)	91
E-LAN (Multipunto)	92
Introducción a las Redes VPN Overlay y Peer-to-Peer.....	92
Implementación de Tecnologías VPN.	92
Técnicas de Implementación Overlay VPN.	92
En capa 1	92
En capa 2	93
IP Tunneling.....	93
VPN Overlay: Transporte en Capa 2.	94
Enrutamiento Capa 3.....	95
Técnicas de Implementación Para VPNs Peer to Peer.	96
VPNs Peer to Peer: Filtro de Paquetes.	96
VPNs Peer to Peer: Distribución Controlada de Rutas.	97
Beneficios de Implementaciones VPN.	98
Inconvenientes de las Implementaciones VPN.	98
Inconvenientes de la Implementación VPN Peer to Peer Tradicional.	98
Categorizando VPNs.	99
Hub y spoke (hub-and-spoke)	99
Malla completa (Full mesh)	100
Malla parcial (Partialmesh)	101
Categorías de negocio VPN.	102
VPN Intranet.....	103
VPN Extranet.....	103
Access VPN	103
Implementación VPN Peer to Peer.....	104
Categoría de conectividad VPN.	104
Central de Servicios de extranet.....	105
Introducción a la Arquitectura VPN de MPLS.....	105
Arquitectura VPN MPLS.	105
Arquitectura VPN MPLS: Terminología.....	106
Arquitectura de un Router PE en una VPN MPLS.....	106
Métodos de Propagación a través de la P-network.	107
Propagación de la Información de Enrutamiento a través de la P-network.	108
Diferenciadores de Rutas.....	110
Route Targets (RT).	111
Funcionamiento de las RTs.....	113
Redefiniendo VPNs.....	113
Topologías VPN Complejas Sobre las Tablas Virtuales de Enrutamiento.	114
Introducción al Modelo de Enrutamiento VPN MPLS.....	114
Requerimientos de Enrutamiento VPN	114
Modelo de Enrutamiento MPLS VPN.....	114
Perspectiva Global del Cliente.	115

Perspectiva de los Routers P	115
Perspectiva de los Routers PE.	116
Soporte de Enrutamiento Para el Servicio de Internet Existente.	116
Tablas de enrutamiento en routers PE.	119
Flujo de las actualizaciones de enrutamiento de extremo a extremo de la conexión:	
Actualización MP-BGP	119
Distribución de Rutas a Routers CE.....	120
Envío de Paquetes MPLS VPN.....	121
Mecanismos de Envío VPN de Extremo a Extremo.	121
VPN PHP (Penultimate Hop Popping).	123
Efectos de MPLS VPN Sobre el Envío de Paquetes.	124
Bibliografía.....	125

ÍNDICE DE FIGURAS

Módulo 1.

Figura 1. 1: Búsqueda de enrutamiento en cada router en una configuración tradicional.....	20
Figura 1. 2: Topología basada en dispositivos capa 2 y capa 3.....	21
Figura 1. 3: Circuito virtual en una red ATM.	22
Figura 1. 4: Planos y niveles del modelo de referencia ATM.	23
Figura 1. 5: Red IP/ATM.	24
Figura 1. 6: Red IP/ATM desde el punto de vista de un enrutador.	25
Figura 1. 7: Ingeniería de tráfico (TE).....	27
Figura 1. 8: FECs.....	27
Figura 1. 9: Caminos y canales virtuales (VPI/VCI).	29
Figura 1. 10: Edge LSRs y LSRs.....	31
Figura 1. 11: ATM edge LSRs y ATM LSRs.	32
Figura 1. 12: Envío de paquetes en modo trama.....	35
Figura 1. 13: Envío de paquetes en modo celda.....	36

Módulo 2.

Figura 2. 1: FEC en un dominio MPLS.	41
Figura 2. 2: Label Switched Path.....	44
Figura 2. 3: LSPs por entrada en la tabla de enrutamiento principal.	45
Figura 2. 4: Edge LSR sobrecargado.	46
Figura 2. 5: Penultimate Hop Popping.	46
Figura 2. 6: Etiqueta MPLS.	47
Figura 2. 7: Sumarización en un dominio MPLS.....	48
Figura 2. 8: Asignación de etiquetas.....	53
Figura 2. 9: Distribución de etiquetas.	53
Figura 2. 10: Actualización de etiquetas en las tablas LIB, LFIB y FIB.	54
Figura 2. 11: Envío de paquetes a través de rutas etiquetadas.	54
Figura 2. 12: Campo TTL en un dominio MPLS.	55
Figura 2. 13: Traceroute en una configuración tradicional.....	56
Figura 2. 14: TTL deshabilitado.....	57
Figura 2. 15: TTL expirado.	57
Figura 2. 16: Asignación de etiquetas por plataforma.....	59
Figura 2. 17: Asignación de etiquetas por interfaz.	59
Figura 2. 18: Fallo en un enlace en un dominio MPLS.....	61
Figura 2. 19: Recuperación de enlace.	62
Figura 2. 20: Switch en una red ATM.	63
Figura 2. 21: Distribución incorrecta de etiquetas.	64
Figura 2. 22: Solicitud de etiquetas en una red ATM.	64
Figura 2. 23: Correcta distribución de etiquetas en una red ATM.	65
Figura 2. 24: Solicitud de etiquetas 1.....	66
Figura 2. 25: Solicitud de etiquetas 2.....	66
Figura 2. 26: Solicitud de etiquetas 3.....	67
Figura 2. 27: Downstream-on-demand.....	67
Figura 2. 28: Inconvenientes del intercalado de celdas 1.	68

Figura 2. 29: Inconvenientes del intercalado de celdas 2.	68
Figura 2. 30: Asignación de etiquetas por cada router conectado.	69
Figura 2. 31: VC-Merge.	70
Figura 2. 32: LDP Hop-Count TLV.	71
Figura 2. 33: Traceroute a través de ATM LSRs.	72
Figura 2. 34: Asignación de etiquetas por plataforma.	73
Figura 2. 35: Asignación de etiquetas por interfaz.	74

Módulo 3.

Figura 3. 1: Esquema de conexión tradicional.	84
Figura 3. 2: Inconvenientes del esquema tradicional.	84
Figura 3. 3: Enlace compartido a través de un multiplexor.	85
Figura 3. 4: Simulación de redes punto a punto a través de un SP.	86
Figura 3. 5: Elementos de una VPN (1).	86
Figura 3. 6: Elementos de una VPN (2).	87
Figura 3. 7: Conmutación de paquetes a través de Circuitos Virtuales (VC).	88
Figura 3. 8: Red MetroEthernet.	89
Figura 3. 9: Conectividad MetroEthernet.	90
Figura 3. 10: Túneles virtuales MetroEthernet.	91
Figura 3. 11: Funcionamiento IPSec.	94
Figura 3. 12: Perspectiva de una P-network desde los routers del cliente.	95
Figura 3. 13: Participación del SP en el transporte y enrutamiento de datos.	96
Figura 3. 14: Filtro de direccionamiento aplicado sobre un router PE común a los clientes.	97
Figura 3. 15: Distribución controlada de rutas implementando POPs.	97
Figura 3. 16: Topología Hub y Spoke.	100
Figura 3. 17: Topología VPN full mesh.	101
Figura 3. 18: Topología VPN malla parcial.	101
Figura 3. 19: VPN intranet.	103
Figura 3. 20: VPN Extranet.	103
Figura 3. 21: VPN peer to peer.	104
Figura 3. 22: Central de servicios de extranet.	105
Figura 3. 23: Elementos de una red VPN MPLS.	106
Figura 3. 24: Arquitectura de un router PE.	107
Figura 3. 25: IGP exclusivo por cliente.	108
Figura 3. 26: Comunicación directa entre routers PE.	108
Figura 3. 27: Intercambio de rutas de clientes usando los routers P.	109
Figura 3. 28: Enrutamiento basado en un único protocolo de enrutamiento entre routers PE.	109
Figura 3. 29: Diferenciadores de rutas (RD).	111
Figura 3. 30: Route Targets.	112
Figura 3. 31: Troncal VPN MPLS vista desde el cliente.	115
Figura 3. 32: Troncal VPN MPLS vista desde los routers P.	115
Figura 3. 33: Troncal VPN MPLS vista desde los routers PE.	116
Figura 3. 34: Acceso a internet a través de un SP distinto al SP VPN.	117
Figura 3. 35: Redistribución de rutas por defecto.	117
Figura 3. 36: Acceso a internet usando tablas virtuales de enrutamiento.	118
Figura 3. 37: Acceso a internet usando tablas virtuales con rutas VPN y no VPN.	119
Figura 3. 38: Requerimientos cumplidos por routers PE.	119

Figura 3. 39: Flujo de actualizaciones en MP-BGP. 120

Figura 3. 40: Inconvenientes del envío VPN end to end. 121

Figura 3. 41: Stack de etiquetas..... 122

Figura 3. 42: VPN PHP. 123

Introducción

Las redes MPLS (Multi Protocol Label Switching) son un tipo de redes privadas de comunicación ofrecidas por las principales empresas de telecomunicaciones con la peculiaridad que utilizan etiquetas capa 2.5 del modelo OSI para tomar las decisiones de enrutamiento. El protocolo MPLS permite encaminar paquetes de cualquier protocolo de red gracias a estas etiquetas. Este protocolo fue desarrollado con el objetivo de permitirle a los routers tomar decisiones de enrutamiento rápidas¹.

MPLS es un método de alto rendimiento para el envío de paquetes a través de una red, habilitando a los routers de frontera para que apliquen etiquetas sobre los paquetes y por consiguiente se pueden tomar decisiones de enrutamiento basadas en estas etiquetas con una búsqueda que requiere un gasto mínimo. MPLS integra tanto el rendimiento como la gestión de tráfico de la capa de enlace de datos con la escalabilidad y flexibilidad de la capa de red².

1 Procesos y herramientas para la seguridad de redes – p.549.

2 RFC 3031: Multiprotocol Label Switching Architecture.

MÓDULO 1

Conceptos de Redes MPLS

Las redes MPLS (Multi Protocol Label Switching) son un tipo de redes privadas de comunicación ofrecidas por las principales empresas de telecomunicaciones con la peculiaridad que utilizan etiquetas capa 2.5 del modelo OSI para tomar las decisiones de enrutamiento. El protocolo MPLS permite encaminar paquetes de cualquier protocolo de red gracias a estas etiquetas. Este protocolo fue desarrollado con el objetivo de permitirle a los routers tomar decisiones de enrutamiento rápidas³.

MPLS es un método de alto rendimiento para el envío de paquetes a través de una red, habilitando a los routers de frontera para que apliquen etiquetas sobre los paquetes y por consiguiente se pueden tomar decisiones de enrutamiento basadas en estas etiquetas con una búsqueda que requiere un gasto mínimo. MPLS integra tanto el rendimiento como la gestión de tráfico de la capa de enlace de datos con la escalabilidad y flexibilidad de la capa de red⁴.

Introducción Básica a los Conceptos de MPLS

Inconvenientes del Enrutamiento IP Tradicional

Antes de abordar los conceptos básicos de MPLS, se deben destacar algunos de los inconvenientes más destacados en el enrutamiento tradicional⁵:

3 Procesos y herramientas para la seguridad de redes – p.549.

4 RFC 3031: Multiprotocol Label Switching Architecture.

5 High Performance Networks: Simplified!

- Pérdida de conexión.
- Para que el enrutamiento de paquetes fuera posible y se distribuyera la información correctamente, todos los routers (enrutadores) debían mantener una tabla de enrutamiento completa.
- Independientemente del protocolo de enrutamiento, los routers siempre envían paquetes basados únicamente en la dirección de destino. La única excepción es el enrutamiento basado en políticas (policy-based routing o PBR), que es una técnica para tomar decisiones de enrutamiento definida por el administrador de la red tomando en cuenta 5 posibles elementos a emplear (IP fuente, puerto fuente, IP destino, puerto destino y protocolo)⁶.
- La búsqueda de enrutamiento se realiza en cada router, lo que quiere decir, que cada router en la red toma una decisión independiente cuando envía paquetes².

MPLS ayuda a reducir el número de búsquedas de enrutamiento y puede cambiar los criterios de envío. Esta capacidad elimina la necesidad de correr un protocolo de enrutamiento particular en todos los dispositivos.

Cada router en el camino de un paquete realiza una búsqueda de enrutamiento basado en el destino para enviarlo (Fig. 1.1), por consiguiente, cada uno de estos debe revisar toda su tabla de enrutamiento, las cuales en algunas situaciones poseen todas las rutas de internet que actualmente superan las 500.000⁷, lo cual hace que este trabajo pueda ser largo y tedioso si se tiene en cuenta que un paquete puede atravesar por más de un router.

Figura 1.1. Búsqueda de enrutamiento en cada router en una configuración tradicional

6 Screen OS Cookbook – p.677.

7 CIDR report.

En una topología basada en dispositivos de capa 2 (switches o conmutadores) y capa 3 (routers), los dispositivos de capa 2 poseen información de cómo interconectar los dispositivos de capa 3 más no saben sobre la información de enrutamiento que estos manejan, por lo tanto, la topología de una capa y otra puede ser diferente y por consiguiente los saltos (Fig. 1.2) que un paquete debe realizar en una capa u otra es diferente, ya que a nivel de capa dos, los enrutadores tiene direccionamiento estático y saben directamente a donde dirigir un paquete mientras que a nivel de capa 3 se utiliza un protocolo de enrutamiento.

Figura 1.2. Topología basada en dispositivos capa 2 y capa 3

Por otra parte, el enrutamiento basado en el destino no provee un mecanismo para realizar el balanceo de carga a través de caminos con velocidades de transmisión distintas. Las PBR pueden ser utilizadas en estos casos empleando otro tipo de parámetros pero no es una solución escalable.

Características Básicas de MPLS

A continuación se presentan algunas de las características básicas de MPLS⁸:

- MPLS es un nuevo mecanismo de switching (conmutación) que usa etiquetas para enviar paquetes independientemente del protocolo de capa 3 utilizado.
- Es la forma más efectiva de integrar IP y ATM en la misma troncal de la red.
- MPLS no es una red IP, aunque sí utiliza los protocolos de enrutamiento IP tales como OSPF y IS-IS.
- MPLS no es una red ATM, aunque puede utilizar switches ATM reprogramados.
- MPLS puede ser implementado tanto en routers como en switches.
- A pesar de la unión de las tecnologías IP y ATM en MPLS, este reduce la sobrecarga de procesamiento en los routers mejorando el rendimiento del envío de paquetes.
- Las etiquetas usualmente corresponden a direcciones de destino capa 3 igual que como se trabaja con DBR (Destination Based routing o enrutamiento basado en el destino). Las etiquetas también pueden corresponder a otros parámetros tales como calidad del servicio (QoS) o dirección de origen.

- En grandes redes, al utilizar el etiquetado ofrecido por MPLS, se obtiene que solo los routers de frontera realizan una búsqueda de enrutamiento IP mientras que los routers centrales de la red envían paquetes basados en una búsqueda simple de etiquetas e intercambio de estas.

Red ATM.

ATM (Asynchronous Transfer Mode), es un modo de transferencia no síncrono que se popularizó en los 80s como un modelo de referencia para integrar todos los servicios en una sola infraestructura en cuanto a calidad del servicio (QoS), seguridad, eficiencia y rapidez.

Las redes ATM están orientadas a conexión, por consiguiente, para que haya comunicación entre dos dispositivos se debe realizar un intercambio de paquetes de establecimiento de sesión, al finalizar ese proceso se establece la conexión en lo que se conocen como *circuitos virtuales* (VC). Estos VCs atraviesan la subred por todos los switches que pertenezcan a la ruta de envío para que estos creen una entrada en sus tablas internas de enrutamiento sobre la conexión que se creó y reserven recursos para cuando estos sean necesarios.

En la gráfica 1.3 se puede apreciar el circuito virtual (línea roja) creado entre el emisor y el receptor para que todos los paquetes que se envíen empleen esa ruta.

Figura 1.3. Circuito virtual en una red ATM

De acuerdo al modelo de referencia ATM, este se compone de 3 planos y 4 niveles. En la figura 1.4 se puede apreciar cada uno de estos.

A continuación se hace una descripción de los planos y niveles:^{9,10}

9 Redes de computadoras – p.63.

10 Redes de banda ancha – p.45.

Figura 1.4. Planos y niveles del modelo de referencia ATM¹¹

Planos del Modelo ATM

Plano de usuario: Este plano se encarga del tráfico generado por protocolos de capas superiores como IP o desde una aplicación ATM (direcciones ATM de IP/ATM, conexión LAN Emulation, etc.) a través de un SVC o PVC entre dos puntos finales ATM.

Plano de control: Este plano realiza todas las funciones relacionadas con el establecimiento y liberación de las conexiones de los SVCs.

Plano de gestión: Este plano le permite a los dispositivos de igual nivel el intercambio de información específica sobre la gestión (a través de celdas OAM – Operation, Administration and Maintenance) y al mismo tiempo permitir la monitorización de los estados de los elementos de la red ATM y su configuración remota.

Niveles del Modelo ATM.

Nivel físico: Al igual que el modelo de referencia OSI, en la capa física, este nivel proporciona la conectividad física entre elementos de una red ATM.

Nivel ATM: Este nivel conecta las celdas OAM con las conexiones de los circuitos virtuales del plano de usuario.

AAL (Capa de adaptación): Este nivel ofrece una interfaz para adaptar las celdas ATM a las tramas de las aplicaciones y/o protocolos y viceversa.

¹¹ <http://platea.pntic.mec.es/jdelucas/masredes.htm>

Capa de usuario (Capa alta de protocolos y aplicaciones): Emplea los servicios ofrecidos por AAL para los planos superiores.

- El plano de usuario utiliza protocolos como IP junto con las aplicaciones de ATM.
- El plano de control utiliza protocolos como Q.2931 y PNNI 1.0.
- El plano de gestión utiliza protocolos de gestión de elementos de red.

IP Sobre ATM Clásico¹².

Las redes IP sobre ATM (IP/ATM) (Fig. 1.5) surgen como respuesta de los SPs (Proveedores de Servicio) para incrementar la capacidad de sus enlaces, optimización del uso de los recursos existentes y aprovechamiento del ancho de banda de cada enlace disponible.

IP/ATM funciona superponiendo una topología virtual de enrutadores IP sobre una topología física de switches ATM. Cada enrutador de la topología se conecta con los demás PVCs que se construyen sobre la topología física de la red ATM.

Figura 1.5. Red IP/ATM

En lo que respecta a los enrutadores, estos aparecen como si estuviesen en una conexión punto a punto (Fig. 1.6) ignorando la topología subyacente que soporta los PVCs de toda la red.

12 MPLS - IP Sobre ATM – LDC.

Figura 1.6. Red IP/ATM desde el punto de vista de un enrutador

Este modelo de red permite que se aproveche la infraestructura existente de ATM, para obtener un ancho de banda más rápido y económico.

El inconveniente de estas redes es que se deben gestionar dos redes diferentes, una física (ATM) y otra lógica (IP).

Modelo de Red Overlay.

Las redes overlay utilizan el modelo IP/ATM. Por lo que los routers no son conscientes de la topología física que soporta los PVC sino que solo es evidente el único enlace que los une.

Este modelo crea dos niveles separados y superpuestos, en donde los protocolos de enrutamiento de capa 2 y capa 3 trabajan separados. En este caso, los switches ATM no son conscientes de las direcciones IP y de los protocolos de enrutamiento aunque finalmente la red tendrá dos esquemas de direccionamiento y dos protocolos de enrutamiento. Por lo tanto cada sistema, utilizará tanto la dirección IP como la dirección ATM, que no están correlacionadas. Así que es necesario utilizar un protocolo de resolución de direcciones que traduzca una dirección a otra.

Una red overlay es una red virtual de nodos y enlaces lógicos construida sobre la red física.

En términos generales, una red overlay está construida lógicamente sobre una infraestructura física que desconoce, y puede ser utilizada para brindar servicios que la topología física no ofrezca¹³ y de esta manera soportar los requisitos especiales de una clase de aplicaciones particulares o de una determinada comunidad de usuarios.

13 Overlay Networks - UC Berkeley – p.2.

Una red informática P2P o “entre iguales”, se refiere a una red que no tiene clientes y servidores fijos, sino una serie de nodos que se comportan a la vez como clientes y como servidores de los demás nodos de la red ¹⁴ (un tipo de aplicación que no ofrece la topología física directamente).

Túnel TE MPLS

En MPLS, el LSP (Label Switched Path o intercambio de rutas por etiqueta), no es más que un túnel por donde se puede enviar el tráfico entre dos extremos. Este camino o túnel MPLS se crea utilizando LDPs (Label Distribution Protocol o protocolo de distribución de etiquetas) como RSVP-TE (ReSerVation Protocol – Traffic Engineering) o CR-LDP (Constraint-based Routing – Label Distribution Protocol). Una de las diferencias que existe entre MPLS e IP es esa. IP basa su enrutamiento salto a salto, es decir, cada router que recibe un paquete hace una búsqueda en su tabla de enrutamiento para saber cuál es la dirección de siguiente salto, mientras que MPLS ya posee una ruta (LSP) predeterminada para enviar los paquetes de la red. Estos paquetes pasan de un conmutador de etiquetas (LSR) a otro a través de todo el dominio MPLS hasta llegar a su destino.

Ingeniería de Tráfico (TE).

MPLS también soporta TE (Traffic-Engineered)¹⁵. La ingeniería de tráfico (TE) se puede definir como el proceso de distribuir sobre toda la topología de la red el tráfico circundante, con el fin de evitar congestiones y enlaces saturados. La mejora de la utilización de la red no implica necesariamente que se obtenga el mejor camino para toda la red, pero sí el mejor camino para un determinado tipo de tráfico (Fig. 1.7). La ingeniería de tráfico en MPLS debe enfocarse en la optimización del rendimiento de una red e involucra tareas como medición del tráfico, evaluación del rendimiento y control del flujo en el Backbone¹⁶. Los túneles TE pueden ser creados basados en el análisis de tráfico para proveer balanceo de carga sobre caminos con velocidades de transmisión diferente.

14 Development of information systems and services over peer-to-peer overlay networks. Muñoz G. Juan P.

15 RFC 2702: Requirements for Traffic Engineering Over MPLS.

16 Ingeniería de tráfico en redes de conmutación de etiquetas. López S. Danilo, Gelvez G. Nancy – p.2

Figura 1.7. Ingeniería de tráfico (TE)

Cuando existen varias rutas, que requieren los mismos requisitos para el transporte de sus paquetes, estos se agrupan en FECs (Forwarding Equivalence Class). Las FECs (Fig. 1.8) sirven para distinguir los tipos de tráfico que serán enviados por los LSP. Esta asignación se hace una sola vez, de allí que no debe hacer una búsqueda en su tabla de enrutamiento cada vez que llega un paquete como lo hace IP. En MPLS dos routers consecutivos han acordado un valor numérico para brindar conexión a través del LSP, este valor numérico es el valor que toma la etiqueta.

Múltiples túneles TE pueden conducir al mismo destino pero pueden utilizar diferentes caminos. El envío tradicional forzaría a que todo el tráfico usará el mismo camino basado en el destino. TE determina el camino a la fuente basado en parámetros adicionales, tales como los recursos disponibles, calidad del servicio, fuente IP, restricciones en la red entre otros (FECs).

Figura 1.8. FECs

MPLS es estratégicamente importante para la TE porque puede proveer la mayoría de las funcionalidades disponibles en un modelo overlay en una manera integrada, y a un costo más bajo que las demás alternativas¹³.

Diferencias Entre MPLS e IP Sobre ATM

- MPLS se implementa en redes ATM para proveer un enrutamiento óptimo a través de switches ATM capa 2.
- Para que MPLS funcione con switches ATM, estos deben estar ejecutando un protocolo de capa 3.
- Otro beneficio de esta configuración es que no hay necesidad de establecer manualmente VCs. Los switches ATM automáticamente crean una malla completa de VCs basados en la información de enrutamiento de capa 3.

Etiquetas MPLS.

El formato de una etiqueta MPLS se muestra a continuación¹⁷:

- Etiqueta de 20 bits: los valores de 0 a 15 están reservados.
- 3 bits de campo experimental: Usado para definir una clase de servicio (Define las prioridades de cola y políticas de descarte)
- 1 bit pila (stack): MPLS permite que se inserten múltiples etiquetas. Este bit determina si esta etiqueta es la última en el paquete, en cuyo caso tendrá un valor de 1.
- 8 bits del campo TTL: Tiene la misma funcionalidad del campo Time To Live en la cabecera de un paquete IP.

Etiqueta	Exp	S	TTL
20	3	1	8

Etiquetas MPLS: Modo Trama¹⁸.

MPLS está diseñado para usarse en cualquier sitio independientemente del medio y del protocolo de capa 1 y capa 2 utilizado. La mayoría de las encapsulaciones de capa 2 están basados en tramas, y MPLS simplemente inserta una etiqueta de 32 bits entre los encabezados de capa 2 y capa 3 (Modo trama MPLS). En este modo, la etiqueta hace parte de la cabecera

Cabecera capa 2	Cabecera MPLS	Cabecera capa 3	Datos de usuario
-----------------	---------------	-----------------	------------------

17 Conmutación de etiquetas multiprotocolo, Unicauca, Rendón G. Álvarez – p.15.

18 Alcatel-Lucent Network Routing Specialist II (NRS II) Self-Study Guide – pp.496-497.

Ejemplo de funcionamiento:

Un router que recibe un paquete:

- Realiza una búsqueda de enrutamiento para determinar la interfaz por la cual debe enviar el paquete.
- Asigna una etiqueta para ese paquete y la inserta entre la cabecera de la trama de la capa 2 y la cabecera del paquete de capa 3. Si el puerto de salida está habilitado para trabajar con MPLS y existe una etiqueta de salto siguiente para el destino, el router cambia el Ethertype (campo en el Ethernet frame para indicar que protocolo esta encapsulado en el segmento de la trama ethernet) de capa 2 para indicar que es un paquete etiquetado.
- Envía el paquete etiquetado.

Los routers intermedios enrutan el paquete basados en el valor de la etiqueta.

Etiquetas MPLS: Modo Celda.

Las redes ATM son un caso especial ya que estas redes fragmentan los paquetes en celdas (Modo celda MPLS) con un tamaño fijo de 53 bytes y por lo tanto una etiqueta no puede insertarse en cada uno de esos fragmentos (celdas) dada la gran cantidad de espacio requerido. MPLS utiliza los campos identificador de ruta virtual e identificador de circuito virtual (VPI/VCI) de la cabecera ATM como etiqueta para que el modo celda realice las decisiones de envío. Cuando los datos tienen un origen y un destino determinado en una red, para evitar el uso de un canal dedicado para que estos circulen, se aprovecha un único enlace de alta capacidad que permita mezclar estos datos con otros aunque no todos tengan el mismo origen o destino (Fig. 1.9). Para diferenciar unos datos de otros y saber que camino debe ser tomado, se utilizan los identificadores. No obstante como todos viajan por un solo enlace estos canales se llaman virtuales.

Figura 1.9. Caminos y canales virtuales (VPI/VCI)

Ejemplo:

Un router que recibe un paquete.

- Realiza una búsqueda de enrutamiento para determinar la interfaz por la cual debe enviar el paquete.
- El router asigna una etiqueta para ese paquete y la inserta entre la cabecera de la trama de la capa 2 y la cabecera del paquete de capa 3. (La etiqueta completa de MPLS se encuentra presente en todos los paquetes en modo trama, pero en el modo celda sólo se encuentra en la primer celda de un paquete)
- Adicional a la etiqueta, en el modo celda se agrega un encabezado de 5 bytes con tres funciones principales, identificación del canal, información para la detección de errores y si la celda es utilizada o no.
- Envía el paquete. A partir de este momento, el envío de los paquetes se basa sólo en la cabecera ATM.

Componentes de Una Arquitectura MPLS.

MPLS tiene dos grandes componentes¹⁹:

El plano de control (Control plane): El plano de control se encarga del intercambio de información de enrutamiento de capa 3 y el intercambio de etiquetas entre dispositivos adyacentes. Contiene complejos mecanismos para intercambiar información de enrutamiento (OSPF, EIGRP, IS-IS y BGP), y etiquetas (TDP (Tag Distribution Protocol), LDP (Label Distribution Protocol), BGP), y RSVP (Resource Reservation Protocol), este último es empleado por MPLS TE para lograr el intercambio).

El plano de datos (Data plane): El plano de datos se encarga del envío de paquetes basado en la dirección de destino o en las etiquetas. Esto también se conoce como el plano de envío (forwarding plane). La tabla LFIB (Label Forwarding Information Base) se usa para enviar paquetes basados en las etiquetas. Esta tabla está poblada por los protocolos de intercambio de etiquetas (TDP o LDP o ambos) utilizados.

Un protocolo de enrutamiento de capa 3 es necesario para propagar la información de enrutamiento de esta capa. Un mecanismo de intercambio de etiquetas es simplemente un complemento para propagar las etiquetas que son utilizadas para destinos de capa 3.

En términos más sencillos, el plano de control sirve para aprender sobre las rutas para el envío de paquetes, y el plano de datos se utiliza para enviar los paquetes basados en lo aprendido.

¹⁹ MPLS Control Plane and Forwarding Plane Interaction, INE.

LSR (Label Switch Router).

En preparación para una descripción más detallada de MPLS, se presenta una terminología que será utilizada a lo largo del documento.

- LSR (Router conmutador de etiquetas): Dispositivo que envía paquetes basado principalmente en etiquetas.
- Edge LSR: Dispositivo cuya función principal se basa en etiquetar o remover etiquetas de los paquetes.

Los LSRs y edge LSRs usualmente son capaces de hacer la conmutación basados en las etiquetas y enrutamiento IP. Sus nombres están basados en su posición en un dominio MPLS. Todos los routers que tienen habilitados todos los puertos para ejecutar MPLS son llamados LSRs (Fig. 1.10) porque son los que más envían paquetes etiquetados. Los routers que tienen algunas interfaces que no están habilitadas para MPLS están ubicados usualmente en la frontera de un dominio MPLS de un SA. Estos routers también envían paquetes basados en direcciones IP y etiquetas si están las interfaces habilitadas para ello.

Figura 1.10. Edge LSRs y LSRs

ATM LSR

Los LSRs que utilizan el modo celda, están divididos en las siguientes categorías (Fig. 1.11):

- ATM LSRs: Si estos son switches ATM, todas las interfaces están habilitadas para MPLS y el envío de paquetes está basado únicamente en las etiquetas.
- ATM edge LSRs: Segmentan los paquetes en celdas y los envían al dominio MPLS ATM, o re-ensamblan celdas en paquetes y los envían fuera del dominio.

Se debe recordar que estos equipos solo envían celdas, por lo tanto los paquetes entrantes son segmentados (celdas) y nuevamente ensamblados o integrados en un solo paquete antes de abandonar el dominio MPLS.

Figura 1.11. ATM edge LSRs y ATM LSRs

Arquitectura de las LSRs.

Las LSRs de todos los tipos deben realizar estas funciones:

- Intercambiar información de enrutamiento de capa 3. Los ATM LSRs también deben intercambiar información de enrutamiento de capa 3 del plano de control.
- Intercambiar etiquetas (Plano de control).
- Enviar paquetes o celdas (Plano de datos).
- El modo trama debe enviar paquetes basados en las etiquetas de 32 bits.
- El modo celda debe enviar paquetes basado en etiquetas codificadas en los campos VPI/VCI de la cabecera de ATM.

El plano de datos realiza las siguientes tareas:

- Intercambiar información de enrutamiento independientemente del tipo de LSR.
- Intercambiar etiquetas de acuerdo al tipo de MPLS (modo trama o modo celda)

Arquitectura de ATM LSR.

La función principal de un LSR es enviar paquetes etiquetados. Por lo tanto, cada LSR necesita un protocolo de enrutamiento de capa 3 (OSPF, EIGRP, IS-IS) y un protocolo de distribución de etiquetas (LDP, TDP).

LDP llena la tabla LFIB en el plano de datos que es usado para enviar paquetes etiquetados.

Arquitectura de Edge LSR.

Los Edge LSRs también envían paquetes IP basados en la dirección de destino y son etiquetados opcionalmente si existe alguna.

Las siguientes combinaciones son posibles:

- Un paquete IP recibido es enviado basado en la dirección IP de destino y enviado como un paquete IP.
- Un paquete IP recibido es enviado basado en la dirección IP de destino y enviado como un paquete etiquetado.
- Un paquete recibido con una etiqueta es enviado basado en la etiqueta. La etiqueta es cambiada y el paquete es enviado.

Los siguientes escenarios se pueden presentar si la red no ha sido configurada apropiadamente:

- Un paquete etiquetado recibido es desechado si la etiqueta no se encuentra en la tabla LFIB, inclusive si existe el destino IP en la tabla de enrutamiento también llamada Forwarding Information Base (FIB)
- Un paquete IP recibido es desechado si el destino no se encuentra en la tabla FIB, inclusive si hay un camino para enviar paquetes etiquetados hacia el destino indicado en la etiqueta.

Introducción a las Etiquetas MPLS y Pila (Stack) de Etiquetas.

En MPLS, una etiqueta es un identificador de 4 bytes utilizado para identificar un FEC (Forwarding Equivalence Class), o dicho de otra manera, sirve para identificar un grupo de paquetes IP que son enviados de la misma manera (mismo camino, mismo tratamiento, etc.). La etiqueta que se configura en un paquete particular representa el FEC al cual ese paquete está asignado.

Sin embargo, como se verá más adelante, es más provechoso tener un modelo general en el cual un paquete etiquetado pueda contener varias de estas etiquetas organizadas como última en entrar, primera en salir (last-in, first-out stack). A este grupo de etiquetas se le conoce como stack de etiquetas. Un paquete que no está etiquetado puede ser pensado como un paquete cuyo stack de etiquetas está vacío²⁰.

Pila de Etiquetas.

Una etiqueta no contiene ninguna información acerca del protocolo de capa 3 que está siendo transportado en un paquete.

20 RFC 3031: Multiprotocol Label Switching Architecture.

Los siguientes valores del Ethertype (campo en la trama Ethernet para indicar que protocolo esta encapsulado en el segmento de carga útil en una trama Ethernet) de entrada son usados para identificar los protocolos de capa 3 con la mayoría de encapsulaciones de capa 2:

- Unlabeled IP unicast: ID de proceso (0x0800) que indica que los datos de usuario (payload) de la trama es un paquete IP.
- Labeled IP unicast: ID de proceso (0x8847) que indica que los datos de usuario de la trama es un paquete IP unicast con al menos una etiqueta precediendo la cabecera IP. El bit de pila indica cuando comienza la cabecera IP.
- Labeled IP multicast: ID de proceso (0x8848) que identifica que los datos de usuario de la trama es un paquete IP multicast con al menos una etiqueta precediendo la cabecera IP. El bit de pila indica cuando comienza la cabecera IP.

Como se indicó previamente, MPLS soporta múltiples etiquetas en un mismo paquete. Las siguientes aplicaciones pueden agregar etiquetas a un paquete:

- MPLS VPNs: El multiprotocolo Border Gateway Protocol (MP-BGP) es utilizado para propagar una segunda etiqueta adicional a la que fue propagada inicialmente por el TDP o LDP.
- MPLS TE: MPLS TE usa RSVP para establecer túneles LSP. RSVP también propaga otras etiquetas adicionales a las propagadas por LDP o TDP.

Una combinación de estos mecanismos con algunas otras características podría resultar en tres o más etiquetas insertadas en un mismo paquete.

Reenvío MPLS.

Un paquete IP viajando a lo largo de un dominio MPLS puede experimentar las siguientes situaciones²¹:

- Agregación de una etiqueta o stacks de éstas cuando ingrese a un dominio MPLS a través de un edge LSR.
- Intercambiar la etiqueta en el tope del stack con una etiqueta de siguiente salto o un stack de etiquetas en un LSR.
- Remover una etiqueta del tope del stack en el extremo final del túnel LSP (usualmente un salto antes del edge LSR de salida, o también puede realizarse en el de entrada).

ATM LSRs soporta el intercambio de solamente una etiqueta (operación ATM normal).

Los pasos básicos a ser utilizados para el envío de paquetes en el modo Trama (Fig. 1.12) son los siguientes:

21 Understanding MPLS Label Operations on EX Series Switches, juniper.

- Al ingresar un paquete a un dominio MPLS el edge LSR realiza una búsqueda de enrutamiento y le impone una etiqueta.
- Los LSRs intermedios solo intercambian etiquetas pero pueden enviar paquetes que en vez de etiquetas tengan una dirección IP (solo en modo trama).
- Al llegar al edge LSR de salida del dominio MPLS, este remueve la etiqueta y realiza una búsqueda de enrutamiento para enviar el paquete.

Figura 1.12. Envío de paquetes en modo trama

Los pasos básicos a ser utilizados para el envío de paquetes en el modo Celda (Fig. 1.13) son los siguientes:

- Las etiquetas (VPI/VCI) se asignan durante el proceso de búsqueda IP en el ATM Edge LSR de ingreso, y posteriormente los paquetes son divididos en celdas.
- Los ATM LSRs al interior del dominio MPLS intercambian las etiquetas basadas en el contenido de la tabla ATM de conmutación. Los ATM LSRs no pueden enviar paquetes IP.
- En los ATM Edge LSR de salida, se remueven las etiquetas (las celdas son reensambladas nuevamente en paquetes), y se realiza una búsqueda de enrutamiento para enviar los paquetes.

Figura 1.13. Envío de paquetes en modo celda

La diferencia entre el modo trama y el modo celda, es que en el modo trama la etiqueta se le asigna a una dirección y la etiqueta cambia entre LSRs pero con una asignación directa sobre la dirección IP, en cambio en ATM LSRs se hace un intercambio directo entre etiquetas.

Identificando Aplicaciones MPLS.

Aplicaciones Usadas con MPLS.

MPLS puede ser utilizado en múltiples aplicaciones como se describen a continuación^{22,23}:

- Enrutamiento IP unicast es la aplicación más común para MPLS.
- Enrutamiento IP multicast se trata de forma separada debido a los diferentes requerimientos de envío.
- MPLS TE es un complemento en MPLS que provee un uso de los enlaces de forma más inteligente y eficiente.
- Diferentes QoS pueden ser proveídos con MPLS.
- MPLS VPNs están implementadas usando etiquetas para permitir que se traslade el espacio de direcciones entre VPNs.
- Cualquier transporte sobre MPLS (AToMPLS) es una solución para el transporte de paquetes de capa 2 sobre una troncal IP o MPLS.

22 Alcatel-Lucent Network Routing Specialist II (NRS II) Self-Study Guide – p.949.

23 MPLS-Enabled Applications: Emerging Developments and New Technologies – p.164.

El plano de datos (plano de envío) es el mismo independientemente de la aplicación. El plano de control, sin embargo, necesita de mecanismos más apropiados para intercambiar información de enrutamiento y etiquetas.

Independientemente de la aplicación, la funcionalidad de MPLS se divide entre el plano de control y el plano de datos:

- Las aplicaciones solo difieren en el plano de control.
- Todas las aplicaciones usan un plano de datos de conmutación de etiquetas común.
- El plano de datos de un Edge LSR capa 3 puede variar.
- En general, una etiqueta es asignada a un FEC.

El término FEC, es usado para describir los paquetes que son enviados basados en características comunes (IP destino, QoS, etc.).

Enrutamiento IP Unicast.

Una configuración de enrutamiento unicast usualmente requiere de los siguientes dos componentes en el plano de control:

- Un protocolo de enrutamiento IP (OSPF, IS-IS, entre otros): El protocolo de enrutamiento porta la información sobre las redes que son alcanzables.
- Un protocolo de distribución de etiquetas (LDP o TDP): El protocolo de distribución de etiquetas liga las etiquetas a redes aprendidas a través del protocolo de enrutamiento.

Estos dos componentes son suficientes para crear una malla completa de túneles LSP.

A cada red de destino encontrada en la IP forwarding table se le asigna una etiqueta. Esa es la razón por la cual un FEC es asignado a una red específica.

Enrutamiento IP Multicast.

El enrutamiento IP multicast también puede usar MPLS. En este caso no se requiere un protocolo dedicado para soportar tráfico multicast a través de un dominio MPLS.

El FEC es igual a una dirección de destino multicast almacenada en la tabla de enrutamiento multicast.

MPLS TE

MPLS TE tiene los siguientes requerimientos especiales:

- Cada LSR debe ver la topología completa de la red (Solamente IS-IS y OSPF soportan la topología completa).
- Cada LSR necesita información adicional acerca de los enlaces en la red. Esta información incluye recursos disponibles y restricciones. IS-IS y OSPF tienen extensiones para propagar esta información adicional.
- Tanto RSVP o CR-LDP son utilizados para establecer túneles TE y para propagar etiquetas.

Cada Edge LSR debe estar en condiciones de crear estos túneles.

Calidad del Servicio (QoS)

Diferentes tipos de QoS se obtienen utilizando los bits experimentales o creando túneles LSP separados para diferentes clases. Las extensiones a TDP o LDP son usadas para crear múltiples túneles LSP para el mismo destino (uno para cada clase).

Redes Virtuales Privadas (VPN)

Las redes son aprendidas a través de un IGP (IS-IS, OSPF, entre otros) desde un cliente o usando BGP desde otros routers internos.

MPLS VPNs usa una etiqueta adicional para determinar la VPN y la red VPN destino. MP-BGP es usado para propagar información de enrutamiento VPN y etiquetas a través de un dominio MPLS. TDP o LDP es necesario para enlazar los Edge LSRs con un túnel LSP.

En VPN se utilizan dos etiquetas:

- La primera etiqueta apunta al router de salida (Esta etiqueta se asigna a través de LDP o TDP).
- La segunda etiqueta identifica la interfaz de salida sobre el router de salida o a una tabla de enrutamiento donde se desarrolla la búsqueda de enrutamiento.

MÓDULO 2

Asignación y Distribución de Etiquetas.

Introducción a la Distribución Típica de Etiquetas en el Modo Trama de MPLS.

Propagación de Etiquetas a través de Una Red.

Una de las aplicaciones de MPLS es el enrutamiento unicast. Una etiqueta es asignada a las redes de destino IP y más tarde se utiliza para etiquetar paquetes hacia esos destinos (Fig. 2.1). En la terminología de MPLS, un FEC es igual a una red de destino.

Figura 2.1. FEC en un dominio MPLS

Los protocolos de enrutamiento son usados para propagar la información de enrutamiento IP. MPLS agrega una nueva pieza de información que debe ser intercambiada entre routers adyacentes.

A continuación se presentan dos posibles aproximaciones para propagar esta información adicional (etiquetas) entre routers adyacentes:

- Extender la funcionalidad de los protocolos de enrutamiento existentes.
- Crear un nuevo protocolo dedicado al intercambio de etiquetas.

La primera aproximación requiere mucho más esfuerzo y tiempo debido a los diferentes protocolos de enrutamiento que existen. IS-IS, OSPF, entre otros. Este primer enfoque también causa que haya problemas de interoperabilidad entre routers que soporten esta nueva característica con los routers que no. Por lo tanto, el IETF (Internet Engineering Task Force) seleccionó el segundo enfoque creando el protocolo de distribución de etiquetas (LDP) por el MPLS working group²⁴.

El plano de control consiste de un protocolo de enrutamiento que intercambia información de enrutamiento y mantiene el contenido de la tabla principal de enrutamiento.

El LDP o el Tag Distribution Protocol (TDP) propietario de Cisco intercambian las etiquetas en el plano de control y las almacenan en la tabla LIB (Base de información de etiquetas). Esta información se usa luego en el plano de datos para proveer funcionalidad a MPLS como se indica a continuación:

- Se añade una etiqueta en la tabla FIB o Forwarding Información Base (Base de información para el reenvío) para relacionar un prefijo IP a una etiqueta de siguiente salto en la tabla de enrutamiento IP.
- Una etiqueta generada localmente se añade a la tabla LFIB o label forwarding information base (Base de información para el reenvío de etiquetas) y la relaciona con una etiqueta de siguiente salto.

Ejemplo:

- A través de un protocolo de enrutamiento como IS-IS u OSPF un LSR aprendió una red destino con una etiqueta asociada de un LSR anterior.

24 RFC 5036: LDP Specification.

- Posteriormente, la tabla LIB (Label Information Base) mapea esta red con la etiqueta correspondiente al LSR next hop.

- Con esa información aprendida se pasa al plano de datos que es donde se realiza el envío de paquetes, cuando llega una ruta entrante.

En este caso, solo se manejó el aprendizaje y envío basado en etiquetas, cuando se trabaja también con direcciones IP, en el plano de control se mapea la red, y en el plano de datos se utiliza la tabla FIB (Forwarding Information Base).

Los siguientes escenarios de envío son posibles cuando MPLS está habilitado en un router:

- Un paquete IP entrante se envía como un paquete IP. Para enviarlo se utiliza la tabla FIB.
- Un paquete IP entrante se envía como un paquete IP etiquetado. Para enviarlo se utiliza la tabla FIB.
- Un paquete etiquetado entrante se envía como un paquete IP etiquetado. Para enviarlo se utiliza la tabla LFIB.

Rutas Conmutadas por Etiquetas (LSP).

La secuencia de LSRs que un paquete atraviesa hacia un FEC particular (Fig. 2.2), comenzando desde el edge LSR de ingreso hasta el edge LSR de salida se conoce como Label Switched Path (LSP) o ruta conmutada por etiqueta. Los MPLS LSPs son unidireccionales, por lo tanto se requiere un LSP en cada dirección para tráfico bidireccional.

Figura 2.2. Label Switched Path

El camino de un LSP puede ser seleccionado salto-a-salto (hop-by-hop) o especificarse directamente por el nodo origen. Cuando el camino de un LSP es seleccionado salto-a-salto, por ejemplo a lo largo del camino encontrado por el IGP (OSPF, IS-IS), tal LSP es denominado *LSP enrutado salto-a-salto*. En contraste, un LSP cuyo camino está especificado explícitamente en el nodo de origen es llamado TE LSP. El LDP establece el camino LSP salto-a-salto, y el RSVP-TE establece el camino LSP en ingeniería de tráfico²⁵.

Cada LSR intercambia la etiqueta superior del paquete que está atravesando el LSP. En el envío IP unicast MPLS, los FECs están determinados por las redes de destino que se encuentran en la tabla de enrutamiento principal²⁶.

²⁵ Optical Networking Standards: A Comprehensive Guide for Professionals – p.454.

²⁶ Network Dictionary – p.278.

Figura 2.3. LSPs por entrada en la tabla de enrutamiento principal

Por lo tanto, un LSP es creado para cada entrada encontrada en la tabla de enrutamiento principal (Fig. 2.3). Las entradas BGP son la única excepción, no obstante será tratado más adelante.

El IGP se utiliza para llenar las tablas de enrutamiento en todos los routers dentro de un dominio MPLS. LDP o TDP se emplean para propagar las etiquetas en estas redes y construir LSPs.

MPLS TE puede ser usado para que LSP tome un camino diferente al seleccionado por un IGP.

Propagando Etiquetas Utilizando PHP (Penultimate Hop Popping).

En la forma tradicional para el envío de paquetes etiquetados, el edge LSR se sobrecarga (Fig. 2.4) de operaciones MPLS, ya que cuando el paquete llega al router de salida este debe remover la etiqueta y adicionalmente hace una búsqueda de enrutamiento para enviar el paquete fuera del dominio MPLS.

Figura 2.4. Edge LSR sobrecargado

Sin embargo, realizar esta doble búsqueda, primero de etiqueta y luego de dirección IP no es una manera óptima para enviar paquetes etiquetados. Por consiguiente, para solucionar este inconveniente se creó el Penultimate Hop Popping (PHP) que elimina la necesidad de realizar una doble búsqueda en el edge LSR de salida (Fig. 2.5) transmitiéndole esta operación al penúltimo router (el router antes del last hop (edge router) dentro del dominio MPLS). Por ejemplo si existe n LSPs que terminan en el mismo edge router pero con caminos diferentes, estas operaciones pueden distribuirse en los penúltimos routers y no en uno solo²⁷.

Figura 2.5. Penultimate Hop Popping

La función PHP opera de la siguiente manera:

27 MPLS Overview, Juniper.

- El último LSR en el LSP se configura una etiqueta predefinida llamada “Pop”.
- El término Pop en el LFIB significa que sea removida la etiqueta superior en el stack de etiquetas en vez de intercambiarla con la etiqueta de siguiente salto. Por lo tanto, el último router antes del router de salida quita la etiqueta.
- Cuando el paquete llegue al router de salida este evita realizar una búsqueda entre las etiquetas porque ya está listo para hacer el next-hop con el cual solo debe hacer una búsqueda de enrutamiento IP convencional.

El PHP optimiza levemente el rendimiento de MPLS reduciendo tantas búsquedas LFIB en el mismo número de LSPs que terminen en un mismo edge LSR.

Una limitante de PHP es que no funciona en ATM ya que las etiquetas (VPI/VCI) hacen parte de los datos de usuario y no pueden ser removidas.

El campo de etiquetado tiene un tamaño de 32 bits (Fig. 2.6) y hay un campo específico de etiqueta de 20 bits. Los valores del 0 al 15 están reservados. Dos de esos valores son el 1 y el 3 que corresponden a la etiqueta Pop con el valor de 1 para TDP y 3 para LDP. Esta etiqueta le indica a los routers receptores del paquete que remuevan la etiqueta en vez de intercambiarla con una etiqueta de 1 o 3. Entonces lo que será mostrado en la tabla LIB del router será una etiqueta implícitamente nula.

Figura 2.6. Etiqueta MPLS

Sumarización en LSP.

La sumarización en LSP presenta un inconveniente cuando se están transportando rutas más específicas que otras (192.168.0.0/24 es más específica que 192.168.0.0/16, y la primera puede estar sumarizada en la segunda). Si bien son rutas diferentes, en MPLS cada una de estas debe tener un túnel LSP dedicado si ambas aparecen en la tabla principal de enrutamiento. Sin embargo, si hay un LSR intermedio que esté sumarizando (Fig. 2.7) estas rutas, para evitar que muchas rutas específicas se propaguen por la red y la saturen, genera un rompimiento en los túneles LSP en dos, ya que el LDP o TDP propagan etiquetas al mismo tiempo que el IGP distribuye las rutas. Por lo tanto, el LSR que está realizando tareas de sumarización, que se entiende como el extremo final de un LSP, siempre propagará la etiqueta POP a la ruta más general (192.168.0.0/16) que sería la originada en ese router, y asignará una etiqueta con un valor X a la ruta más específica (192.168.0.0/24). Sin embargo,

al ser la ruta sumariada la ruta que se propaga, el router sumariador hará POP y el envío estará basado en direccionamiento IP y no en etiquetas, por lo tanto un router vecino que reciba esta actualización no tendrá como acceder a la red con la etiqueta X ya que esa información fue suprimida en el router sumariador. Aunque el router vecino si podrá volver a utilizar las etiquetas para seguir enviando información a otros routers.

Figura 2.7. Sumarización en un dominio MPLS

Teniendo en cuenta lo anterior, no debe existir sumarización en una red MPLS donde se requiera que exista un túnel LSP de extremo a extremo (como en las VPNs MPLS) o en una red MPLS en modo celda ya que estas redes no pueden enviar paquetes IP.

Asignación de Etiquetas en Una Red MPLS Modo Trama.

Terminología: Los términos upstream y downstream, al igual que ingreso y salida, se refieren a la dirección del flujo de datos. Teniendo esto en cuenta, el término downstream se refiere al flujo de paquetes de datos que van desde el ingreso hasta la salida, y la asignación de etiquetas se distribuyen en la dirección upstream, desde la salida hasta el ingreso. El nodo de salida en un dominio MPLS es el nodo downstream más lejano posible. Este nodo también es conocido como tunnel end point o punto final del túnel.

- El enrutamiento IP unicast y la funcionalidad MPLS pueden ser divididos en los siguientes pasos:
- Intercambio de información de enrutamiento usando un protocolo de enrutamiento (IS-IS, OSPF, entre otros).
- Generación de etiquetas locales (Una única etiqueta local es asignada a cada destino IP encontrado en la tabla principal de enrutamiento y almacenado en la tabla LIB). Los LSRs anuncian sus etiquetas asignadas a los otros LSRs.
- Propagación de etiquetas locales a routers adyacentes, donde estas etiquetas podrían ser usadas como etiquetas de salto siguiente (almacenadas en las tablas FIB y LFIB para habilitar la conmutación de etiquetas).

De acuerdo a las etiquetas recibidas, los LSRs construyen su estructura de datos (LIB, LFIB y FIB).

Las siguientes estructuras de datos contienen información de las etiquetas:

- El LIB (Label Information Base) se encuentra en el plano de control y es la base de datos usada por LDP donde un prefijo IP está relacionado con una etiqueta que solo tiene un significado local y con una etiqueta de salto siguiente que ha sido aprendida de un vecino downstream.

- El LFIB (Label Forwarding Information Base) se encuentra en el plano de datos y es la base de datos usada para enviar paquetes etiquetados. Las etiquetas locales propagadas previamente a los upstream neighbors son relacionadas con las etiquetas de salto siguiente, recibidas previamente de los downstream neighbors.

- El FIB (Forwarding Information Base) se encuentra en el plano de datos y es la base de datos usada para enviar paquetes IP sin etiquetar. Un paquete enviado es etiquetado si una etiqueta de salto siguiente está disponible para un red IP destino específica. De otra manera, un paquete IP no es etiquetado.

Cuando una etiqueta es asignada a un prefijo IP de una red, esta se almacena en dos tablas:

- Tabla LIB: Esta tabla se utiliza para mantener la correspondencia entre el prefijo IP (de una red cualquiera), el tipo de etiqueta (local o de un vecino), y la etiqueta de siguiente salto (cuando es la primera vez que se está asignando una etiqueta a una red, la etiqueta de siguiente salto todavía no se encuentra disponible ya que no se han propagado).

- Tabla LFIB: Esta tabla contiene la etiqueta local, la acción que debe realizar y el salto siguiente. La primera vez que se generan las etiquetas, la acción que debe tomar esta tabla es el pop, y se utiliza hasta que haya una etiqueta de siguiente salto para la red.

Las estructuras LIB y LFIB tienen que ser inicializadas en el LSR que asigna la etiqueta.

Distribución y Aviso de Etiquetas.

A continuación se describe el proceso de asignación y distribución de etiquetas:

- Cada LSR asigna una etiqueta para cada destino en la tabla de enrutamiento IP (Fig. 2.8). Este proceso de asignación es asíncrono, es decir, cada LSR puede asignar una etiqueta a un destino sin que los demás lo hayan hecho (Las etiquetas solo tienen un significado local, de allí que deban intercambiarse antes de ser enviadas a otro router).

- En cada LSR, la etiqueta generada se almacena en dos tablas creadas: la tabla LIB y la tabla LFIB.

Figura 2.8. Asignación de etiquetas

- El router que generó la etiqueta debe propagarla a todos sus vecinos LSRs independientemente de si estos son upstream o downstream (Fig. 2.9). Esta etiqueta será utilizada como etiqueta de salto siguiente.

Figura 2.9. Distribución de etiquetas

- Una vez que un router reciba una actualización LDP este puede llenar la pieza faltante en sus tablas LIB, LFIB y FIB como se muestra en la figura 2.10:
- La etiqueta recibida es almacenada en la tabla LIB como la etiqueta para llegar a una determinada red (desde el router que generó la etiqueta).
- La etiqueta recibida se agrega a la tabla FIB para habilitar la funcionalidad de frontera de MPLS (Paquetes IP entrantes sean enviados como paquetes etiquetados).
- La etiqueta local en la tabla LFIB crea una correspondencia hacia la nueva etiqueta recibida en vez de hacer la acción pop (los paquetes entrantes que estén etiquetados

pueden ser enviados como paquetes etiquetados), porque ya existe una etiqueta de salto siguiente.

Figura 2.10. Actualización de etiquetas en las tablas LIB, LFIB y FIB

- Los paquetes IP enviados, son etiquetados solamente en los segmentos del camino donde las etiquetas han sido asignadas (Fig. 2.11).

Figura 2.11. Envío de paquetes a través de rutas etiquetadas

Una vez estas tablas estén completas se entiende que MPLS está funcionando totalmente.

Detección de Bucles en el Modo Trama.

La detección de bucles en una red MPLS se basa en más de un mecanismo.

La mayoría de los bucles de enrutamiento son prevenidos por el IGP de la red. En el envío de paquetes IP unicast simplemente se usa el camino más corto determinado por el IGP. Estos caminos generalmente están libres de bucles.

No obstante, un bucle de enrutamiento puede ocurrir (por ejemplo por rutas estáticas mal configuradas), por tal motivo, las etiquetas de MPLS también contienen un campo de Tiempo de Vida (TTL) que previene que los paquetes caigan en un bucle infinito.

La funcionalidad del TTL en MPLS es igual al utilizado en el envío de paquetes IP tradicional. Cuando un paquete IP es etiquetado, el valor del TTL de la cabecera IP se copia al campo TTL en la cabecera de la etiqueta. Esto se llama propagación TTL.

Operación Tradicional del TTL.

El TTL opera de la siguiente manera²⁸:

- Cuando un paquete IP ingresa a un dominio MPLS (Fig. 2.12), el TTL se copia desde la cabecera IP hasta la cabecera de la etiqueta (Únicamente se modifica el TTL de la etiqueta al interior del dominio MPLS, el TTL de la cabecera IP permanece igual).
- Cuando el paquete etiquetado va a salir del dominio MPLS, el TTL se copia desde la cabecera de la etiqueta a la cabecera IP.

Figura 2.12. Campo TTL en un dominio MPLS

28 RFC 3034: Use of Label Switching on Frame Relay Networks Specification.

Detección de Bucles con el TTL.

Los paquetes etiquetados son desechados cuando el TTL llega hasta 0²⁹.

Por otra parte, en caso de que no se quiera tener la opción del TTL, esta se puede deshabilitar.

La propagación del TTL puede deshabilitarse para esconder los routers centrales de los usuarios finales. Al deshabilitar la propagación del TTL provoca que los routers establezcan un valor de 255 en este campo cuando un paquete IP está etiquetado³⁰.

Aunque se deshabilite esta opción la red todavía está protegida en contra de bucles indefinidos, pero es poco probable que los routers centrales tengan que enviar una respuesta ICMP a un usuario generando paquetes traceroute, ya que los traceroute a través de un dominio MPLS no muestran ningún router central.

Traceroute con la Propagación TTL Deshabilitada.

En la forma tradicional, la primera vez que un usuario realiza un traceroute, el edge LSR desechará el paquete (Fig. 2.13) y enviará un mensaje de ICMP de TTL expirado al emisor.

Figura 2.13. Traceroute en una configuración tradicional

La segunda vez que el emisor haga un traceroute el TTL se aumentará en 1 y con este mensaje sería suficiente para conocer sobre la existencia de un router (un salto adicional) al interior del dominio MPLS y a medida que se incrementa el valor del TTL, irá conociendo sobre todos los routers por los que atraviesa un paquete al interior de una red. Sin embargo,

²⁹ RFC 3063: MPLS Loop Prevention Mechanism.

³⁰ Disabling Normal TTL Decrementing, Juniper.

cuando el TTL se ha deshabilitado en el dominio MPLS (Fig. 2.14) la segunda vez que un emisor envíe un traceroute con el TTL igual a 2, al interior del dominio MPLS se restará este valor en 1 pero el edge LSR no copia el TTL que viene del exterior sino que establece su valor en 255 en el TTL de la etiqueta.

Figura 2.14. TTL deshabilitado

De esta manera el paquete irá pasando por todos los routers hasta llegar al otro extremo del dominio MPLS. Cuando el paquete llegue al router de frontera, este volverá a restablecer el TTL original del paquete IP y desechará el paquete porque en ese momento el TTL tendrá un valor de cero y expirará (Fig. 2.15), por lo tanto enviará un mensaje de TTL expirado al emisor.

Figura 2.15. TTL expirado

Deshabilitando el TTL, el usuario solo conocerá la existencia de los Edge LSRs y no sabrá de los routers centrales³¹.

Impacto de Deshabilitar la Propagación del TTL.

Si se desea deshabilitar la propagación TTL, se debe asegurar que se realice en todos los routers del dominio MPLS.

El TTL puede ser habilitado de manera opcional únicamente para el tráfico enviado desde fuera del dominio MPLS, lo cual le permite a los administradores usar traceroute desde los routers centrales para la resolución de problemas en la red. El traceroute ejecutado desde los LSRs no usa el valor inicial de 255.

Asignación de Etiquetas.

A continuación se presentan dos posibles enfoques para la asignación de etiquetas en una red³²:

- Asignación de etiqueta por plataforma: Un espacio de etiquetas por plataforma (Fig. 2.16) es un pool de valores de etiquetas definidas para el router completo. Normalmente, la tabla LFIB no tiene asociada una interfaz específica, por tanto, el espacio de etiquetas es asignado a una red destino (FEC) y anunciada a todos los vecinos. La etiqueta debe ser única localmente y puede ser usada en todas las interfaces, pero las etiquetas que son asignadas a diferentes FECs no pueden tener el mismo valor.
- Como se ve en la figura al lado izquierdo, el enrutador puede asignar el mismo valor de etiqueta a varias interfaces siempre y cuando estas sean utilizadas para llegar al mismo destino ya que ese valor es propagado a todos los vecinos. Sin embargo, cuando una de las interfaces se asocia con un FEC, ésta ya no puede tener el mismo valor usado en todas las interfaces del router y debe cambiarse, convirtiéndose única para un tráfico específico y por lo tanto no puede ser usada por otras interfaces así la etiqueta pertenezca a un pool por plataforma. Por eso, en el diagrama de la izquierda en dos interfaces las etiquetas cambiaron puesto que se asociaron a un FEC.
- Esta es la operación por defecto en el modo trama.
- Asignación de etiqueta por interfaz: Un espacio de etiquetas por interfaz es un pool de valores de etiquetas definidos para cada interfaz (Fig. 2.17) en la cual MPLS esté habilitado. Con el espacio de etiquetas por interfaz, las etiquetas únicas de cada interfaz se pueden asignar a un FEC en un formato basado por interfaz. En este caso, la etiqueta asignada a una interfaz puede ser reusada sobre otra interfaz con un FEC diferente. Sin embargo, estas etiquetas deben ser únicas para cada interfaz.

31 Disabling Normal TTL Decrementing, Juniper.

32 MPLS for Metropolitan Area Networks – p.21.

Figura 2.16. Asignación de etiquetas por plataforma

Figura 2.17. Asignación de etiquetas por interfaz

El espacio de etiquetas por plataforma usa menor cantidad de recursos que los empleados por interfaz porque la misma etiqueta se propaga a todas las interfaces³³.

Asignación de Etiquetas por Plataforma.

Beneficios e Inconvenientes de la Asignación de Etiquetas por Plataforma.

Inconvenientes: Un router adyacente puede enviar paquetes con una etiqueta que no le han anunciado previamente (label spoofing). Si la conmutación de etiquetas no ha sido habilitada por la interfaz que se está recibiendo el paquete con el label spoofing, el paquete se desechará, pero si esa funcionalidad si está habilitada sobre dicha interfaz, el paquete podría ser enviado causando un posible problema de seguridad ya que un vecino LSR puede enviar paquetes con cualquier etiqueta en el LFIB.

Beneficios: Se generan tablas LIB y LFIB más pequeñas por lo tanto el intercambio de etiquetas es más rápido.

Introducción a la Convergencia en el Modo Trama.

Operación del Estado o Comportamiento Estable (Steady-State).

Como se mencionó anteriormente, MPLS se encuentra completamente funcional cuando el IGP y el LDP (o TDP) han llenado todas las tablas de los LSRs que se mencionan a continuación:

- Tabla principal de enrutamiento.
- Tabla LIB.
- Tabla FIB.
- Tabla LFIB.

Aunque LDP toma un tiempo algo extenso para intercambiar etiquetas (comparado con IGP), una red puede usar la tabla FIB mientras LDP converge, de esta manera no hay tiempo de inactividad de enrutamiento mientras LDP intercambia etiquetas entre LSRs adyacentes.

Fallo de Enlace.

Cuando se presenta un fallo en el enlace de un dominio MPLS todas las entradas que pertenezcan a ese enlace caído se retiran de las tablas donde se encuentra.

33 Alcatel-Lucent Network Routing Specialist II (NRS II) Self-Study Guide – p.504.

A continuación se indica cómo se maneja un fallo en el enlace en un dominio MPLS.

- La convergencia global y total de la red depende de la convergencia del IGP usado en el dominio MPLS.
- Cuando un router pierde el enlace con un router vecino (Fig. 2.18) y tiene un camino alternativo, determina que este último debe ser el nuevo camino para alcanzar la red y etiqueta los paquetes de acuerdo a la nueva ruta establecida.

Tabla de enrutamiento R1		Red [X]	Salto siguiente [R2]		X
FIB R1		Red [X]	Salto siguiente [R2]	Etiqueta = 15	X
LFIB R1		Etiqueta local = 10	10 → 15	Salto siguiente [R2]	X
LIB R1		Red [X]	Etiqueta local	10	X
			R2	15	
			R3	5

Figura 2.18. Fallo en un enlace en un dominio MPLS

El LDP almacena todas las etiquetas en la tabla LIB, inclusive si las etiquetas no son usadas, porque puede que el IGP decida usar otro camino en caso de fallo y así poder determinar cuál es la etiqueta de siguiente salto para el destino.

Convergencia del Protocolo de Enrutamiento Después de un Fallo.

Después de que un IGP determine que hay otro camino disponible, se crea una nueva entrada en la tabla FIB. Esta nueva entrada apunta hacia el router del camino alternativo. Con esta información las tablas FIB y LFIB enrutan el LSP a través del nuevo router del camino alternativo.

La convergencia MPLS en el modo trama no afecta el tiempo de convergencia global. La convergencia de MPLS ocurre inmediatamente después de la convergencia del protocolo de enrutamiento basado en las etiquetas almacenadas en el LIB.

Recuperación del Enlace.

Cuando se recupera un enlace (Fig. 2.19), el IGP es quien determina que este se encuentra disponible nuevamente y cambia la dirección de siguiente salto hacia la red a través del

enlace que se acaba de levantar. Sin embargo, cuando el router trate de establecer la etiqueta de siguiente salto para la red, debe esperar a que converjan las sesiones LDP para poder que se actualicen las tablas.

Figura 2.19. Recuperación de enlace

Para no detener el envío de paquetes, se aplica una acción POP en la tabla LFIB del router emisor mientras se establece la sesión LDP, y mientras tanto se utiliza enrutamiento basado en la dirección destino. Este proceso adiciona un retardo adicional al tiempo de convergencia global en MPLS. El tiempo de inactividad en la red de destino, no se ve afectada por la convergencia LDP ya que los paquetes IP siguen siendo enviados tradicionalmente hasta que la etiqueta de salto siguiente esté disponible nuevamente. El tiempo de inactividad de la red destino solo se ve afectada cuando la convergencia está siendo realizada por el IGP. MPLS TE puede ser utilizado para prevenir un tiempo de inactividad prolongado cuando un enlace falla o cuando se está restableciendo.

Aunque este comportamiento no tiene un impacto significativo en el enrutamiento IP tradicional, si puede influenciar significativamente las redes MPLS VPNs debido a que el tráfico VPN solo puede ser enviado hasta que la sesión LDP esté operando completamente.

Introducción a la distribución tradicional de etiquetas sobre interfaces LC-ATM y Combinación de Circuitos Virtuales (VC Merge).

Inconvenientes de las Redes MPLS Modo Celda.

El modo Celda posee unas diferencias significativas respecto al modo trama debido a algunos requerimientos específicos de ATM como las que se indican a continuación:

- ATM utiliza Celdas y no tramas. Un único paquete puede ser encapsulado en múltiples celdas. Las celdas tienen una longitud fija, lo que significa que las etiquetas normales no pueden ser usadas porque podrían incrementar el tamaño de la celda (El tamaño de un datagrama IP es de longitud variable y puede pasar los miles de bytes hasta 65.535 bytes, mientras que una celda posee un tamaño fijo de 53 bytes). El campo de identificador VPI/VCI en la cabecera ATM es usada como una etiqueta MPLS. Un túnel LSP es por lo tanto llamado circuito virtual en la terminología de ATM
- Los Switches y routers ATM usualmente tienen un número limitado de circuitos virtuales que puedan usar. MPLS establece una malla completa de túneles LSP (en este caso circuitos virtuales), lo que puede resultar en un número extremadamente grande de túneles ya que se incrementará en la cantidad de veces que el paquete se fragmente, puesto que cada cabecera de una celda posee el identificador VPI/VCI.

En conclusión, las etiquetas en el modo Celda son un recurso limitado.

Construyendo la Tabla de Enrutamiento IP.

Aunque en el modo celda no se puedan enviar paquetes IP, el establecimiento de sesiones entre routers adyacentes y búsqueda de caminos en caso de fallo de un enlace, tanto como la construcción de la tabla de enrutamiento requiere de un IGP.

En el plano de control, cada Switch ATM actúa como un router IP, y las tablas de enrutamiento se construyen como si los Switches fueran routers. Por tal motivo, estos switches se ven como un salto IP adicional en la red (Fig. 2.20).

Figura 2.20. Switch en una red ATM

Debido a que los switches ATM no pueden enviar paquetes IP, las etiquetas no pueden ser asignadas y distribuidas asincrónicamente (ya que no habría flujo de datos) como se ve en la figura 2.21.

Figura 2.21. Distribución incorrecta de etiquetas

En vez de ello, el router inicia una secuencia ordenada de solicitudes (Fig. 2.22) sobre el lado upstream de la red ATM.

La tabla de enrutamiento se encuentra poblada cuando la solicitud ha recibido una respuesta con la etiqueta asignada a los destinos IP de la tabla de enrutamiento.

Figura 2.22. Solicitud de etiquetas en una red ATM

Interfaz LC-ATM

Una interfaz label-switching-controlled ATM (LC-ATM) es una interfaz ATM controlada por el componente de control de conmutación de etiqueta. Cuando un paquete atraviesa por dicha interfaz, este se trata como si fuera un paquete etiquetado. Cualquier par de routers o switches ATM con una conexión LDP a través de una interfaz LC-ATM usarán la

negociación LDP para determinar qué tipo de etiqueta será usada sobre esa interfaz si VCI o una combinación de VPI/VCI^{34,35}.

Solicitud y Asignación de Etiquetas.

Las etiquetas tienen que ser solicitadas explícitamente sobre las interfaces LC-ATM. Un router debe solicitar una etiqueta para cada destino en la tabla de enrutamiento con el next-hop alcanzable sobre una interfaz LC-ATM.

Figura 2.23. Correcta distribución de etiquetas en una red ATM

Un switch ATM puede responder una solicitud de etiqueta de siguiente salto solo si este ya tiene asignada una etiqueta de salida para la red a la cual apunta la etiqueta de la solicitud entrante (Fig. 2.23). Solo puede operar de esta forma ya que estas redes no pueden realizar búsqueda IP.

Ejemplo: Un router externo (Emisor) en la figura 2.24, envía un paquete a un dominio MPLS en modo celda para llegar a la red X a través del router de frontera (ER1).

34 RFC 4368: Multiprotocol Label Switching (MPLS) Label-Controlled Asynchronous Transfer Mode (ATM) and Frame-Relay Management Interface Definition.

35 RFC 3035: MPLS using LDP and ATM VC Switching.

Figura 2.24. Solicitud de etiquetas 1

El edge LSR de ingreso (ER1) envía el paquete al switch ATM (S1). Como este switch no puede hacer búsqueda de direcciones IP (Fig. 2.25), este no tiene permitido responder con su etiqueta local a menos que ya tenga la etiqueta de siguiente salto.

Figura 2.25. Solicitud de etiquetas 2

Debido a que S1 no tiene una etiqueta de salto siguiente, le envía la solicitud al siguiente vecino (Fig. 2.26), y así sucesivamente hasta que llegue al otro router de frontera (ER2) o switch que sí tenga configurado una etiqueta de salto siguiente.

Figura 2.26. Solicitud de etiquetas 3

ER2 regresa la solicitud al switch anterior (S2) con su etiqueta local (Fig. 2.27) y de esta manera S2 podrá responderle S1 con su etiqueta local puesto que ya tiene configurada una etiqueta de salida para la red solicitada. Esta operación se conoce como asignación de etiquetas “downstream-on-demand”³⁶. Al igual que en el modo trama, la etiqueta recibida se almacena en las tablas LIB, FIB y LFIB.

Figura 2.27. Downstream-on-demand

Un segundo router (Emisor2) realiza una solicitud de etiqueta similar al caso anterior para llegar a la misma red X (Fig. 2.28). El LSR que reciba esa solicitud responderá inmediatamente pero enviará una etiqueta local diferente a la que tiene en sus tablas. Esto sucede porque los switches ATM usan valores VPI/VCI por interfaz, lo que quiere decir que las etiquetas deben ser únicas por cada interfaz, por consiguiente no pueden ser reutilizadas.

Figura 2.28. Inconvenientes del intercalado de celdas 1

La situación anterior provoca que ahora el S1 posea dos etiquetas locales en su LFIB para enviar paquetes hacia un mismo destino.

Inconvenientes del Intercalado de Celdas.

Si por alguna circunstancia el router o switch que tiene dos etiquetas locales (S1 en el ejemplo anterior), recibe una solicitud hacia el mismo destino desde los dos routers que tiene conectados (los que generaron sus dos etiquetas locales) al mismo tiempo, estos dos circuitos virtuales se combinarán en uno solo ya que la etiqueta de salida desde S1 hasta S2 es la misma (Fig. 2.29). No obstante, el hardware de conmutación virtual de ATM estándar no soporta esta situación, y por consiguiente, los paquetes de dos fuentes diferentes que han sido divididos se pueden intercalar en el proceso de emisión y recepción de fragmentos entre routers.

Figura 2.29. Inconvenientes del intercalado de celdas 2

Por lo tanto, el router receptor está imposibilitado para re-ensamblar esas celdas en dos paquetes diferentes porque desde su punto de vista son uno solo. A continuación se presentan dos posibles soluciones:

- Asignar una nueva etiqueta downstream para cada solicitud. Esta solución resultaría en un número elevado de etiquetas.
- Almacenar en un buffer las celdas del segundo paquete hasta que todas las celdas del primer paquete se envíen. Esta solución da como resultado un retraso mayor en la entrega de paquetes debido al buffering.

Inconvenientes del Intercalado de Celdas. : Asignación Adicional de Etiquetas.

Una de las opciones para solucionar el problema de intercalado es asignar una etiqueta local para cada router que realice una solicitud.

Este método consiste en realizar una solicitud de etiqueta como si ninguno tuviera configurado una etiqueta de siguiente salto hasta que el edge router devuelva la solicitud marcando una etiqueta local nueva para cada solicitud realizando “downstream-on-demand”. Sin embargo, como se ve en la figura 2.30, la cantidad de información por cada tabla sería muy elevada si se tiene en cuenta que pueden haber *n* solicitudes desde *n* sitios diferentes.

Figura 2.30. Asignación de etiquetas por cada router conectado

Combinación de Circuitos Virtuales (VC Merge).

- VC Merge es una solución en la cual las celdas entrantes se bloquean hasta que la última celda llegue al siguiente router (Fig. 2.31).
- Cuando llegan todas las celdas del primer paquete, las celdas del otro paquete que se encuentran en el buffer se envían al next-hop ATM LSR.

Esta opción reduce el número de etiquetas (circuitos virtuales) necesitados en una red ATM, pero incrementa el retardo promedio en toda la red.

Figura 2.31. VC-Merge

Beneficios:

- El mayor beneficio de VC merge es que minimiza el número de etiquetas (valores VPI/VCI) necesitados en la parte ATM de la red, ya que estas pueden ser reutilizadas.

Inconvenientes:

- Los requerimientos de buffering en el ATM LSR son mayores.
- Hay un mayor incremento en el retardo de entrega de paquetes.
- Las redes ATM con una carga pesada se parecen más a las redes basadas en tramas.

Detección de Bucles en Modo Celda.

Cuando se despliega MPLS a través de switches y routers ATM que tienen interfaces LC-ATM, el mecanismo usado para la detección y prevención de bucles en el modo trama no son los adecuados para este tipo de entorno porque el modo celda de MPLS en su cabecera no incluyen un campo TTL. Por lo tanto, este modo debe usar otros mecanismos para prevenir bucles de enrutamiento³⁷.

Una vez más, los bucles se previenen por el IGP de la red. Sin embargo, si hay un bucle, LDP puede identificar las solicitudes LDP que generan el bucle.

37 MPLS and VPN Architectures, Vol. – p.182.

Detección de Bucles en Modo Celda: LDP Hop-Count TLV (Type-Length-Value).

LDP usa un atributo contador de saltos TLV (Type, Length, Value) (Fig. 2.32) para contar saltos en un LSP en la parte ATM del dominio MPLS. Un Hop Count TLV contiene un contador de los LSRs que el mensaje ha atravesado³⁸.

Figura 2.32. LDP Hop-Count TLV

Este contador de saltos puede ser usado para proveer un manejo correcto del TTL desde los ATM edge LSRs a nombre de un ATM LSRs que no pueda procesar paquetes IP. El número máximo de saltos puede ser configurado.

El campo TTL en la cabecera IP o cabecera de etiqueta se decrementa en el número de saltos por el ATM edge LSR de ingreso antes de ser enviado a través de un LVC (Label Virtual Circuit). Si el paquete tiene un TTL de 0 menos, el paquete se descarta.

Traceroute a través de ATM LSRs.

El traceroute se basa en el LDP Hop-Count. Con el Hop Count, el router de frontera conoce cuantos saltos existen al interior de la red desde el ingreso hasta la salida.

En el modo trama se copiaba el TTL de la cabecera del paquete IP entrante, en este caso como los ATM Switches no trabajan con TTL, cada vez que llegue un paquete traceroute se le resta el valor del Hop-Count al valor del TTL del traceroute. Si el valor del TTL no es mayor al Hop-Count el paquete será desechado. Cada que un paquete sea desechado (o reportado por ICMP al origen) el TTL incrementará en uno hasta que finalmente sea mayor que el Hop-Count y de esta manera podrá a travesar la red y conocer el ultimo router de frontera (Fig. 2.33).

38 RFC 5036: LDP Specification.

Figura 2.33. Traceroute a través de ATM LSRs

Introducción a los Modos de Asignación, Distribución y Retención de Etiquetas MPLS.

Asignación de Etiquetas por Interfaz (Per-Interface Label Allocation)

El modo celda de MPLS usa por defecto el espacio de etiqueta por interfaz debido a que los Switches ATM soportan valores VPI/VCI por interfaz para codificar en etiquetas. Por lo tanto, si un router tiene dos enlaces paralelos al mismo switch ATM, se establecen dos sesiones LDP y dos solicitudes de etiquetas por separado.

El LFIB en un switch ATM (se conoce como matriz de conmutación ATM) siempre contiene la interfaz de entrada de los paquetes. Cada etiqueta debe ser asignada a una interfaz individual, pero la misma etiqueta puede ser utilizada en interfaces diferentes pero con significados diferentes.

Asignar las etiquetas por interfaz aumenta la seguridad previniendo la suplantación de etiquetas (label spoofing), ya que los paquetes etiquetados (o celdas ATM) son aceptados solamente por la interfaz que le fue asignada.

Parámetros de Distribución de Etiquetas³⁹.

La arquitectura de MPLS define varios parámetros de asignación y distribución de etiquetas. El espacio de etiquetas tiene dos opciones:

- Etiqueta por Plataforma: donde las etiquetas deben ser únicas para toda la plataforma (router).

El espacio de etiquetas por plataforma es utilizado con el modo trama (Fig. 2.34), donde una etiqueta es asignada a una red destino y enviada a todos los compañeros LDP. Esta etiqueta puede ser usada en cualquier interfaz de entrada. Las etiquetas por plataforma minimizan el número de sesiones LDP y permite (upstream) túneles LSP para (span) enlaces paralelos, debido a que la misma etiqueta es usada en todos esos enlaces. Sin embargo, el espacio de etiquetas por plataforma es menos seguro que el utilizado en las etiquetas por interfaz, debido a que routers que no sean de confianza pueden usar etiquetas que nunca les han asignado.

Figura 2.34. Asignación de etiquetas por plataforma

- Etiqueta por Interfaz: donde las etiquetas deben ser únicas para una interfaz de entrada específica (Fig. 2.35).

39 RFC 5036: LDP Specification.

La tabla LFIB usada en el modo Celda asigna una etiqueta local ligada a una interfaz de entrada y a una etiqueta de siguiente salto apuntando a la interfaz de salida. La etiqueta asignada a un interfaz de entrada puede ser reusada en otra interfaz, y puede tener un significado diferente (asignada a un destino diferente).

Figura 2.35. Asignación de etiquetas por interfaz

Las dos opciones para generación y distribución de etiquetas son las siguientes⁴⁰:

- Distribución no solicitada de etiquetas en sentido origen-destino: Los dispositivos MPLS que utilizan este modo de distribución no esperan una solicitud de otros routers antes de asignarle una etiqueta a un FEC. Tan pronto como el router aprende la ruta le asigna una etiqueta y la distribuye a todos sus vecinos. Este modo se utiliza en el modo trama, donde todos los routers puede generar etiquetas asincrónicamente y propagarlas a routers adyacentes. No hay un mecanismo de control que permita controlar la propagación de etiquetas en modo ordenado.
- Distribución de etiquetas Downstream-on-demand: En este modo de distribución los dispositivos MPLS no le asignan un FEC a una etiqueta hasta que la solicitud enviada desde un router downstream sea respondida por un router upstream. Se utiliza en el modo Celda, donde cada ATM LSR tiene que solicitar una etiqueta para todos los destinos que se encuentren en la tabla de enrutamiento.

Los modos de distribución de etiquetas unsolicited downstream y downstream-on-demand pueden ser combinadas debido a que las etiquetas son asignadas y propagadas salto por salto. La situación usual es que el modo trama utilice el modo de propagación unsolicited downstream, y el modo Celda use la propagación del tipo downstream-on-demand.

40 MPLS Label Distribution Methodology, Juniper.

Otro aspecto de la distribución de etiquetas se enfoca en cómo se asignan las etiquetas⁴¹:

- **Modo de control independiente:** El modo trama utiliza un modo de control independiente, lo que significa que cada LSR toma una decisión independiente para ligar una etiqueta a un FEC y distribuirla a sus respectivos vecinos, es decir, todos los LSRs pueden comenzar a propagar etiquetas independientemente de las demás. El modo de control independiente se combina usualmente con el modo de propagación de etiquetas unsolicited downstream. Un LSR que esté utilizando el modo de control independiente puede ser usado solamente en LSRs con funcionalidad edge LSR (funcionalidades de capa 3).
- **Modo de control ordenado:** El modo Celda utiliza el modo de control ordenado, lo que significa que un LSR solamente liga una etiqueta a un FEC en particular si ha recibido una etiqueta de siguiente salto de un edge LSR o LSR de siguiente salto. El modo de control ordenado se combina usualmente con el modo de propagación de etiquetas downstream-on-demand. Este modo da como resultado una secuencia ordenada de (downstream) solicitudes hasta que se encuentre un LSR que tenga una etiqueta de salto siguiente o se alcance un LSR configurado con un modo de control independiente.

Retención de Etiquetas.

El último aspecto de la distribución de etiquetas observa las etiquetas que son recibidas pero no usadas, como se lista a continuación^{42,43}:

- **Modo de retención liberal:** Cuando un LSR reemplaza las etiquetas en su tabla LFIB porque ha recibido una actualización de una ruta mejor, puede retener la etiqueta anterior y la nueva. En el modo trama se pueden recibir múltiples etiquetas pero solo usar una de estas. Las etiquetas que quedan en desuso se guardan.
- **Modo de retención conservativo:** Cuando un LSR ha recibido una actualización de una ruta mejor puede descartar esta actualización y seguir con la configuración anterior. En el modo celda solo se guardan las etiquetas que fueron solicitadas previamente. Este método utiliza menos recursos.

•

Descubriendo Vecinos LDP⁴⁴.

LDP es un protocolo estándar usado para el intercambio etiquetas entre routers adyacentes. Cisco es propietario del protocolo TDP que tiene la misma funcionalidad de LDP.

41 IP, Ethernet and MPLS Networks: Resource and Fault Management.

42 MPLS: Next Steps – p.41.

43 Managing IP Networks: Challenges and Opportunities – pp.133-134.

44 RFC 5036: LDP Specification.

LDP periódicamente envía mensajes hello. Si otro router está habilitado para LDP (o TDP), este responderá abriendo una sesión TCP con el mismo número de puerto destino (646 o 711).

Mensajes Hello LDP.

Los mensajes hello son mensajes enviados desde un router a todos los otros routers a los que pueda llegar a través de una interfaz.

Al interior de un mensaje hello se puede encontrar lo siguiente:

- Paquetes UDP con una dirección de destino multicast 224.0.0.2 (“todos los routers en una subnet”).
- Puerto destino 646 o 711 (TDP usa el puerto 711).
- El mensaje hello actual, el cual opcionalmente puede contener una dirección de transporte TLV para indicar al vecino que abra la sesión TCP para la dirección de transporte en vez de la dirección IP de origen que se encuentra en la cabecera IP.

El identificador LDP se utiliza para identificar únicamente el vecino y el espacio de etiqueta. Se pueden establecer múltiples sesiones entre un par de LSRs si utilizan múltiples espacios de etiqueta.

Estableciendo una Sesión LDP.

Las sesiones LDP existen entre LSRs que soportan intercambio de etiquetas. Cuando un LSR usa LDP para comunicar más de un espacio de etiquetas a otro LSR, usa una sesión independiente para cada espacio.

El intercambio de paquetes hello entre dos LSRs permite el establecimiento de la sesión.

El establecimiento de sesión es un proceso de dos pasos:

Establecimiento de la Conexión de Transporte.

El intercambio de paquetes hello da como resultado la creación de una “adyacencia hello” entre dos LSRs. A continuación se presentan dos LSRs (LSR1 y el LSR2) para explicar el establecimiento de la conexión.

1. Si LSR1 no tiene todavía una sesión LDP para el intercambio del espacio de etiquetas entre LSR1 y el LSR2, intenta abrir una conexión TCP para una nueva sesión con LSR2.
2. LSR1 determina la dirección de transporte a ser usada en la conexión LDP TCP.
3. LSR1 determina si su rol será activo o pasivo en el establecimiento de la sesión comparando las direcciones. Si la dirección de LSR1 es mayor a la de LSR2, LSR1 será activo, de lo contrario será pasivo.

4. Si LSR1 está activo, intentará establecer la conexión LDP TCP por uno de los puertos 646 o 711.

Inicialización de la Sesión.

Después de que LSR1 y LSR2 han establecido una conexión de transporte, proceden a negociar los parámetros de sesión intercambiando mensajes de inicialización LDP. Entre algunos de los parámetros negociados se encuentran:

- Versión del protocolo LDP (o TDP según el caso).
- Método de distribución de etiquetas.
- Valores de los temporizadores.

Una negociación exitosa finaliza con el establecimiento de una sesión LDP entre LSR1 y LSR2.

Negociación en una Sesión LDP.

La negociación de una sesión LDP es un proceso de tres pasos:

- Establecer la sesión TCP.
- Intercambiar mensajes de inicialización.
- Intercambiar mensajes iniciales keepalive.
-

Una vez se completen estos 3 pasos, los dos routers comenzarán a intercambiar etiquetas de las redes que ellos tienen en sus tablas de enrutamiento.

Negociando el Espacio de Etiquetas.

Si un par de routers está conectado sobre dos o más enlaces paralelos y usando el modo trama, estos tratarán de establecer sesiones múltiples usando el mismo identificador LDP. Debido a que los routers están utilizando etiquetas por plataforma, esta acción tendrá como resultado que solo permanezca una de las sesiones. Las otras se rompen.

El espacio de etiquetas por plataforma está identificado con el ID de espacio de etiqueta con valor igual a 0 en el campo identificador LDP. Ej: LDP ID=1.0.0.1:0

Si los dos routers usan un identificador LDP diferente (por ejemplo, si un enlace usa el modo trama y el otro Celda), se conservarán ambas sesiones.

Una sesión LDP se establece por interfaz excepto para todas las interfaces en modo trama, donde solamente una sesión LDP entre un par de LSRs es requerida.

Descubriendo Vecinos LDP.

Una sesión LDP se establece desde el router con la dirección IP de loopback más alta. Si no hay interfaces de loopback configuradas en el router, se utiliza la dirección IP más alta de una interfaz que haya sido operacional durante el arranque de LDP.

Después de que se establece la sesión TCP, los routers continuarán enviándose paquetes hello para descubrir a otros vecinos o identificar fallos.

LDP Discovery es un mecanismo que le permite a un LSR descubrir vecinos LDP. Este mecanismo no es necesario cuando los vecinos LSR han sido configurados explícitamente. Hay dos variantes del LDP Discovery:

- Mecanismo Discovery básico: Utilizado para descubrir vecinos LSR que están conectados directamente a nivel de enlace.
- Mecanismo Discovery extendido: Usado para localizar LSRs que no están conectado directamente a nivel de enlace.

Mecanismo Discovery Básico.

Para emplear este mecanismo sobre una interfaz, un LSR envía periódicamente paquetes hello LDP de enlace. Estos paquetes son enviados como paquetes UDP direccionados a la dirección multicast 224.0.0.2 (“todos los routers en una subnet”).

Un paquete hello LDP de enlace enviado por un LSR porta el identificador LDP para el espacio de direcciones que el LSR intenta usar para la interfaz y posiblemente información adicional.

El receptor de un paquete hello de enlace sobre una interfaz identifica una “adyacencia hello” y por consiguiente un vecino LDP potencialmente alcanzable a nivel de enlace sobre la interfaz, así como el espacio de etiquetas que el emisor intenta usar para la interfaz.

Mecanismo Discovery Extendido: Vecinos No Adyacentes.

Las sesiones LDP entre LSRs que no están conectados directamente están soportados por LDP extended Discovery.

Para participar del mecanismo Discovery extendido, un LSR envía periódicamente paquetes hello LDP a una dirección específica (Target Hello). Estos paquetes se envían como paquetes UDP direccionados al puerto 646 o 711.

Un paquete LDP hello enviado por un LSR porta el identificador LDP para el espacio de etiquetas que el LSR intenta usar y posiblemente información adicional.

El método extendido difiere del básico en los siguientes aspectos:

- Un Target Hello se envía a una dirección específica mientras que en el Discovery básico lo hace a una dirección multicast.
- A diferencia del método extendido, basic Discovery es simétrico.
- Un LSR inicia el mecanismo Discovery extendido con otro LSR específico (Targeted LSR) y el Target LSR decide si responde o ignora el Target Hello. Un target LSR que elige responder, debe enviar target hellos al LSR que inició la conexión.

El receptor de un paquete LDP target hello identifica una “hello adjacency” con la posibilidad de tener un vecino potencialmente alcanzable a nivel de red y del espacio de direcciones que intenta usar.

El resto de la negociación de la sesión es la misma que la usada para routers adyacentes.

MÓDULO 3

Tecnología MPLS para Redes Virtuales Privadas (VPNs).

Introducción a las Redes Virtuales Privadas (VPNs).

Una red virtual privada (VPN) es un término genérico que abarca el uso de redes públicas o privadas para crear grupos de usuarios que están separados de otros usuarios de la red y que se puedan comunicar entre ellos como si estuvieran todos juntos en una red privada⁴⁵ a través de una troncal.

Si todos los sitios en la VPN pertenecen a la misma empresa, la VPN puede ser vista como una intranet corporativa. Si varios sitios en la VPN pertenecen a diferentes empresas, la VPN puede ser vista como una extranet⁴⁶.

Conectividad de Red Tradicional Basada en Router.

La conectividad de red tradicional basada en Router (Fig. 3.1) fue implementada con enlaces dedicados punto a punto para conectar los sitios de los clientes.

45 RFC 4026: Provider Provisioned Virtual Private Network (VPN) Terminology.

46 RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs).

Figura 3.1. Esquema de conexión tradicional

Implementar el enrutamiento de esta manera tenía un costo relativamente alto por las siguientes razones:

- Los enlaces dedicados punto a punto tenían tiempos de inactividad en los que la capacidad del enlace se perdía porque no siempre existía flujo de datos (Fig. 3.2) y porque no había forma alguna de compartir estos recursos cuando estaban en desuso, dando como resultado un alto costo para el usuario final.

Figura 3.2. Inconvenientes del esquema tradicional

- Cada enlace requería un puerto dedicado en el router, dando como resultado equipos muy costosos.

Si hay múltiples dispositivos en una ubicación para ser conectados a uno o más dispositivos del destino, una sola línea puede ser compartida usando un equipo al final de la línea llamado multiplexor (Fig. 3.3). La multiplexación estadística permite que varios equipos se conecten aunque superen la capacidad de la línea ya que se lleva un registro de los tiempos perdidos y por consiguiente se puede enviar tráfico de varios equipos. Ya que estos equipos en conjunto superan la capacidad del enlace, si todos envían tráfico simultáneamente se pueden presentar retardos en la entrega de paquetes⁴⁷.

Figura 3.3. Enlace compartido a través de un multiplexor

Ventajas de las VPNs.

Las VPNs fueron introducidas tempranamente en la historia de las comunicaciones con tecnologías tales como X.25 y Frame Relay, los cuales usan circuitos virtuales^{48,49} para establecer conexión end-to-end sobre una infraestructura compartida de un proveedor de servicios (Fig. 3.4). Las siguientes tecnologías aunque se consideran obsoletas, todavía comparten los beneficios básicos de las modernas VPNs:

- Los enlaces dedicados para la conectividad de red tradicional basada en Router han sido reemplazados con una infraestructura común que emula enlaces punto a punto para el cliente, dando como resultado un compartimiento estadístico de la infraestructura del proveedor de servicios (SP).
- El compartimiento estadístico de la infraestructura habilita al SP para que ofrezca conectividad a un bajo precio, lo que finalmente se traduce en un bajo costo operacional para el usuario final, puesto que no es uno solo quien debe pagar un enlace sino que el costo se distribuye entre varios.

47 Handbook of Information Security, Key Concepts, Infrastructure, Standards – p.445.

48 RFC 1356: Multiprotocol Interconnect on X.25 and ISDN in the Packet Mode.

49 RFC 2427: Multiprotocol Interconnect over Frame Relay.

Figura 3.4. Simulación de redes punto a punto a través de un SP

Elementos de una VPN.

Hay muchos modelos conceptuales y terminología que describe varias implementaciones y tecnologías VPN. Sin embargo, esta terminología es lo suficientemente genérica para cubrir casi cualquier implementación o tecnología VPN.

La mayor parte de los elementos de una solución global VPN (Fig. 3.5) son los siguientes:

- Red del proveedor (P-network): Es la infraestructura común que el SP utiliza para ofrecer servicios VPN a los clientes.
- Red del cliente (C-network): Es la parte de la red global del cliente que está bajo el control exclusivo del cliente.
- Sitios de cliente (Customersites): Partes contiguas a la C-network.

Figura 3.5. Elementos de una VPN (1)

Una C-network típica implementada con cualquier tecnología VPN contendría sedes de conectividad bajo control del cliente (customer sites) conectados entre sí a través de la infraestructura del proveedor (P-network).

Terminología VPN^{50,51}.

A continuación se presentan los dispositivos que permiten una implementación VPN (Fig. 3.6), los cuales son nombrados basados en su posición en la red:

- CE-R (Customer Edge Router): Es el router en la red del cliente que conecta la C-network o los sitios del cliente SP. También se conocen como dispositivos CE.
- PE (Provider Edge Router): Un PE es el nombre del dispositivo o conjunto de dispositivos ubicados en la frontera de la red del proveedor que se conectan a los CEs. También soportan el manejo de etiquetas a través de un par de routers PE conectados a través de un túnel LSP.
- En las implementaciones tradicionales switched WAN, estos dispositivos debían ser edge switches Frame Relay o X.25.
- Provider Router (P): P se define como un router al interior de la red del proveedor que no tiene interfaces directamente conectadas hacia un cliente. Por lo tanto, un router P no tiene necesidad de conocer sobre los procesos VPN. Estos dispositivos proveen solamente transporte de datos a través de la troncal del SP. Estos dispositivos deben soportar LSP y LDP ya que hacen parte del túnel LSP entre los routers PE, pero no necesariamente deben tener capacidad de ejecutar VPN.

En las implementaciones tradicionales switched WAN, estos dispositivos debían ser switches centrales similares a los routers P.

Figura 3.6. Elementos de una VPN (2)

50 Juniper Networks Field Guide and Reference – p.615.

51 RFC 4026: Provider Provisioned Virtual Private Network (VPN) Terminology.

Switched WANs.

Un enlace punto a punto es una conexión física entre dos estaciones separadas o LANs. Una organización puede crear un enlace punto a punto simplemente instalando su propio enlace físico (cable, fibra, etc.) entre sus sitios. Este método se utiliza normalmente para conectar edificios dentro un campus o similares, sin embargo, para conectarse con ubicaciones que estén alejadas por distancias muy grandes sería extremadamente costoso implementar enlaces físicos dedicados.

Para solucionar este inconveniente se crearon las WAN, que no es más que una red que tiene gran cobertura (ciudad o país) y provee gran cantidad de puntos de acceso a los usuarios. Las switched WAN son WANs que en su interior poseen una malla de redes punto a punto que conectan switches.

Circuitos Virtuales Usados en Switched WANs.

La conmutación de paquetes es una tecnología WAN en la que los usuarios comparten los mismos recursos de transporte de la infraestructura. De este modo se permite un uso más eficiente de los recursos a un menor costo. En una configuración de conmutación de paquetes las redes tienen conexión a la red del proveedor, y muchos clientes comparten la misma red del SP. Cuando se presenta este caso, el SP puede crear circuitos virtuales (VC), como se ve en la figura 3.7, entre los sitios de un cliente por los cuales los paquetes de datos se entregarán desde su red hasta la de sus clientes.

Figura 3.7. Conmutación de paquetes a través de Circuitos Virtuales (VC)

Algunos ejemplos de redes de conmutación de paquetes incluyen, Asynchronous Transfer Mode (ATM), FrameRelay, X.25⁵² y MetroEthernet.

52 Introduction to WAN Technologies, Cisco.

Los circuitos virtuales están clasificados en dos categorías:

- **Circuitos virtuales conmutados (SVC):** Este tipo de circuitos se generan por demanda de un CE, y se utilizan cuando la transmisión de datos es esporádica. Ejemplo, una llamada telefónica.
- **Circuitos Virtuales Permanentes (PVC):** Estos circuitos se establecen manualmente y es dedicado entre dos puntos por lo tanto no deben realizar establecimiento y liberación de conexiones constantemente así como lo hacen los SVCs.

El objetivo de estos circuitos es emular una conexión punto a punto.

Red MetroEthernet.

Las redes MetroEthernet están basadas en el estándar 802.3 de la IEEE. El servicio ofrecido por estas redes es la interconexión de LANs que se encuentran ubicadas dentro de una misma ciudad pero ubicadas en sitios diferentes.

La ventaja de implementar este tipo de redes es que se basa en una tecnología que ya es conocida y ha sido implementada en empresas y residencias.

MetroEthernet ofrece servicios de conectividad MAN/WAN de capa 2 utilizando UNIs Ethernet o dicho de otra forma son puntos de frontera entre la red del cliente y el operador (Fig. 3.8).

Figura 3.8. Red MetroEthernet

Estas redes MetroEthernet también se conocen como red multiservicio y soportan aplicaciones que requieren el envío de tráfico en tiempo real como telefonía IP y video IP.

De acuerdo al estándar 802.3 el medio de transporte puede basarse en fibra óptica o cobre (802.3ah) (Fig. 3.9). Estas redes pueden ser utilizadas como enlaces punto a punto, sin embargo, esta tecnología permite agregar múltiples pares de cobre, lo cual habilita la transmisión de datos a diferentes velocidades y de manera simultánea. Adicionalmente, contar con una infraestructura basada en cobre presenta beneficios en cuanto a la disponibilidad de la red ya que estos enlaces se construyen por múltiples pares de líneas de cobre y resulta prácticamente imposible que se presente una rotura interna en todos los enlaces al mismo

tiempo. En caso de falla parcial el ancho de banda se reduce proporcionalmente. Como complemento, la fibra óptica se puede implementar como troncal para transportar todo el tráfico pesado de un lugar a otro.

Figura 3.9. Conectividad MetroEthernet

Red MetroEthernet: Proveedor de Servicios.

Al interior de un SP, la red MetroEthernet está compuesta por Switches, y al igual que con las redes ATM, estas crean conexiones virtuales EVC (Ethernet Virtual Connection) similar a los circuitos virtuales VC (Fig. 3.10). Con la implementación de estos túneles virtuales se consiguen dos cosas:

- Asegurar la privacidad y seguridad de los usuarios que comparten el canal virtual de aquellos que no pertenecen a él.
- Establecer conexión entre dos o más UNIs mediante el uso de tramas Ethernet.

Figura 3.10. Túneles virtuales MetroEthernet

Estos circuitos EVC están categorizados en dos tipos:

E-LINE (punto a punto)

E-LAN (Multipunto)

Uno de los servicios soportados por las redes MetroEthernet el VLAN tag supporting, lo cual permite adaptarse a nuevas tecnologías y topologías de diseño.

Introducción a las Redes VPN Overlay y Peer-to-Peer.

Implementación de Tecnologías VPN.

Las implementaciones tradicionales de VPN estaban basadas en el modelo overlay (una red que se ejecuta independientemente sobre otra, aunque soportada sobre su infraestructura) en la cual un ISP vendía circuitos virtuales entre sitios del cliente como un reemplazo para enlaces punto a punto dedicados tradicionales.

El modelo overlay tenía un número de inconvenientes, que serán vistos más adelante. Para superar estos problemas se introdujo un nuevo modelo llamado VPN peer to peer. En este modelo, el ISP participa activamente en el enrutamiento del cliente.

Técnicas de Implementación Overlay VPN.

En capa 1

En la implementación overlay VPN en la capa 1, el SP ofrece circuitos de capa 1 (bit pipes) implementados con tecnologías tales como ISDN, servicio digital cero (DS0), E1, T1,

Synchronous Digital Hierarchy (SDH), o SONET con el que se establece una conectividad de capa física entre los sitios del cliente. El cliente es responsable por la encapsulación de capa 2 entre los dispositivos del cliente y el transporte de datos IP a través de la infraestructura.

En capa 2

Una implementación de VPN capa 2, es modelo tradicional switched WAN. Este modelo se implementaba con tecnologías como X.25, FrameRelay, ATM, y Switched Multimegabit Data Service (SMDS). El SP es responsable DE transportar Tramas de capa 2 entre sitios del cliente, y el cliente es responsable de las capas superiores.

IP Tunneling⁵³.

El IP tunneling se utiliza para transportar tráfico de un protocolo sobre una red que no soporta ese protocolo directamente. Por ejemplo, NetBIOS o IPX pueden ser encapsulados en un paquete IP para viajar por una red de enlace TCP/IP WAN. Dos conocidas tecnologías tipo tunneling son seguridad IP (IPSec) y encapsulación genérica de enrutamiento (GRE). GRE es sencillo y rápido de implementar y soporta múltiples protocolos de enrutamiento pero no provee seguridad y por lo tanto no es factible para utilizarlo en internet.

En el caso de IPSec, se utilizan los protocolos AH y ESP para garantizar la confidencialidad, autenticación e integridad de la comunicación. Adicionalmente, IPSec puede proteger los protocolos de capas superiores (Modo transporte) o el datagrama IP completo (Modo túnel), siendo este último de mayor interés para el contenido del documento.

En el modo túnel, el paquete IP original se encapsula en otro paquete IP, para proveer protección al paquete encapsulado.

Al encapsular un paquete IP dentro de otro (cubierta), la cabecera IP del paquete original se vuelve parte de los datos de usuario y la cabecera que queda visible es la de la cubierta. IPSec provee autenticación de capa de red y encriptación para hacer que la transferencia de datos sobre internet sea segura. IPSec soporta solamente IP.

Paquete normal.

Paquete IPSec.

53 TCP/IP Tutorial and Technical Overview – p.812.

El tunneling requiere un procesamiento intermedio mientras se enruta. El destino final en la cabecera de la cubierta que es usualmente un Firewall IPSec o router, desempaqueta el túnel, y con la cabecera original envía el paquete a su destino real (Fig. 3.11). El costo de procesamiento se compensa con la seguridad.

Figura 3.11. Funcionamiento IPSec

Una ventaja notable del IP tunneling es la posibilidad de intercambiar paquetes con direcciones IP privadas entre dos intranets sobre una red pública de internet, que requiere direcciones globales únicas. Esto sucede porque la cabecera original no es procesada por los routers de internet (esta solo es entendida por el Gateway origen y destino).

Con el éxito de IP y las tecnologías asociadas, algunos SPs comenzaron a implementar troncales netamente IP para ofrecer servicios VPN basados en IP. En otros casos, los clientes querían tomar ventaja del bajo costo y disponibilidad universal del internet para construir redes privadas de bajo costo.

VPN Overlay: Transporte en Capa 2.

Otra técnica de tunneling fue implementada primero en redes dial-up (servicio de internet sobre una línea telefónica analógica y un MODEM), que permitía establecer una conexión entre el gateway de una empresa y un usuario empleando una sesión PPP.

Para hacer transparente el transporte del proveedor del servicio a los usuarios, las tramas PPP se intercambian entre sitios de un cliente (usualmente un usuario dial-up y un sitio central). Para establecer la conexión se requería tanto la negociación del protocolo a utilizar como autenticación del cliente.

En general del pool del protocolo PPP, las siguientes son las implementaciones más utilizadas en PPP forwarding:

- Protocolo de envío capa 2 (L2F Protocol)⁵⁴: Este protocolo (desarrollado por Cisco Systems) permite realizar el tunneling de la capa de enlace de o para protocolos de niveles superiores capa 3 hacia arriba. Usando estos túneles, es posible establecer túneles desde usuarios remotos hasta los sitios centrales.
- Protocolo de tunneling Punto a punto (PPTP)⁵⁵: Este protocolo (desarrollado por Microsoft) permite intercambiar datos desde un cliente hasta el servidor de forma segura usando una VPN.
- Protocolo de tunneling capa 2 (L2TP Protocol)⁵⁶: Este protocolo (desarrollado por Cisco) se utiliza para dirigirlos servicios telefónicos sobre un túnel en internet hasta un determinado punto final. Este protocolo define el establecimiento de túneles basado en L2F.
- The PPP Protocolo de Control para Cifrado (ECP)⁵⁷: Este protocolo provee un método estándar para transportar datagramas multiprotocolo sobre enlaces punto a punto.

Enrutamiento Capa 3.

Desde la perspectiva de capa 3, una P-network es invisible a los routers del cliente, (Fig. 3.12) los cuales están conectados con enlaces punto a punto simulados. El protocolo de enrutamiento corre directamente entre los routers del cliente que establecen adyacencias e intercambian información de enrutamiento.

El SP no tiene conocimiento sobre el enrutamiento y rutas del cliente, la responsabilidad de este sólo consiste en transportar datos punto a punto entre los sitios de un cliente.

Figura 3.12. Perspectiva de una P-network desde los routers del cliente

54 RFC 2341: Cisco Layer Two Forwarding (Protocol) "L2F".
 55 RFC 2637: Point-to-Point Tunneling Protocol (PPTP).
 56 RFC 2661: Layer Two Tunneling Protocol "L2TP".
 57 RFC 1968: The PPP Encryption Control Protocol (ECP).

Técnicas de Implementación Para VPNs Peer to Peer.

El modelo VPN overlay tiene un número de inconvenientes, el más significativo es la necesidad para los clientes de establecer enlaces punto a punto o VCs entre sitios. La fórmula para calcular cuántos enlaces punto a punto o VCs se necesitan en el peor de los casos es $(n - 1)/2$, donde n es el número de sitios para ser conectados. Y dado que este número de enlaces podía crecer a medida que el valor de n fuese más grande, se introdujo el concepto de VPN Peer to peer para proveer al cliente un transporte de datos óptimo a través de la troncal del SP. En esta modalidad el SP participa activamente en el enrutamiento del cliente (no solo provee enlaces punto a punto), aceptando las rutas, transportándolas a través de la troncal del SP, y propagándolas a otros sitios del cliente (Fig. 3.13).

Figura 3.13. Participación del SP en el transporte y enrutamiento de datos

VPNs Peer to Peer: Filtro de Paquetes.

La primera solución VPN peer to peer apareció con el despliegue generalizado de IP en las redes de los proveedores de servicio. Esta arquitectura que estaba diseñada hacia troncales públicas (internet), fue transformada para utilizarse como solución en la cual los clientes estarían totalmente aislados pero con la capacidad de intercambiar datos corporativos de forma segura.

La implementación VPN peer to peer más común permitió que un router PE fuese compartido entre dos o más clientes. Los filtros de paquetes fueron utilizados sobre los routers PE compartidos para aislar los clientes (Fig. 3.14). En esta implementación, era común para el SP asignar una porción de su espacio de direcciones a cada cliente y administrar los filtros de paquetes en los routers PE para garantizar que los sitios de un cliente siempre fueran alcanzables, pero que los diferentes clientes estuviesen separados.

Figura 3.14. Filtro de direccionamiento aplicado sobre un router PE común a los clientes

VPNs Peer to Peer: Distribución Controlada de Rutas.

Algunos SPs, como se ve en la figura 3.15, han implementado soluciones más eficientes basadas en la distribución controlada de rutas y no quedarse únicamente en el uso de filtros. Este enfoque requiere un router PE dedicado por cliente en cada punto de presencia (POP). En el núcleo del SP, los P routers contienen todas las rutas de los clientes, y los routers PE dedicados contienen solamente las rutas de un único cliente. El aislamiento de clientes se alcanza únicamente a través de la falta de información de enrutamiento en el router PE.

Figura 3.15. Distribución controlada de rutas implementando POPs

Beneficios de Implementaciones VPN.

Cada modelo VPN tiene un número de beneficios. Por ejemplo, overlay VPNs tienen las siguientes ventajas:

- Son fáciles de implementar desde la perspectiva del cliente y el proveedor.
- El ISP no participa en el enrutamiento del cliente, haciendo el punto de demarcación entre el ISP y el cliente más fácil de manejar.
-

Por otra parte, las VPNs peer to peer proveen las siguientes ventajas:

- Enrutamiento óptimo entre sitios del cliente sin ningún diseño especial o esfuerzo de configuración.
- Fácil aprovisionamiento de VPNs adicionales o sitios de clientes, debido a que el ISP provee solo los sitios más no los enlaces entre estos sitios de clientes individuales.

Inconvenientes de las Implementaciones VPN.

Así como cada modelo tiene sus ventajas, estos también presentan una serie de inconvenientes:

- Overlay VPNs requieren una malla completa de VCs entre sitios de un cliente para proveer enrutamiento óptimo intra-sitio.
- Todos los VCs entre sitios de un cliente tienen que ser provisionados manualmente, y el ancho de banda debe ser provisionado con un enfoque sitio a sitio (lo cual no siempre es fácil de lograr).
- La implementación VPN overlay basada en IP (con IPSec o GRE) incurre en encapsulaciones pesadas sobrepasando el rango de 20-80 bytes por datagrama transportado.

Los mayores inconvenientes de las VPNs peer to peer se derivan de la participación del SP en el enrutamiento del cliente, como se menciona a continuación:

- El SP se vuelve responsable por el correcto enrutamiento del cliente y por una rápida convergencia de la C-network después de un fallo de enlace.
- Los routers PE tienen que llevar todas las rutas de los clientes que el SP desconocía en el modelo VPN overlay.
- El SP necesita tener conocimiento detallado del enrutamiento IP, el cual no está disponible fácilmente en los grupos de trabajo de los SPs tradicionales.

Inconvenientes de la Implementación VPN Peer to Peer Tradicional.

Todas las implementaciones VPN antes de MPLS o peer to peer tenían un inconveniente en común.

Los clientes tenían que compartir el mismo espacio global de direcciones, ya sea utilizando sus propias direcciones IP públicas o dependiendo del espacio de direcciones asignadas por el proveedor. En ambos casos, conectar un nuevo cliente a un servicio VPN peer to peer usualmente requiere una re-numeración IP al interior de la C-network, esto último es una tarea que los clientes están poco dispuestos a realizar.

Las VPNs peer to peer basadas en filtrado de paquetes también incurrierían en un alto costo operacional asociado con el mantenimiento y degradación del rendimiento de los filtros de paquetes debido al uso pesado, ya que cada paquete debe pasar por él.

Las VPNs peer to peer implementadas con routers PE por cliente, son fáciles de mantener y pueden proveer un rendimiento óptimo de enrutamiento, pero suelen ser más costosos porque cada cliente requiere un router dedicado en cada POP. Así que este enfoque se utiliza si el proveedor tiene solo un pequeño número de clientes.

Categorizando VPNs⁵⁸.

Muchas empresas tienen una o más oficinas centrales con oficinas separadas. En algunos casos, estas oficinas separadas necesitan acceder a recursos que se encuentran en otras instalaciones, como pueden solo necesitar los recursos que se encuentran en la oficina central.

La categoría VPN más antigua está basada en la topología de enlaces punto a punto en una implementación VPN overlay. Algunas categorías son las siguientes.

- **Hub y spoke (hub-and-spoke):** la topología hub-and-spoke (Fig. 3.16) es la reducción definitiva de la topología de malla parcial. Desde una perspectiva administrativa, las redes hub-and-spoke son más sencillas de administrar porque todos los sitios (spokes) se conectan a un solo sitio o sitios centrales (hub). Por consiguiente son fáciles de escalar porque hay un mínimo de enlaces que se deban mantener. Otra ventaja es que es más fácil de administrar en cuanto a la seguridad al igual que lo hacen los SPs para cada red conectada, ya que la seguridad y los servicios pueden ser administrados de forma centralizada en un hub y no en cada spoke.

Para prevenir puntos únicos de fallo, la topología hub-and-spoke algunas veces es extendida a una topología redundante hub-and-spoke.

58 Juniper SRX Series – pp.545-547.

Figura 3.16. Topología Hub y Spoke

- **Malla completa (Full mesh):** La topología de malla completa (Fig. 3.17) provee un circuito virtual dedicado entre cualquier par de CE routers en la red.

Aunque una topología hub-and-spoke podría utilizarse comúnmente debido a su simplicidad, hay algunos factores que pueden hacer que este modelo no sea una opción factible para la red. Primero, todo el tráfico debe ir desde un spoke hasta el hub y luego del hub al spoke cuando se envíe tráfico entre spokes. Esto puede dar como resultado un rendimiento sub-óptimo y causar problemas de latencia en especial cuando el hub esté recibiendo mucho tráfico. Este inconveniente en la latencia es un problema común que enfrentan inclusive hoy en día las redes modernas que ejecutan aplicaciones en tiempo real como VoIP y video conferencia que están expuestas a inconvenientes de latencia y anchos de banda y que generalmente trabajarían mejor si estuviesen conectadas directamente entre ellas. Por consiguiente, la topología full mesh (malla completa) se implementa mayormente para conectar oficinas remotas dentro de una organización (no es muy común para organizaciones separadas) porque le permite a un sitio comunicarse directamente con otros. La desventaja de esta topología es la complejidad de su implementación, la incapacidad de escalar, y la sobrecarga administrativa asociada con el mantenimiento de todas las VPNs, más el costo adicional que esto representa para los clientes.

Figura 3.17. Topología VPN full mesh

- **Malla parcial (Partialmesh):** La topología de malla parcial (Fig. 3.18) es un híbrido entre hub-and-spoke y full mesh que reduce el número de VCs e intenta combinar las ventajas de cada modelo. En las redes VPN con malla parcial, algunos spoke tienen conexión directa con otros para mejorar el ancho de banda y latencia proporcionando un transporte óptimo entre la mayoría de sitios. La ventaja que sobresale en este modelo es que las oficinas remotas todavía se conectan al hub pero también se conectan a otros. Esto mejora el rendimiento de aplicaciones en tiempo real.

Figura 3.18. Topología VPN malla parcial

Las grandes redes usualmente despliegan una combinación de capas de estas tecnologías. Aquí hay algunos ejemplos:

- Una malla parcial en la red central.
- Una topología redundante hub-and-spoke para grandes spokes conectados a routers distribuidos (hubs).
- Una topología simple hub-and-spoke para locaciones remotas no críticas (home offices).

En resumen se tienen las siguientes topologías:

Topología Hub-and-spoke Overlay VPN.

La topología hub-and-spoke es la topología VPN overlay más simple, todos los sitios remotos están enlazados con un único VC a un router CE central. El enrutamiento también es extremadamente fácil, se puede realizar enrutamiento estático o emplear un protocolo vector distancia.

Topología Redundante hub-and-spoke.

Una topología redundante de hub-and-spoke introduce redundancia en los sitios centrales (topologías más complejas podrían introducir redundancia con routers en los spoke).

Cada sitio remoto está enlazado con dos routers centrales a través de dos VCs. Los dos VCs pueden ser usados para balancear la carga o utilizar una configuración principal/respaldo.

Topología Malla Parcial Overlay.

Las topologías en malla parcial se usan en ambientes donde factores de costo o complejidad evitan que se implemente una malla completa entre sitios de clientes. Los VCs en una topología de malla parcial pueden ser establecidos basados en los siguientes criterios:

- Patrones de tráfico entre sitios.
- Disponibilidad de la infraestructura física.
- Consideraciones de costo.

Categorías de negocio VPN.

A continuación se presenta una lista de algunas de las categorías VPN más populares basadas en las necesidades del negocio que ellas satisfacen⁵⁹:

59 Lección 30: Definición, tipos y configuraciones de VPN. Universidad nacional y a distancia.

- **VPN Intranet:** Las intranet se utilizan en organizaciones que disponen de redes locales ubicadas en diferentes sedes, y que a su vez éstas poseen una propia red privada o intranet de acceso restringido al personal. Si por razones administrativas se desea que desde cualquier sede se pueda acceder a las demás intranets, se puede emplear una VPN para interconectarlas y formar una VPN intranet única (Fig. 3.19).

Figura 3.19. VPN intranet

- **VPN Extranet:** En ocasiones cuando una empresa está interesada en compartir los recursos de la intranet con entidades externas como proveedores o clientes, se emplea un VC directo (Fig. 3.20).

Estas redes que permiten acceso a otros participantes mediante VCs se llaman VPNs extranet.

Figura 3.20. VPN Extranet

- **Access VPN:** Access VPNs son redes virtuales privadas dial-up (VPDNs) que proveen acceso dial-up a una red cliente.

Implementación VPN Peer to Peer.

En una implementación VPN Peer to peer (Fig. 3.21) todos los sitios de un cliente están conectados a la P-network. El costo de la implementación de este modelo es bajo ya que usualmente cada organización paga los costos de su conectividad para participar en la extranet y conseguir conectividad total a los otros sitios.

Figura 3.21. VPN peer to peer

Categoría de conectividad VPN.

Las VPNs discutidas hasta ahora han sido sencillas en términos de conectividad, como se describe aquí:

- En la mayoría de los casos, se requiere conectividad total entre sitios. En una implementación overlay ya sea intranet o extranet, este requerimiento usualmente significa que un sitio común actúe como un sitio de tránsito.
- En una implementación overlay de una extranet VPN, la comunidad está limitada a los sitios que tienen VC directos establecidos entre ellos.

A continuación se describe un número de topologías VPN avanzadas con requerimientos de conectividad más complejos.

- Superposición de VPNs, en el que un sitio participa en más de una VPN.
- Central de Servicios VPN, en el que los sitios están divididos en dos clases: sitios servidores, que puede comunicarse con todos los otros sitios, y sitios clientes, que puede comunicarse solo con los servidores y no con otros clientes.
- Administrador de redes VPN, el cual es utilizado para gestionar los dispositivos CE en escenarios donde el ISP es dueño de los dispositivos y él mismo los administra.

Central de Servicios de extranet.

LA central de servicios de una extranet (Fig. 3.22) consiste en compartir una misma infraestructura para clientes y servidores, por lo tanto comparten los mismos servicios, pero los clientes no pueden utilizar esta misma infraestructura para llegar a otros clientes.

Figura 3.22. Central de servicios de extranet

Introducción a la Arquitectura VPN de MPLS.

Arquitectura VPN MPLS.

La arquitectura VPN MPLS ofrece a los proveedores de servicios una arquitectura VPN peer to peer que combine las mejores características de overlay VPNs (soporte para espacio de direcciones de clientes superpuestas) con las mejores características de VPN peer to peer. A continuación se describen estas características^{60,61}:

- Los routers PE participan en el enrutamiento del cliente, garantizando enrutamiento óptimo entre sitios del cliente.
- Los routers PE llevan un conjunto separado de rutas para cada cliente, dando como resultado un aislamiento perfecto entre clientes.
- Los clientes pueden usar direcciones traslapadas.

60 Juniper Networks Field Guide and Reference – p-615.

61 RFC 4026: Provider Provisioned Virtual Private Network (VPN) Terminology.

Arquitectura VPN MPLS: Terminología.

La terminología de VPN MPLS divide toda la red en una parte controlada por el cliente (C-network) y otra parte controlada por el proveedor (P-network). Las porciones contiguas de la C-network son llamadas sites y están enlazadas con la P-network a través de routers CE (Fig. 3.23). Los CE routers están conectados a los PE routers, los cuales sirven como dispositivos de frontera de las P-network. Los dispositivos centrales en la P-network (routers P), proveen transporte de tránsito a través de la troncal del proveedor y no llevan rutas del cliente.

Figura 3.23. Elementos de una red VPN MPLS

Arquitectura de un Router PE en una VPN MPLS.

La arquitectura de un router PE en una red VPN MPLS (Fig. 3.24) es muy similar a la arquitectura de un POP en el router PE dedicado del modelo peer to peer. La única diferencia es que toda la arquitectura está concentrada en un solo dispositivo físico. Cada cliente tiene asignada una tabla virtual de enrutamiento que corresponde al router PE dedicado en el modelo tradicional peer to peer. El enrutamiento a través de la troncal del proveedor esta realizado por otro proceso de enrutamiento que usa una tabla de enrutamiento IP global correspondiente al router P intra POP en el modelo tradicional peer to peer.

Figura 3.24. Arquitectura de un router PE

Métodos de Propagación a través de la P-network.

Aunque las tablas virtuales de enrutamiento proveen aislamiento entre clientes, los datos de estas tablas todavía necesitan ser intercambiados entre routers PE para habilitar la transferencia de datos entre sitios ligados a diferentes routers PE. Por lo tanto, un protocolo de enrutamiento es necesario para que transporte todas las rutas del cliente a través de la P-network, al mismo tiempo que mantiene la independencia del espacio de direcciones para clientes individuales.

Se debe recordar que la red interna del SP debe estar lo más aislada posible del enrutamiento de rutas que no sean del interior de la red para no saturarla.

Una solución evidente que se ha implementado en varios vendedores de VPN, es correr un IGP por cada cliente (Fig. 3.25). Hay dos implementaciones comunes. Ambas requieren un protocolo de enrutamiento por cliente que se ejecute entre routers PE.

En una implementación, los routers P participan en el enrutamiento del cliente y pasan la información de enrutamiento del cliente entre routers PE.

Figura 3.25. IGP exclusivo por cliente

En la otra implementación, los routers PE están conectados a través de túneles punto a punto por ejemplo IPSec (Fig. 3.26), escondiendo de esta manera la información de enrutamiento a los routers P.

Figura 3.26. Comunicación directa entre routers PE

Esta solución, aunque es muy simple para implementar (y algunas veces usadas por algunos clientes), no es apropiada en el entorno de un SP debido a que simplemente no es escalable por las siguientes razones:

- Los routers PE tienen que correr un gran número de protocolos de enrutamiento.
- Los routers P deben llevar todas las rutas de los clientes.

Propagación de la Información de Enrutamiento a través de la P-network.

Dado que la solución mencionada anteriormente no es óptima, una opción más factible para afrontar el problema de propagación de rutas es desplegar un único protocolo de enrutamiento que pueda intercambiar todas las rutas de los clientes a través de la P-network. Aunque este enfoque es mejor que el anterior, los routers P todavía están involucrados con el enrutamiento del cliente (Fig. 3.27), por lo tanto, esta propuesta conserva algunos de los mismos problemas de escalabilidad de la opción mencionada anteriormente.

Figura 3.27. Intercambio de rutas de clientes usando los routers P

La mejor alternativa para realizar la propagación de rutas de los clientes al interior del SP es ejecutar un único protocolo de enrutamiento entre los routers PE (Fig. 3.28) que intercambiarán todas las rutas del cliente sin involucrar a los routers P estableciendo enlaces entre los routers de frontera. Esta solución es escalable. Algunos de los beneficios de esta solución son los siguientes:

- El número de protocolos de enrutamiento corriendo entre routers PE no aumenta con un crecimiento de clientes.
- Los routers P no llevan las rutas de los clientes.

Figura 3.28. Enrutamiento basado en un único protocolo de enrutamiento entre routers PE

La siguiente decisión de diseño a ser tomada en cuenta es la elección de un protocolo de enrutamiento entre los routers PE. Dado que el número total de routers de clientes se espera sea grande, el único protocolo con la escalabilidad requerida es BGP. De hecho, BGP es usado en las arquitecturas VPN MPLS para transportar rutas de los clientes directamente entre routers PE.

La arquitectura VPN MPLS difiere considerablemente de la solución VPN peer to peer tradicional (el soporte de superposición del espacio de direcciones del cliente).

Con el despliegue de un único protocolo (BGP) intercambiando todas las rutas de los clientes entre routers PE surge un nuevo inconveniente, y es como hará BGP para propagar un gran número de prefijos idénticos que pertenecen a diferentes clientes entre routers PE.

La única solución eficiente para enviar rutas de clientes a través de un SP es expandiendo los prefijos IP de los clientes con un único prefijo que los haga únicos.

Diferenciadores de Rutas.

Un diferenciador de ruta RD (Route Distinguisher) es un valor de 8 bytes, que junto con una dirección de 4 bytes IPv4, identifican una familia de direcciones VPN-IPv4. Si dos VPNs utilizan los mismos prefijos IPv4, el router PE traduce estos dos valores (RD+IPv4) en un prefijo único llamado VPN-IPv4 de 12 bytes. Con esto se garantiza que si la misma dirección o direcciones se utilizan en dos o más VPNs diferentes, es posible instalar dos rutas completamente diferentes hacia esas dos direcciones.⁶²

El RD es usado únicamente para transformar direcciones de clientes de 4 bytes de IPv4 en direcciones únicas de 12 bytes VPNv4.

Las direcciones VPNv4 son intercambi

adas solo entre routers PE, estas nunca son usadas entre routers CE (Fig. 3.29). Por lo tanto, cuando se configure BGP entre routers PE, este debe soportar el intercambio tradicional de prefijos IPv4 y el intercambio de prefijos VPNv4. Una sesión BGP entre routers PE es consecuentemente llamada una sesión BGP multiprotocolo (MP-BGP), este tipo de sesiones permite llevar rutas de múltiples familias de direcciones.⁶³

La propagación de rutas de un cliente a través de una red VPN MPLS se realiza de la siguiente manera:

1. Un router CE envía una actualización de enrutamiento IPv4 a un router PE.
2. El router PE agrega un RD de 64 bits a la actualización de enrutamiento IPv4, dando como resultado un prefijo VPNv4 único globalmente de 12 bytes.
3. El prefijo VPNv4 se propaga a través una sesión IBGP multiprotocolo (MP-IBGP) a otro router PE.
4. El router PE receptor remueve el RD del prefijo VPNv4, quedando únicamente un prefijo IPv4 (4 bytes).
5. El prefijo IPv4 es enviado a los otros routers CE dentro de una tabla de enrutamiento IPv4.

62 RFC 4026: Provider Provisioned Virtual Private Network (VPN) Terminology.

63 <https://tools.ietf.org/html/draft-ietf-l3vpn-rfc2547bis-03>

Figura 3.29. Diferenciadores de rutas (RD)

El RD no tiene un significado especial, solo se usa con el objetivo de hacer globalmente únicas las direcciones IPv4 que se están solapando al viajar por la red del SP. Este se usa como un identificador VPN, no obstante, este diseño basado en RDs no es soportado en las topologías de los clientes¹⁹.

El RD es configurado en el router PE como parte de la configuración del sitio VPN. El RD no es configurado en el router CE y no es visible para el cliente.

Las topologías normales de VPN requieren solamente un RD por cliente, incrementado la posibilidad de que el RD pueda servir como un identificador VPN. Este diseño, sin embargo, no permitiría la implementación de topologías VPN más complejas, tal como el sitio de un cliente que pertenece a múltiples VPNs.

Route Targets (RT).

Dado que al utilizar RDs no se puede indicar que un sitio participa en más de una VPN, es necesario establecer un método con el cual un conjunto de identificadores VPN pueda ligarse a una ruta para indicar que ésta es miembro de varias VPNs.

Para soportar este requerimiento, se introdujeron los Route Targets (RTs) en la arquitectura VPN de MPLS. Un RT es un atributo que puede ser pensado como el identificador de un grupo de sitios, o más precisamente, de un grupo de tablas virtuales de enrutamiento.

Asignando un RT particular a una ruta VPN, permite que esa ruta sea ubicada en todas las tablas virtuales usadas para enrutar el tráfico recibido de los sitios que tengan asociado ese RT (Fig. 3.30). Es decir, un RT puede ser visto como un FEC.

Figura 3.30. Route Targets

Cada tabla virtual de enrutamiento está asociada con uno o más atributos RT⁶⁴, ya que de acuerdo al tipo de tráfico o necesidades pueden existir varias rutas asociadas.

Cuando una ruta VPN-IPv4 o VPNv4 es creada por un router PE, esta se asocia con los RTs. Los RTs son transportados en BGP como atributos de la ruta.

Cualquier ruta asociada con un RT debe distribuirse a cada router PE que tenga una tabla virtual de enrutamiento con el RT configurado. Cuando dicha ruta es recibida por un router PE, esta puede ingresarse a las tablas de enrutamiento virtual asociados al RT, dependiendo de los resultados del proceso de decisión BGP y el IGP⁶⁵, ya que puede existir más de una ruta dirigida al mismo VPN-IPv4.

Así como las comunidades BGP estándar, un conjunto de comunidades extendidas pueden ser ligadas a una ruta BGP para satisfacer los requerimientos de topologías VPN más complejas. Estas comunidades portan el significado del atributo y su valor.

Las comunidades extendidas BGP son valores de 8 bytes. La semántica de las comunidades BGP extendidas están codificadas en el orden de valores de 16 bits, haciendo esos bits útiles para un número de diferentes aplicaciones, tal como MPLS VPN RTs. En resumen los Route Targets son necesarios porque:

64 RFC 4026: Provider Provisioned Virtual Private Network (VPN) Terminology.

65 RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs).

- Algunos sitios deben participar en más de una VPN.
- El RD no puede ayudar a identificar si un sitio está participando en más de una VPN.

Funcionamiento de las RTs.

Hay un conjunto de RTs que un router PE liga a una ruta en el momento que esta es convertida de una ruta IPv4 a una ruta VPNv4. Estos RTs son llamados “Targets exportados” y están configurados de manera separada para cada tabla virtual de enrutamiento en un router PE. Los RTs exportados identifican miembros de una VPN.

Otro grupo de RTs que un router PE utiliza para determinar si la ruta VPNv4 recibida de otro router PE puede importarse en su tabla virtual de enrutamiento asociada con un sitio, son llamados “Target importados”. Cada tabla virtual de enrutamiento en un router PE puede tener configurados varios RTs importados para identificar el conjunto de VPNs de las cuales la tabla virtual de enrutamiento está aceptando rutas.

Los dos conjuntos de RTs (importados y exportados) son diferentes⁶⁶.

En topologías VPN traslapadas, los RTs son usados para identificar miembros de una VPN. Las topologías VPN avanzadas (por ejemplo, central de servicios VPN) usan RTs en escenarios más complejos.

En resumen se tiene que los RTs exportados:

- Identifican miembros VPN.
- Se agrega a la ruta del cliente cuando esta se convierte en una ruta VPNv4.

Y los RTs importados:

- Se asocian con cada tabla virtual de enrutamiento.
- Seleccionar rutas para ser insertadas en la tabla virtual de enrutamiento.

Redefiniendo VPNs.

Con la introducción de topologías VPN más complejas, la definición de VPN tuvo la necesidad de cambiar. Una VPN es simplemente una colección de sitios compartiendo una información común de enrutamiento. En términos del switched WAN tradicional (por ejemplo, en terminología de X.25), tal concepto se llamaría “grupo de usuarios cerrado (CUG)”

66 <https://tools.ietf.org/html/draft-ietf-l3vpn-rfc2547bis-03>

En la implementación clásica de VPN, todos los sitios conectados a una VPN comparten una vista de enrutamiento común. En VPNs complejas, sin embargo, un sitio puede ser parte de más de una VPN, lo que tendría como resultado que se necesiten diferentes requerimientos de enrutamiento para sitios que pertenecen a una solo VPN y para aquellos que pertenecen a más de una. Estos requerimientos de enrutamiento tienen que ser soportados con múltiples tablas virtuales de enrutamiento en los routers PE.

Topologías VPN Complejas Sobre las Tablas Virtuales de Enrutamiento.

Una única tabla virtual de enrutamiento puede ser usada solamente para sitios con requisitos de conectividad idénticos. Topologías VPN complejas, por lo tanto, requiere más de una tabla virtual por VPN.

Si los sitios con diferentes requerimientos están asociados con la misma tabla virtual de enrutamiento, algunos de estos sitios podrían tener la capacidad de acceder a destinos que no deberían ser alcanzables.

Debido a que cada tabla virtual de enrutamiento requiere un RD, el número de RDs en una red VPN de MPLS incrementa con la introducción de VPNs traslapadas.

Introducción al Modelo de Enrutamiento VPN MPLS.

Requerimientos de Enrutamiento VPN

Los diseñadores de la tecnología MPLS VPN se enfrentaron con los siguientes requerimientos de enrutamiento:

- Los routers CE no deberían tener conocimiento de MPLS VPN, estos routers solo deberían ejecutar un protocolo de enrutamiento estándar.
- Los routers PE deben soportar los servicios MPLS VPN y los servicios tradicionales de internet.
- Para hacer de MPLS VPN una solución escalable, los routers P no deben llevar rutas VPN.

Modelo de Enrutamiento MPLS VPN.

El modelo de enrutamiento MPLS VPN debe cumplir las siguientes características:

- La troncal MPLS VPN debería verse como una troncal corporativa estándar a los routers CE.

- Los routers CE deben correr un protocolo de enrutamiento estándar (EBGP, OSPF, IS-IS), o enrutamiento estático para intercambiar actualizaciones de enrutamiento con los routers PE.
- Los routers PE se deben ver ante los routers CE como routers normales en la C-network.

Perspectiva Global del Cliente.

Desde la perspectiva del cliente (Fig. 3.31), la troncal MPLS VPN se ve como una troncal BGP intra-compañía con routers PE realizando la redistribución de rutas entre sitios individuales y el centro de la troncal. La regla estándar de diseño usada por empresas en las troncales BGP puede aplicarse al diseño de la C-network.

Los routers P están ocultos del cliente. La topología interna de la troncal BGP por consiguiente también es invisible al usuario.

Figura 3.31. Troncal VPN MPLS vista desde el cliente

Perspectiva de los Routers P.

Desde la perspectiva de los routers P (Fig. 3.32), la troncal MPLS VPN luce aún más simple, los routers P no participan en el enrutamiento MPLS VPN y no llevan rutas VPN. Los routers P ejecutan solamente una troncal IGP con otros routers P y PE e intercambian información acerca de las subredes internas. El despliegue de BGP sobre routers P no es necesario para una apropiada operación MPLS VPN. Podría ser necesario sin embargo, para soportar la conectividad tradicional de internet.

Figura 3. 32: Troncal VPN MPLS vista desde los routers P.

Perspectiva de los Routers PE.

Los routers PE son los únicos routers en la arquitectura MPLS VPN que ven todos los aspectos de enrutamiento de la red VPN (Fig. 3.33). Los routers PE están en capacidad de hacer lo siguiente:

- Intercambiar rutas VPN IPv4 (estas no son las mismas VPNv4 o VPN-IPv4) con routers CE a través de varios protocolos de enrutamiento corriendo en las tablas virtuales de enrutamiento.
- Intercambiar rutas VPNv4 a través de sesiones MP-IBGP con otros routers PE.
- Intercambiar rutas internas con routers P y otros routers PE a través del IGP.

Figura 3.33. Troncal VPN MPLS vista desde los routers PE

Soporte de Enrutamiento Para el Servicio de Internet Existente.

Muchos sitios VPN necesitarán acceder a internet, así como también necesitarán acceder a otras VPNs.

Los requerimientos de enrutamiento para routers PE también se extiende para soportar conectividad a internet, los routers PE tienen que intercambiar rutas de internet con otros routers PE, los routers CE no participan en el enrutamiento de internet, y los routers P pueden participar en la tabla de enrutamiento. Sin embargo, el enrutamiento de internet debería deshabilitarse en los routers P para hacer la red central más estable.

A continuación se presentan algunas alternativas para proporcionar acceso a internet a una red VPN⁶⁷:

- En algunas VPNs, uno o más sitios obtendrán acceso a internet a través de un Gateway (o un firewall) entre la interfaz del router CE (que no está ligada a una tabla virtual de enrutamiento) y el ISP (Fig. 3.34). Este ISP puede ser o no ser de la misma organización que ofrece los servicios de VPN. El tráfico desde/hacia el Gateway estaría enrutado de acuerdo a la tabla de enrutamiento por defecto del router PE.

67 RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs).

Figura 3.34. Acceso a internet a través de un SP distinto al SP VPN

En este caso, los sitios que tengan acceso a internet pueden distribuir una ruta por defecto hacia sus routers PE respectivos, los cuales redistribuirán esas rutas hacia los demás routers PE y sitios de la VPN (Fig. 3.5). Esto provee acceso a internet para todos los sitios de la VPN.

Figura 3.35. Redistribución de rutas por defecto

En este modelo, no hay intercambio de rutas entre la tabla de enrutamiento del router PE y las tablas virtuales de enrutamiento. Los procedimientos de distribución de rutas VPN y la distribución de rutas de internet son completamente diferentes.

- Algunas VPNs pueden obtener acceso a internet a través de una interfaz de una tabla virtual de enrutamiento (tabla de enrutamiento virtual de acceso a internet). Si un paquete, que es recibido por un router PE sobre una interfaz de la tabla virtual, posee una dirección de destino que no coincida con ninguna ruta en la tabla virtual

de enrutamiento, entonces puede ser ligado a la tabla de enrutamiento por defecto del router PE cuyo enrutamiento está basado en MPLS. Si por el contrario existe una coincidencia en la tabla virtual, el paquete puede ser enviado de forma nativa (enrutamiento normal sin tener presente la tecnología MPLS) a través de la troncal de internet (Entre routers PE) en vez de enviarse por MPLS (Fig. 3.36).

Para que el tráfico fluya sin ningún inconveniente desde internet hasta la interfaz de la tabla virtual, algunas de las rutas de la tabla virtual deben ser exportadas a la tabla de enrutamiento de internet.

En este esquema, la tabla de enrutamiento por defecto podría tener todo el enrutamiento a internet, o podría tener una ruta por defecto hacia otro router que si contenga enrutamiento completo de internet en su tabla de enrutamiento por defecto.

Figura 3.36. Acceso a internet usando tablas virtuales de enrutamiento

- Suponga que el PE tiene la capacidad de almacenar rutas que no sean VPN en su tabla virtual. Si la dirección de destino de un paquete coincide con una ruta que no sea VPN, entonces el paquete se transmite nativamente, en vez de enviarse a través de MPLS. Si la tabla virtual contiene una ruta por defecto que no sea VPN, todos los paquetes hacia internet coincidirán con esta, y serán enviados nativamente al siguiente salto a través de la ruta por defecto. En ese siguiente salto, la dirección de destino del paquete será buscada en la tabla de enrutamiento por defecto y puede que coincida con más rutas específicas (Fig. 3.37).

Esta técnica estaría disponible solamente si ninguno de los routers CE está distribuyendo una ruta por defecto.

Figura 3.37. Acceso a internet usando tablas virtuales con rutas VPN y no VPN

Tablas de enrutamiento en routers PE.

Los routers PE satisfacen varios requerimientos (Fig. 3.38) que se le han impuesto por utilizar varias tablas de enrutamiento IP, como se indica a continuación:

- La tabla global de enrutamiento contiene todas las rutas centrales aprendidas por el IGP y las rutas de internet aprendidas de la tabla global IPv4 BGP.
- Las tablas VRF (tablas virtuales) en routers CISCO contiene un conjunto de rutas para sitios con requisitos de enrutamiento idéntico. Las VRFs se llenan con información intra-VPN IGP intercambiada con routers CE y con rutas VPNv4 recibidas a través de sesiones MP-BGP desde otros routers PE.

Figura 3.38. Requerimientos cumplidos por routers PE

Flujo de las actualizaciones de enrutamiento de extremo a extremo de la conexión: Actualización MP-BGP

El proceso del flujo de las actualizaciones (Fig. 3.39) se describe a continuación:

- Los routers PE reciben actualizaciones de enrutamiento IPv4 desde los routers CE y las instalan en la tabla virtual de enrutamiento apropiada.
- Los routers PE exportan rutas VPN desde las tablas virtuales en MP-BGP y las propaga como rutas VPNv4 a otros routers PE.
- El router PE receptor importa la ruta VPNv4 entrante en la tabla virtual apropiada basado en los route targets (RTs) ligados a cada ruta.
- Las rutas instaladas en la tabla virtual de enrutamiento se convierten nuevamente en rutas IPv4 y se propagan a los routers CE.

Figura 3.39. Flujo de actualizaciones en MP-BGP

Una actualización MP-BGP intercambiada entre routers PE contiene lo siguiente:

- Direcciones VPNv4.
- Comunidades BGP extendidas (RT es requerido, Site of Origen (SOO), es opcional).
- Etiquetas usadas para el envío de paquetes VPN.
- Atributos BGP mandatorios.

Opcionalmente, las actualizaciones MP-BPG pueden contener cualquier otro atributo BGP, por ejemplo, preferencia local, MED, o una comunidad BGP estándar.

Se debe recordar que las sesiones MP-BGP entre routers PE son sesiones IBGP y están sujetas a las mismas reglas que aplican para las sesiones IBGP estándar como lo es el horizonte dividido, así como una malla completa de sesiones MP-IBGP. Si se utilizan route reflectors la operación debe ser igual (transparente).

Distribución de Rutas a Routers CE⁶⁸.

Las rutas VPNv4 se instalan en las tablas virtuales de enrutamiento en los routers PE receptores. La ruta entrante VPNv4 se importa a la tabla virtual solamente si posee un RT que coincida con al menos un RT importado configurado en la tabla virtual.

⁶⁸ RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs).

Si el PE ubica una ruta en particular en la tabla virtual, podrá utilizarla para enrutar paquetes recibidos desde un CE particular, con esta información el PE puede distribuir esa ruta al CE.

Existen más restricciones en la propagación de rutas desde el PE hasta el CE además de la configuración del horizonte dividido: El atributo SOO (Site Of Origin) ligado a la ruta VPNv4 controla la propagación de la ruta IPv4 a los routers CE. Una ruta insertada en una tabla de enrutamiento no debe propagarse a un router CE si el SOO adjunto a la ruta es igual al atributo SOO asociado con el router CE (el mismo SOO del emisor). Así el SOO también puede ser utilizado para prevenir bucles de enrutamiento en redes MPLS VPN con sitios multihomed.

En la mayoría de los casos, será suficiente para el router PE simplemente distribuir una ruta por defecto hacia el router CE. En algunos casos inclusive podría ser suficiente configurar una ruta por defecto en el CE hacia el PE.

Envío de Paquetes MPLS VPN.

Mecanismos de Envío VPN de Extremo a Extremo.

Enviar paquetes con un enfoque orientado al envío de paquetes MPLS VPN a través de una troncal MPLS VPN sería etiquetar los paquetes del cliente con la etiqueta asignada por el LDP hasta que llegue el al router PE de salida. Los routers centrales (P) nunca verían el paquete IP del cliente, en vez de ello, los routers P solo verán un paquete etiquetado dirigido hacia el router de salida. Los routers P solo desarrollarían operaciones sencillas de conmutación de paquetes basados en las etiquetas.

Infortunadamente, el paquete IP del cliente no contiene ninguna información VPN o VRF que pueda ser usada para realizar una búsqueda virtual en el router de salida (ya que la etiqueta solo contiene el router de salida al que se dirige). Así, el router de salida no sabría cual tabla virtual debe utilizar para hacer una búsqueda de envío y por consiguiente deberá desechar el paquete (Fig. 3.40).

Figura 3.40. Inconvenientes del envío VPN end to end

Para tratar de solucionar esta situación se podría utilizar un stack (pila) de etiquetas para decirle al router PE de salida qué hacer con el paquete VPN. Cuando se usa un stack de etiquetas, el router PE de ingreso etiqueta los paquetes IP con dos etiquetas. La etiqueta superior en el stack es la etiqueta LDP que indica el router de salida. Esta etiqueta garantiza que el paquete atravesará la troncal MPLS VPN y arribará al router de frontera.

Para una apropiada operación de MPLS VPN se requiere una segunda etiqueta VPN que fue asignada previamente por el router de salida a cada ruta VPN de los routers CE y a cada ruta sumariada al interior del router PE, y que luego será asignada por el router de entrada a las actualizaciones entrantes (Fig. 3.41).

Figura 3.41. Stack de etiquetas

Esta etiqueta debe ser propagada desde el router de salida hasta el router de ingreso para que haya un envío de paquetes correcto empleando MP-BGP como el mecanismo de propagación. Cada actualización MP-BGP porta una etiqueta asignada por el router PE de salida junto con el prefijo VPNv4 de 12 bytes.

Finalmente el router PE de ingreso tiene 2 etiquetas asociadas con una ruta VPN remota. Una etiqueta indica el salto siguiente asignada a través del LDP para hacer los saltos siguientes, empleando para ello la tabla LIB (Label Information Base) local. Y también la etiqueta asignada por el router PE de salida. Esta última etiqueta le indica al router de salida como enviar los paquetes VPN entrantes. Esta etiqueta puede apuntar directamente hacia una interfaz de salida, en cuyo caso el router solo debería realizar una búsqueda de etiquetas en el paquete VPN, o también podría apuntar a una tabla virtual, en cuyo caso el router

debería realizar una búsqueda de etiquetas para encontrar la tabla virtual objetivo y luego desarrollar una búsqueda de dirección IP dentro de la tabla virtual para enviar el paquete.

La segunda etiqueta apunta hacia una interfaz de salida siempre que el router CE sea el siguiente salto de la ruta VPN.

Ambas etiquetas se combinan en un stack de etiquetas y se instalan en la tabla virtual.

Estas dos etiquetas en el stack satisfacen los siguientes requerimientos de envío de MPLS VPN:

- Los routers P realizan conmutación de etiquetas sobre la etiqueta LDP asignada hasta el router de salida.
- El router PE de salida desarrolla una búsqueda en la etiqueta VPN y luego otra búsqueda IP en la tabla virtual apuntada por la etiqueta.

VPN PHP (Penultimate Hop Popping).

La opción PHP (Retirar la etiqueta superior del stack en el salto anterior al router de salida) puede ser realizada en redes MPLS modo trama. En estas redes el último router P (Penúltimo antes del router PE) en el túnel LSP (Label Switched Path) quita la etiqueta LDP, y el router PE recibirá un paquete etiquetado que contiene solo la etiqueta VPN a la que se dirige el paquete, o simplemente un paquete IP⁶⁹ (Fig. 3.42). En la mayoría de los casos, con solo una búsqueda de etiqueta sobre ese paquete en el router de salida es suficiente para enviar el paquete hacia el router CE.

Figura 3.42. VPN PHP

Efectos de MPLS VPN Sobre el Envío de Paquetes.

Para una propagación exitosa de paquetes MPLS VPN a través de una troncal MPLS, debe existir un túnel LSP entre los routers PE que sea estable. Esto se debe a que la segunda etiqueta en el stack solo es reconocida por el router de salida ya que él fue quien la originó.

A continuación se presentan dos escenarios que pueden causar que el túnel LSP entre los routers PE se rompa:

- Si la dirección IP del router PE se anuncia como una ruta BGP, no tendrá una etiqueta LDP correspondiente y el stack no será construido correctamente.
- Si los routers P realizan la sumarización de un rango de direcciones en la cual se encuentra la dirección del router PE de salida, el túnel LSP se verá afectado en el punto de sumarización.

Bibliografía

Request for Comments (RFC).

PROCESOS Y HERRAMIENTAS PARA LA SEGURIDAD DE REDES

Editorial: UNED.

Año: 2004.

Autores: Castro gil Manuel Alonso, Díaz Orueta Gabriel, Alzórriz Armendáriz Ignacio, Sancristóbal Ruiz Elio.

ScreenOS Cookbook.

Editorial: O'Reilly Media, Inc.

Año: 2008.

Autores: Stefan Brunner, Vik Davar, David Delcourt, Ken Draper, Joe Kelly, Sunil Wadhwa.

High Performance Networks: Simplified!

Editorial: SKNCOE Computer Department.

Autores: Dnyanada Arjunwadkar, Nivedita Wadke, Koninika Patil.

Voice Over MPLS.

Editorial: McGraw Hill Professional.

Año: 2002.

Autor: Daniel Minoli.

INGENIERÍA DE TRÁFICO EN REDES DE CONMUTACIÓN DE ETIQUETAS.

Artículo.

Año: 2009.

Autor: Danilo Alfonso López Sarmiento, Nancy Yaneth Gelvez García.

Conmutación de Etiquetas Multiprotocolo (MPLS) .

Presentación Dr. Ing. Álvaro Rendón Gallón.

Año: 2012.

Autor: Álvaro Rendón Gallón.

Alcatel-Lucent Network Routing Specialist II (NRS II) Self-Study Guide: Preparing for the NRS II Certification Exams.

Editorial: John Wiley & Sons.

Año: 2011.

Autores: Glenn Warnock, Amin Nathoo.

MPLS-Enabled Applications: Emerging Developments and New Technologies.

Editorial: John Wiley & Sons.

Año: 2010.

Autores: Ina Minei, Julian Lucek.

Redes de banda ancha.

Editorial: Marcombo.

Año: 1997.

Autores: José Manuel Caballero, José Manuel Caballero Artigas.

Redes de computadoras.

Editorial: Pearson Educación.

Año: 2003.

Autor: Andrew S. Tanenbaum.

Optical Networking Standards: A Comprehensive Guide for Professionals.

Editorial: Springer Science & Business Media.

Año: 2007.

Autor: Khurram Kazi.

Network Dictionary.

Editorial: Javvin Technologies Inc.

Año: 2007.

Autor: Jielin Dong.

MPLS for Metropolitan Area Networks.

Editorial: CRC Press.

Año: 2004.

Autor: Nam-Kee Tan.

MPLS and VPN Architectures, Volumen 1.

Editorial: Cisco Press.

Año: 2003.

Autores: Ivan Pepelnjak, Jim Guichard.

IP, Ethernet and MPLS Networks: Resource and Fault Management.

Editorial: John Wiley & Sons.

Año: 2013.

Autor: André Pérez.

Managing IP Networks: Challenges and Opportunities.

Editorial: John Wiley & Sons.

Año: 2003.

Autores: Salah Aidarous, Thomas Plevyak.

MPLS: Next Steps: Next Steps.

Editorial: Morgan Kaufmann.

Año: 2008.

Autores: Bruce S. Davie, Adrian Farre.

PARTE 2

ÍNDICE PARTE II

Introducción.....	135
Módulo 1.....	137
Implementación de VPN MPLS.....	139
Usando VPN MPLS.....	139
Tabla de Enrutamiento Virtual.....	139
Uso de las Tablas Virtuales.....	142
Creación de Una Tabla Virtual.....	143
Sesión MP-BGP Entre Routers PE.....	143
Intercambio de Rutas con BGP.....	143
Vecinos BGP.....	144
Propagación de Comunidades MP-BGP.....	145
Configuración de Protocolos de Enrutamiento a Pequeña Escala Entre Routers PE y CE.....	145
Protocolos de Enrutamiento PE-CE.....	145
OSPF como protocolo de enrutamiento entre routers PE-CE.....	146
Modelo Jerárquico Mejorado de OPSE.....	146
Propagación de Rutas OSPF de los Clientes a Otros Routers PE.....	148
MPLS L3VPN en OSPF.....	150
Objetivos de OSPF en VPN MPLS.....	151
Reglas de una Troncal L3VPN OSPF.....	153
Prevención de Bucles.....	153
Prevención de Bucles: Down Bit (DN bit).....	154
Campo de Etiqueta OSPF.....	154
Optimización en el Envío de Paquetes a través de la Troncal VPN MPLS.....	155
Enlace Simulado (Sham Link).....	158
Razones para Limitar el Número de Rutas en una Tabla Virtual.....	160
BGP como Protocolo de Enrutamiento Entre Routers PE-CE.....	160
Inconvenientes del Reemplazo del SA (AS-Override Issues).....	160
Identificando Inconvenientes de Allow as-in.....	163
Implementación de allow as-in.....	164
Utilizando el Atributo SOO para Prevención de Bucles.....	165
Resolución de Problemas en VPN MPLS.....	167
Verificación del Flujo de Información.....	168
Verificación del Flujo de Datos.....	169
Módulo 2.....	171
MPLS VPNs Complejas.....	173
Uso de las Características Avanzadas de Importar y Exportar en las Tablas Virtuales.....	173
Características Avanzadas de la Tabla Virtual.....	173
Importación Selectiva de la Tabla Virtual.....	174
Exportación Selectiva de la Tabla Virtual.....	175
VPNs Traslapadas.....	175
Participantes de una VPN Traslapada.....	177
Uso de una VPN Traslapada.....	177

Central de Servicios VPN.....	178
Características de Acceso de una Central de Servicios VPN.....	178
Características de Enrutamiento de una Central de Servicios VPN.....	179
Modelo del Flujo de Datos en la Central de Servicios VPN.	179
Requerimientos de Configuración de una Central de Servicios VPN.....	180
Gestión del Servicio en Routers CE.	180
Requisitos de los Routers Gestionados.	180
Requerimientos de la Tabla Virtual y del Identificador de Ruta (RD).....	181
 Módulo 3.....	 183
Acesso a Internet Desde una Red MPLS VPN.	185
Topologías VPN de Acceso a Internet.	185
Acceso Clásico a Internet para un Cliente VPN.	185
Requerimientos de Direccionamiento en el Acceso Clásico a Internet.....	186
Flujo del Tráfico de Internet en una Troncal MPLS VPN.....	187
Métodos de Acceso a Internet Desde Cada Sitio de un Cliente.....	188
Beneficios.....	189
Desventajas.....	189
Acceso a Internet Desde Cada Sitio de un Cliente: Direccionamiento.	189
Acceso a Internet Desde Cada Sitio de un Cliente: Troncal MPLS VPN.....	190
Servicio de Central de Firewalls (Central Firewall Service).	191
Servicio de Firewall Central: Direccionamiento.	192
Servicio de Firewall Central: Flujo de Tráfico.....	192
Acceso a Internet al Por Mayor.	193
Acceso a Internet al Por Mayor: Direccionamiento.....	194
Implementación de los Métodos VPN de Acceso a Internet.....	195
Los Modelos de Diseño Más Implementados.	195
Acceso a Internet a través de Enrutamiento Global.	195
Acceso a Internet a través de Interfaces Separadas o Subinterfaces.....	195
Beneficios.....	195
Desventajas.....	196
Acceso a Internet en VPNs.	196
Separación del Acceso a Internet de los Servicios VPN.....	196
Acceso a Internet Separado de las VPNs.	196
Implementando Sub-interfaces Separadas.	196
Acceso Clásico a Internet para un Cliente VPN.	197
Acceso a Internet desde Cada Sitio de un Cliente.	197
Acceso a Internet Separado.	198
Implementando el Acceso a Internet Como una VPN Separada.....	199
Acceso a Internet Como una VPN Separada.	199
Implementando Acceso a Internet Redundante.	200
Implementación del Acceso a Internet Clásico Para un Cliente VPN.....	201
Acceso a internet desde cada sitio de un cliente.....	201
Acceso a Internet a través de un Servicio de Firewall Central.....	202
Acceso a la Internet al Por Mayor.	203
Ejecutando una Troncal de Internet en una VPN.	204
 Bibliografía.	 205

Índice de figuras

Módulo 1

Figura 1. 1: Esquema para tablas de enrutamiento virtuales.	140
Figura 1. 2: Tabla virtual utilizando una misma instancia del protocolo de enrutamiento en dos VPNs.	141
Figura 1. 3: Tabla virtual utilizando instanciaciones diferentes del mismo protocolo de enrutamiento en dos VPNs.	141
Figura 1. 4: Instancia de enrutamiento para la tabla virtual.	142
Figura 1. 5: Interfaces asociadas a tablas virtuales de enrutamiento.	143
Figura 1. 6: Tipos de vecino BGP.	144
Figura 1. 7: Dominio OSPF.	146
Figura 1. 8: Áreas y sitios en un dominio OSPF.	147
Figura 1. 9: Área troncal directamente conectada a un sitio.	147
Figura 1. 10: Router de frontera de área (ABR).	148
Figura 1. 11: Distribución de rutas VPN-IPv4 empleando MP-BGP.	149
Figura 1. 12: Redistribución de rutas OSPF.	150
Figura 1. 13: Troncal L3VPN.	151
Figura 1. 14: Troncal L3VPN entre routers ABR.	152
Figura 1. 15: Continuidad de enrutamiento OSPF con la arquitectura de troncal L3VPN OSPF.	152
Figura 1. 16: Bucles de enrutamiento en un dominio OSPF.	153
Figura 1. 17: Ruta distribuida con el DN bit.	154
Figura 1. 18: Sitios de cliente como sitios de tránsito.	155
Figura 1. 19: Sitios de cliente como sitios de tránsito 2.	156
Figura 1. 20: Sitios de cliente como sitios de tránsito 3.	157
Figura 1. 21: Flujo indeseado VS flujo deseado.	157
Figura 1. 22: Puerta trasera entre dos sitios VPN.	158
Figura 1. 23: Enlace simulado.	159
Figura 1. 24: Funcionamiento tradicional de prevención de bucles.	161
Figura 1. 25: Funcionamiento del reemplazo del SA (AS-Override) [1].	161
Figura 1. 26: Funcionamiento del reemplazo del SA (AS-Override) [2].	162
Figura 1. 27: Funcionamiento AS-Override (3).	162
Figura 1. 28: Perspectiva VPN de un router CE enlazando dos VPNs.	163
Figura 1. 29: Perspectiva física de un router CE enlazando dos VPNs.	163
Figura 1. 30: Perspectiva de VPN MPLS de un router CE enlazando dos VPNs.	163
Figura 1. 31: Regla de prevención de bucles.	164
Figura 1. 32: Característica Allowas-in.	165
Figura 1. 33: Esquema general del atributo SoO.	166
Figura 1. 34: Remoción del ANS en router PE a través de un route-map.	166
Figura 1. 35: Funcionamiento del atributo SoO.	167

Módulo 2

Figura 2. 1: Funcionamiento de la importación selectiva.	174
Figura 2. 2: Funcionamiento de la exportación selectiva.	175
Figura 2. 3: VPNs con espacio de direcciones traslapado.	176
Figura 2. 4: Uso de las VPNs traslapadas.	177
Figura 2. 5: Central de servicios VPN.	178
Figura 2. 6: Uso de la central de servicios VPN.	179
Figura 2. 7: Gestión de routers CE desde un punto centralizado.	181

Módulo 3

Figura 3. 1: Acceso clásico a internet a través de un firewall.....	186
Figura 3. 2: Inconvenientes de cuello de botella en el acceso a internet tradicional.	187
Figura 3. 3.1: Diseño de troncal MPLS VPN y troncal de internet compartida.	187
Figura 3.3.2. Diseño de troncal MPLS VPN y troncal de internet compartida (escenario detallado).....	188
Figura 3. 4: Acceso a internet desde cada sitio de un cliente utilizando NAT.....	189
Figura 3. 5: Acceso a internet desde cada sitio cliente utilizando un enlace compartido.....	190
Figura 3. 6: Firewall dedicado por cliente.....	191
Figura 3. 7: Firewall centralizado.....	191
Figura 3. 8: Acceso a internet desde cada sitio de un cliente utilizando NAT entre los sitios y el firewall central.....	192
Figura 3. 9: Flujo de tráfico en una implementación con firewall central.....	193
Figura 3.10.1: Servicio de troncal de internet compartida entre varios ISPs.....	194
Figura 3.10.2: Servicio de troncal de internet compartida entre varios ISPs(Detallada).....	194
Figura 3. 11: Acceso clásico a internet para un cliente VPN.....	197
Figura 3. 12: Acceso a internet desde cada sitio cliente.....	198
Figura 3. 13: Acceso a internet como VPN separada en las tablas virtuales del cliente.....	199
Figura 3. 14: Acceso a internet redundante.....	200
Figura 3. 15: Acceso a internet clásico para un cliente VPN.....	201
Figura 3. 16: Acceso a internet desde cada sitio cliente VPN.....	202
Figura 3. 17: Acceso a internet a través de un servicio de firewall central.....	203
Figura 3. 18: servicio general de acceso a internet.....	204

Introducción

Las redes MPLS (MultiProtocolLabelSwitching) son un tipo de redes privadas de comunicación ofrecidas por las principales empresas de telecomunicaciones con la peculiaridad que utilizan etiquetas capa 2.5 del modelo OSI para tomar las decisiones de enrutamiento. El protocolo MPLS permite encaminar paquetes de cualquier protocolo de red gracias a estas etiquetas. Este protocolo fue desarrollado con el objetivo de permitirle a los routers tomar decisiones de enrutamiento rápidas⁷⁰.

MPLS es un método de alto rendimiento para el envío de paquetes a través de una red, habilitando a los routers de frontera para que apliquen etiquetas sobre los paquetes y por consiguiente se pueden tomar decisiones de enrutamiento basadas en estas etiquetas con una búsqueda que requiere un gasto mínimo. MPLS integra tanto el rendimiento como la gestión de tráfico de la capa de enlace de datos con la escalabilidad y flexibilidad de la capa de red⁷¹.

70 Procesos y herramientas para la seguridad de redes – p.549.

71 RFC 3031: Multiprotocol Label Switching Architecture.

MÓDULO 1

Implementación de VPN MPLS.

Usando VPN MPLS.

Tabla de Enrutamiento Virtual.

En las redes VPNs es necesario crear una tabla de enrutamiento que sea independiente de la principal y de otras tablas de enrutamiento. Esta tabla tiene varios nombres de acuerdo a los principales proveedores pero el concepto es sí es el mismo. Cisco llama a estas tablas VRF (Virtual Routing and Forwarding), Huawei la llama enrutamiento VPN (VPN routing) y Juniper se refiere a ella como instancias de enrutamiento⁷².

Para emplear un concepto claro, de ahora en adelante estas tablas VRF o instancias de enrutamiento, serán llamadas tablas virtuales de enrutamiento o tablas virtuales.

Cada router PE mantiene un número separado de tablas de enrutamiento (forwardingtables). Una de estas tablas es la tabla de enrutamiento principal (o de enrutamiento por defecto), y las otras son tablas virtuales de enrutamiento⁷³.

Esta tabla es una instancia de enrutamiento y envío para un conjunto de sitios con requerimientos de conectividad idénticos y puede ser utilizada para un solo sitio VPN (Fig. 1.1) o para muchos sitios conectados al mismo Router de Frontera del Proveedor o router PE.

72 VRFs–Basic concept.

73 RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs).

Figura 1.1. Esquema para tablas de enrutamiento virtuales

Algunos atributos VPN MPLS asociados con las tablas virtuales son los siguientes⁷⁴:

- El identificador de ruta (RD), el cual es agregado a todas las rutas (RD + IP address) exportadas desde la tabla virtual dando como resultado las direcciones VPNv4.
- Un conjunto de export targets (RT), los cuales están ligados a cualquier ruta exportada desde la tabla virtual.
- Un conjunto de RTs importados, los cuales son usados para seleccionar rutas VPNv4 que van a ser importadas a la tabla virtual.

No todos los dispositivos de los fabricantes como Cisco, Juniper y Huawei permiten crear varias instancias de enrutamiento de los protocolos como RIP, LDP, IS-IS o BGP. El software tradicional de Cisco solo podría ejecutar una única copia o instancia de estos protocolos, en cambio Juniper si los soporta⁷⁵.

En el caso de Cisco no se podrían utilizar estos protocolos directamente entre routers PE y CE en ambientes de VPN puesto que cada VPN necesita una instancia separada y aislada del protocolo de enrutamiento para evitar enrutamiento indeseado entre VPNs (Fig. 1.2). Adicionalmente, las VPNs pueden solaparse (uso de las mismas direcciones al interior de cada VPN) el espacio de direcciones lo que puede causar confusiones de enrutamiento si todas las VPNs comparten la misma copia del protocolo de enrutamiento.

⁷⁴ RFC 4026: Provider Provisioned Virtual Private Network (VPN) Terminology.

⁷⁵ Routing Instances Overview Juniper.

Figura 1. 2. Tabla virtual utilizando una misma instancia del protocolo de enrutamiento en dos VPNs

El protocolo OSPF es una solución tanto para Cisco, Juniper y Huawei para crear múltiples instancias del mismo protocolo de enrutamiento⁷⁶ de forma aislada y separada (Fig. 1.3) aunque agrega una sobrecarga adicional a los router⁷⁷ PE y CE.

Figura 1.3. Tabla virtual utilizando instanciaciones diferentes del mismo protocolo de enrutamiento en dos VPNs

Cuando se implementan varias instancias de un protocolo de enrutamiento, cada instancia contiene sus propios parámetros de enrutamiento, por ejemplo temporizadores,

⁷⁶ OSPFv2 Multi-Instance Extensions.

⁷⁷ Guía de diseño de OSPF, Cisco.

parámetros de autenticación, interfaces pasivas, vecinos, etc. Esta independencia le permite al administrador de la red una mayor flexibilidad en la implementación de protocolos de enrutamiento entre routers PE y CE.

Uso de las Tablas Virtuales.

Cada tabla virtual posee unas instancias que se le asignan a cada VPN que tenga conectada (Fig. 1.4). El router PE debe encargarse de mantener estas instancias separadas y actualizarlas manualmente o a través de un protocolo de enrutamiento. Las rutas que se reciban desde una instancia del protocolo de enrutamiento configurado para la tabla virtual se insertan en la tabla de enrutamiento virtual correspondiente. Cada una de estas tablas soporta los mecanismos como filtros, procesos de selección de ruta, entre otros.

Figura 1.4. Instancia de enrutamiento para la tabla virtual

La tabla FIB (Forwarding Information Base) se construye a partir de la tabla virtual y se usa para enviar todos los paquetes recibidos a través de las interfaces asociadas con cada tabla virtual. Cualquier interfaz, ya sea física o lógica puede estar asociada con una tabla virtual (Fig. 1.5).

Cuando un router PE recibe un paquete de un router CE, el PE debe determinar sobre que VC (Virtual Circuit o Circuito Virtual) ha llegado el paquete para determinar que tabla o tablas virtuales puede emplear para enviar el paquete. En general, para determinar el VC sobre el que el paquete llegó, el PE toma nota de la interfaz física por la que recibió el paquete⁷⁸.

⁷⁸ RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs).

Figura 1.5. Interfaces asociadas a tablas virtuales de enrutamiento

No hay un límite para el número de interfaces asociadas con una tabla virtual (El límite lo da el número de interfaces del router). Sin embargo, en la práctica cada interfaz puede ser asignada a solamente una tabla virtual porque el router necesita identificar de manera única la tabla FIB a ser usada para los paquetes recibidos sobre una determinada interfaz.

Creación de Una Tabla Virtual.

Una tabla virtual comienza con el despliegue de un servicio VPN MPLS para un cliente y consiste en cuatro pasos obligatorios:

- Crear una tabla virtual.
- Asignar un RD único a cada tabla virtual creada en el router PE.
- Especificar RTs importados y exportados para la tabla virtual.
- Asignar interfaces a las tablas virtuales.

Sesión MP-BGP Entre Routers PE.

Intercambio de Rutas con BGP.

Independientemente de la arquitectura VPN MPLS, el router PE puede usar actualizaciones de rutas BGP IPv4 para recibir y propagar rutas de internet en las situaciones donde los routers PE también son usados para proveer conectividad a internet a los clientes.

El proceso de BGP en VPN MPLS habilita al router para realizar tres tareas separadas⁷⁹:

- Intercambiar actualizaciones de enrutamiento BGP con routers CE como se hace en la configuración tradicional BGP.
- Intercambiar rutas VPNv4 a través de la troncal VPN MPLS utilizando MP-BGP entre routers PE.
- Intercambiar rutas VPN con routers CE a través de sesiones EBGp por cada tabla virtual.

Los tres mecanismos de intercambio tienen lugar en un proceso BGP (Porque solo se puede configurar un proceso BGP por router). Las familias de direcciones (IPv4 Unicast, IPv4 Multicast, IPv6 Unicast, IPv6 Multicast, entre otras) llamadas así desde la perspectiva de la configuración de un router, son usadas para configurar los 3 mecanismos independientes de intercambio de rutas.

Vecinos BGP.

La arquitectura VPN MPLS, como se ve en la figura 1.6, define dos tipos de vecinos BGP:

- Vecinos globales BGP (otros routers PE) con los cuales un router PE puede intercambiar múltiples tipos de rutas. Estos vecinos se encuentran establecidos en la definición global de BGP y solamente tienen que estar activados para ciertas familias de direcciones. Las familias que no se encuentren activadas no serán recibidas para realizar intercambios.
- Vecinos BGP por tabla virtual (routers CE), los cuales están configurados bajo su correspondiente familia de direcciones (IPv4).

Figura 1.6. Tipos de vecino BGP

Los pasos a seguir para realizar la configuración de vecinos PE son:

- Configurar el router PE remoto como vecino BGP global.
- Definir los parámetros que afectarán el intercambio de rutas BGP (por ejemplo, dirección origen para la sesión TCP).

79 Multiprotocol BGP MPLS VPN, Cisco.

- Seleccionar la familia de direcciones VPNv4 y activar los vecinos BGP para intercambio de rutas VPNv4.
- Configurar parámetros específicos VPNv4 BGP adicionales (filtros, routemaps, etc) dentro de la familia de direcciones VPNv4.

Propagación de Comunidades MP-BGP.

La arquitectura VPN MPLS introdujo el atributo BGP “comunidad extendida” (extended community) sin reemplazar la “comunidad estándar”.

A diferencia de la propagación de las comunidades estándar que se configuran manualmente, las comunidades extendidas se propagan por defecto ya que de esto depende que VPN MPLS tenga una operación exitosa.

Configuración de Protocolos de Enrutamiento a Pequeña Escala Entre Routers PE y CE.

Protocolos de Enrutamiento PE-CE.

Después de realizar la configuración de las tablas virtuales y establecer la conectividad MP-IBGP entre routers PE, se debe trabajar con los protocolos de enrutamiento entre el router PE y los routers CE que tengan conectados. Los protocolos de enrutamiento PE-CE como RIP o EIGRP deben configurarse individualmente para cada tabla virtual. Los sitios en la misma VPN que se encuentran en diferentes tablas virtuales no pueden compartir el mismo protocolo de enrutamiento PE-CE. Por tal motivo es una buena razón agrupar tantos sitios en una misma tabla virtual como sea posible y configurar un protocolo de enrutamiento PE-CE por cada una de estas tablas para evitar que la tarea administrativa sea dispendiosa. Los protocolos de enrutamiento por tabla virtual se pueden configurar de dos maneras:

- Como una familia individual de direcciones ligada al mismo proceso de enrutamiento.
- Como procesos de enrutamiento separados. Esta opción es utilizada en protocolos de enrutamiento más complejos que necesitan una topología de base de datos separada para cada tabla virtual (ej, OSPF).

Configurar RIP como protocolo de enrutamiento PE-CE es aún más fácil que configurar BGP. Al momento de configurar RIP se pueden utilizar los parámetros estándar empleados tradicionalmente.

Por defecto, el contador de saltos en RIP se inserta en el atributo MED de BGP cuando las rutas aprendidas a través de RIP han sido redistribuidas al interior de BGP por el router PE de ingreso.

Al utilizar RIP con otros protocolos se debe configurar la métrica manualmente.

Los mecanismos utilizados por RIP para detectar bucles son el horizonte dividido y SOO80.

OSPF como protocolo de enrutamiento entre routers PE-CE⁸¹.

Es de esperarse que muchas VPNs utilicen OSPF como su IGP. Esto no quiere decir que los routers PE también deban utilizar OSPF para conectarse con los routers CE. Cada sitio puede usar OSPF como su protocolo de enrutamiento intra-sitio, mientras utilizan BGP o RIP para distribuir rutas a un PE. No obstante, es conveniente que cuando se utiliza OSPF como protocolo IGP en una VPN, el enlace PE-CE también lo sea.

Modelo Jerárquico Mejorado de OPSF.

El protocolo de enrutamiento OSPF fue diseñado para soportar redes jerárquicas con una troncal central o área 0. Una red que esté corriendo OSPF es dividida en áreas. Toda la red OSPF (área 0 y las demás áreas) es conocida como dominio OSPF (Fig. 1.7).

Figura 1.7. Dominio OSPF

Las áreas OSPF en la red del cliente pueden corresponder a sitios individuales, pero a menudo también se pueden encontrar las siguientes situaciones:

- Una única área puede abarcar múltiples sitios (por ejemplo, en la figura 1.8, un cliente decide usar un área por región, pero la región contiene múltiples sitios).

80 Configuring MPLS Basic VPN with RIP on Customer Side, Cisco.

81 RFC 4577: OSPF as the Provider/Customer Edge Protocol for BGP/MPLS IP Virtual Private Networks (VPNs).

Figura 1.8. Áreas y sitios en un dominio OSPF

- El área troncal puede extenderse a sitios individuales (Fig. 1.9).
En esta situación, se debe tener en cuenta que aunque el área 0 se pueda extender a más de un sitio, esto no es recomendable ya que esta área se debe reservar como troncal entre todas las áreas. Por otra parte, existen 254 valores adicionales para utilizar y dejar el 0 solo con funciones de troncal.

Figura 1.9. Área troncal directamente conectada a un sitio

Al interior de un determinado dominio OSPF, existen routers intermedios que no pertenecen completamente al área troncal u otra área, son partícipes de ambas. A este tipo de router se le conoce como router ABR (Area Border Router) o router de frontera de área (Fig. 1.10).

Figura 1.10. Router de frontera de área (ABR)

Los routers de área de frontera son un tipo de router que está localizado en el borde de una o más áreas, y se utiliza para establecer conexión entre la troncal y las áreas OSPF⁸². Es un miembro de ambas redes, tanto de la troncal como de las áreas que conecta, por consiguiente, este router almacena y mantiene de forma separada información de enrutamiento o tablas de enrutamiento independientemente de la troncal y de la topología de las áreas a las cuales esté conectado.

Un router PE que esté ligado a más de un dominio OSPF debe correr una instancia independiente de OSPF para cada una de estas. Si el PE utiliza OSPF como su IGP, la instancia de OSPF corriendo como IGP debe ser independiente y estar separada de cualquier otra instancia de OSPF que el PE esté ejecutando. Cada interfaz que esté ligada a un sitio VPN no debe tener más de una instancia OSPF.

VPN define la notación de tabla virtual por sitio. Si una tabla virtual está asociada con una interfaz en particular, y la interfaz pertenece a una instancia particular de OSPF, entonces se dice que esta instancia está asociada con la tabla virtual. Si dos interfaces pertenecen a la misma instancia OSPF, entonces ambas interfaces deben estar asociadas con la misma tabla virtual.

Si una interfaz está enlazando un PE con un CE, y esa interfaz está asociada con una tabla virtual, entonces el CE estará asociado con la tabla virtual.

Propagación de Rutas OSPF de los Clientes a Otros Routers PE.

OSPF es utilizado para distribuir rutas desde un CE hasta un PE, y la mejor de estas rutas de acuerdo al proceso de selección de mejor ruta es la que se instala en la tabla virtual.

82 Areas and Area Border Routers, Juniper.

En VPN, BGP es utilizado para distribuir rutas VPN-IPv4 entre routers PE (Fig. 1.11). Una ruta OSPF instalada en una tabla virtual puede ser exportada a través de la redistribución de BGP como una ruta VPN-IPv4 para que llegue a otros PEs. En los otros PEs, una ruta VPN-IPv4 puede ser importada por una tabla virtual y luego redistribuirla a una o más instancias OSPF asociadas con esta tabla virtual.

El modelo de enrutamiento VPN MPLS introduce una troncal BGP en la red del cliente. Diferentes copias de un proceso IGP corren en cada sitio de manera independiente, y MP-BGP es usado para propagar las rutas entre estos sitios. Por lo tanto, cada router PE debe redistribuir las rutas entre clientes, routers PE-CE y la troncal BGP.

Entonces se tiene que:

- Desde la perspectiva del cliente, una red basada en VPN MPLS tiene una troncal BGP con un IGP corriendo en los sitios del cliente.
- La redistribución entre el IGP y BGP se realiza para propagar las rutas de los clientes a través de la troncal VPN MPLS.

Figura 1.11. Distribución de rutas VPN-IPv4 empleando MP-BGP

La redistribución IGP-BGP introducida por el modelo de enrutamiento VPN MPLS no encaja muy bien en las redes de los clientes que ejecutan OSPF. Cuando un cliente OSPF migra a un servicio VPN MPLS, cualquier ruta que sea redistribuida en OSPF desde otro protocolo de enrutamiento será redistribuida como ruta OSPF externa. Las rutas OSPF recibidas por un router PE son propagadas a través de la troncal MPLS y se redistribuyen de nuevo en OSPF hacia otros sitios como rutas externas OSPF (Fig. 1.12).

Con la redistribución tradicional de OSPF-BGP, no se preserva el tipo de ruta OSPF (Interna o externa) cuando se redistribuye en BGP. Por lo tanto, cuando esa misma ruta se redistribuya de nuevo en OSPF, siempre aparecerá como una ruta externa OSPF.

- * Área 1 y área 2 pertenecen a una misma VPN y comparten un rango de direcciones.
- * Cuando área 1 envía una ruta OSPF interna a la troncal BGP esta se convierte en una ruta VPN-IPv4.
- * Al distribuir la ruta OSPF del área 1 al área 2 esta debería ser local pero llega como externa.

Figura 1.12. Redistribución de rutas OSPF

A continuación se indican algunas de las restricciones asociadas con las rutas externas OSPF⁸³:

- Las rutas externas no pueden ser sumariadas.
- Las rutas externas se inundan a través de todas las áreas OSPF.
- Las rutas externas pueden usar diferentes tipos de métricas que no son comparables al costo OSPF.
- Las rutas externas no se insertan en áreas stub o áreas not-so-stubby (NSSAs), estas últimas son un tipo de área stub que puede importar rutas externas de Sistemas Autónomos (SAs) y enviarlas al backbone, pero ninguna de las dos puede recibir rutas externas de SAs desde el backbone u otras áreas.
- Las rutas internas siempre se prefieren sobre rutas externas independientemente del costo.

Debido a las situaciones mencionadas, migrar un cliente OSPF hacia un servicio VPN MPLS podría tener un fuerte impacto sobre el enrutamiento de ese cliente. La arquitectura VPN MPLS por lo tanto debe extender el modelo de enrutamiento clásico OSPF-BGP para soportar una migración que sea transparente a los clientes.

MPLS L3VPN en OSPF.

MPLS L3VPN o en terminología cisco conocida como supertroncal, de ahora en adelante troncal L3VPN, es una tecnología basada en routers PE (Fig. 1.13), y se utiliza para propagar rutas VPN empleando MPLS para enviar paquetesVPN sobre la o las troncales de un SP (Service Provider).⁸⁴

83 RFC 3101: The OSPF Not-So-Stubby Area (NSSA) Option.

84 04-MPLS L3VPN Configuration, H3C.

La troncal L3VPN OSPF se implementa con MP-BGP entre routers PE pero de una manera completamente transparente a los routers OSPF presentes en la red. Con esta nueva arquitectura se permite que la troncal OSPF (Área 0) se divida en varios segmentos.

Figura 1.13. Troncal L3VPN

Objetivos de OSPF en VPN MPLS.

A continuación se presentan los objetivos que debe cumplir la troncal L3VPN OSPF:

- La troncal L3VPN no debe usar la redistribución estándar OSPF-BGP.
- La continuidad OSPF debe proveerse a través de la troncal VPN MPLS, como se indica a continuación:

Las rutas internas OSPF deben mantenerse como rutas internas OSPF.

Las rutas externas OSPF deben mantenerse como rutas externas OSPF.

Las rutas que no sean OSPF y se redistribuyan en OSPF deben aparecer como rutas externas OSPF en OSPF.

Las métricas OSPF y tipos de métricas (externa 1 o externa 2) deben ser preservadas.

- La troncal L3VPN OSPF debe ser transparente a los routers CE que corren el protocolo OSPF estándar.

La troncal L3VPN VPN MPLS aparece como otra capa de jerarquía en la arquitectura OSPF. Los routers PE que conectan áreas regulares OSPF a la troncal L3VPN aparecen como ABRs en las áreas OSPF a los cuales están ligados (Fig. 1.14).

Figura 1.14. Troncal L3VPN entre routers ABR

Desde la perspectiva de un router CE OSPF estándar, los routers PE insertan rutas inter-áreas desde otras áreas al área en la cual el router CE está presente. Los routers CE no conocen la existencia de la troncal L3VPN o de otras áreas presentes más allá de la troncal L3VPN VPN MPLS, pero sí reconocen las áreas de los otros extremos que están más allá de la L3.

En la figura 1.15, se presenta como se preserva la continuidad de enrutamiento OSPF con la arquitectura de troncal L3VPN OSPF:

- La ruta intra-área OSPF descrita en el LSA (Link-stateadvertisement) de OSPF, se inserta al interior de la troncal L3VPN OSPF que la redistribuye a través de MP-BGP. La sumarización de rutas puede ser realizada en la frontera de redistribución por el router PE.
- La ruta que viaja a través de MP-BGP es propagada a otros routers PE e insertada como una ruta OSPF en otras áreas OSPF. Debido a que la troncal L3VPN aparece como otra área detrás del router PE (actuando como ABR), la ruta MP-BGP derivada de la ruta intra-área siempre se inserta como una ruta inter-área. Después la ruta inter-área puede ser propagada en otras áreas OSPF por ABRs dentro de los sitios del cliente.

Figura 1.15. Continuidad de enrutamiento OSPF con la arquitectura de troncal L3VPN OSPF

Reglas de una Troncal L3VPN OSPF.

A continuación se presenta un resumen de las reglas de la troncal L3VPN OSPF:

- Los routers PE se publican ellos mismos como ABRs. La troncal L3VPN aparece como otra área a los routers CE.
- Las rutas redistribuidas desde BGP a OSPF aparecerán como rutas inter-área sumariadas o como rutas externas en otras áreas dependiendo el tipo de LSA.

Como consecuencia de la segunda regla, las rutas del área troncal de un sitio aparecen como rutas inter-área (no como rutas troncales) en las áreas troncales de otros sitios.

Para configurar OSPF como protocolo de enrutamiento PE-CE se debe realizar lo siguiente:

- Configurar una copia de OSPF por tabla virtual.
- Configurar la redistribución de MP-BGP en OSPF.
- Configurar la redistribución de OSPF en MP-BGP.

Prevención de Bucles.

Los desarrolladores de OSPF toman muchas precauciones para evitar bucles de enrutamiento entre áreas OSPF, por ejemplo, rutas intra-áreas siempre se prefieren sobre rutas internas. Estas reglas no funcionan al momento de introducir las troncales L3VPN. Por ejemplo un área OSPF que tenga dos routers PE ligados recibe dos veces la misma información (Fig. 1.16).

Esto quiere decir que una ruta enviada desde un router PE a un router CE, también puede ser recibida por otro PE desde uno de los CE y la vuelva a redistribuir a la troncal ocasionando posibles bucles de enrutamiento.

Figura 1.16. Bucles de enrutamiento en un dominio OSPF

Para prevenir la presencia bucles por la redistribución de rutas entre OSPF (ejecutándose entre routers PE-CE) y MP-BGP (corriendo entre routers PE), se introdujeron los siguientes dos mecanismos:

- Down bit (DN bit) en el campo de opción de la cabecera del OSPF LSA.
- Sitio de origen o Site of Origin (SOO) de BGP, que será visto más adelante.

Prevención de Bucles: Down Bit (DN bit).

El DN bit debe ser introducido en la cabecera de un LSA tipo 3. Los routers PE configuran este bit cuando redistribuyen las rutas desde MP-BGP a OSPF (Fig. 1.17). Así se garantiza que un router CE envía un LSA tipo 3 a un router PE, este último no redistribuirá más la ruta.

Sin embargo, los PEs nunca redistribuyen rutas OSPF con el DN bit configurado en MP-BGP.

El bit DN se utiliza entre los routers PE para indicar qué rutas fueron insertadas en la base de datos de la topología de OSPF desde la troncal L3VPN VPN MPLS y lograr así que no sean redistribuidas nuevamente en la troncal L3VPN. El router PE que redistribuye la ruta MP-BGP como ruta OSPF en la base de datos de topología OSPF también configura el bit DN. Los routers PE restantes utilizan el bit DN para evitar que esta ruta sea redistribuida de nuevo en MP-BGP.

Figura 1.17. Ruta distribuida con el DN bit

Campo de Etiqueta OSPF.

El DN bit detiene los bucles de enrutamiento entre MP-BGP y OSPF, pero no puede detener los bucles de enrutamiento cuando se involucran múltiples dominios OSPF.

Los bucles de enrutamiento introducidos por la redistribución de rutas entre dominios OSPF se pueden solucionar con la ayuda del campo etiqueta, utilizando las reglas de redistribución estándar OSPF-BGP. Este campo en rutas externas OSPF sirve para detectar bucles de enrutamiento que atraviesen varios dominios.

En la redistribución estándar OSPF-BGP u OSPF-OSPF, se aplican las siguientes reglas:

- Siempre que un router redistribuya una ruta BGP en OSPF, el campo de etiqueta en el tipo 5 (o tipo 7, este tipo solo está presente en CISCO) en el LSA es configurado con el ASN del router distribuidor.
- El campo de etiqueta de una ruta externa OSPF se propaga a través de los dominios OSPF cuando esta ruta se redistribuye en otro dominio OSPF.
- Además de estos mecanismos estándar, los routers PE filtran rutas OSPF externas basadas en su campo de etiqueta y no se redistribuyen en MP-BGP aquellas que tengan un campo de etiqueta igual al ASN. Dicho de otra forma, los routers PE filtran las rutas OSPF externas a MP-BGP con un campo de etiqueta OSPF con un valor igual al ASN (De forma similar al mecanismo usado por BGP con el AS-Path).

Optimización en el Envío de Paquetes a través de la Troncal VPN MPLS.

La implementación de la troncal L3VPN MPLS con MP-BGP tiene otras implicaciones más allá de los potenciales bucles de enrutamiento entre OSPF y BGP.

Al trabajar con la troncal L3VPN, es posible que los sitios de un cliente actúen como un sitio de tránsito (Figs. 1.18-1.20) como se describe a continuación:

- El área 1 distribuye una ruta a la troncal BGP para que a través de MP-BGP le llegue la actualización a los routers PE B y C.

Figura 1.18. Sitios de cliente como sitios de tránsito

- EL router B está conectado al área 2, así que este redistribuye la ruta al interior del área.
- El router C, está conectado al área 2 y al área 3. Cuando el router C reciba la ruta (si tiene configurado el DN bit no la propagará de nuevo en el área 2) este recibirá dos actualizaciones de la misma ruta, una a través de la sesión MP-IBGP y otra de la sesión OSPF.

Figura 1.19. Sitios de cliente como sitios de tránsito 2

- OSPF tiene una distancia administrativa de 110 mientras que las rutas de MP-IBGP son de 200, por lo tanto la ruta aprendida a través de OSPF será la que ingrese a la tabla de enrutamiento y siempre será preferida sobre MP-IBGP, lo que causa que el área 2 se convierta en un sitio de tránsito para que las rutas lleguen al área 3.

Figura 1.20. Sitios de cliente como sitios de tránsito 3

Para evitar que los sitios de los clientes actúen como partes de tránsito de la red VPN MPLS y los paquetes tengan un flujo deseado (Fig. 1.21), las reglas de selección de ruta OSPF en routers PE necesitan ser cambiadas. Los routers PE tienen que ignorar todas las rutas OSPF (para propósitos de enrutamiento) con el DN bit configurado, porque estas rutas se originaron en la troncal MP-BGP (desde otros sitios) por consiguiente, la ruta MP-BGP debe ser usada como la ruta óptima hacia el destino.

Figura 1.21. Flujo indeseado VS flujo deseado

Para implementar esta regla se utiliza el bit de enrutamiento (routing bit) en el LSA de OSPF. Para las rutas configuradas con el DN bit, el bit de enrutamiento se borra y estas rutas nunca entran en la tabla de enrutamiento IP, incluso si son seleccionados como las mejores rutas por el algoritmo SPF (Shortest Path First). Sólo entrarán aquellas que tengan el routing bit.

Por consiguiente los paquetes de datos fluirán a través de la troncal VPN MPLS, siguiendo solamente las rutas MP-BGP más no las rutas OSPF derivadas de las rutas MP-BGP.

Enlace Simulado (Sham Link).

Aunque las conexiones PE-CE asumen que el único camino entre dos sitios cliente es a través de la troncal VPN MPLS, pueden existir puertas traseras (backdoors) entre sitios VPN.

En la gráfica 1.22 hay dos sitios en la misma área OSPF. Cada sitio está ligado a un router PE diferente, pero también existe un enlace OSPF alternativo (backdoor link) intra-área conectando estos dos sitios.

Es posible tratar estos dos sitios como una única VPN que tiene una conexión multihomed con la troncal. Esto se puede realizar y es adecuado, dado que si existen varios sitios que pertenecen a la misma área OSPF, el camino sobre el enlace alternativo (backdoor) siempre será seleccionado porque OSPF prefiere caminos intra-área que inter-área. Los routers PE propagan rutas OSPF aprendidas de la troncal VPN como caminos inter-área. Por esta razón, los enlaces backdoor entre sitios VPN deben ser tenidos en cuenta para que el enrutamiento se desarrolle de acuerdo a la política definida.

Figura 1. 22. Puerta trasera entre dos sitios VPN

Si los enlaces backdoor entre sitios son utilizados solamente como enlaces de respaldo y no participan en el servicio VPN, esta ruta no debe seleccionarse como la mejor. Para que el camino deseado sea nuevamente a través de la troncal, se debe crear un enlace (lógico)

OSPF adicional intra-área entre tablas virtuales de ingreso y salida en los routers PE correspondientes. Este enlace es llamado *enlace simulado* (o sham link) y es transportado por la troncal L3VPN (Fig. 1.23).

Este enlace se requiere entre cualquier par de sitios VPN que pertenezcan a la misma área OSPF y compartan un enlace alternativo (back door). Si no existe un enlace alternos entre los sitios, no será requerido un enlace simulado.

Un enlace simulado puede ser visto como una relación entre dos tablas virtuales. Si dos tablas virtuales están conectadas a través de este tipo de enlace, cada tabla virtual debe estar asociada con una dirección en el extremo final del enlace simulado. Esta dirección es una dirección IPv4 de 32 bits y debe pertenecer al espacio de direcciones de la VPN y no del SP y debe poder ser configurable.

Las direcciones asignadas a este enlace no deben ser propagadas por OSPF sino por la troncal BGP.

Figura 1.23. Enlace simulado

Un paquete del protocolo OSPF enviado sobre un enlace simulado (Sham link) de un router PE a otro, debe tener como dirección de origen la dirección del enlace simulado configurada en el router PE emisor y dirección destino la dirección del enlace simulado configurada en router PE receptor. La dirección IP del paquete será distribuida por BPG como una dirección VPN-IPv4 de un router PE a otro a través de la troncal VPN, lo que significa que este paquete puede pasar por múltiples saltos, en tal caso, el campo TTL debe configurarse apropiadamente.

Si no hay una ruta BGP hacia la dirección del extremo de la conexión del enlace simulado (sham link), esa dirección aparecerá como inalcanzable, así que este enlace se verá caído.

El intervalo de paquetes hello para un enlace simulado es de 10 segundos y el intervalo para declarar el enlace muerto es de 40 segundos.

Debido a que un enlace simulado es visto como un enlace intra-área entre routers PE, se crea una adyacencia OSPF y ocurre un intercambio de base de datos (para ese proceso OSPF) a través del enlace. El router PE ya puede inundar los sitios con LSAs (tipo 1 ya que solo está involucrada un área) atravesando la troncal. Como resultado se crea la conectividad intra-área deseada.

Razones para Limitar el Número de Rutas en una Tabla Virtual.

La arquitectura VPN MPLS logra un acoplamiento robusto entre el cliente y el SP, dando como resultado una serie de ventajas. Este acoplamiento robusto también podría tener algunas desventajas debido a que el SP está expuesto a los errores de diseño y configuración en las redes de los clientes, y a ataques de denegación de servicio basados en el comportamiento del protocolo de enrutamiento debido a que cualquier cliente puede generar cualquier número de rutas usando los recursos en los routers PE.

El administrador de la red puede limitar el número de rutas en una tabla virtual (independientemente si viene de routers CE o PE), al igual que lo hace con el número máximo de prefijos en BGP. También se puede configurar un mensaje de sistema para que advierta al administrador cuando el número de rutas exceda un umbral.

Estos mensajes del sistema pueden ser configurados para que aparezcan en ciertos intervalos de tiempo, esto con el objetivo de evitar una denegación de servicio indirectamente a la estación de trabajo del administrador.

Esta forma de limitar las rutas en una tabla virtual puede ser utilizada como complemento a los servicios de VPN MPLS. Si un usuario desea un nivel de servicio superior, debería estar dispuesto a pagar más para agregar más rutas VPN en la red.

BGP como Protocolo de Enrutamiento Entre Routers PE-CE.

Inconvenientes del Reemplazo del SA (AS-OverrideIssues).

La regla de prevención de bucles BGP no permite que dos Sistemas autónomos con ASNs iguales estén conectados a través de otro SA (Fig. 1.24). Si se presenta una configuración de este tipo, las actualizaciones de enrutamiento de un sitio A serán desechadas por el otro sitio B ya que el AS-Path indicará el mismo ASN y por lo tanto no habrá conectividad entre sitios.

Figura 1.24. Funcionamiento tradicional de prevención de bucles

Cuando se están migrando los clientes de una red tradicional overlay VPN a una arquitectura VPN MPLS, no es extraño encontrarse con la topología de un cliente que posee el mismo ASN empleado en otros sitios. Este requerimiento puede causar algunos inconvenientes en cuanto a bucles de enrutamiento en BGP, como se indicó anteriormente. Sin embargo, el procedimiento de actualización del AS-Path en BGP, llamado reemplazo del SA (AS-Override), ha sido modificado para abordar este problema.

El nuevo procedimiento de actualización del AS-Path soporta el uso de un mismo ASN en muchos sitios (incluso entre varias VPN solapadas) y no requiere una distinción entre ASNs públicos y privados⁸⁵.

Cuando se utiliza el reemplazo del SA (AS-Override) en los routers PE, este actúa de la siguiente manera¹⁴:

- El procedimiento solo se utiliza si el primer ASN en el AS-Path es igual al ASN del router receptor. En este caso el ASN del emisor se reemplaza con el ASN del SP (Fig. 1.25).

Figura 1.25. Funcionamiento del reemplazo del SA (AS-Override) [1]

85 Understanding AS Override, Juniper.

- Si el primer ASN tiene múltiples ocurrencias (debido al as pathprepending), estas son reemplazadas con el ASN del SP (Fig. 1.26).

Figura 1.26. Funcionamiento del reemplazo del SA (AS-Override) [2]

- Las ocurrencias del ASN que estén presentes más adelante en el AS-Path no serán reemplazadas porque estas sí indican un bucle de enrutamiento real (Fig. 1.27).

Figura 1.27. Funcionamiento AS-Override (3)

- Una copia extra del ASN del SP es agregada al AS-Path. El procedimiento estándar para agregación de ASNs se realiza en cada actualización EBGp.

Identificando Inconvenientes de Allow as-in.

En algunas implementaciones de seguridad, las VPNs de un cliente están enlazadas por un (router cliente que realiza tareas de seguridad tales como filtrado de acceso o registro de accesos. Esta configuración no es usual porque se desvía de la funcionalidad de VPN MPLS.

La configuración en la cual un router cliente enlaza dos VPNs en una troncal VPN MPLS puede ser vista desde varias perspectivas como se menciona a continuación:

- Desde la perspectiva VPN, es un router CE que enlaza dos VPNs (Fig. 1.28).

Figura 1.28. Perspectiva VPN de un router CE enlazando dos VPNs

- Desde la perspectiva física, el router CE está conectado a través de dos enlaces separados (interfaz física o lógica) a dos routers PE (Fig. 1.29).

Figura 1.29. Perspectiva física de un router CE enlazando dos VPNs

- En términos de VPN MPLS, el router CE tiene dos enlaces en la P-network (Fig. 1.30).

Figura 1.30. Perspectiva de VPN MPLS de un router CE enlazando dos VPNs

No hay ningún problema con la configuración propuesta por el cliente si la configuración se analiza desde algunas de las perspectivas mencionadas anteriormente ya que todas las configuraciones representan conexiones válidas y opciones de enrutamiento factibles. El problema surge cuando esta configuración se analiza desde el punto de vista de BPG, en la cual, el router CE debe propagar las rutas entre los dos routers PE que pertenecen al mismo SA (Desde la perspectiva de BGP el router CE tiene dos conexiones al mismo SA), y por consiguiente ocurrirán problemas con el AS-Path. Este problema puede solucionarse con una actualización de software en el caso de Cisco.

Implementación de allow as-in.

La regla de prevención de bucles BGP evita que un router PE acepte actualizaciones de enrutamiento enviadas por un router CE si esa actualización ya contiene el ASN de la troncal VPN MPLS (lo cual sucederá si el router CE está propagando rutas entre dos VPNs) (Fig. 1.31).

La solución a este problema de enrutamiento BGP es implementar AS-override en el router CE. Esta solución no es aplicable en todas las situaciones de los clientes.

Las redes necesitan soportar topologías en las cuales un router CE sin AS-override soporte enlaces entre dos VPNs. Por lo tanto existe una necesidad específica de modificar el mecanismo de prevención de bucles BGP en los routers PE. La característica “allow-as-in” soporta situaciones en las cuales un router PE recibe rutas con su propio ASN en el AS-path.

Figura 1.31. Regla de prevención de bucles

Con esta característica configurada en un vecino BGP del router PE, evita que el router PE deseche las actualizaciones entrantes que tengan su ASN en el AS-Path, si esta proviene de su vecino. Para prevenir bucles de enrutamiento reales, el número de ocurrencias del ASN de la troncal VPN MPLS puede limitarse y las actualizaciones entrantes que superen este límite pueden desecharse (Fig. 1.32).

Figura 1.32. Característica Allowas-in

Así se tiene que as-override se implementa en routers CE y allow as-in en routers PE⁸⁶.

Utilizando el Atributo SOO para Prevención de Bucles.

Muchos de los aspectos de la prevención de bucles de BGP son ignorados cuando se está implementando alguna de las características AS-override o allowas-in. No obstante, los bucles de enrutamiento todavía pueden ser detectados manualmente contando el número de ocurrencias de un ASN en el AS-Path en un escenario de enrutamiento BGP end-to-end asegurándose que el campo allowas-in en el vecino es lo suficientemente bajo para prevenir bucles.

Esta capacidad de detectar bucles puede presentar un problema particular cuando BGP es combinado con otros protocolos de enrutamiento PE-CE. La comunidad extendida BGP, SOO, puede ser utilizada como un mecanismo adicional de prevención de bucles en estos escenarios.

86 neighbor allowas-in | WAN, Routing and Switching, Cisco forum.

La función de este atributo únicamente tiene el propósito de identificar el conjunto de rutas aprendidas desde un sitio particular. Este atributo es necesario en algunos casos para asegurarse que una ruta aprendida desde un sitio a través de una conexión PE-CE, no sea distribuida de nuevo al sitio a través de otro enlace PE-CE⁸⁷.

El SOO y otros mecanismos de prevención de bucles solo se necesitan para redes clientes con sitios multihomed. Los bucles pueden ocurrir inclusive en redes clientes que tienen solamente sitios stub.

A continuación se presentan dos maneras de configurar el atributo SOO sobre una ruta BGP.

- Cuando un router PE recibe una ruta desde un router CE BGP, este remueve el ASN (Fig. 1.33-1.34) y configura el atributo SOO que es único por sitio para evitar conflictos con ASNs repetidos (Fig. 1.35). Esta asignación se realiza a través de un route-map de entrada.

Figura 1.33. Esquema general del atributo SoO

Figura 1.34. Remoción del ANS en router PE a través de un route-map

87 RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs).

Figura 1.35. Funcionamiento del atributo SoO

De esta manera, si se tiene configurado el horizonte dividido, la ruta aprendida no volverá a distribuirse por la interfaz que se aprendió, sin embargo como se observa en la figura 1.35, existe otro router PE, este al ver que el sitio de origen (SOO) es de una red que está conectada directamente, tampoco la volverá a distribuir.

- Para las demás rutas, a través de un route-map en la interfaz de entrada específica se configura el atributo SOO. Este atributo configurado por el route-map, se liga a la ruta BGP cuando una ruta IGP recibida a través de esa interfaz es redistribuida en BGP.

Los filtros de salida basados en el SOO también dependen del protocolo de enrutamiento usado, como se describe aquí:

- Si se utiliza EBGp como protocolo de enrutamiento PE-CE, se puede utilizar los route-maps de salida en un router PE para denegar rutas que coincidan con unos valores particulares del SOO (Fig. 35).
- Para los demás protocolos de enrutamiento, el SOO puede ser aplicado a las rutas aprendidas a través de una interfaz en particular durante la redistribución en BGP. El filtrado se desarrolla basado en el SOO configurado en el route-map, en la interfaz de salida, antes de que la actualización se envíe hacia el router CE.

La diferencia entre estas dos formas de configuración radica en que en la primera el route-map se asigna directamente sobre las rutas aprendidas desde un router CE y en la otra se aplica sobre una tabla virtual a las rutas que se han aprendido desde el IGP a una interfaz específica (para las rutas que se van a redistribuir).

Resolución de Problemas en VPN MPLS.

La resolución de problemas en VPN MPLS consiste principalmente en estos dos pasos:

- Verificar el flujo de la información de enrutamiento (etiquetas para rutas IGP, MTU).
- Verificar el flujo de datos o envío de paquetes.

Verificación del Flujo de Información

A continuación se presenta un listado de ítems a tener en cuenta cuando se verifique el flujo de información:

Los routers PE deben recibir correctamente las rutas CE.

- La resolución de problemas del flujo de la información de enrutamiento requiere la verificación de la información propagada entre routers CE. El primer paso es revisar la información de enrutamiento intercambiada desde los routers CE hasta los routers PE. Los routers PE deben estar recibiendo rutas del cliente a través de CE.

La redistribución de rutas en MP-BGP se debe propagar con las comunidades extendidas apropiadas.

- Las rutas recibidas por el router PE necesitan ser redistribuidas en el MP-BGP. De otra forma estas no serán propagadas a otros routers PE. Algunos errores de configuración comunes en este paso son los siguientes:
 - Fallar en la configuración de la redistribución entre protocolos de enrutamiento PE-CE y la tabla virtual.
 - Usar un route-map al momento de realizar la redistribución que filtre rutas CE.

Los filtros automáticos de rutas están basados en RTs. Se debe verificar que los RTs ligados a la ruta CE en el router PE coincidan con al menos uno de los RTs que han sido configurados como RTs importados en la tabla virtual del router PE receptor.

Funcionamiento correcto del proceso de selección de ruta BGP.

- En entornos más complejos con sitios de clientes multihomed, el proceso de selección de ruta BGP podría afectar la apropiada operación de VPN MPLS. Se deben usar los parámetros del proceso de selección de ruta BGP estándar (peso, preferencia local,...). El atributo MED no debería ser cambiado en la troncal VPN MPLS si se planea utilizar la redistribución de rutas desde el IGP del router PE hacia BGP.

Adición correcta de rutas VPNv4 en las tablas virtuales de los routers PE.

- Las rutas VPNv4 recibidas por el router PE tienen que ser insertadas en la tabla virtual apropiada.
- Un error común en la configuración de este paso es configurar RTs equivocados en la tabla virtual.
- Se debe ser paciente cuando se estén solucionando los problemas en este caso ya que la importación de rutas en la tabla virtual no es inmediata y puede tardar más de un minuto en el peor de los casos.

Redistribución de rutas VPNv4 desde BGP en el protocolo de enrutamiento PE-CE.

- Las rutas recibidas a través de MP-BGP y que se insertan en la tabla virtual necesitan ser redistribuidas en el protocolo PE-CE.

Correcta propagación de rutas VPNv4 a otros routers CE.

- Este último paso pero no el menos importante, indica que las rutas redistribuidas en el protocolo PE-CE deben ser propagadas a los routers CE. Se puede una ruta por defecto desde un router CE hacia un router PE.

Verificación del Flujo de Datos.

Revisar que el contenido de la tabla LFIB este configurado correctamente en el router PE de salida.

MÓDULO 2

MPLS VPNs Complejas.

Uso de las características avanzadas de importar y exportar en las tablas virtuales.

Algunas características de las tablas virtuales de enrutamiento permiten ser más selectivas con las rutas, especificando cuales de ellas serán añadidas y cuáles no. También se debe limitar el número de rutas que un cliente puede instanciar en una tabla virtual.

Características avanzadas de la tabla virtual.

Las características avanzadas de importar y exportar permiten desplegar topologías MPLS VPN más avanzadas y complejas, o también sirven para incrementar la estabilidad de la troncal MPLS VPN.

- Importación selectiva: Cada VPN puede tener una política que sirva para determinar qué criterios adicionales pueden implementarse para importar otras rutas a las tablas virtuales de los PEs aparte de los RTs de la tabla virtual.
- Exportación selectiva: Permite ligar RTs específicos a un subconjunto de rutas exportadas de una tabla virtual. Por defecto, los mismo RTs se adjuntan a todas las rutas exportadas.
- Una política de exportación debe evaluar todas las rutas recibidas sobre la sesión del protocolo de enrutamiento utilizado con el CE1.
- Límite de rutas: El límite de rutas en la tabla virtual permite limitar el número de rutas

que el cliente u otros routers PE pueden insertar en la tabla virtual. Esta característica previene consecuencias indeseables tales como errores de configuración, consumo exhaustivo de memoria o ataques de denegación de servicios.

Importación Selectiva de la Tabla Virtual.

La importación selectiva de rutas en una tabla virtual permite limitar aún más los criterios de importación de rutas, utilizando un route-map configurado de tal manera que pueda filtrar las rutas seleccionadas por el filtro de RTs importados (RT importfilter). Las rutas importadas en una tabla virtual son rutas BGP, así que se pueden usar condiciones de coincidencia en un route-map para que coincida con cualquier atributo BGP de una ruta. Estos atributos incluyen comunidades, preferencia local, MED, AS-Path, etc.

Figura 2.1. Funcionamiento de la importación selectiva

Cuando el route-map que es usado para filtrar las rutas importadas (importroute-mapfilter) se combina con el filtro utilizado para los RT importados (RT importfilter), una ruta debe pasar primero por el filtro de RT importados y luego el route-map para las rutas importadas (Fig. 2.1). Las condiciones necesarias que debe cumplir una ruta para ser importada en una tabla virtual son las siguientes:

- Al menos uno de los RTs adjuntos a la ruta debe coincidir con uno de los RTs configurados en la tabla virtual.
- La ruta debe ser permitida por el route-map.

Como se puede ver en la gráfica 1, las rutas VPN-IPv4 traen configurados unos atributos, pero solo aquellas que satisfagan las condiciones de ambos filtros podrán importarse a la tabla virtual, en este caso es solo la ruta que llega la interfaz 3, las otras dos no coinciden o en el AS_Path o el RT.

Se puede incrementar la seguridad de una extranet VPN permitiendo solamente subredes predefinidas para ser insertadas en la tabla virtual, y de esta manera se previene que se inserten subredes no aprobadas.

Exportación Selectiva de la Tabla Virtual.

Algunas topologías MPLS VPN avanzadas son fáciles de implementar si se pueden ligar varios RTs a las rutas exportadas desde la misma tabla virtual. Esta capacidad permite que un subconjunto de rutas exportadas de una tabla virtual sea importado a otras. La mayoría de los servicios en que los clientes necesitan conectarse a un servidor común (voicegateways, aplicaciones del servidor) caen en esta categoría.

La función del route-map para exportar rutas provee exactamente esta misma funcionalidad. Un route-map puede ser especificado para cada tabla virtual y de esta manera adjuntarle RTs adicionales a rutas exportadas de esta tabla virtual (Fig. 2.2). El route-map para exportar rutas (Exportroute-map) solamente liga los RTs. No hace tareas de filtrado.

Los atributos ligados a una ruta que tiene configurado un route-map para rutas exportadas (Exportroute-map), se combinan con los atributos RT exportados. Si se especifican los RTs exportados en una tabla virtual y se configuran con un route-map para exportar rutas, todos los RTs se ligarán a la ruta exportada.

Figura 2.2. Funcionamiento de la exportación selectiva

El route-map para exportar rutas (Exportroute-map) provee una funcionalidad casi idéntica a la ofrecida por un route-map empleado para importar rutas (Importroute-map), pero aplicada a una tabla virtual diferente. Cualquier requerimiento que pueda ser implementado con un route-map para exportar rutas, también puede ser implementado con un route-map para importar rutas. Sin embargo, la implementación de los route-map para exportación puede ser más complicada y más difícil de administrar.

VPNs Traslapadas.

Si dos VPNs no tienen sitios en común, entonces éstas pueden utilizar un espacio de direcciones traslapado puesto que este espacio utilizado en una VPN1 tendrá un significado completamente diferente al usado en una VPN2 (Fig. 2.3). Esta es una situación común

cuando las VPNs utilizan un espacio de direcciones privado⁸⁹. Aunque al interior de cada VPN cada dirección si debe ser única e irrepetible.

Ambas VPNs poseen el mismo direccionamiento privado pero no hay ningún inconveniente puesto que cada una es independiente de la otra

Figura 2.3. VPNs con espacio de direcciones traslapado

MPLS puede soportar VPNs traslapadas a través del concepto de los RTs. Una VPN traslapada se presenta cuando al menos un sitio CE necesita ser alcanzable por CEs en diferentes VPNs.

Existen muchas variaciones de VPNs traslapadas. Un SP puede proveer servicios a muchos clientes, entonces el SP implementa sitios CE que necesitan ser alcanzados por un subconjunto de clientes. Algunos clientes de un SP pueden requerir conectividad hacia uno de sus compañeros a través de la red MPLS.⁹⁰

Las VPNs traslapadas se emplean usualmente para conectar partes de dos VPNs separadas (Fig. 2.4). Estas VPNs solo conectan con los sitios centrales de cada VPN. Un nuevo atributo RT de comunidad extendida se utiliza para identificar las redes que están siendo originadas en los sitios a los cuales también pertenece la VPN traslapada. Esta acción puede requerir una nueva tabla virtual, dando como resultado un nuevo RD (Identificador de ruta). Las redes originadas en estos sitios se exportan con dos RTs que pertenecen a las comunidades extendidas: Un RT se configura para la VPN original y el otro RT para la VPN traslapada.

89 RFC 4364: BGP/MPLS IP Virtual Private Networks (VPNs)

90 CCIE Routing and Switching Certification Guide – p.850.

Figura 2.4. Uso de las VPNs traslapadas

Participantes de una VPN Traslapada.

Cuando dos clientes VPN quieren compartir alguna información, pueden decidir interconectar sus sitios centrales. Para lograr esto, se crean dos VPNs, cada una conteniendo el sitio central de un cliente y sus sitios remotos. Posteriormente, se crea una tercer VPN que traslapa parcialmente con las VPNs de los clientes pero que conecta solamente con sus sitios centrales. Los sitios centrales pueden comunicarse entre sí y con sus respectivos sitios remotos. Las direcciones usadas en los sitios centrales, deben ser únicas en ambas VPNs.

Otra opción a utilizar es un doble Network Address Translation (NAT) con unas direcciones registradas para ser importadas y exportadas entre los dos sitios centrales⁹¹.

Cuando se diseña el direccionamiento se debe prestar atención ya que si un sitio que está participando en más de una VPN está propagando una ruta por defecto hacia los demás sitios, este puede atraer tráfico de esos sitios y actuar como un sistema de tránsito entre VPNs, dándole posibilidad de comunicación a otros sitios que no deberían.

Uso de una VPN Traslapada.

Los dos usos más típicos para este tipo de VPNs son los siguientes:

- Las compañías que usan MPLS VPN para implementar los servicios de intranet y extranet podrían utilizar VPNs traslapadas. En este escenario cada compañía participando en la extranet VPN probablemente desplegará un mecanismo de seguridad en sus routers CE para prevenir que otras compañías participando en la VPN tengan acceso a otros sitios en la VPN del cliente.
- Una compañía consciente de la seguridad, podría decidir limitar la visibilidad entre los diferentes departamentos de la organización. Las VPNs traslapadas pueden ser la solución en este caso.

91 Using VPN Translation With Overlapping Subnets, Cisco.

Los inconvenientes de seguridad podrían forzar a una empresa a migrar a una red MPLS VPN inclusive si esta no está utilizando los servicios MPLS VPN de un SP.

Los sitios de las VPNs traslapadas están configurados con una tabla virtual del mismo RD por conjunto de sitios con la misma membresía VPN. Los RTs están configurados basados en la membresía VPN de cada sitio respectivamente.

Central de Servicios VPN.

Una central de servicios VPN se usa cuando más de una red virtual privada necesita compartir un conjunto común de servicios. Estos servicios residen en la central de servicios VPN, a la cual se conectan las demás VPNs que necesitan los recursos. Por otra parte, las VPNs que están conectadas a la central de servicios, no pueden verse entre sí⁹². La central de servicios VPN se implementa utilizando dos comunidades extendidas RT, donde uno importa rutas a la VPN y el otro las exporta. Los sitios clientes hacen lo opuesto. Se necesitan dos comunidades extendidas RT para prevenir a los sitios clientes de intercambiar información de enrutamiento.

Características de Acceso de una Central de Servicios VPN.

Una central de servicios VPN (Fig. 2.5) es una topología con las siguientes características:

- Algunos sitios (“server sites”) se pueden comunicar con otros sitios.
- Los demás sitios (“clientsites”) se pueden comunicar solamente con los server sites.

Figura 2.5. Central de servicios VPN

Esta topología, como se ve en la figura 2.6, puede ser utilizada en las siguientes situaciones:

92 Multiprotocol Label Switching, Wendell Odom.

- ElSP ofrece servicios a todos los clientes permitiéndoles acceder a una VPN común (Server sites.).
- Dos o más compañías quieren intercambiar información compartiendo un conjunto común de servidores.
- Una compañía consciente de la seguridad, separa sus departamentos y les permite acceder a servidores comunes.

Figura 2.6. Uso de la central de servicios VPN

Características de Enrutamiento de una Central de Servicios VPN.

Hay un modelo de enrutamiento específico usado para implementar una central de servicios VPN.

- Las rutas de los clientes necesitan ser exportadas al server site.
- Las rutas del servidor necesitan ser exportados al cliente y a los server sites.
- Ninguna ruta se intercambia entre sitios cliente.

Modelo del Flujo de Datos en la Central de Servicios VPN.

En la topología de la central de servicios VPN, la tabla virtual del cliente contiene solamente rutas del sitio del cliente y rutas de los sitios del servidor. Esta configuración evita que los sitios cliente se comuniquen con otros sitios clientes.

La tabla virtual de un servidor en esta topología contiene rutas del sitio o sitios ligados a la tabla virtual, y también rutas de otros sitios clientes y servidores. Los hosts en sitios servidores pueden por lo tanto comunicarse con hosts en otros sitios.

Si el sitio central está propagando una ruta por defecto a otros sitios, puede resultar en sitios clientes viendo a cada uno a través del router CE en el sitio central.

En resumen:

- Las tablas virtuales del cliente contiene rutas del servidor. Por consiguiente los clientes pueden comunicarse con los servidores.
- Las tablas virtuales del servidor contienen rutas del cliente y otros servidores. Por consiguiente, los servidores puede comunicarse con los clientes y otros servidores.
- Las tablas virtuales de los clientes no contiene rutas de otros clientes. Por consiguiente los clientes no se pueden comunicar con otros clientes.
- El administrador de la red se debe asegurar que no haya una fuga cliente-a-cliente a través de los sitios servidores.

Requerimientos de Configuración de una Central de Servicios VPN.

Para configurar una central de servicios VPN se deben completar los siguientes requerimientos:

- Una tabla virtual separada por cada cliente.
- Una tabla virtual por cada router PE conectado a un server site.
- Un único RD en cada sitio cliente.
- Un único RD en cada conjunto de server sites.
- Un RT importado-exportado con el mismo valor del RD, para cada sitio cliente.

Gestión del Servicio en Routers CE.

Un proveedor de servicios puede implementar la gestión de la red VPN (network management VPN) para administrar la red VPN y para gestionar los routers CE de todas las VPNs. Un par de comunidades extendidas RT se usan para lograr este objetivo. Un RT exporta las direcciones de loopback del router CE y las importa en la tabla virtual de la gestión de la red VPN. El otro RT exporta las redes desde la tabla virtual asociada con los servicios operativos de la red VPN y los importa en todas las tablas virtuales.

Requisitos de los Routers Gestionados.

Si el ISP está gestionando los routers del cliente (Fig. 2.7), es conveniente tener un punto central que tenga acceso a todos los routers CE pero este no debe tener acceso a los otros destinos en los sitios clientes. Este requerimiento se implementa usualmente desplegando una VPN separada para propósitos de gestión de la red. Esta VPN necesita ver todas las interfaces de loopback de todos los routers CE.

Todos los routers CE tienen que ver la VPN que gestiona la red. El diseño es similar al de la central de servicios VPN. La única diferencia es que se deben marcar únicamente las interfaces de loopback para que sean importadas en la VPN de gestión.

Figura 2.7. Gestión de routers CE desde un punto centralizado

Requerimientos de la Tabla Virtual y del Identificador de Ruta (RD).

El diseño de la tabla virtual y del RD es el mismo que el de la central de servicios VPN. La única diferencia entre esta topología y la topología de la central de servicios VPN combinada con una topología VPN sencilla es el proceso de marcado RT durante la exportación de rutas.

En general se debe realizar lo siguiente:

- Crear una tabla virtual de enrutamiento por cada cliente VPN por cada router PE.
- Asignar el mismo RD para cada uno de los clientes de la table virtual de enrutamiento.
- Crear un NMS (Network Management System) en el router PE-CS (Central de servicios).
- Asignar un único RD a la tabla de enrutamiento del NMS.

La configuración en los routes CE gestionados es la siguiente:

- Configurar el RT importado-exportado por cliente en todas las tablas virtuales de los clientes.
- Configurar el RT importado-exportado en la tabla virtual del NMS.
- Importar rutas con el RT NMS en la tabla virtual del cliente.
- Exportar las direcciones de loopback desde la tabla virtual del cliente RT para NMS.
- Importar rutas de cliente RT para NMS en la tabla virtual del NMS.

MÓDULO 3

Acceso a Internet Desde una Red MPLS VPN.

Integrar los servicios de internet con una red MPLS VPN es uno de los requerimientos de negocio más comunes de un Proveedor de servicios (Service Provider (SP)).

Topologías VPN de Acceso a Internet.

Acceso Clásico a Internet para un Cliente VPN.

El acceso clásico a internet es implementado a través de un firewall que conecta la red del cliente a internet de modo seguro⁹³. La red privada del cliente (o VPN si el cliente está utilizando un servicio VPN) y el internet están conectados solamente a través del firewall (Fig. 3.1).

- El cliente VPN se conecta a internet a través de un sitio central (o sitios centrales).
- Un firewall entre el cliente VPN y el internet es desplegado solamente en el sitio central.

93 Iris Biometric Model for Secured Network Access – p.10.

Figura 3.1. Acceso clásico a internet a través de un firewall

Requerimientos de Direccionamiento en el Acceso Clásico a Internet.

Los requisitos de direccionamiento para un acceso clásico a internet (como se describen aquí), son muy simples:

- El cliente tiene asignado un pequeño bloque del espacio de direcciones públicas usadas por el firewall.
- El cliente normalmente usa un espacio de direcciones privadas al interior de su red.
- El firewall realiza una traducción de direcciones (NAT) entre las direcciones privadas del cliente y las direcciones públicas asignadas al cliente por el SP. De forma alterna, el firewall podría realizar una función proxy a nivel de aplicación que aísle las direcciones IP públicas y privadas.

Existen varios beneficios asociados con el diseño clásico de acceso a internet entre los que se encuentran los siguientes:

- Es una configuración conocida y usada en todo el mundo para conectarse a internet desde una red corporativa. Por lo tanto el nivel de conocimientos requeridos para realizar esta implementación no es avanzado.
- Solo hay un punto de interconexión entre la red segura del cliente y la internet. La seguridad del acceso a internet debe ser manejada únicamente en este punto central.

La mayor desventaja de este diseño es el flujo de tráfico, todo el tráfico de la red del cliente a internet debe pasar a través del firewall central. Mientras que esto puede que no sea un inconveniente para clientes pequeños, si puede representar serias limitaciones en las grandes organizaciones con muchos usuarios, especialmente cuando los usuarios están separados geográficamente (Fig. 3.2).

Figura 3.2. Inconvenientes de cuello de botella en el acceso a internet tradicional

Flujo del Tráfico de Internet en una Troncal MPLS VPN.

El inconveniente del flujo de tráfico se hace aún más notorio cuando el cliente VPN (basado por ejemplo en servicios MPLS VPN) y el tráfico de internet comparten la misma troncal del ISP (Fig. 3.3.1). En este caso, el tráfico desde un sitio del cliente (línea verde) debe atravesar la troncal del ISP como tráfico VPN y retornar a la misma troncal por el firewall corporativo, terminando en un servidor muy cercano al sitio original.

Figura 3.3.1. Diseño de troncal MPLS VPN y troncal de internet compartida

Figura 3.3.2. Diseño de troncal MPLS VPN y troncal de internet compartida (escenario detallado)

Basado en este análisis, los inconvenientes de diseño del firewall central pueden resumirse como se mencionan a continuación:

- El enlace entre el sitio central y la troncal del SP tiene que estar sobredimensionada, porque tiene que transportar todo el tráfico de internet del cliente.
- La troncal del ISP es sobre-utilizada, porque el mismo tráfico cruza la troncal dos veces, primero como tráfico VPN y luego como tráfico de internet (o viceversa).
- Los tiempos de respuesta y calidad del servicio pueden verse afectados. Esto se debe a que el tráfico entre el sitio de un cliente y destino en internet siempre debe cruzar el firewall central, incluso cuando el destino de internet está muy cerca al sitio del cliente.

Estos inconvenientes han llevado a redes de grandes usuarios e ISPs a considerar diseños alternos en el que cada sitio de un cliente pueda originar y recibir tráfico de internet directamente.

Métodos de Acceso a Internet Desde Cada Sitio de un Cliente.

Para superar las limitaciones de acceso a internet a través de un firewall central, algunos clientes han pasado a diseños en los que cada sitio de un cliente tiene acceso a internet propio e independiente. Mientras que este diseño soluciona los inconvenientes del flujo de tráfico, el inconveniente asociado a la seguridad se expone aún más, ya que cada sitio debe

protegerse individualmente en contra del acceso no autorizado desde internet (Fig. 3.4). Este diseño es aplicado primordialmente en grandes sitios o VPNs extranet, en la que cada sitio ya está asegurado contra los otros que participan en la VPN extranet.

- **Beneficios:**

- Flujo óptimo de datos desde y hacia internet.

- **Desventajas:**

- Cada sitio debe configurar su protección contra accesos no autorizados.
- Es más fácil establecer una configuración extranet ya que cada sitio está protegido de los demás sitios que participan de la extranet.

Figura 3.4. Acceso a internet desde cada sitio de un cliente utilizando NAT

Acceso a Internet Desde Cada Sitio de un Cliente: Direcccionamiento.

Para obtener acceso a internet desde cada sitio, estos requieren al menos algunas direcciones IP públicas.

Los siguientes dos métodos pueden ser utilizados para alcanzar esta meta:

- Un pequeño bloque del espacio de direcciones públicas pueden ser asignadas a cada sitio de un cliente. Se utiliza un NAT en cada router CE entre las direcciones privadas y las públicas en cada sitio.
- Si el cliente ya está utilizando direcciones IP públicas en la VPN, la funcionalidad del NAT no es necesaria. Desafortunadamente esta opción solo está disponible para aquellos clientes que poseen grandes bloques de direcciones IP públicas.

Acceso a Internet Desde Cada Sitio de un Cliente: Troncal MPLS VPN.

Para obtener acceso a internet desde cada sitio de un cliente, cada router CE debe enviar tráfico VPN hacia otros sitios de un cliente y enviar tráfico de internet hacia destinos de internet. Los dos tipos de tráfico se envían usualmente sobre el mismo enlace físico para minimizar costos (Fig. 3.5). La encapsulación Switched WAN (Framerelay o ATM) puede ser utilizada para separar el tráfico VPN y el tráfico de internet en diferentes circuitos virtuales, o el tráfico también puede compartir el mismo enlace lógico, reduciendo así los niveles de seguridad. Por otra parte, la debilidad de seguridad en este diseño (menos complejo) se ve compensado por un flujo de tráfico óptimo entre cada sitio y los destinos en internet.

Los dos tipos de tráfico comparten el mismo enlace, solo se hace la distinción para observar como fluye cada uno de estos.

Figura 3.5. Acceso a internet desde cada sitio cliente utilizando un enlace compartido

Servicio de Central de Firewalls (Central Firewall Service).

Para los clientes que no quieren la complejidad de gestionar su propio firewall, un servicio de gestión de firewall ofrecido por el SP es una buena alternativa. Estos clientes quieren que el SP se haga cargo de los problemas de seguridad relacionados con su conexión a internet.

El SP puede implementar un firewall dedicado (Fig. 3.6) en cada sitio de un cliente (incrementando costos) o utilizando un firewall central (Fig. 3.7) que provea acceso a internet seguro para todos los clientes.

Figura 3.6. Firewall dedicado por cliente

Figura 3.7. Firewall centralizado

Servicio de Firewall Central: Direccionamiento.

El firewall central, alojado por el SP, tiene que usar direcciones públicas para internet. Las direcciones privadas pueden ser usadas entre el firewall central y los clientes individuales. No obstante, estas direcciones necesitan ser coordinadas entre el SP y el cliente para prevenir conflictos de enrutamiento y direcciones traslapadas. Los clientes utilizando el servicio de un firewall central están limitados al direccionamiento asignado por el SP, en la misma manera en que están limitados a las direcciones públicas asignadas por el ISP (Fig. 3.7).

Los clientes que utilicen el servicio de un firewall central y que todavía deseen mantener su propio espacio de direcciones al interior de sus redes pueden utilizar NAT en sus routers CE (Fig. 3.8), conectando su red privada a la red de tránsito que enlaza sitios de un cliente al firewall central.

Los SPs usualmente utilizan direcciones IP privadas entre el firewall central y los clientes. Siempre hay un riesgo de que se traslapen las direcciones entre el espacio de direcciones coordinado entre el SP y el cliente con las rutas propias del cliente. Por lo tanto, el router CE que esté haciendo la función de NAT tiene que soportar la traducción de direcciones entre conjuntos de direcciones IP traslapadas.

Figura 3.8. Acceso a internet desde cada sitio de un cliente utilizando NAT entre los sitios y el firewall central

Servicio de Firewall Central: Flujo de Tráfico.

El flujo de tráfico entre sitios participando en el servicio de un firewall central (Fig. 3.9) está limitado por los requerimientos de seguridad del servicio como se describe a continuación:

- El tráfico entre sitios de un cliente y la internet debe fluir libremente, restringido únicamente por las funciones de seguridad del firewall central.
- El tráfico entre sitios de un cliente individual nunca debe fluir a través de la VPN que enlaza los sitios de un cliente con el firewall central. Este tráfico debe fluir al interior de la VPN del cliente.
- El tráfico entre clientes usando el firewall central no está permitido, porque los clientes individuales no están protegidos de accesos externos. (Esta es la tarea del SP, manejado por el firewall central). El tráfico inter-cliente puede dar pie a potenciales problemas de seguridad.

Figura 3.9. Flujo de tráfico en una implementación con firewall central

Acceso a Internet al Por Mayor.

Algunos SPs quieren ofrecen el acceso a internet, más no el servicio de internet. En este caso el ISP usa la infraestructura de transporte IP de otro(s) ISPs para llegar a los usuarios finales. El modelo de negocio de este servicio varía. Los usuarios finales podrían ser clientes del ISP que es dueño de la troncal de datos (Ejemplo, un operador de cable), el cual ofrece acceso a internet a través de varios ISPs como un servicio de valor agregado. De otra manera, el ISP al cual le pertenece la troncal de acceso a internet podría actuar como mayorista, vendiendo la infraestructura de transporte a los SPs, que luego cobran a los usuarios finales todo el paquete (Fig. 3.10.1 y Fig 3.10.2).

Figura 3.10.1 Servicio de troncal de internet compartida entre varios ISPs

Figura 3.10.2: Servicio de troncal de internet compartida entre varios ISPs (Detallada).

Cuando un ISP es dueño de la troncal y provee acceso a internet a los clientes, ese ISP usualmente quiere ofrecer a una amplia gama de proveedores de donde escoger para satisfacer varios requerimientos de confiabilidad y conectividad. La selección de los ISPs y el correspondiente proceso de configuración deberían ser tan sencillos como sea posible.

Acceso a Internet al Por Mayor: Direccionamiento.

Independientemente del modelo de negocio usando en el acceso a los servicios de internet al por mayor, los requerimientos de direccionamiento siempre son los mismos. El ISP asigna una porción de su espacio de direcciones a los usuarios finales conectados a la troncal de acceso a internet. El operador de operadores que ofrece un canal IP a otros operadores por consiguiente, debe usar un pool de direcciones diferentes para cada ISP.

Implementación de los Métodos VPN de Acceso a Internet

Los Modelos de Diseño Más Implementados.

Los diseñadores de la red que quieren ofrecer acceso a internet y servicios MPLS en la misma troncal MPLS pueden escoger entre estos dos diseños:

- Separar el acceso a internet de los servicios VPN, ofreciendo el enrutamiento a internet a través del enrutamiento global en los routers PE.
- Enrutamiento hacia internet implementado como otra VPN en la red del ISP.

Acceso a Internet a través de Enrutamiento Global.

La implementación del acceso a internet a través de un enrutamiento global es idéntica a construir una troncal IP ofreciendo servicios de internet. Los protocolos BGP e IPv4 se despliegan entre routers PE para intercambiar rutas de internet, y la tabla de enrutamiento global en los routers PE es usada para enviar el tráfico hacia los destinos.

El acceso a internet se implementa a través de interfaces separadas que no están ubicadas en ninguna tabla virtual (configuración tradicional de acceso a internet).

Acceso a Internet a través de Interfaces Separadas o Subinterfaces.

Configurar el acceso a internet a través de enlaces lógicos separados es fácil porque es el equivalente de una combinación del acceso clásico a internet y los servicios VPN que muchos clientes usan hoy en día. Esta configuración también es compatible con todos los servicios de internet requeridos por algunos clientes (por ejemplo, recibir enrutamiento total de internet de un SP) y por consiguiente hay muchas opciones de diseño.

Los inconvenientes con este diseño es el incremento de la complejidad o costo de la conectividad entre los routers PE-CE. La separación del servicio de internet y la conectividad VPN requiere dos enlaces físicos separados o un único enlace físico con encapsulación WAN que soporte subinterfaces (por ejemplo, FrameRelay).

Beneficios:

- La configuración es conocida.
- Fácil de implementar.

Desventajas:

- Requiere enlaces físicos separados o encapsulación WAN que soporte sub-interfaces.

Acceso a Internet en VPNs.

El mayor beneficio de implementar el acceso a internet como una VPN separada es el incremento del aislamiento entre la troncal del proveedor y la internet, lo que da como resultado mayor seguridad. La flexibilidad de las topologías MPLS VPN también proveen algunas opciones de diseño innovador que permitan a los SPs ofrecer servicios que no son posibles de implementar con solo enrutamiento IP.

El inconveniente evidente de implementar el acceso a internet como una VPN en la arquitectura MPLS VPN es la escalabilidad. Ya que una VPN no puede llevar el enrutamiento completo de internet debido a los problemas de escalabilidad asociados con el transporte de más de 500.000 rutas al interior de una sola VPN.

Separación del Acceso a Internet de los Servicios VPN.

Existen algunas situaciones en las que el factor costo evita que se implementen enlaces físicos separados para la VPN y para el tráfico de internet.

Acceso a Internet Separado de las VPNs.

El acceso a internet siempre puede implementarse con el modelo de implementación tradicional, con dos enlaces entre el sitio o sitios de un cliente y la red del ISP (Un enlace a internet y un enlace VPN). Los dos enlaces pueden ser implementados con un enlace físico si se usa encapsulación de capa 2 que soporte sub-interfaces (Framerelay, ATM o VLAN).

La implementación del modelo de acceso a internet tradicional provee el diseño de máxima flexibilidad, porque el acceso a internet está separado completamente de los servicios MPLS. Sin embargo, las limitaciones del enrutamiento IP tradicional previene este método de implementación de ser usado para soluciones innovadoras de acceso a internet tales como el acceso a internet al por mayor.

Implementando Sub-interfaces Separadas.

En las situaciones donde el factor costo evita que se implementen enlaces físicos separados para cada VPN y el tráfico de internet, las sub-interfaces pueden ser utilizadas para crear enlaces lógicos sobre una única interfaz física. Las sub-interfaces pueden ser configuradas solamente en enlaces WAN usando Framerelay o encapsulación ATM (Incluyendo xDLS)

y sobre enlaces LAN usando cualquier encapsulación VLAN, Inter-Switch Link Protocol (ISL) o 802.1q. Para los demás tipos de encapsulación, una interfaz túnel (túneles con otros protocolos como L2TP) puede ser usada entre el router PE y el router CE.

Sin embargo, el uso de interfaces túnel no es recomendable por las siguientes razones de seguridad:

- Una interfaz túnel sobre un router PE no tiene conocimiento de la tabla virtual y de la VRF. Los puntos de conexión del túnel tienen que estar en una tabla global de enrutamiento, el tráfico VPN debe ir sobre el túnel a través de una interfaz de internet.
- Es muy fácil suplantar túneles de encapsulación genérica de enrutamiento (GRE) (si la llave del túnel está configurada, y la llave es conocida). Un intruso de internet puede generar fácilmente tráfico que puede aparecer como si vinieran sobre el túnel GRE del router CE y por lo tanto ser enviada en la VPN del cliente. En esta configuración los paquetes globales pueden terminar en el espacio VPN.

Acceso Clásico a Internet para un Cliente VPN.

La configuración clásica de acceso a internet para un cliente VPN está basada en un diseño separado de acceso a internet. Este modelo es una combinación perfecta para los clientes buscando servicios clásicos de acceso a internet (firewall entre el router CE de la central de servicios y el router CE receptor de internet [Fig. 3.11]).

Figura 3.11. Acceso clásico a internet para un cliente VPN

Acceso a Internet desde Cada Sitio de un Cliente.

Para las necesidades de acceso a internet de los clientes desde cada sitio, dos enlaces físicos (o lógicos) entre el router CE y su router PE, podría llegar a ser demasiado complejo o demasiado costoso (Fig. 3.12).

Acceso a Internet Separado.

Los beneficios de un diseño de acceso a internet separado son los siguientes:

- Es ampliamente usado y fácil de entender.
- Soporta todos los requerimientos de un cliente, incluyendo conectividad de clientes multihomed con enrutamiento completo de internet.
- Adicionalmente, este modelo permite la implementación de todos los servicios de internet, incluyendo sesiones BGP con clientes.

Los inconvenientes son:

- Requiere dos enlaces físicos dedicados entre los routers PE-CE o encapsulación WAN o LAN específica que podría no ser adecuada para todos los clientes.
- Los routers PE deben tener la capacidad de realizar enrutamiento de internet hop-by-hop y usar si bien la ruta por defecto para alcanzar internet o llevar la tabla de enrutamiento completa.
- Los servicios avanzados de acceso a internet (la administración del firewall central o el servicio de acceso a internet al por mayor) no puede realizarse del todo con este modelo.

Figura 3.12. Acceso a internet desde cada sitio cliente

Implementando el acceso a internet como una VPN separada.

Acceso a internet como una VPN separada.

La arquitectura MPLS VPN sugiere una solución obvia de acceso a internet para clientes VPN: Define el internet como otra VPN y usa varias topologías VPN para implementar varios tipos de acceso a internet.

Bajo este diseño, los routers con salida a internet aparecen como routers CE para la troncal MPLS VPN, y el acceso de los clientes a la troncal de internet, que se encuentra separada de la troncal VPN, se habilita combinando la VPN de internet con la VPN del cliente en la misma tabla virtual (topología VPN traslapada [Fig. 3.13]).

Figura 3.13. Acceso a internet como VPN separada en las tablas virtuales del cliente

La VPN de internet no debería contener la tabla de enrutamiento completa de internet porque haría que la solución no fuera escalable completamente. Los routers con salida a internet (routers CE) deberían anunciar una ruta por defecto hacia los routers PE. Para optimizar el enrutamiento local, las rutas locales (o regionales) también deben insertarse en la VPN de internet.

Cada cliente que necesite acceso a internet está asignado a la misma VPN como el punto de salida hacia la internet.

Cuando se implementa el acceso a internet como una VPN separada, la troncal de internet se mantiene separada de la troncal MPLS VPN, dando como resultado un incremento en la seguridad de la troncal MPLS VPN (por ejemplo, los dispositivos finales, donde se inicia o termina una comunicación, solo pueden alcanzar los routers PE, pero no los P routers). Los clientes de la VPN están conectados a internet a través de una apropiada configuración de la tabla virtual.

Implementando Acceso a Internet Redundante.

Un acceso redundante a internet, como se ve en la figura 3.14, se puede lograr fácilmente cuando el servicio de internet está implementado como una VPN en la troncal MPLS VPN, como se describe aquí:

- Múltiples enrutadores con salida a internet (actuando como routers CE) tienen que estar conectados a la troncal MPLS VPN para garantizar redundancia a nivel de enlace y de router.
- Todos los enrutadores con salida a internet propagan la ruta por defecto a los routers PE, dando como resultado redundancia en el enrutamiento.
- Los enrutadores con salida a internet también anuncian las rutas de internet locales como IPs o subredes públicas que pertenezcan a otros sitios de la misma organización. Debido a que estas rutas se anuncian con diferentes atributos BGP (el más notable es el MED), los routers PE seleccionan el router apropiado CE receptor de internet como el punto de salida hacia esos destinos.
- El atributo MED también puede usarse para indicar la ruta por defecto preferida a los routers PE. En esta configuración, un router CE receptor de internet actúa como un internet Gateway primario, y el otro router CE actúa como respaldo.
- La redundancia establecida hasta el momento cubre el camino entre sitios de un cliente y los routers CE receptores de internet. Una falla en la troncal de internet podría romper la conectividad para los clientes si los routers CE receptores de internet anuncian la ruta por defecto incondicionalmente. El anuncio incondicional de esta rutase configura en los routers CE, y estos la anunciaran a los routers PE solamente si los routers CE receptores de internet siempre y cuando estos puedan alcanzar otros destinos.

Figura 3.14. Acceso a internet redundante

Implementación del Acceso a Internet Clásico Para un Cliente VPN.

El modelo de acceso a internet clásico puede ser fácilmente implementado con el acceso a internet configurado como una VPN sobre la troncal MPLS VPN (Fig. 3.15). El enlace entre un router PE y el internet router CE es asignado a la tabla virtual de internet y el enlace entre un router PE y router central CE es asignado a la tabla virtual del cliente. La sesión EBGp multihop puede ser configurada entre el internet Gateway y el internet router CE.

Figura 3.15. Acceso a internet clásico para un cliente VPN

Acceso a internet desde cada sitio de un cliente.

El acceso a internet desde cada sitio de un cliente (Fig. 3.16) es la mejor implementación con una VPN traslapada, como se describe a continuación:

- Las rutas del cliente se marcan con una RT específica de cliente.
- Las rutas de internet están marcadas con una RT especial (internet).
- Los sitios de un cliente que necesitan llegar a internet están ubicados en una tabla virtual separada. Las rutas de internet y del cliente son importadas en esta tabla virtual, y las rutas exportadas de esta tabla virtual son marcadas con los RTs del cliente y de internet.

Figura 3.16. Acceso a internet desde cada sitio cliente VPN

Acceso a Internet a través de un Servicio de Firewall Central.

El servicio de gestión del firewall central debería ser implementado con la topología de la central de servicios VPN (con el firewall central siendo el sitio servidor y todos los routers CE residiendo en sitios de un cliente [Fig. 3.17]). Para los clientes con sus propias VPNs implementadas sobre la misma troncal MPLS VPN, debería ser usada la topología que traslade la VPN del cliente y la VPN de los servicios centrales.

La central de servicios VPN previene el intercambio directo de tráfico entre sitios de un cliente, dando como resultado un mecanismo de seguridad efectiva para los clientes de este servicio.

La conectividad entre el firewall central y el internet se implementa de la misma manera que el acceso a internet clásico para clientes de internet. Si el internet está configurado sobre una VPN, la interfaz pública del firewall debe estar conectada a un interfaz de un router PE que está ubicada en la tabla virtual de internet.

Figura 3.17. Acceso a internet a través de un servicio de firewall central

Acceso a la Internet al Por Mayor.

El acceso a la internet al por mayor se implementa creando una VPN separada para cada ISP. El internet Gateway del ISP (actuando como un router CE hacia una MPLS VPN sobre la troncal de acceso a internet) anuncia una ruta por defecto, la cual es usada para el enrutamiento al interior de la VPN (Fig. 3.18).

Los clientes están vinculados a los ISPs simplemente ubicando el enlace PE-CE en la tabla virtual asociada con el ISP. Cambiar un ISP se vuelve tan fácil como reasignar la interfaz a una tabla virtual diferente y atendiendo los inconvenientes de asignación. Para los clientes usando métodos de acceso soportando la asignación dinámica de direcciones, la nueva dirección IP del cliente es asignada automáticamente desde espacio de direcciones del nuevo ISP.

Figura 3.18. Servicio general de acceso a internet

Ejecutando una Troncal de Internet en una VPN.

El acceso a internet implementado como una VPN separada tiene los siguientes inconvenientes:

- Un enrutamiento completo de internet no puede ser soportado al interior de una VPN, por lo tanto, se debe utilizar enrutamiento por defecto hacia los internet gateways, lo que podría generar potencialmente un enrutamiento sub-óptimo.
- La troncal de internet está posicionada como un cliente hacia la troncal MPLS VPN. Si el SP ejecuta servicios de internet y servicios MPLS VPN en el mismo grupo de routers, la interconexión entre los dos servicios podría requerir de consideraciones especiales.

Los beneficios de este diseño, descritos aquí, compensan con creces las limitaciones:

- El diseño del modelo soporta todos los servicios de acceso a internet, que va desde el acceso tradicional a internet hasta servicios innovadores tales como el acceso a internet al por mayor.
- El diseño también soporta todos los requerimientos del cliente, incluyendo enrutamiento total de internet sobre las rutas de los clientes.

Bibliografía

Requestfor Comments (RFC).

Handbook of Information Security, Key Concepts, Infrastructure, Standards.

Editorial: John Wiley and Sons.

Año: 2006.

Autor: Hossein Bidgoli.

Juniper Networks Field Guide and Reference.

Editorial: Addison-Wesley Professional.

Año: 2002.

Autores: Aviva Garrett, Gary Drenan, Cris Morris, Juniper Networks, Inc.

TCP/IP Tutorial and Technical Overview.

Editorial: IBM Redbooks.

Año: 2006.

Autores: Lydia Parziale, Dr. Wei Liu, Carolyn Matthews, Nicolas Rosselot, Chuck Davis, Jason Forrester, David T. Britt, IBM Redbooks.

Juniper SRX Series.

Editorial: O'Reilly Media, Inc.

Año: 2013.

Autores: Brad Woodberg, Rob Cameron.

MPLS-Enabled Applications: Emerging Developments and New Technologies.

Editorial: John Wiley & Sons.

Año: 2010.

Autores: Ina Minei, Julian Lucek.

CCIE Routing and Switching Certification Guide.

Editorial: Cisco Press.

Año: 2009.

Autores: Wendell Odom, Rus Healy, Denise Donohue.

Iris Biometric Model for Secured Network Access.

Editorial: CRC Press.

Año: 2013.

Autor: Franjeh El Khoury.

*Este libro terminó de imprimirse en Noviembre de 2018, en los talleres
gráficos de Publiprint S.A.S., bajo el cuidado de los autores.
Pereira, Risaralda, Colombia.*

En este libro se encontrará información sobre las redes MPLS (Multi Protocol Label Switching) abarcando conceptos básicos y esenciales, ingeniería de tráfico, arquitectura de una red MPLS y funcionamiento de las etiquetas desde su asignación hasta su distribución hasta su implementación en redes virtuales privadas VPN. Adicionalmente, se encontrarán gráficos detallados ejemplificando los conceptos complejos de este protocolo.

Las redes MPLS son un tipo de redes privadas de comunicación ofrecidas por las principales empresas de telecomunicaciones con la peculiaridad que utilizan etiquetas capa 2.5 del modelo OSI para tomar las decisiones de enrutamiento. El protocolo MPLS permite encaminar paquetes de cualquier protocolo de red gracias a estas etiquetas. Este protocolo fue desarrollado con el objetivo de permitirle a los routers tomar decisiones de enrutamiento rápidas .

MPLS es un método de alto rendimiento para el envío de paquetes a través de una red, habilitando a los routers de frontera para que apliquen etiquetas sobre los paquetes y por consiguiente se pueden tomar decisiones de enrutamiento basadas en estas etiquetas con una búsqueda que requiere un gasto mínimo. MPLS integra tanto el rendimiento como la gestión de tráfico de la capa de enlace de datos con la escalabilidad y flexibilidad de la capa de red.

ISBN: 978-958-722-314-9

9 789587 223149

eISBN:978-958-722-356-9