

MPLS COMO SOLUCIÓN METROPOLITANA AL TRANSPORTE DE DATOS

RUDY EDUARDO MENDOZA PUELLO

LUIS EDUARDO PAREJA BAENA

**UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA ELECTRICA, ELECTRÓNICA Y MECATRÓNICA
CARTAGENA DE INDIAS**

2004

MPLS COMO SOLUCIÓN METROPOLITANA AL TRANSPORTE DE DATOS

**RUDY EDUARDO MENDOZA PUELLO
LUIS EDUARDO PAREJA BAENA**

**Monografía presentada como requisito parcial para optar al título de
Ingenieros Electrónicos**

**DIRECTOR
ING. GONZALO GARZÓN**

**UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR
FACULTAD DE INGENIERÍA ELECTRICA, ELECTRÓNICA Y MECATRÓNICA
CARTAGENA DE INDIAS
2004**

AUTORIZACIÓN

Cartagena de Indias D.T. y C., Viernes 14 de Enero de 2005

Yo, **RUDY EDUARDO MENDOZA PUELLO**, identificado con Cédula de Ciudadanía # 9.296.580 de Turbaco, autorizo a la **UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR** para el uso de mi monografía titulada “**MPLS COMO SOLUCIÓN METROPOLITANA AL TRANSPORTE DE DATOS**” y para su publicación en el catálogo online de la biblioteca.

RUDY EDUARDO MENDOZA PUELLO

C.C. # 9.296.580 de Turbaco

Debe registrarse esta autorización ante notario público.

AUTORIZACIÓN

Cartagena de Indias D.T. y C., Viernes 14 de Enero de 2005

Yo, **LUIS EDUARDO PAREJA BAENA**, identificado con Cédula de Ciudadanía # 9.292.269 de Turbaco, autorizo a la **UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR** para el uso de mi monografía titulada “**MPLS COMO SOLUCIÓN METROPOLITANA AL TRANSPORTE DE DATOS**” y para su publicación en el catálogo online de la biblioteca.

LUIS EDUARDO PAREJA BAENA

C.C. # 9.292.269 de Turbaco

Debe registrarse esta autorización ante notario público.

Cartagena, Noviembre de 2004

Señores

COMITÉ DE PROYECTOS DE GRADO

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

Escuela de ingeniería

Ciudad

Estimados señores:

La presente tiene como objeto comunicarles que he aceptado la monografía titulada “MPLS como solución metropolitana al transporte de datos” de los estudiantes Rudy Eduardo Mendoza Puello y Luis Eduardo Pareja Baena.

Cordialmente,

ISAAC ZUÑIGA SILGADO

Ing. de Sistemas

Cartagena, Noviembre de 2004

Señores

COMITÉ DE PROYECTOS DE GRADO

UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR

Escuela de Ingenierías

Ciudad

Estimados señores:

La presente tiene como objeto comunicarles que he dirigido a los estudiantes Rudy Eduardo Mendoza Puello y Luis Eduardo Pareja Baena en la monografía titulada “MPLS como solución metropolitana al transporte de datos”, presentada como requisito para optar el título de Ingenieros Electrónicos.

Cordialmente,

GONZALO GARZÓN

Ingeniero de Sistemas.

Cartagena, Noviembre de 2004

Señores

**COMITÉ DE PROYECTOS DE GRADO
UNIVERSIDAD TECNOLÓGICA DE BOLÍVAR**

Escuela de Ingenierías

Ciudad

Estimados señores:

La presente tiene como objeto presentarles la monografía titulada “MPLS como solución metropolitana al transporte de datos”, como requisito para optar el título de Ingenieros Electrónicos.

Cordialmente,

Rudy Eduardo Mendoza Puello

Luis E. Pareja Baena

ARTÍCULO 105

La Universitaria Tecnológica de Bolívar se reserva el derecho de propiedad intelectual de todos los trabajos de grado aprobados y no pueden ser explotados comercialmente sin su autorización.

Nota de aceptación

Presidente del jurado

Jurado

Jurado

Cartagena, Noviembre de 2004

Dedicatoria de Rudy Eduardo Mendoza

**A mi madre por todo el apoyo
que me ha brindado y porque ha dado
todo lo que le ha sido humanamente posible
por verme hoy convertido en un profesional.**

Cartagena, Noviembre de 2004

Dedicatoria de Luis Eduardo Pareja

**A Dios por haberme dado la fortaleza
y porque siempre me ha iluminado
mostrándome el camino a tomar
para salir adelante.**

RESUMEN

El enrutamiento IP tradicional tiene varias limitaciones bien conocidas, que van desde los problemas de escalabilidad a los problemas para implementar la ingeniería del tráfico y la deficiente integración con los backbones de Capa 2 ya existentes en las redes de los grandes proveedores de servicios. Con el rápido crecimiento de la red de Internet y el establecimiento de IP como protocolo de Capa 3 en la mayoría de los entornos, los inconvenientes del enrutamiento IP tradicional son cada vez más y más obvios.

MPLS se ha creado para combinar las ventajas del enrutamiento y el envío sin conexiones de Capa 3 con el envío de Capa 2, que sí emplea conexiones. MPLS claramente separa el plano de control, donde los protocolos de enrutamiento de Capa 3 establecen las rutas utilizadas para el envío de paquetes, del plano de datos, donde las rutas conmutadas por etiquetas de Capa 2 envían los paquetes de datos a través de la infraestructura MPLS. MPLS también simplifica el envío de datos mediante saltos, sustituyendo la función de consulta de Capa 3 realizada en los routers tradicionales por una sencilla conmutación por etiquetas. La simplicidad del envío de paquetes del plano de datos y sus similitudes con las tecnologías de Capa 2 existentes, permiten al equipamiento WAN tradicional (ATM o switches Frame Relay) volver a desplegarse como nodos MPLS (soportando el enrutamiento IP en el plano de control) simplemente con unas actualizaciones del software de su plano de control.

El componente de control en el nodo MPLS utiliza su estructura de datos interna para identificar las clases de tráfico potencial (también llamadas clases equivalentes de envío). Entre los componentes de control en los nodos MPLS se utiliza un protocolo para intercambiar el contenido de la base de datos FEC y la

asignación FEC-a-etiqueta. La tabla FEC y la asignación FEC-a-etiqueta se utilizan en los LSR de contorno para etiquetar los paquetes de entrada y enviarlos a la red MPLS. La base de información de envío de etiquetas (LFIB) se construye en cada nodo MPLS a partir de los contenidos de las tablas FEC y de las asignaciones FEC-a-etiqueta intercambiados entre los nodos. La LFIB se emplea entonces para propagar los paquetes etiquetados a través de la red MPLS, de modo similar a la función realizada por una matriz de conmutación ATM en los switches ATM.

La arquitectura MPLS es lo suficientemente genérica como para soportar otras aplicaciones aparte del enrutamiento IP. Las adiciones más simples a la arquitectura son el enrutamiento multidifusión IP y la ampliación de la calidad de servicio. El mecanismo MPLS de envío orientado a la conexión, junto con las consultas de Capa 2 basadas en etiquetas en la red principal, también ha habilitado una amplia gama de aplicaciones nuevas, desde la ingeniería del tráfico hasta verdaderas redes privadas virtuales igual a igual.

ÍNDICE DE CONTENIDO

	Pág
INTRODUCCIÓN	1
OBJETIVO GENERAL	2
OBJETIVOS ESPECÍFICOS	2
ANTECEDENTES	3
1. MPLS a grandes rasgos	5
1.1 Escalabilidad y flexibilidad de los envíos basados en el protocolo IP	6
1.2 El paradigma del enrutamiento de la capa de red	6
1.3 Servicios de paquetes diferenciados	11
1.4 Envío y control independientes	13
1.5 Propagación de información de enrutamiento exterior	13
1.6 Introducción a la Conmutación de etiquetas multiprotocolo (MPLS)	14
1.7 Arquitectura MPLS: la construcción de bloques	17
1.8 Imposición de etiquetas en el contorno de la red	21
1.9 Envío de paquetes MPLS y rutas conmutadas por etiquetas	23
1.10 Otras aplicaciones de MPLS	25
2. MPLS en modo trama	29
2.1 Funcionamiento del plano de datos en MPLS en modo trama	31
2.2 Cabecera de la pila de etiquetas MPLS	33
2.3 Conmutación de etiquetas en MPLS en modo trama	37
2.4 Conmutación de etiquetas MPLS con la pila de etiquetas	39
2.5 Enlaces de etiquetas y propagación en MPLS en modo trama	40
2.6 Establecimiento de la sesión LDP/TDP	42
2.7 Distribución y enlace de etiquetas	44
2.8 Convergencia en una red MPLS en modo trama	48
2.9 Omisión del penúltimo salto	52

2.10 Interacción de MPLS con el Protocolo de gateway fronterizo	55
2.11 Mpls en modo trama a través de medios Wan conmutado	58
2.12 Funcionamiento de MPLS en modo trama a través de Frame Realy	58
2.13 Mpls en modo trama a través de la misma interfaz ATM	61
3. MPLS en modo celda	63
3.1 Conectividad del plano de control en una interfaz LC-ATM	64
3.2 Conectividad del plano de control MPLS en el software Cisco IOS	65
3.3 Implementación del plano de control en un switch ATM	66
3.4 Envío de paquetes etiquetados a través de un dominio LSR ATM	67
3.5 Distribución y asignación de etiquetas en un dominio LSR ATM	68
3.6 Convergencia a lo largo de un dominio LSR ATM	69
4. Características avanzadas de MPLS	70
4.1 Control de la distribución de las asignaciones de etiquetas	70
4.2 Encapsulación MPLS a través de enlaces Ethernet	72
4.3 Descubrimiento de la MTU IP de la ruta	73
4.4 Detección y prevención de bucles en MPLS	74
4.5 Detección y prevención de bucles en MPLS en modo trama	74
4.5.1 Modo trama: detección de bucles en el plano de datos	75
4.5.2 Modo trama: prevención de bucles en el plano de control	75
4.6 Detección y prevención de bucles en MPLS en modo celda	76
4.6.1 Modo celda : prevención y detección de bucles en el plano de control	76
4.6.2 Modo celda: detección de bucles en el plano de datos	78
4.7 Resumen de ruta en una red con MPLS habilitada	79
5. CONCLUSIONES	82
6. RECOMENDACIONES	83
REFERENCIAS BIBLIOGRAFICAS	84
GLOSARIO	86

ANEXOS

Anexo 1. Comandos MPLS (Cisco y Nortel Networks)	94
Anexo 2. Algunas empresas que ofrecen MPLS	99

LISTA DE TABLAS

Tabla 1.1. Acciones desempeñadas por distintos tipos de LSR	20
Tabla 1.2. Protocolos de control utilizados en diversas aplicaciones MPLS	27
Tabla 2.1. Direcciones loopback en la red SuperNet	30
Tabla 2.2. Comandos de configuración del IOS utilizados para iniciar MPLS en una interfaz	41

LISTA DE FIGURAS

Figura 1.1. Red IP de ejemplo, basada en un ATM principal	8
Figura 1.2. Red de ejemplo que se beneficiaría de la ingeniería del tráfico	11
Figura 1.3. Arquitectura básica de un nodo MPLS realizando el enrutamiento IP	17
Figura 1.4. Arquitectura de un LSR de contorno	19
Figura 1.5. Imposición y envío de etiquetas MPLS	23
Figura 1.6. La arquitectura LSR de contorno utiliza términos del Cisco IOS	25
Figura 1.7. Diversas aplicaciones MPLS y sus interacciones	26
Figura 2.1. Arquitectura LSR de contorno	30
Figura 2.2. Red del proveedor de servicios SuperNet	31
Figura 2.3. Envío de un paquete entre el POP de San José y el cliente de Nueva York	32

Figura 2.4. Posición de la etiqueta MPLS en una trama de Capa 2	34
Figura 2.5. Cabecera de la pila de etiquetas MPLS	34
Figura 2.6. Resumen de las técnicas de encapsulación MPLS	36
Figura 2.7. Conmutación de etiquetas con la pila de etiquetas MPLS	40
Figura 2.8. Doble búsqueda en el router POP de Nueva York	53
Figura 2.9. Omisión del penúltimo salto en la red SuperNet	54
Figura 2.10. Pérdida de conectividad en la red sin BGP en los routers principales	56
Figura 2.11. propagación del paquete hacia el destino BGP en una red con MPLS habilitada	57
Figura 2.12 Encapsulación de MPLS en modo trama a través de PVC ATM	60
Figura 2.13. Conectividad MPLS a través de MPLS ATM	61
Figura 2.14. MPLS en modo trama y en modo celda a través de la misma interfaz ATM	62
Figura 3.1. Red SuperCell: Implementación ATM	64
Figura 3.2. Ejecución de los protocolos de señalización en un switch ATM	66
Figura 4.1 Mecanismo de descubrimiento de la MTU	73
Figura 4.2 Detección de Bucles usando el campo TTL en una red IP	75
Figura 4.3 Procesamiento del objeto TLV contador de saltos	77
Figura 4.4 Propagación del contador de saltos entre los LSR ATM	78
Figura 4.5 procesamiento del campo TTL del paquete IP antes del proceso SAR	79
Figura 4.6 Resumen de ruta en una red MPLS	80

INTRODUCCIÓN

Hoy por hoy las aplicaciones novedosas y cada vez mas demandantes que han surgido en Internet han producido un aumento de la necesidad de transmitir información; además se requiere que esta transmisión se haga garantizando ciertos parámetros de Calidad de Servicio como pueden ser el retardo máximo y el número de paquetes que puedan ser descartados sin afectar la calidad de la transmisión de la información. Debido a que esta calidad de servicio requerida no puede ser asegurada por los protocolos TCP/IP, se han desarrollado diferentes tecnologías para superar este inconveniente, entre estas tecnologías está la que nos es motivo de estudio en esta monografía y es la tecnología MPLS.

La tecnología MPLS (Multiprotocol Label Switching) permite superar ciertas deficiencias de los niveles superiores como TCP/IP y a la vez mejora el factor de transmisión debido a que en vez de realizar el envío de paquetes a través de enrutamientos basados en direcciones IP este se realiza mediante conmutación a través de etiquetas. Además a MPLS unidifusión se le ha especificado el funcionamiento de RSVP-TE y el CR-LDP para asegurar parámetros como reserva de recursos y retardo máximos para un flujo de información.

OBJETIVO GENERAL

Presentar ante la comunidad académica en general la tecnología de Conmutación de Etiquetas Multiprotocolo, MPLS, como alternativa viable para la transmisión de datos en la Internet del nuevo siglo.

OBJETIVOS ESPECÍFICOS

- Dar a conocer el trabajo de MPLS como una arquitectura que provee escalabilidad y flexibilidad a los envíos basados en protocolo IP.
- Explicar los modos de funcionamiento de MPLS (modo trama y modo celda) para entender así la inmensa flexibilidad de esta nueva tecnología.
- Mostrar detalladamente las implementaciones de MPLS realizadas con el Software Cisco IOS y resaltar cada uno de sus comandos principales.

ANTECEDENTES

ATM es hoy en día el principal soporte de datos sobre el que se ofrecen multitud de servicios. La mediación ATM/MPLS surge como la solución ideal para interconectar los mundos ATM e IP. La influencia de Internet en el dinámico mercado de las telecomunicaciones ha generado una gran demanda de flexibilidad a la vez que un mayor control sobre los costos. Esta influencia provoca una necesidad importante de replantear la arquitectura de las próximas generaciones de redes, los conceptos fundamentales en esta nueva mentalidad de red son convergencia, consolidación, migración y simplificación.

Parece claro que la capa de servicio del futuro consistirá en una red IP con capacidad multiservicio. La ubicuidad, simplicidad y estructura abierta de IP lo convierte en un catalizador natural para las nuevas aplicaciones, servicios, tráfico y, consecuentemente, para los nuevos ingresos. Los desarrollos de los estándares de Calidad de Servicio (QoS) IP y la ingeniería de tráfico basada en la conmutación de etiquetas multiprotocolo (MPLS) proporcionará las capacidades técnicas para hacer viables estas redes IP multiservicio.

El núcleo de la red está evolucionando hacia lo que puede denominarse red óptica de paquetes. El principal motor de esta evolución es la reducción del costo por megabit (ancho de banda) en esta parte de la red. Los operadores de red encaran grandes desafíos a la hora de construir nuevas redes fiables con núcleo óptico IP-MPLS "carrier grade". Los productos y servicios IP están todavía luchando con la necesidad de trabajar en una red "carrier class" en la que la disponibilidad de 99,999 por ciento es la norma, y donde cualquier indisponibilidad no esperada puede costar miles de millones de dólares en pérdida de negocio. Cada vez más, el desarrollo de la tecnología IP-MPLS está revalidando las cualidades de ATM

emulando muchas de sus características y funciones hasta tal punto que la convergencia de IP-MPLS y ATM en el núcleo es ahora técnicamente factible. Uno de los primeros ejemplos de esta convergencia es la introducción de la mediación ATM sobre un núcleo de red IP-MPLS, en el cual el tráfico ATM puede ser encapsulado de forma transparente a través del núcleo IP-MPLS usando túneles LSP.

De la misma manera que ATM ha sido usado para transportar tráfico multiservicio sobre una red de área amplia, ahora existe la oportunidad de utilizar MPLS para transportar tráfico ATM a través de un núcleo IP-MPLS. Cuando el tráfico ATM es mediado sobre una red IP-MPLS, las conexiones ATM se transportan transparentemente sobre túneles LSP establecidos entre puntos del borde del núcleo. En la red convergente ATM/MPLS, hay túneles LSP entre las pasarelas de mediación ATM/MPLS que rodean el borde de la red MPLS. Estos LSP sirven como túneles de transporte a través de la red MPLS. La red ATM ve a los nodos de mediación ATM/MPLS como conmutadores ATM, y a los túneles LSP como simples enlaces virtuales ATM punto a punto que conectan los nodos ATM. El desafío de la mediación es construir los túneles LSP a través del núcleo MPLS de tal forma que proporcione el mismo o mejor nivel de servicio que el enlace físico ATM. En la pasarela de mediación ATM/MPLS, las conexiones que atraviesan desde la red ATM a la red MPLS se admiten en el túnel LSP de la misma manera que lo serían en un enlace físico ATM. Una función de control de admisión de las conexiones en la pasarela de mediación ATM/MPLS garantiza que el túnel LSP tiene suficientes recursos para acomodar los requerimientos de servicio de las conexiones ATM. Los mecanismos de colas y planificación usados para lanzar las tramas MPLS conteniendo tráfico ATM en los túneles LSP serán funcionalmente equivalentes a los usados para lanzar células ATM en enlaces físicos ATM.

1. MPLS A GRANDES RASGOS

Normalmente, cualquier paquete IP enviado analiza la dirección IP de destino contenida en la cabecera de la capa de red de cada paquete a medida que el paquete se desplaza desde su origen a su destino final. El router analiza la dirección IP de destino de modo independiente en cada salto en la red. Los protocolos de enrutamiento dinámico o la configuración estática construyen la base de datos necesaria para analizar la dirección IP de destino (la tabla de enrutamiento). El proceso de llevar a cabo el enrutamiento IP tradicional también se denomina enrutamiento unidifusión basado en el destino salto a salto.

Aunque este método funciona muy bien, y obviamente ha sido ampliamente utilizado, presenta ciertas restricciones, de las que se tiene conocimiento desde hace algún tiempo, que disminuyen su flexibilidad. Por ello, se impone contar con nuevas técnicas para dirigir y expandir la funcionalidad de una infraestructura de red basada en el protocolo IP.

Este primer capítulo está dedicado a identificar estas restricciones, presentando además una nueva arquitectura, conocida como **Conmutación de etiquetas multiprotocolo (MPLS)**, que ofrece soluciones a algunas de estas restricciones. Los capítulos siguientes explican en primer lugar los detalles de la arquitectura MPLS en un entorno puro de router, y después en un entorno mixto switch ATM/router.

1.1 ESCALABILIDAD Y FLEXIBILIDAD DE LOS ENVÍOS BASADOS EN EL PROTOCOLO IP

Para comprender bien todos estos aspectos que afectan a la escalabilidad y la flexibilidad de las redes tradicionales de envío de paquetes IP, conviene empezar por revisar algunos de los mecanismos principales de envío con el protocolo IP y su interacción con la infraestructura subyacente (redes locales o de área amplia). Con esta información, podrá identificar cualquier inconveniente de este sistema, y quizá proponer algunas alternativas q podrían mejorarlo.

1.2 EL PARADIGMA DEL ENRUTAMIENTO DE LA CAPA DE RED

El envío tradicional de paquetes por la capa de red (por ejemplo, el envío de paquees IP por Internet) se apoya en la información proporcionada por los protocolos de enrutamiento de la capa de red (por ejemplo, Primero la ruta libre más corta [OSPF] o Protocolo de gateway fronterizo [BGP]), o en el enrutamiento estático, para tomar una decisión de en independiente en cada salto (router) dentro de la red. La decisión de envío se basa exclusivamente en la dirección IP unidifusión de destino. Todos los paquetes para el mismo d tino siguen la misma ruta a través de la red, si no existen otras rutas de acceso de igual costo. Siempre que un router tenga dos rutas de igual costo hacia el destino, los paquetes dirigidos a ese destino podrían tomar una o ambas rutas, con lo que en cierta medida compartiría la carga.

Los routers ejecutan el proceso de decisión que selecciona la ruta que toma un paquete. Estos dispositivos de capa de red participan en la captación y distribución de información de capa de red y ejecutan la conmutación de Capa 3 en base a los

contenidos de la cabecera de la capa de red de cada paquete. Puede conectar los routers directamente mediante enlaces punto a punto, o redes de área local (por ejemplo, con un hub compartido o una MAU [unidad de conexión al medio]), o también puede conectarlos mediante switches LAN o WAN (por ejemplo, switches Frame Relay o ATM). Estos switches de Capa 2 (LAN o WAN) desafortunadamente no tienen la capacidad de contener información de enrutamiento de Capa 3 o seleccionar la ruta que debería tomar un paquete a través del análisis de sus direcciones de destino de Capa 3. Así, los switches de Capa 2 (LAN o WAN) no se pueden involucrar en los procesos de decisión de envío de paquetes de Capa 3. En el caso del entorno WAN, el diseño de red tiene que establecer las rutas de Capa 2 manualmente a través de la red WAN. Estas rutas envían entonces los paquetes de Capa 3 entre los routers conectados físicamente a la red de Capa 2.

Las rutas de Capa 2 LAN son fáciles de establecer (todos los switches LAN son transparentes a los dispositivos conectados a ellos). El establecimiento de la ruta de Capa 2 WAN es más complejo. Normalmente, las rutas de Capa 2 WAN se basan en el paradigma punto a punto (por ejemplo, circuitos virtuales en la mayoría de las redes WAN) y se establecen sólo bajo solicitud mediante configuración manual. Cualquier dispositivo de enrutamiento (router de entrada) en el contorno de la red de Capa 2 que quiera enviar paquetes de Capa 3 a cualquier otro dispositivo de enrutamiento (router de salida), necesita, por tanto, establecer una conexión directa a través de la red con el dispositivo de salida o enviar sus datos a un dispositivo diferente para la transmisión al destino final.

Considere, por ejemplo, la red que se muestra en la Figura 1.1.

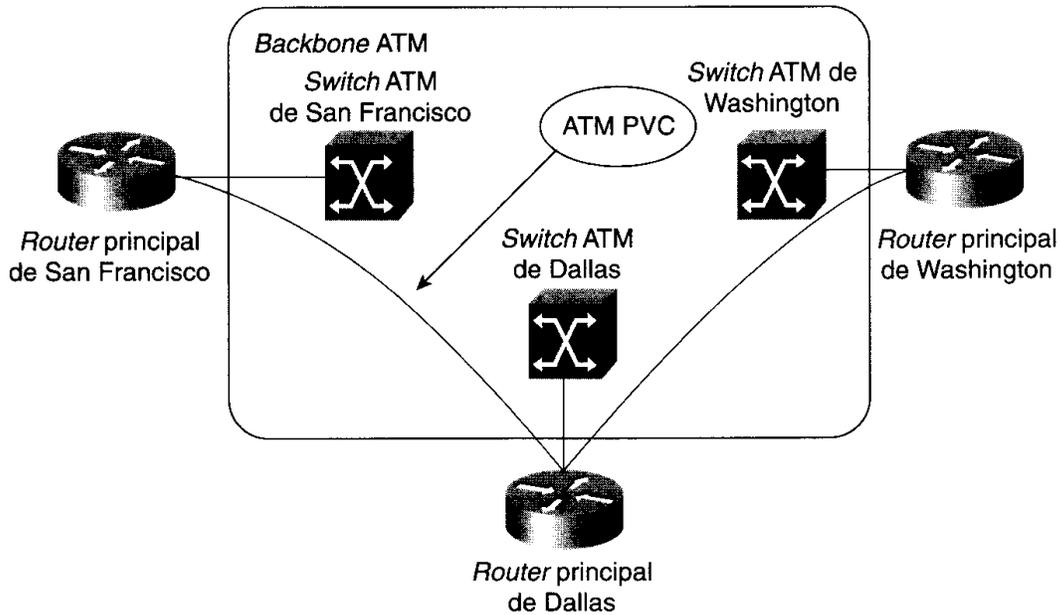


Figura 1.1. Red IP de ejemplo, basada en un ATM principal.

La red que se ilustra en la Figura 1.1 se basa en un ATM principal rodeado de otros routers que realizan el envío de capa de red. Asumiendo que las únicas conexiones entre los routers son las que se muestran en la Figura 1. 1, todos los paquetes enviados desde San Francisco hacia o a través de Washington, se deben enviar al router de Dallas, donde se analizan y se envían de regreso por la misma conexión ATM de Dallas al router de Washington. Este paso adicional introduce una demora en la red y carga innecesariamente la CPU del router de Dallas, así como el enlace ATM entre el router de Dallas y el switch ATM adyacente de Dallas.

Para garantizar que el envío de paquetes por la red sea óptimo, debe existir un circuito ATM virtual entre cualquiera de los dos routers conectados al ATM principal. Aunque esto podría ser fácil de conseguir en redes pequeñas, como la de la Figura 1.1, se pueden presentársenos problemas de escalabilidad en redes

grandes, donde se conectan varias decenas o, incluso, centenares de routers a la misma WAN principal.

Los siguientes puntos ilustran los problemas de escalabilidad que podría encontrarse:

- Cada vez que un nuevo router se conecta al núcleo WAN de la red, debe establecerse un circuito virtual entre ese router y cualquier otro router, si se necesita un enrutamiento óptimo.
- En algunas configuraciones de protocolos de enrutamiento, cada router adjunto a núcleo WAN de Capa 2 (construido con switches ATM o Frame Relay) necesita un circuito virtual dedicado a cada router adjunto al principal. Para conseguir la redundancia principal deseada, cada router debe establecer también una adyacencia de protocolo de enrutamiento con cada uno de los routers adjuntos al principal. La malla completa de adyacencias de routers resultante lleva a que cada router que tenga una cantidad considerable de protocolos de enrutamiento vecinos, producirá una gran cantidad de tráfico de enrutamiento. Por ejemplo, si la red utiliza OSPF o IS-IS como protocolos de enrutamiento, cada router propagará cada cambio en la topología de la red a cada uno de los otros routers conectados al mismo backbone WAN, resultando un enrutamiento de tráfico proporcional al cuadrado del número de routers existentes.
- Disponer de circuitos virtuales entre los routers es complejo, debido a que es muy difícil predecir la cantidad exacta de tráfico entre dos routers cualquiera de la red. Para simplificar esta disposición, algunos proveedores de servicios optan por no ofrecer servicios garantizados en la red: velocidad

de información suscrita (CIR) cero en una red Frame Relay o conexiones de velocidad de bits sin especificar (UBR) en una red ATM.

La falta de intercambio de información entre los routers y los switches WAN no ha sido un tema de preocupación para los proveedores de servicios de Internet tradicionales que emplean backbones constituido tan sólo por routers, o los proveedores de servicios tradicionales que ofrecen únicamente servicios WAN (circuitos virtuales ATM o Frame Relay). Sin embargo, hay varios aspectos que empujan a ambos grupos hacia los diseños de backbones mixtos:

- A los proveedores de servicios tradicionales se les pide que ofrezcan servicios IP. Quieren sacar más provecho a sus inversiones y basan estos nuevos servicios en sus infraestructuras WAN existentes.
- A los proveedores de servicios se les pide que ofrezcan garantías de una mayor calidad de servicio (QoS), que son más fáciles de satisfacer con switches ATM que con los routers tradicionales.
- El rápido incremento de las necesidades de ancho de banda anteriores a la introducción de interfaces de routers ópticos, ha forzado a ciertos proveedores de servicios a comenzar a utilizar la tecnología ATM debido a que las interfaces de los routers en ese momento no conseguían las velocidades ofrecidas por los switches ATM.

Es claro entonces que hay que emplear un mecanismo diferente para habilitar el intercambio de información de capa de red entre los routers y los switches WAN y permitir a los switches participar en el proceso de decisión de envío de paquetes,

de modo que ya no sean imprescindibles las conexiones directas entre routers de contorno o límite.

1.3 SERVICIOS DE PAQUETES DIFERENCIADOS

El envío convencional de paquetes IP emplea sólo la dirección IP de destino contenida dentro de la cabecera de Capa 3 de un paquete para tomar una decisión de envío. El paradigma de sólo destino salto a salto usado actualmente supone un freno para el avance de varios enfoques innovadores en el diseño de redes y la optimización del flujo de tráfico. En la Figura 1.2, por ejemplo, el enlace directo entre el router principal de San Francisco y el router principal de Washington envía el tráfico que entra en la red desde cualquiera de los puntos de presencia (POP) del área de la Bahía, aunque dicho enlace pudiera congestionarse y los enlaces desde San Francisco a Dallas y de Dallas a Washington pudieran estar muy poco cargados.

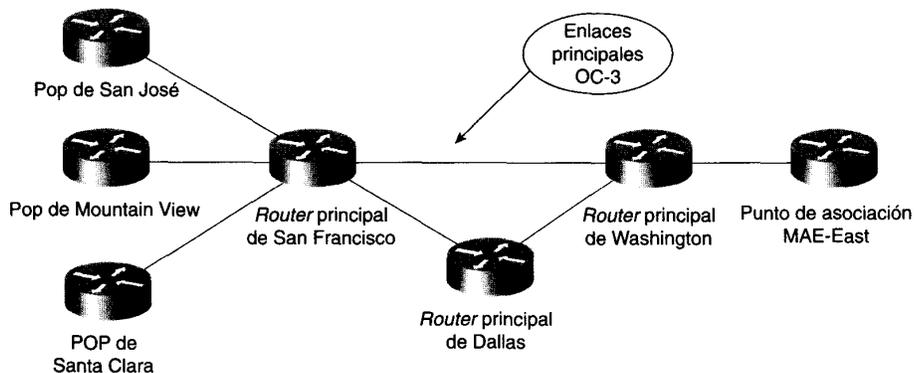


Figura 1.2. Red de ejemplo que se beneficiaría de la ingeniería del tráfico.

Aunque ciertas técnicas existentes afectan al proceso de decisión, como el enrutamiento basado en normas (PBR), no existe una sola técnica escalable para decidir la ruta completa que debe tomar un paquete a través de la red hasta su destino final. En la red que se muestra en la Figura 1.2, el enrutamiento basado en normas debe desplegarse en el router principal de San Francisco para desviar algo del tráfico del área de la Bahía hacia Washington a través de Dallas. La utilización de algunas funciones como PBR en los routers principales podría reducir enormemente el rendimiento de un router principal y dar como resultado un diseño de red más bien no escalable. Idealmente, los routers de contorno (por ejemplo, el POP de Santa Clara en la Figura 1.2) pueden especificar cuáles son los enlaces principales que deben seguir los paquetes.

Debido a que la mayoría de los proveedores de servicios instalan redes con rutas redundantes, hay un requisito imprescindible para permitir al dispositivo de enrutamiento de entrada ser capaz de decidir sobre el envío de paquetes, que afecta a la ruta que toma un paquete a través de la red, y de aplicar una etiqueta a ese paquete, que indica a los demás dispositivos la ruta que debe tomar el paquete.

Este requisito también debería permitir a los paquetes que se han destinado para la misma red IP, tomar rutas alternativas en lugar de la ruta determinada por el protocolo de enrutamiento de Capa 3. Esta decisión también debería basarse en otros factores diferentes a la dirección IP de destino del paquete, como desde qué puerto se aprendió el paquete, la calidad del nivel de servicio que requiere el paquete, etcétera.

1.4 ENVÍO Y CONTROL INDEPENDIENTES

Con el envío convencional de paquetes IP, cualquier cambio en la información que controla el envío de paquetes se comunica a todos los dispositivos dentro del dominio de enrutamiento. Este cambio siempre implica un periodo de convergencia dentro del algoritmo de envío.

Ciertamente sería deseable un mecanismo que permitiera cambiar la forma en que se envían los paquetes, sin afectar a los otros dispositivos de la red. Para implementar tal mecanismo, los dispositivos de envío (routers) no deberían limitarse a la información de la cabecera IP para enviar el paquete; por ello, se debe agregar una etiqueta adicional al paquete enviado que indique el comportamiento de envío deseado. Con el envío de paquetes realizándose sobre la base de etiquetas adjuntas a los paquetes IP originales, cualquier cambio en el proceso de decisión puede comunicarse a los otros dispositivos a través de la distribución de etiquetas nuevas. Debido a que estos dispositivos envían tráfico basándose en la etiqueta adjunta, los cambios deberían producirse sin que tuvieran ningún impacto sobre los dispositivos que realizan el envío de paquetes.

1.5 PROPAGACIÓN DE INFORMACIÓN DE ENRUTAMIENTO EXTERIOR

El envío convencional de paquetes en el núcleo de una red IP requiere que se publique la información de enrutamiento externa en todos los dispositivos de enrutamiento de tránsito. Esto es necesario para que los paquetes puedan enrutarse basándose en la dirección de destino almacenada en la cabecera de la capa de red del paquete. Para continuar el ejemplo de secciones anteriores, los routers principales de la Figura 1.2 deberían almacenar todas las rutas de Internet que podrían propagar paquetes entre los clientes del área de la Bahía y un punto de asociación en MAE-East.

Este método tiene implicaciones de escalabilidad en términos de propagación de ruta, uso de memoria y utilización de la CPU de los routers principales, y no es una función realmente necesaria si todo lo que quiere hacer es pasar un paquete desde uno de los contornos de la red a otro.

Es obvia la necesidad de un mecanismo que permite a los dispositivos de enrutamiento interno conmutar los paquetes a través de la red desde un router de entrada hacia un router de salida sin tener que analizar la dirección de destino de la capa de red.

1.6 INTRODUCCIÓN A LA CONMUTACIÓN DE ETIQUETAS MULTIPROTOCOLO (MPLS)

La Conmutación de etiquetas multiprotocolo (MPLS) es una tecnología emergente destinada a encauzar muchos de los actuales retos que plantea el envío de paquetes en el entorno actual de internetworking. Los miembros de la comunidad IETF han realizado un gran esfuerzo para presentar un conjunto de normas al mercado y evolucionar las ideas de diferentes proveedores e individuos en el área de la conmutación de etiquetas. El documento IETF draft-ietf-mpls-framework contiene el marco de esta iniciativa y describe el objetivo principal del siguiente modo:

La arquitectura MPLS describe los mecanismos para realizar la conmutación de etiquetas, que combina los beneficios del envío de paquetes basados en la conmutación de Capa 2 con los beneficios del enrutamiento de Capa 3. De forma similar a las redes de Capa 2 (por ejemplo, Frame Relay o ATM), MPLS asigna etiquetas a los paquetes para su transporte a través de redes basadas en paquetes o celdas. El mecanismo de envío a través de la red es el intercambio de

etiquetas, en cuyas unidades de datos (por ejemplo, un paquete o una celda) se transporta una etiqueta corta, de longitud fija, que indica a los nodos de conmutación que hay a lo largo de la ruta de los paquetes la forma de procesar y enviar los datos.

La diferencia más significativa entre las tecnologías MPLS y la tradicional WAN es la forma en que se asignan las etiquetas y la capacidad de transportar una pila de etiquetas adjuntas a un paquete. El concepto de una pila de etiquetas habilita nuevas aplicaciones, como la ingeniería del tráfico, las redes privadas virtuales, el reenrutamiento rápido alrededor de un enlace y los fallos de los nodos, etcétera.

El envío de paquetes en MPLS contrasta mucho con el entorno actual de las redes sin conexiones, en las que cada paquete se analiza sobre la base de salto a salto, se comprueba su cabecera de Capa 3, y se toma una decisión de envío independiente en base a la información extraída de un algoritmo de enrutamiento de capa de red.

La arquitectura se divide en dos componentes separados: el componente de envío (también denominado plano de datos) y el componente de control (llamado también plano de control). El componente de envío emplea una base de datos de envío de etiquetas mantenida por una conmutación por etiquetas, para ejecutar el envío de paquetes de datos basándose en las etiquetas transportadas por los paquetes. El componente de control es el responsable de la creación y mantenimiento de la información de envío de etiquetas (a lo que nos referiremos como enlaces) entre un grupo de switches de etiqueta interconectados. La Figura 1.3 muestra la arquitectura básica de un nodo MPLS realizando el enrutamiento IP.

Cada nodo MPLS debe ejecutar uno o más protocolos de enrutamiento IP (o confiar en un enrutamiento estático) para intercambiar la información de enrutamiento IP con otros nodos MPLS de la red. En este sentido, cada nodo MPLS (incluyendo los switches ATM) es un router IP en el plano de control.

De manera similar a los routers tradicionales, los protocolos de enrutamiento IP pueblan la tabla de enrutamiento. En los routers IP tradicionales, la tabla de enrutamiento IP se emplea para construir la caché de envío IP (caché de switching rápido en el Cisco IOS) o la tabla de envío IP (Base de información de envío [FIB] en el Cisco IOS) utilizada por el Envío expreso de Cisco (CEF).

En un nodo MPLS, la tabla de enrutamiento IP se emplea para determinar el intercambio de enlace de etiquetas, donde los nodos MPLS adyacentes intercambian etiquetas para las subredes individuales almacenadas en la tabla de enrutamiento IP. El intercambio de enlace de etiquetas para el enrutamiento IP basado en destinos unidifusión se realiza utilizando el Protocolo de distribución de etiquetas identificativas (TDP) patentado por Cisco o el Protocolo de distribución de etiquetas (LDP) especificado por el IETF.

El proceso de control del enrutamiento IP MPLS utiliza las etiquetas intercambiadas entre nodos MPLS adyacentes para construir la tabla de envíos de etiquetas, que es la base de datos del plano de envío que se emplea para enviar los paquetes etiquetados a través de la red MPLS.

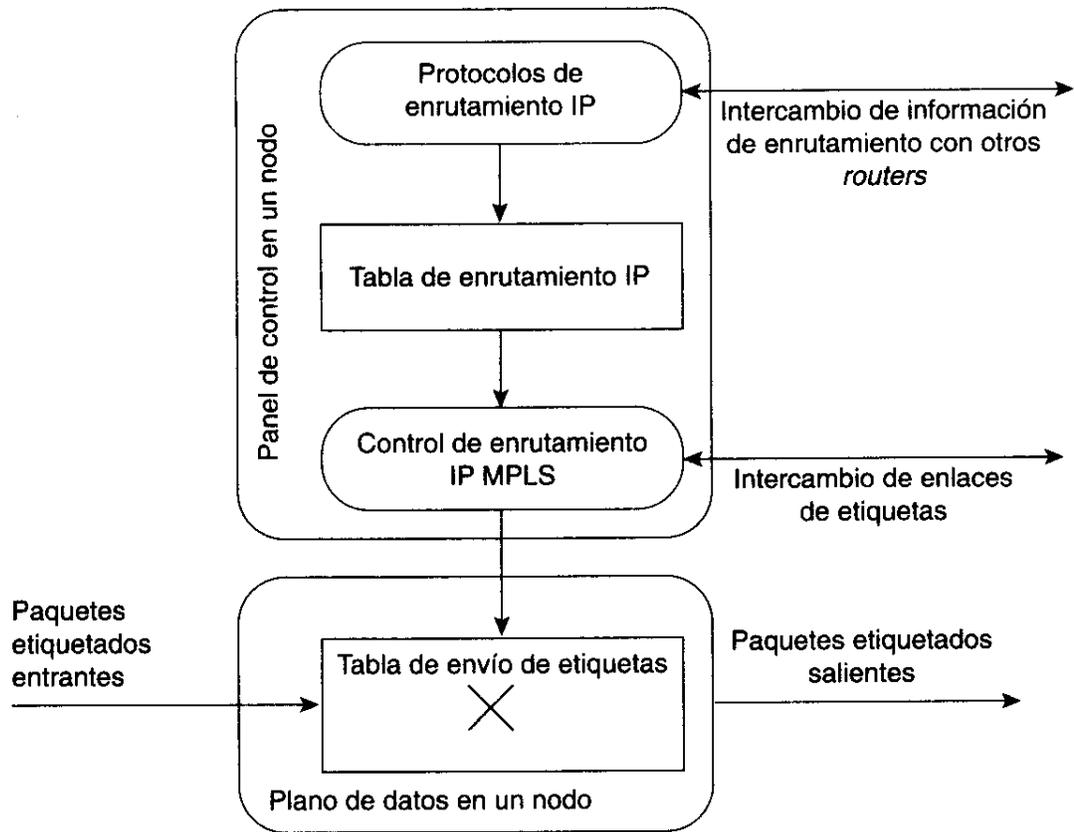


Figura 1.3. Arquitectura básica de un nodo MPLS realizando el enrutamiento IP.

1.7 ARQUITECTURA MPLS: LA CONSTRUCCIÓN DE BLOQUES

Como con cualquier nueva tecnología, aparecen nuevos términos para describir los dispositivos que conforman la arquitectura. Estos términos nuevos describen la funcionalidad de cada dispositivo y sus funciones en la estructura del dominio MPLS.

El primer dispositivo novedoso es el router de conmutación por etiquetas (LSR). Todo router o switch que implemente procedimientos de distribución de etiquetas y que pueda enviar paquetes basándose en etiquetas, entra en esta categoría. La función básica de los procedimientos de distribución de etiquetas es la de permitir que un LSR distribuya sus enlaces de etiquetas a otros LSR de la misma red MPLS. (El Capítulo 2 explica en detalle los procedimientos de distribución de etiquetas.)

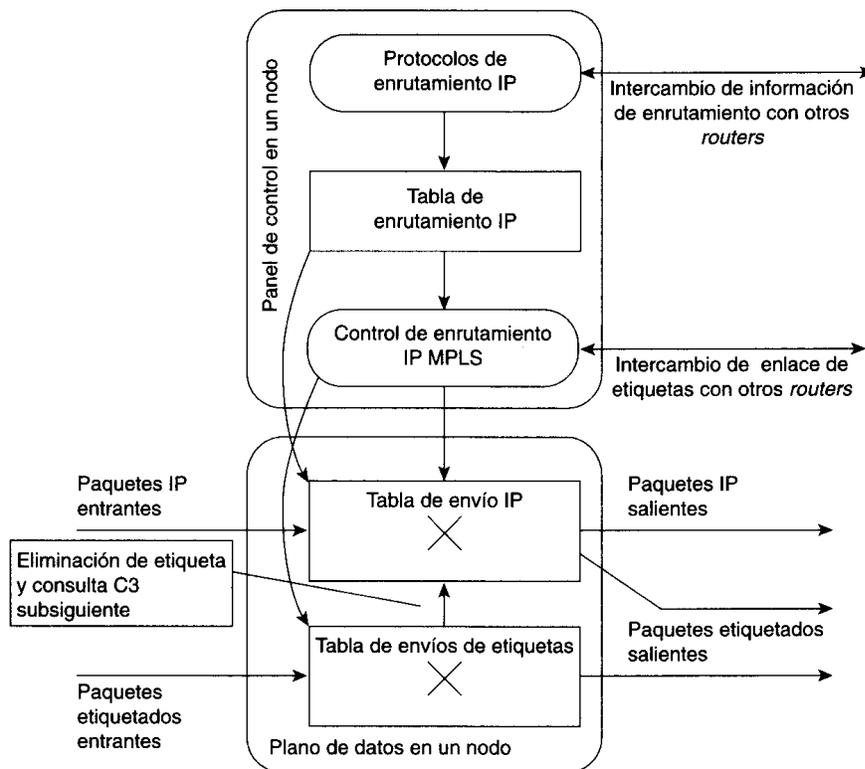
Existen diferentes tipos de LSR que se diferencian por la funcionalidad que proporcionan a la infraestructura de red. Estos diferentes tipos de LSR se describen en la arquitectura como LSR de contorno, LSR ATM y LSR ATM de contorno. La distinción entre los diferentes tipos de LSR es puramente arquitectónica (una sola caja puede servir para varias funciones).

Un LSR de contorno es un router que realiza tanto la imposición de etiquetas (también llamada acción push) como la determinación de etiquetas (también llamada acción pop) en el contorno de la red MPLS. La imposición de etiquetas es el acto de añadir una etiqueta, o una pila de etiquetas, a un paquete en el punto de entrada (con respecto al flujo de tráfico desde el origen al destino) del dominio MPLS. La determinación de etiquetas es lo contrario, es decir, el acto de eliminar la última etiqueta de un paquete en el punto de salida antes de que se envíe a un vecino que está fuera del dominio MPLS.

Todo LSR que tenga vecinos que no sean MPLS se considera un LSR de contorno. No obstante, si este LSR tuviera alguna interfaz conectada a través de MPLS a un LSR ATM, entonces se ha de considerar también como un LSR ATM de contorno. Los LSR de contorno emplean la tradicional tabla de envíos IP, incrementada con información de etiquetado, para etiquetar paquetes IP o para

eliminarlas etiquetas de los paquetes etiquetados antes de enviarlos a nodos que no son MPLS. La Figura 1.4 muestra la arquitectura de un LSR de contorno.

Un LSR de contorno amplía la arquitectura del nodo MPLS de la Figura 1.3 con componentes adicionales en el plano de datos. La tabla de envío IP se construye sobre la base de la tabla de enrutamiento IP y se amplía con información de etiquetado. Los paquetes IP entrantes se pueden enviar como paquetes IP puros hacia nodos que no son MPLS, o pueden ser etiquetados y enviarse como paquetes etiquetados a otros nodos MPLS. Los paquetes etiquetados entrantes se pueden enviar como paquetes etiquetados a otros nodos MPLS. Para los paquetes etiquetados destinados a nodos que no son MPLS, se elimina la etiqueta y se realiza una consulta de Capa 3 (envío IP) para encontrar el destino que no es



MPLS.

Figura 1.4. Arquitectura de un LSR de contorno.

Un ATM-LSR es un switch ATM que puede actuar como LSR. La familia de switches LS1010 y BPX de Cisco Systems, son buenos ejemplos de este tipo de LSR. Como puede verse en los siguientes capítulos, el LSR ATM efectúa el enrutamiento IP y la asignación de etiquetas en el plano de control y envía los paquetes de datos utilizando mecanismos de conmutación por celdas ATM adicionales en el plano de datos. En otras palabras, la matriz de conmutación ATM de un switch ATM se utiliza como tabla de envío de etiquetas de un nodo MPLS. Por ello, los switches ATM tradicionales pueden redespigarse como LSR mediante una actualización del software de sus componentes de control.

La Tabla 1.1 resume las funciones realizadas por los distintos tipos de LSR. Hay que advertir que cualquier dispositivo individual en la red puede realizar más de una función (por ejemplo, puede ser LSR de contorno y LSR ATM de contorno al mismo tiempo).

Tabla 1.1. Acciones desempeñadas por distintos tipos de LSR.

Tipo de LSR	Acciones realizadas por distintos tipos de LSR
LSR	Envía paquetes etiquetados.
LSR de contorno	<p>Puede recibir un paquete IP, efectúa consultas de Capa 3, e impone una pila de etiquetas antes de enviar el paquete dentro del dominio LSR.</p> <p>Puede recibir paquetes etiquetados, eliminar etiquetas, realizar consultas de Capa 3 y enviar el paquete IP hacia su siguiente salto.</p>
LSR ATM	Ejecuta protocolos MPLS en el plano de control para establecer circuitos ATM virtuales.

Envía paquetes etiquetados como celdas ATM.		
LSR contorno	ATM	de Puede recibir un paquete etiquetado o no etiquetado, segmentarlo en celdas ATM y enviar las celdas hacia el siguiente salto LSR ATM. Puede recibir celdas ATM de un LSR ATM adyacente, reensamblar estas celdas en el paquete original y después enviar el paquete como paquete etiquetado o no etiquetado.

1.8 IMPOSICIÓN DE ETIQUETAS EN EL CONTORNO DE LA RED

La imposición de etiquetas se ha descrito ya como un acto de adición de una etiqueta en un paquete, cuando éste entra en un dominio MPLS. Se trata de un a función de contorno, lo que significa que los paquetes se etiquetan antes de enviarse al dominio MPLS.

Para realizar esta función, un LSR de contorno debe comprender dónde se ha encabezado el paquete y qué etiqueta, o pila de etiquetas, se debería asignar al paquete. En un envío de etiqueta de Capa 3 convencional, cada salto en la red realiza una consulta en la tabla de envíos IP para la dirección de destino IP almacenada en la cabecera de Capa 3 del paquete. Selecciona una dirección IP de siguiente salto para el paquete en cada iteración de la consulta y, eventualmente, envía el paquete fuera de una interfaz hacia su destino final.

La elección del siguiente salto para el paquete IP es una combinación de dos funciones. La primera función separa el conjunto de paquetes posibles en un conjunto de prefijos de destino IP. La segunda función efectúa la asignación de

cada prefijo de destino IP a una dirección IP de siguiente salto. Esto significa que cada destino en la red se alcanza mediante una ruta respecto al flujo de tráfico que va desde un dispositivo de entrada hasta el dispositivo de salida de destino (podrían habilitarse múltiples rutas si el equilibrado de la carga se realiza utilizando rutas de costo equivalente o rutas de costo desigual, como ocurre con algunos protocolos IGP, como, por ejemplo, IGRP mejorado).

En la arquitectura MPLS, los resultados de la primera función se conocen como clases equivalentes de envío (FEC). Éstas vendrían a ser como un grupo de paquetes IP que se envían de la misma manera, por la misma ruta, y con idéntico tratamiento

Con el envío IP convencional, el procesamiento de paquetes se efectúa en cada salto en la red. No obstante, cuando se introduce MPLS, se asigna un paquete particular a una FEC particular una sola vez, y esto tiene lugar en el dispositivo de contorno a medida que el paquete entra en la red. La FEC a la que se asigna el paquete se codifica entonces como un identificador corto de longitud fija, conocido como etiqueta.

Cuando se envía un paquete al siguiente salto, se añade la etiqueta al final del paquete IP, de modo que el siguiente dispositivo en la ruta del paquete pueda enviarlo basándose en la etiqueta codificada en lugar de a través del análisis de la información de la cabecera de Capa 3. La Figura 1.5 ilustra todo el proceso de imposición y envío de etiquetas.

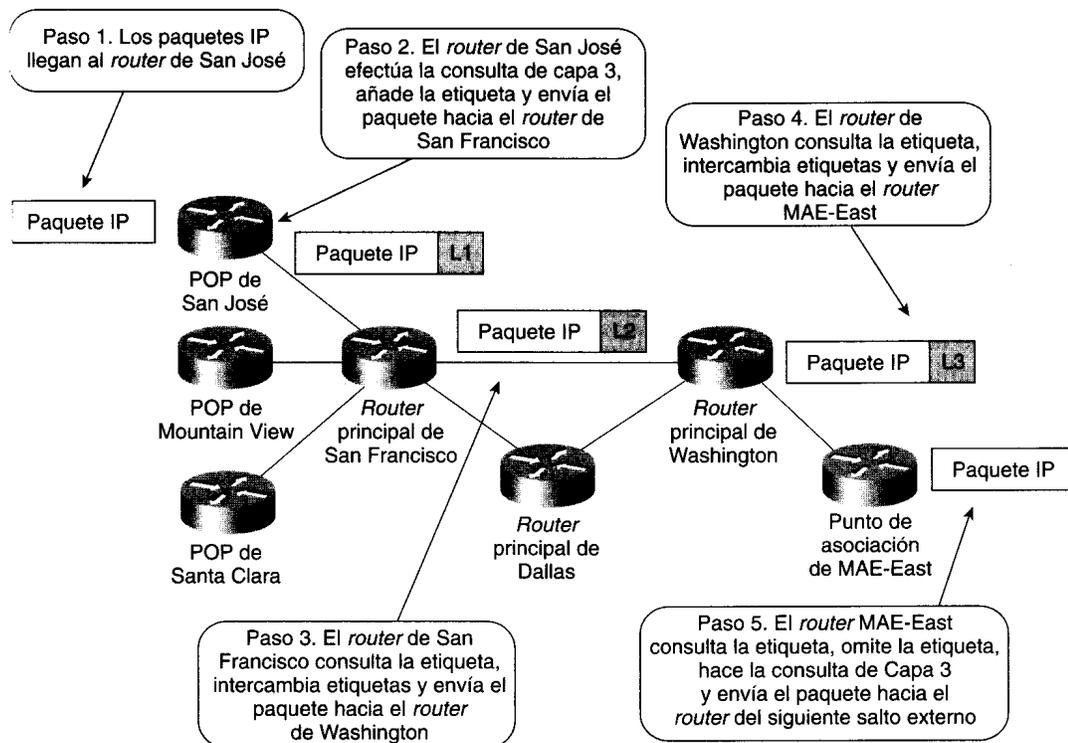


Figura 1.5. Imposición y envío de etiquetas MPLS.

1.9 ENVÍO DE PAQUETES MPLS Y RUTAS CONMUTADAS POR ETIQUETAS

Todos los paquetes entran en una red MPLS por un LSR de entrada y salen de la red MPLS por un LSR de salida. Este mecanismo crea lo que se conoce como ruta conmutada por etiquetas (LSP), que esencialmente describe el conjunto de LSR a través del cual debe pasar un paquete etiquetado para llegar al LSR de salida para una FEC particular. Esta LSP es unidireccional, lo que significa que se empleará una LSP diferente para el tráfico de retorno desde una FEC determinada.

La creación de la LSP es un esquema orientado a la conexión porque la ruta se establece antes que cualquier flujo de tráfico. Sin embargo, el establecimiento de esta conexión se basa en información topológica más que en la necesidad de un flujo de tráfico. Esto significa que la ruta se crea independientemente de si en ese momento hay tráfico esperando a pasar por la ruta hacia un conjunto particular de FEC.

A medida que el paquete atraviesa la red MPLS, cada LSR intercambia la etiqueta entrante por una etiqueta saliente, muy similar al mecanismo utilizado actualmente en ATM, donde el VPI/VCI se intercambia por un par VPI/VCI diferente cuando sale del switch ATM. Esto continúa hasta alcanzar el último LSR, conocido como LSR de salida.

Cada LSR mantiene dos tablas, que almacenan información relacionada con el componente de envío MPLS. La primera, conocida en el Cisco IOS como Base de información de etiquetas (TIB) y LIB en términos MPLS estándar, mantiene todas las etiquetas asignadas por este LSR y las asignaciones de estas etiquetas a las etiquetas recibidas de cualquiera de los vecinos. Estas asignaciones de etiquetas se distribuyen mediante el empleo de protocolos de distribución de etiquetas, que se explican con más detalle en el Capítulo 2.

Igual que múltiples vecinos pueden enviar etiquetas para el mismo prefijo IP aunque pudiera no ser el siguiente salto IP actualmente en uso en la tabla de enrutamiento para el destino, no todas las etiquetas de la TIB/LIB deben utilizarse para el envío de paquetes. La segunda tabla, conocida en el Cisco IOS como Base de información de envío de etiquetas (TFIB, y LFIB en términos MPLS estándar), se utiliza durante el envío de paquetes y almacena sólo las etiquetas que en ese momento está usando el componente de envío MPLS.

En términos del Cisco IOS y de la terminología del Envío expreso de Cisco (CEF) la arquitectura LSR de contorno de la Figura 1.4 podría rediseñarse como se muestra en la Figura 1.6 (se eligió un LSR de contorno debido a que su función es un superconjunto de un LSR que no es de contorno).

1.10 OTRAS APLICACIONES DE MPLS

La arquitectura MPLS, como se ha explicado hasta ahora, permite una perfecta integración de los routers tradicionales y de los switches ATM en un backbone IP unificado (arquitectura IP+ATM). Sin embargo, la verdadera fuerza de MPLS estriba en que ha dado origen a otras aplicaciones, desde la ingeniería del tráfico hasta las redes privadas virtuales igual a igual. Todas las aplicaciones MPLS utilizan la funcionalidad del plano de control, similar al plano de control de enrutamiento IP que se muestra en la Figura 1.6, para establecer la base de datos de conmutación de etiquetas. La Figura 1.7 expone la interacción existente entre estas aplicaciones y la matriz de conmutación de etiquetas

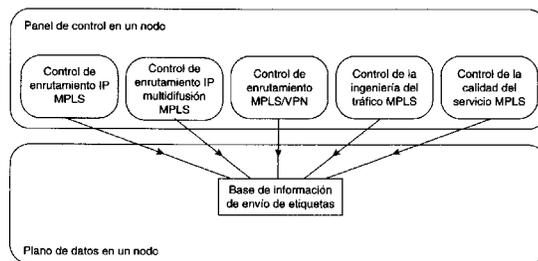


Figura 1.6. La arquitectura LSR de contorno utiliza términos del Cisco IOS.

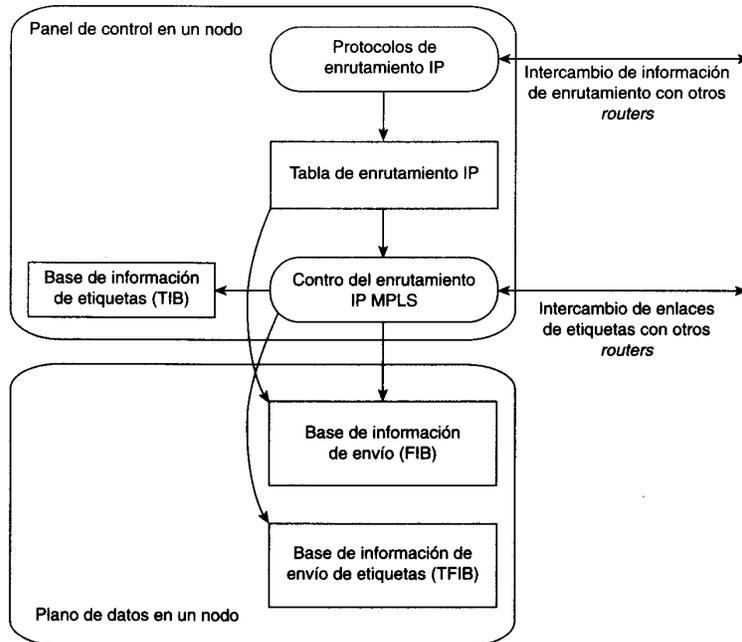


Figura 1.7. Diversas aplicaciones MPLS y sus interacciones

Cada aplicación MPLS tiene el mismo conjunto de componentes que la aplicación de enrutamiento IP:

- Una base de datos que define la tabla de clases equivalentes de envío (FEC) para la aplicación (la tabla de enrutamiento IP en una aplicación de enrutamiento IP).
- Los protocolos de control que intercambian los contenidos de la tabla FEC entre los LSR (protocolos de enrutamiento IP o enrutamiento estático en una aplicación de enrutamiento IP).

- El proceso de control que realiza el enlace de etiquetas a las FEC y un protocolo para intercambiar los enlaces de etiquetas entre los LSR (TDP o LDP en una aplicación de enrutamiento IP).
- Opcionalmente, una base de datos interna de asignación de etiquetas a las FEC (base de información de etiquetas en una aplicación de enrutamiento IP).

Cada aplicación utiliza su propio conjunto de protocolos para intercambiar la tabla FEC o la asignación FEC-a-etiqueta entre nodos. La Tabla 1.2 resume los protocolos y las estructuras de datos.

Tabla 1.2. Protocolos de control utilizados en diversas aplicaciones MPLS.

Aplicación	Tabla FEC	Protocolo de control utilizado para construir la tabla FEC	Protocolo de control utilizado para intercambiar la asignación FEC - a-etiqueta
Enrutamiento IP	Tabla de enrutamiento IP	Cualquier protocolo de enrutamiento IP	Protocolo de distribución de etiquetas (TDP o LDP)
Enrutamiento multidifusión IP	Tabla de enrutamiento multidifusión	PIM	Extensiones PIM versión 2

Enrutamiento VPN	Tabla de enrutamiento por cada VPN	La mayoría de los protocolos de enrutamiento IP entre el proveedor de servicios y el cliente, BGP multiprotocolo en la red del proveedor de servicios	BGP multiprotocolo
Ingeniería de tráfico	Definición de túneles MPLS	Definiciones de interfaz manual, extensiones a IS-IS u OSPF	RSVP o CR-LDP
Calidad del servicio MPLS	Tabla de enrutamiento IP	Protocolos de enrutamiento IP	Extensiones a TDP LDP

2. MPLS EN MODO TRAMA

En el Capítulo 1 vimos la arquitectura MPLS en general, así como los conceptos implícitos propios de la misma. Este capítulo aborda una aplicación en particular: el enrutamiento IP unidifusión basado en el destino en un entorno estrictamente de routers (llamado también MPLS en modo trama debido a que los paquetes etiquetados se intercambian como tramas en la Capa 2). El Capítulo 3 explica el enrutamiento IP unidifusión basado en destinos en el entorno ATM (llamado también MPLS en modo celda debido a que los paquetes etiquetados se transportan en celdas ATM).

Este capítulo aborda en primer lugar el plano de datos MPLS, asumiendo que las etiquetas es donde de alguna manera se establece un acuerdo entre los routers. La sección siguiente explica los mecanismos exactos empleados para distribuir las etiquetas entre los routers, y la última sección trata la interacción entre los protocolos de distribución de etiquetas, el Protocolo de gateway interior (IGP) y el Protocolo de gateway fronterizo (BGP) en una red de un proveedor de servicios.

A lo largo del capítulo se hace referencia a la arquitectura genérica de un router de conmutación de etiquetas MPLS (LSR), tal como se muestra en la Figura 2.1, y empleamos de ejemplo la red de un proveedor de servicios (denominado SuperNet), ilustrada en la Figura 2.2 para cualquier listado de código o depuración.

U red de SuperNet utiliza enlaces serie sin numerar basados en interfaces loopback que tienen las direcciones IP de la Tabla 2.1.

Tabla 2.1. Direcciones loopback en la red SuperNet

Router	Interfaz loopback
San José	172.16.1.1/32
Mountain View	172.16.1.2/32
Santa Clara	172.16.1.3/32
San Francisco	172.16.1.4/32
Dallas	172.16.2.1/32
Washington	172.16.3.1/32
Nueva York	172.16.3.2/32
MAE-East	172.16.4.1/32

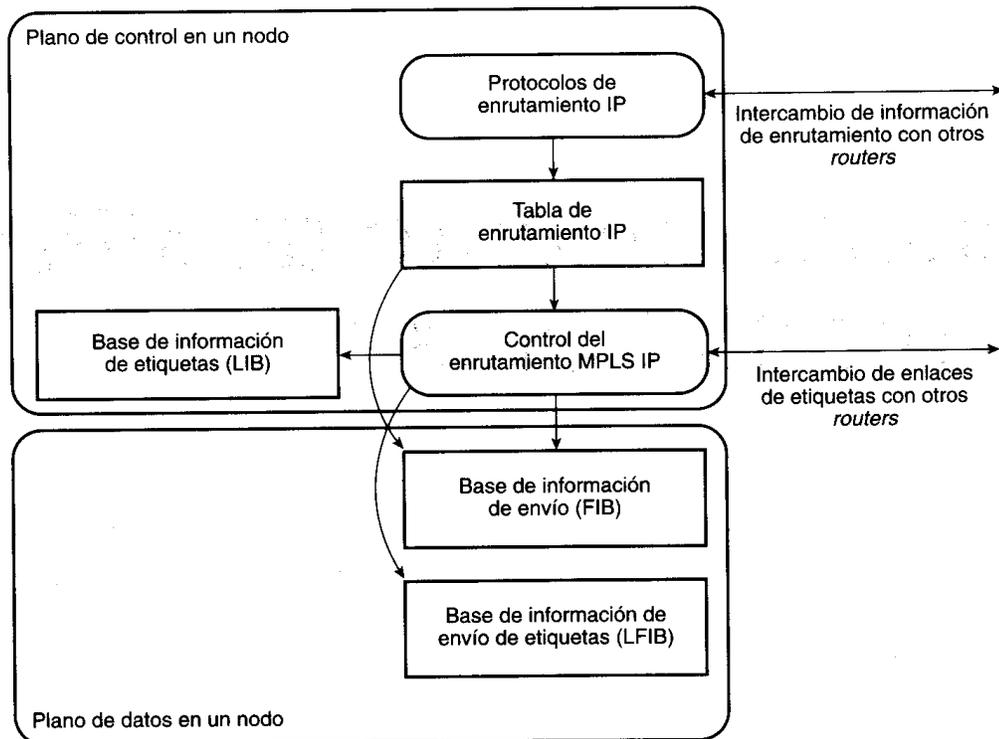


Figura 2.1. Arquitectura LSR de contorno.

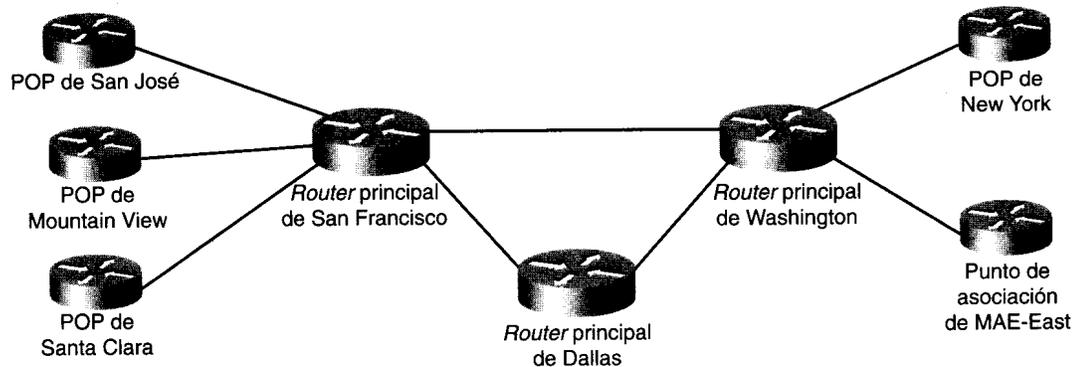


Figura 2.2. Red del proveedor de servicios SuperNet.

2.1 FUNCIONAMIENTO DEL PLANO DE DATOS EN MPLS EN MODO TRAMA

El Capítulo 1 describe brevemente la propagación de paquetes IP a través de un backbone MPLS. Se dan tres pasos principales en este proceso:

- El LSR de contorno de entrada recibe un paquete IP, clasifica el paquete en una clase equivalente de envío (FEC), y etiqueta el paquete con la pila de etiquetas de salida correspondiente a la FEC. Para el enrutamiento IP unidifusión basado en el destino, la FEC corresponde a la subred de destino y la clasificación del paquete es una consulta tradicional de Capa 3 en la tabla de envío.
- Los LSR principales reciben sus paquetes etiquetados y emplean las tablas de envío para intercambiar etiquetas entrantes en el paquete entrante con la etiqueta saliente correspondiente a la misma FEC (subred IP en este caso).

- Cuando el LSR de contorno de salida para esta FEC concreta recibe el paquete etiquetado, le quita la etiqueta y realiza una consulta tradicional de Capa 3 en el paquete IP resultante.

La Figura 2.3 muestra estos pasos realizados en la red de SuperNet para un paquete que atraviesa la red desde el POP de San José hacia un cliente conectado al POP de Nueva York.

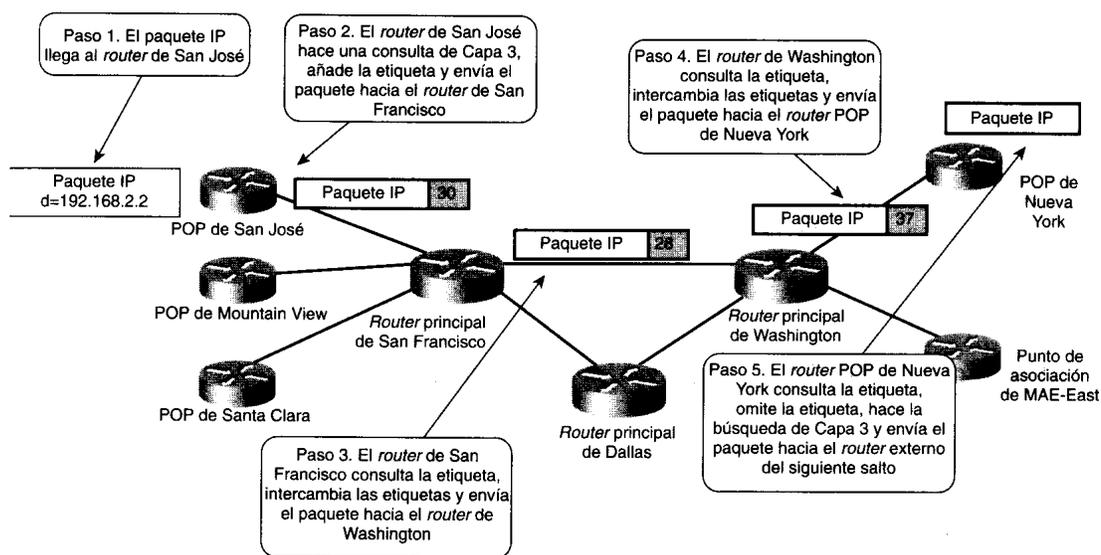


Figura 2.3. Envío de un paquete entre el POP de San José y el cliente de Nueva York.

El router POP de San José recibe un paquete con la dirección de destino 192.168.2.2 y realiza una consulta tradicional de Capa 3 a través de la tabla de envío IP (denominada también Base de información de envío [FIB]).

La entrada en la FIB (que se muestra en el Ejemplo 2.1) indica que el router POP de San José debería enviar el paquete IP que acaba de recibir como paquete etiquetado. Así, el router de San José impone la etiqueta "30" al paquete antes de que sea enviado al router de San Francisco, lo que supone la primera pregunta: ¿Dónde se impone la etiqueta y cómo sabe el router de San Francisco que el paquete recibido es un paquete etiquetado y no un paquete exclusivamente IP?

Ejemplo 2.1. Entrada CEF en el router POP de San José.

SanJose#show ip cef 192.168.2.0

192.168.2.0/24, version 11, cached adjacency to Serial1/0/1

0 packets, 0 bytes

 tag information set

 local tag: 29

 fast tag rewrite with Sel/0/11, point2point, tags imposed: {30}

 via 172.16.1.4, Serial1/0/1, 0 dependencies

 next hop 172.16.1.4, Serial1/0/1

 valid cached adjacency

 tag rewrite with Sel/0/11, point2point, tags imposed: {30}

2.2 CABECERA DE LA PILA DE ETIQUETAS MPLS.

Por varios motivos, siendo único el rendimiento de la conmutación, la etiqueta MPLS se debe insertar por delante de los datos etiquetados en una implementación en modo trama de la arquitectura MPLS. La etiqueta MPLS se inserta así entre la cabecera de Capa 2 y los contenidos de la Capa 3 de la trama de Capa 2, como se muestra en la **Figura 2.4.**

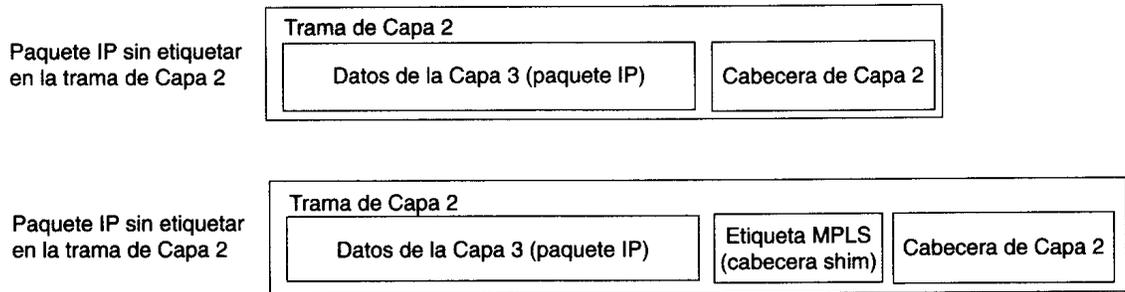


Figura 2.4. Posición de la etiqueta MPLS en una trama de Capa 2.

Debido a la forma en que se inserta la etiqueta MPLS entre el paquete de Capa 3 y la cabecera de Capa 2, la cabecera de la etiqueta MPLS se denomina cabecera shim. La cabecera de la etiqueta MPLS (detallada en la Figura 2.5) contiene la etiqueta MPLS (20 bits), la información de clase de servicio (tres bits, llamados también bits experimentales en la documentación del IETF sobre MPLS) y el campo de ocho bits Tiempo de existencia (TTL) (que tiene funciones idénticas en cuanto a la detección de bucles que el campo IP TTL) y un bit llamado parte inferior de la pila.

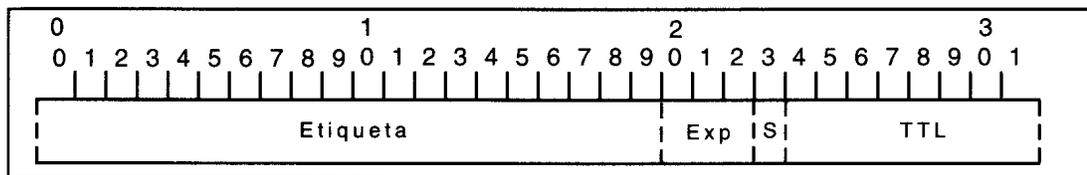


Figura 2.5. Cabecera de la pila de etiquetas MPLS.

La parte inferior de la pila se implementa como una pila de etiquetas MPLS, que en el Capítulo 1 se define como la combinación de dos o más cabeceras de

etiquetas unidas a un solo paquete. El enrutamiento IP unidifusión simple no utiliza la pila de etiquetas, pero otras aplicaciones MPLS, incluyendo las redes privadas virtuales basadas en MPLS o la ingeniería del tráfico MPLS, confían enormemente en ellas.

Con la cabecera de la pila de etiquetas MPLS insertada entre la cabecera de Capa 2 y la sobrecarga de la Capa 3, el router de envío debe tener algunos medios para indicar al router receptor que el paquete que se transmite no es un datagrama IP puro, sino un paquete etiquetado (un datagrama MPLS). Para facilitar esta tarea, se han definido nuevos tipos de protocolos que se definen sobre la Capa 2, del modo siguiente:

- En entornos LAN, los paquetes etiquetados que transportan paquetes de Capa 3 unidifusión y multidifusión usan valores ethertype tales como 8847 hex y 8848 hex. Estos valores ethertype pueden utilizarse directamente en medios Ethernet (incluyendo Fast Ethernet y Gigabit Ethernet) y también como parte de la cabecera SNAP en otro medio LAN (incluyendo Token Ring y FDDI).
- En los enlaces punto a punto que emplean la encapsulación PPP, se introdujo un nuevo Protocolo de control de la red (NCP) denominado Protocolo de control MPLS (MPLSCP). Los paquetes MPLS están marcados con el protocolo PPP, cuyo valor de campo es 8281 hex.
- Los paquetes MPLS transmitidos a través de un DLCI Frame Relay entre un par de routers se marcan con el IP de protocolo de capa de red Frame Relay SNAP (NLPID), seguido de una cabecera SNAP con el valor ethertype 8847 hex.

- Los paquetes MPLS transmitidos entre un par de routers por un circuito virtual Foro ATM se encapsulan con una cabecera SNAP que utiliza valores ethertype iguales a los utilizados en un entorno LAN.

La Figura 2.6 muestra el resumen de las técnicas de encapsulación MPLS.

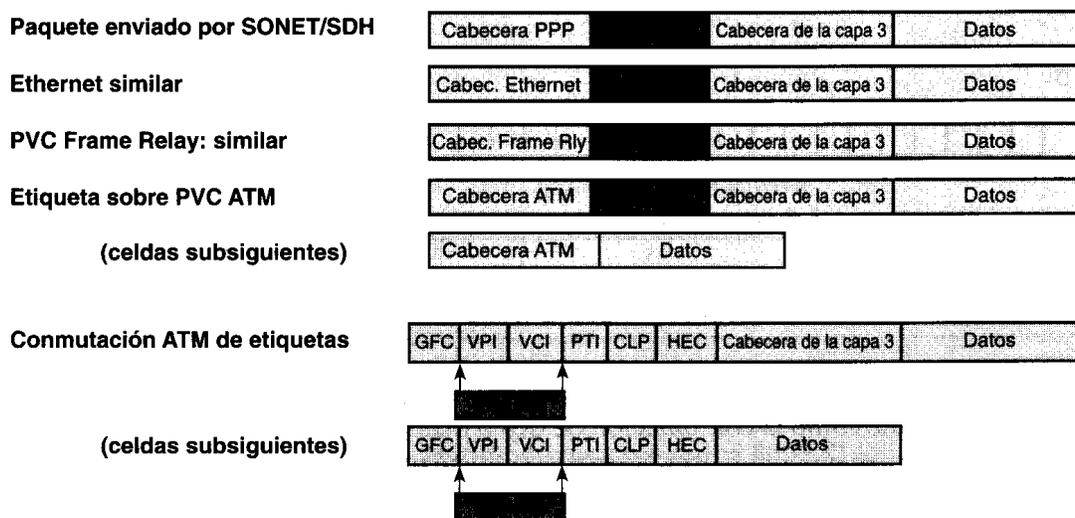


Figura 2.6. Resumen de las técnicas de encapsulación MPLS.

El router de San José del ejemplo que se ilustra en la Figura 2.3 inserta la etiqueta MPLS en el frontal del paquete IP que acaba de recibir, encapsula el paquete etiquetado en una trama PPP con un valor de campo de protocolo PPP de 8281 hex, y envía la trama de Capa 2 hacia el router de San Francisco.

2.3 CONMUTACIÓN DE ETIQUETAS EN MPLS EN MODO TRAMA

Después de recibir la trama PPP de Capa 2 desde el router de San José, el router de San Francisco inmediatamente identifica el paquete recibido como un paquete etiquetado basándose en el valor del campo de protocolo PPP y realiza una consulta de etiqueta en su Base de información de envío de etiquetas (LFIB).

La entrada LFIB, correspondiente a la etiqueta 30 de entrada (y visualizada en el Ejemplo 2.2), conduce al router de San Francisco a reemplazar la etiqueta 30 por una etiqueta 28 saliente y a propagar el paquete hacia el router de Washington.

Ejemplo 2.2. Entrada LFIB para la etiqueta 30 en el router de San Francisco.

SanFrancisco#**show tag forwarding-table tags 30 detail**

Local tag	Outgoing tag	Prefix or VC or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
30	28	192.168.2.0/24	0	Se0/0/1	172.16.3.1

MAC/Encaps=14/18, MTU=1504, Tag Stack{28}
00107H59E2000107BEC6BO08847 0001CO00

Per-packet load-sharing

El paquete etiquetado se propaga de manera similar a través del backbone de SuperNet hasta que alcanza el POP de Nueva York, donde la entrada LFIB indica al router de Nueva York omitir la etiqueta y envíe el paquete sin etiquetar (véase el Ejemplo 2.3).

Ejemplo 2.3. Entrada LFIB en el router de Nueva York.

NewYork#show tag forwarding-table tags 37 detail

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
37	untagged	192.168.2.0/24	0	Se2/1/3	192.168.2.1

MAC/Encaps=0/0, MTU=1504, Tag Stack{}

Per-packet load-sharing

Un router Cisco ejecutando el software Cisco IOS y operando como un LSR MPLS en MPLS en modo trama, puede realizar varias acciones sobre un paquete etiquetado:

- Acción pop de etiqueta (omisión de la etiqueta). Elimina la etiqueta superior de la pila de etiquetas MPLS y propaga la sobrecarga restante, ya sea como un paquete etiquetado (si el bit de la parte inferior de la pila es cero) o como un paquete IP sin etiquetar (el campo Tag Stack de la LFIB esta vacío).
- Intercambiar la etiqueta. Sustituye la etiqueta superior de la pila de etiquetas MPLS por otro valor (el campo Tag Stack de la LFIB es una etiqueta larga).
- Acción push de etiqueta. Sustituye la etiqueta superior de la pila de etiquetas MPLS por un conjunto de etiquetas (el campo Tag Stack de la LFIB contiene varias etiquetas).
- Agregar. Elimina la etiqueta superior de la pila de etiquetas MPLS y hace una búsqueda de Capa 3 en el paquete IP subyacente. La etiqueta eliminada es la etiqueta de la parte inferior de la pila de etiquetas MPLS; de lo contrario, se descarta el datagrama.

- Desetiquetar. Elimina la etiqueta superior de la pila de etiquetas MPLS y envía el paquete IP subyacente al siguiente salto IP especificado. La etiqueta eliminada es la etiqueta de la parte inferior de la pila de etiquetas MPLS; de lo contrario, se descarta el datagrama.

2.4 CONMUTACIÓN DE ETIQUETAS MPLS CON LA PILA DE ETIQUETAS

La operación de conmutación de etiquetas se realiza de la misma forma, independientemente de que el paquete etiquetado contenga sólo una etiqueta o una pila de etiquetas con varias etiquetas profundas. En ambos casos, el LSR que conmuta el paquete actúa sólo en la etiqueta superior de la pila, ignorando las demás etiquetas. Esta función permite habilitar diversas aplicaciones MPLS en las que los routers de contorno pueden acordar unas reglas de clasificación de paquetes y etiquetas asociadas sin conocimiento de otros routers principales.

Por ejemplo, asumamos que el router de San José y el router de Nueva York de la red de SuperNet soportan redes privadas virtuales basadas en MPLS y que han acordado que a la red 10.1.0.0/16, que se puede alcanzar a través del router de Nueva York, se le asigna un valor de etiqueta de 73. Los routers principales en la red de SuperNet (San Francisco y Washington) no están al tanto de tal cosa.

Para enviar un paquete a un host de destino en la red 10.1.0.0/16, el router de San José construye una pila de etiquetas. La etiqueta de la parte inferior de la pila es la etiqueta acordada con el router de Nueva York, y la etiqueta superior de la pila es la etiqueta asignada a la dirección IP del router de Nueva York por el router de San Francisco. Cuando la red propaga el paquete (como se ilustra en la Figura 2.7), la etiqueta superior se conmuta exactamente como en el ejemplo en que un

paquete IP puro se ha propagado a través del backbone y la segunda etiqueta de la pila alcanza intacta el router de Nueva York.

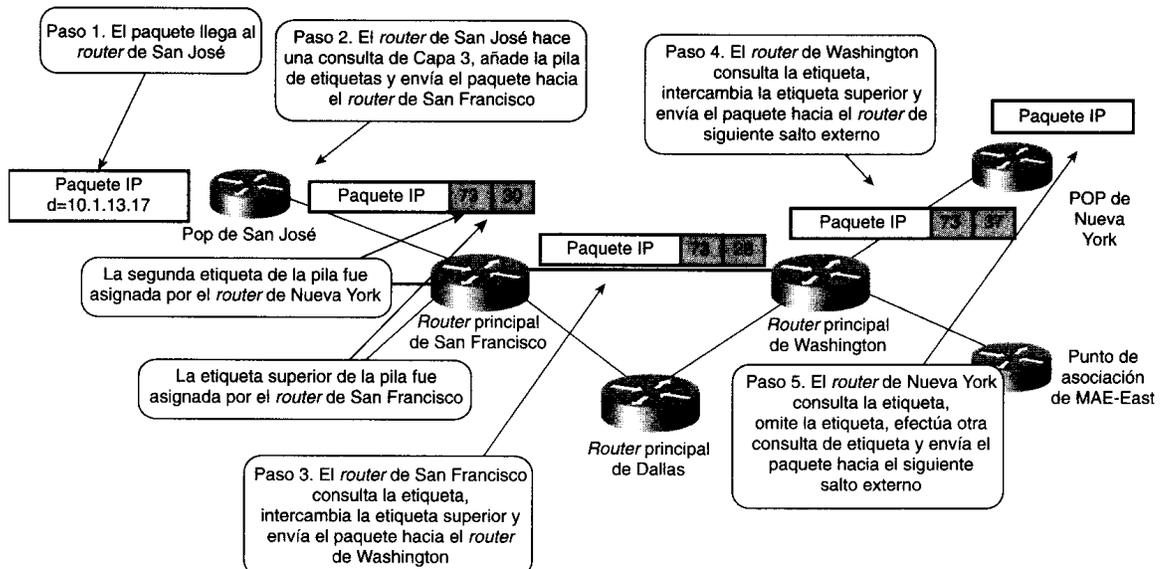


Figura 2.7. Conmutación de etiquetas con la pila de etiquetas MPLS.

2.5 ENLACES DE ETIQUETAS Y PROPAGACIÓN EN MPLS EN MODO TRAMA

La sección anterior identifica los mecanismos necesarios para enviar paquetes etiquetados entre los LSR utilizando interfaces tramadas (LAN, enlaces punto a punto o circuitos virtuales WAN). Esta sección está dedicada a los enlaces FEC a etiqueta y su propagación entre los LSR sobre interfaces tramadas.

El software Cisco IOS implementa dos protocolos de enlace de etiquetas que pueden emplearse para asociar subredes IP con etiquetas MPLS con la finalidad de un enrutamiento unidifusión basado en destinos:

- **TDP (antiguo Protocolo de distribución de etiquetas).** El protocolo patentado por Cisco disponible en el software IOS versión 11.1CT, así como en la 12.0 y todas las versiones del IOS siguientes.
- **LDP (Protocolo de distribución de etiquetas).** El protocolo de enlace de etiquetas estándar del IETF disponible en la versión 12.2T.

TDP y LDP son funcionalmente equivalentes y se pueden utilizar simultáneamente en la red, aún con diferentes interfaces del mismo LSR. Debido a su equivalencia funcional, esta sección muestra sólo los comandos de depuración y monitorización TDP.

Los comandos que figuran en la Tabla 2.2 se emplean para iniciar el etiquetado de paquetes MPLS para los paquetes IP unidifusión y los protocolos asociados en una interfaz.

Tabla 2.2. Comandos de configuración del IOS utilizados para iniciar MPLS en una interfaz.

Tarea	Comando IOS
Inicia el etiquetado de paquetes MPLS y ejecuta TDP en la interfaz especificada.	tag-switching ip
Selecciona el protocolo de distribución de etiquetas en la interfaz especificada.	mpls label-distribution [ldp tdp both]

2.6 ESTABLECIMIENTO DE LA SESIÓN LDP/TDP

Cuando se inicia MPLS en la primera interfaz de un router, se inicia el proceso TDP/LDP y se crea la estructura de la Base de información de etiquetas (LIB). El router trata también de descubrir otros LSR en las interfaces ejecutando MPLS a través de los paquetes hello TDP. Estos paquetes hello TDP se envían como paquetes UDP difusión o multidifusión, haciendo que el descubrimiento del LSR vecino sea automático. El comando `debug tag tdp transport` puede monitorizar los hellos TDP. El Ejemplo 2.4 muestra el inicio del proceso TDP y el Ejemplo 2.5 ilustra el establecimiento correcto de un TDP adyacente.

Ejemplo 2.4. Inicio TDP después de configurarla primera interfaz para MPLS.

```
SanFrancisco#debug tag tdp transport
```

```
TIDP transport events debugging is on
```

```
SanFrancisco#conf t
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
SanFrancisco(config)#interface serial 1/0/1
```

```
SanFrancisco(config-subif)#tag-switching ip
```

```
1d20h: enabling tdp on Serial1/0/1
```

```
1d20h: tdp: 1<tdp_start: tdp_process_ptr = 0x80137826C
```

```
1d20h: tdp: tdp_set - intf - id: intf 0x80E491374, Serial1/0/1, not tc-atm, intf_id 0
```

```
1d20h: enabling tdp on Serial1/0/1
```

```
1d20h: tdp: Got TDP Id
```

```
1d20h: tdp: Got TDP TCP Listen socket
```

```
1d20h: tdp: tdp_hello_process tdp initd
```

```
1d20h: tdp: tdp_hello_process start hello for Serial1/0/1
```

```
1d20h: tdp: Got TIDP UDP socket
```

Ejemplo 2.5. Descubrimiento de un vecino TDP.

```
1d20h: tdp: Send hello; Serial1/0/1, src/dst 172.16.11.4/255.255.255.255, inst_id 0
1d20h: tdp: Rcvd hello; Serial1/0/ 1 , from 172.16.1.1 (172.16.1 .1 : 0) , intf_id 0,
opt
0x4
1d20h: tdp: Hello from 172.16.1.1 (172.16.1.1:0) to 255.255.255.255, opt 0x4
```

También se pueden presentar casos en los que un LSR adyacente quiera establecer una sesión LDP o TDP con el LSR bajo consideración, pero la interfaz que les conecta no esté configurada para MPLS debido a razones de seguridad u otras de tipo administrativo. En tal caso, la salida de la depuración es similar al listado que se muestra en el Ejemplo 2.6 y muestra los paquetes hello ignorados que se han recibido a través de las interfaces en las que no se ha configurado MPLS.

Ejemplo 2.6. Establecimiento de la sesión TDP.

```
ld20h: tdp: New adj 0x80EA92D4 from 172.16.1.1 (172.16.1.1:0), Serial1/0/1
ld20h: tdp: Opening conn; adj 0x80EA92D4, 172.16.1.4 <-> 172.16.1.1
ld20h: tdp: Conn is up; adj 0x80EA92D4, 172.16.1.4:11000 <-> 172.16.1.1:711
ld20h: tdp: Sent open PIE to 172.16.1.1 (pp 0x0)
ld20h: tdp: Rcvd open PIE from 172.16.1.1 (pp 0x0)
```

Después de establecerse la sesión TDP, es monitorizada constantemente con los paquetes activos TDP para asegurar que aún sigue funcionando. El Ejemplo 2.7 muestra el paquete activo TDP.

Ejemplo 2.7. Activos TDP

```
ld20h: tdp: Sent keep_alive PIE to 172.16.1.1:0 (pp 0x0)
```

```
ld20h: tdp: Rcvd keep_alive PIE from 172.16.1.1:0 (pp 0x0)
```

Los vecinos TDP y el estatus de las sesiones TDP individuales también se pueden monitoriar con el comando `show tag tdp neighbor`, como se muestra en el Ejemplo 2.8. Este listado se tomó en el momento en que el router de San José era el único vecino TDP del router de San Francisco.

Ejemplo 2.8. Muestra del listado del vecino TDP

```
SanFrancisco#show tag-switching tdp neighbor
```

```
Peer TDP Ident: 172.16.1.1:0; Local TDP Ident 172.16.1.4:0
```

```
TCP connection: 172.16.1.1.711 - 172.16.1.4.11000
```

```
State: Oper; PIEs sent/rcvd: 4/4; ; Downstream
```

```
Up time: 00:01:05
```

```
TDP discovery sources:
```

```
Serial/0.1
```

```
Addresses bound to peer TDP Ident:
```

```
172.16.1.1
```

El comando visualiza los identificadores TDP de los routers local y remoto, la dirección IP y los números de los puertos TCP entre los que se ha establecido la conexión TDP, la conexión uptime y las interfaces a través de las cuales se ha descubierto el vecino TDP, así como la dirección IP de la interfaz utilizada por el vecino TDP.

2.7 DISTRIBUCIÓN Y ENLACE DE ETIQUETAS

Tan pronto como se crea la base de información de etiquetas (LIB) en un router, se asigna una etiqueta a cada clase equivalente de envío conocida por el router. Para el enrutamiento unidifusión basado en el destino, la FEC es equivalente a un prefijo IGP en la tabla de enrutamiento IP. Así, la etiqueta se asigna a cada prefijo en la tabla de enrutamiento IP y se guarda en la LIB la asignación que hay entre los dos.

La base de información de etiquetas siempre se mantiene sincronizada con la tabla de enrutamiento IP: en cuanto aparece una nueva ruta que no es BGP en la tabla de enrutamiento IP, se asigna y enlaza una nueva etiqueta a la nueva ruta. Los listados de debug tag tc1p bindings muestran el enlace subred a etiqueta. El Ejemplo 2.9 muestra un listado de ejemplo.

Ejemplo 2.9. Enlaces etiqueta a prefijo de ejemplo.

```
SanFrancisco#debug tag-switching tdp bindings
TDP Tag Information Base (TIB) changes debugging is on
ld20h: tagcon: tibent(172.16.1.4/32): created; find route tags request
ld20h: tagcon: tibent(172.16.1.4/32): 1cl tag 1 (#2) assigned
ld20h: tagcon: tibent(172.16.1.1/32): created; find route tags request
ld20h: tagcon: tibent(172.16.1.1/32): 1cl tag 26 (#4) assigned
ld20h: tagcon: tibent(172.16.1.3/32): created; find route tags request
ld20h: tagcon: tibent(172.16.1.3/32): lcl tag 27 (#6) assigned
ld20h: tagcon: tibent(172.16.1.2/32): created; find route tags request
ld20h: tagcon: tibent(172.16.1.2/32): 1cl tag 28 (#8) assigned
ld20h: tagcon: tibent(192.168.1.0/24): created; find route tags request
ld20h: tagcon: tibent(192.168.1.0/24): lcl tag 1 (#10) assigned
ld20h: tagcon: tibent(192.168.2.0/24): created; find route tags request
```

ld20h: tagcon: tibent(192.168.2.0/24): lcl tag 29 (#12) assigned

Debido a que el LSR asigna una etiqueta a cada prefijo IP en su tabla de enrutamiento en cuanto aparece el prefijo en la tabla de enrutamiento, y la etiqueta la utilizan otros LSR para enviar los paquetes etiquetados hacia el LSR que realiza la asignación, este método de asignación y distribución de etiquetas se denomina control independiente de la etiqueta con distribución de etiquetas de flujo descendente no solicitado:

- La asignación de etiquetas en los routers se efectúa independientemente de si el router ya ha recibido o no una etiqueta para el mismo prefijo de su siguiente salto. Por ello, la asignación de etiquetas en los routers se denomina control independiente.
- El método de distribución no es solicitado porque el LSR asigna la etiqueta y publica la asignación a los vecinos de flujo ascendente independientemente de si otros LSR necesitan la etiqueta. La otra posibilidad es disponer del método de distribución bajo demanda. Un LSR sólo asigna una etiqueta a un prefijo IP y la distribuye a los vecinos de flujo ascendente cuando le es solicitada. El Capítulo 3 explica este método con mayor detalle.
- El método de distribución es de flujo descendente cuando el LSR asigna una etiqueta que pueden utilizar otros LSR (LSR de flujo ascendente) para enviar paquetes etiquetados y publica estas asignaciones de etiquetas a sus vecinos. La arquitectura de conmutación de etiquetas inicial dispone también de recursos para la distribución de etiquetas de flujo ascendente,

pero ni la implementación de la conmutación de etiquetas actual ni la arquitectura MPLS necesitan este tipo de método de distribución.

Todos los enlaces de etiquetas se publican inmediatamente a todos los demás routers a través de las sesiones TDP. Las publicaciones también pueden examinarse mediante comandos de depuración. El listado se tomó en el router de San Francisco después de que la ruta hacia 192.168.2.0/24 se propagara desde Nueva York a San Francisco vía IGP y fuera introducida en la tabla de enrutamiento del LSR de San Francisco.

Ejemplo 2.10. Entrada de la base de información de etiquetas en el router de San Francisco,

```
SanFrancisco#show tag-switching tdp bindings 192.168.2.0
```

```
  tib entry: 192.168.2.0/24, rev 7
```

```
    local binding: tag: 30
```

```
    remote binding: tsr: 172.16.1.1:0, tag: 33
```

```
    remote binding: tsr: 172.16.1.2:0, tag: 35
```

```
    remote binding: tsr: 172.16.1.3:0, tag: 23
```

```
    remote binding: tsr: 172.16.2.1:0, tag: 59
```

```
    remote binding: tsr: 172.16.3.1:0, tag: 28
```

```
SanFrancisco#
```

El router podría recibir enlaces TDP de varios vecinos, pero sólo utiliza algunos de ellos en las tablas de envío, como se explica a continuación:

- El enlace de etiqueta desde el router de siguiente salto se introduce en la entrada FIB correspondiente. Si el router no recibe el enlace de etiqueta del

router de siguiente salto, la entrada FIB especifica que los paquetes para este o aquel destino deberían enviarse sin etiquetar.

- Si el router recibe un enlace de etiqueta desde el router de siguiente salto, la etiqueta local y la etiqueta de siguiente salto se introducen en la LFIB. Si el router de siguiente salto no asigna una etiqueta al prefijo correspondiente, la acción de salida en la LFIB no está etiquetada. El Ejemplo 2.11 muestra ambos casos.

Ejemplo 2.11. Información de envío de etiquetas en el router de San Francisco,

```
SanFrancisco#show tag forwarding-table tags 30-31
```

Local tag	Outgoing tag or VC	Prefix or Tunnel Id	Bytes tag switched	Outgoing interface	Next Hop
30	28	192.168.2.0/32	0	Se0/0/1	172.16.3.1
31	untagged	192.168.100.4/32	0	Se1/0/3	172.16.1.3

2.8 CONVERGENCIA EN UNA RED MPLS EN MODO TRAMA

Un aspecto importante de las redes MPLS es el tiempo de convergencia de la red. Algunas aplicaciones MPLS (por ejemplo, un diseño MPLS/VPN o BGP basado en MPLS) no operan correctamente a menos que se pueda enviar un paquete etiquetado a lo largo de todo el trayecto, desde el LSR de contorno de entrada hasta el LSR de contorno de salida. En estas aplicaciones, el tiempo de convergencia necesario para el Protocolo de gateway interior , IGP) para converger en torno a un fallo en la red principal puede aumentarse retrasando la propagación de la etiqueta.

En una red MPLS en modo trama, si se utiliza el modo de retención liberal, en combinación con el control de etiqueta independiente y la distribución de etiquetas de flujo descendente no solicitada, se minimiza el retraso de convergencia TDP/LDP. Cada router que emplea el modo de retención liberal, normalmente tiene asignaciones de etiqueta para un prefijo dado desde todos sus vecinos TDP/LDP, de manera que siempre pueda encontrar una etiqueta de salida apropiada siguiendo la convergencia de la tabla de enrutamiento sin preguntar a su nuevo router de siguiente salto acerca de la asignación de etiqueta.

Los ejemplos siguientes se basan en un escenario de fallo (el enlace entre Washington y San Francisco no responde) en la red de SuperNet, ilustrando la convergencia inmediata. Los ejemplos solamente tienen en cuenta la ruta hacia la red 192.168.100.2/32, adjunta al router de Nueva York.

Los listados del comando show (véase el Ejemplo 2.11) en el estado inicial indican que la ruta objetivo se alcanza a través de la interfaz Serial0/0/1 a través del siguiente salto 172.16.3.1.

Ejemplo 2.12. Escaneo de la LFIB después de producirse el fallo del enlace.

```
SanFrancisco#sh debug
```

```
IP routing:
```

```
    IP routing debugging is on
```

```
Tag Switching:
```

```
    TDP Tag Information Base (TIB) changes debugging is on
```

```
    TIDP tag and address advertisements debugging is on
```

```
    Cisco Express Forwarding related TIFIB services debugging is on
```

```
SanFrancisco#
```

```
3d03h: %LINK-5-CHANGED: Interface Serial0/0/1, changed state to down
```

```
3d03h: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial0/0/1,
changed state to down
3d03h: TFIB: fib scan start:needed:1,unres:0,mac:0,mtu:,loadinfo:0,scans aborted
0
3d03h: TFIB: fib check cleanup for 192.168.100.2/32,index=0,return-value=0
3d03h: TFIB: fib-scanner-walk,resolve path 0 of 192.168.100.2132
3d03h: TFIB: resolve tag rew, pref ix=192.168.100.2/32, has tag_info,no parent
3d03h: TFIB: finish fib res 192.168.100.21/32:index 0,parent outg tag no parent
3d03h: TFIB: set fib rew: pfx 192.168.100.2/32,index=0,add=1,tag rew-adj=Serial
0/0/1
3d03h: TFIB: Update TFIB for 192.168.100.2132, fib no loadinfo, tfib no
loadinfo, per_pkt,resolved=1
3d03h: TFIB: fib_scanner_end
```

La interfaz averiada se elimina entonces de la tabla de enrutamiento y las rutas asociadas también se eliminan de la tabla de enrutamiento IP. Debido a que no existe actualmente una ruta alternativa de igual costo hacia 192.168.100.2/32, se elimina la ruta completamente de la tabla de enrutamiento y la entrada asociada se borra de la LFIB (véase el Ejemplo 2.13).

Ejemplo 2.13. Tabla de enrutamiento y limpieza de la LFIB.

```
3d03h: RT: interface Serial0/0/1 removed from routing table
3d03h: RT: delete route to 192.168.100.2 via 0.0.0.0, Serial0/0/1
3d03h: RT: no routes to 192.168.100.2, flushing
3d03h: TFIB: tfib_fib_delete,192.168.100.2/32,fib->count=1
3d03h: TFIB: fib complete delete: prefix=192.168.100.2/32,inc tag=28,del info=1
3d03h: TFIB: deactivate tag rew for 192.168.100.2/32,index=0
3d03h: TFIB: Update TFIB for 192.168.100.2132, fib no loadinfo, tfib no loadinfo,
```

```
per_pkt,resolved=0
```

```
3d03h: TFIB: set fib rew: pfx 192.168.100.2/32,index=0,add=0,tag_rew-adj=Serial  
0/0/1
```

Una ruta alternativa hacia 192.168.100.2 pasa por el router de Denver. El proceso OSPF instala de inmediato la ruta alternativa en la tabla de enrutamiento. Se crean las entradas CEF y LFIB correspondientes y la entrada LFIB obtiene la etiqueta asignada por 172.16.2.1 (el router de Denver) como su etiqueta de salida. La nueva entrada LFIB se instala sin ninguna interacción TDP/LDP con los vecinos TDP/LDP (véase el Ejemplo 2.14).

Ejemplo 2.14. La ruta alternativa se instala en la tabla de enrutamiento,

```
3d03h: RT: add 192.168.100.2/32 via 172.16.2.1, ospf metric [110/21]  
3d03h TFIB: post table chg,ROUTE - LIP 192.168.100.2/32,loadinfo ct=1  
3d03h TFIB: find_rt_tgs,192.168.100.2/32, meth 1,res_next_hop=172.16.2.1,  
Se0/0/2 ,next_hop 172.16.2.1  
3d03h: TFIB: route tag chg 192.168.100.2/32,idx=0,inc=28,outg=28,enabled=0x1  
3d03h TFIB: create tag info 192.168.100.2/32,inc tag=28,has no info  
3d03h: TFIB: resolve tag rew,prefix=192.168.100.2/32,has tag_info,no parent  
3d03h TFIB: finish fib res 192.168.100.2/32:index 0,parent outg tag no parent  
3d03h TIFIB: set fib rew: pfx 192.168.100.2/32,index=0,add=1,tag_rew-  
>adj=FastEt hernet0/0  
3d03h TFIB: Update TFIB for 192.168.100.2/32, fib no loadinfo, tfib no loadinfo  
per_pkt,resolved=1
```

Como último paso, todas las entradas desde el vecino TDP 172.16.3.1 (el router de Washington), que ya es inalcanzable, se eliminan de la base de información de etiquetas (véase el Ejemplo 2.15).

Ejemplo 2.15. Se eliminan las entradas LIB recibidas desde el router de Washington.

```
3d03h tagcon: tibent(192.168.100.2/32): rem tag 1 from 172.16.3.1:0 removed
```

```
3d03h tagcon: no route_tag_change for: 192.168.100.2/32
```

```
    for tsr 172.16.3.1:0: tsr is not next hop
```

```
3d03h: TFIB: resolver repetición: compartir reescritura de matriz 192.168.100.2/32
```

2.9 OMISIÓN DEL PENÚLTIMO SALTO

Un LSR de contorno de salida en una red MPLS podría tener que realizar dos consultas en un paquete recibido de un MPLS vecino y destinado para una subred fuera del dominio MPLS. Debe inspeccionar la etiqueta de la cabecera de la pila de etiquetas y consultar la etiqueta sólo para advertir que tiene que omitir la etiqueta e inspeccionar el paquete IP subyacente. Tendrá que efectuar otra consulta de Capa 3 adicional en el paquete IP antes de que pueda enviarlo a su destino final. La Figura 2.8 muestra el proceso correspondiente en la red de SuperNet.

La consulta doble en el router POP de Nueva York podría reducir el rendimiento de dicho nodo. Más aún, en entornos donde la conmutación IP y MPLS se realizan en hardware, el hecho de que pudiera realizarse una doble búsqueda podría incrementar significativamente la complejidad de la implementación del hardware. Por ello, se ha introducido en la arquitectura MPLS la omisión del penúltimo salto (PHP).

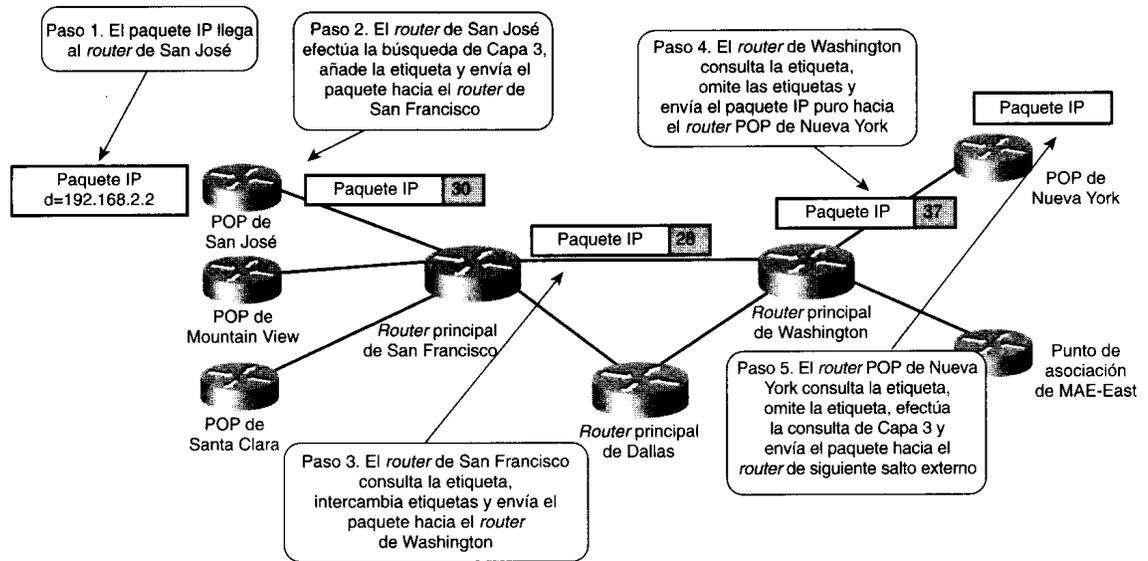


Figura 2.8. Doble búsqueda en el router POP de Nueva York.

Con la omisión del penúltimo salto, el LSR de contorno puede solicitar una operación de omisión de etiqueta desde sus vecinos de flujo ascendente. En la red de SuperNet, el router de Washington omite la etiqueta del paquete (paso 4 en la Figura 2.9) y envía un paquete P puro al router de Nueva York. Entonces, el router de Nueva York efectúa una búsqueda simple de Capa 3 y envía el paquete hacia su destino final (paso 5 en la Figura 2.9).

La omisión del penúltimo salto se solicita a través de TDP o LDP utilizando un valor de etiqueta especial (1 para TDP, 3 para LDP) que también se conoce como valor nulo implícito.

Cuando el LSR de salida solicita la omisión del penúltimo salto para un prefijo IP, la entrada LIB local en el LSR de salida y la entrada LIB remota en los LSR de flujo ascendente indican el valor imp-null, y la entrada LFIB del penúltimo LSR indica una operación de omisión de etiqueta (véase el Ejemplo 2.16).

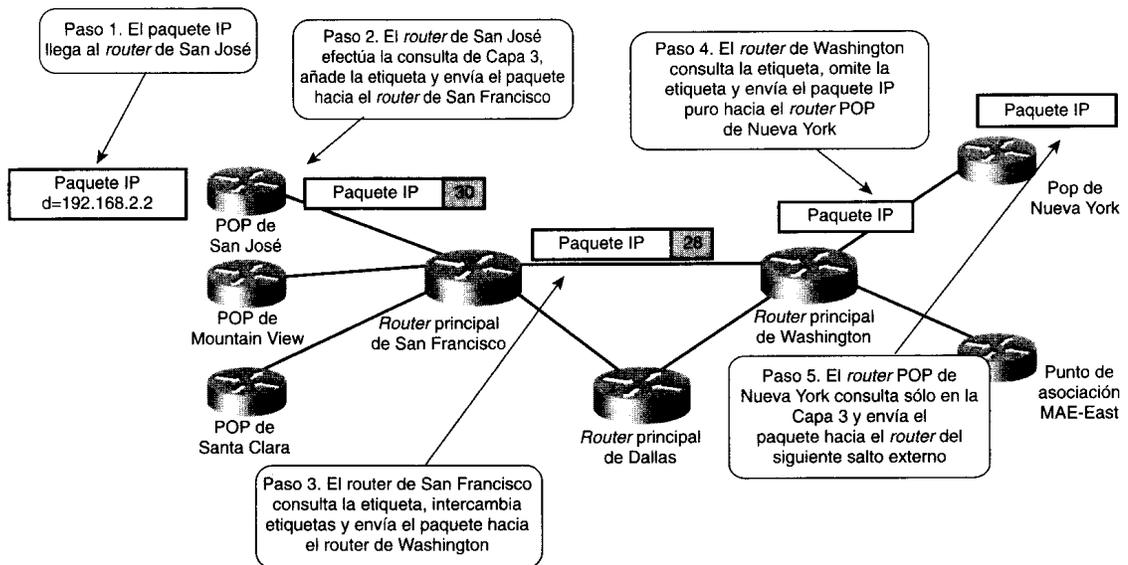


Figura 2.9. Omisión del penúltimo salto en la red SuperNet.

Ejemplo 2.16. Entradas LIB en los LSR de contorno y penúltimo.

```
NewYork#show tag tdp binding 192.168.2.0 24
```

```
tib entry: 192.168.2.0/24, rev 10
```

```
local binding: tag: imp-null(1)
```

```
remote binding: tsr: 172.16.3.1:0, tag: 28
```

```
Washington#show tag tdp binding 192.168.2.0 24
```

```
tib entry: 192.1168.2.0/24, rev 10
```

```
local binding: tag: 28
```

```
remote binding: tsr: 172.16.3.2:0, tag: imp-null(1)
```

```
remote binding: tsr: 172.16.1.4:0, tag: 30
```

```
remote binding: tsr: 172.16.2.1:0, tag: 37
```

2.10 INTERACCIÓN DE MPLS CON EL PROTOCOLO DE GATEWAY FRONTERIZO

En la sección "Distribución y enlace de etiquetas", anteriormente en este capítulo, vimos que se asigna una etiqueta a cada prefijo IP en la tabla de enrutamiento IP de un router que actúa como LSR, siendo la única excepción las rutas aprendidas a través del Protocolo de gateway fronterizo (BGP). No se asignan etiquetas a estas rutas y el LSR de contorno de entrada utiliza la etiqueta asignada al siguiente salto BGP para etiquetar los paquetes enviados hacia los destinos BGP. Para ilustrar este hecho, supongamos que el router de MAE-East de la red de SuperNet recibe una ruta para la red 192.168.3.0 desde un router en el sistema autónomo 4635. La ruta es propagada a través de la red de SuperNet con el router MAE-East de AS4635 como siguiente salto BGP. Cuando se busca en la tabla BGP en el router de San José y en las entradas de la tabla FIB correspondientes, se puede ver que se emplea la misma etiqueta (28) para etiquetar los paquetes para el destino BGP y para el siguiente salto BGP.

La interacción entre MPLS, IGP y BGP brinda al diseñador de redes una perspectiva completamente nueva del diseño de redes. De acuerdo con el funcionamiento tradicional, BGP se tiene que ejecutar en cada router del núcleo de la red del proveedor de servicios para permitir el envío correcto de paquetes. Por ejemplo, la información BGP de MAE-East tiene que propagarse hacia todos los routers principales de la red de SuperNet (Washington, Denver y San Francisco). Si esto no fuera posible, los routers principales no podrían enrutar los paquetes hacia el destino BGP, como se ilustra en la Figura 2.10.

Si, de todos modos, la red de SuperNet ejecuta MPLS, el router de San José propaga el paquete hacia un destino BGP como un paquete etiquetado con la etiqueta asociada con el siguiente salto BGP. Debido a que el siguiente salto BGP

siempre debe anunciarse en el IGP de la red que lo está ejecutando, todos los routers intermedios ya deben tener una asignación de etiqueta entrante a saliente para ese destino en su LFIB y deben propagar el paquete etiquetado hacia el LSR de salida (MAE-East), Pero no necesitan ejecutar BGP. La Figura 2.11 presenta todo el proceso.

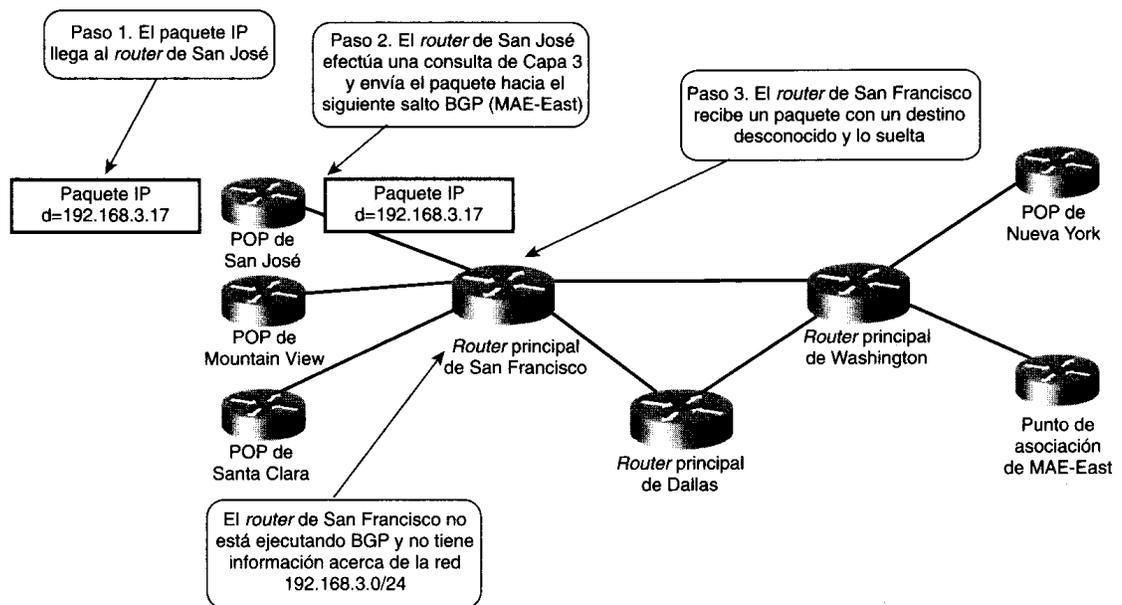


Figura 2.10. Pérdida de conectividad en la red sin BGP en los routers principales.

La eliminación del proceso BGP de los routers principales de la red de un proveedor de servicios tiene varias ventajas:

- Las tablas de enrutamiento de los routers principales se hacen mucho más estables debido a que los routers principales no procesan las fluctuaciones de las rutas en Internet.

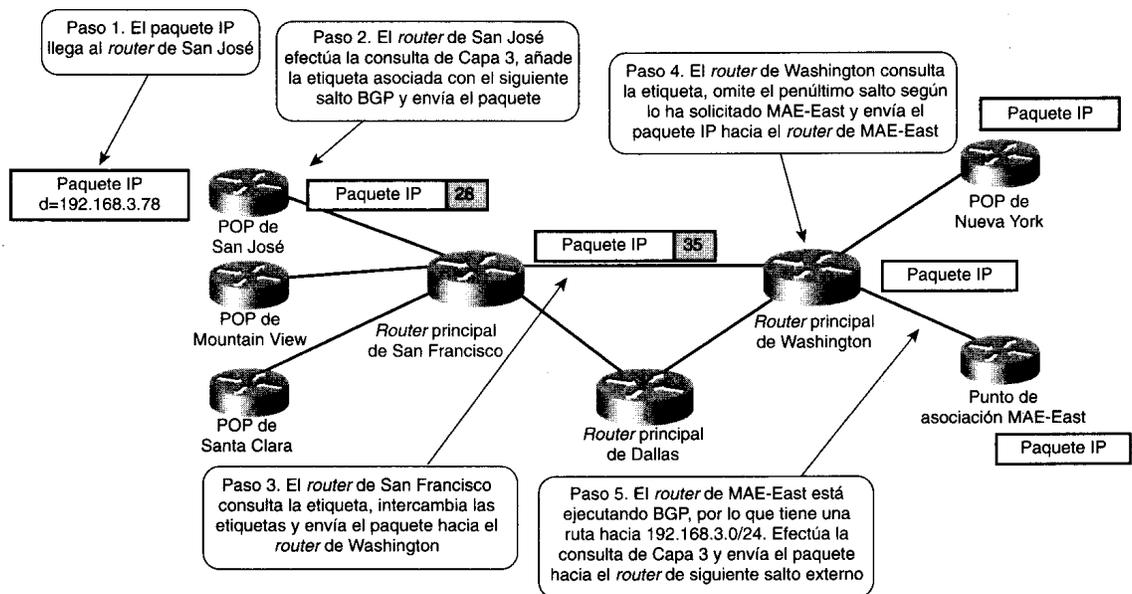


Figura 2.11. Propagación del paquete hacia el destino BGP en una red con MPLS habilitada.

- Se reduce la necesidad de memoria en los routers principales debido a que no tienen que almacenar las rutas de Internet (alrededor de 70.000 a 80.000 rutas, que requieren entre 20 a 40 MB de memoria en un router).
- Se reduce enormemente la utilización de la CPU en los routers principales debido a que no tienen que procesar actualizaciones BGP.

Es sumamente recomendable el despliegue de MPLS, aun cuando el backbone IP del proveedor de servicios esté formado estrictamente por routers. El Capítulo 13 se centra más en la eliminación de BGP en el núcleo de la red de un proveedor de servicios y en las ventajas que esto conlleva, especialmente en un entorno VPN.

2.11 MPLS EN MODO TRAMA A TRAVÉS DE MEDIOS WAN CONMUTADOS

La infraestructura de Capa 2, que proporciona el medio sobre el que puede funcionar MPLS en modo trama, a menudo puede suministrarse utilizando tecnología WAN conmutada, como Frame Relay o ATM. MPLS se puede ejecutar en modo celda a través de ATM, pero no al utilizar Frame Relay o cuando la estructura ATM está construida usando los PVC Foro ATM tradicionales. Esto significa que debe ser posible ejecutar MPLS en modo trama a través de estos tipos de interfaces, para así poder desplegar MPLS extremo a extremo a lo largo de la red.

consideremos el despliegue de MPLS a través de interfaces Frame Relay y PVC ATM. También explica el uso de MPLS en los modos celda y trama a través de la misma interfaz física.

2.12 FUNCIONAMIENTO DE MPLS EN MODO TRAMA A TRAVÉS DE FRAME RELAY

En Frame Relay debe establecerse una sesión, o circuito virtual (VC), antes de que comience cualquier flujo de datos por la red Frame Relay. El VC actúa como un enlace punto a punto para el envío de datos entre dispositivos CPE conectados.

Utilizando estos VC, se puede establecer el envío MPLS y la distribución de etiquetas entre dos dispositivos finales de la misma forma que sobre cualquier otro tipo de interfaz que funcione en modo trama.

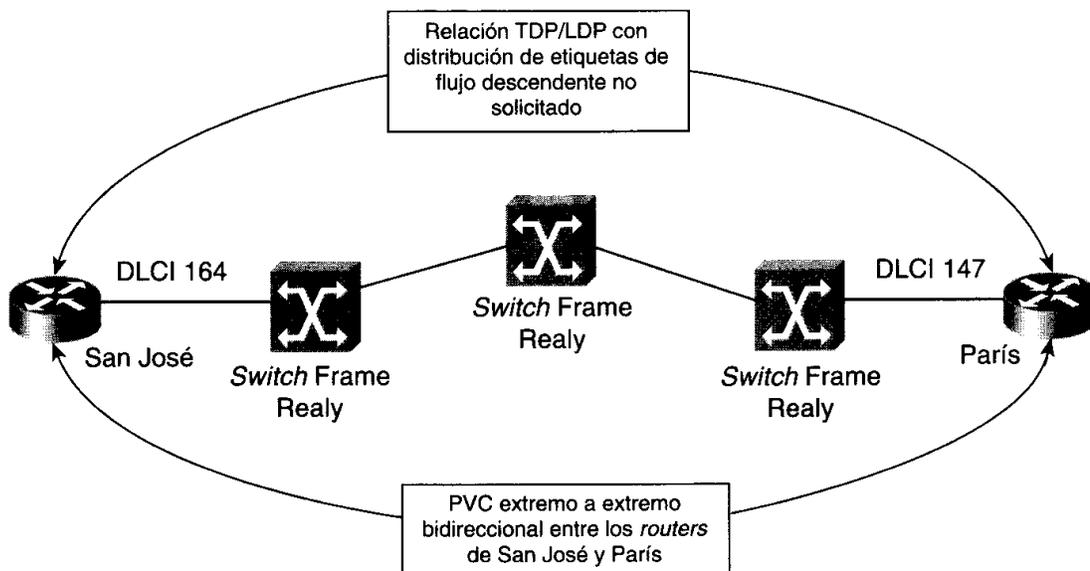


Figura 2.11. Conectividad MPLS a través de PVC Frame Relay.

La Figura 2.11 ilustra dos routers conectados a través de una red Frame Relay. Si se centra en el router de San José, podrá ver que direcciona el VC utilizando un identificador de conexión de enlace de datos (DLCI). Desde la perspectiva de este router, cualquier ruta aprendida desde su vecino de protocolo de enrutamiento a través de su VC (París en este caso) tiene una dirección de envío de siguiente salto apuntando al router de París.

Hay dos formas de encapsular paquetes IP en la implementación que hace Cisco Systems, Inc. de Frame Relay. Lo primero es utilizar la encapsulación Cisco (la predeterminada) y, en segundo lugar, utilizar la encapsulación RFC 1490 (IETF). MPLS envía y controla las funciones mediante cualquier encapsulación. La Figura 2.12 muestra los dos métodos de encapsulación y cómo se añade la información MPLS a la trama.

Encapsulación Cisco Frame Relay

7E Indicador	Cabecera Frame Relay	Ethertype (8847)	Cabecera etiqueta MPLS	Sobrecarga datos	FCS	7E Indicador
-----------------	-------------------------	---------------------	---------------------------	---------------------	-----	-----------------

RFC 1490 Frame Relay Encapsulation

7E Indicador	Cabecera Frame Relay	UI Control 0x03	Pad opcional 0x00	NLPID 0x80 (SNAP)	OUI 0x00-00-00	Ethertype (8847)	Cabecera etiqueta MPLS	Sobrecarga datos	FCS	7E Indicador
-----------------	-------------------------	--------------------	----------------------	----------------------	-------------------	---------------------	---------------------------	---------------------	-----	-----------------

Figura 2.12. Encapsulación MPLS a través de Frame Relay.

Funcionamiento de MPLS en modo trama a través de PVC ATM

Puede ser deseable ejecutar MPLS en modo trama a través de PVC ATM. Se trata de una configuración perfectamente válida.

Este tipo de conectividad, desde el punto de vista MPLS, es esencialmente el mismo que el descrito en la sección sobre Frame Relay anterior. El esquema de asignación de etiquetas utiliza el modo independiente, y la distribución de etiquetas utiliza el flujo descendente no solicitado. La Figura 2.13 muestra un ejemplo de este tipo de conectividad.

En la Figura 2.13 puede ver que los routers de San José y París están conectados a través de PVC ATM punto a punto. De nuevo, utilizando el comando `show tag-switching tdp neighbor` se confirma que la distribución de etiquetas de flujo descendente no solicitado está en vigor a través de la interfaz y, por consiguiente, que MPLS está funcionando en modo trama.

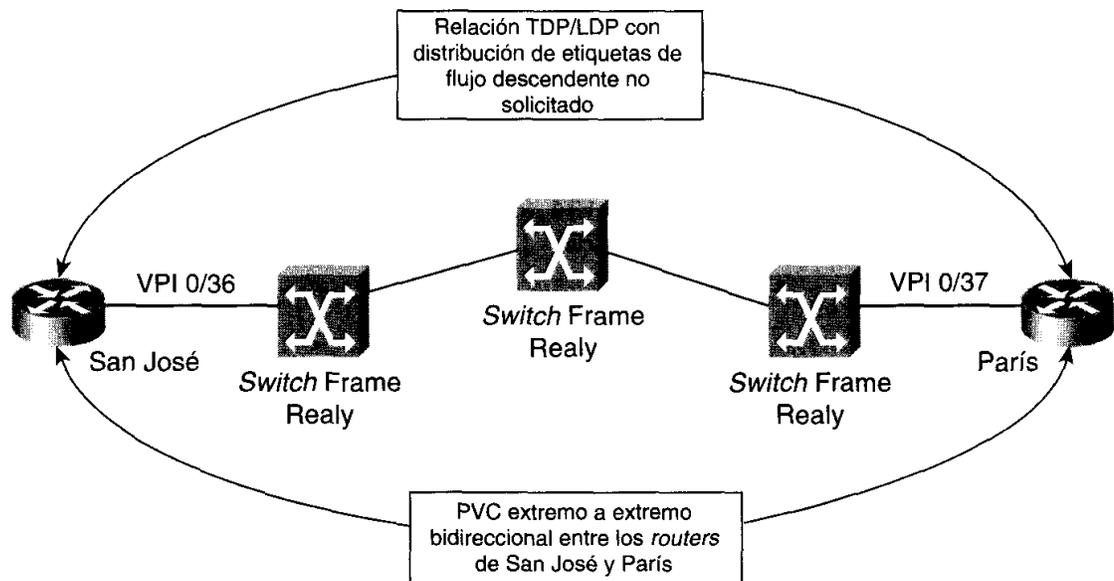


Figura 2.13. Conectividad MPLS a través de MPLS ATM.

2.13 MPLS EN MODO CELDA Y EN MODO TRAMA A TRAVÉS DE LA MISMA INTERFAZ ATM

Podría ser deseable en algunos despliegues de la arquitectura MPLS ejecutar MPLS tanto en modo trama como en modo celda a través de la misma interfaz ATM física, por ejemplo al enlazar dos redes ATM privadas con MPLS habilitada a través de una red ATM pública que ofrece únicamente los servicios PVC Foro ATM.

Este tipo de conectividad es posible gracias al uso de subinterfaces con diferentes tipos de subinterfaz en la configuración de la interfaz ATM del router. Estas subinterfaces se pueden configurar para ejecutar MPLS en modo celda o se pueden configurar para ejecutar el modo trama. La Figura 2.14 ilustra esta técnica.

La topología de ejemplo de la Figura 2.14 muestra que los routers de San José y París tienen una conexión PVC punto a punto entre sí, pero también ejecutan MPLS en modo celda directamente con el switch MPLS ATM.

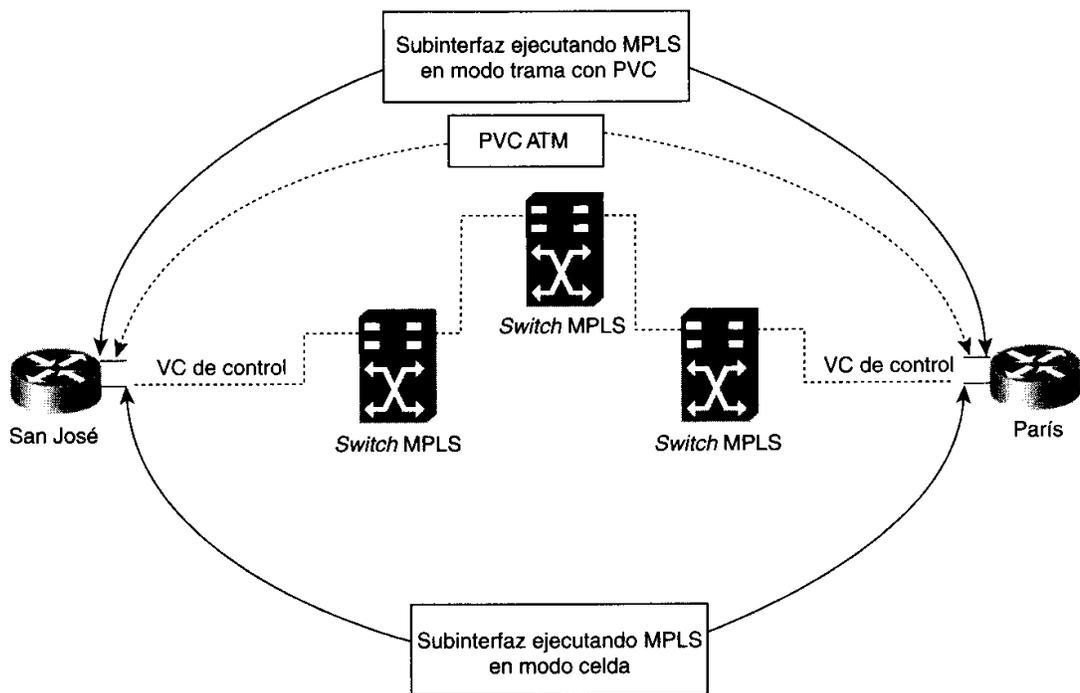


Figura 2.14. MPLS en modo trama y en modo celda a través de la misma interfaz ATM.

3. MPLS EN MODO CELDA

El diseño y la arquitectura de la tecnología ATM presentan varios retos para una implementación ATM de la tecnología MPLS:

- Los paquetes IP del plano de control no se pueden intercambiar directamente en una interfaz ATM. Se debe establecer un VC de control entre los nodos MPLS adyacentes para intercambiar los paquetes del plano de control.
- Los switches ATM no pueden realizar la consulta de etiquetas.
- Los switches ATM no pueden realizar la consulta de Capa 3.

Términos específicos del mundo ATM que empleados a lo largo de este capítulo:

- **Conmutación de etiquetas controlada por una interfaz ATM** (interfaz LC-ATM). Es una interfaz de un router o de un switch ATM en la que se ha asignado el valor VPI/VCI mediante los protocolos de control MPLS (TDP o LDP).
- **LSR ATM** es un switch ATM que ejecuta los protocolos MPLS en el plano de control y que realiza el envío MPLS entre las interfaces LC-ATM en el plano de datos mediante la conmutación de celdas ATM tradicional.
- Un **LSR basado en tramas** es un LSR que envía tramas completas entre sus interfaces. Un ejemplo típico de LSR basado en tramas es un router tradicional. Un LSR basado en tramas también puede tener interfaces LC-ATM, pero tan sólo realiza la conmutación de etiquetas basada en tramas de la pila de etiquetas; no puede llevar a cabo la conmutación de celdas como en un LSR ATM.

- Un **dominio LSR ATM** es un conjunto de LSR ATM interconectados por interfaces LC-ATM
- Un **LSR ATM** de contorno es un LSR basado en tramas con al menos una interfaz LCATM.

Emplearemos una red sencilla (véase la Figura 3.1) idéntica a la red del Capítulo 2, donde los routers principales se han sustituido por switches ATM.

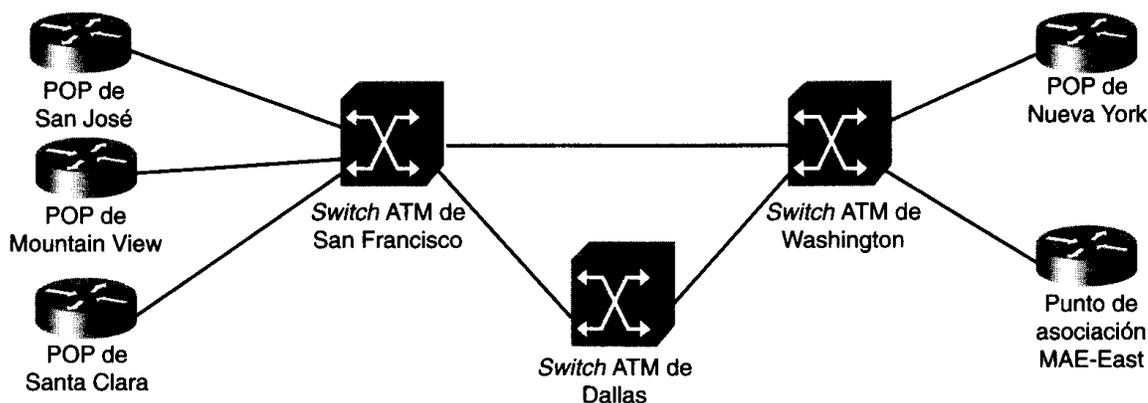


Figura 3.1. Red SuperCell: Implementación ATM.

3.1 CONECTIVIDAD DEL PLANO DE CONTROL EN UNA INTERFAZ LC-ATM

La arquitectura MPLS necesita que los planos de control de los LSR adyacentes tengan una conectividad IP plena para poder intercambiar enlaces de etiquetas, así como otros paquetes de control.

3.2 CONECTIVIDAD DEL PLANO DE CONTROL MPLS EN EL SOFTWARE CISCO IOS

La conectividad del plano de control en el software Cisco IOS se establece tan pronto como se configura MPLS en una interfaz ATM de un router o de un switch ATM. Los mecanismos de configuración son ligeramente diferentes:

- En un router, se puede crear una interfaz LC-ATM configurando una subinterfaz ATM separada con el tipo de interfaz tag-switching, como se muestra en el Ejemplo 3.1, y configurando MPLS en dicha subinterfaz.
- En un switch, se puede configurar MPLS en una interfaz ATM, de manera similar a como está configurada MPLS en las interfaces de router en modo trama, como se muestra en el Ejemplo 3.2.

Ejemplo 3.1. Configuración de la interfaz LC-ATM en un router.

```
SanJose#configure terminal  
SanJose(config)#interface atm 2/0/0.1 tag-switching  
SanJose(config-if)#ip unnumbered loopback 0  
SanJose(config-if)#tag-switching ip
```

Ejemplo 3.2. Configuración de una interfaz LC-ATM en un switch ATM basado en IOS.

```
SanFrancisco#configure terminal  
SanFrancisco(config)#interface atm 2/1/3  
SanFrancisco(config-if)#ip unnumbered loopback 0  
SanFrancisco(config-if)#tag-switching ip
```

3.3 IMPLEMENTACIÓN DEL PLANO DE CONTROL EN UN SWITCH ATM

Al desplegar MPLS en los LSR ATM, el procesador central del switch ATM debe soportar la señalización MPLS y los protocolos de configuración VC. Los dos conjuntos de protocolos se ejecutan de modo transparente de lado a lado, como se puede ver en la Figura 3.2.



Figura 3.2. Ejecución de los protocolos de señalización en un switch ATM.

La implementación Cisco Systems de un controlador externo es el Controlador de la conmutación por etiquetas (LSC) para la familia BPX de switches ATM. El LSC se conecta al BPX mediante una interfaz ATM estándar. El protocolo Interfaz de switch virtual (VS1) que actúa entre el LSC y el switch ATM soporta las adiciones y eliminaciones de VC. Todas las operaciones MPLS de las capas superiores (intercambio de actualizaciones de enrutamiento, construcción de tablas de enrutamiento, intercambio de etiquetas a través de un TDP o un LI)P) se realizan mediante un controlador externo que utiliza el control VC 0/32.

3.4 ENVÍO DE PAQUETES ETIQUETADOS A TRAVÉS DE UN DOMINIO LSR ATM

El envío de paquetes etiquetados a través de un dominio LSR ATM se realiza en tres pasos diferentes:

1. El acceso LSR ATM de contorno recibe un paquete etiquetado o sin etiquetar y encuentra el valor VPI/VCI de salida, valor que utiliza como etiqueta de salida.
El paquete etiquetado se segmenta en celdas ATM y se envía al siguiente LSR ATM.
2. Las celdas de los swtiches LSR ATM se basan en el valor VPI/VCI de la cabecera de la celda ATM.
3. El LSR ATM de contorno de salida vuelve a ensamblar las celdas en un paquete etiquetado. La consulta de la etiqueta se basa en los valores VPI/VCI de las celdas de entrada, no en la etiqueta superior de la pila de la cabecera de la etiqueta MPLS.

Las principales diferencias entre la conmutación de etiquetas basada en tramas y la conmutación de etiquetas basada en celdas son las siguientes:

- La consulta de la etiqueta para el envío de etiquetas basado en tramas se realiza basándose en la etiqueta superior de la pila de la cabecera de la etiqueta MPLS. En el envío basado en celdas, la consulta se realiza basándose en los valores VPI/VCI de las cabeceras de las celdas ATM.
- El mecanismo de conmutación en la conmutación de etiquetas basada en celdas es la conmutación de celdas ATM tradicional basada en los valores

VPI/VCI de las cabeceras de las celdas. Los LSR ATM ignoran completamente la pila de etiquetas MPLS.

- El LSR ATM de contorno de entrada establece a 0 la etiqueta superior de la pila de la cabecera de la etiqueta MPLS.

3.5 DISTRIBUCIÓN Y ASIGNACIÓN DE ETIQUETAS EN UN DOMINIO LSR ATM

La asignación y distribución de etiquetas en un dominio LSR ATM puede utilizar el mismo procedimiento que la MPLS basada en tramas. El número tan pequeño de VC que soporta una interfaz ATM hace de estos circuitos un recurso peligroso que hay que controlar. Por tanto, es necesario conservar la asignación y distribución de las etiquetas en las interfaces ATM.

Para asegurarse de que el número de VC ubicados en las interfaces LC-ATM sigue siendo el mínimo, los LSR de flujo ascendente lanzan la asignación y distribución de etiquetas sobre las interfaces LC-ATM. Un LSR de flujo ascendente que necesite una etiqueta para enviar paquetes etiquetados hacia el siguiente salto deberá solicitar una etiqueta desde su LSR de flujo ascendente.

El proceso de asignación y distribución de etiquetas a lo largo del dominio LSR ATM tiene las siguientes características:

- La asignación de etiquetas en dispositivos con capacidad para consultar la Capa 3 (routers) se realiza sin importar si el router ya ha recibido una etiqueta para el mismo prefijo desde su router de siguiente salto.

- Sólo se realiza si se ha asignado la correspondiente etiqueta de flujo descendente.
- El método de distribución en las interfaces LC-ATM es el flujo descendente bajo demanda, ya que un LSR sólo asigna una etiqueta a través de la interfaz LC-ATM cuando la solicita específicamente un LSR de flujo ascendente.

3.6 CONVERGENCIA A LO LARGO DE UN DOMINIO LSR ATM

En el Capítulo 2 vimos que un despliegue MPLS en una red con un único router no aumenta el tiempo total de convergencia tras un fallo en la red (el tiempo de convergencia aumenta tras la recuperación de un enlace). Sin embargo, la convergencia en una red ATM puede cambiar considerablemente cuando se despliega MPLS. En una red ATM tradicional, el tiempo de convergencia se basa en los siguientes componentes:

- Un router de contorno tenía que detectar el fallo de un router adyacente mediante la señalización ATM, las celdas ATM de operación y mantenimiento (OAM), o las pausas en el protocolo de enrutamiento (tiempos muertos o tiempos de espera).
- El router de contorno que detectaba el fallo del router adyacente propagaba inmediatamente el cambio en la topología de la red a todos los demás routers.
- En los protocolos de estado de enlace, todos los routers tenían que volver a computar una nueva topología de red, normalmente tras un breve retraso.

4. CARACTERÍSTICAS AVANZADAS DE MPLS

Ya hemos visto cómo se distribuyen las etiquetas MPLS entre vecinos TDP/ LDP adyacentes. Sin embargo, puede que llegue a ser necesario restringir la distribución de esta información, o incluso bloquear la publicación de la información. Este capítulo aborda esta posibilidad y analiza porqué puede ser útil al desplegar MPLS. Este capítulo también explica cómo la implementación de la arquitectura MPLS de Cisco Systems, Inc. puede negociar paquetes grandes a través de ciertos tipos de medios que tienen una unidad máxima de transmisión (MTU) que no permite añadir etiquetas MPLS, por defecto, a los paquetes mayores de 1500 bytes.

Por último, este capítulo analiza cómo MPLS puede detectar y prevenir bucles de envío y determina cómo el agregar la información de enrutamiento IP puede afectar a la funcionalidad de la red.

4.1 CONTROL DE LA DISTRIBUCIÓN DE LAS ASIGNACIONES DE ETIQUETAS

La decisión de asignar una etiqueta a una FEC depende del modo de control que está funcionando. Existen dos modos: solicitado e independiente. Cuando utiliza el modo independiente, que es el modo predeterminado al utilizar MPLS en modo trama, un LSR enlaza una etiqueta a una FEC, independientemente de la etiqueta que tenga que recibir del siguiente LSR.

Puede ver la configuración necesaria para el LSR de Washington en el Ejemplo 4.1.

Ejemplo 4.1. Ejemplo de configuración de tag-switching advertise-tags.

```
hostname Washington
!  
tag-switching advertise-tags for 1 to 2  
tag-switching tdp router-id Loopback0  
!  
interface Loopback0  
  ip address 194.22.15.3 255.255.255.255  
!  
interface ATM0/0/0  
  no ip address  
  no atm ilmi-keepalive  
!  
interface ATM0/0/0.1 point-to-point  
  description ** interface to San Jose **  
  ip address 10.1.1.14 255.255.255.252  
  atm pvc 1 20 20 aal5snap  
  tag-switching ip  
!  
interface Ethernet0/1/0  
  description ** interface to Paris **  
  ip address 10.2.1.22 255.255.255.252  
  tag-switching ip  
!  
interface POS2/0/0  
  description ** interface to New York **  
  ip address 10.1.1.21 255.255.255.252  
  tag-switching ip
```

```
!  
access-list 1 permit 194.22.15.0 0.0.0.255  
access-list 1 deny any  
access-list 2 deny 195.22.15.1
```

El comando tag-switching advertise-tags sólo se puede usar al trabajar en MPLS en modo trama. Esto significa que si el enlace entre dos LSR es a través de una interfaz LC-ATM, entonces el filtrado de asignaciones de etiquetas no es posible.

La razón para esta restricción es que al ejecutarse a través de una interfaz LC-ATM, el router usa el modo de control LSP solicitado y la distribución de etiquetas de flujo descendente bajo demanda. Al utilizar este modo de funcionamiento, los recursos de la interfaz se usan como etiquetas. En el caso de ATM, son las parejas VPI/VCI y se conocen como circuitos virtuales de etiqueta (LVC). El Capítulo 3 habla de LVC. La consecuencia de esto es que si se filtra la publicación de asignaciones de etiquetas, entonces todo el tráfico que pasa por el enlace se enviará a través del circuito virtual de control (VPI 0 VCI 32). Esto es así porque el prefijo de destino se mostrará como **sin etiquetar** dentro de la LFIB, y cualquier tráfico hacia ese prefijo será enrutado.

4.2 ENCAPSULACIÓN MPLS A TRAVÉS DE ENLACES ETHERNET

Una de las dificultades que rodean el uso de la encapsulación MPLS es el despliegue de enlaces Ethernet dentro de la topología usando cualquiera de las encapsulaciones Ethernet soportadas.

El uso de MPLS dentro de la red hace que un paquete crezca de tamaño, debido a que se añaden etiquetas en la pila de etiquetas. Cada entrada de la cabecera de una etiqueta tiene una longitud de 4 octetos. Esto significa que si se recibe un paquete con 1500 octetos de sobrecarga, y se pone en la pila una cabecera de

etiqueta, la trama necesita ser enviada con una sobrecarga de 1504 octetos. A causa de la restricción en cuanto al tamaño máximo de una trama entre los diversos tipos de medios Ethernet, esto podría causar un problema porque la MTU de esos enlaces es más pequeña que la que tienen los paquetes.

4.3 DESCUBRIMIENTO DE LA MTU IP DE LA RUTA

La idea básica que subyace tras el descubrimiento de la MTU de la ruta es que un host de origen asume inicialmente que la MTU de la ruta de una conexión particular, es la MTU del primer salto y envía todos los datagramas de esa ruta con el bit DF (no fragmentar) establecido. No se envía ningún datagrama que sea mayor que la MTU del primer salto. Los hosts que no usan estos procedimientos no enviarán datagramas más largos de 576 octetos.

Cuando un router recibe un paquete más grande que la MTU de la interfaz de salida hacia el destino contenido en el paquete entrante y el bit DF está definido en el paquete, envía un mensaje ICMP de destino inalcanzable con un código 4 (se necesita fragmentación y está definido DF) de vuelta al origen del paquete. La Figura 4.1 ilustra este proceso.

Cuando se llevan a cabo esos procedimientos, los paquetes se pueden enviar con éxito a través de un backbone MPLS sin fragmentación.

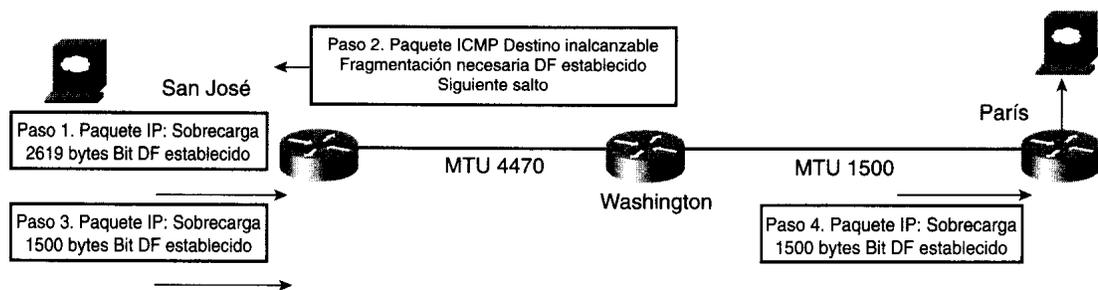


Figura 4.1. Mecanismo de descubrimiento de la MTU.

Todo esto estaría bien si todos respondieran a los mecanismos descritos previamente. Sin embargo, la realidad es que algunos hosts no utilizan el descubrimiento de la MTU y envían datagramas que son más grandes de 576 octetos. Además, algunos firewal1s desechan los mensajes ICMP de destino inalcanzable, lo que rompe de hecho el mecanismo de descubrimiento de la MTU.

Cisco Systems presenta para esas dificultades una alternativa que permite a un puerto Ethernet de un router aceptar paquetes MPLS que tengan una sobrecarga mayor de 1500 octetos. Esto se logra aumentando la MTU del puerto Ethernet a 1526 octetos, que constituye el tamaño máximo estándar de una trama Ethernet de 1518 octetos, más 8 octetos para dos niveles de etiquetas MPLS. En la solución MPLS de Cisco, este parámetro se configura usando el comando tag-switching mtu en la interfaz de salida.

4.4 DETECCIÓN Y PREVENCIÓN DE BUCLES EN MPLS

Un bucle de envío en una red IP es el proceso por el cual un router envía un paquete por la ruta incorrecta (tan lejos como su vecino le permita) hacia un destino particular basándose en la información contenida en su tabla de enrutamiento. Esto puede suceder por una mala configuración de los routers.

En relación con la arquitectura MPLS, debe considerar el plano de control y el plano de datos y cómo se desarrolla la prevención de bucles tanto en modo trama como en un backbone en modo celda.

4.5 DETECCIÓN Y PREVENCIÓN DE BUCLES EN MPLS EN MODO TRAMA

Cuando utiliza este modo, las etiquetas se asignan a las FEC basándose en la existencia de la FEC en la tabla de enrutamiento del LSR. Usando estas

asignaciones de etiquetas, puede establecer rutas conmutadas por etiqueta (LSP) a través de la red MPLS. Teniendo en cuenta este conocimiento, puede comprender cómo cada LSR puede detectar y prevenir los bucles de envío.

4.5.1 Modo trama: detección de bucles en el plano de datos

En una red de enrutamiento IP estándar, los bucles de envío se pueden detectar examinando el campo TTL, de un paquete IP entrante. Usando este campo, cada router en la ruta del paquete disminuye su valor en 1; si el campo alcanza el valor 0, se deshecha el paquete y el bucle de envío se rompe. La Figura 4.2 ilustra este mecanismo.

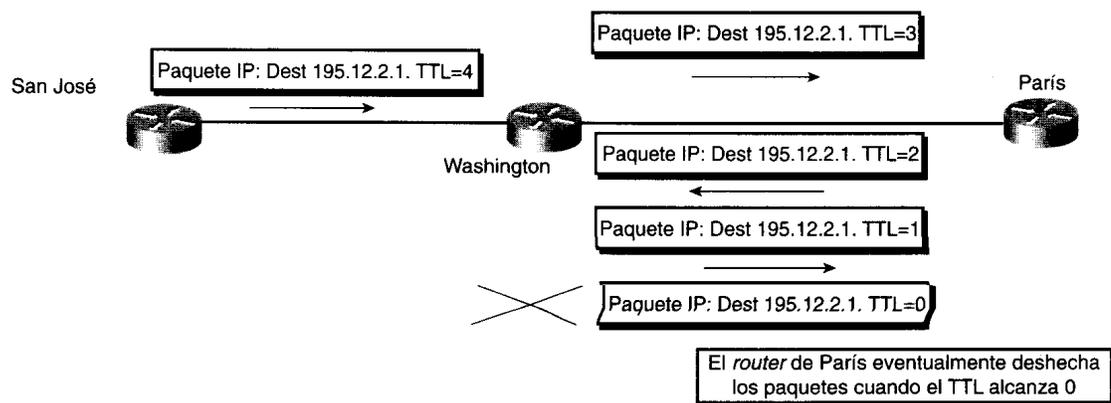


Figura 4.2. Detección de bucles usando el campo TTL en una red IP.

4.5.2 Modo trama: prevención de bucles en el plano de control

En una red de enrutamiento IP estándar, la prevención de bucles de envío es el trabajo del protocolo de enrutamiento interior. Dado que en una solución MPLS en modo trama cada LSR utiliza estos mismos protocolos de enrutamiento para

publicar su tabla de enrutamiento, la información que se usa para formar las LSP dentro de la red es la misma que en una red de enrutamiento IP estándar.

4.6 DETECCIÓN Y PREVENCIÓN DE BUCLES EN MPLS EN MODO CELDA

Los mecanismos que se usan para la detección y prevención de bucles en un despliegue en modo trama no son adecuados para este tipo de entorno. Esto es así porque no existe el concepto de TTL dentro de la cabecera de celda ATM, por tanto, son necesarios nuevos mecanismos específicos del entorno ATM para poder desplegar MPLS con éxito a través de este tipo de red.

4.6.1 modo celda : prevención y detección de bucles en el plano de control

El plano de control utiliza por defecto procedimientos de distribución de etiquetas de flujo descendente bajo demanda con asignación de etiquetas solicitadas. La asignación y distribución de las etiquetas tiene lugar basándose en solicitudes más que en la presencia de una FEC particular en la tabla de enrutamiento del LSR ATM. Asimismo, se puede usar una asignación de etiquetas independiente en los LSR ATM , lo que significa que un LSR ATM puede asignar una etiqueta para cada FEC, independientemente de si ha recibido ya una asignación de etiquetas desde un vecino LSR ATM de flujo descendente. En caso contrario, se envía bajo demanda un mensaje de solicitud de etiqueta al vecino de flujo descendente para una FEC particular, para pedir una asignación de etiquetas para esta FEC.

Este mecanismo se implementa con el uso de un contador de saltos TLV, que contiene una relación del número de LSR ATM que ha atravesado la solicitud de etiqueta o el mensaje de asignación de etiquetas. Cuando un LSR ATM recibe un mensaje de solicitud de etiqueta, si no es el LSR ATM de salida para la FEC contenida dentro del mensaje o no tiene una etiqueta para la FEC, inicia su propio

mensaje de solicitud de etiqueta y lo envía al LSR ATM de siguiente salto. Este LSR ATM se determina también a través del análisis de la tabla de enrutamiento. Si el mensaje de solicitud de etiqueta original contenía un objeto TLV contador de saltos, el LSR ATM incluye también su propio mensaje de solicitud de etiqueta, pero incrementa el contador de saltos en 1. Ésta es la operación inversa a TTL, donde se disminuye el TTI, en uno, aunque se usa el mismo concepto de número máximo de saltos.

Cuando un LSR ATM detecta que el contador de saltos ha alcanzado el máximo valor configurado (254 en la implementación de Cisco), considera que el mensaje ha atravesado un bucle. La Figura 4.3 ilustra este proceso.

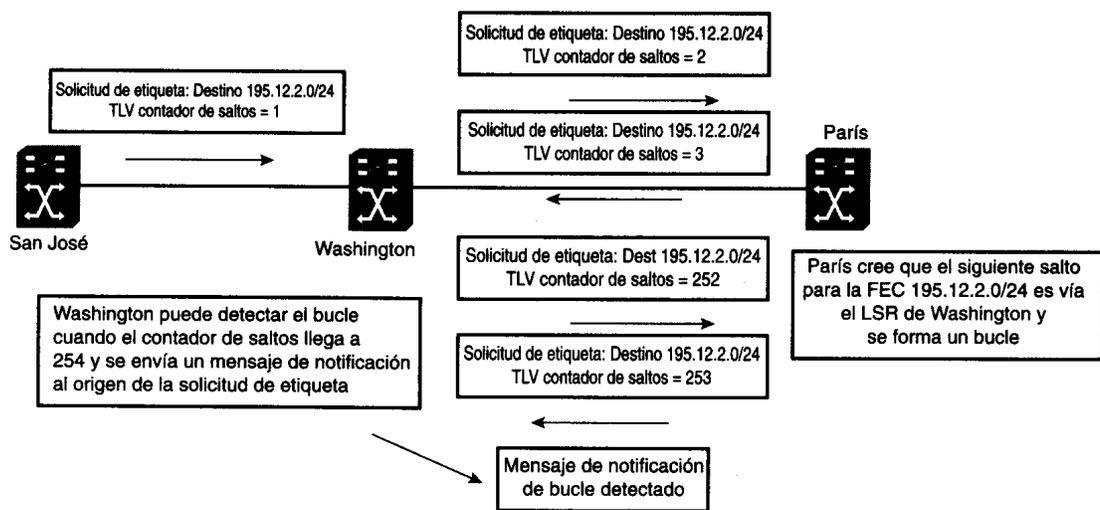


Figura 4.3. Procesamiento del objeto TLV contador de saltos.

4.6.2 Modo celda: detección de bucles en el plano de datos

Ya vimos que una cabecera de celda ATM carece del concepto de TTL. La consecuencia de esto es que cada LSR ATM tiene la información necesaria para determinar el número de saltos necesario para alcanzar el punto de salida ATM de una LSP, y esta información se puede usar dentro del plano de datos del despliegue de MPLS en modo celda. La Figura 4.4 muestra la propagación de la información del contador de saltos entre los LSR ATM.

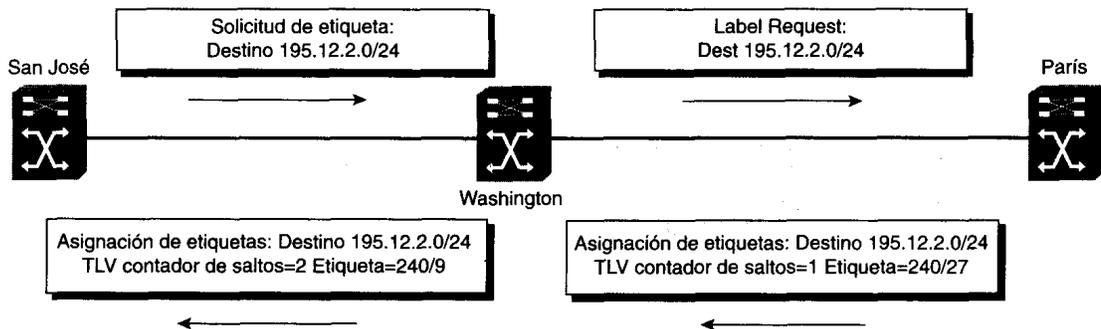


Figura 4.4. Propagación del contador de saltos entre los LSR ATM.

En el ejemplo que se muestra en la Figura 4.4 se ve que el LSR de contorno ATM de San José puede determinar que para alcanzar el punto de salida de la LSP para la FEC 195.12.2.0/24, un paquete debe atravesar 2 saltos. Gracias a esta información, el LSR de contorno ATM de San José puede procesar el campo TTL de un paquete IP entrante antes de la segmentación del paquete en celdas ATM. La Figura 4.5 muestra este proceso.

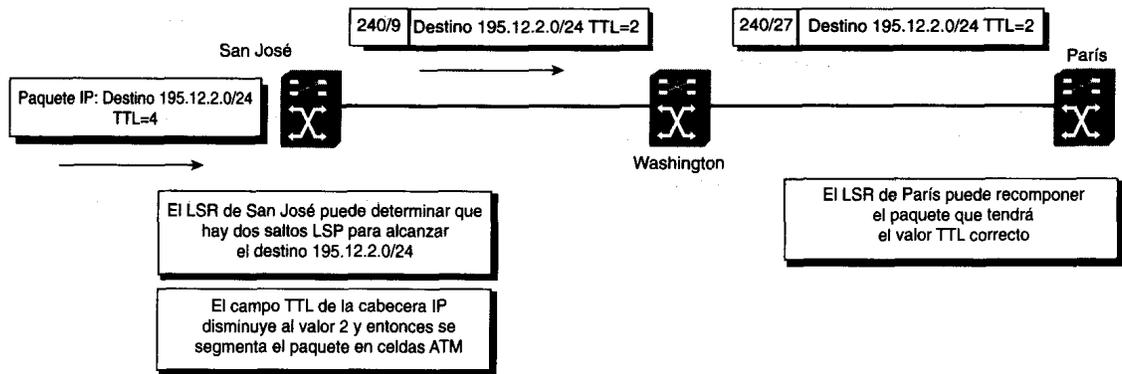


Figura 4.5. Procesamiento del campo TTL del paquete IP antes del proceso SAR.

4.7 RESUMEN DE RUTA EN UNA RED CON MPLS HABILITADA

En cualquier despliegue basado en IP, tanto si se usan protocolos de enrutamiento IP estándar como si se ejecuta IP a través de una red MPLS, el resumen de ruta es una parte importante de la estructura de la red. El resumen de ruta proporciona el mecanismo necesario para reducir el tamaño de la tabla de enrutamiento de Capa 3 empaquetando un cierto número de prefijos en un resumen de ruta menos específico, lo que ayuda a reducir la cantidad de memoria que necesitan los dispositivos de la red, y también ayuda a reducir el gasto necesario para calcular rutas a través de la topología de la red.

En un despliegue MPLS, este resumen puede ayudar a reducir el número de etiquetas porque sólo es necesaria una etiqueta para el resumen de ruta. Se puede ver un ejemplo de este resumen y la distribución de etiquetas correspondiente en la Figura 4.6.

En esta figura puede ver que el LSR de Washington recibe dos prefijos /24, 174.24.9.0/24 y 174.24.10.0/24, del LSR de París a través de su protocolo de enrutamiento interno. El LSR de Washington está configurado para enviar un resumen de ruta, 174.24.0/16, que abarca todas las rutas más específicas que aprendió del LSR de París.

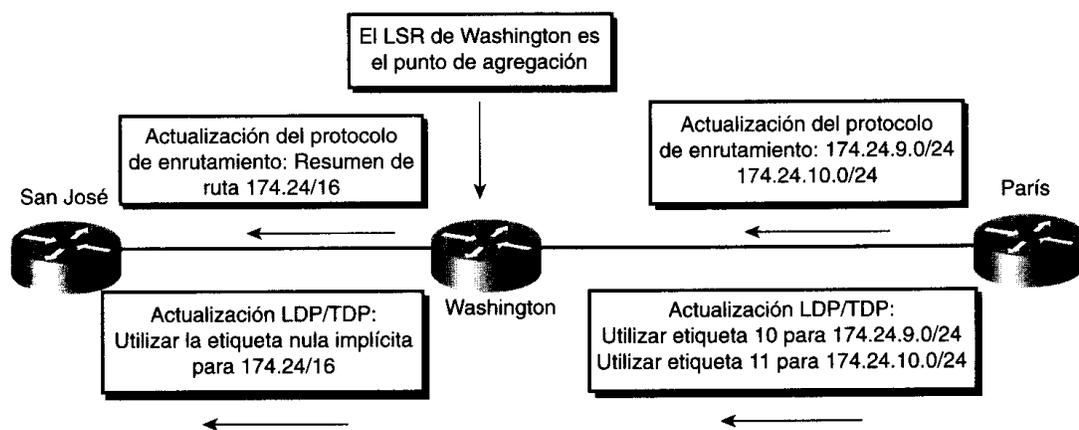


Figura 4.6. Resumen de ruta en una red MPLS.

Usando esta configuración, el LSR de Washington se convierte en el punto de agregación para las LSP que usan el resumen de ruta. Esto significa que cada LSP que utilice el resumen de ruta debe terminar en el LSR de Washington. El resultado es que el LSR de Washington debe examinar el etiquetado de segundo nivel de cada paquete y, según lo que encuentre, decidir la acción que se lleva a cabo. Si hay una etiqueta, el LSR conmuta el paquete basándose en esa etiqueta. Si no hay ninguna etiqueta, el LSR debe examinar la información de la cabecera de Capa 3 para poder reclasificar el paquete.

Dado que es necesario reclasificar los paquetes en el punto de agregación, es imperativo que el dispositivo que proporciona la agregación no sea un switch ATM, debido a que un switch ATM no tiene hardware para procesar la información de

Capa 3 con la que reclasificar cualquier paquete, ya que sólo usa el VPI/VCI entrante como referencia para determinar el puerto de salida, y el VPI/VCI de salida que se debería usar para la celda entrante.

5. CONCLUSIONES

La Conmutación de Etiquetas Multiprotocolo, MPLS, aparece como una posible solución para proporcionar QoS e Ingeniería de tráfico a una red global que soporte todo tipo de tráfico. Es una solución con grandes posibilidades de éxito debido a la facilidad a la hora de migrar una red actual (FR, ATM, Ethernet...) a MPLS, siendo el primer paso la coexistencia entre ellas mediante software añadido a equipos actuales. Una importante ventaja de una red única es la simplificación en cuanto a administración de una sola de red, sobre la se pueden crear tantas redes virtuales como sea necesario. Esto facilitará enormemente la labor a los proveedores de servicio al tiempo que les permitirá ofrecer servicios de valor añadido, pues es lo que en definitiva acabará marcando la diferencia entre ellos. A fecha de hoy, ya hay operadores migrando a esta solución como es el caso de, por ejemplo, Cable & Wireless, Equant, Genuity y MCI World-Com.

Los fabricantes también se han volcado de lleno en el desarrollo del software necesario para la migración y del equipamiento propio de MPLS. Tanto CISCO como Nortel Networks, Juniper Networks o Nokia (entre otros) disponen de grupos de trabajo especializados desarrollando este nuevo estándar. Éste es el punto clave para que los proveedores de servicio puedan comprobar la aceptación de MPLS en el mercado, dando así el primer paso hacia una nueva etapa para las redes de comunicaciones. Una etapa, si todo evoluciona siguiendo la trayectoria actual, muy prometedora.

6. RECOMENDACIONES

El objetivo de las VPNs es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y vídeo sobre infraestructuras de comunicaciones eficaces y rentables. La popularización de las aplicaciones TCP/IP, así como la expansión de las redes de los NSPs, ha llevado a tratar de utilizar estas infraestructuras IP para el soporte de VPNs, tratando de conseguir una mayor flexibilidad en el diseño e implantación y unos menores costes de gestión y provisión de servicio, pero el problema que plantean estas IP VPNs es que están basadas en un modelo topológico superpuesto sobre la topología física existente, a base de túneles extremo a extremo (o circuitos virtuales) entre cada par de routers de cliente en cada VPN. De ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento cuando se quieren añadir nuevos emplazamientos.

En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una "nube común" en las que solamente pueden entrar los miembros de la misma VPN. Es por esto que creemos indispensable el estudio de la implantación de VPNs con MPLS y ponemos este tema a consideración a los lectores como tema de investigación.

REFERENCIAS BIBLIOGRÁFICAS

- BARBERÁ José. MPLS: UNA ARQUITECTURA DE BACKBONE PARA LA INTERNET DEL SIGLO XXI, 2003
- GARCÍA Jesús, RAYA José Luis y RODRIGO Víctor. ALTA VELOCIDAD Y CALIDAD DE SERVICIO EN REDES IP. Coedición: Alfaomega-Rama. 2003.
- BLACK, Uyles TECNOLOGÍAS EMERGENTES PARA REDES DE COMPUTADORAS".. Pearson Education. 2001.

SITIOS WEB

- SEMERIA C., "Multiprotocol Label Switching: Enhancing Routing in the New Public Network", Juniper Networks Inc., White Paper, <http://www.juniper.net/techcenter/techpapers/mpls/mpls.html>, marzo 1999
- SEMERIA C., "Traffic Engineering for the New Public Network", Juniper Networks Inc., White Paper, enero 1999, http://www.juniper.net/techcenter/techpapers//TE_NPN.html
- SEMERIA C., Stewart III J.W., "Optimizing Routing Software for Reliable Internet Growth", Juniper Networks Inc., White Paper, julio 1999, <http://www.juniper.net/techcenter/techpapers/optimizing-routing-sw.fm.html>
- Charter IETF sobre MPLS <http://www.ietf.org/html.charters/mpls-charter.html>

- REDFORD R., "Enabling Business IP Services with Multiprotocol Label SWitching", Cisco Systems, Inc., White Paper, 1999
http://www.cisco.com/warp/public/cc/cisco/mkt/wan/ipatm/tech/mpls_wp.htm
- Cisco,
http://www.cisco.com/warp/public/cc/cisco/mkt/servprod/dial/tech/ievpn_rg.htm
- "Delivering New World Virtual Private Networks with MPLS", Cisco Systems, Inc., White Paper,
http://www.cisco.com/warp/public/cc/cisco/mkt/servprod/dial/tech/mpls_wi.htm
- MPLS Forum : An industry forum to promote MPLS:
<http://www.mplsforum.org/>
- MPLS Resource Center : Clearinghouse for information on MPLS:
<http://www.mplsrc.com/>
- MPLS Working Group : Chartered by IETF to develop standards related to MPLS. The Web site includes all relevant RFCs and Internet Drafts:
<http://www.ietf.org/html.charters/mpls-charter.html>

GLOSARIO

ATM	Modo de Transferencia Asíncrono. La tecnología llamada Asynchronous Transfer Mode (ATM) es el corazón de los servicios digitales integrados que ofrecen las nuevas redes digitales de servicios integrados de Banda Ancha. El tráfico del ciberespacio, con su voluminoso y tumultuoso crecimiento, impone a los operadores de redes públicas y privadas una alta demanda de ancho de banda y flexibilidad de soluciones robustas. La versatilidad de la conmutación de paquetes de longitud fija, denominadas celdas ATM, son las tablas más calificadas para soportar la demanda de Internet. Cada celda compuesta por 53 bytes, de los cuales 48 (opcionalmente 44) son para transporte de información y los restantes para uso de campos de control.
Backbone	Un backbone es el enlace de gran caudal o una serie de nodos de conexión que forman un eje de conexión principal. Es la columna vertebral de una red.
BGP	Protocolo de gateway fronterizo. Protocolo para enrutamiento interdominio en grandes redes, que es parte de TCP/IP (Transmission Control Protocol / Internet Protocol). BGP está definido por el documento RFC (Request For Comments) 1105 preparado por Cisco e IBM .
Bucles	El bucle de red ocurre cuando dos componentes de un equipo de una red están conectados por más de una ruta, por lo que los paquetes circulan alrededor de la red constantemente sin llegar a su destino. Un concentrador repetidor detecta los bucles de red y automáticamente

divide uno de sus puertos para abrir el bucle.

Cabecera

Caché

Almacenamiento local y temporal de información en un browser (navegador. Una de sus funciones es reducir el tiempo de respuesta y el consumo de anchobanda de red, en demandas equivalentes futuras.

CEF

Envío expreso de Cisco

Conmutador

Un conmutador (switch) solamente envía información cuando es necesario (a diferencia del concentrador, que envía información a todos sus puertos). Una vez que aprende qué dispositivos pueden alcanzarse a través de cada puerto, el conmutador solamente pasará paquetes a los puertos adecuados. De este modo, un conmutador puede reducir la cantidad de tráfico en gran medida, y mejorar el rendimiento de la red. Un conmutador, como el OfficeConnect Switch, se utiliza generalmente para conectar concentradores entre sí, o para facilitar conexiones dedicadas a estaciones de alto rendimiento.

CPE

Equipo terminal del abonado

CPU

Central Processing Unit. Unidad central de procesamiento. Es el procesador que contiene los circuitos lógicos que realizan las instrucciones del computador. Es un Chip que contiene millones de transistores encargados de realizar las operaciones que encomendamos al computador. No obstante, por sí solo no sirve para nada, porque debe estar conectada a la placa madre. La placa madre provee de corriente eléctrica a la CPU y le permite comunicarse con el resto de dispositivos.

Datagrama	Es un mensaje TCP/IP o IPX que contiene direcciones fuente y de destino de Internet y datos que se utilizan para encaminar un paquete a través de una red. Datagramas son las unidades de información primaria que se utilizan en Internet
DLCI	Identificador de conexión de datos de enlace
Enlace	Conexión física entre dos nodos en una red.
Ethernet	Tipo de red de área local desarrollada en forma conjunta por Xerox, Intel y Digital Equipment. Se apoya en la topología de bus, anillo, estrella. La red ethernet ofrece un ancho de banda de 10 y 100 Mbps siendo éstas las velocidades más populares.
Etiquetas	
Fast Ethernet	Opera a una velocidad de 100Mbps y por lo tanto tiene un ancho de banda 10 veces mayor que Ethernet, lo cual le permite hacer frente a mayores cantidades de tráfico; como resultado de esta mayor velocidad, la operación se realiza 10 veces más rápidamente que en Ethernet. Fast Ethernet funciona a través de los diferentes (cables) 100 BASE: por ejemplo, 100 BASE-FX y 100 BASE-TX.
	Las redes de Fast Ethernet operan a una velocidad de 100Mbps, y se basan en el método de acceso a red 10 BASE-T Ethernet CSMA/CD, extensión de la norma IEEE 802.3.
FEC	Clases equivalentes de envío
FIB	Base de información de envío
Frame Relay	Frame Relay es un protocolo de conmutación de paquetes

de alta velocidad utilizado en redes WAN. Es popular en las conexiones LAN to LAN a lo largo de distancias remotas, y está indicado para transferir datos e imágenes. Debido a su arquitectura de paquete de longitud variable, no es la tecnología más eficiente para transmitir voz y vídeo. Frame Relay es más popular en los EE.UU. que en Europa.

Gateway	Puente. Sistema de información que transfiere información entre sistemas o redes incompatibles.
Gigabit Ethernet	Gigabit Ethernet es una extensión de los estándares IEEE 802.3 Ethernet de 10 Mbps (Ethernet) y 100 Mbps (Fast Ethernet). Gigabit Ethernet opera a una velocidad de 1000 Mbps y mantiene una compatibilidad absoluta con la base instalada de nodos Ethernet.
IGP	Protocolo de gateway interior
ILMI	Interfaz de administración local integrada
Interfaz	Método de comunicación entre computador y hombre, mediante iconos, ventanas o sonidos, en el caso de interfaces con Mac y Windows.
Internet	Internet fue un proyecto del Ministerio de Defensa estadounidense conocido como A.R.P.A.N.E.T. Tras haber transcurrido algunos años, el Reino Unido se integró a la red que cubría a gran parte de las universidades y centros científicos de Estados Unidos. Con el paso del tiempo se conectarían los demás países de Europa y algunos países de Asia. En los noventa ya se hablaba de una red internacional. Pero fue hasta la aparición de WWW que se logró conectar a millones de personas desde sus hogares y lugares de trabajo para unificar los recursos, esto trajo

consigo el comercio, los negocios financieros, y el entretenimiento. Internet es una colección de miles de redes de computadores, es por ello que constituye un fenómeno sociocultural y comunicacional de gran escala, una nueva forma de realizar comunicaciones.

IP	Protocolo Internet. Es el protocolo de envío de paquetes donde el paquete tiene una dirección destino, y éste se envía sin acuse de recibo. Cuando una persona se conecta a Internet, se le asigna una dirección IP.
IS-IS	Sistema intermedio-sistema intermedio
LDP	Protocolo de distribución de etiquetas
LSC	Controlador de la conmutación por etiquetas
LSP	Ruta conmutada por etiqueta
LSR	Router de conmutación por etiquetas
LVC	Circuitos virtuales de etiqueta
Modelo OSI	<p>Modelo de referencia de Interconexión de modelos abiertos. El modelo de referencia OSI es un estándar global de la industria, utilizado en las operaciones red, con el fin de definir cómo se comunican los protocolos a través de una red. El modelo de referencia OSI se desarrolló para ayudar a los desarrolladores a crear aplicaciones que sean compatibles en productos de distintas marcas.</p> <p>Aprender las capas y funciones de OSI ayuda a entender las redes de comunicaciones.</p> <p>Resumidamente, cuando un dispositivo en una red quiere comunicarse con otro enviando un mensaje (por ejemplo, un correo electrónico), el mensaje pasa a través de las capas del modelo. Cada una de las siete capas vincula</p>

instrucciones al mensaje, hasta que el paquete entero adopta una forma que puede pasar a través de la red. El mensaje es descifrado por el modelo a medida que el mensaje avanza a través de las capas hasta llegar a su destino final.

MPLS	Conmutación de Etiquetas Multiprotocolo.
MPLSCP	Protocolo de control MPLS
MSS	Tamaño máximo de segmento
NCP	Protocolo de control de la red
OAM	Operación y mantenimiento
Paquete	Un paquete es una unidad de información que se envían entre sí las estaciones de trabajo y otro equipo a través de la red. Cuando se envía información desde un computador (como puede ser un archivo de texto), se transmite a través de la red como una serie de paquetes.
	<p>Un paquete consiste en un conjunto de bits que forman un solo bloque de datos, y que contiene una cabecera formado por información de control como es el emisor, el receptor, y datos de control de errores, además del mismo mensaje. Debido a que son unidades de datos de red similares, los términos <i>paquete</i> y <i>trama</i> se utilizan indistintamente.</p>
PBR	Enrutamiento basado en normas
PHP	Omisión del penúltimo salto
Protocolo	Un protocolo es una serie de reglas que utilizan dos computadores para comunicar entre si.
PVP	Ruta virtual permanente
QoS	Calidad de servicio

Router	Un router es una pieza de hardware o software que conecta dos o más redes. Asegura el encaminamiento de una comunicación a través de una red.
SFD	Delimitador de trama inicial
Switches	
TCP	Protocolo para el Control de la Transmisión
TCP/IP	TCP/IP son las siglas de Transmission Control Protocol/Internet Protocol, el lenguaje que rige todas las comunicaciones entre todos los computadores en Internet. TCP/IP es un conjunto de instrucciones que dictan cómo se han de enviar paquetes de información por distintas redes. También tiene una función de verificación de errores para asegurarse que los paquetes lleguen a su destino final en el orden apropiado. IP, Internet Protocol, es la especificación que determina hacia dónde son encaminados los paquetes, en función de su dirección de destino. TCP, o Transmission Control Protocol, se asegura de que los paquetes lleguen correctamente a su destino. Si TCP determina que un paquete no ha sido recibido, intentará volver a enviarlo hasta que sea recibido correctamente.
TDP	Protocolo de distribución de etiquetas
TDP/LDP	
Trama	Conjunto de bits que forman un bloque de datos básico. Generalmente, una trama contiene su propia información de control, en la que se incluye la dirección del dispositivo al que está siendo enviado.

Desde uno de los componentes de equipo de red, los

cuadros pueden ser unidestinados (enviados a un solo dispositivo), multidestinados (enviados a dispositivos múltiples) o difundidos (enviados a todos los dispositivos).

TTL	Tiempo de existencia
UNI	Interfaz red-usuario
VC	Circuito virtual
VCI	Identificador de circuito virtual
VPI	Identificador de ruta virtual
VPN	Red Privada Virtual. Una red virtual privada (VPN) es una red segura de datos privada establecida a través de Internet, por medio de la cual se reduce en gran medida la cuenta telefónica, porque se accede a ella marcando un número local de tarifa gratis. Utilizando el backbone principal de Internet se necesita hacer una menor inversión en infraestructura de red privada.
VSI	Protocolo de switch virtual
WAN	Redes de Área Extensa. Siglas de Wide Area Network. Red que conecta computadores distantes por medio de línea telefónicas o por otro tipo de enlace.
X.25	Estándar CCITT (1976) para los protocolos y formatos de mensajes que definen la interfaz entre una terminal y una red de conmutación de paquetes.

ANEXOS

ANEXO 1.COMANDOS MPLS DE CISCO SYSTEMS Y NORTEL NETWORKS

Tabla A.1. Estructura de los comandos MPLS de Cisco Systems frente a los de conmutación por etiquetas.

Comando LDP	Comando TDP	Descripción
mpls ldp advertise-labels	tag-switching advertise-labels	Controla la distribución de las etiquetas (entrantes) asignadas localmente por LDP/TDP.
mpls ldp atm control-mode	tag-switching atm allocation-mode	Controla el modo utilizado por las solicitudes de manipulación del enlace de etiquetas en las interfaces LC-ATM.
mpls ldp atm vc-merge	tag-switching atm vc-merge	Controla si la función vc-merge está soportada por los VC de unidifusión de etiquetas.
mpls ldp maxhops	tag-switching atm maxhops	Limita el número de saltos permitidos en un I-SP establecido por el flujo descendente en el método bajo demanda de la distribución de etiquetas.
mpls ip (global)	tag-switching ip (global)	Habilita el envío MPLS de paquetes IPv4 junto con las

		rutas enrutadas normalmente para la plataforma.
mpls ip (interfaz)	tag-switching (interfaz)	Habilita el envío MPLS de paquetes IPv4 junto con las rutas enrutadas normalmente para una interfaz particular.
mpls ldp discovery	tag-switching tdp discovery	Configura el intervalo entre la transmisión de mensajes hello de descubrimiento LDP/TDP consecutivos, el tiempo de espera para un vecino LDP/TDP descubierto, o los vecinos desde los cuales las solicitudes para el envío de "hellos" se pueden aceptar.
mpls ldp holdtime	tag-switching tdp holdtime	Cambia el tiempo que se mantiene una sesión LDP/TDP en ausencia de mensajes LDP/TDP procedentes de un equipo vecino.
show mpls atm-ldp bindings	show tag-switching	Visualiza las entradas especificadas atm-tdp bindings desde las bases de datos de enlaces de

		etiquetas ATM LDP/TDP.
show mpls atm-ldp capability	show tag-switching atrn-tdp capability	Visualiza las capacidades ATM de MPLS negociadas con los vecinos LDP/TDP para las interfaces LC-ATM.
show mpls interfaces	show tag-switching interfaces	Visualiza información acerca de una o más interfaces configuradas para la conmutación por etiquetas.
show mpls ldp bindings	show tag-switching tdp bindings	Visualiza el contenido de la base de información de etiquetas (LIB).
show mpls ldp discovery	show tag-switching tdp discovery	Visualiza el estado del proceso de descubrimiento LDP/TDP.
show mpls ldp neighbor	show tag-switching tdp neighbor	Visualiza el estado de las sesiones LDP/TDP.
show mpls ldp parameters	show tag-switching tdp parameters	Visualiza los parámetros LDP/TDP actuales.

Tabla A.2. Comandos MPLS de Nortel Networks

Comando	Descripción
config p2p-vpn <VPN-ID>	Configura una VPN P2P donde VPN-ID indica que se debe escribir un valor integral entre 1 y 65535 que representa la identidad única de la VPN
show ports discard main <ports>	Muestra estadísticas acerca de los paquetes que fueron descartados o borrados durante el ingreso o egreso de

	un puerto
show ports discard extended <ports>	Muestra estadísticas acerca de los paquetes que fueron descartados o borrados durante el 8664GB OSM
show mpls ip vftn info	VFTN se refiere a la tabla VPN-a-FEC-a-NHLFE la cual es específica para la P2P-VPNs.
config ethernet <ports> service-type <l2uni vpls ip>	Configura un puerto para VPLS-VPNs. Donde <ports> indica que se debe escribir un valor para el número del slot y del puerto de los puertos que se están configurando.
config vpls-vpn <VPN_ID>	Configura las VPLS-VPNs. Donde VPN_ID es el número específico de los VPLS-VPN que se desean configurar.
config adm	Configura el ADM (Mecanismo de Auto Descubrimiento).
config mlt <mid>	Crea una MLT (MultiLink Trunks). Donde mid indica que se debe escribir un valor entre 1 y 32 que representa un identificador MLT único.
config mlt <mid> add	Añade miembros troncales a la MLT. Donde mid indica que se debe escribir un valor entre 1 y 32 que representa un identificador MLT.
config mlt <mid> remove	Quita miembros troncales a la MLT. Donde mid indica que se debe escribir un valor entre 1 y 32 que representa un identificador MLT.
config mlt <mid> ip	Asigna una dirección IP a una MLT. Donde mid indica que se debe escribir un valor entre 1 y 32 que representa un identificador MLT.
config mlt <mid> ip ospf	Asigna una interfase IP OSPF a la MLT especificada. Donde mid indica que se debe escribir un valor entre 1 y 32 que representa un identificador MLT.
show vpls-vpn info [vpn-	Muestra la configuración para todas las VPLS-VPNs

id <value>] [tunnel-
group-id
<value>]

para una VPLS-VPN o para pares remotos que son accesibles usando un grupo de túnel específico. El valor *vpn-id* es un parámetro opcional (en el rango de 1 a 65535) que indica el número de identificación específico de la VPLS-VPN. Si no se escribe un valor *vpn-id* específico, el sistema muestra información acerca de todas las VPLS-VPNs.

El valor *tunnel-group-id* es un parámetro opcional que indica un par remoto el cual es accesible usando un grupo de túnel específico.

ANEXO 2. ALGUNAS EMPRESAS QUE OFRECEN MPLS

- **BT-MPLS España:**
<http://www.btglobalservices.com/es/products/mpls>
- **Orbitel Colombia:**
<http://www.orbitel.com.co>
- **Nortel Networks:**
<http://www.nortelnetworks.com/corporate/technology/mpls/index.html>
- **Cisco Colombia:**
<http://www.cisco.com/warp/public/732/Tech/mpls>
- **Siemens Region Andina:**
www.siemens.com.co/SiemensDotNetClient_Andina
- **Cable & Wireless**
<http://www.cw.com/>
- **Equant**
<http://www.equant.com/>
- **MCI World-Com**
<http://www.mci.com/>