

TÉCNICA MPLS PARA OPTIMIZACIÓN DE TRÁFICO EN REDES IP



CAROLINA ANDREA CARRASCAL REYES
CLAUDIA XIMENA MOSQUERA LEYTON

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERÍA ELECTRÓNICA Y TELECOMUNICACIONES
GRUPO DE I+D EN NUEVAS TECNOLOGÍAS EN TELECOMUNICACIONES
POPAYÁN
2001

TÉCNICA MPLS PARA OPTIMIZACIÓN DE TRÁFICO EN REDES IP

CAROLINA ANDREA CARRASCAL REYES
CLAUDIA XIMENA MOSQUERA LEYTON

Monografía para optar al título de
Ingeniero en Electrónica y Telecomunicaciones

Director

Ing. Esp. OSCAR J. CALDERÓN CORTÉS

UNIVERSIDAD DEL CAUCA
FACULTAD DE INGENIERIA ELECTRÓNICA Y TELECOMUNICACIONES
GRUPO DE I+D EN NUEVAS TECNOLOGÍAS EN TELECOMUNICACIONES
POPAYÁN
2001

TABLA DE CONTENIDO

INTRODUCCIÓN	1
1. REDES IP - CONCEPTOS FUNDAMENTALES.....	3
1.1 EVOLUCIÓN DE LAS REDES IP.....	3
1.2 ARQUITECTURA MODULAR DE LAS REDES IP	4
1.3 NIVEL INTERNET	7
1.4 ENRUTAMIENTO EN LAS REDES IP	11
1.4.1 Generalidades de Enrutamiento.....	11
1.4.2 Clasificación de los Protocolos de Enrutamiento	13
1.4.2.1 Protocolos de Enrutamiento Interno (IGP)	13
1.4.2.2 Protocolos de Enrutamiento Externo (EGP)	15
1.4.3 Proceso de Enrutamiento.....	15
1.5 PROBLEMAS EN LAS REDES IP	16
2. INGENIERÍA DE TRÁFICO.....	18
2.1 ANTECEDENTES	18
2.2 CONCEPTO DE INGENIERÍA DE TRÁFICO	19
2.2.1 Contexto de la Ingeniería de Tráfico	20
2.2.1.1 Contexto de Red	20
2.2.1.2 Contexto del Problema.....	21
2.2.1.3 Contexto de la Solución.....	22
2.2.1.4 Contexto de Operación e Implementación.....	22
2.3 EVOLUCIÓN DE LA INGENIERÍA DE TRÁFICO	23
2.3.1 Modelo Clásico.	23
2.3.2 Enrutamiento Adaptativo (en la ARPANET)	23
2.3.3 Enrutamiento Dinámico.....	24
2.3.4 Enrutamiento del Tipo de Servicio (ToS - Type of Service)	24

2.3.5	Multitrayectos de Igual Costo (ECMP - Equal Cost MultiPath)	25
2.3.6	Nimrod	25
2.3.7	Modelo Superpuesto	25
2.3.8	Enrutamiento Restringido (CR - Constraint Based Routing)	26
2.4	FUNCIONES DE OPTIMIZACIÓN Y EVALUACIÓN DEL DESEMPEÑO	26
2.4.1	Funciones de optimización	26
2.4.1.1	Gestión de tráfico	27
2.4.1.2	Gestión de Capacidad	28
2.4.2	Funciones de evaluación del desempeño	29
2.5	MODELO DE LA INGENIERÍA DE TRÁFICO	30
2.5.1	Componentes del Modelo de la Ingeniería de Tráfico	32
2.5.1.1	Subsistema de medidas	32
2.5.1.2	Modelado, Análisis Y Simulación	33
2.5.1.3	Optimización	33
2.6	CLASIFICACIÓN DE LA INGENIERÍA DE TRÁFICO	34
2.6.1	Dependiente del Tiempo vs Dependiente del Estado vs Dependiente de Eventos	34
2.6.2	Offline vs Online	35
2.6.3	Centralizado vs Distribuido	35
2.6.4	Local vs Global	35
2.6.5	Prescriptivo vs Descriptivo	36
2.6.6	Bucle Abierto vs Bucle Cerrado	36
2.6.7	Táctico vs Estratégico	36
2.7	REQUERIMIENTOS DE LA INGENIERÍA DE TRÁFICO	36
2.7.1	Requerimientos Genéricos No Funcionales	37
2.7.2	Requerimientos de encaminamiento de Tráfico	38
2.7.3	Requerimientos de Medidas	39
2.7.4	Requerimientos de Supervivencia de Red	39
2.7.5	Ingeniería de Tráfico en Ambientes de Servicios Diferenciados	40
2.7.6	Control en la Red	40
2.7.7	Gestión de congestión	41
3.	CONMUTACIÓN DE ETIQUETAS MULTIPROTOCOLO - MPLS: CONCEPTOS Y CARACTERÍSTICAS	43
3.1	EVOLUCIÓN DE MPLS	43
3.2	DEFINICIÓN DE MPLS	45
3.3	ARQUITECTURA MPLS	48
3.3.1	Estructura de Red	48
3.3.2	Clase Equivalente de Envío (FEC - Forwarding Equivalence Class)	49

3.3.3	Descripción de Etiquetas	50
3.3.4	Encapsulación de Etiquetas	51
3.3.5	Pila De Etiquetas.....	53
3.3.6	Trayecto Conmutado de Etiquetas (LSP - Label Switched Path)	54
3.4	CONMUTACIÓN DE ETIQUETAS	55
3.5	OPERACIONES SOBRE LAS ETIQUETAS	56
3.5.1	Asignación de Etiquetas	57
3.5.2	Mapeo de la etiqueta entrante (ILM - Incoming Label Map)	59
3.5.3	Mapeo del FEC a un NHLFE (FTN - FEC to NHLFE Map)	60
3.5.4	Protocolo de Distribución de Etiquetas	60
3.5.4.1	Distribución de etiquetas usando RSVP	60
3.5.4.2	Distribución de etiquetas usando LDP	61
3.5.4.3	Distribución de etiquetas usando CR-LDP	63
3.5.4.4	Distribución de etiquetas usando BGP.....	64
3.5.4.5	Modos de distribución de etiquetas	65
3.5.5	Unión de Etiquetas	65
3.5.6	Agregación	65
3.6	ENRUTAMIENTO MPLS	66
3.6.1	Enrutamiento explícito.	66
3.6.2	Enrutamiento Restringido	67
3.7	CONTROL DE ESTABLECIMIENTO DE LSPs	67
3.8	FUNCIONAMIENTO GLOBAL DE MPLS	69
3.9	APLICACIONES.....	70
3.9.1	Redes Privadas Virtuales (VPN - Virtual Private Network)	70
3.9.2	Ingeniería de Tráfico	71
3.9.3	Calidad de Servicio QoS.....	71
3.9.4	Redes Ópticas	72
3.9.5	Voz sobre IP con MPLS	72
4.	INGENIERÍA DE TRÁFICO CON MPLS	75
4.1	CONCEPTOS GENERALES DE MPLS EN LA TE	75
4.2	COMPONENTES DE TE-MPLS	77
4.2.1	Componente de Control.	78
4.2.1.1	Módulo de Distribución de Información.....	79
4.2.1.2	Tablas de Enrutamiento.	79
4.2.2	Componente de Envío.....	81
4.2.2.1	Selección de Trayectos.	82

4.2.2.2	Análisis y Planeación Offline.	83
4.3	TRONCALES DE TRÁFICO	83
4.3.1	Troncales de Tráfico Bidireccionales.	84
4.3.2	Operaciones Básicas Sobre las Troncales de Tráfico.	84
4.3.3	Atributos Básicos de las Troncales de Tráfico.	85
4.4	ENRUTAMIENTO RESTRINGIDO	85
4.4.1	Métricas para Calcular el Trayecto.	87
4.4.2	Selección de la Ruta Óptima.	89
4.4.3	CR con Restricciones de Retardo y Jitter.	90
4.4.4	CR con Restricciones de Retardo.	91
4.5	BALANCE DE CARGA.....	91
4.5.1	División del Tráfico.	92
4.5.2	Proceso de Medidas.	93
4.6	FUNCIONALIDADES DE TE-MPLS	94
4.6.1	QoS en TE-MPLS.....	94
4.6.2	Recuperación de Fallas	99
4.6.2.1	Detección de Fallas.....	102
4.6.2.2	Notificación de Fallas.	102
4.6.2.3	Topología del Modelo de Recuperación de Fallas.....	104
4.6.2.3.1	Recuperación Local	104
4.6.2.3.2	Reparación Global.....	105
4.6.2.4	Tolerancia a Fallas.....	106
4.6.3	Mecanismos de Prevención de Bucles (Loops).....	107
5.	CRITERIOS DE DISEÑO Y MIGRACIÓN DE LAS REDES MPLS	111
5.1	JUSTIFICACIÓN DE LA MIGRACIÓN A UNA RED MPLS.....	111
5.2	ESTRUCTURA DE RED	112
5.3	CRITERIOS DE DISEÑO.....	113
5.3.1	Localización y Diseño de los Puntos de Presencia	115
5.3.2	Dimensionamiento de los Enlaces del Backbone.....	117
5.3.3	Diseño del Enrutamiento IP	122
5.3.4	Dimensionamiento del Espacio de las Etiquetas MPLS	128
5.3.5	Diseño del Sistema TE-MPLS para Soporte de QoS.....	130
5.3.6	Resultados del Diseño de la Red Colombiana.	142
5.3.6.1	Descripción de los Enrutadores MPLS	143
5.3.7	Evaluación y Optimización de la Red	144
5.3.7.1	Optimización de tiempos de convergencia	145

5.4 ASPECTOS A TENER EN CUENTA EN LA IMPLEMENTACION DE MPLS146

6. CONCLUSIONES Y RECOMENDACIONES 148

ACRÓNIMOS 154

BIBLIOGRAFÍA 158

ANEXOS

ANEXO A. Enrutamiento en Redes de Paquetes.

ANEXO B. Calidad de Servicio.

ANEXO C. RSVP Signaling Extensions for MPLS Traffic Engineering.

TABLA DE FIGURAS

Figura 1.1.	Relación entre el Modelo de Referencia OSI y el Conjunto de Protocolos TCP/IP.	5
Figura 1.2.	Formato de Datagrama IP.	7
Figura 1.3.	Formato del Campo Tipo de Servicio.	8
Figura 2.1.	Ciclo de QoS.	28
Figura 2.2.	Interacción entre la Ingeniería de Tráfico y la Red.	30
Figura 2.3.	Modelo del Proceso de Ingeniería de Tráfico.	31
Figura 3.1.	Modelo Superpuesto.	44
Figura 3.2.	Pila de Protocolos.	46
Figura 3.3.	Dominio MPLS.	49
Figura 3.4.	Concepto de Granularidad.	50
Figura 3.5.	Encapsulación Genérica.	51
Figura 3.6.	ATM como Nivel de Enlace de Datos.	52
Figura 3.7.	Frame Relay como Nivel de Enlace de Datos.	52
Figura 3.8.	Pila de Etiquetas.	53
Figura 3.9.	Intercambio de Etiquetas.	56
Figura 3.10.	Flujo de Establecimiento de un LSP por medio de RSVP.	60
Figura 3.11.	Formato de los Mensajes LDP.	61
Figura 3.12.	Encaminamiento de un LSP-LDP a través de un LSP-RSVP.	62
Figura 3.13.	LSP-LDP a través de LSP-RSVP con un mismo LER de Entrada.	63
Figura 3.14.	Flujo de Establecimiento de un LSP por medio de CR-LDP.	63
Figura 3.15.	Formato de las Etiquetas y el Prefijo de Dirección Codificado en BGP.	64
Figura 3.16.	Establecimiento LSP Ordenado (Parte A).	68
Figura 3.17.	Establecimiento LSP Ordenado (Parte B).	68
Figura 3.18.	Funcionamiento MPLS.	69
Figura 3.19.	Modelo de Referencia de VoMPLS.	73
Figura 4.1.	Componentes de la TE-MPLS.	77
Figura 4.2.	Módulos del Componente de Control.	78
Figura 4.3.	Componente de Distribución de Información.	79
Figura 4.4.	Tablas de Enrutamiento y Envío MPLS Cuando se Configura la TE con BGP.	80
Figura 4.5.	Tablas de Enrutamiento y Envío MPLS Cuando se Configura la TE con BGP-IGP.	81
Figura 4.6.	Cálculo de Rutas Explícitas en el LER de Entrada.	82
Figura 4.7.	Componente de Selección de Trayectos.	83
Figura 4.8.	Interacción Entre CR e IGP Convencional.	86

Figura 4.9. Contexto Operacional CR.....	86
Figura 4.10. Algoritmo de Distribución.....	92
Figura 4.11. Posición Relativa de los Componentes de la Estructura QoS.....	94
Figura 4.12. Estructura del Campo DS.....	95
Figura 4.13. Nuevos Campos de la Tabla de Envío.....	96
Figura 4.14. Funcionamiento de WRED.....	98
Figura 4.15. Conmutación Protegida.....	101
Figura 4.16. Reenrutamiento Rápido.....	101
Figura 4.17. RNT en una red MPLS.....	104
Figura 4.18. Recuperación de Enlace.....	104
Figura 4.19. Recuperación de Nodo Sin Objeto Almacén de Ruta.....	105
Figura 4.20. Recuperación de Nodo Con Objeto Almacén de Ruta.....	105
Figura 4.21. Reparación Global.....	106
Figura 4.22. Reparación Global con Trayectos Shortcut.....	106
Figura 4.23. LSR Tolerante a Fallas.....	107
Figura 4.24. Ejemplo del Algoritmo PD.....	109
Figura 4.25. Estructura de los mensajes "thread".....	109
Figura 4.26. Ejemplo del Algoritmo Colored Threads.....	110
Figura 5.1. Estructura de los ISPs.....	113
Figura 5.2. Red Colombiana.....	114
Figura 5.3. Configuraciones de los PoPs.....	115
Figura 5.4. Estructura de los PoP.....	117
Figura 5.5. Anchos de Banda de las Líneas de Acceso.....	118
Figura 5.6. Proceso de Cálculo de los Enlaces.....	121
Figura 5.7. Ancho de Banda Total de los Enlaces.....	122
Figura 5.8. Punto de Vista Físico.....	123
Figura 5.9. Punto de Vista Funcional.....	124
Figura 5.10. Punto de Vista de Enrutamiento.....	124
Figura 5.11. Costos de los Enlaces de la Red Colombiana.....	125
Figura 5.12. Árbol SPF.....	127
Figura 5.13. Topología de Red MPLS.....	132
Figura 5.14. Reajuste de los Anchos de Banda de los Enlaces.....	133
Figura 5.15. Anchos de Banda Totales de los Enlaces después del Reajuste.....	134
Figura 5.16. Asignación Final de los Anchos de Banda.....	135
Figura 5.17. Costos Totales.....	137
Figura 5.18. Recuperación de Fallas de Nodo.....	140
Figura 5.19. Recuperación de Fallas de Enlace.....	140
Figura 5.20. Red MPLS con Recuperación de Fallas.....	141
Figura 5.21. Monitoreo de Tráfico en la Red MPLS.....	142
Figura 5.22. Interacción de los Componentes del Sistema TE-MPLS.....	143
Figura 5.23. Modelo de un LSR.....	144
Figura 5.24. Migración hacia MPLS.....	147

ÍNDICE DE TABLAS

Tabla 4.1. Tabla de Conexión Inversa para LSR3.....	103
Tabla 5.1. Matriz de Tráfico Unidireccional.	119
Tabla 5.2. Matriz de Tráfico Bidireccional.	120
Tabla 5.3. Capacidades Estimadas y Asignadas de los Enlaces.	122
Tabla 5.4. Bases de Datos de Estado de Enlace para R1, R2, y R4.	126
Tabla 5.5. Tabla de los Trayectos más Cortos.....	126
Tabla 5.6. Tabla de Enrutamiento para R1.	127
Tabla 5.7. LIB para R1.....	130
Tabla 5.8. Capacidades Estimadas y Asignadas.	134
Tabla 5.9. Tabla Final de Enrutamiento IP.	137
Tabla 5.10. LIB de MPLS.	139

INTRODUCCIÓN

El crecimiento de las redes IP y el incremento en la demanda de nuevos servicios, plantea un desafío para los Proveedores de Servicio de Internet (ISPs - Internet Service Provider), quienes para mantenerse al ritmo de la demanda deberán evolucionar sus redes a estructuras escalables, multiservicio, fáciles de gestionar y con funcionalidades que les permitan satisfacer los requerimientos de Calidad de Servicio (QoS - Quality of Service) exigidos por los usuarios.

La industria del sector de las telecomunicaciones está en una búsqueda constante de soluciones a problemas de escalabilidad e interoperabilidad, y han generado propuestas que combinan las mejores características de las tecnologías de nivel de enlace y nivel de red para simplificar los procesos de enrutamiento y envío de paquetes. Estas propuestas (IP Switching, Tag Switching, Aggregate Route-Based IP Switching, IP Navigator y Cell Switching Router) que surgieron como una primera aproximación a las tecnologías de conmutación multinivel, eran propietarias y sólo satisfacían necesidades particulares.

En vista que el concepto de conmutación multinivel ofrecido por estas propuestas era innovador e introducía cambios tecnológicos fundamentales en las redes, el Grupo de Trabajo en Ingeniería de Internet (IETF - Internet Engineering Task Force) decidió definir una tecnología estándar que reuniera las características más relevantes de cada una de ellas. Fue así como surgió la tecnología de Conmutación de Etiquetas Multiprotocolo (MPLS - Multiprotocol Label Switching), que busca incrementar las funcionalidades de la red combinando eficazmente las funciones de control de enrutamiento con la simplicidad y rapidez de la conmutación de nivel de enlace. Al integrar en una sola tecnología lo mejor de cada nivel, MPLS ofrece nuevas posibilidades en la gestión del backbone, así como en la provisión de nuevos servicios de valor agregado.

MPLS usa la conmutación IP junto con el algoritmo de intercambio de etiquetas para optimizar el envío de paquetes sin alterar los protocolos de enrutamiento IP existentes. Aunque MPLS en un principio fue creada para cumplir el anterior propósito, actualmente se está consolidando como una tecnología que ofrece nuevas capacidades de enrutamiento, donde no sólo se toma en cuenta el prefijo de dirección para encaminar los paquetes, sino que también se consideran las necesidades de los proveedores y de los usuarios que se reflejan en restricciones de ancho de banda, espacio en el buffer, niveles de QoS, etc.

Otro aspecto importante en MPLS es la separación de los componentes de envío y control, que facilita el desarrollo de servicios de enrutamiento avanzados sin la necesidad de modificar el paradigma de envío de paquetes. Esta separación permite implementar satisfactoriamente las

funcionalidades de ingeniería de tráfico sin los problemas de compatibilidad, gestión y costos que se presentaban con las tecnologías convencionales. Todas estas características han permitido que los proveedores de servicio se interesen en MPLS para transformar sus infraestructuras y convertirlas en las redes de la próxima generación.

A raíz del interés despertado por esta tecnología en los sectores educativo y comercial a nivel mundial, surgió la necesidad de realizar este trabajo que identifica las debilidades de la tecnología IP actual y recopila los aspectos de mayor interés de MPLS que hacen parte de la solución a estos problemas.

El objetivo de este trabajo es analizar la influencia que ha tenido MPLS en el entorno de las telecomunicaciones y su interacción con tecnologías como IP, Frame Relay, ATM, VPNs, QoS, Ingeniería de tráfico y redes ópticas, para finalmente generar unos criterios de diseño y migración de las redes IP a MPLS.

Esta monografía introduce los conceptos principales de las redes IP, la ingeniería de tráfico y MPLS, y consta de 6 capítulos estructurados de la siguiente forma:

Capítulo I. Redes IP - Conceptos Fundamentales. En este capítulo se establecen las bases de funcionamiento en los aspectos relacionados a la conmutación y el enrutamiento de las redes IP.

Capítulo II. Ingeniería de Tráfico en Redes IP. Plantea de manera global los conceptos más relevantes de la ingeniería de tráfico en las redes IP.

Capítulo III. Conmutación de Etiquetas Multiprotocolo MPLS: Conceptos y Características. Presenta un marco teórico, bases conceptuales y aspectos particulares relacionados con esta tecnología, además de la forma en que MPLS interactúa en campos como: calidad del servicio, redes privadas virtuales, integración IP/ATM, aplicación en redes ópticas, entre otras.

Capítulo IV. Ingeniería de Tráfico con MPLS. Describe cómo MPLS influye en el campo de la ingeniería de tráfico, identificando los aspectos particulares en los que da una solución a los problemas de las redes actuales.

Capítulo V. Criterios de Diseño y Migración de las Redes MPLS. De acuerdo a la información recopilada se definen los criterios para aplicar la técnica MPLS en las redes IP.

Capítulo VI. Conclusiones y Recomendaciones. En este capítulo se recogen las conclusiones y recomendaciones del trabajo realizado.

La realización de este trabajo, fortalece los conocimientos de las nuevas tecnologías que están incursionando en el campo de las telecomunicaciones y establece las bases para futuros proyectos en esta área.

1. REDES IP - CONCEPTOS FUNDAMENTALES

Las redes de datos surgieron por la necesidad existente de intercambiar información entre sistemas de cómputo para el procesamiento de datos. Como consecuencia, se desarrollaron una serie de protocolos para facilitar la comunicación entre sistemas heterogéneos y que se han convertido en el fundamento de las redes IP y en particular de Internet. Actualmente éste conjunto de protocolos se conoce como Protocolos TCP/IP o Protocolos Internet.

Los Protocolos TCP/IP fueron adoptados por una gran número de usuarios, desde proveedores de servicio, entes educativos y de investigación, empresas comerciales y gubernamentales hasta los usuarios finales, lo cual condujo a que se convirtiera en un estándar de facto. La acogida de los protocolos TCP/IP se debió a su independencia de la tecnología y su amplio conjunto de protocolos estándar, que brinda interoperabilidad y un alto nivel de funcionalidad.

En este capítulo se presenta una visión general de las características de funcionamiento de la arquitectura modular TCP/IP, principalmente del nivel Internet, con el fin de detallar los problemas que afrontan las redes IP actualmente.

1.1 EVOLUCIÓN DE LAS REDES IP

A principios de la década de 1970 apareció ARPANET, una red utilizada para interconectar un pequeño grupo de computadores de instituciones universitarias y de investigación con los de la red DARPA (US Defense Advanced Research Projects Agency - Agencia de Proyectos de Investigación Avanzados del Departamento de Defensa de los EUA), como parte de un trabajo conjunto sobre la creación e interconexión de redes.

Esta red fue creciendo rápidamente durante algunos años, pero fue en 1972 cuando se comenzó a investigar la forma en que los paquetes de información podían moverse a través de varias redes de diferentes tipos que no eran necesariamente compatibles. Este proyecto, que buscaba conectar los computadores de forma transparente, recibió el nombre de "Internetting" y para referirse al sistema de redes funcionando conjuntamente se utilizó el nombre de "Internet".

La Internet continuó su expansión a nivel internacional, permitiendo el intercambio de gran cantidad de datos y convirtiéndose en el medio ideal para el manejo de información, debido en gran parte a los nuevos medios creados para facilitar a los usuarios el acceso a la misma.

Internet usa para su interconexión el conjunto de protocolos TCP/IP cuyas especificaciones son de dominio público, y es ampliamente utilizado por todos los elementos de red para su intercomunicación. Se debe tener en cuenta que en Internet existen elementos cuyo hardware y software son de clases muy diferentes, y existen distintos medios de conexión; es aquí donde se encuentra una de las grandes ventajas de TCP/IP, pues al ser compatible con cualquier sistema operativo y con cualquier tipo de hardware la comunicación entre diversos sistemas de cómputo es posible.

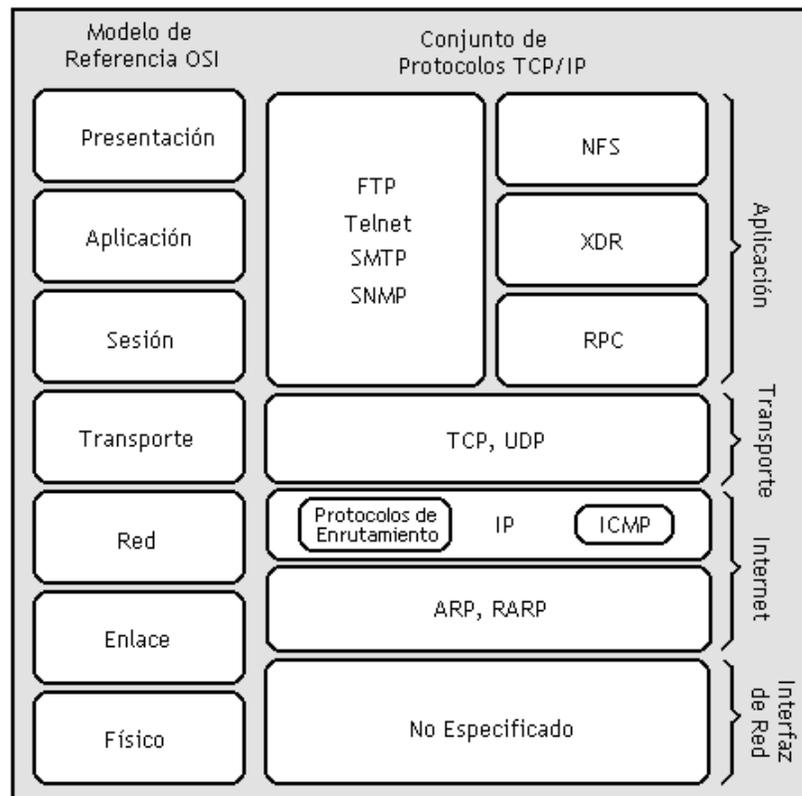
Internet, así como las redes que utilizan el conjunto de protocolos TCP/IP (redes IP), son redes de conmutación de paquetes, en las cuales los datos para ser transferidos a través de la red son divididos en pequeñas unidades llamadas *paquetes* que son procesados individualmente en cada enrutador hasta llegar a su destino. Un paquete, el cual usualmente contiene solo unos pocos cientos de bytes de datos, transporta una identificación que permite a los nodos intermedios establecer la forma de enviarlo a su destino final. En éstas redes, un conjunto de paquetes que tienen el mismo origen y destino, no necesariamente siguen la misma ruta para alcanzar dicho destino. En la conmutación de paquetes se pueden procesar simultáneamente múltiples comunicaciones entre computadores; pero si la actividad en la red se incrementa, se tiende a disminuir la capacidad empleada por cada uno de los equipos que están haciendo uso del enlace.

1.2 ARQUITECTURA MODULAR DE LAS REDES IP

La arquitectura modular TCP/IP es un modelo común de referencia que especifica y clasifica las funciones desempeñadas por los protocolos de comunicación, en niveles o capas similares a las implementadas por el modelo de referencia OSI.

La arquitectura TCP/IP está compuesta por cuatro capas o niveles, una sobre la otra, que cooperan entre sí, y en donde las capas inferiores brindan servicios a las capas superiores y a su vez, cada una de ellas intercambia información con su capa par en el nodo remoto para realizar las funciones de comunicación exitosamente.

En la Figura 1.1 se ilustra la relación entre los niveles del modelo de referencia OSI (Open System Interconnection) y el conjunto de Protocolos TCP/IP.



ARP - Addresses Resolution Protocol *Protocolo de Resolución de Direcciones*
 FTP - File Transfer Protocol *Protocolo de Transferencia de Archivos*
 ICMP - Internet Control Message Protocol *Protocolo de Mensajes de Control en Internet*
 RARP - Reverse Addresses Resolution Protocol *Protocolo de Resolución de Direcciones Inverso*
 SNMP - Simple Network Management Protocol *Protocolo de Gestión de Red Simple*
 TCP - Transmission Control Protocol *Protocolo de Control de Transmisión*
 UDP - User Datagram Protocol *Protocolo de Datagramas de Usuario*
 RPC - Remote Procedure Call *Llamadas a Procedimientos Remotos*
 XDR - eXternal Data Representation *Representación Externa de Datos*
 NFS - Network File System *Sistema de Archivos de Red*

Figura 1.1. Relación entre el Modelo de Referencia OSI y el Conjunto de Protocolos TCP/IP.

- **Nivel de Aplicación:** Es el nivel más alto, y está constituido por protocolos que proveen servicios (correo electrónico, transferencia de archivos, conexión remota, gestión de red, etc.) a los usuarios finales. Los programas de aplicación requieren de un protocolo específico en el nivel de aplicación (SNMP, FTP, Telnet, HTTP, etc). Las aplicaciones interactúan con uno de los protocolos del nivel de transporte para enviar o recibir datos. Cada programa de aplicación escoge el estilo de transporte necesario, el cual puede ser una secuencia de mensajes individuales o un flujo continuo de bytes. El nivel de aplicación corresponde a los niveles de sesión, presentación y aplicación del modelo OSI.

- **Nivel de Transporte:** La principal tarea de la capa de transporte es proporcionar la comunicación extremo a extremo desde un programa de aplicación a otro. El nivel de transporte debe regular el flujo de información, además de proveer un transporte fiable para asegurar que los datos lleguen sin errores y en secuencia a su destino. El software de transporte divide el flujo de datos que recibe del nivel de aplicación en pequeñas unidades (llamados segmentos) y pasa cada segmento con una dirección de destino a la capa siguiente para su transmisión. Este nivel coincide con el nivel de transporte del modelo OSI. Los protocolos más comunes en éste nivel son el TCP y el UDP.
- **Nivel Internet:** Este nivel se encarga del direccionamiento y encaminamiento de los datos hacia el sistema destino; encapsula el segmento en datagramas IP, le adiciona una cabecera, usa un algoritmo de enrutamiento para determinar si el datagrama será entregado directamente o enviado a un enrutador, y lo pasa a la interfaz de red apropiada para la transmisión. También maneja los datagramas entrantes, chequea su validez, y usa un algoritmo de enrutamiento para decidir si el datagrama debe ser procesado localmente o reenviado. El nivel de Internet corresponde al nivel de red del modelo de referencia OSI.
- **Nivel Interfaz de Red:** El nivel más bajo de la arquitectura es el responsable de aceptar los datagramas IP, encapsularlos en tramas, y transmitirlos sobre una red específica. Una interfaz de Red consiste de un controlador de dispositivo (generalmente proporcionado por el fabricante del hardware) y de un protocolo específico que depende del tipo de red sobre la que se está trabajando (X.25, LAN, X.21, etc.). Este nivel corresponde a los niveles físico y de enlace del modelo de referencia OSI.

Para comprender el funcionamiento de ésta arquitectura, es necesario entender cómo interactúan los niveles durante el proceso de comunicación.

Como el modelo de referencia indica, los protocolos (los cuales componen las diversas capas o niveles) son como una pila de bloques constitutivos uno encima del otro. Los datos pasan desde la capa superior de la pila hacia la siguiente hasta que son transmitidos por los protocolos de nivel de acceso a la red. En el extremo remoto, los datos se entregan desde el nivel inferior hacia la aplicación receptora.

Una capa individual no necesita saber cómo los niveles superiores o inferiores funcionan, simplemente necesita conocer cómo pasar los datos entre ellas.

Cada nivel en la pila adiciona información de control en la cabecera para asegurar su propia entrega y cada capa trata la información recibida de los niveles superiores como datos a ser transmitidos colocando su propia cabecera al frente de éstos. Este proceso es conocido como encapsulación.

Cuando los datos son recibidos en el sistema remoto, ocurre el proceso inverso (conocido como desencapsulación): cada nivel retira su información de la cabecera antes de pasar los

datos al nivel superior de la pila. La información fluye de abajo hacia arriba, y las capas la interpretan como un campo de cabecera y uno de datos.

Este mecanismo, conocido como comunicación par a par, permite a cada nivel en el sistema origen comunicarse con su nivel par en el sistema remoto.

En las redes IP, la funcionalidad más importante es la forma en que los datos son encaminados desde el origen hasta el destino. Esta función se realiza en el nivel Internet, conformado por varios protocolos que desempeñan las funciones de encaminamiento de los datos entre redes. En la siguiente sección se tratan más a fondo las funciones de éste nivel.

1.3 NIVEL INTERNET

El protocolo más importante en ésta capa es el Protocolo Internet (IP-Internet Protocol). IP proporciona un servicio de distribución de paquetes no orientado a la conexión, es decir, no intercambia mensajes de control para establecer una conexión extremo a extremo antes de transmitir la información del usuario. Al ser un protocolo no orientado a la conexión, pueden presentarse pérdidas, datagramas duplicados, y desorden en la recepción de los mismos. Estas características hacen de IP un protocolo del "mejor esfuerzo" o un *Protocolo no confiable*.

Las labores de recuperación de errores dependen de protocolos de nivel superior. Sin embargo, el nivel Internet define el Protocolo de Mensajes de Control de Internet (ICMP - Internet Control Message Protocol) para la notificación de situaciones anómalas del sistema. IP también dependerá de protocolos de otros niveles para establecer conexiones en caso de que algún protocolo de aplicación requiera de servicios orientados a la conexión.

IP determina una unidad básica, llamada datagrama, y una serie de reglas para su procesamiento en las redes IP. Un datagrama consta de una cabecera con información necesaria para el funcionamiento del protocolo, y una parte de datos, que corresponde a la información de usuario o carga útil a transportar. La cabecera esta formada por una parte fija de 20 bytes, y una parte opcional de longitud variable como se muestra en la Figura 1.2.

bits
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 32

Versión	IHL	Tipo de Servicio	Longitud Total	
Identificación			Bandera	Desplazamiento del Fragmento
TTL		Protocolo	Suma de Verificación de Cabecera	
Dirección IP de Origen				
Dirección IP de Destino				
Opciones				
Datos				

Figura 1.2. Formato de Datagrama IP.

- **Versión.** Indica la versión del protocolo Internet usada para la creación del datagrama y asegura que todos los demás sistemas (enrutadores y nodos) que lo procesan interpreten los distintos campos en forma correcta. Si un enrutador recibe un datagrama con una versión IP que no conoce, sencillamente lo descarta, evitando una interpretación errónea del datagrama.
- **Longitud de Cabecera IP (IHL - IP Header Length).** Especifica la longitud de la cabecera del datagrama en múltiplos de palabras de 32 bits; si la longitud de los campos opcionales no es múltiplo exacto de 32 bits se utiliza un campo de relleno al final de la cabecera. El valor mínimo para la longitud de la cabecera es 5 y el máximo es 15.
- **Tipo de Servicio.** Especifica el manejo del datagrama durante su transmisión a través de la red. La información de este campo permite encaminar los paquetes por la ruta más óptima, y se utiliza para tomar decisiones acerca de cuales paquetes descartar en situaciones de congestión. Los tres primeros bits indican la precedencia, la cual puede ser de 0 a 7: 0 es la precedencia normal y 7 es reservado para los paquetes. Los siguientes tres bits definen la prioridad del retardo, rendimiento y fiabilidad. Los dos últimos bits son reservados para el futuro. La Figura 1.3 muestra el formato de éste campo.

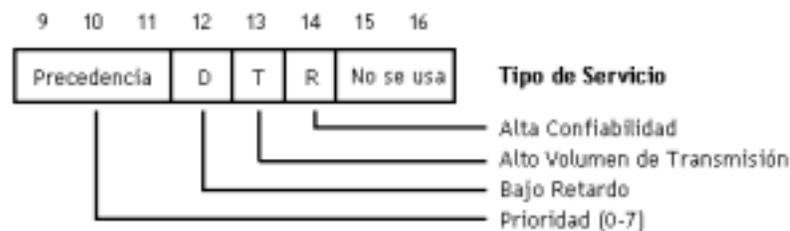


Figura 1.3. Formato del Campo Tipo de Servicio.

- **Longitud Total.** Especifica la longitud en bytes del datagrama IP, incluyendo datos y cabecera. El valor máximo es de 65536 bytes.
- **Identificación.** Es un número único que usa el transmisor para identificar cada uno de los datagramas emitidos. Este campo se usa para ayudar a reconocer las partes de un datagrama que han sido fragmentado en el camino.
- **Bandera.** Constituido por tres bits de los cuales actualmente se usan dos, el primer bit, no fragmentado DF (Don't Fragment) cuando está a 1 indica que el datagrama no puede ser fragmentado. El segundo bit de más fragmentos MF (More Fragments) fijado a 1 especifica que el datagrama es un fragmento y que no es el último. Si esta a 0 indica que éste es el último fragmento (o bien que el datagrama original no esta fragmentado). El tercer bit no es usado.
- **Desplazamiento del fragmento (Offset).** Sirve para indicar en que posición del datagrama original se ubica éste fragmento.

- **Tiempo de Vida (TTL - Time To Live).** Representa el número máximo de saltos que un datagrama puede existir en la red antes de ser descartado, evitando que viajen indefinidamente. Un datagrama puede existir un máximo de 255 saltos. En cada enrutador por el cual pasa el datagrama, el campo TTL es decrementado en 1, si se alcanza el valor de 0 es descartado. El valor inicial de TTL fija el número máximo de saltos que podrá dar, y por tanto debe ser lo suficientemente grande como para que llegue a su destino.
- **Protocolo.** Representa el protocolo de nivel de transporte que recibirá el datagrama entrante. Normalmente utiliza TCP y UDP; pero puede identificar 255 protocolos del nivel de transporte.
- **Suma de verificación de la cabecera (Checksum).** Sirve para detectar errores producidos en la cabecera del datagrama. Este campo se recalcula en cada salto debido a que siempre al menos un campo de la cabecera cambia, por ejemplo TTL.
- **Dirección IP de origen.** Indica la dirección IP del nodo origen.
- **Dirección IP de destino.** Indica la dirección IP del nodo destino.
- **Opciones.** Utilizada para transmitir información adicional relacionada con la seguridad, el enrutamiento de origen, registro de ruta, identificación del flujo y marca de tiempo. El campo tiene una longitud variable que podría no ser múltiplo de 32 bits. Para garantizar que el número total de bytes en la cabecera sea divisible por cuatro se utiliza un campo de relleno al final del campo opciones.
- **Datos.** Contiene la información generada por los niveles superiores de la pila de protocolos TCP/IP.

IP define reglas o mecanismos que permiten a los nodos procesar la información de los datagramas, de modo que puedan ser reenviados hasta alcanzar su destino.

Para enviar los paquetes al destino, el protocolo IP necesita de un esquema de direccionamiento independiente del hardware. Este consiste en asignar a cada nodo un número único de 32 bits, conocido como dirección IP, que normalmente suele representarse como cuatro cifras de 8 bits separadas por puntos. Las direcciones IP tienen una estructura jerárquica: una parte corresponde al identificador de la red, y la otra al nodo dentro de esa red.

Para adaptarse a las necesidades de tamaño de las redes, se crearon diferentes clases de direcciones:

Clase A: Estas direcciones utilizan únicamente el primer byte para identificar la red con un valor comprendido entre 1.0.0.0 y 127.0.0.0. los tres últimos bytes corresponden a cada uno de los nodos que pertenecen a la red.

Clase B: El identificador de la red se obtiene de los dos primeros bytes, que tiene un valor entre 128.1 y 191.254, esto permite 16320 redes de 65024 nodos cada una.

Clase C: Las redes clase C tienen un rango de direcciones desde 192.0.0.0 hasta 223.255.255.0, contando con tres octetos para identificar la red. Por lo tanto hay cerca de 2 millones de redes de este tipo con un máximo de 254 nodos.

Clases D, E, F: Comprenden las direcciones entre 224.0.0.0 y 254.0.0.0 y están reservadas para uso futuro o con fines experimentales.

Con base en la dirección IP, el nivel Internet determina el próximo salto que debe tomar el paquete hacia su destino.

Como cada una de las redes por las que pasará el paquete pueden utilizar tecnologías diferentes, entonces, el tamaño máximo del paquete que manejan dichas redes puede variar.

El tamaño máximo de paquete recibe el nombre de Unidad de Transferencia Máxima (MTU - Maximum Transfer Unit), y ninguna red puede transmitir un paquete de mayor tamaño que el MTU especificado. Si un paquete recibido desde una red es muy grande, es función de la capa Internet adaptar su tamaño al valor del MTU, dividiéndolo en pequeños segmentos a través del proceso de fragmentación.

En el proceso de fragmentación, es necesario segmentar el paquete en un número arbitrario de fragmentos que después serán reensamblados en el nodo destino. Se requiere de información de control que permita la reconstrucción del paquete original eliminando posibles duplicados y recuperando tramas perdidas. Para lograrlo, el nodo origen proporciona un valor al campo identificador, que determinará qué segmentos pertenecen a un mismo datagrama.

En el receptor, el valor del campo identificación asegura que los fragmentos de diferentes paquetes no sean combinados. El campo offset indicará la posición de cada fragmento en el paquete original.

El proceso de reensamblado se realizará únicamente por la unidad de destino, pues no tiene sentido hacerlo en un nodo intermedio, ya que no se garantiza que todos los fragmentos de un paquete pasen por el mismo nodo para llegar al destino.

Al recibir un fragmento, el nodo destino inicia un temporizador a la espera de recibir todos los fragmentos que componen el paquete original, en caso de que el tiempo preestablecido pase el datagrama se descartará.

Durante el direccionamiento y reensamblado de datagramas dentro de un nodo o un enrutador, el nivel Internet puede descartar algunos paquetes. Hay diversas causas por las que un datagrama puede ser descartado, tales como errores de transmisión, existencia de congestión, posibles peticiones de cambios de ruta, que un nodo ó red sea inalcanzable, etc. Si no se cuenta con funciones de información de errores, un nodo no sabrá si los repetidos intentos de enviar un datagrama a cierto destino son infructuosos. Es por ello que se emplea el Protocolo de Mensajes de Control de Internet (ICMP - Internet Control Message Protocol) que proporciona un mecanismo de comunicación de información de control y de errores entre los nodos intermedios por los cuales viajan los paquetes.

ICMP es un protocolo de mantenimiento y gestión de red que ayuda a supervisar el funcionamiento de la misma, cumpliendo una serie de funcionalidades que aseguran la entrega de los paquetes, y consta de un conjunto de mensajes de control que son enviados a los nodos dentro de la red. Si un mensaje no puede ser enviado satisfactoriamente, ICMP no intentará enviarlo de nuevo, evitando sobre carga de mensajes. Algunos de los mensajes más comunes son: Informe de errores, Pruebas de alcanzabilidad, Control de congestión, Notificación de cambio de ruta, Medición del rendimiento y Direccionamiento de red.

1.4 ENRUTAMIENTO EN LAS REDES IP

1.4.1 Generalidades de Enrutamiento

En un sistema de conmutación de paquetes, el enrutamiento¹ se refiere al proceso de determinar la trayectoria más óptima que un datagrama debe seguir para alcanzar su destino.

A los dispositivos que determinan las trayectorias se les denomina enrutadores. En el proceso de enrutamiento intervienen los nodos origen y destino, así como los nodos intermedios.

El enrutamiento en las redes IP consiste en un paradigma de enrutamiento basado en el destino, es decir, que un paquete es enrutado de acuerdo a la dirección de destino contenida en la cabecera IP. El mecanismo de envío utilizado es el enrutamiento salto por salto, donde los paquetes a transmitir son analizados individualmente, y viajan por diferentes trayectos para llegar a su destino.

Para decidir la trayectoria que seguirá el paquete, la capa Internet consulta la tabla de enrutamiento presente en cada uno de los nodos de la red, en la cual se almacena la información acerca de cómo un paquete viajará hacia su destino. IP busca en la tabla de enrutamiento el identificador de red extraído de la dirección de destino y de acuerdo a los resultados de ésta búsqueda, IP decide si el paquete se envía directa o indirectamente al destino. Si el nodo destino se encuentra en la misma red local de la fuente, se usa el enrutamiento directo para la entrega del paquete; de otra manera, si el destino y la fuente

¹ Ver Anexo A - Enrutamiento en Redes de Paquetes.

están en diferentes redes, el paquete antes de entregarse al destino debe atravesar un nodo intermedio, este procedimiento se denomina enrutamiento Indirecto.

La creación y mantenimiento de las tablas de enrutamiento puede llevarse a cabo de varias formas:

Manualmente: Las tablas son creadas por el administrador de la red, y no cambian hasta que él las modifique. Si un proceso de enrutamiento usa estas tablas para definir la ruta por la cual enviar el paquete, se conoce como enrutamiento estático. Este tipo de enrutamiento no es tolerante a fallas: si un enrutador falla los enrutadores vecinos no perciben la falla.

Dinámicamente: Las tablas se mantienen y modifican automáticamente mediante la comunicación entre enrutadores. El enrutamiento dinámico usa estas tablas para determinar la ruta más óptima. Para actualizar las tablas de enrutamiento se utilizan protocolos que permiten el intercambio de información de encaminamiento entre los enrutadores. El enrutamiento dinámico es tolerante a fallas: si un enrutador falla sus vecinos propagan esta información a los otros enrutadores para actualizar sus tablas de enrutamiento.

Para permitir que los enrutadores intercambien información de enrutamiento y definan políticas de intercambio de tráfico se ha creado el concepto de Sistema Autónomo (AS - Autonomous System). Se entiende por Sistema Autónomo la red que es administrada o gestionada por una autoridad común y con un protocolo de enrutamiento homogéneo.

Los Sistemas Autónomos pueden verse como un conjunto distribuido de nodos interconectados mediante enlaces lógicos. Cada enlace utiliza varias métricas de enrutamiento, cada una de las cuales tiene asociado un valor de costo. Estas métricas son:

- Capacidad. Es una medida del volumen de transmisión del enlace en bits por segundo; un valor alto indica una capacidad más baja. En la práctica, ésta es la métrica que se usa por omisión.
- Retardo. Éste se relaciona con el retardo de tránsito promedio asociado a un enlace y, por tanto, incluye los retardos de colas en enrutadores y servidores. Una vez mas, un valor alto indica un retardo de tránsito mas largo.
- Gasto. Es una medida del costo en dinero implicado en un enlace; un valor alto indica un mayor costo monetario. Desde luego, es preferible usar una red conmutada pública que una red privada.
- Error. Es una medida de la probabilidad residual de errores asociada al circuito; los valores altos indican una mayor probabilidad de errores no detectados.

Con el término costo se indica el valor total acumulativo de los enlaces que se usan en un trayecto específico entre un par de Sistemas Terminales (ES - End System) a través de la red. Por tanto, el costo de camino asociado a una ruta puede diferir dependiendo de la métrica empleada, de modo que al definir el costo de camino más corto se hace referencia a un trayecto calculado empleando una sola métrica de enrutamiento.

1.4.2 Clasificación de los Protocolos de Enrutamiento

Con la definición de los Sistemas Autónomos, se dan dos niveles jerárquicos dentro de las redes IP. El realizado dentro de un Sistema Autónomo y el que se efectúa entre Sistemas Autónomos. El primero se denomina enrutamiento interno o Enrutamiento de Pasarela Interior (IGP - Interior Gateway Protocol). Al enrutamiento entre Sistemas Autónomos se le denomina enrutamiento externo o Enrutamiento de Pasarela Exterior (EGP - Exterior Gateway Protocol).

1.4.2.1 *Protocolos de Enrutamiento Interno (IGP)*

En Internet se usan actualmente diversos protocolos de enrutamiento IGP. Estos pueden agruparse en protocolos de vector distancia (como RIP) y protocolos de estado de enlace (como OSPF e IS-IS).

➤ Protocolos de vector distancia:

✓ *Protocolo de Información de Enrutamiento (RIP - Routing Information Protocol)*

RIP es un protocolo de vector distancia que facilita el intercambio de información de enrutamiento. En cada enrutador permanece una tabla de enrutamiento que indica la distancia mínima hacia cada posible destino, y está dada por el número de saltos. El número de saltos es el número de enrutadores por los que atraviesa un paquete hasta llegar a su destino. Sólo pueden haber hasta 15 enrutadores entre dos nodos cualquiera; las redes que tienen 16 o más saltos se consideran inalcanzables.

Los enrutadores anuncian el contenido de sus tablas de enrutamiento cada 30 segundos a sus enrutadores vecinos, quienes con base en ésta información actualizan sus tablas.

RIP tiene problemas como el conteo a infinito, envío excesivo de información de enrutamiento y problemas de convergencia lenta, lo cual hace de él una solución sólo para redes pequeñas.

➤ Protocolos de estado de enlace:

✓ *Sistema Intermedio - Sistema Intermedio (IS-IS Intermedium System - Intermedium System).*

IS-IS es multiprotocolo y está basado en el estado del enlace. IS-IS permite a cada uno de los enrutadores tener un conocimiento completo de la topología de la red, esto se logra por medio de un procedimiento de enrutamiento llamado inundación, el cual consiste en que cada cierto tiempo los enrutadores envían su información de estado de enlace (identificadores de red y valores de costo de cada uno de los enrutadores vecinos) a cada uno de sus vecinos y a su vez envían una copia de este mensaje a los demás enrutadores, con el fin de actualizar la base de datos de estado de enlace de cada uno de ellos.

Esta información es utilizada por el algoritmo Dijkstra² (también conocido como SPF-Shortest Path First) para calcular el camino más óptimo a los diferentes destinos.

✓ *Abrir Primero el Trayecto más Corto(OSPF - Open Shortest Path First).*

Es un protocolo de estado de enlace muy utilizado por las redes IP, de carácter abierto, basado en IS-IS. Este protocolo soporta diversidad de parámetros para el cálculo de la "métrica" tales como ancho de banda, confiabilidad, retardo, etc. Este protocolo de enrutamiento fue el primero en utilizar el campo *tipo de servicio* de la cabecera del datagrama IP.

Con OSPF un sistema autónomo puede dividirse en grupos contiguos de redes denominados áreas. Es posible resumir las rutas dentro de las áreas para reducir al mínimo las entradas de la tabla de enrutamiento. Las áreas pueden configurarse con una ruta predeterminada que resuma todas las rutas externas al sistema autónomo o al área. Como resultado, OSPF se adapta a grandes redes, y puede detectar y propagar los cambios de topología más rápido que RIP.

El funcionamiento principal del protocolo OSPF esta compuesto de tres fases:

1. Creación de la Base de Datos de Estado de Enlace (LSDB - Link State Data Base).
La LSDB es una base de datos con todos los Anuncios de Estado de Enlace (LSA - Link State Advertisements) que constan de un identificador de enrutador, sus redes conectadas y sus costos configurados por el administrador de la red (los costos de los enlaces son un reflejo de la capacidad del enlace, retardo o costo monetario entre otros; un valor de costo alto indica un mayor número de saltos, capacidad de enlace más baja, mayor costo monetario, etc). Para crear y sincronizar la LSDB es necesario establecer una adyacencia, que es una relación entre los enrutadores del entorno. Una vez establecida la adyacencia, cada enrutador envía su LSA a los enrutadores vecinos ó adyacentes, los cuales a su vez propagan dicha información a sus enrutadores de entorno de tal forma que todos tengan la misma LSDB.
2. Calcular el árbol SPF.
Con la información compilada en la LSDB se crea un árbol SPF de las rutas de acceso hacia los enrutadores y redes. El árbol SPF contiene una única ruta a cada enrutador y red del sistema autónomo. Cada enrutador usa el algoritmo Dijkstra para calcular la ruta de menor costo considerándose como la raíz del árbol. El árbol SPF es distinto para cada enrutador del sistema autónomo.
3. Crear las entradas de la tabla de enrutamiento.
Las entradas de la tabla de enrutamiento se calculan a partir del árbol SPF; el resultado es una serie de rutas OSPF que contienen el identificador de red IP y su

² Ver Anexo A - Enrutamiento en Redes de Paquetes, Parte 1 - Algoritmo Dijkstra.

máscara de subred, la dirección IP de reenvío del enrutador vecino adecuado, la interfaz sobre la cual se alcanza al enrutador vecino y el costo calculado por OSPF para la red. Las rutas OSPF se agregan en la tabla de enrutamiento.

1.4.2.2 Protocolos de Enrutamiento Externo (EGP)

El encaminamiento entre Sistemas Autónomos, más que resolver el problema de encontrar la ruta óptima, debe atender criterios externos para el intercambio de tráfico que obedezcan a razones de tipo político, económico, administrativo, etc. Se trata de decidir el enrutamiento entre redes que pertenecen a organizaciones diferentes (empresas, operadores o países).

➤ EGP2 (Exterior Gateway Protocol)

Es un protocolo usado para intercambiar información de enrutamiento entre sistemas autónomos diferentes. Para diferenciar el protocolo de la clase de enrutamiento EGP, se ha adicionado a su nomenclatura el número 2. EGP2 tiene tres características principales:

- ✓ Soporta un mecanismo de “adquisición de vecinos” que permite que dos enrutadores intercambien información de enrutamiento. Se dice que un enrutador adquiere un par EGP o un vecino EGP. Los pares EGP son vecinos sólo en el sentido que ellos intercambiarán información de enrutamiento, lo cual no tiene noción de proximidad geográfica.
- ✓ Los enrutadores exteriores verifican continuamente si sus vecinos EGP están activos.
- ✓ Los vecinos EGP periódicamente intercambian información de enrutamiento de la red por medio de mensajes de actualización.

➤ Protocolo de Pasarela de Frontera (BGP - Border Gateway Protocol)

Es un protocolo de vector distancia, diferente a casi todos los demás, ya que éste soluciona el problema de conteo a infinito intercambiando información que incluye además de los enrutadores accesibles y el costo, la ruta exacta utilizada en cada caso; así, el enrutador que recibe la información descarta inmediatamente las rutas que pasan por él mismo.

BGP permite introducir manualmente restricciones a reglas de tipo político aplicables al tráfico entre sistemas autónomos. Cualquier ruta que viola una regla recibe automáticamente una ponderación infinita.

1.4.3 Proceso de Enrutamiento

En ésta sección se describe el proceso de enrutamiento de las redes IP para un paquete que pasa por nodos intermedios antes de llegar a su destino.

En el nodo de origen, el programa de aplicación prepara los datos y los pasa al nivel Internet. En éste nivel los datos son encapsulados en datagramas adicionándoles la cabecera IP, en la cabecera se fija el campo TTL a un valor por defecto o a uno especificado por la aplicación y

se calcula la suma de verificación de cabecera (checksum). De acuerdo a la dirección IP destino, se busca en la tabla de enrutamiento (creada por EGP e IGP) la mejor ruta para direccionar el paquete. En caso de no encontrar una ruta para ese destino, el nivel Internet envía un mensaje de error a los niveles superiores informando de éste hecho. De no ser así, el datagrama es entregado al nivel de Interfaz de Red el cual agrega una cabecera al datagrama y envía la trama hacia la Interfaz de Red correspondiente en el siguiente salto.

En cada uno de los enrutadores por los que pasa el paquete antes de llegar a su destino, la cabecera del paquete IP es removida y analizada. Se verifica el campo checksum, y si la suma de verificación falla el paquete es automáticamente descartado; de lo contrario, el enrutador analiza el campo TTL, y si éste es igual a cero, descarta el paquete y envía un mensaje ICMP al nodo origen. Si el TTL es diferente de cero, el enrutador decrementa en uno éste campo, calcula nuevamente el campo checksum y reenvía el paquete de acuerdo a la ruta indicada en su tabla de enrutamiento.

En el destino, el nivel Internet remueve la cabecera IP, determina si la suma de verificación es correcta, y si lo es, entrega el paquete al protocolo de aplicación correspondiente, finalizando de ésta forma el proceso de comunicación entre dos nodos dentro de la red.

1.5 PROBLEMAS EN LAS REDES IP

Las redes IP, en un inicio, fueron creadas para el intercambio de datos sin considerar sus requerimientos de ancho de banda, retardos, jitter, etc. Esto trajo como consecuencia que actualmente, las redes no estén diseñadas para soportar aplicaciones que requieran de una alta calidad de servicio (QoS - Quality of Service). Las redes IP, al ser no orientadas a la conexión, hacen que los paquetes sean direccionados independientemente en cada nodo, limitándolos a los recursos disponibles en cada uno de ellos, generando una red de bajo rendimiento y poca confiabilidad, incapaz de satisfacer los requerimientos deseados por los usuarios (acceso rápido, bajo costo, aplicaciones mas robustas) y proveedores (ancho de banda ilimitado, mejores mecanismos para la gestión de tráfico, redes escalables, evolución de redes a bajo costo, etc.).

Con la demanda de nuevos servicios, las necesidades de interconexión en las redes IP aumentaron rápidamente, incrementando los requerimientos en las capacidades de procesamiento y almacenamiento de las grandes tablas de enrutamiento, que surgen de la adición de nuevos nodos a la red. El aumento del flujo de tráfico causado por las nuevas fuentes, hace necesaria la implementación de políticas de enrutamiento adecuadas que permitan a las redes manejar su tráfico eficientemente, evitando situaciones tales como cuellos de botella, pérdida de paquetes, congestión, etc. Se debe tener en cuenta que los protocolos de enrutamiento usados por las redes IP son poco escalables, lo cual impide optimizar el enrutamiento a través de nuevas políticas, por lo que la implementación de ellas es una labor costosa y dispendiosa para los administradores de la red.

Con el crecimiento de la red, la prestación de los servicios de tiempo real se ve cada vez más afectada, ya que los continuos y numerosos saltos a través de Internet hace que se experimenten retardos que no son aceptables para este tipo de servicios .

Para prevenir éstos problemas, las redes IP deben evolucionar de forma que satisfagan las demandas, requerimientos de capacidad y proporcionen una adecuada prestación de los nuevos servicios. Esto no significa simplemente adicionar más ancho de banda y recursos para manejar la carga de tráfico, sino, incrementar la eficiencia de la red simplificando los procesos de gestión de tráfico, gestión de fallas, gestión de trayectos, etc., que permitan adaptar la infraestructura de la red a las nuevas condiciones existentes.

Con los nuevos retos que enfrentan las redes IP, se han generado dentro del Grupo de Trabajo en Ingeniería de Internet (IETF - Internet Engineering Task Force) tecnologías que dan solución a éstos inconvenientes. La Conmutación de Etiquetas Multiprotocolo (MPLS - Multiprotocol Label Switching) y la Ingeniería de tráfico son dos de ellas, que brindan una alternativa a los proveedores para ofrecer nuevos servicios de alta calidad, con costos de implementación y operación relativamente bajos.

2. INGENIERÍA DE TRÁFICO EN REDES IP

Actualmente, las redes de datos no responden a los nuevos requerimientos y cambios en la demanda de servicios, debido a que sus limitaciones funcionales impiden el adecuado control del tráfico, la gestión eficiente de recursos y la implementación de políticas administrativas. La necesidad de mejorar en estos aspectos ha llevado al desarrollo de mejores y nuevas técnicas de ingeniería de tráfico que proporcionan un control más preciso sobre la operación de la red, optimizan el uso de los recursos y garantizan la entrega de altos niveles de QoS a los usuarios finales.

La introducción de la ingeniería de tráfico para el diseño y operación de las redes públicas IP, convierten el mercado de las telecomunicaciones en un ambiente más competitivo que favorece a los usuarios, al brindarles mejores servicios a menores costos; y a los administradores y proveedores de servicio proporcionándoles infraestructuras más seguras, confiables y de alto rendimiento con menores costos de operación y mantenimiento.

Este capítulo describe las características fundamentales de la Ingeniería de Tráfico, así como su evolución, estructura, clasificación y beneficios en las redes IP.

2.1 ANTECEDENTES

Con el surgimiento de servicios de valor agregado y el crecimiento en la demanda, aparecen nuevos requerimientos de QoS que exigen un control más preciso del tráfico, el uso eficiente de los recursos y en general, un mejor rendimiento en la operación de la red (que el ofrecido hasta el momento por las redes IP). Para proveer tales capacidades, se ha desarrollado la Ingeniería de Tráfico (TE - Traffic Engineering) que optimiza el desempeño de las redes y brinda una QoS garantizada. La Ingeniería de tráfico es actualmente un tema de intensa discusión en el campo de las telecomunicaciones al igual que en el Grupo de Trabajo de Ingeniería en Internet (IETF - Internet Engineering Task Force).

Históricamente, la ingeniería de tráfico ha sido difícil de implementar en las redes públicas IP.

La razón ha sido las limitadas capacidades funcionales de los protocolos de enrutamiento usados en éste tipo de tecnologías. Los actuales IGP's siempre usan el trayecto mas corto para el envío de tráfico, y aunque se conservan recursos, se presentan problemas como congestión que disminuyen el desempeño de la red; e inadecuada asignación de recursos, que hace que algunos segmentos de red sean subutilizados mientras otros son sobreutilizados. Además, para la creación de las tablas de enrutamiento, estos protocolos no tienen en cuenta la carga, el estado actual de los recursos ni las características de tráfico, impidiendo que la red responda

rápidamente a situaciones imprevistas (congestión, fallas en los enlaces, cuellos de botella, etc.) que limitan los niveles de QoS entregados a los usuarios finales. Estos inconvenientes no han facilitado la integración de los nuevos servicios de valor agregado en una misma plataforma que responda a las diferentes características de tráfico y desempeño, y a la vez conserve los niveles de rendimiento propios del sistema. Con la Ingeniería de tráfico se pretende asegurar que la red sea gestionable, escalable y cumpla con los requerimientos operacionales exigidos por cada una de las diferentes clases de servicio.

Consecuentemente, la ingeniería de tráfico es un problema de control que requiere de un manejo preciso sobre las funciones de enrutamiento para alcanzar los objetivos de desempeño operacional.

Alcanzar los objetivos de la ingeniería de tráfico en las redes IP puede ser difícil debido a las limitaciones de IPv4, al comportamiento dinámico del tráfico IP y a los continuos cambios en los recursos de la red; por lo cual es útil el desarrollo de un mecanismo que tenga capacidades de control para implementar las funciones de TE en una red IP.

2.2 CONCEPTO DE INGENIERÍA DE TRÁFICO

La ingeniería de tráfico esta relacionada con la optimización y evaluación del desempeño de las redes IP por medio de tecnologías y principios científicos para medir, modelar, caracterizar y controlar el flujo de tráfico.

La TE es una herramienta que controla la respuesta de la red a la demanda del tráfico y a otros estímulos (fallas en los enlaces, congestión, etc.) facilitando una operación segura y eficiente mediante mecanismos y políticas que incrementan la integridad de la red, y reducen su vulnerabilidad a las interrupciones del servicio. Con las funciones de TE se incrementa el valor de la red porque se proporcionan capacidades de re-enrutamiento que permiten al tráfico ser dirigido hacia trayectos alternos en caso de fallas o situaciones de congestión en la ruta primaria.

Por otra parte, la aplicación de los conceptos de TE ayuda a identificar y estructurar metas y prioridades que garanticen la QoS, e interviene en la valoración y análisis de la realización de estas metas.

La TE establece objetivos que son vistos como un proceso interactivo y continuo para el mejoramiento en el desempeño de la red y dependen de las capacidades, restricciones de operación y servicios entregados a los usuarios. Estos objetivos de desempeño son categorizados como: objetivos *orientados al tráfico* y *orientados a los recursos*.

Los objetivos de desempeño orientados al tráfico están relacionados con el aumento de la calidad del servicio y buscan disminuir la pérdida de paquetes, reducir el retardo, incrementar el rendimiento y establecer Acuerdos de Nivel de Servicio (SLAs - Service Level Agreements).

Estadísticamente, los objetivos orientados al tráfico (variación del retardo, promedio de pérdidas de paquetes, etc.) pueden ser muy útiles para la prestación de los nuevos servicios en las redes IP.

Los objetivos de desempeño orientados a los recursos están relacionados con los aspectos de optimización de la infraestructura que aseguran que ningún recurso en los segmentos de red sea sobreutilizado ó subutilizado. La adecuada gestión de los recursos es la base para alcanzar dichos objetivos.

La disminución de la congestión es una de las principales metas de la ingeniería de tráfico que puede ser clasificada tanto como un objetivo orientado al tráfico como uno orientado a los recursos. La congestión se manifiesta en dos escenarios: cuando los recursos de red son insuficientes o inadecuados para manejar la carga ofrecida y cuando el tráfico no es distribuido adecuadamente entre los recursos.

En el primer caso, la congestión se evita aumentando la capacidad de la red con técnicas de control de congestión clásica. Las técnicas clásicas tratan de regular la demanda de tal forma que el tráfico se adapte a los recursos disponibles, y para lograrlo usa mecanismos como el control de flujo, la gestión de colas, limitaciones de la tasa de transferencia, procesamiento de enlaces, entre otros. En el segundo caso, los problemas se solucionan asignando eficientemente los recursos y adoptando políticas para balancear la carga. El objetivo de esta estrategia es reducir al máximo la congestión ó alternativamente mejorar el uso de los recursos. Cuando la congestión se disminuye a través de una asignación eficiente de recursos, se logra reducir la cantidad de paquetes perdidos, disminuir el retardo en el procesamiento de los paquetes e incrementar el rendimiento en la red; por lo tanto, la calidad de servicio percibida por el usuario final se incrementa significativamente.

Con la implementación de la ingeniería de tráfico los ISPs ofrecerán más servicios con una QoS garantizada que satisfaga los requerimientos de los usuarios e incremente los ingresos y reduzca los costos de operación de los proveedores de servicios, convirtiéndolos en entes más competitivos dentro del mercado de las telecomunicaciones.

2.2.1 Contexto de la Ingeniería de Tráfico

En las redes de datos, existen diferentes escenarios donde se pueden presentar múltiples problemas de desempeño y para los cuales la ingeniería de tráfico establece políticas de solución enmarcadas en las características del entorno. De acuerdo a los objetivos de desempeño la TE se define en los siguientes escenarios:

2.2.1.1 Contexto de Red

El contexto de red define políticas de acuerdo a la estructura, políticas, características, restricciones, atributos de calidad y criterios de optimización de la red. Bajo este contexto, la red se presenta como un sistema dinámico distribuido que consiste de tres subsistemas:

subsistema de restricciones es el conjunto de elementos de red interconectados que proporcionan un servicio de transporte para el tráfico IP sujeto a ciertas limitaciones. El *subsistema de demanda* representa el tráfico transportado dentro del dominio. Y el *subsistema de respuesta* que consiste de procesos, protocolos y mecanismos que facilitan el transporte del tráfico dentro de la red.

Las redes IP deben funcionar adecuadamente aún en presencia de diferentes clases de tráfico con requerimientos de servicio específicos, estableciendo restricciones de capacidad y QoS. Respecto a las restricciones de capacidad, los elementos y recursos de red tienen características específicas que limitan la forma de manejar la demanda de tráfico. Los recursos pueden equiparse con mecanismos de control de tráfico para coordinar varias actividades de procesamiento y acceso simultáneo de diferentes paquetes, regulando el comportamiento del tráfico y ejerciendo control sobre la forma en que los elementos de red responden a estímulos internos y externos. Con las restricciones de capacidad se busca incrementar eficientemente la utilización de los recursos mientras se reduce la posibilidad de congestión.

Los requerimientos de QoS pueden expresarse como restricciones de integridad (pérdida de paquetes) o restricciones temporales en la entrega de paquetes (retardo y variación del retardo).

Para establecer las restricciones de capacidad y QoS, se consideran las características dinámicas de las redes IP atribuidas a la variación en la demanda, a la interacción entre varios procesos y protocolos, y a la rápida evolución de la infraestructura que requiere de la constante integración de nuevas tecnologías y elementos de red.

2.2.1.2 Contexto del Problema

Este contexto define los problemas que enfrenta la ingeniería de tráfico. El contexto se relaciona con la identificación, abstracción de características relevantes, representación, formulación, especificación de requerimientos, y especificación de características deseables para una solución aceptable.

Algunos problemas definidos en este contexto son:

- Aspectos referentes a la formulación explícita de problemas de desempeño de la red, identificación de requerimientos de la solución y la manera de medir y caracterizar la eficacia de la solución.
- Problemas referentes al cálculo y estimación de parámetros del estado de la red. Una solución efectiva depende de una buena estimación de la carga de tráfico ofrecida, de las restricciones de los recursos y de la topología asociada.
- Problemas relacionados a caracterizar el estado de la red y evaluar su desempeño bajo una variedad de escenarios. El problema de la evaluación del desempeño involucra dos

aspectos, uno relacionado con la evaluación del desempeño a nivel del sistema o también conocido como “macro-estado”, y otro relacionado con la evaluación a nivel de recursos o “micro-estado”. Los mecanismos de ingeniería de tráfico que tratan con la optimización del desempeño a nivel de sistema se les conocen como “macro-TE”, y a los mecanismos de optimización a nivel de recursos como “micro-TE”.

- Problemas de optimización del desempeño de la red. Estos problemas requieren de un cierto grado de control de gestión de recursos, control de enrutamiento y aumento en la capacidad de los elementos de red.

2.2.1.3 Contexto de la Solución

El contexto de la solución indica cómo resolver los problemas de la ingeniería de tráfico analizando, evaluando y seleccionando alternativas entre diferentes cursos de acción. Generalmente, el contexto se centra en el establecimiento de conclusiones acerca del estado actual o futuro de la red, además de tomar las decisiones apropiadas para elegir el curso de acciones a seguir. En el contexto de la solución se emplean las siguientes herramientas:

- Un conjunto de políticas, objetivos y requerimientos para la evaluación y optimización del desempeño.
- Herramientas en línea (online), fuera de línea (offline) y mecanismos para medir, caracterizar, modelar, controlar el tráfico IP, asignar recursos, y distribuir el tráfico dentro de la infraestructura.
- Conjunto de restricciones operacionales, protocolos de red, y sistemas de ingeniería de tráfico.
- Conjunto de metodologías cuantitativas y cualitativas para la abstracción, formulación y solución de los problemas de la ingeniería de tráfico.
- Conjunto de parámetros de control administrativo que pueden ser manipulados por medio de un sistema de gestión de configuración. Este sistema incluye subsistemas de control, contabilidad y revisión de configuración.
- Conjunto de principios para la evaluación, optimización y mejoramiento del desempeño de red.

2.2.1.4 Contexto de Operación e Implementación

El contexto de operación e implementación realiza la planeación, organización y ejecución de los componentes del sistema de ingeniería de tráfico. La planeación comprende un conjunto de acciones para cumplir con los objetivos deseados. La organización, determina y asigna las responsabilidades de cada uno de los componentes del sistema y coordina las actividades para

alcanzar los objetivos de la TE. La ejecución es la aplicación de acciones correctivas y preventivas para mantener las metas de ingeniería de tráfico.

2.3 EVOLUCIÓN DE LA INGENIERÍA DE TRÁFICO

La optimización de las redes de datos comenzó junto con el surgimiento de la ARPANET cuyas capacidades de gestión eran muy limitadas. A medida que la demanda de servicios aumentaba, los ISPs vieron la necesidad de actualizar sus redes con el fin de responder a los nuevos requerimientos. En un principio las soluciones fueron incrementar el ancho de banda de los enlaces y la capacidad de los dispositivos de enrutamiento, pero esta solución no fue adecuada para soportar las continuas variaciones en la demanda. Se requería de un mecanismo mucho más eficiente para soportar y controlar las cargas de tráfico dentro de la red. Con el transcurso del tiempo se fueron generando modelos para la gestión de tráfico que finalmente se convirtieron en lo que hoy se conoce como ingeniería de tráfico. Los principales modelos se describen a continuación.

2.3.1 Modelo Clásico.

En éstas redes la TE se realiza manipulando las medidas de enrutamiento, que permanecen fijas e independientes del estado de la red y de las características del tráfico. El enrutamiento se realiza salto por salto, y los paquetes IP atraviesan innumerables enrutadores hasta llegar a su destino. Cada enrutador toma decisiones independientes para entregar el tráfico al siguiente salto basándose en medidas simples, tales como, el número de saltos ó un valor establecido administrativamente. En caso que los enrutadores enfrenten problemas de congestión, simplemente se descarta la información y se notifica al nodo origen de este hecho.

Este enrutamiento no es adecuado en redes extensas porque genera un número de limitaciones en cuanto a la distribución del tráfico, el uso de los recursos, las capacidades de procesamiento de paquetes y la disponibilidad de ancho de banda que hacen que la red no responda adecuadamente a situaciones irregulares.

La ingeniería de tráfico basada en medidas no es escalable, es decir, no se adapta al crecimiento de la demanda ni al tamaño de la red. Si el número de enlaces aumenta es muy difícil asegurar que las medidas se ajusten sin desbalancear la carga de tráfico. Este sistema ofrece una aproximación de ensayo y error en lugar de una solución científica.

2.3.2 Enrutamiento Adaptativo (en la ARPANET)

En el enrutamiento adaptativo, las decisiones se toman de acuerdo al estado de la red. Cada nodo mantiene una tabla, la cual contiene información del tiempo estimado que le toma a un paquete atravesar un trayecto dado hacia su destino. De acuerdo a la tabla de enrutamiento

los paquetes son enviados a su destino a través del trayecto cuyo tiempo total de transmisión es el mínimo. Esta tabla con los tiempos mínimos es transmitida periódicamente a los nodos vecinos. El camino más corto, en términos del conteo de saltos es también propagado para proporcionar información de conectividad.

Una desventaja de ésta aproximación es que los cálculos del enlace dinámico tienden a crear congestión que se traslada de un segmento a otro resultando en oscilación e inestabilidad en la red.

2.3.3 Enrutamiento Dinámico

Las redes de datos evolucionaron desde la ARPANET y adoptaron algoritmos de enrutamiento dinámico con control distribuido para establecer los trayectos que los paquetes tomarían hacia su destino. Los algoritmos de enrutamiento dinámico son adaptaciones de los algoritmos del camino más corto donde los costos se basan en métricas de enlace. Las métricas de enlace dependen de cantidades estáticas o dinámicas; las cantidades estáticas son establecidas administrativamente de acuerdo a criterios locales y las cantidades dinámicas pueden ser función de las medidas de congestión en la red, tales como el retardo o pérdida de paquetes.

Una de las razones que ocasionó la poca acogida de éste método, fue la asignación estática de la métrica de enlace que no tomaba en cuenta la matriz de tráfico de la red. Además, los protocolos de enrutamiento, a la hora de tomar las decisiones de envío, no consideraban las características del flujo y las restricciones de capacidad, generando concentración del tráfico y por lo tanto congestión. Incluso, si las métricas son asignadas de acuerdo a las matrices de tráfico, se pueden presentar cargas no balanceadas debido a errores en los pronósticos del volumen y distribución de la carga y cambios en las matrices ocasionados por la naturaleza temporal de los patrones de tráfico, políticas BGP entre pares, etc.

Las limitaciones de éste sistema de enrutamiento motivaron el interés en las tecnologías orientadas a trayectos con enrutamiento explícito y enrutamiento restringido para que se adaptaran al estado real de la red.

2.3.4 Enrutamiento del Tipo de Servicio (ToS - Type of Service)

En éste enrutamiento los paquetes que tienen el mismo destino son asignados a una ruta de acuerdo a la información del campo ToS de la cabecera IP, con este campo se definen clases ToS que pueden ser clasificadas como bajo retardo y alto rendimiento. Cada enlace es asociado con múltiples costos y cada costo es usado para calcular las rutas de un ToS particular, generando a través de un cálculo muy dispendioso, el árbol de los trayectos más cortos para cada uno de los diferentes ToS.

La ingeniería de tráfico es difícil de desempeñar con el modelo de enrutamiento ToS debido a que cada tipo de tráfico permanece exclusivamente sobre el camino más corto de enrutamiento, lo cual resulta en concentración del tráfico en algunos segmentos de la red.

2.3.5 Multitrayectos de Igual Costo (ECMP - Equal Cost MultiPath)

El ECMP es una técnica que mejora las deficiencias del algoritmo SPF en los sistemas de enrutamiento de pasarela interior. En el algoritmo clásico SPF, si existen dos o más trayectos de igual costo, el algoritmo escoge sólo uno de ellos para el transporte del flujo del tráfico. En ECMP éste algoritmo es modificado ligeramente, y cuando ocurre ésta situación, el tráfico es distribuido entre los múltiples caminos de igual costo.

En ECMP, los costos de enlace son estáticos y los límites de ancho de banda no son considerados, de modo que ECMP distribuye la carga lo mas equitativamente posible entre los trayectos de igual costo, sin tener en cuenta el estado de congestión de cada uno de ellos, haciendo que unos trayectos se encuentren mas congestionados que otros. Además, la distribución de la carga entre múltiples trayectos sólo se realiza si ellos tienen un costo idéntico.

2.3.6 Nimrod

Nimrod es un sistema desarrollado para enrutamiento específico de servicios heterogéneos en las redes IP, sujeto a las múltiples limitaciones de capacidad en los recursos de la infraestructura física. Nimrod es un protocolo de enrutamiento de estado de enlace que soporta envío de paquetes orientados a trayectos, es decir, antes de enviar los paquetes a su destino se establece una ruta de transporte entre los nodos de origen y destino.

Aunque Nimrod no fue muy utilizado en las redes públicas IP, introdujo un número de conceptos claves como el enrutamiento explícito (selecciona los trayectos en los nodos origen) que han generado iniciativas recientes de enrutamiento restringido.

2.3.7 Modelo Superpuesto

En el modelo superpuesto, una red de circuitos virtuales como en el Modo de Transferencia Asíncrono (ATM - Asynchronous Transfer Mode) o Frame Relay es utilizada para proveer enlaces punto a punto entre los enrutadores IP que se encuentran en la frontera del dominio. Los enrutadores IP no tienen conocimiento de la red de conmutadores subyacente a la vez que la red de conmutadores no sabe que está transportando paquetes IP.

Algunos problemas de éste modelo son la difícil construcción y gestión de dos tecnologías diferentes; la disminución de fiabilidad, debido a que el número de elementos sobre los caminos de enrutamiento son mayores; y la escalabilidad, ya que el número de adyacencias

crece cuadráticamente con el número de enrutadores. La tendencia, por tanto, es evolucionar a un núcleo conformado por enrutadores IP y hacia una solución más integrada.

2.3.8 Enrutamiento Restringido (CR - Constraint Based Routing)

El enrutamiento restringido se refiere a los sistemas de enrutamiento que calculan las rutas de acuerdo a un conjunto de limitaciones y requerimientos que dependen de la red misma o de políticas administrativas. Estas limitaciones pueden ser respecto al ancho de banda, conteo de saltos, retardo y características de los recursos de red. Las limitaciones también pueden ser atributos de ciertas tecnologías y contextos en los cuales existen restricciones en las soluciones dadas por la función de enrutamiento.

En el enrutamiento restringido, la fuente es responsable de determinar el trayecto hacia el destino usando protocolos de señalización que faciliten el intercambio de la información del estado de la red. Finalmente, el enrutamiento restringido busca la optimización total de la red mientras minimiza costos.

2.4 FUNCIONES DE OPTIMIZACIÓN Y EVALUACIÓN DEL DESEMPEÑO

2.4.1 Funciones de optimización

La optimización en la ingeniería de tráfico se logra por medio de la gestión de capacidad y la gestión del tráfico. La gestión de capacidad abarca la planeación, enrutamiento, control y gestión de los recursos. La gestión de tráfico comprende gestión de colas, mecanismos de conservación de ancho de banda, programación y otras funciones que regulan el tráfico dentro de la red, además de protocolos, algoritmos de QoS y políticas que permiten diferenciar paquetes e imponer comportamientos apropiados para un flujo de tráfico dado.

La optimización se relaciona con el control del sistema y depende de modelos de negocios, de las restricciones operacionales y de las capacidades de la red.

Los aspectos de control dentro de la ingeniería de tráfico pueden ser preventivos y correctivos. Los sistemas de control preventivos toman medidas para evitar futuros estados desfavorables en la red, mientras que los sistemas de control correctivos solucionan problemas que se están presentando. Estos sistemas cuentan con capacidades de control automático que se adaptan rápidamente a los cambios significativos en el estado de la red sin afectar su estabilidad.

2.4.1.1 *Gestión de tráfico*

La gestión de tráfico es un conjunto de funciones que describen la forma de controlar el tráfico de voz, datos y video dentro de una misma plataforma. Cada proveedor de servicio puede controlar el comportamiento de los diferentes tipos de tráfico adaptándose a cambios en la carga y a fallas en la red, asegurando altos niveles de desempeño y garantizando QoS extremo a extremo.

Las funciones de gestión de tráfico pueden ser descentralizadas y distribuidas a los nodos de la red, centralizadas y localizadas en un sistema de control central, ó desempeñadas por una combinación híbrida de éstas aproximaciones.

Las funciones de gestión de tráfico son:

- **Métodos de enrutamiento.** El control de enrutamiento es un factor importante para la ingeniería de tráfico. El enrutamiento influye en muchas de las medidas del desempeño asociadas con la red, tales como, rendimiento, retardo y utilización. En una red de área amplia, es muy difícil proveer una buena calidad de servicio sin un control de enrutamiento efectivo. El sistema de enrutamiento debe seleccionar rutas que cumplan con un conjunto de características, restricciones y políticas administrativas para dar una respuesta rápida a las variaciones de la carga de tráfico. Los métodos de selección del trayecto son categorizados en los siguientes cuatro tipos: Enrutamiento Fijo (FR - Fixed Routing), en el cual se establece una relación jerárquica entre las diferentes subredes; Enrutamiento Dependiente del Tiempo (TDR - Time-Dependent Routing), donde las tablas de enrutamiento son actualizadas en un intervalo de tiempo fijo durante el día o la semana; Enrutamiento Dependiente del Estado (SDR - State-Dependent Routing) en el cual las tablas de enrutamiento son alteradas automáticamente de acuerdo al estado de la red; y Enrutamiento Dependiente de los Eventos (EDR - Event-Dependent Routing) en el que las tablas de enrutamiento son actualizadas localmente basándose en el éxito o fracaso de las conexiones .

- **Métodos de gestión de QoS.** La QoS es la capacidad de una red para proporcionar de forma consistente algún nivel de seguridad en la entrega de los datos. La QoS selecciona y clasifica paquetes IP en diferentes clases de tráfico y asigna los recursos apropiados para entregarlos de acuerdo a criterios como el tipo de aplicación, direcciones IP fuente y destino, etc. El proceso de QoS se divide en cuatro funciones, monitoreo de red, establecimiento de políticas, aplicación de políticas, y reporte y revisión, como se muestra en la Figura 2.1. Estas funciones forman un ciclo que se realimenta asegurando que los objetivos se cumplan . Las redes y aplicaciones son ambientes dinámicos y las implementaciones de QoS necesitan una revisión continua de las prioridades y políticas que pueden requerir ajustes para adaptar el ciclo QoS al estado actual de la red.



Figura 2.1. Ciclo de QoS.

- **Métodos de gestión de la tabla de enrutamiento.** Este método genera automáticamente las tablas de enrutamiento con base en la topología y estado de la red. La Información de actualización topológica, el estado actual de la red o recomendaciones de enrutamiento, se intercambia entre los nodos para seleccionar los trayectos y para determinar las reglas de diseño de las tablas de enrutamiento.
- **Enrutamiento de transporte dinámico.** El enrutamiento de transporte dinámico mejora la respuesta de la red ante situaciones de falla (de nodos o enlaces) o variaciones en la carga del tráfico. Ofrece ventajas de simplicidad de diseño y robustez, y proporciona la generación automática de enlaces, enrutamiento en diversos trayectos, y rápido restablecimiento para mejorar la utilización y el desempeño de la capacidad de transporte bajo altos niveles de carga.

La gestión de tráfico provee monitoreo del desempeño de la red a través de la recolección, encaminamiento de tráfico y desempeño de datos. La gestión de tráfico utiliza controles de bloqueo de direcciones de destino por conexión, modificación de tablas de enrutamiento y controles de selección/reenrutamiento de trayectos cuando las circunstancias así lo requieran.

2.4.1.2 *Gestión de Capacidad*

La gestión de capacidad mediante el control del diseño de red, planea, procesa y provee la capacidad necesaria para satisfacer los objetivos de desempeño a un costo mínimo. El control de diseño realiza funciones de monitoreo semanal/diario del desempeño, y de ajuste y pronóstico de la capacidad de la red a corto tiempo.

El monitoreo semanal y diario del desempeño es necesario para identificar los problemas de la red. Si se detectan problemas, las funciones de ajuste de red realizan la actualización de la tabla de enrutamiento y si es necesario se incrementa la capacidad de la red en corto tiempo para mitigar los problemas

La gestión de capacidad comprende el diseño de enrutamiento y el diseño de capacidad. El diseño de enrutamiento adapta la tabla de envío para corregir los problemas en la prestación del servicio, cuando sea necesario. El diseño de la capacidad provee las funciones necesarias para soportar las variaciones del tráfico y así satisfacer los niveles de QoS extremo a extremo.

La gestión de capacidad abarca una serie de modelos que colaboran con el cumplimiento de los objetivos de desempeño.

- **Modelo de diseño de capacidad de enlace.** En caso de congestión es responsabilidad de este modelo conmutar el tráfico hacia un trayecto alternativo y determinar la capacidad del enlace directo y del alternativo para que el tráfico sea transportado a un costo mínimo. El modelo del diseño utiliza un procedimiento de optimización para determinar el tráfico enviado por el trayecto directo y el enviado por el trayecto alternativo.
- **Modelo de selección del trayecto más corto.** Este modelo determina el trayecto más corto para transportar el tráfico desde el nodo origen al destino, proporcionando un enrutamiento más eficiente y flexible que se adapte rápidamente a las variaciones de la carga de tráfico en la red.
- **Modelo de diseño de red multihora.** Este modelo se usa para determinar la capacidad de red necesaria en cada hora del día, para satisfacer los cambios temporales de la carga y para determinar la capacidad reservada en la red.
- **Modelo de diseño para las variaciones diarias de la carga.** Estos modelos describen las técnicas para el manejo de las variaciones que suceden día a día en el diseño de la capacidad.
- **Modelo de diseño de la capacidad reservada y pronosticada inciertamente.** Este modelo describe los medios para responder a errores en la proyección de las cargas de tráfico en el diseño de la capacidad de red.

2.4.2 Funciones de evaluación del desempeño

Otro aspecto importante a tratar en la ingeniería de tráfico es la evaluación del desempeño que monitorea la eficacia de los métodos de TE y verifica que se cumplan las metas de desempeño. Los resultados de esta evaluación se usan para identificar y predecir problemas en la red.

Las técnicas más usadas para realizar la evaluación del desempeño son los métodos analíticos, de simulación y los métodos empíricos (basados en medidas). Cuando se usan los métodos analíticos y de simulación, los enlaces y nodos de la red son modelados para capturar características relevantes de operación, tales como topología, ancho de banda, espacio en el buffer y políticas de servicio. Los modelos analíticos se usan para representar las características de tráfico dinámicas y de desempeño que reflejen fielmente la operación de las entidades de red.

La simulación se usa para evaluar el desempeño de la red o para verificar y validar las aproximaciones analíticas, pero es costosa y no siempre provee suficiente información del

estado actual de la red. Para la evaluación del desempeño resulta apropiado usar una combinación de estos métodos.

2.5 MODELO DE LA INGENIERÍA DE TRÁFICO

La ingeniería de tráfico interactúa con la red mediante funciones que definen políticas y métodos para asegurar un rendimiento óptimo y una adecuada utilización de los recursos respondiendo a la demanda de servicios presente y futura como se muestra en la Figura 2.2.

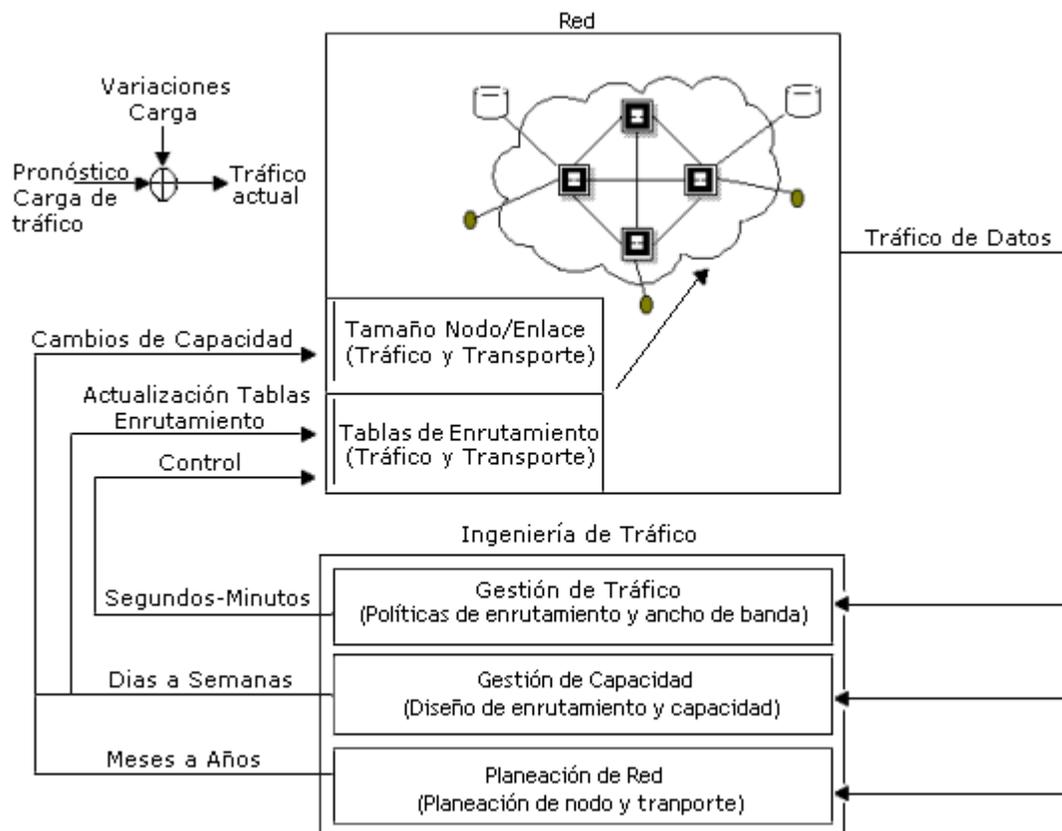


Figura 2.2. Interacción entre la Ingeniería de Tráfico y la Red.

El bloque central representa la red, la cual puede tener varias arquitecturas y configuraciones. Las configuraciones abarcan redes de área metropolitana, redes nacionales y redes internacionales, que soportan estructuras jerárquicas y no jerárquicas o una combinación de ambas. En este bloque también se encuentran las tablas de enrutamiento que describen el trayecto seleccionado desde un nodo origen a un nodo destino que satisfacen un requerimiento de conexión particular. Las entradas que maneja la red son las cargas de tráfico que consisten de la demanda promedio más las variaciones en la carga y los pronósticos de la demanda de tráfico.

El bloque de ingeniería de tráfico describe las funciones de gestión de tráfico, gestión de capacidad y planeación de la red. Estas funciones son bucles de realimentación interactivos cuyo objetivo es adaptar la capacidad y el enrutamiento de la red a las variaciones de carga de tráfico. Las variaciones pueden suceder en intervalos de tiempo como segundos, minutos, horas, días, semanas, etc.

Para alcanzar los objetivos de desempeño se define un modelo de TE, descrito como una secuencia de acciones que se realizan para mejorar la operación de las redes. Éste modelo es implementado dentro del bloque de ingeniería de tráfico y puede ser desarrollado explícita ó implícitamente.

El modelo de ingeniería de tráfico formula políticas de control, observa el estado de la red monitoreando el sistema, caracteriza el tráfico y aplica acciones de control para conducir la red a un estado deseado. El modelo de ingeniería de tráfico como se muestra en la Figura 2.3, es un proceso adaptativo que involucra cuatro fases interactivas.

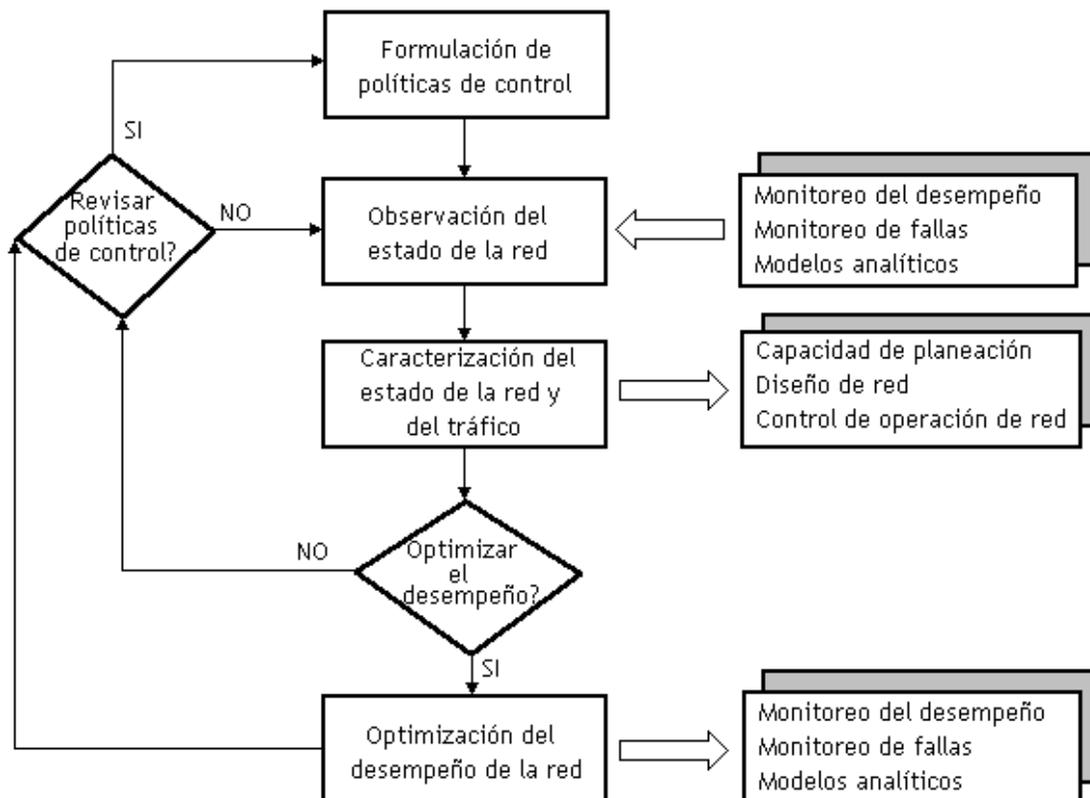


Figura 2.3. Modelo del Proceso de Ingeniería de Tráfico.

La primera fase se ocupa de la formulación de políticas de control que gobiernan la operación de la red. Las políticas de control dependen de muchos factores incluyendo el modelo predominante de los negocios, los costo de operación y mantenimiento de la red, el modelo de ingresos ó utilidades, las restricciones de operación y criterios de optimización.

La segunda fase del modelo usa un conjunto de funciones para observar el estado de la red. Esta fase es un mecanismo de realimentación que involucra la adquisición de datos para evaluar la operación de la red y actividades de preprocesamiento tales como reducción y transformación de datos.

La tercera fase analiza el estado de la red y caracteriza la carga de tráfico. El análisis del desempeño puede ser preventivo y/o correctivo. El análisis preventivo identifica problemas que aún no existen, pero podrían manifestarse en el futuro. El análisis correctivo identifica los problemas presentes, determina sus causas mediante diagnósticos y evalúa alternativas para remediar el problema. Varias técnicas cualitativas y cuantitativas se aplican en el proceso de análisis y caracterización. La fase de análisis investiga la concentración y distribución del tráfico a través de la red, identificando cuellos de botella, asignación ineficiente de enlaces, puntos de fallas, etc. Los inconvenientes de la red resultan de muchos factores, como por ejemplo, la arquitectura, diseño y configuración de la infraestructura. Los resultados del análisis se usan para optimizar el desempeño, controlar, diseñar y planificar la red.

La cuarta fase del modelo corresponde a la optimización del desempeño de la red. Esta fase involucra un proceso de decisiones que selecciona e implementa un conjunto de acciones de un grupo de alternativas. Las acciones de optimización usan técnicas apropiadas para controlar el tráfico ofrecido ó para controlar la distribución del tráfico a través de la red. Las acciones de control usan un sistema de configuración para modificar las restricciones de los recursos, adicionar o incrementar la capacidad de los enlaces, modificar ó ajustar los parámetros asociados con el enrutamiento (medidas IGP, atributos BGP), manipular los parámetros de gestión, etc. La optimización del desempeño puede incluir un proceso de planeación para mejorar la arquitectura, diseño, capacidad, tecnología y configuración de los elementos de red haciendo que se adapten al crecimiento actual y futuro.

2.5.1 Componentes del Modelo de la Ingeniería de Tráfico.

El modelo contiene 3 componentes que colaboran con el proceso de la ingeniería de tráfico. Los componentes son: el subsistema de medidas, el subsistema de análisis y modelado, y el subsistema de optimización.

2.5.1.1 *Subsistema de medidas*

El subsistema de medidas juega un papel importante dentro del modelo de la ingeniería de tráfico. El estado de operación de la red puede determinarse sólo mediante medidas, las cuales son necesarias para determinar la calidad de los servicios de red y para evaluar la eficacia de las políticas de TE. Los datos proporcionados por el sistema de medidas mejoran adaptativamente el desempeño de la red, en respuesta a eventos y estímulos originados dentro y fuera de la misma. Un subsistema de medidas es más eficaz cuando se adquiere y se aplica sistemáticamente.

Cuando se desarrolla un sistema de medidas que soporta las funciones de ingeniería de tráfico, se consideran las siguientes preguntas: ¿por qué las medidas son necesarias en este contexto?, ¿qué parámetros serán medidos?, ¿cómo se realizan las medidas?, ¿dónde se desarrollan las medidas?, ¿cuándo pueden desarrollarse las medidas?, ¿cómo podrían monitorearse frecuentemente las variables a ser medidas?, ¿qué nivel de precisión y seguridad se desea de las medidas?, ¿qué nivel de precisión y seguridad se alcanza realmente con las medidas?, ¿hasta que punto el sistema de medidas puede interferir con el monitoreo de los componentes y variables de la red?; las respuestas a estas preguntas determinan las metodologías y herramientas apropiadas en un contexto determinado de la ingeniería de tráfico.

Existe una diferencia importante entre el sistema de medidas y el sistema de evaluación. Las medidas entregan los datos originales relacionados a las variables y parámetros del estado de los elementos monitoreados y la evaluación toma los datos originales para hacer inferencias con respecto al sistema de monitoreo.

Las medidas pueden ocurrir a diferentes niveles de abstracción, por ejemplo, las medidas pueden usarse para manejar las características a nivel de paquetes, características a nivel de flujos, características a nivel de usuarios, características de tráfico agregado, características a nivel de componentes, etc.

2.5.1.2 Modelado, Análisis y Simulación

Un modelo de red es una representación abstracta de todas las características y atributos relevantes de los enlaces, de los nodos y de las limitaciones. Con esta representación se facilita el análisis y simulación para pronosticar y planear el comportamiento de la red cuando se enfrenta a diferentes situaciones. En general, los modelos de ingeniería de tráfico pueden dividirse en estructurales y de comportamiento. Los modelos estructurales se enfocan en la organización de la red y sus componentes y los modelos de comportamiento se enfocan en la dinámica de la red y la carga de tráfico.

Las herramientas de simulación son muy útiles en la ingeniería de tráfico, porque a través de ellas es posible visualizar e imitar el comportamiento de la red, y así identificar la manera de evolucionar para adaptarse a las futuras demandas.

Estas herramientas se emplean durante el proceso de planeación para descubrir problemas de la red (puntos de falla que pueden requerir de una redundancia adicional, cuellos de botella, congestión, etc.) y proveer ideas que den solución a estos problemas de desempeño. Los sistemas de simulación se utilizan para validar la eficacia de las soluciones planteadas por la TE sin necesidad de interferir con el funcionamiento de la red.

2.5.1.3 Optimización

La optimización trata de resolver los inconvenientes de la red transformándolos en conceptos que permitan la identificación e implementación de una solución. La optimización de la red puede ser correctiva o preventiva. En la optimización correctiva, el objetivo es solucionar un

problema actual o que está empezado, en la optimización preventiva la meta es mejorar el desempeño de la red anticipándose a dar soluciones a futuros problemas.

La optimización de la red es un proceso continuo y puede consistir de subprocesos de optimización en tiempo real y de subprocesos de planeación que no necesariamente deben desarrollarse en tiempo real. La diferencia entre estos dos subprocesos es la escala de tiempo y las acciones que realizan.

Uno de los objetivos principales de la optimización en tiempo real es controlar la distribución y el encaminamiento del tráfico sobre la infraestructura existente para evitar y mitigar la congestión. Cuando se presentan incidentes aleatorios tales como cambios en la demanda del tráfico se pueden ocasionar problemas de congestión que afectan la operación de la red y es función del subproceso de optimización resolver estos problemas en cuestión de microsegundos, minutos u horas.

Una de las funciones del subproceso de planeación es iniciar las acciones para evolucionar sistemáticamente en la arquitectura, tecnología, topología y en la capacidad de la red, de forma que soporte el crecimiento y los cambios en la demanda. Cuando se presenta un problema, el subproceso de optimización provee una solución inmediata, que podría no ser la mejor opción, entonces, la planeación de red es necesaria para perfeccionar la solución y mejorar la situación.

La planeación y la optimización en tiempo real son actividades complementarias. Una buena planeación hace que la optimización sea más fácil; y una correcta optimización provee varias ideas para la planeación de la red.

2.6 CLASIFICACIÓN DE LA INGENIERÍA DE TRÁFICO

La clasificación de los sistemas de ingeniería de tráfico puede ser constituida de acuerdo a los siguientes parámetros:

2.6.1 Dependiente del Tiempo vs Dependiente del Estado vs Dependiente de Eventos

En el enrutamiento dependiente del tiempo, la información de las variaciones de tráfico almacenada en el historial se utiliza para programar planes de enrutamiento y otros mecanismos de control de ingeniería de tráfico. Los algoritmos dependientes del tiempo no se adaptan a las variaciones aleatorias del tráfico ni a las condiciones cambiantes de la red.

En la ingeniería de tráfico dependiente del estado los planes de enrutamiento se modifican automáticamente de acuerdo al estado actual de la red, respondiendo a las variaciones del tráfico.

Los métodos de ingeniería de tráfico dependientes de eventos se distinguen de los métodos dependientes del tiempo y del estado en la forma de seleccionar los trayectos. Mientras los modelos dependientes de estado usan mecanismos de inundación para la selección de los trayectos, los métodos dependientes de eventos no lo requieren.

2.6.2 Offline vs Online

La ingeniería de tráfico requiere el cálculo de planes de enrutamiento, los cuales pueden ser realizados offline u online. El cálculo offline se realiza en escenarios donde los planes de enrutamiento no necesitan ejecutarse en tiempo real.

El cálculo online se requiere cuando los planes de enrutamiento deben adaptarse a las condiciones cambiantes de la red. A diferencia del cálculo offline, el cálculo online se enfoca hacia cálculos rápidos y simples para seleccionar las rutas, asignar adecuadamente los recursos, y realizar el balance de carga.

2.6.3 Centralizado vs Distribuido

El control centralizado tiene un sistema central que determina los planes de enrutamiento y otros parámetros de control, en beneficio de cada dispositivo de enrutamiento. El sistema central recolecta periódicamente información proveniente de todos los enrutadores acerca del estado de la red y realimenta la información de enrutamiento a cada uno de ellos. El ciclo de actualización de enrutamiento es un parámetro crítico que influye directamente sobre el desempeño de la red. El control centralizado necesita alto poder de procesamiento y elevado control del ancho de banda.

En el control distribuido cada enrutador determina automáticamente la selección de los trayectos en base a la visión que cada uno de ellos tiene de la red. La información del estado de la red debe obtenerse por el enrutador usando algún método de distribución. La información del estado de la red también puede difundirse bajo condiciones excepcionales.

2.6.4 Local vs Global

Los algoritmos de ingeniería de tráfico necesitan información local y global del estado de la red. La información local corresponde al estado de un segmento del dominio, por ejemplo, ancho de banda y la relación de pérdida de paquetes de un trayecto en particular. La información global corresponde al estado de todo el sistema, por ejemplo una matriz de tráfico global y la información de carga de los enlaces de la red.

Es posible que un algoritmo de ingeniería de tráfico que realice una optimización global, se base en información de estado local. Similarmente, un algoritmo puede encontrar una solución óptima para un subdominio basándose en información de estado global.

2.6.5 Prescriptivo vs Descriptivo

Un sistema de ingeniería de tráfico prescriptivo, evalúa alternativas y recomienda un curso de acción. La TE prescriptiva puede dividirse en correctiva o preventiva. La correctiva establece acciones para solucionar una anomalía existente, la preventiva, establece un curso de acción para mejorar el desempeño de la red aún cuando no existen inconvenientes.

La ingeniería de tráfico descriptiva caracteriza el estado de la red y evalúa el impacto de varias políticas sin recomendar algún curso de acción particular.

2.6.6 Bucle Abierto vs Bucle Cerrado

En el control de la ingeniería de tráfico de bucle abierto, la acción de control no usa información de realimentación del estado actual de la red sino que usa su propia información local para alcanzar sus propósitos.

En la ingeniería de tráfico de bucle cerrado, la acción de control usa información de realimentación del estado de la red, la cual puede ser tomada del historial u obtenida de medidas actuales.

2.6.7 Táctico vs Estratégico

La ingeniería de tráfico táctica ayuda a solucionar problemas de desempeño específicos (estados de congestión) que ocurren en la red desde una perspectiva táctica, sin considerar estrategias imperativas globales.

La ingeniería de tráfico estratégica aborda los problemas desde perspectivas más organizadas y sistemáticas, tomando en consideración las consecuencias de las políticas y acciones específicas.

2.7 REQUERIMIENTOS DE LA INGENIERÍA DE TRÁFICO

Para implementar un modelo robusto de ingeniería de tráfico, se necesitan soportar ciertos requerimientos claves que permiten optimizar el desempeño, facilitar operaciones de red, mientras se ofrece a los usuarios finales la QoS apropiada.

Un requerimiento de ingeniería de tráfico se define como la capacidad necesaria para resolver un problema ó cumplir con un objetivo. Estos requerimientos pueden ser clasificados en *requerimientos no funcionales* y *requerimientos funcionales*.

Los requerimientos no funcionales están relacionados con los atributos de calidad o características del estado de un sistema de ingeniería de tráfico. Los requerimientos

funcionales estipulan las funciones que un sistema TE debe desempeñar para cumplir con sus objetivos y solucionar los problemas de red.

2.7.1 Requerimientos Genéricos No Funcionales

Los requerimientos no funcionales para la ingeniería de tráfico son: utilidad, automatización, escalabilidad, estabilidad, visibilidad, sencillez, eficacia, fiabilidad, supervivencia, corrección, mantenimiento, interoperabilidad y seguridad. Para un contexto dado, algunos de estos requerimientos pueden ser indispensables mientras que otros pueden ser opcionales. Por tanto, la prioridad debe establecerse durante la fase de desarrollo de un sistema de TE para adaptarlo a un contexto operacional específico.

A continuación se definen algunos aspectos de los requerimientos no funcionales para la ingeniería de tráfico.

- **Utilidad.** La utilidad se refiere a la facilidad con que un sistema de ingeniería de tráfico puede ser desarrollado y utilizado dentro de una red existente.
- **Automatización.** Se pretende automatizar todas las funciones de TE que sean posibles para minimizar la intervención humana en el control y análisis de la operación de la red. La automatización es indispensable particularmente en las grandes redes IP debido a los altos costos que trae la intervención humana y a los riesgos causados por sus errores. Con la automatización, se introducen dentro de la red componentes inteligentes con procesos de realimentación automática.
- **Escalabilidad.** Un sistema de ingeniería de tráfico puede ser escalable y proveer la funcionalidad requerida con un mínimo conjunto de mecanismos a un bajo costo. Un sistema es escalable si permanece en operación aún cuando la red evolucione, (número de enrutadores, enlaces, y volumen de tráfico). Un sistema TE con una arquitectura escalable no afecta desfavorablemente otras funciones ni procesos en la red y no consume muchos recursos con la distribución de la información de estado.
- **Estabilidad.** La estabilidad es un estado operacional donde la red no oscila de un estado a otro garantizando que se mantengan sus características de capacidad para entregar de forma rápida y segura los servicios a los usuarios finales.
- **Flexibilidad.** Un sistema de ingeniería de tráfico flexible permite a un administrador de red adaptar las políticas de optimización a un ambiente en particular.
- **Visibilidad.** En los sistema de ingeniería de tráfico se cuenta con mecanismos que reúnen y analizan medidas estadísticas para determinar cómo esta funcionando la red. Las estadísticas manejadas son las matrices de tráfico, latencia, pérdida de paquetes, y otras medidas de desempeño que son establecidas por el sistema de medidas y se emplean como indicadores de las condiciones predominantes de la red.

- **Sencillez.** En la TE es importante que el sistema sea claro, conveniente y con interfaces de usuario intuitivas para facilitar su uso. Aunque un sistema TE tiene estructuras y algoritmos complejos, la complejidad puede ocultarse tanto como sea posible a los administradores de red a través de las interfaces de usuario. La sencillez es esencial para una operación eficiente y a bajos costos.
- **Supervivencia.** La supervivencia es la capacidad para mantener el nivel de QoS aún cuando se presentan fallas dentro de la red. Para implementar esta capacidad es necesario introducir redundancia dentro de la arquitectura, diseño y operación de la red. El tiempo requerido para restaurar el servicio después de una falla, depende de varios factores tales como: el contexto particular en que ocurre la falla, la arquitectura, el diseño, las características de protocolos y elementos de red, las aplicaciones y servicios deteriorados por la falla, etc. La extensión y el impacto de la interrupción del servicio depende de qué tan largo es el tiempo de la interrupción, la importancia de los recursos y el tipo de servicio afectado. La supervivencia puede solucionarse a nivel de dispositivos y a nivel de red de forma que se adaptan a diferentes necesidades.
- **Interoperabilidad.** La interoperabilidad es un requerimiento clave para implementaciones que aseguren una evolución rápida y confiable de la red. En cuanto sea posible, los sistemas TE y sus componentes deben ser desarrollados con protocolos estándares basados en interfaces que permitan la interoperación con otros sistemas.
- **Seguridad.** La seguridad ejerce un control sobre ciertos aspectos funcionales de la red para lograr los objetivos de desempeño, garantizar la integridad de los sistemas TE y para proyectar las vulnerabilidades de la red.

2.7.2 Requerimientos de encaminamiento de Tráfico

El encaminamiento se encarga de asignar el tráfico a los trayectos previamente establecidos, ya sea a través del enrutamiento restringido o por algún otro medio, para satisfacer ciertos requerimientos.

Una característica importante de la función de encaminamiento de tráfico es la capacidad para establecer múltiples trayectos entre los nodos de origen y destino, además de la posibilidad de distribuir el tráfico entre los nodos de acuerdo a las políticas existentes. Cuando el tráfico es dividido en trayectos múltiples se debe tener especial cuidado en asegurar que los paquetes en el destino sean organizados apropiadamente.

Los mecanismos que realizan las funciones de encaminamiento de tráfico deben apuntar a reducir la congestión en la red. Si la carga de tráfico total no puede ser adaptada o si el enrutamiento y las funciones de encaminamiento no pueden reaccionar de forma rápida a las condiciones cambiantes de la red, el sistema de encaminamiento de tráfico debe respaldarse en los mecanismos de control (gestión de colas y procesamiento) para minimizar la congestión,

es decir, los mecanismos que desempeñan las funciones de encaminamiento de tráfico deben complementarse con los mecanismos de control de congestión existentes.

2.7.3 Requerimientos de Medidas

La recolección de medidas y estadísticas es de gran importancia para soportar las funciones de ingeniería de tráfico, por lo tanto, son necesarias capacidades adicionales para el análisis de las estadísticas que deben evolucionar junto con la red.

Las estadísticas de tráfico pueden ser clasificadas en intervalos de tiempo cortos y largos. Los intervalos de tiempo largos son muy útiles ya que pueden reflejar la carga de la red, así como las tendencias de tráfico por temporadas, es decir, produciendo perfiles de las variaciones del tráfico por días, horas y semanas, obteniendo estadísticas tales como características de las horas más congestionadas, patrones de crecimiento de tráfico, problemas persistentes de congestión, cuellos de botella y utilización desbalanceada de los enlaces causadas por anomalías en el enrutamiento. El monitoreo de las estadísticas de tráfico puede también describir las características de una red que soporta múltiples clases de servicios.

Las medidas de tráfico estadísticas deben indicar de forma fiable y razonable el estado actual de la red en escalas de tiempo cortas, reflejando así la utilización del enlace y el estado de congestión, el cual se puede medir por medio del retardo excesivo, pérdida de paquetes y alta utilización de los recursos.

2.7.4 Requerimientos de Supervivencia de Red

La supervivencia de red es la capacidad para mantener el servicio aún en presencia de fallas, recobrando rápidamente las interrupciones de la red y manteniendo la QoS requerida para los servicios existentes.

Con los nuevos desarrollos se ha llegado a una supervivencia multinivel, donde las tecnologías proporcionan capacidades de protección y restauración, en términos de escala de tiempo, y a diferentes niveles de ancho de banda (desde un nivel de paquetes a un nivel de longitud de onda). Las capacidades de protección y restauración son sensitivas a diferentes clases de servicios y diferentes modelos de utilidad en la red.

El impacto de la interrupción varía significativamente para diferentes clases de servicios dependiendo de su duración que puede variar de milisegundos a horas.

Debe existir coordinación entre las capacidades de protección y restauración para asegurar que la supervivencia de red permanezca a un costo razonable. Para llevar a cabo esta coordinación se necesita de los siguientes requerimientos:

- Funciones de protección y restauración a varios niveles que incrementen la redundancia y robustez evitando el manejo ineficiente de los recursos de red.
- Notificación oportuna y segura de fallas a través de la red .
- Alarmas y otras capacidades de monitoreo y reporte de fallas proveídos a niveles apropiados.

2.7.5 Ingeniería de Tráfico en Ambientes de Servicios Diferenciados

Los crecientes requerimientos para soportar múltiples clases de tráfico en las redes IP, han hecho que los flujos sean diferenciados o clasificados de acuerdo a algunos criterios como el retardo, el jitter o en términos de campos comunes en la cabecera IP, para brindarles el trato adecuado dependiendo de sus características.

Las clases de servicio pueden soportarse en un ambiente de servicios diferenciados a lo largo del trayecto de enrutamiento, usando mecanismos de provisionamiento de servicio, y configurando apropiadamente las funcionalidades de los enrutadores extremos (clasificación del tráfico, etiquetado, monitoreo y configuración). Todo esto se logra con la ayuda de una adecuada gestión de buffer y mecanismos de procesamiento de paquetes.

Para proveer una mejor calidad de servicio en un dominio de servicios diferenciados, no es suficiente el uso de éstos mecanismos de gestión, es aconsejable además el control de desempeño de algunas clases de servicio, implementando ciertas relaciones entre la carga de tráfico producida y la cantidad de recursos de red destinados para esa clase de servicio. Esta relación entre demanda y recursos asignados puede implementarse usando una combinación de, por ejemplo, mecanismos de TE que representen la relación deseada entre la cantidad de tráfico producida por una clase de servicio dado y los recursos destinados a satisfacer esa clase ó mecanismos que regulen dinámicamente los recursos destinados a una clase de servicio dada, para relacionarla a la cantidad de tráfico contribuido por esa clase de servicio.

También es aconsejable controlar el desempeño del tráfico de alta prioridad sobre el de prioridad baja. Esto se logra controlando la cantidad de tráfico de alta prioridad que es enrutada a través de un trayecto dado, o incrementando la capacidad del enlace de modo que el tráfico de baja prioridad pueda tener la calidad de servicio adecuada o deseada.

2.7.6 Control en la Red

A causa del rápido crecimiento de las redes, se han desarrollado mecanismos que permiten el control y el monitoreo constante de la red para evaluar el cumplimiento de los requerimientos de los servicios y las políticas administrativas. Las funciones de control deben ser seguras, fiables y estables y deben funcionar adecuadamente inclusive en momentos en que existan inconvenientes como congestión y ataques de seguridad. Las acciones de control involucran la

modificación de parámetros de gestión de tráfico, de parámetros asociados con el enrutamiento y de los atributos y restricciones asociados con los recursos.

Los mecanismos de control pueden ser manuales (configuraciones administrativas), parcialmente automatizados o totalmente automatizados (sistemas de gestión basados en políticas). Los mecanismos automatizados son especialmente útiles en la interconexión de redes a gran escala, porque facilitan la implantación de sistemas de gestión y políticas de soporte de las funciones de control (distribución de la carga y protección/recuperación de la red) necesarias para la ingeniería de tráfico.

2.7.7 Gestión de congestión

Se dice que un elemento está congestionado si experimenta una sobrecarga de tráfico continua durante cierto intervalo de tiempo ocasionando disminución en la calidad del servicio entregada al usuario. Una situación de congestión puede crecer y propagarse rápidamente generando una disminución drástica en el rendimiento de la red.

Uno de los objetivos de la ingeniería de tráfico es detectar los problemas de congestión y adoptar medidas correctivas que eviten que éste problema se propague y afecte el rendimiento total de la red.

Para combatir los problemas de congestión, se han establecido sistemas encaminados a dar una respuesta rápida y eficiente que asegure que el nivel de QoS se mantenga aun en presencia de éstos problemas. Estas políticas de gestión pueden ser clasificadas de la siguiente forma:

- Escala del tiempo de respuesta.
 - ✓ **Largo (semanas a meses)**. Se trabaja sobre una escala de tiempo relativamente larga para aumentar la capacidad de la red basándose en estímulos o pronósticos de la demanda futura y la distribución de tráfico. Una de las acciones que realiza éste sistema es la adición de mas rutas y enlaces dentro de la red, actividad que es muy costosa y puede durar meses o incluso años.
 - ✓ **Medio (minutos a días)**. Contiene varias políticas de control que incluyen el ajuste de parámetros BGP o IGP para enrutar el tráfico hacia ciertos segmentos y la reconfiguración de la topología lógica de la red para la distribución adecuada de la carga. Los mecanismos que responden a escalas de tiempo medio, dependen de un sistema de medidas que monitorean cambios en la distribución del tráfico, en la carga y en la utilización de los recursos de la red que permiten tomar las acciones de control necesarias para evitar situaciones de congestión.
 - ✓ **Corto (pico segundos a minutos)**. Esta categoría incluye funciones de procesamiento a nivel de paquetes, mecanismos de enrutamiento tales como gestión pasiva y activa

del buffer, gestión de colas, etc. Estos mecanismos son usados para controlar e indicar la congestión a los sistemas finales de modo que ellos puedan regular adaptativamente la tasa con que el tráfico es entregado a la red.

➤ Mecanismos preventivo y correctivo.

- ✓ **Correctivo.** Estos sistemas solucionan los problemas de congestión existentes monitoreando e identificando los problemas de congestión, e inicializa acciones relevantes para mitigar la situación. Todos estos sistemas pueden ser clasificados en escalas de tiempo largos y medios.
- ✓ **Preventivo.** Los sistemas toman acciones para prevenir la congestión en base a estimaciones o predicciones de futuros problemas. Estos sistemas no necesariamente responden de forma inmediata a los problemas de congestión y pueden clasificarse en escalas de tiempo largos y medios.

➤ Mecanismos del lado de la demanda y del lado del proveedor.

- ✓ **Lado del proveedor.** Para reducir y evitar los problemas de congestión se incrementan la capacidad disponible en la red y se reasignan recursos para redistribuir el tráfico sobre la infraestructura y de este modo controlar y evitar la congestión.
- ✓ **Lado de la demanda.** Para mitigar los problemas de congestión se restringe el acceso a los recursos congestionados y regulan dinámicamente la demanda del tráfico.

En las redes IP, para solucionar los problemas de congestión se pueden utilizar una combinación de éstos sistemas, los cuales operan en múltiples escalas de tiempo.

Si los componentes de la ingeniería de tráfico son integrados e implementados adecuadamente, los Proveedores de Servicio tendrán un control más preciso sobre el flujo de tráfico y podrán economizar el ancho de banda a través de la red. La ventaja principal de implementar la ingeniería de tráfico es que la planificación y la gestión se llevan a cabo de manera flexible, a menores costos y con mayor QoS para los usuarios finales.

3. CONMUTACIÓN DE ETIQUETAS MULTIPROTOCOLO - MPLS: CONCEPTOS Y CARACTERÍSTICAS

MPLS se ha ido consolidando como la solución a muchos de los problemas que se presentan actualmente en las redes IP, pues ofrece un mejor desempeño en cuanto a flexibilidad, escalabilidad y gestión, y además, permite combinar en una sola plataforma multiservicio el rendimiento y flexibilidad de la conmutación del nivel de enlace con la inteligencia del enrutamiento del nivel 3, convirtiéndola en una alternativa de evolución hacia las redes de la siguiente generación. MPLS inicialmente fue enfocada en la optimización del envío de los paquetes IP, pero durante su proceso de desarrollo, se le han adicionando nuevas características que han conducido a la vinculación de MPLS en diferentes áreas de aplicación tales como la Ingeniería de Tráfico, las Redes Privadas Virtuales, las Redes Ópticas, etc.

Aunque MPLS aun se encuentra en proceso de estandarización ha tenido gran acogida por parte de las empresas involucradas en el sector de las telecomunicaciones, contribuyendo a que se adapte rápidamente a las necesidades de los usuarios finales y de los proveedores de servicio.

Este capítulo describe las características y el funcionamiento de MPLS así como sus beneficios, componentes y aplicación en las redes de telecomunicaciones.

3.1 EVOLUCIÓN DE MPLS

Desde sus inicios, Internet ha evolucionando en respuesta a las nuevas necesidades de los usuarios y ha incentivado el desarrollo de una gran variedad de nuevas aplicaciones, sin embargo, los cambios que ha enfrentado no han sido suficientes para satisfacer todos los requerimientos de los diferentes tipos de servicios. Por consiguiente, Internet debe transformarse a modelos que permitan ir más allá del nivel de "mejor esfuerzo", que incrementen el desempeño y faciliten la integración de nuevas tecnologías que consoliden a Internet como la red pública de datos de la siguiente generación.

Los ISPs para mantenerse al ritmo de la demanda incrementaron el tamaño, el ancho de banda y la velocidad de las redes, dando solución a los problemas de capacidad, pero esto requería grandes inversiones y no brindaba alternativas para los inconvenientes de enrutamiento e ingeniería de tráfico. Por esta razón se buscaron nuevas opciones que mejoraran el desempeño de las redes. Fue entonces cuando las redes IP evolucionaron de una topología basada sólo en enrutadores a un modelo de IP sobre ATM (IP/ATM) buscando aprovechar las ventajas de una tecnología secundaria que tuviera capacidades de gestión de tráfico (como

ATM), y al mismo tiempo eludir las limitaciones de los sistemas IP respecto a la ingeniería de tráfico. El modelo IP/ATM presenta la superposición de una topología virtual de enrutadores IP, localizados en la frontera del dominio, sobre una topología real de conmutadores ATM ubicada en el núcleo de la red, como se muestra en la Figura 3.1.

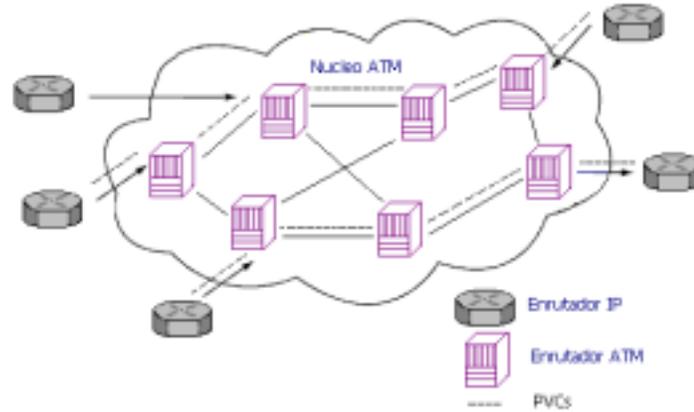


Figura 3.1. Modelo Superpuesto.

Este modelo superpuesto utiliza los circuitos virtuales de ATM para establecer conexiones punto a punto entre los enrutadores IP de la frontera. Los enrutadores IP desconocen la topología real de la infraestructura ATM y los conmutadores ignoran que están transportando paquetes IP.

Algunas de sus ventajas son el ancho de banda disponible a precios competitivos, la rapidez de transporte de datos que proporciona los conmutadores ATM y la introducción de funciones de gestión de tráfico que brindan mayores niveles de desempeño. Sin embargo, el principal problema de éste modelo es la gestión y mantenimiento de dos redes con tecnologías completamente diferentes, que incrementa la complejidad de la arquitectura y diseño de la red, además presenta problemas de fiabilidad porque existe un mayor número de dispositivos a lo largo de un trayecto. Otro problema adicional es la escalabilidad, pues el número de adyacencias se incrementa cuadráticamente con el número de enrutadores.

A raíz de esto, se buscó una solución mas integrada y con menos inconvenientes que el modelo superpuesto de IP/ATM. Surgieron varias propuestas con el fin de desarrollar una solución con las características de desempeño de los conmutadores ATM y el control de un enrutador IP y fue así como un grupo de proveedores generaron soluciones de conmutación multinivel que integraban dichas características. Entre los principales trabajos se encuentran IP Switching diseñado por Ipsilon/Nokia, Tag Switching desarrollado por Cisco Systems, Aggregate Route-Based IP Switching (ARIS) de IBM Corporation, IP Navigator de Cascade/Ascend/Lucent Technologies y Cell Switching Router (CSR) desarrollado por Toshiba.

Todas estas soluciones combinan las mejores propiedades de la conmutación ATM (rapidez y capacidad) y del enrutamiento IP (simplicidad y escalabilidad), que permiten integrar los niveles 2 y 3 de forma efectiva sin los problemas presentados por el modelo IP/ATM. El

principal logro de éstas aproximaciones fue la creación de un enrutador extremadamente rápido y eficiente que soporta software de enrutamiento IP. Al tener los protocolos de enrutamiento estándar corriendo sobre el núcleo del sistema, se obtienen beneficios como la eliminación del problema de escalabilidad del modelo superpuesto, reducción del volumen de tráfico generado por el IGP y la visibilidad de la topología física del núcleo de la red a los procedimientos de enrutamiento.

El problema fundamental de estas soluciones de conmutación multinivel, fue su falta de interoperabilidad, pues cada una utilizaba tecnologías diferentes, además, la mayoría de ellas sólo podían operar sobre infraestructuras ATM. Estos problemas llevaron a la creación de la tecnología de Conmutación de Etiquetas Multiprotocolo como respuesta a los requerimientos de interoperabilidad, eficiencia y escalabilidad de las redes IP.

3.2 DEFINICIÓN DE MPLS

La Conmutación de Etiquetas Multiprotocolo (MPLS - Multiprotocol Label Switching) surgió como respuesta al esfuerzo realizado por Grupo de Trabajo en Ingeniería de Internet (IETF - Internet Engineering Task Force), en la búsqueda de una solución acorde a las exigencias actuales de Internet, y como paso final en la evolución de las tecnologías de conmutación multinivel. MPLS fue originalmente presentado como la manera de optimizar el proceso de envío de paquetes, pero ahora se está consolidando como la tecnología estándar que ofrece nuevas capacidades a las grandes redes IP.

MPLS es una tecnología orientada a la conexión que permite a los proveedores de servicio controlar el flujo de tráfico IP que se transmite por sus redes. Para ello, MPLS define un mecanismo para establecer trayectos virtuales a través de la red, el cual admite que el tráfico sea encaminado dinámica o manualmente dentro de esos trayectos.

Los enrutadores y conmutadores MPLS construyen sus propias tablas de direcciones haciendo transparente al nivel 3 los procesos de encaminamiento, creando trayectos extremo a extremo que aseguran la entrega de la información al destino correspondiente. MPLS es un medio para proporcionar algunas de las características de las redes orientadas a conexión a las redes sin conexión. En el encaminamiento no orientado a la conexión, la dirección de destino de un paquete es examinada cada vez que dicho paquete pasa por un nodo. La ruta del paquete se adapta en función del estado de las tablas de encaminamiento de cada nodo, pero, como la ruta no puede predecirse, es difícil reservar recursos que garanticen la QoS. Además, las búsquedas en las tablas de encaminamiento hacen que cada nodo pierda cierto tiempo, que se incrementa en función de la longitud de la tabla. Sin embargo, MPLS permite a cada nodo asignar una etiqueta a cada uno de los elementos de la tabla y comunicarla a los nodos vecinos.

MPLS integra las funcionalidades de nivel 3 de enrutamiento con los mecanismos de nivel 2 de la conmutación, por esto algunas veces es conocida como la tecnología de nivel 2.5. En la

Figura 3.2 se ilustra la pila de protocolos que puede usarse en la operación de MPLS. El diagrama es dividido en varias partes, protocolos de enrutamiento IP (OSPF, BGP, etc.), conmutación de etiquetas, Base de Información de Etiquetas (LIB -Label Information Base), protocolos de señalización para la distribución de etiquetas (LDP, CR-LDP), protocolos de nivel 2 (PPP, ATM, Frame Relay) y, TCP y UDP usados por los protocolos de señalización.

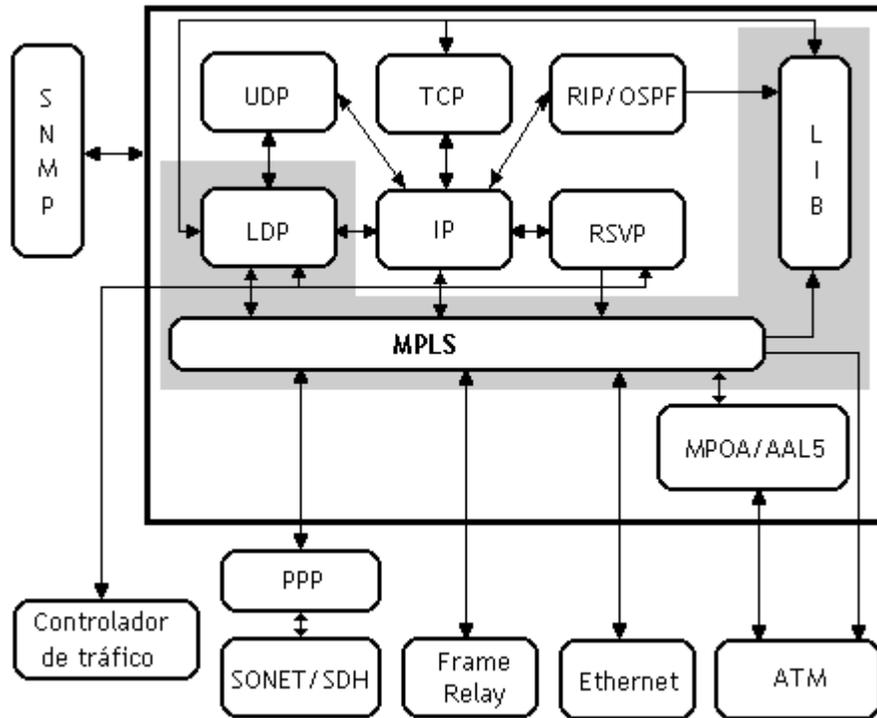


Figura 3.2. Pila de Protocolos.

El objetivo del comité de trabajo de MPLS es estandarizar una tecnología base que combine el uso del intercambio de etiquetas en el componente de envío, con el enrutamiento de nivel de red en el componente de control. Al existir una clara separación entre las funciones de éstos componentes, cada una de las partes puede evolucionar individualmente sin afectar a la otra, por lo cual la evolución se torna fácil, menos costosa y menos propensa a errores.

Para alcanzar estos objetivos, el grupo de trabajo de MPLS ha entregado una solución que satisface un número de requerimientos tales como:

- MPLS funciona sobre cualquier tecnología de nivel de enlace. Si la tecnología de nivel 2 soporta un campo de etiquetas, éste es utilizado para encapsular la etiqueta MPLS. Si por el contrario, la tecnología de nivel de enlace no soporta un campo de etiquetas, una etiqueta MPLS estándar se agrega entre las cabeceras de nivel de enlace y nivel de red.

- MPLS soporta el envío de flujos de tráfico unicast y multicast. Para el flujo multicast se recomienda un método que consiste en mapear una etiqueta entrante en un conjunto de etiquetas salientes.
- MPLS es compatible con el Modelo de Servicios Integrado del IETF. MPLS, al ser estandarizado por el IETF es compatible con los desarrollos realizados por este Grupo de Trabajo.
- MPLS está diseñado para soportar el constante crecimiento de la Internet. Por el nuevo enfoque dado por MPLS a la ingeniería de tráfico, redes privadas virtuales y calidad de servicio, brinda un amplio soporte frente a los posibles cambios evolutivos de Internet.
- MPLS soporta operaciones de administración y mantenimiento. Esto es posible gracias a las facilidades de gestión que tienen los enrutadores que soportan esta tecnología y a la capacidad de enrutamiento explícito que poseen.
- MPLS es interoperable entre los distintos proveedores. El Grupo de Trabajo de MPLS del IETF ha hecho un gran esfuerzo en conjunto con varios proveedores y empresas del sector, para estandarizar las tecnologías de Conmutación Multinivel y así garantizar la interoperabilidad entre cada uno de los productos.
- MPLS soporta QoS. Gracias a las funcionalidades de MPLS para la ingeniería de tráfico y la reservación de recursos hace que se garantice la transmisión adecuada de todo tipo de tráfico.

MPLS es considerada como la siguiente etapa en la evolución de las redes IP y esto se debe a las siguientes características que hacen de MPLS una red multifuncional y multipropósito:

- Entre las características principales dentro del dominio MPLS está la adición de una etiqueta de longitud fija a cada uno de los paquetes IP que ingresan al dominio y el uso de un protocolo de distribución de etiquetas para el establecimiento de los Trayectos Conmutados de Etiquetas (LSP - Label Switched Path). Cabe anotar que las decisiones de enrutamiento serán tomadas en base a la etiqueta MPLS adicionada a la entrada del dominio, y no a la información de la cabecera IP. Una vez el paquete abandone el dominio la etiqueta MPLS será removida.
- MPLS aprovecha su capacidad de establecimiento de trayectos virtuales para aplicar parámetros de ingeniería de tráfico que garanticen el ancho de banda necesario y una limitada variación del retardo para el transporte del flujo de datos. El dispositivo de red que soporta MPLS debe estar en la capacidad de monitorear y reportar el actual estado de los recursos que están siendo utilizados en cada interfaz.
- MPLS incrementa las capacidades de enrutamiento mejorando la operación de los protocolos IP convencionales.

- MPLS aprovecha las ventajas de las tecnologías orientadas y no orientadas a la conexión. En MPLS se establece una conexión virtual entre dos puntos (característica de las redes orientadas a la conexión) sobre una red de datagramas (no orientada a la **conexión**). De ésta forma se aprovecha dicha conexión virtual para la prestación de servicios sensibles a retardos y a la pérdida de paquetes, y se mantiene la eficiencia de las tecnologías no orientadas a la conexión.
- Con MPLS son necesarios menos dispositivos que los empleados en el modelo superpuesto, la fiabilidad es por lo tanto incrementada y los costos de operación son reducidos. Adicionalmente, el diseño de la red y su arquitectura se hacen más simples.
- MPLS hace posible que el tráfico sea conmutado a través de enrutadores IP sin la necesidad de revisar la cabecera de cada paquete IP antes de enviarlo al próximo salto, debido al establecimiento de trayectos virtuales que hacen que la cabecera de los paquetes solo sea analizada en la entrada y la salida del trayecto.
- Con MPLS, la Internet podrá finalmente transportar todos los tipos de tráfico, desde datos hasta voz y video.

El resultado es una arquitectura inteligente, distribuida, fácil de gestionar, escalable y que evoluciona de acuerdo a los cambios exigidos por los nuevos servicios, además, MPLS usa protocolos de enrutamiento estándar como OSPF que facilitan su introducción con cambios e interrupciones mínimas.

3.3 ARQUITECTURA MPLS

Como cualquier otra tecnología, MPLS tiene su propio conjunto de conceptos y componentes que se integran entre sí para desempeñar las funciones de enrutamiento, control, establecimiento de trayectos, etc. requeridas para mejorar el funcionamiento de la red. Para comprender cómo funciona MPLS, a continuación se da una breve descripción de cada uno de sus componentes.

3.3.1 Estructura de Red

Una red MPLS consiste de un conjunto de dispositivos que soportan las funcionalidades de MPLS. Cuando todos los dispositivos de red están bajo una misma administración se le conoce como *Dominio MPLS*, como se muestra en la Figura 3.3. Los dispositivos básicos que conforman el Dominio MPLS se clasifican en dos grandes grupos: Enrutador de Frontera de Etiquetas (LER - Label Edge Router) y Enrutador de Conmutación de etiquetas (LSR - Label Switching Router). Los LERs y LSRs son enrutadores o conmutadores con mayores capacidades funcionales, soportan enrutamiento de nivel de red, conmutación de nivel de enlace y

conmutación por etiquetas. Cada uno de estos elementos tienen funciones específicas para el envío de los paquetes dentro del dominio MPLS.

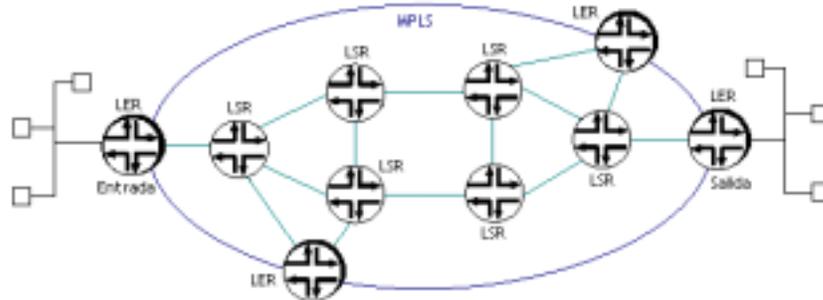


Figura 3.3. Dominio MPLS.

- **Enrutador de Frontera de Etiqueta - LER.** El LER es un dispositivo de alta velocidad y gran desempeño, localizado en la frontera del dominio, cuya función principal es proporcionar la conexión entre la red MPLS y otras redes de diferentes características. El LER desempeña todas las funciones necesarias para manejar el tráfico que entra y sale del dominio MPLS, tales como clasificar paquetes, asignar y remover etiquetas, etc. Es importante tener en cuenta que el LER hace parte de la red y es un punto de control y gestión para los proveedores de servicio.
- **Enrutador de Conmutación de Etiquetas - LSR.** El LSR es un dispositivo que proporciona alta velocidad de conmutación y se localiza en el núcleo del dominio. El LSR es el responsable de manejar el tráfico y participa en el intercambio de información para establecer los trayectos dentro del dominio MPLS.

3.3.2 Clase Equivalente de Envío (FEC - Forwarding Equivalence Class)

MPLS usa el concepto de Clase Equivalente de Envío para referirse a un conjunto de paquetes con características comunes que son enviados a través de un mismo trayecto, aún cuando sus destinos sean diferentes. En términos generales, cuando los paquetes entran al dominio son divididos o clasificados en subconjuntos llamados FEC, esta clasificación se lleva a cabo teniendo en cuenta algunos factores como la dirección IP de la fuente, dirección IP del destino, versión del protocolo IP, campos TTL y tipo de servicio entre otros. Un ejemplo de FEC es un conjunto de paquetes unicast cuyas direcciones de destino corresponden a un mismo prefijo de dirección; otro FEC sería un grupo de paquetes donde las direcciones de fuente y destino son las mismas.

Un FEC puede ser clasificado en "granularidad gruesa" (coarse) o "granularidad fina" (fine). La elección del nivel de granularidad ayuda a preservar los recursos de red porque permite compartir la misma etiqueta entre muchos destinos, mejorando los beneficios de la conmutación. Algunas de las granularidades que se usan en un ambiente MPLS son:

Prefijo IP: Consiste en todos los paquetes que corresponden a un mismo prefijo IP de destino, al cual se le ha asignado su propio camino en la tabla de envío. Este tipo es de granularidad gruesa y proporciona ciertas ventajas tales como la reducción de los mensajes de señalización y manejo de un conjunto grande de paquetes como una clase de tráfico determinado. Esta granularidad puede no ser escalable en grandes redes con LSRs que tienen un limitado rango de etiquetas.

Enrutador de Salida: Consiste en el tráfico que comparte un enrutador de salida y por consiguiente un mismo segmento del trayecto LSP. Este tipo representa una granularidad gruesa.

Flujo de Aplicación: Representa una granularidad fina que es menos escalable que los otros tipos, en la cual los flujos de aplicación mantienen su propio trayecto conmutado y cuya ventaja es proporcionar conmutación extremo a extremo manejando diferentes requerimientos de QoS. Es recomendable utilizarla en ambientes empresariales y comerciales.

En la Figura 3.4 se presenta la idea del concepto de granularidad.



Figura 3.4. Concepto de Granularidad.

3.3.3 Descripción de Etiquetas

El concepto principal en MPLS es asignar una etiqueta a cada uno de los paquetes IP que entran al dominio MPLS. La etiqueta es un identificador de longitud fija que se agrega al paquete para determinar cómo será enviado a través de la red. La etiqueta sólo tiene significado local entre dos dispositivos que se están comunicando dentro del dominio. La etiqueta que se agrega al paquete representa la clase equivalente de envío a la cual él pertenece.

La etiqueta es usada en los enrutadores MPLS como índice para consultar la tabla de envío y determinar cómo será transportado un paquete hasta su destino final. Esto se logra gracias a la información que resume la etiqueta acerca del enrutamiento del paquete: Destino, Procedencia, Miembros de redes privadas virtuales, Información de QoS, La ruta para el paquete como elección para la ingeniería de tráfico (TE).

En general, la etiqueta es un número entero positivo de 20 bits que se encuentra en el rango 0 - 1048575; este rango se divide de la siguiente forma:

0 a 15. Reservado a etiquetas con semántica especial.

16 a 1023. Reservado al uso de etiquetas para la configuración manual del trayecto, asegurando que no haya conflictos con las etiquetas asignadas dinámicamente.

1024 a 99.999. Reservado para aplicaciones futuras.

100.000 a 1048575. Para la negociación, asignación, reuso y liberación automática de etiquetas. Generalmente las etiquetas por plataforma son asignadas al rango 100000-799999 y las etiquetas por interfaz son asignadas en el rango 800000-1048575.

3.3.4 Encapsulación de Etiquetas

La etiqueta adicionada al paquete IP tiene sólo significado local (puede ser modificada de interfaz a interfaz), por consiguiente no modifica la información de la cabecera tan sólo la encapsula. En MPLS se utiliza la técnica denominada *Encapsulación Genérica*, la cual es independiente del protocolo y encapsula el paquete de nivel de red, aunque puede ser utilizada para encapsular los protocolos de nivel de enlace. Es función de los LER encapsular los paquetes que entran al dominio MPLS, los enrutadores analizan el contenido de la cabecera IP y seleccionan la etiqueta apropiada para encapsularlos. En comparación con el enrutamiento convencional, el análisis no sólo se basa en la dirección de destino IP.

Según las referencias del IETF, MPLS funciona sobre cualquier tipo de tecnología de transporte. Por ello, si MPLS funciona sobre tecnologías como PPP, Ethernet, etc., se usa la encapsulación genérica que consiste en agregar una cabecera de 4 octetos que contiene un campo específico para la etiqueta y se inserta entre la cabecera de nivel 2 y la cabecera de nivel 3. El formato de la cabecera genérica MPLS se muestra en la Figura 3.5.

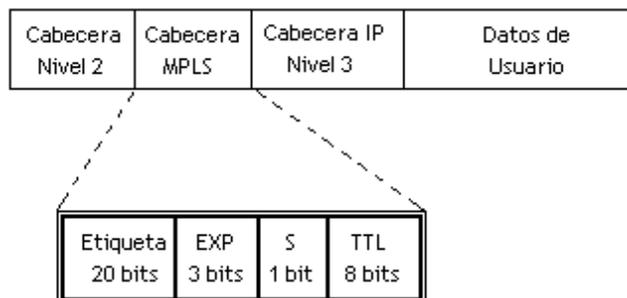


Figura 3.5. Encapsulación Genérica.

La cabecera esta compuesta de un campo Etiqueta (20 bits) que indica el valor actual de la etiqueta MPLS. El campo EXP (3 bits) identifica la Clase de Servicio (derivado del campo CoS

de la cabecera IP) y es considerado un campo experimental que esta siendo utilizado para implementaciones de QoS. El campo Stack (1 bit) indica la existencia de una pila de etiquetas. Por último se encuentra el campo TTL (8 bits) que proporciona la funcionalidad estándar TTL de las redes IP.

Si los protocolos de enlace disponen de un campo para etiquetas, como es el caso de Frame Relay y ATM, la técnica de encapsulación utiliza las cabeceras de nivel 2 o en otros casos las cabeceras de nivel 3 para encapsular la etiqueta. En ATM los campos VPI/VCI (Virtual Path Identifier/Virtual Circuit Identifier) y en Frame Relay el campo DLCI se usan como la etiqueta MPLS. (Figuras 3.6. y 3.7).

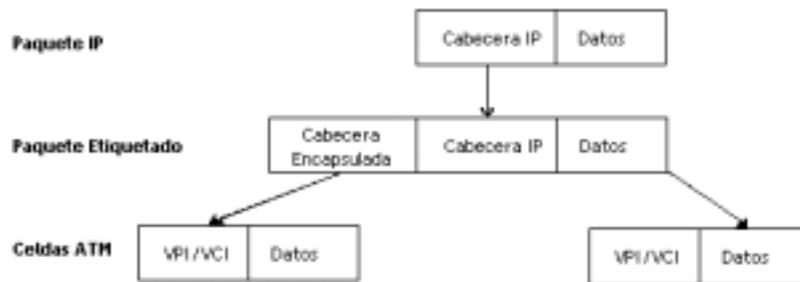


Figura 3.6. ATM como Nivel de Enlace de Datos.

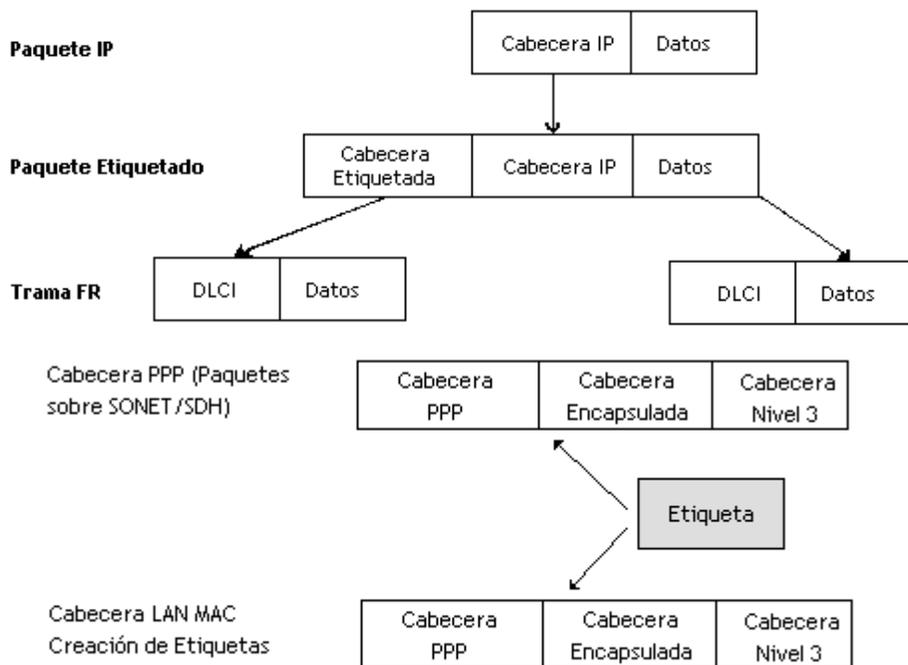


Figura 3.7. Frame Relay como Nivel de Enlace de Datos.

La encapsulación especifica un conjunto de reglas para procesar el campo TTL. Estas reglas permiten que el comportamiento de la red MPLS sea similar al de una red IP desde la

perspectiva del manejo TTL. El campo TTL es algunas veces usado para funciones de prevención de bucles, alcance de los paquetes multicast y soporte de comandos "tracerouter". La manera de procesarlo depende de la técnica de encapsulación utilizada. Si el valor de la etiqueta esta encapsulado entre las cabeceras de nivel 2 y nivel 3, el procesamiento del TTL es muy similar al del Protocolo Internet. Cuando se encapsula un paquete por primera vez en la frontera del dominio, se copia el valor del campo TTL de la cabecera IP al de la cabecera MPLS. Durante el transporte del paquete a través del LSP, el valor TTL es reducido en 1 en cada LSR hasta alcanzar la salida del dominio donde la etiqueta se retira y se copia el TTL de la cabecera MPLS al de la cabecera IP.

Si el valor de etiqueta es encapsulado en la cabecera de nivel 2 y los paquetes son enviados por conmutadores de nivel de enlace (conmutadores ATM), no es posible reducir el valor TTL porque no se dispone de este campo. Un segmento LSP donde no se puede reducir el valor TTL es llamado "Segmento LSP no TTL", en cuyo caso, se reduce el campo TTL IP cuando la etiqueta es removida, permitiendo que un LSP parezca un salto simple que beneficia a la funcionalidad tracerouter. Este comportamiento es útil cuando el operador de red desea encubrir detalles de la topología de red.

Otro aspecto importante a tratar en la encapsulación es la fragmentación del paquete, un paquete etiquetado puede requerir fragmentación, como se hace con los datagramas IP. Es posible que al adicionar una o más etiquetas al paquete, su tamaño sea mayor al valor MTU (acordado previamente por los enrutadores durante la fase inicial) y se requiera fragmentación aunque el paquete IP no tenga requerimientos de este tipo. Si un paquete MPLS necesita ser fragmentado, la fragmentación se aplica al datagrama IP y la pila de etiquetas se adjunta a cada fragmento.

3.3.5 Pila De Etiquetas

MPLS permite que un paquete soporte un número arbitrario de etiquetas organizadas como una pila LIFO - últimas en entrar primeras en salir -, lo cual se conoce como "pila de etiquetas" (Figura 3.8). La etiqueta en la base de la pila es llamada etiqueta de nivel 1, las etiquetas arriba de ella son numeradas consecutivamente hasta la de nivel n; se dice entonces que la pila es de longitud n.



Figura 3.8. Pila de Etiquetas.

El propósito de la pila de etiquetas es permitir una jerarquía multinivel que facilite operaciones de túneles dentro del dominio MPLS. Aunque MPLS soporta una jerarquía multinivel, el procesamiento de un paquete etiquetado es completamente independiente del

nivel de jerarquía. Los enrutadores MPLS toman sus decisiones de envío basándose exclusivamente en la etiqueta superior de la pila.

Después que la etiqueta superior es procesada, las operaciones que puede realizar un enrutador sobre la pila son:

- **Push:** Adiciona una nueva etiqueta en la parte superior de la pila. Si la longitud de la pila es mayor que cero, los campos EXP y TTL de la nueva etiqueta podrían derivarse de las etiquetas de niveles inferiores. En caso contrario, la nueva etiqueta será la primera en la pila y los campos TTL y EXP se derivan de la cabecera del paquete IP.
- **Pop:** Remueve la etiqueta superior de la pila. Si la etiqueta removida es la última en la pila, el valor TTL se copia a la cabecera del paquete IP; pero si se tienen múltiples etiquetas, los campos EXP y TTL de la nueva etiqueta podrían derivarse de la anterior.
- **Swap:** Reemplaza el valor de la etiqueta de nivel superior por un nuevo valor. Los bits de EXP y TTL son copiados de la etiqueta anterior, y el campo TTL es copiado y reducido en 1.
- **Push múltiple:** Adiciona múltiples etiquetas (superior a 2) en la parte superior de la pila de etiquetas.
- **Swap and Push:** Reemplaza la etiqueta superior con un nuevo valor, seguido de la adición de una nueva etiqueta en la parte superior de la pila.

3.3.6 Trayecto Conmutado de Etiquetas (LSP - Label Switched Path)

Un LSP es un camino virtual a través del cual los paquetes asignados a un mismo FEC viajan a lo largo de la red. Cada LSP es creado por la concatenación de uno o más saltos, permitiendo que un paquete sea enviado desde un LSR a otro a través del dominio MPLS. El primer enrutador que interviene en un LSP se le denomina enrutador de entrada o de cabecera, al último enrutador se le llama enrutador de salida o de cola; y a los enrutadores entre los LERS de entrada y salida se les conoce con el nombre de enrutadores de tránsito o LSRs. Un LSP es de naturaleza unidireccional, es decir que los paquetes fluyen en una sola dirección desde el enrutador de entrada al enrutador de salida, por tanto para el tráfico dúplex se requiere de dos LSPs, uno para cada dirección del tráfico. El trayecto cuya dirección de transferencia de paquetes es desde el nodo de entrada hacia el nodo de salida toma el nombre de LSP downstream, en caso contrario será un LSP upstream.

Un enrutador MPLS puede hacer parte de múltiples LSPs. El enrutador puede ser la entrada, la salida o el enrutador de tránsito de múltiples LSPs por lo que un LSP puede tomar la forma de árbol punto a multipunto. Un árbol resulta de la unión de trayectos conmutados en un nodo, cuando varios LSP upstream para un flujo dado, son unidos a un LSP downstream.

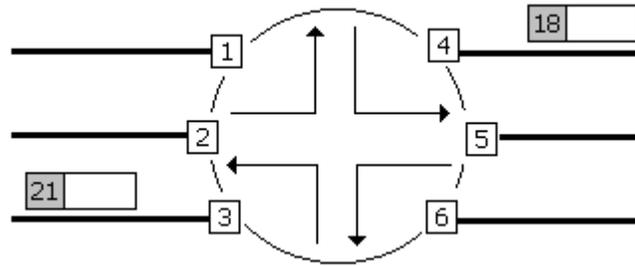
3.4 CONMUTACIÓN DE ETIQUETAS

La operación básica de una red MPLS involucra la conmutación de etiquetas para enviar los datos a través de la red, este algoritmo es similar al usado en las redes ATM y Frame Relay para la transmisión de los paquetes. La idea principal de la conmutación es la asignación e intercambio de etiquetas que permiten el establecimiento de los trayectos LSP. Cuando el paquete entra a la red, el LSR lo analiza y asigna una etiqueta basándose en la dirección de destino y en otra información contenida en su cabecera. La etiqueta asignada se asocia a la ruta que el paquete tomará para alcanzar el nodo de salida requerido y puede usarse para especificar las características de manejo del tráfico garantizando altos niveles de QoS.

La conmutación de etiquetas requiere de la clasificación de paquetes a la entrada del dominio MPLS para asignar la etiqueta inicial de cada paquete y determinar el LSP a usar. La decisión es un asunto local que se basa en factores como la dirección de destino, requerimientos QoS y el estado actual de la red. Esta flexibilidad hace de MPLS una tecnología muy atractiva para los operadores de red.

Una red con conmutación de etiquetas cumple el mismo propósito que las redes enrutadas convencionales: entregar el tráfico a uno o más destinos en forma segura, pero la conmutación de etiquetas provee una serie de beneficios comparado con el enrutamiento salto por salto:

- La conmutación de etiquetas puede ser usada por múltiples servicios y tipos de tráfico.
- El intercambio de etiquetas provee flexibilidad en la manera de asignar los paquetes a los FECs. Los paquetes pueden ser asignados a un FEC de acuerdo a consideraciones políticas, dirección de fuente, tipo de aplicación, punto de entrada de la red, punto de salida o una combinación de estas.
- Los proveedores de servicios pueden construir los LSPs para soportar requerimientos de aplicaciones específicas y son designados para minimizar el número de saltos, satisfacer ciertos requerimientos de ancho de banda, desempeño, etc.
- El beneficio de la conmutación es la habilidad de tomar algún tipo de tráfico específico de usuario, asociarlo a un FEC y dirigir el FEC a un LSP que satisfaga los requerimientos, permitiendo un control preciso del flujo en la red, logrando que sea más efectiva y pueda proporcionar más servicios.
- La conmutación de etiquetas requiere solamente un algoritmo de envío para soportar tráfico unicast y multicast. El algoritmo usado es conocido como algoritmo de intercambio de etiquetas. En la Figura 3.9 se ilustra la operación del algoritmo usado por un LSR. Un paquete es recibido por la interfaz 3 y contiene un valor de etiqueta 21. El LSR, usa la información de la tabla de envío, reemplaza la etiqueta con el valor 18 y envía el paquete por la interfaz de salida 14.



Interfaz Entrada	Etiqueta Entrada	Interfaz Salida	Etiqueta Salida
⋮	⋮	⋮	⋮
3	21	4	18
3	56	6	135
⋮	⋮	⋮	⋮

Figura 3.9. Intercambio de Etiquetas.

3.5 OPERACIONES SOBRE LAS ETIQUETAS

Antes de estudiar las operaciones que los enrutadores MPLS ejercen sobre las etiquetas, es necesario conocer las etiquetas especiales que colaboran en el proceso de envío de los paquetes.

Las etiquetas especiales son definidas en el proceso de encapsulación, y se encuentran en el rango 0 al 15; los valores de 4 al 15 están reservados para aplicaciones futuras. El valor 0 representa la Etiqueta Explícita Nula IPv4 (Explicit Null Label IPv4). Este valor es legal sólo cuando la etiqueta es única. El valor indica que la etiqueta puede ser retirada por el LSR del último salto (penúltimo enrutador del LSP) y que el paquete puede ser enviado con base a la información de la cabecera IPv4. Esta etiqueta es usada en los casos donde la encapsulación es necesaria, pero no se requiere de una etiqueta válida, por ejemplo, para conservar el campo EXP que garantice la QoS en el último salto del LSP, aunque la etiqueta no sea requerida en el último salto.

El valor 1 representa la Etiqueta de Alerta al Enrutador (Router Alert Label). Este valor es legal en cualquier sitio de la pila excepto en la etiqueta de nivel 1 ó etiqueta base. El LSR que recibe el paquete, quita la etiqueta superior de la pila y envía el paquete de acuerdo a la información de la siguiente etiqueta. No es válido usar este valor en la base de la pila porque no hay asociación con una red en particular.

El valor 2 representa la Etiqueta Explícita Nula IPv6 (Explicit Null Label IPV6). Este valor es legal sólo cuando la etiqueta es única. La etiqueta indica que el enrutador del último salto puede retirar la etiqueta y enviar el paquete basándose en la cabecera IPv6. La razón para

tener dos valores diferentes para IPv4 e IPv6 es la necesidad de distinguir el protocolo de nivel 3 que ha sido encapsulado.

La Etiqueta Implícita Nula (Implicit Null Label) esta representada por el valor 3. Es una etiqueta que un LSR puede asignar y distribuir, pero nunca aparece en la cabecera MPLS. Cuando un LSR recibe un paquete, consulta su LIB y se da cuenta que existe una asociación a una etiqueta implícita nula, entonces en lugar de reemplazar la etiqueta superior de la pila, el LSR la retira y envía el paquete resultante al siguiente salto. Aunque este valor nunca aparece en la encapsulación, es necesario especificarlo para usarlo en el protocolo de distribución de etiquetas.

Las etiquetas especiales son usadas entre el enrutador de salida y el penúltimo enrutador de un LSP. Si el LSP esta diseñado para enviar solamente paquetes IPv4, el enrutador de salida indica al penúltimo enrutador usar el valor 0 como etiqueta del último salto. Si el LSP esta configurado para transportar únicamente paquetes IPv6, el LER indica al penúltimo LSR usar el valor 2 como etiqueta de último salto.

El LER indica al penúltimo LSR usar el valor 3 como etiqueta final, que es un requisito para que en el penúltimo salto, la etiqueta sea retirada, y el LER no procesa un paquete MPLS, ya que él recibe directamente la carga (ya sea IPv4, IPv6, u otros). Esto reduce el número de consultas MPLS realizadas por el LER de salida.

Realizar la operación pop en el penúltimo salto de un LSP tiene la ventaja de agilizar el envío de paquetes al destino final. Si un LER recibe un paquete MPLS, primero consulta la etiqueta top de la pila y determina que él es el LER de salida, después retira la etiqueta y examina el resto del paquete. Si hay otra etiqueta en la pila, el LER consulta la etiqueta y envía el paquete de acuerdo al resultado de la consulta. En este caso el enrutador se comporta como un LSR de tránsito. Si no hay más etiquetas al realizar la operación pop, el paquete se envía de acuerdo a la dirección de destino de nivel de red. Lo anterior conduce a que el enrutador de salida lleve a cabo dos consultas: consulta dos etiquetas, o consulta una etiqueta y una dirección de la cabecera IP.

Si penúltimo retira la etiqueta, el LER de salida consulta la etiqueta superior de la pila para tomar decisiones acerca del envío, pero si el paquete no tiene etiqueta el LER utiliza la cabecera IP para transmitir el paquete al destino final. Este proceso permite que el LER consulte una vez la etiqueta, o la dirección IP, además el penúltimo LSR también realiza sólo una consulta de la etiqueta, facilitando el envío del paquete al destino final.

3.5.1 Asignación de Etiquetas

Un concepto fundamental en MPLS es la asociación de una etiqueta a un paquete IP, conocido como *Asignación de Etiquetas*. Antes de asociar la etiqueta, el paquete IP es asignado a un FEC cuando entra a la red MPLS, después el FEC es encaminado por un LSP de acuerdo con el valor de la etiqueta y de la información de la tabla de enrutamiento.

Para la asignación se usa dos tipos de etiquetas, las Etiquetas por Interfaz y las Etiquetas por Plataforma. Las Etiquetas por Interfaz son únicas para cada interfaz y se encuentran en el rango 800.000 a 1'048.575. Las etiquetas de interfaces diferentes son asignadas independientemente, es decir, que una etiqueta recibida por una interfaz no está relacionada con otra del mismo valor recibida por otra interfaz. Al utilizar estas etiquetas, un LSR puede asignar un mismo valor de etiqueta a dos FECs, siempre y cuando los paquetes sean enviados por interfaces diferentes. Las Etiquetas por Plataforma están ubicadas en el rango 100.000 a 799.999, estos valores de etiqueta son únicos para todo el LSR, y no se permite que en varias interfaces se tenga etiquetas del mismo valor.

Si un LSR está diseñado para consultar etiquetas que están dentro de un rango determinado, entonces el LSR debe asegurarse que la asignación de etiquetas esté dentro de ese rango.

La asignación de etiquetas es el resultado de algunos eventos o políticas que indican la necesidad de realizar la asignación. Estos eventos se dividen en dos grupos, modelo de manejo de datos (Data Driven) y el modelo de manejo de la información de control (Control Driven). En el modelo de manejo de datos, las asignaciones son creadas cuando el tráfico llega a un LER. Un enrutador puede crear una asignación cuando detecta el primer paquete del flujo, o después de que llegue un número determinado de paquetes. La ventaja de este modelo consiste en que las asignaciones son establecidas sólo cuando hay tráfico para usarlas, de esta manera, se reduce el número de entradas en la tabla de envío. Sin embargo, este modelo tiene desventajas cuando se utiliza en el núcleo de redes de área amplia, porque podría generar un gran número de flujos individuales y los enrutadores necesitarían de sofisticadas capacidades de clasificación de paquetes para identificar los flujos de tráfico. Otras desventajas de este modelo son:

- Latencia (retardo) entre el reconocimiento del flujo y la asignación de la etiqueta a ese flujo.
- La presencia de una cantidad significativa de flujos con ciclos de vida cortos, puede imponer una carga pesada en la red.
- Limitada escalabilidad de la red puesto que el número de LSPs es proporcional al número de flujos individuales.

En el manejo de información de control, la asignación de etiquetas se establece en respuesta a la actualización en el proceso de enrutamiento o a la recepción de información de control. Actualmente MPLS utiliza este modelo para la asignación de etiquetas debido al número de ventajas que tiene al implementarse en una red de área amplia:

- Las etiquetas son asignadas y distribuidas antes que se reciba el tráfico de usuario. Esto significa que si existe una ruta en la tabla de envío se le asigna una etiqueta, y así cuando llega el tráfico de usuario este es enviado inmediatamente evitando retardos.

- La escalabilidad es mayor que en el modelo de manejo de datos porque el número de LSPs es proporcional al número de entradas en la tabla de envío y no al número de flujos individuales.
- En una topología estable, la carga de la asignación y distribución de etiquetas es baja comparada con el modelo de manejo de datos donde los LSPs son establecidos cuando llega un nuevo flujo.

En la arquitectura MPLS existen tres formas para asignar etiquetas: Asignación Downstream no solicitada ó Asignación Downstream, Asignación Upstream y Downstream sobre demanda. La diferencia entre ellas radica en cómo son asignadas las etiquetas y cómo es distribuida la información de asignación.

En la Asignación Downstream, la decisión de vincular una etiqueta a un FEC se realiza por un nodo downstream e informa a los LSRs upstream, así, la etiqueta entrante es asignada localmente y la etiqueta saliente remotamente (por el LSR downstream). En la Asignación Upstream el LSR upstream realiza la asociación e informa a los demás LSRs. La etiqueta entrante es asignada remotamente y la de salida localmente. En la Asignación Downstream Bajo Demanda un LSR upstream solicita una asignación de etiqueta a un nodo downstream, el cual la realiza e informa a los LSRs upstream.

La elección de alguna de las formas de asignación depende de las características de las interfaces que soporta una implementación. Sin embargo las tres técnicas se pueden usar en la misma red, y para lograr su integración, el LSR upstream y el downstream deben acordar la técnica a usar.

MPLS, además de asignar una etiqueta a un FEC, asigna una etiqueta a las entradas de la tabla de envío. Antes de entrar a estudiar este tipo de asignación, es necesario comprender el concepto de *Entrada de Envío de Etiqueta para el Siguiete Salto (NHLFE - The Next Hop Label Forwarding Entry)*. Un NHLFE representa las entradas que conforman la tabla de envío y se usa para determinar cómo enviar un paquete a través de la red. Entre la información que contiene un NHLFE se encuentra el siguiente salto del paquete (Interfaz de salida), la etiqueta saliente y/o las operaciones sobre la pila de etiquetas (pop, push, swap), encapsulación de enlace de datos para usarla cuando se transmite el paquete, información sobre los recursos (opcional) y las políticas para el manejo del paquete (opcional).

3.5.2 Mapeo de la etiqueta entrante (ILM - Incoming Label Map)

El ILM asigna cada etiqueta entrante a un conjunto de NHLFEs. Un ILM es usado cuando los paquetes que llegan a un LSR para ser enviados al siguiente salto, son paquetes etiquetados. Si un ILM mapea una etiqueta a un conjunto de NHLFEs que contienen más de un elemento, sólo un elemento del conjunto se elige antes de enviar el paquete. El mapeo de la etiqueta entrante es útil cuando se desea balancear la carga sobre múltiples trayectos de igual costo.

3.5.3 Mapeo del FEC a un NHLFE (FTN - FEC to NHLFE Map)

El FTN vincula cada uno de los FECs a un conjunto de NHLFEs. FTN es usado cuando un paquete llega a un enrutador MPLS como un paquete IP que será etiquetado antes de enviarse.

El mapeo es necesario porque pueden existir NHLFEs con múltiples elementos para un FEC y se debe seleccionar sólo uno para transmitir el paquete. Al igual que en ILM, el FTN es útil para balancear la carga sobre múltiples trayectos de igual costo.

El mapeo de ILM y FTN se puede modificar a causa del reenrutamiento cuando un trayecto falla o por el desarrollo de procedimientos para balancear las cargas.

3.5.4 Protocolo de Distribución de Etiquetas

Una vez se establezcan las asignaciones entre las etiquetas y los FEC, esta información se debe propagar a los LSRs adyacentes para que cada uno cree su propia tabla de enrutamiento y se establezca un LSP a través del cual serán transportados los paquetes a través de la red, a este proceso se le conoce como *Distribución de Etiquetas*. El control y establecimiento de los LSPs se realiza por medio de protocolos de señalización. Los principales protocolos de señalización utilizados para la distribución de etiquetas son el Protocolo de Reservación de Recursos (RSVP - Resources reSerVation Protocol), el Protocolo de Distribución de Etiquetas (LDP - Label Distribution Protocol), Protocolo de Distribución de Etiquetas con Enrutamiento Restringido (CR-LDP - Constraint-Routed LDP), y BGP. A continuación se explica cada uno de ellos.

3.5.4.1 Distribución de etiquetas usando RSVP

RSVP fue desarrollado originalmente para la reservación de recursos en las redes IP, pero más adelante se le adicionaron nuevas características para que sirviera como protocolo de distribución de etiquetas y más funcionalidades para ingeniería de tráfico de modo que brindara soporte para señalización, establecimiento de niveles de prioridad, reenrutamiento, reoptimización de los trayectos y detección de bucles. RSVP es un protocolo separado del nivel 3 que usa los datagramas IP para intercambiar mensajes de establecimiento del trayecto entre los pares LSRs. RSVP no necesita mantener sesiones TCP, pero como consecuencia, debe controlar la pérdida de los mensajes.

El flujo básico para establecer un LSP usando RSVP se muestra en la Figura 3.10.

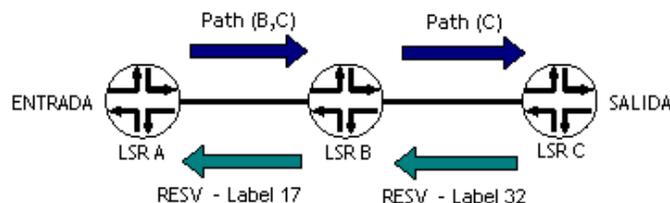


Figura 3.10. Flujo de Establecimiento de un LSP por medio de RSVP.

El LSR de ingreso (LSR A) desea establecer un nuevo LSP hacia LSR C. Los parámetros de tráfico requeridos para el nuevo trayecto y las políticas administrativas de red permiten a LSR A determinar que la ruta para el nuevo LSP debe ir a través de LSR B. Esta nueva ruta no es la misma que utilizaría el enrutamiento salto por salto. LSR A construye un mensaje Path con una ruta explícita (B, C) y detalles acerca de los parámetros de tráfico necesarios. LSR A envía el mensaje Path a LSR B como un datagrama IP.

LSR B recibe la solicitud del mensaje Path y determina que él no es el enrutador de salida para éste LSP, modifica la ruta en el mensaje y envía la solicitud hacia el LSR C.

LSR C determina que él es el enrutador de salida y basándose en los parámetros de tráfico solicitados, establece y reserva los recursos necesarios para el LSP. Entonces, selecciona una etiqueta para el nuevo trayecto y distribuye la etiqueta al LSR B en un mensaje Resv, el cual también contiene los parámetros actuales de los recursos reservados.

LSR B recibe el mensaje Resv y lo compara con la solicitud original usando el identificador de LSP (LSP ID) contenido tanto en el mensaje Path como en el Resv. Determina qué recursos se reservaron, asigna una etiqueta para el LSP, establece la tabla de envío y pasa la nueva etiqueta al LSR A en un mensaje Resv. Este último no reenvía el mensaje ni asigna una nueva etiqueta por ser la entrada del nuevo LSP. Para mantener el trayecto debe existir un intercambio periódico de mensajes Path y Resv entre los nodos.

3.5.4.2 Distribución de etiquetas usando LDP

Es un nuevo protocolo definido por el IETF para la distribución de etiquetas que consta de un conjunto de mensajes y procedimientos a través de los cuales los LSRs establecen LSPs a lo largo de la red. LDP se puede usar sobre diferentes mecanismos de control LSP y sobre los modelos de asignación de manejo de datos y manejo de información de control.

Dos LSRs que intercambian información de asignación de etiquetas usando LDP se conocen como *pares LDP* y entre ellos se intercambian cuatro clases de mensajes que sirven para diferentes propósitos y son los *mensajes de descubrimiento (Discovery Messages)* utilizados por los LSRs para advertir de su presencia en la red enviando periódicamente mensajes Hello, *mensajes de sesión (Session Messages)* los cuales establecen y mantienen las sesiones LDP, *mensajes de advertencia (Advertisement Messages)* usados para crear, cambiar y eliminar los vínculos entre las etiquetas y los FECs, y *mensajes de notificación (Notification Messages)* que transportan avisos e información de errores. El formato de estos mensajes se ilustra en la Figura 3.11.

1 bit	15 bits	16 bits	32 bits	Variable	Variable
U	Tipo de mensaje	Longitud de mensaje	ID de mensaje	Parámetros obligatorios	Parámetros opcionales

Figura 3.11. Formato de los Mensajes LDP.

Para establecer un LSP dentro de un dominio MPLS, los LSRs detectan la presencia de sus vecinos directos a través de un procedimiento de descubrimiento básico basado en UDP. Después de advertir su presencia en la red, los LSRs inician una sesión bidireccional para intercambiar información de etiquetas con sus pares LDP. Los dos LSRs establecen una conexión TCP y luego, intercambian mensajes de inicialización para negociar parámetros de sesión tales como la versión del protocolo LDP, el método para la distribución de las etiquetas, valores de tiempo y rangos VPI/VCI (si el nivel 2 es una red ATM), etc. Finalmente, la sesión LDP es establecida por un mensaje de mantenimiento de la conexión.

Durante una sesión LDP, las asignaciones de etiquetas pueden ser realizadas por los procedimientos de distribución downstream no solicitada ó distribución de etiquetas downstream sobre demanda.

RSVP y LDP pueden ejecutarse al mismo tiempo sobre el mismo dominio. El LSP establecido por LDP (LSP-LDP) será encaminado a través del LSP establecido por RSVP (LSP-RSVP). La Figura 3.12 muestra un LSP-LDP dirigido a través de un LSP-RSVP. El óvalo interno representa el dominio RSVP mientras que el externo representa al dominio LDP. RSVP ha establecido el LSP a través de los enrutadores B, C, D y E, con una secuencia de etiquetas de L3, L4. LDP ha establecido un LSP a través de los enrutadores A, B, E, F y G con una secuencia de etiquetas L1, L2, L5. LDP ve el LSP-RSVP entre los enrutadores B y E como un único salto.

Cuando el paquete llega al enrutador A, ingresa al LSP-LDP, y la etiqueta L1 es agregada a su cabecera. Cuando el paquete llega al enrutador B, la etiqueta L1 es reemplazada por una etiqueta L2. Debido a que el paquete está ingresando al LSP-RSVP, una segunda etiqueta (L3) es también adicionada a la cabecera.

La etiqueta L3 es entonces intercambiada por una nueva etiqueta L4 en el enrutador C y cuando el penúltimo enrutador del LSP-RSVP (D) es alcanzado por el paquete, la etiqueta superior es retirada de la pila. El enrutador E intercambia la etiqueta L2 por una nueva etiqueta L5 y el penúltimo enrutador del LSP-LDP (F) retira la última etiqueta.

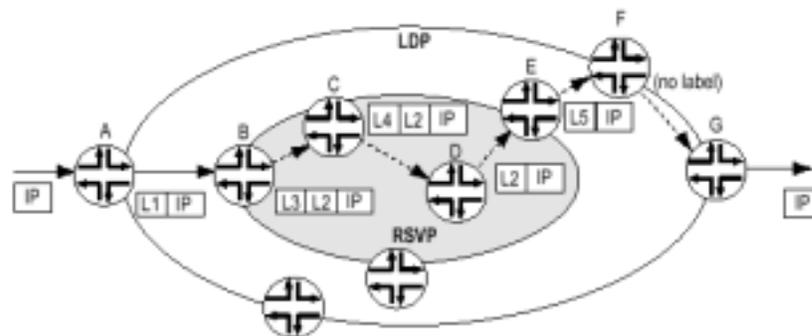


Figura 3.12. Encaminamiento de un LSP-LDP a través de un LSP-RSVP.

La Figura 3.13 requiere de una doble operación de asignación de etiqueta (L1, L2) debido a que el enrutador de ingreso (A) es el mismo para los dominios RSVP y LDP. El enrutador D es el penúltimo salto del LSP-LDP de modo que L2 es retirada por éste enrutador.

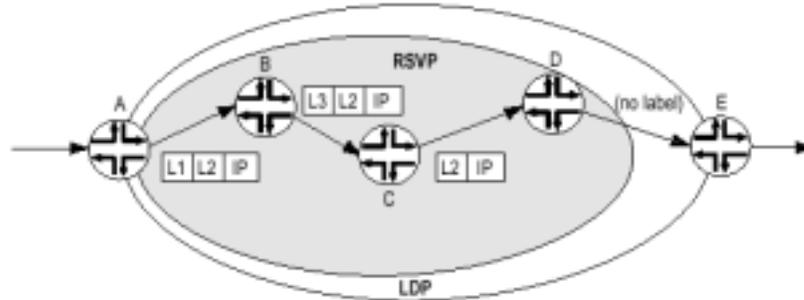


Figura 3.13. LSP-LDP a través de LSP-RSVP con un mismo LER de Entrada.

3.5.4.3 Distribución de etiquetas usando CR-LDP

CR-LDP es un conjunto de extensiones de LDP diseñado específicamente para facilitar el enrutamiento restringido de los LSPs. Al igual que LDP, en CR-LDP los mensajes de señalización son enviados solo una vez y no es necesario refrescar el estado de la información continuamente, además, se utiliza UDP como mecanismo de transporte de los mensajes de descubrimiento y se usa TCP para el intercambio de los mensajes de sesión, advertencia y notificación, permitiendo una distribución fiable de mensajes de control. CR-LDP se ha diseñado para soportar servicios diferenciados y clases de servicio configurables por el operador. También proporciona capacidades para establecimiento estricto y libre de trayectos, además de reoptimización y establecer de niveles de prioridad de los mismos.

El flujo básico para el establecimiento de un LSP usando CR-LDP se muestra en la Figura 3.14.

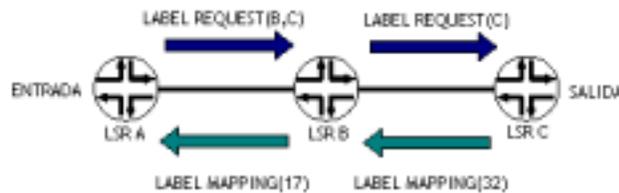


Figura 3.14. Flujo de Establecimiento de un LSP por medio de CR-LDP.

El LSR de ingreso (LSR A) desea establecer un nuevo LSP hacia LSR C, para lo cual construye un mensaje de LABEL_REQUEST con una ruta explícita (B, C) y detalles acerca de los parámetros de tráfico necesarios. LSR A reserva los recursos que necesita para el nuevo LSP y entonces envía el mensaje LABEL_REQUEST a LSR B sobre una sesión TCP.

LSR B recibe el mensaje LABEL_REQUEST y reserva los recursos necesarios para el nuevo LSP, modifica la ruta en el mensaje LABEL_REQUEST y pasa el mensaje a LSR C. Si es necesario, LSR B puede modificar la reserva hecha para el nuevo LSP si los parámetros fueron marcados como negociables en el LABEL_REQUEST.

LSR C realiza cualquier negociación final sobre los recursos, hace la reservación para el nuevo LSP, le asigna una etiqueta y la distribuye hacia LSR B en un mensaje LABEL_MAPPING, el cual contiene los detalles acerca de los parámetros de tráfico finales reservados para el LSP.

LSR B recibe el mensaje LABEL_MAPPING y lo compara con la solicitud original usando el identificador de LSP (LSP ID) contenido tanto en el mensaje LABEL_REQUEST como en el LABEL_MAPPING. El LSR B asigna una etiqueta para el LSP, establece la tabla de envío y pasa la nueva etiqueta al LSR A en un mensaje LABEL_MAPPING. Con LSR A finaliza el proceso del establecimiento del trayecto.

3.5.4.4 Distribución de etiquetas usando BGP

BGP se puede utilizar para distribuir etiquetas MPLS. La información referente a las etiquetas para una ruta particular puede ser llevada en los mismos mensajes de actualización de BGP usando las extensiones multiprotocolo de BGP4 que soportan diferentes familias de direcciones, como IPv4 o IPv6. MPLS simplemente define una nueva familia de direcciones, donde las direcciones incluyen no sólo un prefijo de dirección, sino también una o más etiquetas. El formato de las etiquetas y el prefijo de dirección codificado en BGP se muestra en la Figura 3.15.

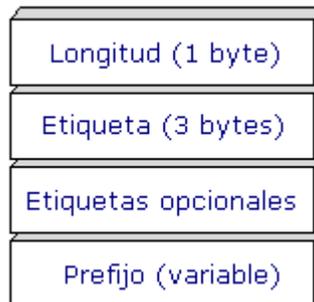


Figura 3.15. Formato de las Etiquetas y el Prefijo de Dirección Codificado en BGP.

El campo de longitud es el número total de bits de la(s) etiqueta(s) mas el prefijo de dirección. Inmediatamente después de la(s) etiqueta(s) se encuentra el prefijo de dirección para el cual la etiqueta (o pila de etiquetas) ha sido asignada. El prefijo puede ser cualquier número largo de bits (mas de 32 para direcciones IPv4).

Con ésta combinación de prefijo de dirección y etiquetas, cualquier dispositivo que soporte BGP podrá también advertir una etiqueta o pila de etiquetas usada por los paquetes que están en esa ruta.

3.5.4.5 *Modos de distribución de etiquetas*

MPLS define el tratamiento que se le dará a la información de asignación de etiquetas recibida desde un LSR que no es el siguiente salto de un FEC dado. Los LSRs tienen la alternativa de mantener un trayecto para tales asignaciones o simplemente podrá descartarlas, a estas alternativas se les conoce con el nombre de modos de retención liberal y conservativo respectivamente.

Cuando un LSR opera en el modo de retención de etiquetas liberal, él mantiene la asignación entre una etiqueta y un FEC que son recibidos desde un LSR que no corresponde al siguiente salto. La principal ventaja de este modo de retención es la respuesta rápida a cambios en el enrutamiento y su desventaja es el alto consumo de etiquetas lo que es particularmente importante para dispositivos que almacenan información de envío de etiquetas en su hardware, como es el caso de los ATM-LSR. Si un LSR opera en el modo de retención de etiqueta conservativo, él descarta tales asignaciones. Este modelo requiere que el LSR mantenga pocas etiquetas y es recomendado en ATM-LSR.

3.5.5 **Unión de Etiquetas**

El proceso por el cual a todos los paquetes de un FEC con etiquetas entrantes diferentes se les asigna una misma etiqueta de salida, se conoce como *unión de etiquetas*. El proceso de *unión de etiquetas* consiste en la capacidad de un LSR de enviar paquetes que provienen de interfaces diferentes y con etiquetas diferentes, por una misma interfaz y con la misma etiqueta de salida, siempre y cuando tengan el mismo destino. Si un LSR no puede ejecutar la *unión de etiquetas*, entonces los paquetes que llegan con etiquetas diferentes, son enviados con etiquetas de salida diferentes.

Como caso particular suponga que existe un LSR que por algún tipo de limitación sólo puede realizar la unión de cuatro etiquetas entrantes en una única etiqueta de salida. Entonces, si llegan 6 etiquetas para ser unidas a un solo FEC, el LSR podría realizar la unión de esas 6 etiquetas entrantes en dos etiquetas de salida.

Usar el proceso de unión de etiquetas reduce al máximo el número de etiquetas que son necesarias para el envío de los paquetes a través de la red, a diferencia de aquellos casos en que las etiquetas son tantas como los enrutadores que se encuentran en el dominio.

3.5.6 **Agregación**

En el dominio MPLS la *agregación* consiste en unir un conjunto de FECs que siguen una misma ruta, en un solo FEC, y a este FEC se le asigna una misma etiqueta. La agregación reduce la cantidad de etiquetas necesarias para la transmisión del paquete y reduce el tráfico de control de distribución de etiquetas.

La asignación se puede realizar a dos niveles de granularidad, granularidad gruesa, en que los FECs son unidos a un sólo FEC, ó dentro de un conjunto de FECs; y la granularidad fina donde no todos los FECs son agregados. En la asignación de etiquetas podría suceder que dos LSR adyacentes no tengan el mismo nivel de granularidad, en cuyo caso el procedimiento sería similar al descrito en la unión de etiquetas.

3.6 ENRUTAMIENTO MPLS

Los LSP se establecen dinámicamente basándose en la información de enrutamiento obtenida por los protocolos y por los resultados de los procesos de asignación y distribución de etiquetas. MPLS especifica tres formas de seleccionar la ruta de un LSP, enrutamiento salto por salto, enrutamiento explícito y enrutamiento restringido.

El enrutamiento salto por salto permite que cada LSR determine el siguiente salto para cada FEC, basándose en su información local de enrutamiento. Este método es usado actualmente en las redes IP. Un LSP cuya ruta ha sido seleccionada usando el enrutamiento salto por salto se le denomina *LSP salto por salto*. Este tipo de enrutamiento no garantiza una reserva adecuada de recursos de acuerdo a las características del tráfico, por lo tanto, MPLS para garantizar una QoS extremo a extremo se adapta al enrutamiento explícito y restringido, explicados en la siguiente sección.

3.6.1 Enrutamiento explícito.

Una ruta explícita es, en términos generales, una secuencia de saltos desde el nodo de entrada al de salida, pero que han sido predeterminados. Con el enrutamiento explícito, el LER de entrada o de salida especifica algunos o todos los LSRs que conforman el LSP. Un LSP que ha sido establecido con enrutamiento explícito se llama LSP Explícito o ER-LSP.

Una ruta Explícita puede clasificarse en "estricta" o "libre". Si un LER especifica todos los nodos e interfaces para el LSP, el LSP es una ruta estricta y debe usar la secuencia de nodos en el orden indicado. En una ruta libre, el LER especifica sólo algunos LSRs del LSP y se debe mantener el orden establecido, si es necesario podrá incluir saltos adicionales para alcanzar los nodos especificados. Una vez una ruta libre ha sido establecida puede modificarse (al igual que una ruta salto por salto) o puede ser configurada de modo que no pueda cambiar.

En el enrutamiento explícito el no es necesario que los paquetes transporten información de la ruta explícita en su cabecera porque ya ha sido especificada en el momento de la creación del LSP. El enrutamiento explícito es más eficiente, facilita la introducción de políticas de enrutamiento, métodos de gestión de red y provee rutas alternas a los LSPs en el caso de que se presenten problemas en la red.

3.6.2 Enrutamiento Restringido

La ruta de un LSP puede restringirse por muchos requerimientos establecidos en el LSR de entrada. Una Ruta Explícita es un ejemplo de una ruta restringida donde la restricción es el orden en el cual debe alcanzarse un LSR. Otras restricciones pueden imponerse por las características del tráfico transportado e incluyen ancho de banda, retardo, cantidad de recursos y prioridad.

Un LSR de entrada puede calcular completamente la ruta, basándose en las restricciones y la información que tiene acerca del estado actual de la red, con el fin de producir una ruta explícita que satisfaga las restricciones. Alternativamente, el enrutamiento restringido permite realizar una variación en el enrutamiento convencional, donde cada LSR determina el próximo salto usando información local acerca de la disponibilidad de los recursos.

3.7 CONTROL DE ESTABLECIMIENTO DE LSPs

Los FECs que corresponden a prefijos de direcciones son distribuidos por medio de un algoritmo de enrutamiento dinámico. El establecimiento del LSP por el cual viajarán estos FECs se realiza con técnicas de control LSP independiente u ordenado.

En la técnica de control independiente, un LSR reconoce a un FEC particular y toma sus propias decisiones para asignar una etiqueta a ese FEC, para después distribuir y advertir de la asignación a sus vecinos. Es muy similar al proceso de enrutamiento de datagramas IP, en el cual los nodos determinan la manera de tratar cada paquete de forma independiente, pero requiere de algoritmos para adaptar rápidamente el enrutamiento a cambios en la red y así asegurar la entrega correcta de cada datagrama.

En el control LSP ordenado, un LSR sólo asigna una etiqueta a un FEC si él es un LER de salida para ese FEC o si ha recibido una asignación para ese FEC desde su siguiente salto. Bajo el control ordenado, el establecimiento de un LSP puede ser iniciado desde su entrada o desde su salida, de esta manera, el proceso de asignación de etiquetas es ordenado desde la entrada a la salida o viceversa. El control ordenado asegura que el tráfico en un FEC siga un trayecto con propiedades específicas, como por ejemplo, una cantidad determinada de recursos, o un tráfico que no atraviese un nodo 2 veces, ayudando a proveer capacidades de prevención de bucles. Un ejemplo de este proceso se muestra en la Figura 3.16. En la Figura 3.16, el nodo E ha identificado que él es la salida para un prefijo de dirección 192.69/16, para el cual tiene una ruta directa. E asigna una etiqueta para ese FEC (6) y advierte de tal asignación a su único vecino, el nodo D. Al recibir el anuncio (Figura 3.17), D asigna una etiqueta (8) y lo anuncia a sus vecinos A y C. De esta manera el establecimiento del LSP se hace de forma ordenada desde la salida hacia la entrada.

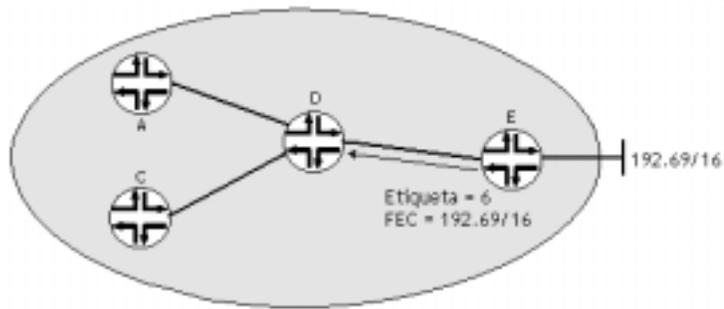


Figura 3.16. Establecimiento LSP Ordenado (Parte A).

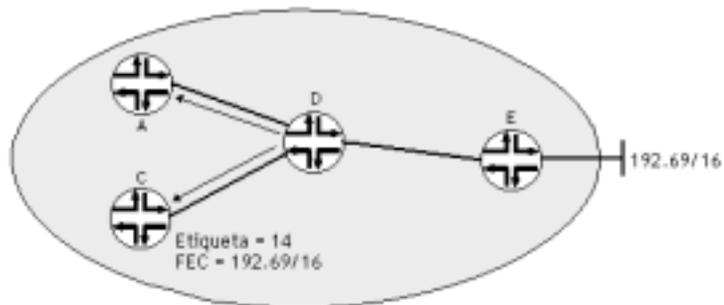


Figura 3.17. Establecimiento LSP Ordenado (Parte B).

La arquitectura MPLS permite elegir entre estas dos técnicas, porque ambas ofrecen sus propias ventajas y desventajas. La elección de cualquiera de ellas afecta la forma en que los FECs son seleccionados para asignar las etiquetas. Con el control independiente, cada LSR toma su propia decisión sobre cómo dividir un conjunto de paquetes dentro de un FEC; por ejemplo, podría decidir que cada prefijo de su tabla de enrutamiento sea representado por un FEC. Si los LSRs toman decisiones diferentes sobre un FEC no es posible establecer el LSP. En el control ordenado, la selección la hace el LER de entrada y todos los LSRs a lo largo del LSP usan el mismo FEC que eligió el LER, pero es necesario que los LSRs puedan determinar el siguiente salto para asegurar que la información sea recibida desde el LSR correcto.

De otro lado, en el control ordenado hay un incremento en el tiempo que toma establecer un LSP. En general, se requiere propagar la asignación a todos los LSRs antes de establecer el LSP. Durante este periodo, los paquetes pueden entrar en un estado de espera o ser descartados, a diferencia de lo que ocurre con el control independiente que permite a todos los LSRs establecer y advertir de la asignación de etiquetas sin mayores retardos (por la espera de mensajes propagados desde un extremo de la red a otro). Además, el hecho que los LSRs puedan recordar la asignación de sus vecinos (que no son el siguiente salto) permite el establecimiento rápido de nuevos LSPs cuando ocurren cambios en el enrutamiento.

3.8 FUNCIONAMIENTO GLOBAL DE MPLS

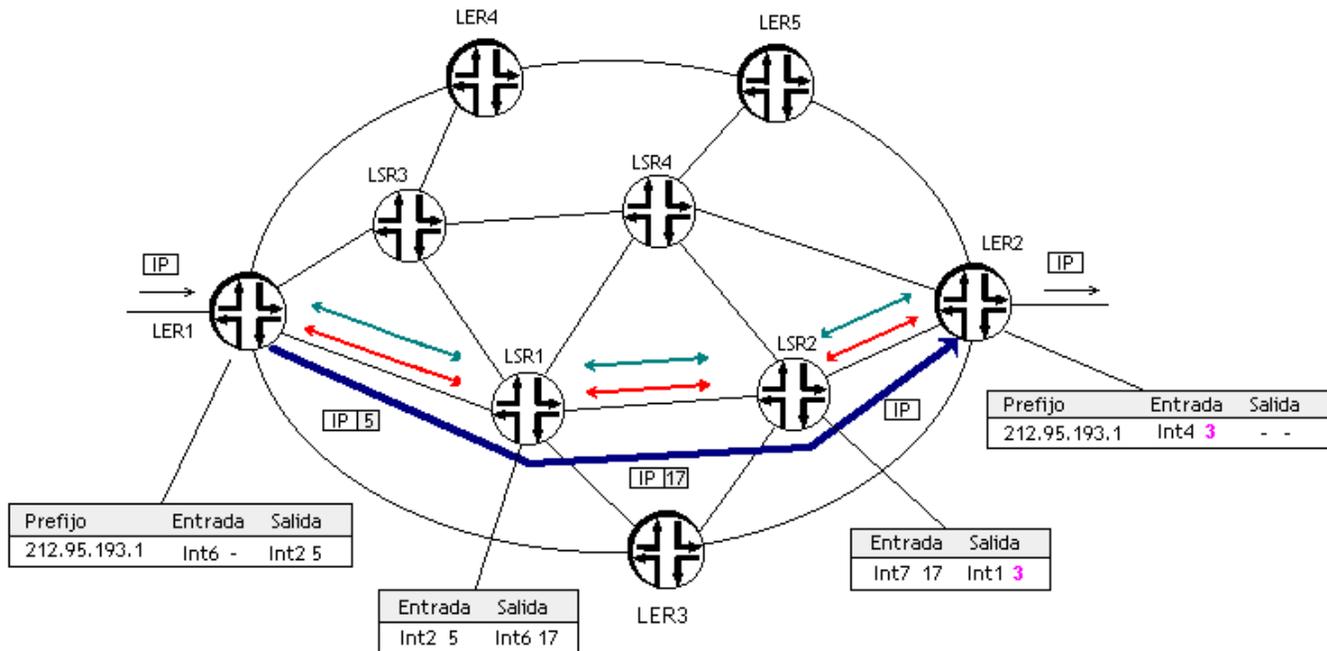


Figura 3.18. Funcionamiento MPLS.

Después de estudiar todos los conceptos generales involucrados en la tecnología MPLS se describe el esquema global de funcionamiento para el transporte del tráfico desde la fuente al destino, tomando como ejemplo la red que se muestra en la Figura 3.18, la cual funciona sobre la tecnología Ethernet.

En un dominio MPLS, antes de iniciar el envío de datos, es necesario que cada uno de los LSRs conozca la topología de la red por medio de algún protocolo de enrutamiento (OSPF, IS-IS, CR, RIP, etc.), con el fin de generar sus tablas de envío y así determinar la forma de alcanzar sus redes destino.

Cuando un paquete IP cuya dirección destino es 212.95.193.1 ingresa al dominio MPLS, el LER de entrada (LER1) analiza la cabecera IP y consulta su tabla de enrutamiento. En base a los resultados de ésta consulta, el paquete se clasifica dentro de un FEC (correspondiente al prefijo de dirección IP) y se le asigna una etiqueta (5) que a su vez identifica el LSP (previamente establecido por algún protocolo de señalización) por medio del cual cruzará el dominio MPLS. Los otros campos de la cabecera MPLS son obtenidos de la información de la cabecera del paquete IP entrante.

El LSR1 recibe el paquete etiquetado, analiza el valor de la etiqueta y la utiliza como índice para consultar en la tabla de envío la interfaz de salida y el nuevo valor de etiqueta (17). El

LSR1 reduce en 1 el valor TTL. Si éste valor es cero el paquete se descarta, sino se envía al siguiente salto con el nuevo valor de etiqueta.

El LSR2 recibe el paquete, analiza el valor de la etiqueta, consulta la tabla de envío y determina que él es el penúltimo salto, por lo cual remueve la etiqueta y envía el paquete al LER de salida (LER2).

El LER2 recibe el paquete, lo analiza y después de consultar la tabla de envío se da cuenta que él es el LER de salida para ese LSP, procede a remover la etiqueta del paquete (si la hay) y lo enruta a su destino usando los protocolos de enrutamiento convencionales.

3.9 APLICACIONES

Debido a las características de MPLS, existen muchos campos de aplicación en los cuales ésta tecnología ha demostrado ser la mejor opción para solucionar los diferentes tipos de problemas que se presentan en cada una de las áreas en que MPLS actúa. A continuación se exponen de forma general, los principales campos de acción de MPLS.

3.9.1 Redes Privadas Virtuales (VPN - Virtual Private Network)

Una VPN es una infraestructura creada para ofrecer servicios a usuarios geográficamente dispersos con funcionalidades equivalentes a las prestadas por una red privada, pero sobre una red pública. Los servicios de las redes privadas virtuales representan una fuente de nuevos ingresos para los proveedores de servicios y una opción de conectividad más económica para cualquier tipo de empresa u organización. Las VPNs se basan en modelos superpuestos donde la conectividad se brinda por medio de circuitos virtuales extremo a extremo. Estas soluciones traen consigo desventajas como la poca flexibilidad en la previsión y gestión de la red, así como problemas de escalabilidad al añadir nuevos circuitos virtuales. Con MPLS se ofrecen servicios de VPN fiables, gestionables y escalables.

El modelo de MPLS se acopla a las características de la red solucionando los problemas de las VPNs actuales. En MPLS, en lugar de conexiones dedicadas extremo a extremo entre cada uno de los nodos, establece enlaces a una "nube común" en la cual solamente pueden ingresar los miembros de dicha VPN. Las nubes se implementan por medio de los LSPs garantizando la reserva del ancho de banda para ofrecer servicios con una QoS apropiada. Además los LERs son reforzados para soportar múltiples dominios de enrutamiento basándose en la tecnología "enrutador virtual" que resuelve los problemas de direcciones privadas soportando múltiples tablas de envío, una para cada VPN. Las tablas se usan para guardar de forma separada los espacios de direcciones de cada empresa.

Las principales ventajas que trae MPLS en la implementación de VPNs son la clasificación de los flujos de tráfico dependiendo de la Clase de Servicio, y la QoS extremo a extremo proveída

por medio del enrutamiento explícito que aprovecha las ventajas de la ingeniería de tráfico de responder globalmente a parámetros críticos para la prestación del servicio.

3.9.2 Ingeniería de Tráfico

La aplicación inicial y más importante de MPLS es la ingeniería de tráfico cuyo objetivo básico es adaptar los flujos de tráfico a los recursos físicos de la red. En general, MPLS ofrece una solución más eficiente, que permite desviar el tráfico fuera de los puntos congestionados, y asegura que los flujos críticos (con requerimientos de QoS específicos) siempre van a tener un camino, gracias a los mecanismos de control que permiten al administrador de la red el establecimiento de rutas explícitas especificando el camino físico exacto de un LSP. Con los mecanismos de control se pueden obtener estadísticas de uso de los LSPs, que se utilizan en la planificación de la red y como herramientas de análisis de cuellos de botella y carga en los enlaces, lo que resulta bastante útil para planes de expansión futura.

La ventaja de la ingeniería de tráfico MPLS es que se puede hacer directamente sobre una red IP, al margen de que haya o no una infraestructura ATM subyacente, todo ello de manera más flexible y con menores costos de planificación y gestión para el administrador, y con mayor calidad de servicio para los clientes.

3.9.3 Calidad de Servicio QoS

Con el crecimiento en la demanda, las redes actuales enfrentan problemas de bajo rendimiento y confiabilidad, conduciendo a que los proveedores ofrezcan a sus clientes determinados grados de servicio, sin la posibilidad de proporcionar aplicaciones en tiempo real. En estas redes es casi imposible garantizar la QoS porque la decisión de encaminamiento es efectuada salto por salto con modelos de "mejor esfuerzo", en donde los dispositivos hacen lo necesario para entregar el tráfico a su destino, sin tener en cuenta el tipo de tráfico que transportan, los requerimientos de ancho de banda, límites y variaciones de los retardos, etc. Con MPLS los proveedores entregan servicios IP con un rendimiento predecible. MPLS asigna QoS a un flujo de paquetes de manera que cuando éstos atraviesen la red sean manipulados de forma específica. Para lograrlo, clasifica los paquetes en FECs teniendo en cuenta la clase de servicio y determinando así los recursos necesarios para su transporte. Los proveedores podrán entonces ofrecer servicios de nivel QoS "absoluto" para voz y video en tiempo real y podrán seguir ofreciendo los niveles de "Mejor esfuerzo".

Los principales beneficios de la aplicación de mecanismos de QoS son los siguientes:

- Asignación eficiente de los recursos, con la ayuda de protocolos diseñados para este fin. No es necesario configurar caminos virtuales para cada clase de servicio, lo cual beneficia principalmente la aplicación de VPNs en MPLS, ya que los métodos tradicionales requieren la configuración de circuitos virtuales extremo a extremo separados para cada clase de servicio de cada una de las VPNs.

- Flexibilidad. MPLS usa eficientemente el ancho de banda y no requiere de procedimientos de establecimiento puesto que la asignación de los recursos se realiza antes de la iniciación del servicio.

3.9.4 Redes Ópticas

Con el crecimiento de las redes ópticas y la Multiplexación por División de Onda (DWDM - Dense Wavelength Division Multiplexing), se pretende adaptar MPLS a este tipo de ambientes y para ello se está creando una versión para el dominio óptico: MPLS Generalizado (GMPLS - Generalized MPLS). Los canales ópticos son similares a los LSP y los OXCs (Optical Cross-Connect) similares a los LSRs. Al igual que los LSRs, los OXCs necesitan de protocolos de enrutamiento como OSPF e IS-IS para intercambiar información referente a la topología, el estado de los enlaces y la disponibilidad de los recursos para el cálculo de los trayectos. Similarmente, se necesitan de protocolos de señalización como RSVP y LDP para automatizar el proceso de configuración de los OXCs y realizar el establecimiento de los trayectos ópticos.

El objetivo de GMPLS es proporcionar un plano de control a los OXCs con la habilidad de establecer canales ópticos, que soporte capacidades de ingeniería de tráfico y mecanismos de restauración y protección, a la vez que simplifica la interconexión entre los dispositivos ópticos y los enrutadores de etiquetas en el dominio MPLS. GMPLS ofrece ventajas como la rápida implantación de servicios, la eliminación de niveles de red innecesarios y el ahorro de costos en las operaciones de red debido a la utilización de una amplia variedad de herramientas de gestión de IP.

Aunque aun se requieren de algunas modificaciones a los protocolos de señalización y enrutamiento de MPLS para adaptarse a las características de las redes ópticas, GMPLS se está convirtiendo rápidamente en una opción que promete una solución extremo a extremo rápida y de bajo costo para los ISPs.

3.9.5 Voz sobre IP con MPLS

El interés básico del desarrollo de tecnologías de Voz sobre IP (VoIP), gira entorno a la integración de las comunicaciones de voz y datos en una misma red, brindando la posibilidad de realizar llamadas telefónicas a larga distancia sin recargos adicionales. Las corporaciones podrán disminuir los costos y gestionar los recursos más eficientemente mediante el uso de programas especializados para el control de los sistemas telefónicos. La Integración de las tecnologías existentes como las redes basadas en IP y la Red Telefónica Pública Conmutada (PSTN - Public Switched Telephone Network) son piezas claves para la transición a un nuevo sistema de comunicaciones.

VoIP necesita de la seguridad y QoS proporcionada por las VPNs para alcanzar las necesidades de los usuarios finales. En el pasado, la latencia fue el mayor problema de VoIP usando VPNs

debido al gran tamaño de las cabeceras de los paquetes IP que circulaban por la red. MPLS disminuye el tamaño de las cabeceras de los paquetes y el tiempo de procesamiento en los dispositivos intermedios. Voz sobre MPLS (VoMPLS) proveerá un medio más eficiente para transportar voz en paquetes ya que asigna una pequeña etiqueta a la cabecera sin necesidad de adicionar grandes cantidades de instrucciones especiales para su correcto manejo, a diferencia de los métodos convencionales en los que se utiliza la encriptación de los paquetes y procesos especializados para garantizar la QoS adecuada.

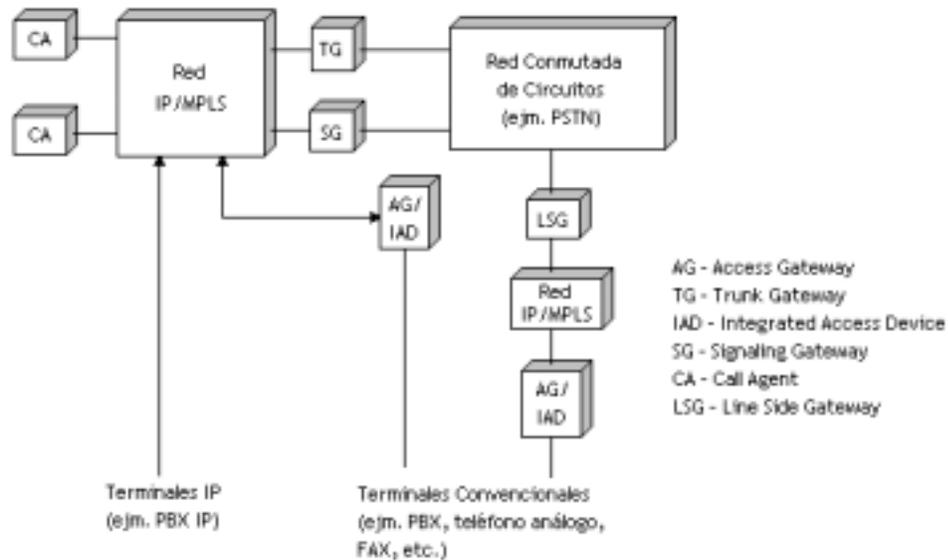


Figura 3.19. Modelo de Referencia de VoMPLS.

El modelo de referencia para VoMPLS (figura 19) consta de dos componentes: el Agente de Llamada (CA - Call Agent) y la Pasarela de Comunicaciones (MG - Media Gateway). En este modelo las funciones de control se encuentran separadas del manejo del flujo de los paquetes de voz. CA y MG pueden localizarse en la misma pieza hardware o en dispositivos separados y usar protocolos específicos para comunicarse.

Los CAs son responsables del control de conexión del MG, del procesamiento de llamadas y otras funciones de gestión. El CA puede controlar el estado de los recursos de los MGs. Es su responsabilidad activar y desactivar los componentes de VoMPLS en el caso de que un elemento de red falle o se presente una congestión severa. Un CA tiene control exclusivo sobre uno o varios MGs, instruyéndolos para que inicien o terminen conexiones con otros MGs.

El MG es una interfaz entre la red de paquetes IP/MPLS y las redes PSTN/ISDN/GSM y actúa como un adaptador para los formatos codificados de voz y fax; es el responsable de convertir la voz (u otros tipos de flujos similares) en flujos de paquetes. Un MG de VoMPLS es el responsable del control lógico de la conexión, la interfaz del agente de llamada y la paquetización/despaquetización de los flujos. El MG actúa como punto final de señalización

de MPLS con la capacidad de establecer LSPs y la responsabilidad de etiquetar/desetiquetar los paquetes de voz.

Una Pasarela de Señalización (SG - Signaling Gateway) debe proveer una interfaz para la información de conexión de llamada entre la red VoMPLS y las redes PSTN/ISDN/GSM. El SG es el esclavo en una relación maestro/esclavo con respecto al CA. El SG está asociado con un conjunto de MGs.

Existen diferentes tipos de dispositivos en una estructura VoMPLS. La Pasarela de Troncales (TG - Trunk Gateway) es un dispositivo de gran capacidad que conecta una red PSTN a una red VoMPLS. Una Pasarela de Acceso (AG - Access Gateway) existe sobre la frontera de la red MPLS y conecta un pequeño número de circuitos subscriptores a la red VoMPLS. Las PBXs se conectan por medio de los AGs. La línea del lado de la pasarela (LSG - Line Side Gateway) permitirá a los usuarios tener acceso al conmutador de Oficina Central en el área cubierta por la red MPLS. Con un Dispositivos de Acceso Integrado (IAD - Integrated Access Device) un diseñador de red puede conectar simultáneamente una red MPLS que transporta voz y datos, una PBX y una red Ethernet local.

Los terminales de voz pueden conectarse directamente a un IAD o a un AG, pero alternativamente también pueden conectarse por medio de una PBX de IP, un adaptador de puerto o una PBX convencional utilizando el gateway adecuado. Un PC puede conectarse directamente a la red usando VoMPLS, o un terminal de voz podría conectarse por medio de un terminal IPPhone o H.323 (dispositivos con una interfaz de red nativa).

El uso de Internet para el transporte de voz ha tenido un lento desarrollo, sin embargo se han alcanzado importantes desarrollos software y hardware en ésta área. VoMPLS es un paso en la evolución de las comunicaciones de voz sobre redes de paquetes.

4. INGENIERÍA DE TRÁFICO CON MPLS

Los recientes desarrollos en MPLS abren nuevas posibilidades para solucionar y/o simplificar las limitaciones de los sistemas IP concernientes a la ingeniería de tráfico. MPLS introduce una nueva arquitectura para el manejo del tráfico, que consiste en la separación funcional de los componentes de envío y control. El objetivo de esta arquitectura es incrementar las capacidades de enrutamiento que faciliten a los administradores el establecimiento de rutas explícitas y permitan asociar las clases de tráfico a troncales con atributos específicos para asegurar la reservación de los recursos en la red.

El IETF ha querido ir más allá y ha formado una arquitectura de ingeniería de tráfico capaz de proporcionar servicios agregados con altos niveles de QoS, por medio de la integración de MPLS con el modelo de servicios diferenciados y el enrutamiento restringido. Esta arquitectura de ingeniería de tráfico con MPLS incrementa la escalabilidad de la red, simplifica la integración de servicios, ofrece recuperación de fallas, prevención de bucles y gestión flexible a menores costos y con mayor QoS para los usuarios finales.

En este capítulo se describen con detalle los componentes, los requerimientos y las funcionalidades (recuperación de fallas, control de bucles, etc.) de la ingeniería de tráfico con MPLS.

4.1 CONCEPTOS GENERALES DE MPLS EN LA TE

La Ingeniería de tráfico es un proceso interactivo de planeación y optimización, cuyo propósito es utilizar eficientemente los recursos e incrementar el desempeño de la red. Las funciones de planeación mejoran de forma sistemática la arquitectura (topología y capacidad de enlace) convirtiéndola en un sistema más robusto, adaptativo y fácil de operar. Las funciones de optimización controlan el encaminamiento y distribución del tráfico sobre la topología física existente para evitar y/o mitigar la congestión y asegurar la entrega del servicio a los usuarios finales.

La optimización es una función indispensable, pues la ocurrencia de incidentes aleatorios (cortes de fibra o cambios en la demanda del tráfico) causan congestión y otros problemas que se manifiestan en la operación de la red, independiente de su buen diseño. El problema se incrementa con el uso de protocolos de enrutamiento dinámico (OSPF, IS-IS), los cuales siempre seleccionan el trayecto más corto para enviar los paquetes y no permiten la distribución equitativa del flujo; si el tráfico excede la capacidad del trayecto provocará una

congestión a la vez que otros trayectos más largos son subutilizados. En principio, éste inconveniente fue solucionado con la implementación de ECMP que distribuye la carga por varios trayectos de igual costo, pero si existe sólo un trayecto disponible ó trayectos con diferentes costos, el ECMP no es la mejor solución. En las pequeñas redes, el administrador puede configurar manualmente el costo de los enlaces para distribuir el tráfico uniformemente, pero este proceso no es recomendable en las grandes redes IP.

Como consecuencia de estas limitaciones, el IETF introdujo mecanismos de enrutamiento restringido, extensiones de IGP, protocolos de señalización y principalmente MPLS como herramientas para implementar TE dentro de la red; esta integración se conoce como Ingeniería de Tráfico MPLS (TE-MPLS - Traffic Engineering MPLS). MPLS provee la mayor parte de las funcionalidades proporcionadas por el modelo superpuesto, de una manera integrada y a menor costo que las actuales alternativas, ofreciendo además la posibilidad de automatizar aspectos de la TE. La TE-MPLS establece trayectos predefinidos a través de la red con determinadas características de desempeño (retardo, variación de retardo y ancho de banda) para soportar diferentes tipos o clases de servicios. Los trayectos predefinidos también ayudan a evitar la congestión en ciertos segmentos de red, trasladando el tráfico de una ruta congestionada a otra ruta alterna, distribuyendo el flujo uniformemente a través de los trayectos disponibles, mejorando el servicio y por supuesto incrementando la utilización de los recursos.

La meta principal de TE-MPLS es controlar la distribución del tráfico evitando la congestión e incrementando el desempeño para responder rápidamente a condiciones cambiantes sin afectar su operación. Esta meta se puede alcanzar gracias a que MPLS brinda una serie de facilidades tales como:

- El administrador, a través de acciones manuales o a través de acciones automatizadas por los protocolos subyacentes, puede crear y gestionar fácilmente LSPs explícitos que no están restringidos por el paradigma de envío basado en el destino.
- Las troncales de tráfico son generadas y mapeadas sobre LSPs.
- Una adecuada implementación de MPLS ofrece menor encabezamiento que las alternativas existentes de TE.
- MPLS permite tanto la unión como la separación de tráfico mientras que el enrutamiento clásico basado en la dirección de destino IP permite sólo la unión.
- MPLS define un conjunto de atributos asociados con los recursos de la red que restringen la ubicación de las troncales de tráfico a través de ellos. Esto también puede verse como restricciones a la topología.
- Las troncales de tráfico tienen atributos que les permiten especificar sus características de desempeño.
- Una estructura basada en enrutamiento restringido selecciona los trayectos de las troncales de tráfico sujeto a restricciones. La estructura de enrutamiento restringido no tiene que ser parte de MPLS, sin embargo, las dos necesitan ser altamente compatibles.
- Los atributos de las troncales de tráfico y los recursos, así como los parámetros asociados con el enrutamiento, representan colectivamente las variables de control que pueden ser

modificadas tanto por acciones administrativas como por agentes automatizados, para conducir la red a un estado deseado. En una red operacional, es deseable que estos atributos puedan ser modificados dinámicamente online sin desestabilizar las operaciones de la red.

Adicionalmente, a través de los LSPs, MPLS ofrece una capacidad similar a la conmutación de circuitos superpuesta al actual modelo de enrutamiento en Internet. Muchos de los propósitos existentes para la TE-MPLS se enfocan sólo en la potencialidad para crear LSPs explícitos, pero esta capacidad no es suficiente para la TE, pues se requiere actualizar las políticas para la optimización del desempeño de las grandes redes operacionales.

4.2 COMPONENTES DE TE-MPLS

En las redes IP convencionales, es difícil migrar a nuevas estrategias de enrutamiento, ya que existe un acoplamiento entre los componentes de envío y control que impide realizar cambios en uno de ellos sin modificar el otro, incrementando el tiempo y dinero invertidos. Con MPLS es posible desacoplar estos componentes (Figura 4.1), permitiéndoles ser modificados e implementados independientemente, facilitando la aplicación de nuevos servicios de enrutamiento sin requerir cambios en el paradigma de envío de paquetes. Esta separación permite combinar la escalabilidad y flexibilidad del enrutamiento de nivel 3, con el desempeño, simplicidad y rapidez de la conmutación de nivel 2. El componente de envío es el responsable de transmitir los paquetes a través de los enrutadores de red y el componente de control es responsable de construir y mantener la tabla de enrutamiento.

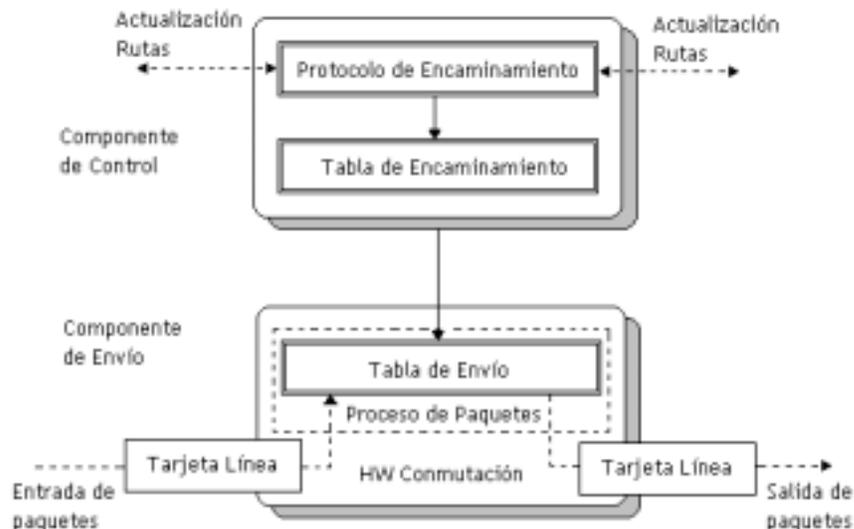


Figura 4.1. Componentes de la TE-MPLS.

Todos los switches y enrutadores desempeñan estas dos funciones ya sean orientados o no orientados a la conexión o usen tramas o celdas. En los enrutadores IP, la función de control

involucra la mayoría de los cálculos de las rutas y usa la información del estado del enlace o vector distancia obtenida por los protocolos de enrutamiento, tales como OSPF o BGP, para actualizar sus tablas de enrutamiento. El envío de tramas es una función a través de la cual, el enrutador simplemente toma cada paquete recibido y basándose en su dirección de destino consulta la tabla de enrutamiento para determinar su "próximo salto".

Así como con los enrutadores IP, los dispositivos MPLS usan protocolos de enrutamiento tales como OSPF o IS-IS para calcular los trayectos de red y su accesibilidad, sin embargo, los LSPs se construyen utilizando los protocolos de señalización CR-LDP o RSVP-TE, los cuales establecen el uso de las etiquetas MPLS a lo largo de cada trayecto. Así como en ATM o Frame Relay, los LSPs son orientados a la conexión y pueden provisionarse manualmente - análogos a los PVCs establecidos por la TE.

En los switches ATM y enrutadores IP, el cálculo y control de los trayectos son independientes del envío, permitiéndoles convertirse en LSRs y convivir en la misma red MPLS, donde un mismo LSP puede transportar flujos basados tanto en celdas como en tramas.

4.2.1 Componente de Control.

Este componente es el responsable de distribuir de manera consistente la información de enrutamiento entre los LSRs y de los procedimientos necesarios para convertir esta información en las tablas de enrutamiento usadas por el componente de envío. Este componente está organizado en módulos que realizan una función de enrutamiento específica, en la Figura 4.2 se observa su organización.

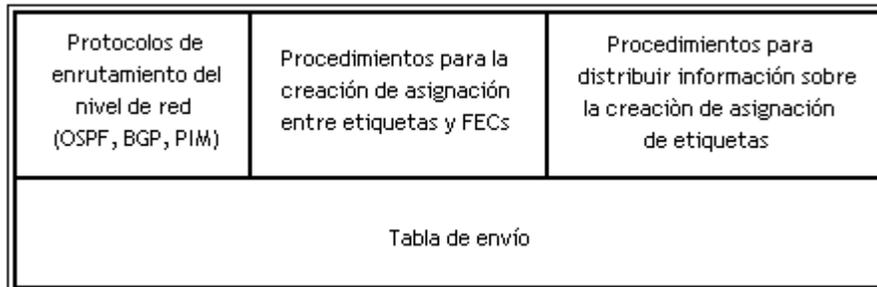


Figura 4.2. Módulos del Componente de Control.

El plano de control está diseñado para trabajar con los protocolos de enrutamiento estándares (OSPF, BGP) y distribuir la información obtenida por estos entre los LSRs. Para llevar a cabo la asignación entre las etiquetas y los FECs usa los mecanismos de Manejo de Datos o Manejo de Información de Control. Finalmente, un LSP no puede utilizarse hasta que sea establecido por el componente de señalización, quien distribuye la información de asignación de etiquetas mediante los protocolos LDP, CR-LDP o RSVP.

4.2.1.1 Módulo de Distribución de Información.

La TE requiere un conocimiento detallado tanto de la topología de red como de la información dinámica acerca de su carga de tráfico obtenida mediante un algoritmo de inundación (usado por los IGPs) que garantiza que los atributos de los enlaces son distribuidos a todos los enrutadores en el dominio. El componente de distribución de información es implementado al definir extensiones para los IGPs de modo que los atributos de los enlaces se incluyen como parte de las advertencias de estado de enlace en cada enrutador; algunos de estos atributos incluyen máximo ancho de banda del enlace, máximo ancho de banda reservable, actual reservación de ancho de banda y otros parámetros asignados al enlace.

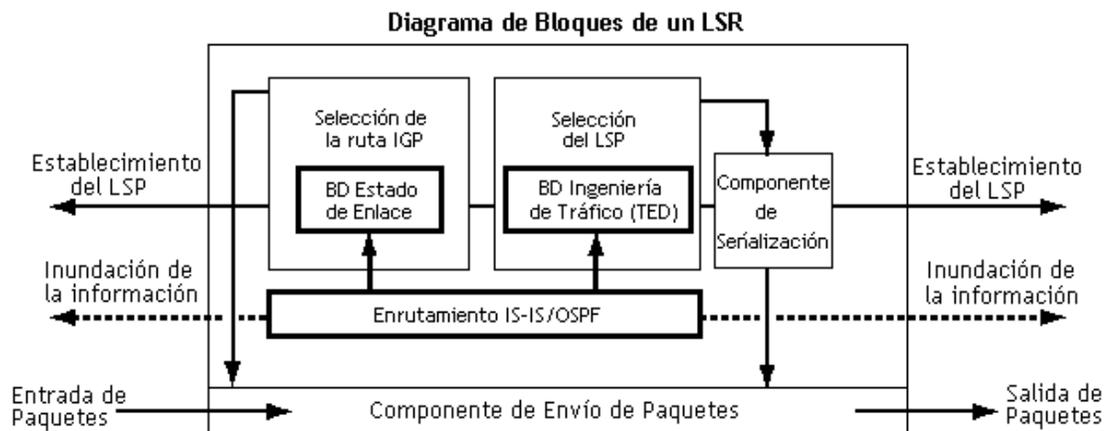


Figura 4.3. Componente de Distribución de Información.

4.2.1.2 Tablas de Enrutamiento.

Cada enrutador mantiene los atributos del enlace e información topológica en una Base de Datos de Ingeniería de Tráfico especializada (TED- Traffic Engineering Database). La TED se usa exclusivamente para calcular los trayectos explícitos y establecer los LSPs a través de la topología física. Se mantiene una base de datos para que el cálculo subsecuente de ingeniería de tráfico sea independiente del IGP y de su base de datos de estado de enlace asociada. Entre tanto, el IGP continúa su operación sin modificación, desempeñando el tradicional cálculo del camino más corto de acuerdo a la información contenida en el enrutador.

Los IGPs y BGP almacenan su información en la tabla de enrutamiento IP principal. Si la ingeniería de tráfico se configura con BGP, solamente él puede usar los trayectos MPLS para el envío de tráfico. La información de los trayectos MPLS se almacena en una tabla de enrutamiento MPLS-BGP donde sólo BGP tiene acceso a ella. BGP usa tanto la tabla de enrutamiento IP como la tabla de enrutamiento MPLS-BGP para resolver las direcciones del próximo salto. Si se configura la TE con BGP-IGP se permite a los IGPs usar las rutas MPLS para el transporte del tráfico y la información de los trayectos MPLS se almacena en la tabla de

enrutamiento IP. (Figuras 4.4 y 4.5 ilustran las tablas de enrutamiento en las dos configuraciones de ingeniería de tráfico).

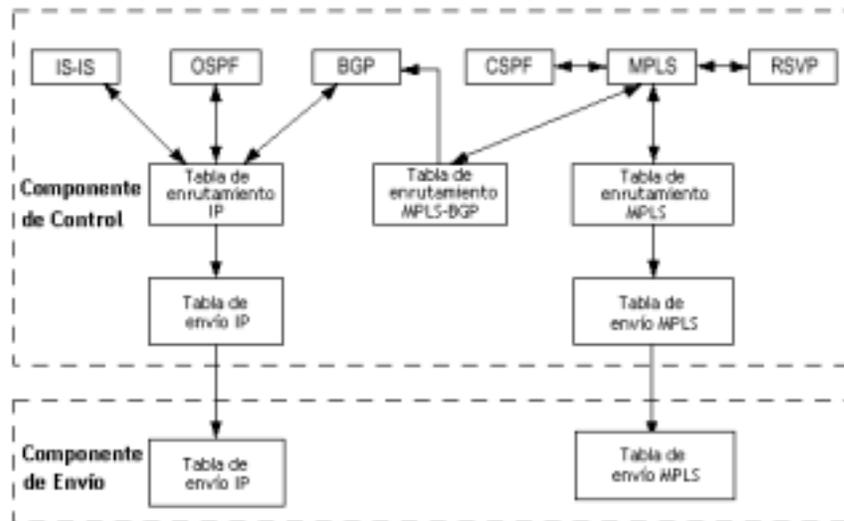


Figura 4.4. Tablas de Enrutamiento y Envío MPLS Cuando se Configura la TE con BGP.

La tabla de enrutamiento MPLS-BGP contiene las direcciones de cada enrutador de salida de los LSPs y se usa para encaminar los paquetes al destino. BGP usa la tabla de enrutamiento MPLS-BGP en el enrutador de entrada para resolver las direcciones del próximo salto.

MPLS también mantiene una tabla de enrutamiento de los trayectos (TED), la cual contiene una lista de los LSRs en cada LSP. Los enrutadores de tránsito usan ésta tabla para dirigir los paquetes al próximo enrutador.

Típicamente, el enrutador de salida en un LSP no consulta la tabla de enrutamiento TED (éste enrutador no necesita consultar dicha tabla debido a que el penúltimo enrutador en el LSP cambia la etiqueta del paquete a un valor 0 o retira la etiqueta). En cada caso, el enrutador de salida envía éste como un paquete IPv4: consulta la tabla de enrutamiento IP y determina cómo enviar el paquete fuera del dominio.

Cuando un enrutador recibe un paquete MPLS, la información en la tabla de envío MPLS indica el próximo enrutador de tránsito en el LSP o determina que este enrutador es el de salida.

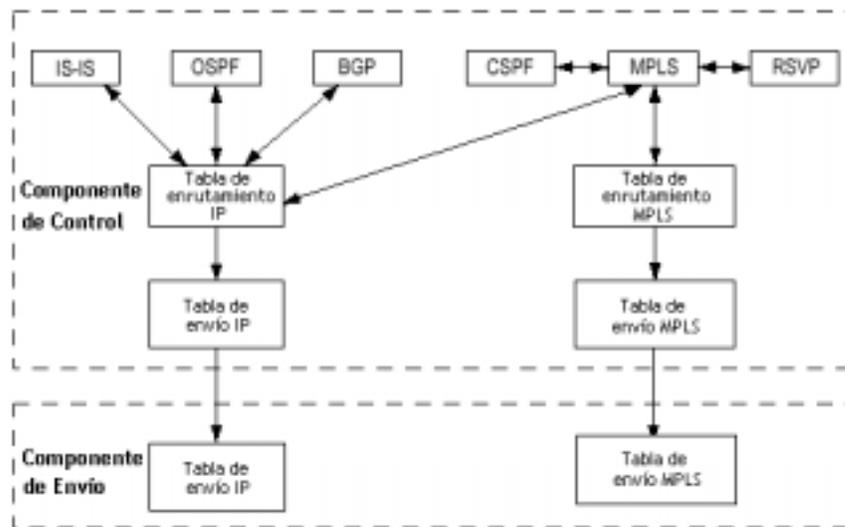


Figura 4.5. Tablas de Enrutamiento y Envío MPLS Cuando se Configura la TE con BGP-IGP.

Cuando BGP busca el prefijo del próximo salto, examina las tablas de enrutamiento IP y MPLS-BGP, y elige aquel que satisface los requerimientos de desempeño y QoS. Si encuentra una entrada para el próximo salto con igual preferencia en ambas tablas, BGP prefiere la entrada encontrada en la tabla MPLS-BGP debido a que sus preferencias son siempre menores que las preferencias del próximo salto de OSPF e IS-IS. Cuando se configuran los LSPs manualmente podría omitirse la preferencia por defecto para los LSPs alterando los procesos de selección del próximo salto.

Cuando BGP selecciona una entrada del próximo salto desde la tabla de enrutamiento MPLS-BGP, almacena ese LSP en la tabla de envío permitiendo que los paquetes destinados para ese próximo salto entren y viajen a lo largo del LSP. Si el LSP es removido o falla, el trayecto es eliminado de la tabla de enrutamiento MPLS-BGP y de la tabla de envío, y BGP usa el próximo salto de la tabla de enrutamiento IP.

4.2.2 Componente de Envío.

Este componente consiste de un conjunto de procedimientos para decidir cómo enviar un paquete a través de una ruta LSP; procedimientos que definen la información y el proceso necesarios para encontrar las entradas en la tabla de enrutamiento. Es responsabilidad de este componente transmitir los paquetes por medio del algoritmo de intercambio de etiquetas, y según la información de la tabla de enrutamiento y la contenida en los paquetes etiquetados.

El componente de envío soporta múltiples protocolos de nivel de red y de nivel de enlace y es implementado en hardware para obtener mayor velocidad, sencillez y eficiencia.

4.2.2.1 Selección de Trayectos.

Después que los atributos del enlace y la información topológica son distribuidos por el IGP y colocados en la TED, cada LER de entrada usa la TED para calcular las rutas de su propio conjunto de LSPs a través del dominio de enrutamiento. La ruta de cada LSP puede representarse de forma explícita (libre o estricta). Una ruta explícita es una secuencia preconfigurada de LSRs que deberán ser parte del trayecto físico del LSP, si el LER de entrada especifica todos los LSRs en el LSP, se dice que el LSP tiene una ruta explícita estricta; sin embargo, si el LER de entrada determina solamente algunos de los LSRs, se dice que el LSP tiene una ruta explícita libre (Figura 4.6). El soporte para rutas explícitas estrictas y libres permite al proceso de selección de trayectos ser flexible cuando es posible, pero limitado cuando es necesario.

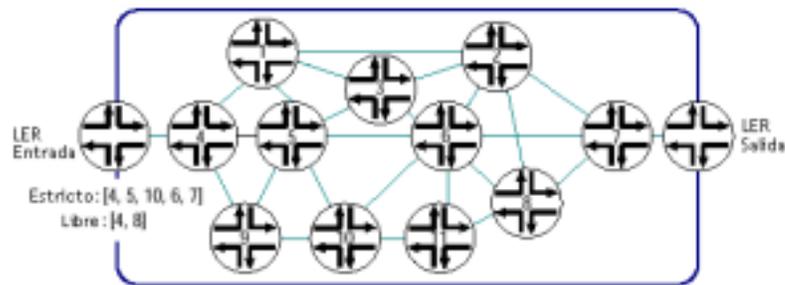


Figura 4.6. Cálculo de Rutas Explícitas en el LER de Entrada.

El LER de entrada determina el trayecto físico para cada LSP aplicando un algoritmo del Trayecto mas Corto Restringido (CSPF - Constraint Shortest Path First) a la información en la TED (Figura 4.7). CSPF es un algoritmo del trayecto más corto modificado para tomar en cuenta restricciones específicas cuando se calcula el trayecto a través de la red. Las entradas en el algoritmo CSPF incluyen:

- Información topológica del estado de los enlaces obtenida por el IGP y mantenida en la TED.
- Atributos asociados con el estado de los recursos de la red (ancho de banda total del enlace, ancho de banda reservable, ancho de banda disponible en el enlace, y otros parámetros asignados al enlace) que son transportados por las extensiones del IGP y almacenados en la TED.
- Atributos administrativos necesarios para el control del tráfico a través del LSP (requerimientos de ancho de banda, máximo conteo de saltos, y requerimientos de políticas administrativas) obtenidos desde la configuración de usuario.



Figura 4.7. Componente de Selección de Trayectos.

Como CSPF considera cada nodo y enlace como candidatos para un nuevo LSP, éste acepta o rechaza un componente de trayecto específico según la disponibilidad de los recursos y las políticas de restricciones del usuario. El resultado del proceso de CSPF es una ruta explícita, que cumple con los requerimientos y consiste de una secuencia de direcciones de LSRs que proveen el trayecto mas corto a través de la red. Este trayecto explícito es entonces pasado al componente de señalización, quien finalmente establece el LSP. El algoritmo CSPF se repite cada vez que el LER de entrada requiera generar un nuevo LSP.

4.2.2.2 *Análisis y Planeación Offline.*

A pesar que el cálculo de trayectos online facilita la gestión, se requiere una herramienta de análisis y planeación offline para optimizar la ingeniería de tráfico globalmente. El cálculo online toma en cuenta las restricciones de los recursos y calcula un LSP a la vez. El orden en el cual se calculan los LSPs juega un rol crítico en la determinación de los trayectos físicos a través de la red. Los LSPs calculados al principio del proceso tienen más recursos disponibles que aquellos LSPs que son calculados posteriormente, pues los primeros consumen los recursos de la red. Si el orden en el cual se calculan los LSPs cambia, el conjunto de trayectos físicos resultante también cambia.

Una herramienta de análisis y planeación offline examina simultáneamente las restricciones de los recursos de cada enlace y los requerimientos de los LSPs, tomando varias horas para realizar cálculos globales, comparar estos resultados y seleccionar la mejor solución global para la red. El resultado es un conjunto de LSPs que optimiza la utilización de los recursos. Después de realizar el cálculo offline, los LSPs pueden establecerse en cualquier orden debido a que cada uno es determinado siguiendo las reglas para la optimización global.

4.3 TRONCALES DE TRÁFICO

Un concepto básico para implementar TE en redes MPLS es la troncal de tráfico, formada por un conjunto de flujos unidireccionales que pertenecen a la misma clase y que siguen un mismo LSP. Esencialmente, una troncal es una representación abstracta de tráfico tratada como un

objeto enrutable, es decir, el trayecto a través del cual el tráfico está circulando puede modificarse. Las troncales de tráfico son similares a los Circuitos Virtuales en ATM y FR.

Las propiedades básicas de las troncales de tráfico son:

- Una troncal de tráfico es un conjunto de flujos pertenecientes a una misma clase. En algunos contextos, puede ampliarse esta definición y permitir a las troncales incluir grupos de tráfico multiclase.
- En un modelo de servicios de clase simple, tal como Internet, una troncal puede encapsular todo el tráfico entre un LER de entrada y uno de salida, o subconjuntos del mismo.
- Una troncal de tráfico es distinta del LSP que atraviesa. En un contexto operacional, una troncal puede cambiar de un trayecto a otro.
- Una troncal de tráfico es unidireccional.

En la práctica, una troncal puede caracterizarse por sus LERs de entrada y salida, el FEC que es mapeado sobre ella, y un conjunto de atributos que determinan sus características de comportamiento.

4.3.1 Troncales de Tráfico Bidireccionales.

Aunque las troncales de tráfico son conceptualmente unidireccionales, en muchos contextos prácticos, es útil crear dos troncales con los mismos extremos para transportar paquetes en direcciones opuestas. Las dos troncales son acopladas de forma lógica la una con la otra. Una de ellas, conocida como troncal de envío transporta el tráfico desde el nodo de origen al de destino, y la otra, conocida como troncal de regreso, transporta el tráfico desde el nodo de destino al de origen. Las Troncales de Tráfico Bidireccionales (BTT - Bidirectional Traffic Trunk) deben cumplir con:

Ambas troncales son instanciadas en un mismo LER conocido como nodo de origen, o en una estación de gestión de red.

- Ninguna de las dos troncales de tráfico puede existir sin la otra, esto significa que ambas son instanciadas y destruidas juntas.

4.3.2 Operaciones Básicas Sobre las Troncales de Tráfico.

Las operaciones básicas sobre las troncales de tráfico que son de importancia para la TE son las siguientes:

- Establecimiento: Crea una troncal de tráfico.
- Activación: Causa que una troncal inicie con el transporte del flujo de datos. El establecimiento y activación de las troncales son eventos lógicamente separados.
- Desactivación: Causa que una troncal de tráfico detenga el transporte del flujo de datos.

- Modificación de los atributos: Modifica los atributos de una troncal de tráfico.
- Reenrutamiento: Causa que una troncal cambie su ruta. Esto se realiza a través de acciones administrativas o automáticamente por los protocolos subyacentes.
- Destrucción: Remueve una instancia de una troncal de tráfico y recupera todos los recursos asignados a ella, tales como espacio de etiquetas y ancho de banda.

4.3.3 Atributos Básicos de las Troncales de Tráfico.

Un atributo es un parámetro asignado a una troncal de tráfico que influye en sus características de comportamiento. Los atributos pueden asignarse explícitamente a las troncales a través de una acción administrativa o pueden asignarse implícitamente por los protocolos subyacentes cuando los paquetes se clasifican y mapean en clases equivalentes a la entrada del dominio MPLS. A pesar de la forma en que los atributos fueron originalmente asignados, es posible que sean modificados administrativamente para cumplir con los objetivos de TE.

Los atributos básicos de las troncales de tráfico significantes para la TE son los siguientes:

- Atributos de parámetros de tráfico. Capturan las características de los flujos (o más precisamente los FEC) que se transportan en la troncal. Tales características son la tasa pico, tasa promedio, tamaño de ráfaga permitido, etc. Los parámetros de tráfico son importantes porque indican los requerimientos de recursos de las troncales.
- Selección genérica de trayectos y atributos de mantenimiento. Define reglas para la selección de las rutas tomadas por las troncales de tráfico así como para las rutas alternas.
- Atributos de prioridad. Definen la importancia relativa de la troncal de tráfico ya que determinan el orden en el cual se realiza la selección de trayectos para cada una de ellas.
- Atributos de capacidad de recuperación. Determinan el comportamiento y las políticas de funcionamiento de las troncales bajo condiciones de fallas.
- Atributos de mantenimiento del orden. Determinan las acciones que deben tomar los protocolos subyacentes cuando una troncal excede los umbrales establecidos al momento de su creación.

4.4 ENRUTAMIENTO RESTRINGIDO

El uso de LSPs con RSVP/CR-LDP provee un modelo ideal para el enrutamiento restringido que convierte la TE en un proceso automático, donde el administrador de la red configura las restricciones para el intercambio de tráfico entre los enrutadores, y el LER de entrada determina los trayectos que satisfacen dichas restricciones e inicia los procesos de señalización para el establecimiento de los LSPs.

Los enrutadores con CR calculan automáticamente rutas explícitas para cada troncal de tráfico, satisfaciendo los requerimientos de la demanda expresados en características del

flujo, disponibilidad de los recursos, políticas administrativas e información del estado de la topología; como consecuencia, el enrutamiento restringido no sólo utiliza los trayectos más cortos para distribuir el tráfico, sino que también puede seleccionar trayectos más largos y menos congestionados. En la selección de los trayectos es necesario contar con información de la topología, y para obtenerla el CR trabaja junto con los IGP (OSPF, IS-IS), que deberán incrementar sus funcionalidades para distribuir la nueva información de estado de enlace, ó simplemente, el CR deberá coexistir con los IGP convencionales, como se muestra en la Figura 4.8.

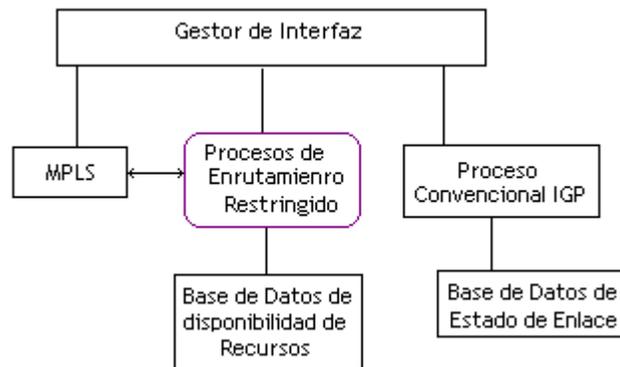


Figura 4.8. Interacción Entre CR e IGP Convencional.

Similares a los mecanismos de TE, los procesos de CR son funcionalmente un problema de control y por tanto requieren de muchos aspectos importantes para su implementación, resumidos en el bucle de control de la Figura 4.9, donde se definen mecanismos para intercambiar información de estado de enlace entre los procesos de CR, y la interacción entre los procesos de CR y de IGP.

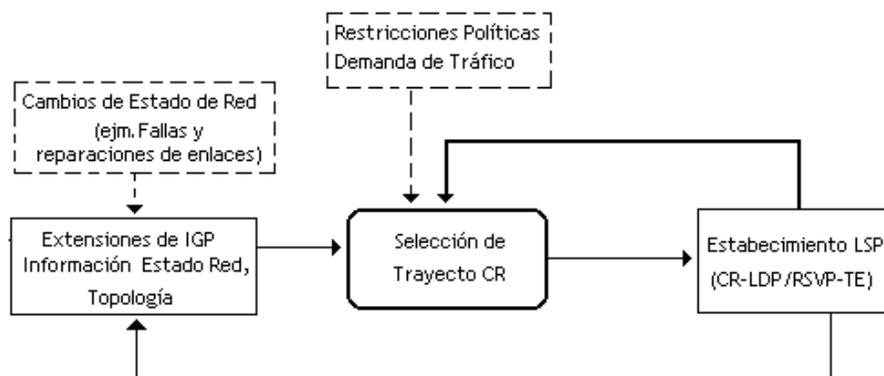


Figura 4.9. Contexto Operacional CR.

El componente IGP es el responsable de recolectar información para construir el mapa topológico de la red y crear una base de datos sobre la disponibilidad de los recursos.

El proceso del CR toma como entradas las características de las troncales, las especificaciones de la ruta (derivado del proceso de clasificación FEC), los atributos de los recursos (derivado del estado de la red IGP) y varias políticas de restricciones para calcular un trayecto (o un conjunto de trayectos) para una troncal determinada.

El protocolo de establecimiento de los LSPs toma como entrada la especificación del trayecto que proviene del proceso del CR e inicia el establecimiento del trayecto. El resultado de esta acción afecta el estado de la red (los recursos son consumidos) y sirve de realimentación en los procesos de CR (el establecimiento del LSP falla y se recalcula).

Estos componentes realizan un constante proceso de realimentación donde las características de uno influyen directamente en el otro. Por ejemplo, los tiempos de respuesta de cada proceso son considerados conjuntamente (tiempo de convergencia IGP, convergencia de CR, tiempo de manejo de troncales). También el tipo y la granularidad de la información pueden estar correlacionadas, es decir, los atributos de los enlaces con los atributos políticos (para IGP) y la granularidad de las troncales de tráfico con las restricciones y propiedades de los LSPs (para CR). Pero lo más importante es la estabilidad de todo el sistema determinada por las características de cada uno de los componentes (resistencia a condiciones transcientes, respuesta a entradas invalidas, etc.).

4.4.1 Métricas para Calcular el Trayecto.

La complejidad de los algoritmos de enrutamiento depende de las restricciones seleccionadas para determinar las rutas. Las métricas más comunes usadas por el CR son el jitter, costos monetarios, ancho de banda, número de saltos, fiabilidad y retardo; éstas métricas se dividen en tres clases definidas así:

“Si $d(i,j)$ es una métrica para el enlace (i,j) , para cualquier trayecto $P = (i, j, k, \dots, l, m)$, la métrica d es:

- *Adaptativa* si : $d(P) = d(i, j) + d(j, k) + \dots + d(l, m)$
- *Multiplicativa* si: $d(P) = d(i, j) * d(j, k) * \dots * d(l, m)$
- *Cóncava* si : $d(P) = \min\{d(i, j), d(j, k), \dots, d(l, m)\}$ ”

De acuerdo a esta definición, el retardo, el jitter, el costo y el número de saltos son métricas adaptativas, la fiabilidad (1 - probabilidad de pérdida) es multiplicativa y el ancho de banda es una métrica cóncava. Cuando los algoritmos de enrutamiento seleccionan rutas óptimas sujetas a restricciones de 2 o más métricas adaptativas y/o multiplicativas se conocen como Algoritmos de Polinomio no Determinístico de Tiempo Completo (NP-Complete - Nondeterministic Polynomia - Time Complete); estos algoritmos generalmente usan la combinación de métricas entre el ancho de banda y alguna de las ya mencionadas (número de saltos, retardo, etc.).

Sin embargo, la prueba de algoritmos no NP-complete se basa en dos suposiciones: todas las métricas son independientes y, el retardo y jitter de un enlace son conocidos a priori. Aunque tales suposiciones pueden ser verdaderas en redes conmutadas de circuitos, las métricas de ancho de banda, retardo y jitter no son independientes en las redes de paquetes, como resultado, los algoritmos polinómicos para calcular las rutas con estas restricciones existen y su complejidad es $O(N * E * e)$, donde N es el número de saltos, E es el número de enlaces, y e ($e \leq E$) es el número de distintos valores de ancho de banda entre todos los enlaces. Sin embargo, el teorema indica que un algoritmo no NP-Complete es muy complejo.

Afortunadamente, los algoritmos para encontrar rutas con restricciones de ancho de banda y número de saltos son muy simples, el más común es el algoritmo Dijkstra. Por ejemplo, para encontrar un trayecto corto entre dos nodos con un ancho de banda superior a 1 Mbps y un número de saltos menor que h , todos los enlaces con ancho de banda menor que 1 Mbps se descartan del árbol, y el algoritmo Dijkstra calcula el trayecto más corto (el proceso de Dijkstra se repite h veces). La complejidad de este algoritmo es $O(N * E)$.

El ancho de banda y el número de saltos son restricciones muy útiles debido a:

1. Las restricciones de ancho de banda permiten a los administradores controlar la utilización del enlace y garantizar niveles de QoS para cada clase de tráfico.
2. Las restricciones de número de saltos indican la cantidad de recursos consumidos por el flujo.
3. Si es necesario, los parámetros de retardo y jitter pueden determinarse por la asignación de ancho de banda y el número de saltos.

En el CR, las rutas son precalculadas para cada clase de tráfico ó calculadas sobre demanda accionadas por la recepción de requisitos de QoS para un flujo. En ambos casos, un enrutador tendrá que actualizar su tabla de enrutamiento con más frecuencia, a causa de los cambios significativos de ancho de banda y parámetros del enlace (aunque no existan cambios en la topología). Por tanto, aunque la complejidad del CR es menor que los algoritmos de enrutamiento dinámico, la carga de los procesos de cálculo en los enrutadores puede ser muy alta.

En la actualidad, la sobrecarga del cálculo de rutas se reduce a través de una serie de aproximaciones como:

- El uso de un contador con tiempo de espera para reducir la frecuencia de cálculo de la tabla de enrutamiento.
- Elección de sólo restricciones de ancho de banda y número de saltos.
- Uso de políticas administrativas para descartar los enlaces no aptos antes de iniciar los cálculos de la tabla de enrutamiento, por ejemplo, si un flujo tiene requerimientos de retardos, los enlaces de altos retardos de propagación, como los satelitales, se descartan antes de iniciar el proceso.

4.4.2 Selección de la Ruta Óptima.

Cuando hay múltiples trayectos que satisfacen las restricciones se usan varios criterios para seleccionar la ruta óptima, eligiendo entre la conservación de los recursos y el balanceo de carga.

Entre las restricciones consideradas en la selección se encuentra la métrica IGP, que es el criterio más significativo para elegir el trayecto más corto a través del cual fluyen los datos. El segundo criterio es el número de saltos: si un flujo atraviesa un trayecto de pocos saltos consume menos ancho de banda y espacio en el buffer. El tercer criterio es el ancho de banda disponible en el trayecto que es el ancho de banda mínimo reservable. De acuerdo a estos criterios, el CR puede elegir cualquiera de las siguientes rutas como el trayecto hacia el destino:

1. Trayecto más corto con ancho de banda más elevado (widest - shortest path): Para elegir este tipo de trayectos, primero se tiene en cuenta que la ruta satisfaga el mínimo número de saltos y posteriormente se verifica que tenga el mayor ancho de banda disponible.
2. Trayecto de ancho de banda más elevado y más corto (Shortest - widest path): Para elegir este trayecto, primero se tiene en cuenta que los enlaces tengan el ancho de banda máximo reservable y posteriormente se verifica que cumpla con un mínimo número de saltos.
3. Trayecto de distancia más corta (Shortest - distance path): como su nombre lo indica, es un trayecto con una distancia corta. La distancia de un trayecto **P** con **K** saltos se define como:

$$Dist(P) = \sum_{i=0}^k \frac{1}{R_i}$$

Donde **R_i** es el ancho de banda del enlace **i**

4. Trayecto alternativo dinámico (Dynamic - alternative path): si **n** es el mínimo de saltos definido para un trayecto, éste es un trayecto widest - shortest path con no más de n+1 saltos.

La primera opción es básicamente la misma del enrutamiento dinámico actual, y se enfatiza en preservar los recursos eligiendo la ruta más corta, su utilización es favorable cuando la carga es muy pesada. La segunda aproximación da prioridad para balancear la carga seleccionando el trayecto que dispone de más ancho de banda, se usa cuando la carga es mediana, y la tercera es una elección entre los dos anteriores.

Estos trayectos son seleccionados con la técnica de filtro secuencial que consiste en realizar combinación de métricas ordenadas según su importancia. Inicialmente, se seleccionan aquellos trayectos que satisfacen la primera métrica y un subconjunto de ellos se descartan basándose en la segunda métrica y así sucesivamente, hasta encontrar uno que satisfaga todas

las restricciones. Por ejemplo, para un trayecto más corto con ancho de banda más elevado, primero el CR identifica los trayectos con un mínimo número de saltos y del conjunto resultante elige aquellos que tengan el mayor ancho de banda.

4.4.3 CR con Restricciones de Retardo y Jitter.

Algunas aplicaciones tienen requerimientos de retardo y jitter, y necesitan algoritmos que seleccionen trayectos que satisfagan dichas restricciones. Estos algoritmos consisten básicamente en convertir las restricciones de retardo y jitter en métricas de ancho de banda y número de saltos. Se define un trayecto P con n saltos para un tráfico que conforma un buffer agujerado $\langle b, r \rangle$ (b longitud del buffer y r la tasa de salida) con un ancho de banda reservado R , retardo D , jitter J y el espacio del buffer B en el salto h :

$$D(P, R, b) = \frac{b}{R} + \frac{nM}{R} + \sum_{i=1}^n \left[\frac{M}{C_i} + i \right] \quad (1)$$

$$J(P, R, b) = \frac{b}{R} + \frac{nM}{R} \quad (2)$$

$$B(P, R, b) = b + hM \quad (3)$$

Donde C_i es la capacidad del enlace (ancho de banda), M el tamaño máximo del paquete e i el retardo de propagación del enlace i .

Si el ancho de banda reservable se conoce, se usa el algoritmo Dijkstra (superior a n saltos) para resolver el problema y su complejidad es $O(N^*E)$, donde E es el número de enlaces en la red.

Sin embargo, si el ancho de banda reservable no es conocido, entonces todos sus posibles valores pueden tenerse en cuenta en el proceso de cálculo. Esto se realiza seleccionando los anchos de banda reservables de todos los enlaces en orden ascendente $r_1 < r_2 < r_3 < r_k \dots < r_e$, $e \leq E$ es el número de los distintos valores de ancho de banda de todos los enlaces de la red. Desde $k=1$ hasta e , se descartan todos los enlaces con ancho de banda menores que r_k , así que la menor cantidad de ancho de banda r_k es reservada para el resto de la red. Después, si hay algún trayecto disponible con un retardo menor que D y con un número de saltos menor que N , el algoritmo Dijkstra podrá encontrar el camino. Si se desea un trayecto con menor retardo, el algoritmo puede ejecutarse e veces (desde $K=1$ hasta e) hasta que el trayecto con el menor retardo sea encontrado. Este algoritmo es llamado Algoritmo Bellman-Ford Iterativo (IBF - Iterative Bellman-Ford) y su complejidad es $O(N^*E*e)$.

Para encontrar un trayecto con requerimientos de retardo y jitter, la restricción del jitter se convierte a restricciones de número de saltos de acuerdo a la fórmula (2). Si el ancho de

banda se conoce, el algoritmo Dijkstra encontrará el trayecto, de otra manera se usa el algoritmo IBF.

Para encontrar trayectos con restricciones de retardo y capacidad de buffer, la restricción de buffer se convierte a número de saltos de acuerdo a la fórmula (3), al igual que en el anterior caso, si el ancho de banda es conocido, se usa el algoritmo Dijkstra para encontrar el trayecto, de otra manera se usa el algoritmo IBF.

4.4.4 CR con Restricciones de Retardo.

Los algoritmos para calcular trayectos con restricción de retardo (tiempo en cola, tiempo de propagación y tiempo de procesamiento) son muy complejos porque el tiempo en cola en cada enrutador no es estático, sin embargo, el tiempo de propagación es una parte significativa del retardo total. Debido a que el tiempo de propagación de un enlace es estático la selección basada en ésta restricción es muy simple. Para calcular los trayectos que cumplan con estas restricciones, primero se usa la métrica del retardo, y posteriormente el algoritmo Dijkstra calcula el trayecto más corto. La métrica puede determinarse a través de la siguiente fórmula:

$$\text{Retardo de propagación} = \text{retardo requerido por la aplicación} - \text{retardo de cola} * \text{número de saltos.}$$

De acuerdo a experiencias obtenidas por los desarrolladores, el valor de tiempo en cola en cada salto se fija en 1 ms, siendo esta una sobre estimación, lo cual asegura que el retardo de propagación suplido por los algoritmos de selección de trayectos es más pequeño que el retardo de propagación tolerable actual.

4.5 BALANCE DE CARGA

La TE establece múltiples LSPs entre dos LERs del dominio y para distribuir el tráfico entre estos trayectos recurre a procesos de balance de carga, que permiten usar de forma equitativa los recursos de red, reduciendo los problemas de congestión. El conjunto de LSPs sobre los cuales la carga se distribuye es predefinido y las políticas son aplicadas a ellos de acuerdo a los requerimientos de desempeño y de QoS.

El proceso de balance de carga es realizado por el LER de entrada del LSP, que actúa como un punto de aplicación de políticas de distribución de estos trayectos y es el encargado de procesar troncales de tráfico que comparten un mismo FEC; bajo este contexto, el problema de balance de carga está relacionado con la selección de las políticas adecuadas para controlar la admisión del flujo a los LSPs. La decisión de admitir un flujo en un LSP se refleja en la relación entre el LSP con el NHFLE dentro de la tabla de enrutamiento apropiada.

Los flujos admitidos en la frontera del dominio se describen por un conjunto de FECs encaminados según la tabla FTN, como consecuencia el balance de carga se considera como la redefinición del FEC para enviar el tráfico al LSP apropiado. En lugar de enviar todo el tráfico por un sólo LSP, las políticas de distribución crean nuevos FECs para dividir el flujo entre los LSPs disponibles.

Los flujos admitidos en un LSP dentro de un dominio se describen por un conjunto de etiquetas mapeadas a los LSPs en el ILM, esta situación se presenta cuando se unen LSPs en un punto particular dentro del dominio. Para distribuir el tráfico en éste punto, el FEC del flujo entrante es identificado por la etiqueta, y las políticas de balance carga se aplican de acuerdo al valor de la etiqueta de entrada.

Para que los procesos de balance de carga controlen la admisión del flujo a los LSPs, se define un algoritmo de 4 fases. La primera toma las medidas de congestión para cada uno de los LSPs, las medidas pueden estar en función de la derivación del retardo y la pérdida de paquetes. En la segunda fase, el algoritmo trata de unificar las medidas de congestión para cada LSP. Una vez se han calculado las medidas, la tercera fase monitorea cada LSP. Si se detecta un cambio significativo en el estado de la red, el algoritmo realiza la cuarta fase donde se ajustan adecuadamente las nuevas medidas de congestión. Finalmente, el algoritmo regresa a la fase 2 y se repite el proceso (Figura 4.10).

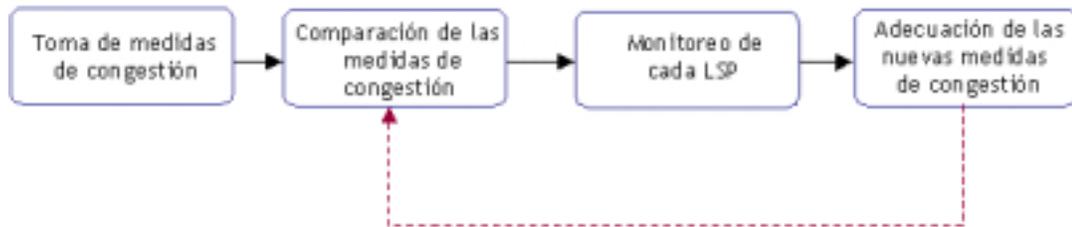


Figura 4.10. Algoritmo de Distribución.

Para desempeñar efectivamente la distribución del tráfico, es necesario conocer las características de los LSPs y los requerimientos de QoS. En general, las características del LSP incluyen retardo, variación de retardo, factor de carga, pérdida de paquetes, ancho de banda disponible, etc. Para el tráfico del mejor esfuerzo no hay requerimientos de QoS específicos, excepto una tasa de paquetes mínima. Las características de los LSPs se determinan por medio de mensajes de prueba: el LER de entrada transmite los paquetes de prueba al LER de salida el cual retorna el paquete y según esta información, el LER de entrada calcula las características del LSP. No se requiere que los LSRs modifiquen el contenido de estos paquetes, pero esta opción podría mejorar el proceso de medida.

4.5.1 División del Tráfico.

La principal función del balance de carga es la división del tráfico entrante que puede desarrollarse dinámica y/o estáticamente.

La división dinámica se basa en un control administrativo relacionado con la hora del día ó con la formación de un bucle de control que tiene en cuenta algunas medidas de los parámetros de red. Con el mecanismo de bucle de control se pretende balancear la carga sujeta a errores en las medidas y retardos. Puede aplicarse a una fracción del tráfico entrante que es enviado a un enlace particular en caso de que algunas medidas sean requeridas, por ejemplo, 20% a un LSP A y un 80% a un LSP C. Los objetivos para éste mecanismo se establecen según la información disponible localmente en el LSR upstream, para evitar los retardos de propagación o la congestión en un segmento de la red.

La división estática de la carga tiene en cuenta la información de la cabecera del paquete (tamaño del paquete, protocolo, número del puerto destino/fuente y la dirección destino/origen) o la interfaz de entrada. De otra manera, el tráfico se divide en partes iguales entre **N** LSPs, es decir, si el tráfico entrante tiene una tasa de **R** bps, cada LSP recibe una tasa **Rt** de:

$$R_t = \frac{R}{N} \text{ bps} \quad (\mathbf{N} = \text{número de LSP})$$

4.5.2 Proceso de Medidas.

La eficacia de cualquier mecanismo de TE depende principalmente del proceso de medidas. El proceso de medidas no requiere de la intervención de los LSRs sino de la participación de los LER de entrada y salida. En este proceso, la métrica más conveniente es el ancho de banda disponible, pero los métodos usados para realizar esta medida son complejos y las medidas no resultan ser muy precisas. Para solucionar este inconveniente, se define el retardo de los paquetes como la métrica más confiable, y para determinar su valor se transmiten paquetes de prueba desde el LER de entrada al de salida. El LER de entrada marca el paquete de prueba con un tiempo **T1**, el LER de salida retornará el paquete de prueba con un tiempo **T2**, si el reloj de entrada es más rápido que el reloj de salida en **Td** entonces el retardo total del paquete (tiempo en cola, tiempo de propagación y tiempo de procesamiento) queda determinado por la siguiente expresión:

$$T_2 - T_1 + T_d$$

Con un grupo de paquetes de prueba se puede estimar fácilmente el retardo promedio de los paquetes. Un punto importante para notar es que la sincronización entre los dos enrutadores no es necesaria.

La probabilidad de pérdida de paquetes es otra métrica que se calcula mediante un grupo de paquetes de prueba. La probabilidad de pérdida se puede determinar codificando un número de secuencia en el paquete para notificar al LER de salida cuantos paquetes se han transmitido desde la entrada, y otro campo para indicar cuantos paquetes se han recibido por el LER de salida. Cuando un paquete de prueba retorna al LER de entrada se calcula la

probabilidad de pérdida basándose en el número de paquetes transmitidos y el de paquetes recibidos.

4.6 FUNCIONALIDADES DE TE-MPLS

La combinación de las capacidades de Ingeniería de tráfico, MPLS y enrutamiento restringido brindan una serie de funcionalidades que permiten el control y la gestión de los recursos de la red asegurando la entrega del nivel de QoS adecuado a cada clase de servicio.

En la actualidad, las funcionalidades de mayor interés en el ambiente de las telecomunicaciones son QoS, recuperación de fallas y mecanismos de prevención de bucles, cada una de ellas tiene características y ventajas específicas que colaboran con el cumplimiento de los objetivos de desempeño de la TE. En las siguientes secciones se tratará cada una de estas funcionalidades.

4.6.1 QoS en TE-MPLS

La necesidad de evolucionar y soportar servicios con características de QoS precisas, condujo al IETF a proponer un modelo cuyo propósito es especificar, implementar y validar un conjunto de servicios y herramientas de TE-MPLS para ofrecer varias clases de servicios, mediante la interacción de cuatro componentes principales: MPLS, Servicios Diferenciados, Enrutamiento Restringido e Ingeniería de Tráfico. En la Figura 4.11 se ilustran estos componentes principales.



Figura 4.11. Posición Relativa de los Componentes de la Estructura QoS.

En esta estructura cada módulo desempeña funciones específicas de acuerdo al nivel en que se encuentra, el modelo de Servicios Diferenciados (DiffServ - Differentiated Services) divide el tráfico en diferentes clases y le da un tratamiento distinto a cada una de ellas. MPLS asigna etiquetas a los paquetes según la clasificación, destino y clase de servicio. El Enrutamiento Restringido calcula rutas sujetas a restricciones de ancho de banda y retardo. MPLS junto con el enrutamiento restringido proveen herramientas útiles para la TE encargada de decidir cómo transmitir el tráfico evitando congestión, de establecer y mantener dinámicamente la

configuración seleccionada para satisfacer los SLAs y de dimensionar la red de acuerdo a las demandas proyectadas.

El modelo de servicios diferenciados propuesto por el IETF define una variedad de mecanismos para clasificar el tráfico en un número reducido de clases de servicio, con diferentes prioridades. Según los requisitos de los usuarios, DiffServ diferencia servicios tradicionales tales como el WWW y el correo electrónico, de otras aplicaciones mucho más dependientes del retardo y la variación del mismo. Para ello se redefine y reestructura el campo ToS (de la cabecera IPv4) como un octeto DS (Figura 4.12.), a través del cual se indica a cada nodo el tratamiento que deben recibir los paquetes que viajan por un trayecto determinado. Diffserv también estandariza un grupo de Comportamiento por Salto (PHB - Per-Hop Behaviour) que define los procesos de selección y descarte de los paquetes en el buffer, umbrales de congestión, perfiles de tráfico, etc.

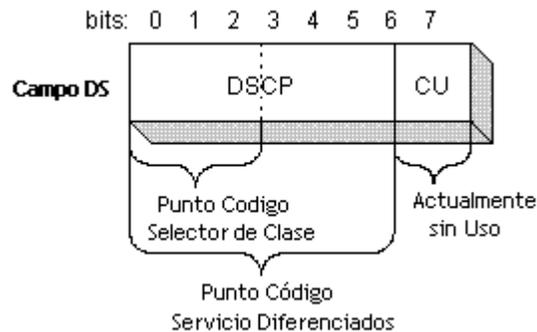


Figura 4.12. Estructura del Campo DS.

El PHB se aplica al paquete que entra al dominio según criterios políticos predeterminados y los resultados se codifican en el campo DS que indica a todos los nodos de un trayecto el tratamiento que debe recibir el paquete. Dependiendo de éste valor es posible ofrecer varias clases de servicio entre las cuales se encuentran:

- Servicio Premium (PS - Premium Service): Servicios de alta prioridad que requieren bajo retardo, bajo jitter y baja probabilidad de pérdida de paquetes.
- Servicio Asegurado (AS - Assured Service): Aplicaciones que requieren una mejor fiabilidad que los servicios del mejor esfuerzo.
- Servicios del Mejor Esfuerzo (BE - Best Effort Service): Servicios tradicionales de baja prioridad que no ofrecen garantías sobre el desempeño.

Para entregar al usuario el servicio adecuado, se definen los SLAs que reflejan las aplicaciones elementales que pueden ofrecerse y soportarse en la red y proporcionan información para establecer los objetivos de desempeño de la TE. Los paquetes se clasifican de acuerdo a los SLAs, la interfaz de entrada, dirección IP fuente/destino, número de puertos, ID del protocolo y el octeto ToS. Este tipo de clasificación se conoce como clasificación multicampo.

El modelo Diffserv se considera como la mejor solución para proveer QoS en la red, pero su éxito depende de las tecnologías de nivel 3 para operar adecuadamente en caso de congestión, dando al tráfico de alta prioridad un mejor tratamiento que al de baja prioridad. Si el problema de congestión se incrementa, DiffServ no proporciona el desempeño adecuado para la entrega del servicio. Por esta razón se integra el modelo DiffServ con las funciones de TE-MPLS para satisfacer los requerimientos de QoS.

El problema está en que ambas tecnologías codifican la clasificación de los paquetes a diferentes niveles, así, los LSRs no podrán leer los resultados de la clasificación del modelo DiffServ, puesto que no inspeccionan el contenido de la cabecera IP. Para solucionar este inconveniente y llevar a cabo la implementación, se usa el valor de la etiqueta MPLS y su campo EXP para indicar la forma en que las clases de servicio se propagarán dentro de los LSPs. Por ejemplo, el administrador puede decidir si un conjunto de clases de servicio se envía por un mismo LSP o por diferentes LSPs. Esta solución también provee flexibilidad en la manera en que las clases de servicio se protegen mediante el reenrutamiento y depende de la combinación de dos tipos de LSPs:

- LSP Deducido del campo EXP (E-LSP - EXP Inferred LSP). Estos LSPs se conocen como E-LSP, cuando el campo EXP de la cabecera MPLS se usa para indicar el PHB y la probabilidad de descarte de los paquetes; mientras que el valor de la etiqueta representa la combinación de un FEC. A la entrada del dominio el campo EXP se codifica de acuerdo a la información de los bits DSCP de la cabecera IP, permitiendo que los E-LSPs sean mucho más económicos en términos de las etiquetas consumidas. Sin embargo, no es fácil asociar la información del campo EXP con los servicios de reenrutamiento.
- LSP Deducido del valor de Etiqueta (L-LSPs - Label Inferred LSPs). Los LSPs son referenciados como L-LSP cuando el valor de la etiqueta indica el PHB que deberá aplicarse al paquete, mientras que el campo EXP determina la probabilidad de descarte. Estos L-LSPs requieren una asociación con los bits DSCP. La principal ventaja del L-LSP es su relación con el servicio de reenrutamiento. La determinación de usar reenrutamiento depende del SLA entre el suscriptor y el proveedor.

Con estos nuevos criterios de asignación de etiquetas es necesario modificar la tabla de envío adicionándole mas campos para adaptarse a las nuevas etiquetas. En la Figura 4.13 se ilustra la modificación de la tabla de envío.

Subred	Siguiente Salto	BE	AS	PS
221.1.29	LSR1	Etiqueta a	Etiqueta b	Etiqueta c
193.4	LSR2	—	—	—

Figura 4.13. Nuevos Campos de la Tabla de Envío.

En esta arquitectura, para garantizar la QoS, primero se configuran los LSPs entre cada par de nodos de entrada y salida que satisfagan los requerimientos y características del tráfico de cada una de las clases de servicio; posteriormente, usando protocolos de señalización se establecen los LSPs conforme a las capacidades de TE, asegurando que los paquetes enviados a lo largo del trayecto reciban el mismo tratamiento y, sean transportados y conmutados rápidamente por los LSRs que conforman el LSP.

En MPLS los LSPs son unidireccionales y es probable que para cada par entrada/salida y para cada clase de tráfico se establezca un LSP, en este caso, un número total de $\frac{C*N(N-1)}{2}$ de

LSPs son necesarios, donde **C** es el número de clases de tráfico y **N** es el número de enrutadores de frontera. Para reducir el número de LSPs, los trayectos de los enrutadores de entrada que comparten el mismo enrutador de salida se unen en un árbol particular, y el total de LSPs es **C*N**. También es posible usar los bits CoS para diferenciar las clases de paquetes de tal forma que los LSPs se reduzcan a **N**. Cuando la cantidad de flujos aumenta, el número de flujos en cada LSP también lo hace, pero el número de LSPs no necesita incrementarse, por tanto la arquitectura es escalable. Para facilitar su operación es necesario distribuir entre los dispositivos de frontera y del núcleo una serie de funciones y mecanismos que se describen a continuación:

- Clasificación de los paquetes:
La función de asignación de la Tasa de Acceso Negociada (CAR - Committed Access Rate) clasifica los paquetes a la entrada de la red antes que la etiqueta sea asignada. La función CAR usa los bits ToS u otro campo de la cabecera IP para clasificar el paquete (asignándolo a una clase de servicio) de acuerdo a la tasa de transmisión de entrada y salida. La función CAR también proporciona la gestión del ancho de banda determinando políticas de manejo de tráfico, de tal forma que si el tráfico excede el umbral, se le asigna parámetros de clases de servicio de menor prioridad o simplemente se descarta. Las políticas se determinan según el puerto físico, dirección MAC, dirección IP, puerto de aplicación, etc. Esta función se configura en las interfaces de frontera para controlar el tráfico que entra y sale de la red.

- Gestión de congestión
El algoritmo de Atención de Colas Equitativa Ponderada (WFQ - Weighted Fair Queuing) proporciona la habilidad de reordenar los paquetes y controlar la latencia en la frontera y en el núcleo, asignando un peso (prioridad) a diferentes clases de servicio para determinar el ancho de banda que será asignado a cada clase. Los pesos asignados son relativos y no absolutos, por tanto los recursos pueden compartirse entre clases de servicio para optimizar el uso del ancho de banda.

- Control de congestión
Entre los mecanismos de control de congestión se encuentran los algoritmos de Detección Aleatoria Preventiva (RED - Random Early Detection) que monitorean la carga del tráfico en un esfuerzo por anticiparse y evitar los problemas de congestión antes de que ocurran. El algoritmo RED monitorea la carga y descarta paquetes sofisticadamente si la

congestión se incrementa. Las fuentes detectan el tráfico descartado y reducen su velocidad de transmisión. El RED está diseñado para trabajar con las fuentes de tráfico TCP incrementando la tasa de transferencia útil y el uso de la capacidad de la red reduciendo al mínimo las pérdidas, a la vez que evita el caos por congestión. El mecanismo de control de congestión más utilizado es el algoritmo RED Ponderado (WRED - Weighted Random Early Detection) que combina las capacidades del RED con la precedencia IP; esta combinación da un trato diferencial a los paquetes de alta prioridad y descarta selectivamente el tráfico de baja prioridad, principalmente cuando las interfaces comienzan a congestionarse. También provee diferentes características de desempeño para varias clases de servicio, las cuales se diferencian según la probabilidad (valor o peso) de descarte. En la Figura 4.14 se ilustra la forma como opera el algoritmo WRED.

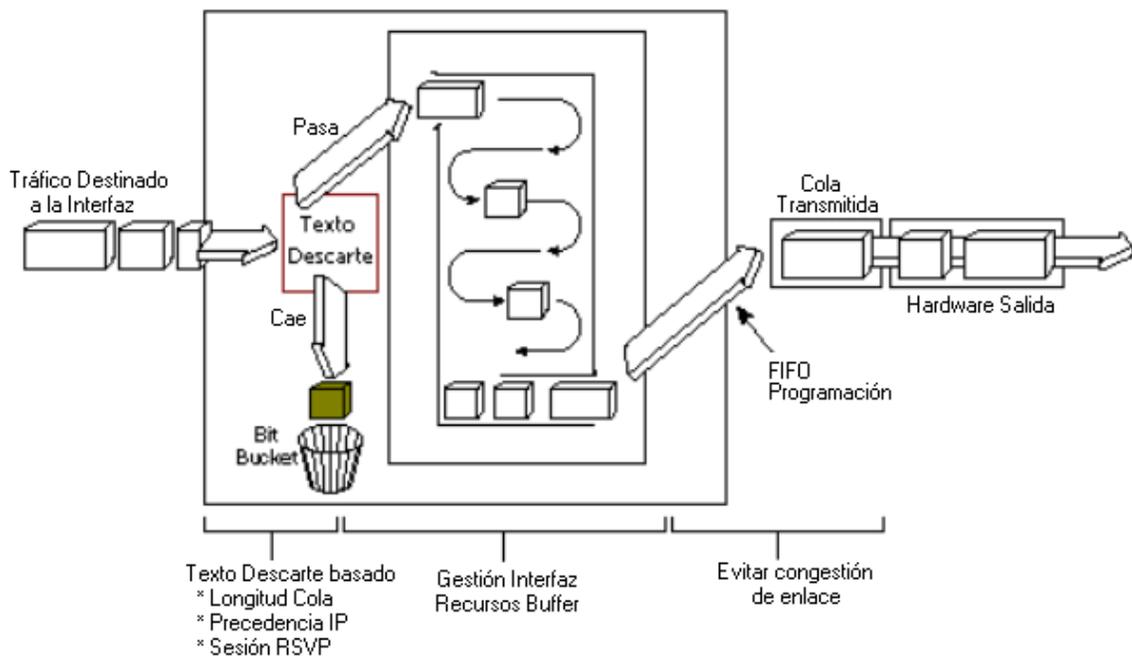


Figura 4.14. Funcionamiento de WRED.

En general, el modelo realiza las siguientes funciones.

1. Los Paquetes IP entran a la frontera del dominio MPLS.
2. El LER de entrada invoca la función CAR para clasificar el paquete y posiblemente fija los bits ToS. Alternativamente, el paquete puede recibirse con los bits ToS ya establecidos.
3. Para cada paquete, el enrutador desempeña una búsqueda basada en la dirección IP para determinar el siguiente salto.
4. La etiqueta apropiada se adiciona al paquete, y se copian los bits de precedencia en el campo EXP de la cabecera MPLS.
5. El paquete etiquetado se envía a la interfaz de salida apropiada.

6. Los paquetes se diferencian por clases, de acuerdo a la probabilidad de descarte (WRED), al ancho de banda y al retardo (WFQ).

4.6.2 Recuperación de Fallas

Un sistema de TE diseñado para proveer QoS debe asegurar la continuidad del servicio, y para ello requiere de un conjunto de procedimientos conocido como *recuperación de fallas* que protege el tráfico transmitido por los diferentes LSPs. La recuperación de fallas consiste en la restauración rápida y completa del tráfico afectado por una falla (enlace o nodo) sin perjudicar otras partes de la red y reduciendo al máximo la pérdida de los datos; así, cuando se produce un error en un trayecto, se buscan enlaces alternos para conmutar el tráfico evitando problemas de congestión e inestabilidad.

Para proveer una estructura de recuperación en las redes MPLS, es necesario distribuir entre los enrutadores procesos de detección, notificación y restauración de fallas, junto con algoritmos y técnicas que permiten incrementar la fiabilidad y disponibilidad de la red, respondiendo rápidamente a situaciones inesperadas con un mínimo de interrupción del servicio. Los propósitos de estas funcionalidades son:

- Facilitar la operación de red verificando su desempeño y reduciendo los costos de operación.
- Facilitar tiempos de convergencia rápidos.
- Reducir el número de puntos particulares de fallas.
- Es aplicable a la protección del tráfico en varias granularidades. Por ejemplo, es posible especificar la recuperación para una porción del tráfico en un trayecto individual, para todo el tráfico de un LSP, o para todo el tráfico de un grupo de LSPs.
- Es aplicable a un LSP extremo a extremo o a un segmento del trayecto.
- Sus acciones no afectan negativamente a otras operaciones de la red.
- Provee diferentes niveles de protección para varias clases de servicio, de acuerdo a sus requerimientos. Por ejemplo, para proteger las aplicaciones de tiempo real los trayectos alternos son preestablecidos o prereservados, mientras que el tráfico del mejor esfuerzo usa protección de trayectos establecidos sobre demanda o simplemente depende de mecanismos de reenrutamiento.
- Tiene en cuenta las acciones de recuperación de los niveles físico y de enlace (1 y 2).
- Preserva las restricciones del tráfico, es decir, de ser necesario el trayecto backup satisface los requerimientos de recursos y las mismas características de desempeño del trayecto primario.

En MPLS hay varias opciones para proveer la protección del tráfico, pero en general hay dos casos de particular interés: *conmutación protegida*, que define un sólo nodo (generalmente la entrada) como el responsable de reparar las fallas, y el *reenrutamiento rápido*, donde los nodos a lo largo del trayecto detectan y reparan los errores. Estos modelos pueden trabajar juntos dentro de un mismo dominio, la conmutación protegida se usa para la restauración

rápida de la conectividad mientras el reenrutamiento rápido determina una nueva configuración óptima para adaptar los trayectos según los objetivos de desempeño de TE.

La conmutación protegida define trayectos (o segmentos) alternos de acuerdo a información de enrutamiento, requerimientos de restauración y consideraciones políticas que aseguran la recuperación de una falla con un mínimo de interrupción del servicio. Estos trayectos podrán o no compartir recursos (enlaces y nodos) con el trayecto primario, pero si ambos comparten elementos que son fuentes de falla se reduce la confiabilidad de la red. En el momento de una falla, el nodo que la detectó la notifica al LSR Conmutador de Trayectos (PSL - Path Switch LSR) encargado de conmutar el tráfico desde el trayecto primario al trayecto alternativo. Como consecuencia la conmutación protegida es considerablemente rápida debido a que el trayecto alternativo no necesita ser señalizado en el momento del error.

Si los recursos (ancho de banda y espacio en el buffer) de los trayectos backup se reservan anticipadamente, éstos llevarán una copia del tráfico del LSP primario, en caso contrario, podrán transportar tráfico extra de baja prioridad que será destituido en caso que se presente una falla en el trayecto primario. Esto conduce a dos subtipos de conmutación protegida:

- Protección 1+1. El LSP backup está en estado de espera y listo para usarse inmediatamente por el tráfico del LSP afectado. Los recursos (ancho de banda, buffer, etc.) son reservados anticipadamente y sólo es necesario conmutar el tráfico al LSP backup, este cambio se indica por medio de mensajes de notificación. En conclusión, la protección 1+1 es muy rápida, pero también muy costosa en términos de los recursos usados.
- Protección 1:1. Los recursos del LSP backup están disponibles para ser utilizados por el tráfico del LSP afectado. Mientras no ocurra una falla los LSPs backup pueden transportar tráfico de baja prioridad. En este subtipo, el tráfico sólo viaja en el trayecto primario, y es conmutado al LSP alternativo si se presenta un error en el trayecto primario. Una vez el proceso de conmutación comienza, el tráfico de baja prioridad transportado por el LSP backup es desplazado por el tráfico protegido. La protección 1:1 usa de forma más eficiente los recursos del trayecto. Esta protección se puede extender a 1:n y m:n.

En la Figura 4.15, el tráfico se transmite por los LSPs primarios. El LSP backup es un trayecto establecido y listo para transportar tráfico. Si se reporta un error en alguno de los LSPs A o B, el tráfico es inmediatamente conmutado al LSP backup que no necesita ser señalizado.

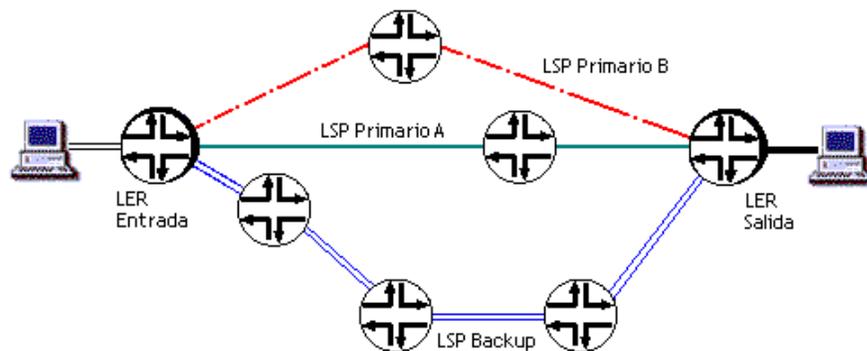


Figura 4.15. Conmutación Protegida.

Los LSPs Backup pueden soportar mas de un LSP primario pero sólo transportan el tráfico del primer LSP que falle. En la Figura 4.15 el LSP es backup para los LSPs primarios A y B. Cuando alguno de ellos falla, el tráfico es conmutado al LSP backup y el otro LSP primario quedará sin protección. Esta forma de operar es aceptable bajo el supuesto que no ocurran fallas en varios LSPs simultáneamente.

El reenrutamiento transmite los datos MPLS a trayectos alternos alrededor del enlace donde se presenta una falla, sin realizar procesos de señalización en el momento de ser detectada. Los trayectos o segmentos backup se establecen sobre demanda después de detectar la falla, según la información y políticas de enrutamiento, configuraciones predefinidas e información de la topología de la red.

Una vez que la falla se detecta, se notifica al PSL quien simplemente actualiza la programación de tal forma que los datos que eran enviados por una interfaz y con una etiqueta específica, se transmitan por otra interfaz y con una etiqueta diferente; como se muestra en la Figura 4.16.

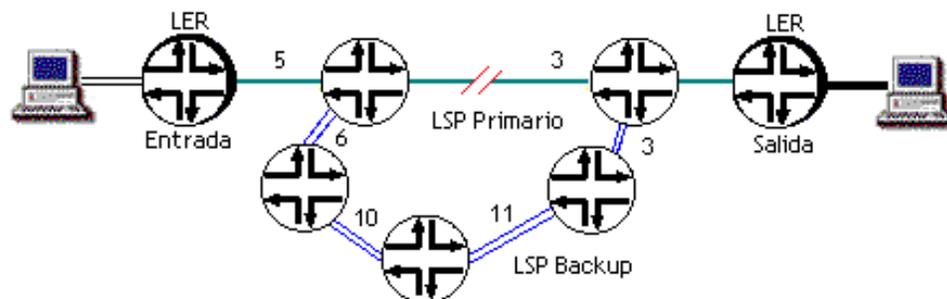


Figura 4.16. Reenrutamiento Rápido.

A diferencia de la conmutación protegida, el reenrutamiento no requiere propagar el error al punto de reparación usando protocolos de señalización, porque el punto de reparación es el punto de detección, convirtiéndolo en un mecanismo más lento pero más económico y simple porque los recursos se asignan sólo cuando ocurre una falla y ésta es detectada.

4.6.2.1 *Detección de Fallas.*

El proceso de recuperación comienza con la detección y localización de fallas dentro de la red. Las fallas se detectan y localizan a través de mecanismos de gestión que consisten de alarmas, diagnósticos, estadísticas, mensajes transmitidos periódicamente entre LSRs adyacentes y señales que indican la ocurrencia de una falla a lo largo de un trayecto. Cuando ocurre algún error en cualquier segmento de red, se difunde una Señal de Indicación de Falla (FIS - Fault Indication Signal) desde el LSR que lo detectó a su vecino upstream o downstream, hasta alcanzar un PSL. Esta señal acciona mecanismos OAM (Operación, Administración y Mantenimiento) del plano de usuario que emite paquetes de Verificación de Conectividad (CV - Connectivity Verification) desde el nodo de entrada al nodo de salida del LSP. El flujo CV detecta fallas relacionadas a errores de enrutamiento así como fallas de enlace y nodo. En el mecanismo de gestión, también se define un Identificador de Fallas hacia Adelante (FDI - Forward Defect Identifier) y un Identificador de Fallas hacia Atrás (BDI - Backward Defect Identifier) que informan de la localización y tipo de falla. Los tipos de fallas que los nodos podrán detectar son:

- Falla de trayecto. Indica la carencia de conectividad del trayecto y se detecta por medio de un test de continuidad como es el caso de los mecanismos de pruebas de enlace entre los LSR vecinos, los cuales intercambian periódicamente mensajes que indican el estado de sus recursos.
- Degradación del trayecto. Indica que los trayectos tienen continuidad, pero la calidad de conexión no es aceptable; esto se detecta por medio de mecanismos de monitoreo de desempeño del trayecto.
- Falla de enlace. Es una falla de bajo nivel que indica la pérdida de conectividad. Si los protocolos de niveles bajos soportan la detección y reporte de fallas, comunican al mecanismo de recuperación MPLS del suceso.
- Degradación del enlace. Indica que el enlace se desempeña en niveles no aceptables.

La habilidad de detectar fallas oportunamente es esencial para mantener una infraestructura de alta disponibilidad con requerimientos de desempeño específicos y se logra monitoreando la red y verificando los niveles de QoS, conectividad, estado de los trayectos alterno y primario, etc.

4.6.2.2 *Notificación de Fallas.*

Si un enrutador detecta una falla en el LSP primario y no puede iniciar el proceso de recuperación directamente, él envía una notificación al PSL para que conmute el tráfico desde el trayecto afectado al LSP alterno. La notificación se realiza a través de mensajes de control procesados salto por salto en cada LSR hasta alcanzar el PSL, éstos mensajes son señales FIS y Señales de Recuperación de Fallas (FRS - Fault Recovery Signal) que son transmitidas en dirección upstream y se clasifican como tráfico de alta prioridad para asegurar que se propaguen oportunamente. La eficiencia del mecanismo de recuperación depende de la confiabilidad y rapidez para notificar las fallas al PSL.

Es importante considerar que los LSPs son entidades unidireccionales y para notificar la falla al PSL es necesario un mecanismo que provea un trayecto en la dirección apropiada para indicar la ocurrencia de una falla y para notificar la reparación de la misma; este trayecto se define por el Árbol de Notificación Inverso (RNT - Reverse Notification Tree) punto a multipunto que es un reflejo exacto del trayecto de trabajo. El RNT se crea durante el proceso de establecimiento de los LSPs primarios, haciendo que los LSRs recuerden su vecino upstream de cada enlace de entrada, para esto, los mensajes de señalización llevan consigo la identificación del nodo upstream para construir una tabla de conexión inversa que contiene la identificación de los nodos y la interfaz de cada LSP, como se indica en la tabla 4.1.

Etiqueta de Entrada	Interfaz de Entrada	Etiqueta de Salida	Interfaz de Salida	Etiqueta de Salida	Interfaz de Salida
N43	I34	N32	I23	N39	I93

Tabla 4.1. Tabla de Conexión Inversa para LSR3.

Cuando un LSR recibe una FIS, él extrae la etiqueta del paquete y la usa como índice para consultar en la tabla de conexión inversa cual será la etiqueta y la interfaz de salida por la que se enviará la FIS. Por ejemplo, en la Figura 4.17, en el enlace L[2,3] ocurre una falla detectada por el LSR3 quien transmite una FIS al LSR2. La FIS contiene la etiqueta entrante del LSP del enlace L[2,3]. El mensaje FIS es recibido por LSR2 quien consulta su tabla de conexión inversa y reenvía la FIS al LSR1, el cual a su vez termina la transmisión de la señal y espera un tiempo antes de iniciar la conmutación.

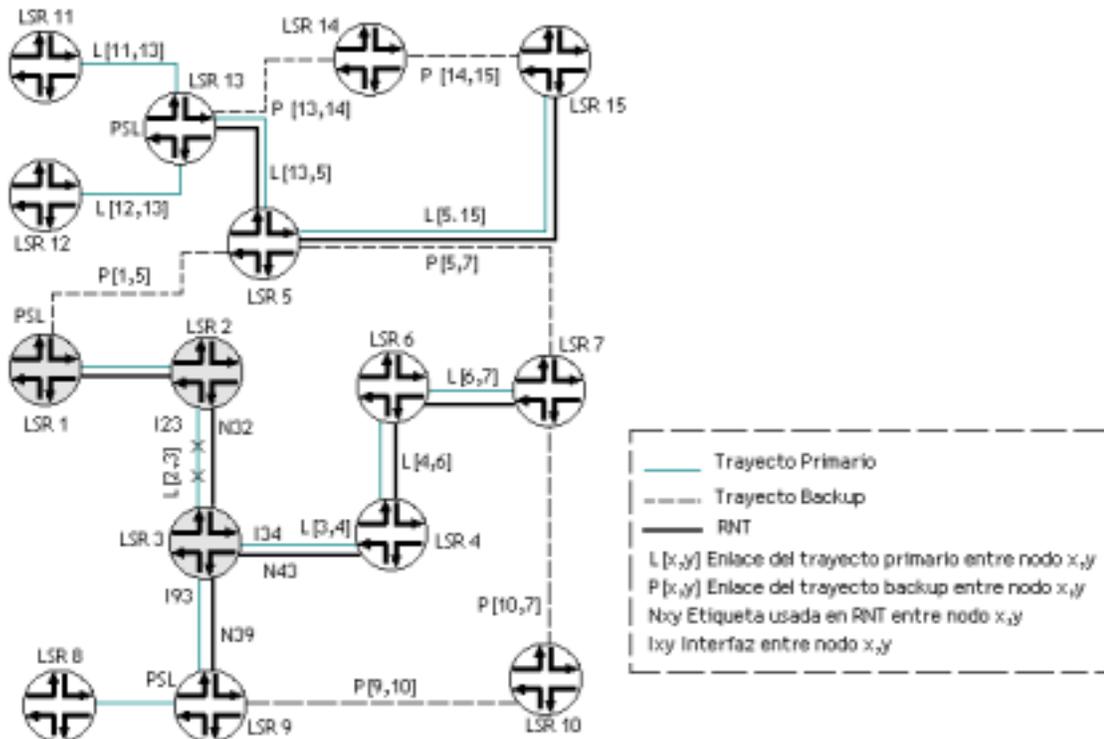


Figura 4.17. RNT en una red MPLS.

4.6.2.3 Topología del Modelo de Recuperación de Fallas

Idealmente, la recuperación se realiza entre la fuente y el destino (reparación global), o sólo en un segmento de red o para un conjunto determinado de trayectos (reparación local). Esto depende de la topología de la red y los requerimientos del proveedor y el usuario, por ejemplo, en la Figura 4.17, el trayecto de trabajo 8-9-3-4-6-7, sólo tiene protección del segmento 9-3-4-6-7.

4.6.2.3.1 Recuperación Local

Con la recuperación local se pretende proteger el dominio contra fallas de un enlace o nodo y reducir la cantidad de tiempo requerida para propagar la señal FIS. La reparación local puede ser de dos tipos:

1. Restauración/recuperación de enlace.

Cuando ocurre una falla en un enlace específico, el trayecto se reconstruye para desviar el tráfico alrededor del enlace afectado. En este caso, el LSR upstream que conecta el enlace que falla, conmuta el tráfico desde un enlace físico a un enlace virtual de tal forma que el tráfico continúa transmitiéndose con un mínimo de interrupción. En la Figura 4.18 se muestra un túnel que se ha establecido para proteger el enlace entre el LSR A y el LSR B.

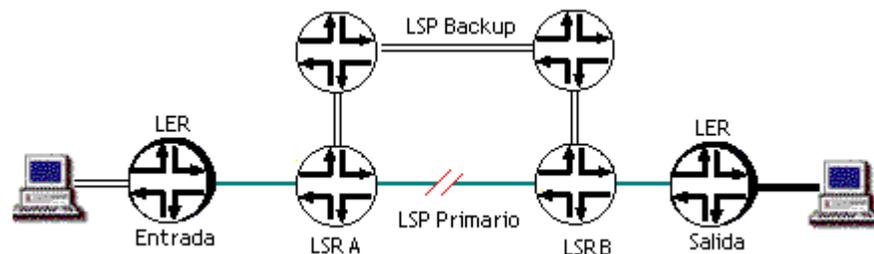


Figura 4.18. Recuperación de Enlace.

2. Restauración/recuperación de nodo.

En este tipo de recuperación, el trayecto backup se configura para desviar el tráfico cuando un LSR del trayecto primario falla. En la Figura 4.20 se muestra un túnel desde el LSR A al LSR C que brinda protección contra fallas al LSR B. Si el LSR A detecta una fallar, el LSP es reenrutado al túnel y el tráfico continúa fluyendo.

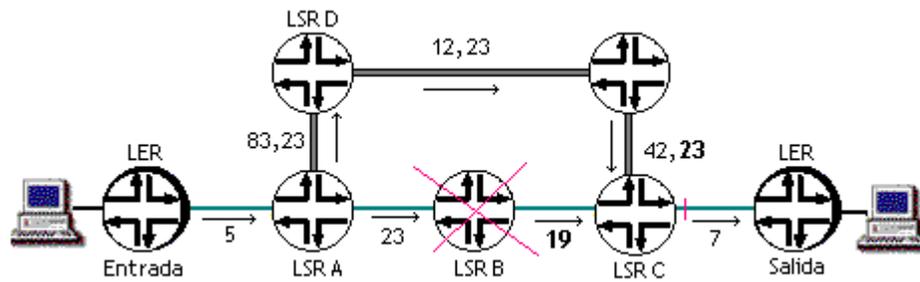


Figura 4.19. Recuperación de Nodo Sin Objeto Almacén de Ruta.

En este modelo es necesario usar la pila de etiquetas para conmutar el tráfico afectado al túnel backup, pero el problema es que los nodos extremos del túnel no son LSRs adyacentes: un paquete enviado por el túnel backup desde el LSR A tiene una pila de etiquetas, donde la etiqueta superior indica que podrá seguir el trayecto alternativo y la etiqueta de nivel 1 esta relacionada con el LSP original. Sin embargo la etiqueta de nivel 1 proporciona información de conmutación sólo para el LSR B, como consecuencia, cuando la etiqueta superior del túnel es removida por el LSR C, la etiqueta de nivel 1 del paquete no es reconocida por él (Figura 4.19). Para solucionar este inconveniente, se define un objeto de almacén de ruta, que consiste en reportar las etiquetas usadas en cada salto durante el establecimiento del LSP, de modo que cada nodo del trayecto conoce las etiquetas usadas en todos los enlaces, y cada LSR puede determinar las etiquetas correctas a usar en la pila de etiquetas cuando el LSP primario falle, como se aprecia en la Figura 4.20.

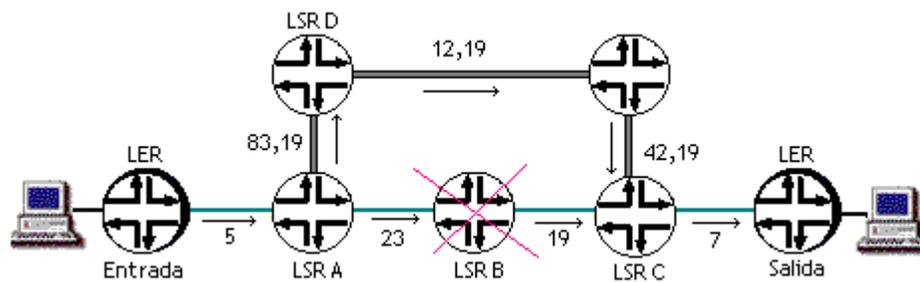


Figura 4.20. Recuperación de Nodo Con Objeto Almacén de Ruta.

4.6.2.3.2 Reparación Global.

Por otra parte, la reparación global se aplica a la restauración extremo a extremo, protegiendo la red contra fallas de enlaces o nodos de un trayecto o un segmento de trayecto, con la excepción de las fallas ocurridas en el LER de entrada. En la reparación global el PSL usualmente esta distante del lugar de la falla y ésta debe notificarse por medio de una señal FIS. En muchos casos, el trayecto backup puede estar completamente desligado del LSP primario. En la Figura 4.21 se ilustra la protección de un LSP primario a través de un trayecto alternativo establecido junto con el primario.

Si ocurre un error en el enlace, el LSR conmuta los datos al trayecto de retorno para transmitirlos hasta el LER de entrada, quien se encarga de llevarlos al trayecto alternativo. Esta solución podría generar altos retardos dependiendo de la longitud del trayecto primario y del lugar donde se origina la falla.

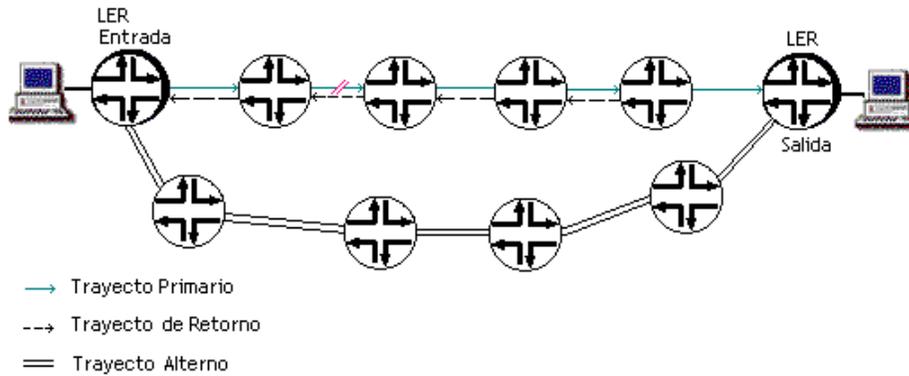


Figura 4.21. Reparación Global.

Si la falla ocurre cerca de la salida, como se muestra en la Figura 4.22, se establece un trayecto shortcut que se conecta con el trayecto alternativo, así el LSR que detecta la falla se reprograma y envía los datos con la etiqueta correcta al trayecto shortcut para alcanzar el LSP alternativo. Este proceso trae complejidad adicional a los protocolos de señalización.

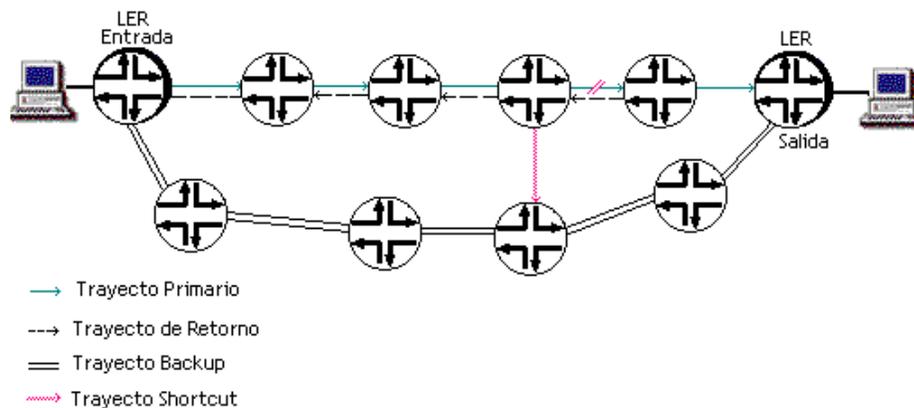


Figura 4.22. Reparación Global con Trayectos Shortcut.

4.6.2.4 Tolerancia a Fallas.

Las fallas de software y hardware dentro de un LSR se reparan mediante mecanismos tolerantes a fallas (TF - Fault Tolerance) que consisten en la duplicación de los componentes del enrutador para proporcionar alta disponibilidad en el núcleo de la red. La disponibilidad, que es una medida del porcentaje del tiempo en que un nodo está en servicio, ayuda a detectar las fallas oportunamente con un mínimo de interrupción del servicio.

Hay varios componentes que pueden fallar en un LSR y es necesario identificarlos para desarrollar una estrategia en caso que ocurra un error en cualquiera de ellos. A nivel de hardware los componentes que conforman un enrutador MPLS son los puertos, la tarjeta de red, la tarjeta controladora o CPU y el módulo de conmutación. A nivel de software, el código reside en las tarjetas controladoras y de red. Los elementos del software que pueden fallar son el código de señalización, la pila de protocolos, el software de enrutamiento, etc. En la Figura 4.23 se ilustra un LSR tolerante a fallas.

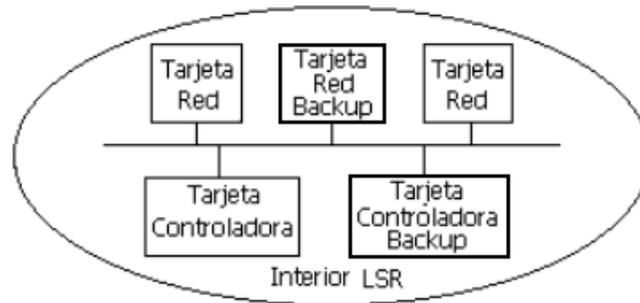


Figura 4.23. LSR Tolerante a Fallas.

En el proceso normal del sistema tolerante a fallas, el componente primario replica datos claves e información de cambios de estado al componente backup de tal forma que la información esté disponible cuando él se haga cargo de los procesos. Esta réplica no puede ser muy frecuente para evitar interrupciones de otros procesos en el componente primario (mientras se espera la respuesta de la réplica) e impedir que el tiempo de establecimiento de un LSP se incremente.

4.6.3 Mecanismos de Prevención de Bucles (Loops).

Como se mencionó anteriormente, en las redes MPLS los paquetes se envían a través de LSPs que se establecen usando protocolos de distribución de etiquetas. Algunos de estos protocolos usan información de los protocolos de enrutamiento de nivel 3 que tienden a formar loops transcientes mientras la convergencia de enrutamiento se lleva a cabo. Para evitar y reducir los efectos de los bucles, MPLS cuenta con tres niveles de control de bucles:

- Detección de bucles: Detecta el loop y termina e ignora el segmento después de un corto periodo de tiempo.
- Prevención de bucles: Previene la formación de loops antes que los paquetes sean enviados.
- Mitigación de bucles: Minimiza los efectos negativos del bucle.

MPLS adopta el mismo mecanismo de control usado por el Protocolo Internet, el cual consiste en descartar los paquetes que circulen por un loop de acuerdo a la información del campo TTL de la cabecera MPLS, sin embargo, hay casos donde el campo TTL no esta disponible, como en ATM y Frame Relay. Una solución para éste problema es usar la técnica de asignación de

buffer como medio para mitigar los efectos de los bucles. En la asignación de buffer, si un paquete cae en un loop, este puede consumir sólo una cantidad limitada de espacio del buffer, y de esta forma los LSRs podrán funcionar correctamente (procesar y enviar paquetes hacia LSPs libres de bucles) y enviar paquetes de actualización para asegurar la convergencia del enrutamiento.

MPLS también usa mecanismos para la detección de bucles basados en el Algoritmo Vector Trayecto/ Algoritmo de Difusión (PD - Path Vectors / Diffusion Algorithm) y en el algoritmo "Colored Thread", diseñados para establecer LSPs libres de loops. El algoritmo PD (Figura 4.24) previene la formación de los bucles usando una lista de direcciones de los LSR, conocida como vector trayecto, por los que pasan los mensajes de requerimiento de etiquetas. Un mensaje de requerimiento que tiene una lista de direcciones se envía a un LSR el cual adiciona su propia dirección al vector antes de enviar el mensaje al siguiente salto. Si un LSR ve su dirección en el vector trayecto, concluirá que se ha formado un loop y es responsabilidad de ese nodo terminar y rechazar el requerimiento de etiqueta. Hay dos variantes de este algoritmo, una permite que cada uno de los nodos almacene el vector trayecto, y en la otra no se realiza tal almacenamiento. Con la primera alternativa se detecta rápidamente la formación de un loop pero se requiere de mucha memoria y complejidad para mantener la información en cada salto.

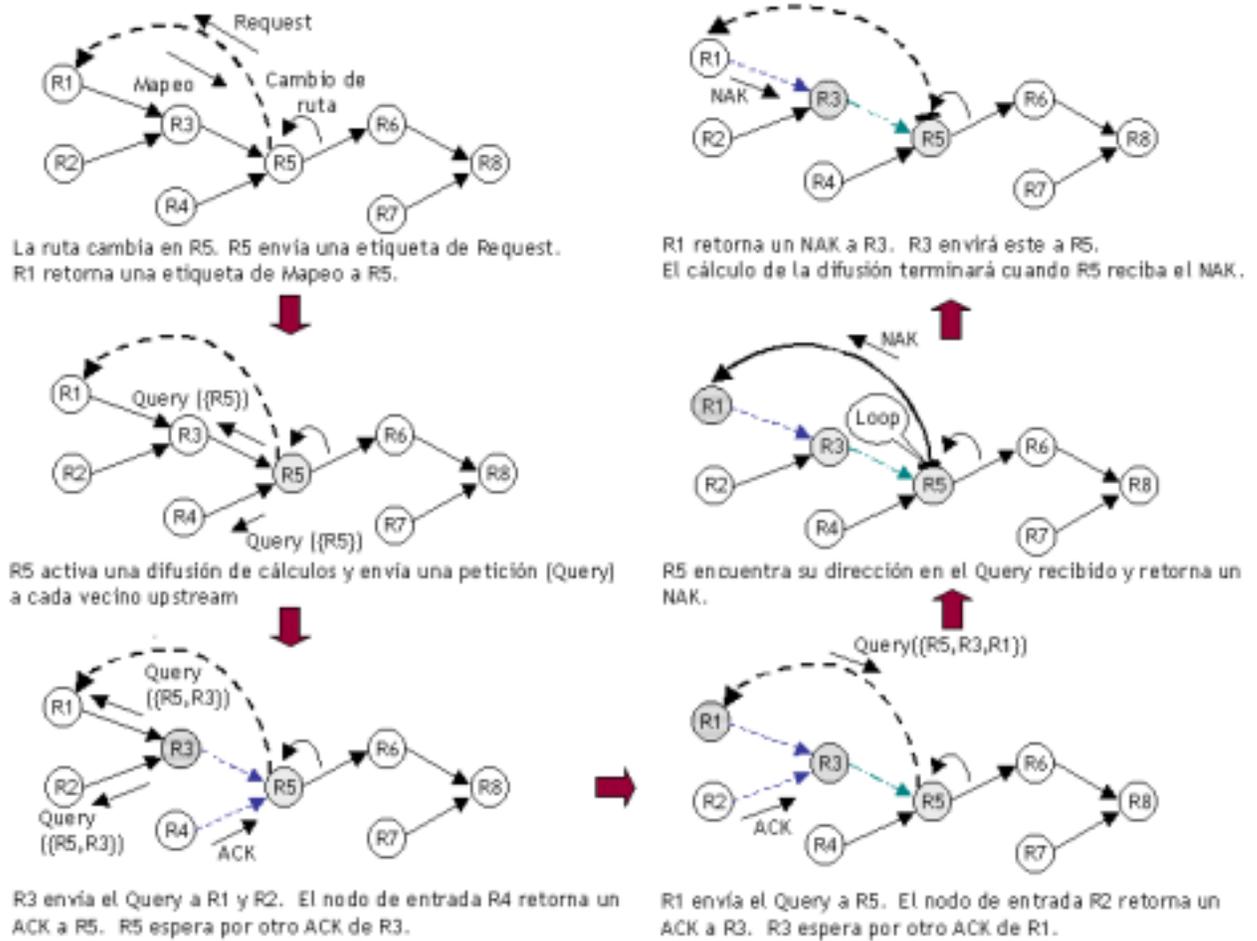


Figura 4.24. Ejemplo del Algoritmo PD.

Finalmente, la última aproximación es la prevención de bucles basada en el algoritmo "Colored Threads" (Figura 4.26). La idea básica es propagar un procedimiento que dé un color a cada enlace a lo largo del LSP en la dirección downstream. Durante el procedimiento, un mensaje con un conjunto de atributos conocidos como "thread" (Figura 4.25), se propaga a los nodos downstream.



Figura 4.25. Estructura de los mensajes "thread".

El campo color está compuesto por la dirección IP y un identificador local que es único para cada nodo, el número de saltos representa el número de enlaces que existen entre el nodo origen y destino y el campo TTL se usa para evitar la ejecución ilimitada del proceso. El valor inicial del campo TTL se fija cuando el color es establecido y se reduce cuando se envía al nodo downstream. El proceso termina cuando el TTL es cero.

Un LSP esta libre de loops, si el nodo que inicia el proceso recibe un reconocimiento de sus nodos downstream. En caso contrario, un LSR que ve un color anteriormente observado concluye que un bucle se ha formado. Cuando esto ocurre, se interrumpe el proceso de establecimiento del LSP hasta que un cambio de enrutamiento libere el loop.

Esta técnica es muy complicada de explicar pero no de implementar, es parte opcional de la arquitectura porque las técnicas de detección y supervivencia pueden ser suficientes en muchos casos. Sin embargo, cuando se requiere de técnicas más robustas, la elección está entre el algoritmo PD y el algoritmo "Colored Threads". Con PD se garantiza el establecimiento de LSPs libres de loops pero la información que transmite y almacena en cada salto podría ser muy grande, lo que no sucede en la técnica "Colored Threads" donde la información transmitida y almacenada es de tamaño constante.

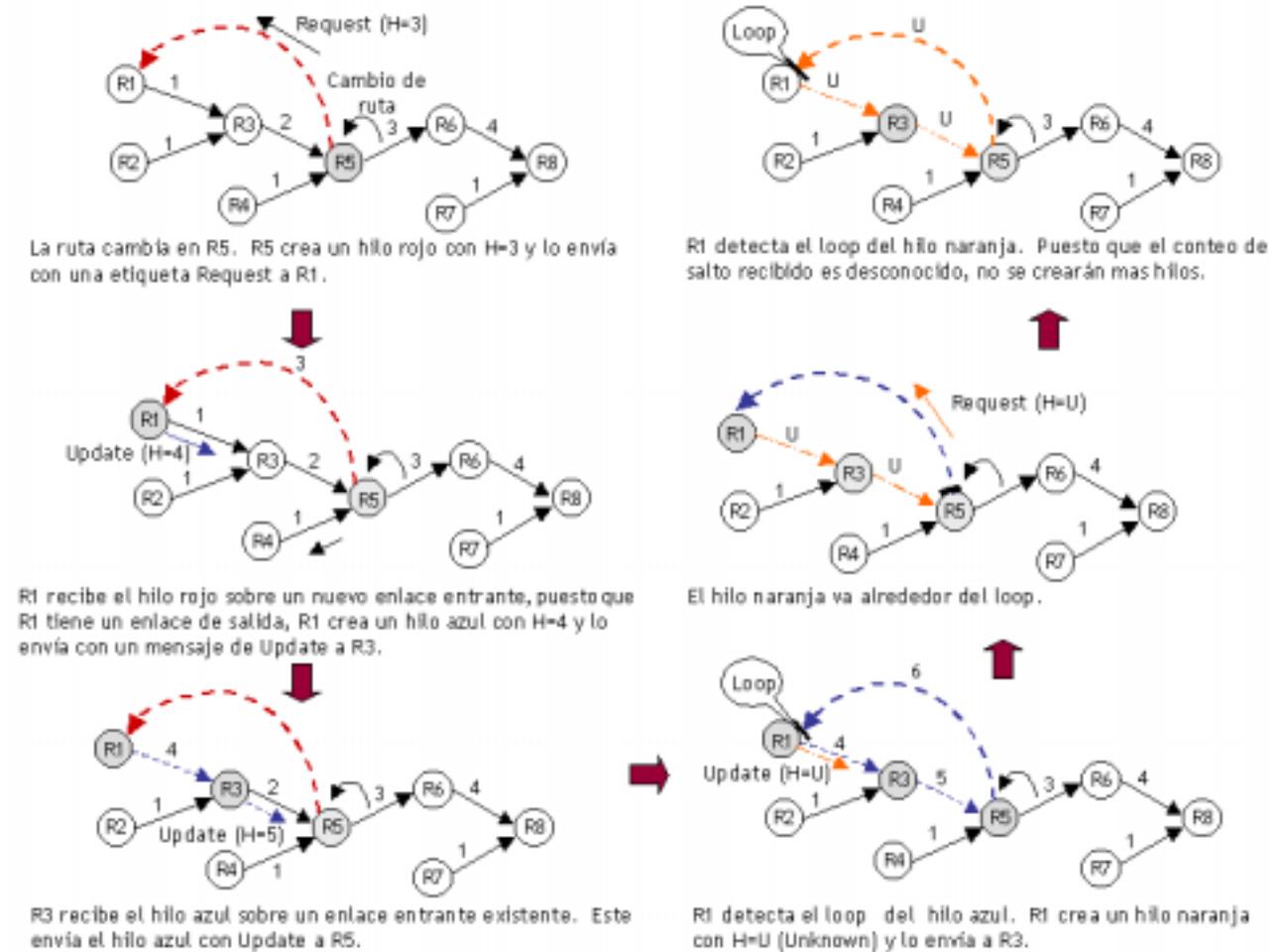


Figura 4.26. Ejemplo del Algoritmo Colored Threads.

5. CRITERIOS DE DISEÑO Y MIGRACIÓN DE LAS REDES MPLS

MPLS adiciona nuevas características a las redes IP, las cuales permiten soportar aplicaciones que mejoran el desempeño, satisfacen las necesidades actuales de los usuarios y hacen de MPLS una tecnología atractiva para los proveedores de servicio que la ven como el próximo paso en la evolución de las redes de telecomunicaciones. Aunque MPLS no se encuentra completamente estandarizada ya está siendo implementada por las grandes compañías de telecomunicaciones.

La interoperabilidad existente de MPLS con otras tecnologías y la similitud en su diseño con el de las redes IP, ha permitido la fácil introducción de MPLS en las redes existentes del mercado.

El propósito de éste capítulo es ilustrar el proceso de diseño para la implementación de una red MPLS con capacidades de TE y que soporte QoS, sobre una red nacional cuyas características son aproximadas a la realidad. El diseño aquí presentado no es un proceso único, por el contrario puede variar de proveedor a proveedor.

5.1 JUSTIFICACIÓN DE LA MIGRACIÓN A UNA RED MPLS

Como se ha discutido a lo largo de éste documento, las actuales redes IP presentan una serie de debilidades (problemas de dimensionamiento, de capacidad, de gestión, de QoS, etc.) que la convierten en una red poco escalable y difícil de manejar. Ha sido necesario el desarrollo de nuevas tecnologías que superen éstos inconvenientes y hagan de Internet una red multiservicio con capacidades de ingeniería de tráfico que mejoren su arquitectura y diseño. Este proceso de evolución a ratificado a MPLS como la tecnología ideal para proveer un diseño, dimensionamiento y gestión de red más óptimo.

Los requerimientos y condiciones que justifican la introducción de la tecnología MPLS en las redes IP son:

- Alto desempeño. Uno de los requerimientos básicos de MPLS es la optimización en la transferencia de los paquetes a través de la red. La separación de las funcionalidades de envío y control brindan un alto desempeño debido a la simplificación en el proceso de envío de los paquetes y la toma de decisiones de enrutamiento, ofreciendo la posibilidad de usar técnicas hardware para implementar las capacidades de envío y de ésta forma disminuir los tiempos de procesamiento y transmisión de los paquetes.

- Amplio alcance. El dominio MPLS tiene una visión más amplia de la topología que cualquier otra tecnología, ya que procesa de manera más óptima la información obtenida por los protocolos de nivel de red, permitiendo incrementar el número de trayectos alternos disponibles a un destino particular.
- Capacidad de recuperación. MPLS garantiza la continuidad del servicio de tal forma que en caso de presentarse una falla, la red responda de forma rápida restaurando el flujo de tráfico y encaminándolo con éxito hacia el destino. Para esto MPLS se soporta en mecanismos de recuperación de fallas que ayudan a mantener el nivel de QoS acordado con el usuario.
- Control de los recursos de red. MPLS soporta la creación de trayectos explícitos, haciendo posible gestionar los recursos asignados a ellos, así como también controla los que se encuentran disponibles en la red; como resultado, los dispositivos son empleados eficientemente y se disminuyen los costos en su operación y mantenimiento.
- Tiempos de convergencia. MPLS disminuye significativamente los tiempos de procesamiento gracias al desempeño de su algoritmo de envío de datos. La reducción de éstos tiempos es uno de los factores que permite a MPLS prestar servicios de tiempo real.
- Compatibilidad. Como su nombre lo indica, MPLS es una tecnología compatible con múltiples protocolos de nivel de enlace y de red que le permiten integrarse fácilmente a cambios funcionales realizados en su estructura de forma rápida y a bajo costo.
- Múltiples servicios. Gracias a la clasificación de los paquetes que se realiza en la entrada del dominio y al control sobre los procesos de enrutamiento, MPLS brinda la arquitectura adecuada para la prestación de Servicios Diferenciados, en la cual los trayectos se establecen anticipadamente para garantizar la reservación de recursos y por lo tanto la QoS.

En resumen, MPLS ofrece a los proveedores de servicio amplias posibilidades para el diseño, dimensionamiento, gestión, QoS, enrutamiento, recuperación de fallas, etc. que la convierten en una infraestructura de red más escalable, operable y robusta.

5.2 ESTRUCTURA DE RED

Antes de empezar con el diseño de una red MPLS, es conveniente conocer la estructura de red de los ISPs convencionales.

Las redes de los ISPs están formadas por los Puntos de Presencia (PoP - Point of Presence) y los enlaces que los conectan, como se muestra en la Figura 5.1. Los PoP constan de una combinación de uno o mas Enrutadores de Acceso (ARs - Access Routers) los cuales

proporcionan el acceso a los clientes, los Enrutadores de Frontera (BRs - Border Routers) usados para la interconexión con otros ISPs, los Enrutadores de Hosting (HRs - Hosting Routers) encargados de proveer el acceso a servidores web de diversas de compañías y los Enrutadores del Núcleo (CR - Core Routers) conectados a otros PoPs.

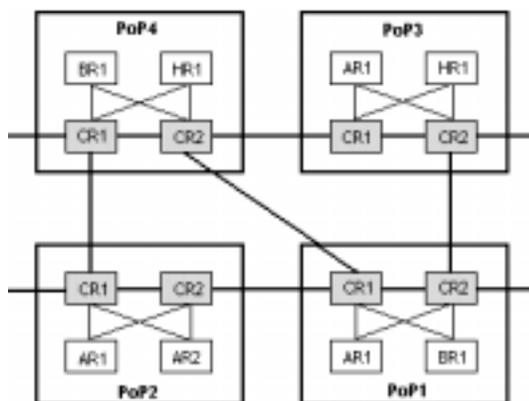


Figura 5.1. Estructura de los ISPs.

Los paquetes provenientes de los ARs, BRs o HRs con destino a otros PoPs deben enviarse primero al CR, el cual a su vez retransmitirá estos paquetes a los CRs en otros PoPs hasta que alcancen sus destinos. Usualmente la arquitectura de los PoPs es altamente simétrica, como se puede ver en la Figura 5.1.

5.3 CRITERIOS DE DISEÑO

El propósito principal del diseño de una red MPLS es producir una infraestructura con la capacidad necesaria para satisfacer los requerimientos de las demandas de tráfico dadas, y de esta forma crear una red que opere óptima y eficientemente. Para lograrlo es importante seguir un proceso de diseño conformado por una serie de pasos lógicos que permiten al diseñador tener un conocimiento completo de la estructura de la red, recolectar información confiable, determinar los sistemas de transmisión y enrutamiento, y juzgar la viabilidad de los resultados logrados en el diseño.

Un proceso de diseño típico consiste de los siguientes pasos:

1. Localización y diseño de los puntos de presencia.
2. Dimensionamiento de los enlaces del backbone
3. Diseño del enrutamiento IP
4. Dimensionamiento del espacio de las etiquetas MPLS
5. Configuración de las características o aplicaciones de MPLS, tales como ingeniería de tráfico y QoS.
6. Evaluación y optimización del diseño de la red.

En este proceso, la mayoría de los pasos son comunes con los del diseño de las redes IP, con la excepción de los pasos 4 y 5 que son específicos de MPLS. A continuación, se ilustra la aplicación de esta secuencia de pasos en una red que se extiende sobre el territorio Colombiano y que está formada por 6 nodos localizados en las principales ciudades del país; como se muestra en la Figura 5.2.



Figura 5.2. Red Colombiana.

5.3.1 Localización y Diseño de los Puntos de Presencia

Para el diseño de los puntos de presencia se debe tener en cuenta:

- Elección de los tipos de enlaces de acceso a ser soportados por la red.
- Elección de los tipos de enlaces del núcleo a ser usados en la red.
- Requerimientos para fiabilidad, incluyendo el uso de troncales redundantes en zonas de alto tráfico, procesadores redundantes, etc. Esto puede restringir la elección de los equipos usados en los PoPs.
- Requerimientos para servicios diferentes a IP o MPLS, y capacidad de los equipos para satisfacer esos requerimientos.
- Localización de los PoPs, determinado principalmente por el lugar donde se encuentran ubicadas las ciudades.
- Volumen de los usuarios finales alrededor de cada locación.

Una vez se han tenido en cuenta los requerimientos para el diseño de los PoPs, MPLS ofrece diferentes opciones para la configuración de los mismos. Algunas de estas configuraciones se muestran en la Figura 5.3.

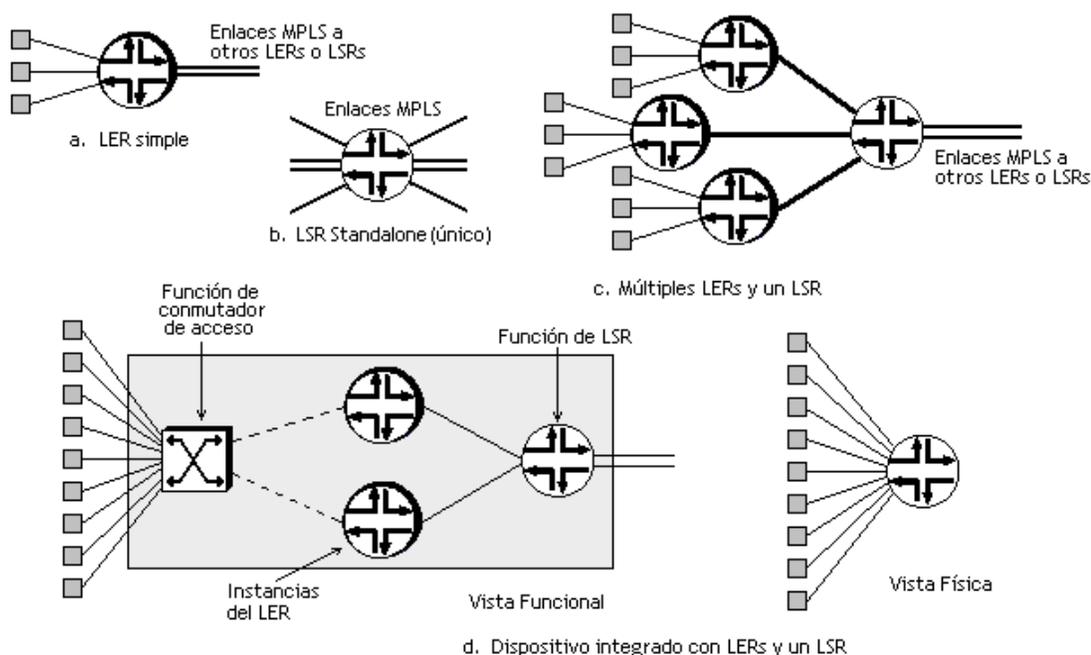


Figura 5.3. Configuraciones de los PoPs.

Un PoP pequeño podría estar formado por un único LER (Figura 5.3.a) y un número de líneas de acceso que pueden ir de menos de 10 a miles, sin embargo, si el volumen de líneas de usuario en un PoP es elevado, se necesitan de varios LERs para satisfacer la demanda. En un PoP con varios LERs, el uso de un LSRs extra como dispositivo de concentración tiene varias ventajas de escalabilidad (Figura 5.3.c):

- Reducción del número de protocolos de enrutamiento por pares hacia afuera del PoP, lo cual ayuda a la escalabilidad de estos protocolos.
- Se evita que el tráfico local tenga que dejar el PoP, es decir, el tráfico para el cual los dispositivos fuente y destino se encuentran dentro del mismo PoP no tendrá que salir de él.
- Se disminuye el número de enlaces requeridos desde el PoP.
- En una red MPLS usando conmutación ATM o Frame Relay y unión de etiquetas, se reduce el número de circuitos virtuales requeridos desde el PoP.

Todas las ventajas anteriores, exceptuando el último punto, se aplican a PoPs en redes tradicionales IP con una estructura análoga a la descrita.

El número de LERs requeridos en un PoP depende de:

- El número total de líneas de acceso.
- El ancho de banda total de las líneas de acceso, calculado de la media de su utilización. Por ejemplo, si la suma de los anchos de banda de las líneas de acceso es 1 Gbps, la utilización no debe exceder los 500 Mbps.

Los LSRs sin enlaces de frontera se usan a menudo ya sea como parte de un PoP o como dispositivos independientes. Algunas condiciones específicas para los LSRs del núcleo son:

- El número y tipo de enlaces del núcleo a ser soportados. Esto es más importante para un LSR del núcleo que soporta varios enlaces centrales que para un LER.
- Capacidad de etiquetas. Todos los LSRs basados en etiquetas soportan unión de LSPs a un destino común, pero tal capacidad es menos común para los LSRs con sólo funcionalidades de conmutación.

La red en estudio esta conformada por 6 nodos, de los cuales los tres principales por el volumen de tráfico que manejan son Bogotá, Medellín y Cali. El nodo en Bogotá es el punto más crítico de la red debido al volumen de tráfico que concentra y, a las características e índice de población de la región. Los nodos de Medellín y Cali atiende también un número significativo de usuarios, además de ser puntos de concentración del tráfico para el noroccidente y sur de país respectivamente. Por estas características, el diseño de los PoPs en estos nodos está condicionado por el número de líneas de usuarios por lo tanto la estructura para el PoP consiste de varios LER y un LSR, como en la Figura 5.4. Para los nodos restantes: Armenia, Barranquilla y Cúcuta, es suficiente una estructura de PoP con un LER único para atender el volumen de tráfico generado por los usuarios en esas regiones.

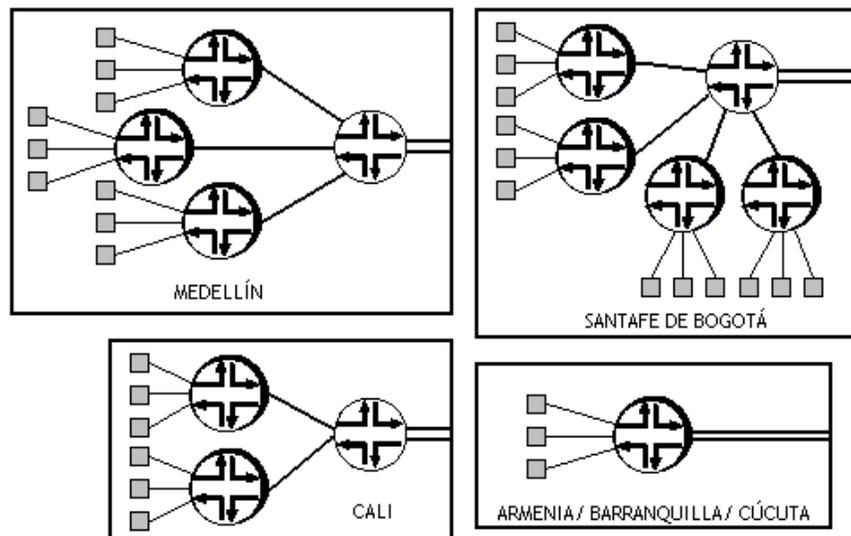


Figura 5.4. Estructura de los PoP.

5.3.2 Dimensionamiento de los Enlaces del Backbone

El proceso de dimensionamiento del ancho de banda de los enlaces en una red MPLS, es el mismo que para una red IP; y su objetivo es definir la capacidad necesaria para satisfacer las demandas actuales y futuras del tráfico. Esto no significa que los resultados del diseño sean los ideales, al contrario, en la etapa final se debe reevaluar y mejorar las características de la red.

Antes de entrar a explicar el proceso de dimensionamiento, vale la pena analizar cualitativamente los fenómenos que se presentan en una red IP debido a las diversas características de clases de tráfico.

Las fuentes generadoras de tráfico en una red tienen en general un comportamiento estocástico, es decir, la carga generada por ellas fluctúa alrededor de un valor (tasa media), y puede llegar hasta un valor máximo (tasa pico). Este hecho hace que el factor de utilización del enlace (y por lo tanto su capacidad efectiva) cambien según la aproximación que se tome para el comportamiento de las fuentes: si se toma su valor medio, el factor de utilización será el máximo y la capacidad efectiva del enlace será igual a su capacidad nominal pero la tasa de pérdida de paquetes será también mayor y por lo tanto no cumplirá con los requerimientos de muchos de los usuarios. Sin embargo, si se toma el peor de los casos (las fuentes transmiten con su tasa pico), el factor de utilización será el menor y la capacidad efectiva del enlace se verá también reducida. Aunque la tasa de pérdida de celdas sea cero en este caso, la aproximación tampoco es válida ya que se da una subutilización de los recursos. Este hecho indica que la capacidad efectiva del enlace se encuentra entre dos límites.

Finalmente, para determinar la capacidad y los tipos de enlaces requeridos, se estima la matriz de tráfico PoP a PoP según la carga y la distribución del tráfico de los usuarios activos de cada uno de ellos. Los pasos a seguir en el dimensionamiento de los enlaces son:

1. Estimación del tráfico desde cada PoP.

Basándose en el ancho de banda total de la línea de acceso, se hace una estimación del tráfico total enviado desde el usuario al PoP, pero esta estimación es para un periodo de tiempo en el cual la red esta muy cargada, lo que asegura un dimensionamiento más adecuado.



Figura 5.5. Anchos de Banda de las Líneas de Acceso.

Para la red en estudio, y teniendo en cuenta las características cambiantes de las fuentes generadoras de tráfico (como se mencionó anteriormente), se estima el total del ancho de banda de la línea de acceso para cada uno de los nodos de la red, como se muestra en la Figura 5.5. Los valores del ancho de banda asignados a cada nodo se estiman de acuerdo a las características de la región (zona industrial, volumen de población, etc.), la cantidad y tipo de usuarios atendidos, y a la experiencia que tenga el diseñador. Sin embargo, el factor de utilización del enlace se establece al 50% del ancho de banda total, cumpliendo con el hecho que la capacidad efectiva del enlace oscila entre los límites de la tasa pico y la tasa media. Por ejemplo para el nodo de Bogotá el ancho de banda estimado es de 1.2 Gbps, por lo tanto el factor de utilización del enlace es de 600 Mbps.

2. Estimación de la Matriz de Tráfico.

El proceso exacto para este paso varia de red a red. Por ejemplo, para la red en estudio, los tres centros principales son Bogotá, Medellín y Cali, donde Bogotá es el mayor de ellos, como se mencionó anteriormente. De acuerdo a las características de la región, a las estimaciones del ancho de banda del paso anterior y a la experiencia del diseñador, se estima un porcentaje de distribución del tráfico entre los nodos que conforman la red. En este caso, se establece que el 46% del porcentaje del tráfico va a Bogotá, el 33% a Medellín, el 17% a Cali, el 1% a Barranquilla, 1.5% a Cúcuta y el 1.5% a Armenia. Con los porcentajes de distribución y el factor de utilización del enlace, se calcula la matriz de tráfico de PoP a PoP que se muestra en la Tabla 5.1.

DESTINO DEL TRÁFICO	PORCENTAJE DE DISTRIBUCIÓN	FUENTE DEL TRÁFICO (Valores dados en Mbps)					
		BOGOTÁ	MEDELLÍN	CALI	ARMENIA	CÚCUTA	BARRANQUILLA
BOGOTÁ	46%	276	207	184	69	69	46
MEDELLÍN	33%	198	148.5	132	49.5	49.5	33
CALI	17%	102	76.5	68	25.5	25.5	17
ARMENIA	1.5%	9	6.75	6	2.25	2.25	1.5
CÚCUTA	1.5%	9	6.75	6	2.25	2.25	1.5
BARRANQUILLA	1%	6	4.5	4	1.5	1.5	1
	100%	600	450	400	150	150	100

Tabla 5.1. Matriz de Tráfico Unidireccional.

3. Flujos del tráfico bidireccional.

En las redes IP, el tráfico desde X a Y fluye por el mismo trayecto (pero en dirección inversa) que el tráfico Y a X. Aunque esta característica no es tenida en cuenta por la mayoría de los protocolos de enrutamiento, es útil usarla en el diseño inicial de la red.

La matriz de los flujos bidireccionales se determina eligiendo el mayor ancho de banda de los tráficos unidireccionales del enlace. Por ejemplo, el ancho de banda del tráfico bidireccional entre Bogotá y Medellín es 207 Mbps (Tabla 5.2), que es el mayor valor de ancho de banda unidireccional entre Bogotá-Medellín (207Mbps) y Medellín-Bogotá (198Mbps).

	BOGOTÁ	MEDELLÍN	CALI	ARMENIA	CÚCUTA	BARRANQUILLA
BOGOTÁ	276	207	184	69	69	46
MEDELLÍN		148.5	132	49.5	49.5	33
CALI			6.8	25.5	25.5	17
ARMENIA				2.25	2.25	1.5
CÚCUTA					2.25	1.5
BARRANQUILLA						1

Tabla 5.2. Matriz de Tráfico Bidireccional.

4. Estimación de los Flujos del Enlace

Este paso involucra el cálculo de los trayectos que seguirá el tráfico a través del backbone de la red. Con los protocolos de enrutamiento IP (OSPF, IS-IS), el cálculo de los trayectos es un proceso sencillo, porque el tráfico sigue aquellos que tienen un número mínimo de saltos, y cuando hay dos o más que cumplen con esta característica, el tráfico se distribuye a través de ellos.

Para determinar la capacidad total de los enlaces, se toma uno de los nodos de la red, se determina el camino más corto hacia cada uno de los posibles PoP destino y se asigna el ancho de banda indicado en la matriz de tráfico bidireccional (Tabla 5.2) a los enlaces que conforman las rutas. Por ejemplo, para transmitir tráfico desde Armenia hasta Barranquilla, la ruta con menor número de saltos es Armenia-Medellín-Barranquilla, por consiguiente, a los enlaces Armenia-Medellín y Medellín-Barranquilla, se les asigna el ancho de banda, 1.5Mbps, indicado en la Tabla 5.2. En caso de que exista mas de un trayecto con el mínimo número de saltos hacia el destino, el ancho de banda se divide equitativamente entre el número de dichos caminos. Por ejemplo para ir de Bogotá a Barranquilla hay dos caminos con el mismo número de saltos: Bogotá-Medellín-Barranquilla y Bogotá-Cúcuta-Barranquilla. El ancho de banda Bogotá-Barranquilla es 46 Mbps, por lo tanto se asigna a cada uno de las rutas hacia Barranquilla $\frac{46}{2} Mbps$. Este proceso se repite para todos los nodos que conforman la red.

Finalmente se hace la suma de los flujos de tráfico que transitan por cada uno de los enlaces. El resultado de esa suma indicará la capacidad del enlace. En la Figura 5.6 se ilustra el proceso completo para el tráfico de la Tabla 5.2.



Figura 5.6. Proceso de Cálculo de los Enlaces.

5. Asignación de la capacidad del enlace.

Basándose en las estimaciones del paso anterior, se asigna la capacidad de los enlaces de la red, esto generalmente involucra la elección de los tipos de enlace (T3/E3, SMT_1, etc.), que son superiores al ancho de banda calculado. En la Figura 5.7, se ilustran los resultados finales del proceso de dimensionamiento de la capacidad de los enlaces. Se debe tener en cuenta que la capacidad de los enlaces obtenidos no es definitiva y será optimizada a través del diseño, pues como se puede observar en la figura existen incompatibilidades entre los enlaces STM y E3.

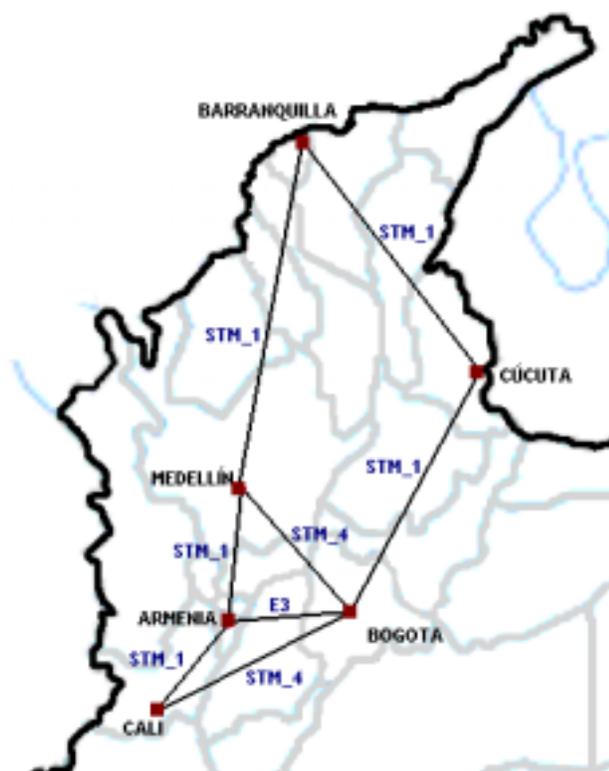


Figura 5.7. Ancho de Banda Total de los Enlaces.

En la Tabla 5.3 se resume las capacidades de los enlaces calculadas y los asignadas.

ENLACE	VALOR ESTIMADO (Mbps)	VALOR ASIGNADO
Armenia-Bogotá	71.25	E3
Armenia-Medellín	125.5	STM_1
Bogotá-Cúcuta	148.75	STM_1
Bogotá-Medellín	286.75	STM_4
Cali-Armenia	100	STM_1
Cali-Bogotá	284	STM_1
Cúcuta-Barranquilla	53.5	STM_1
Medellín-Barranquilla	95	STM_1

Tabla 5.3. Capacidades Estimadas y Asignadas de los Enlaces.

5.3.3 Diseño del Enrutamiento IP

MPLS usa los algoritmos de enrutamiento IP para conocer toda la topología de la red y para determinar las rutas del tráfico. El componente de control de cada LSR usa estos protocolos de la misma manera como lo hacen los enrutadores IP, para intercambiar información de

enrutamiento entre ellos. Como consecuencia, OSPF ó IS-IS ven a la red MPLS exactamente igual que una red IP, bajo la perspectiva de tres puntos de vista:

1. Físico: Representa los dispositivos y enlaces físicos de la red. En la Figura 5.8 se presenta la infraestructura física de la red en estudio.

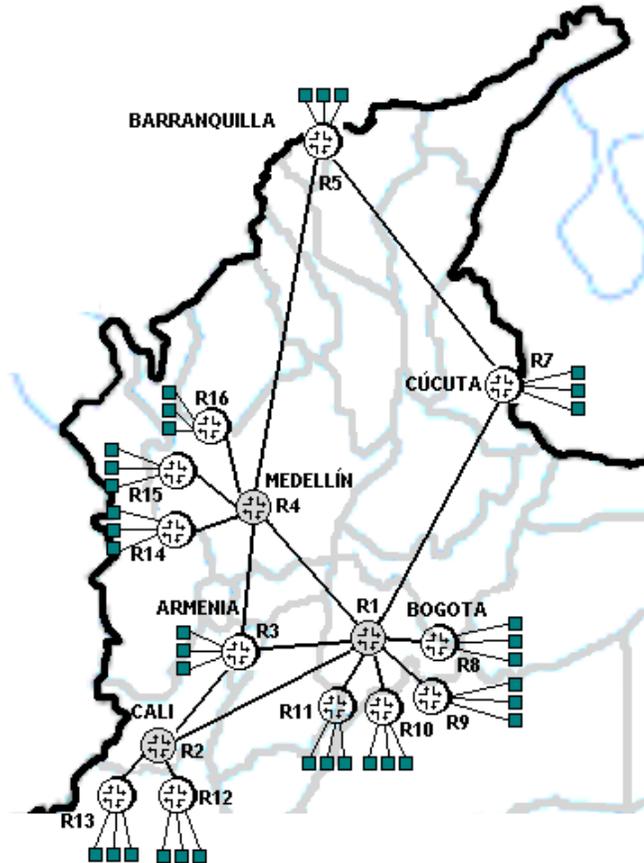


Figura 5.8. Punto de Vista Físico.

2. Funcional: Si un elemento tiene varias funciones, estas se pueden mostrar separadamente. Por ejemplo, si analizamos los LERs del dominio, estos cumplen con las funciones de conmutación de circuito virtual permanente que pueden separarse funcionalmente de las funciones de conmutación MPLS. En la Figura 5.9 se ilustra la topología de una sección de la red Colombiana.

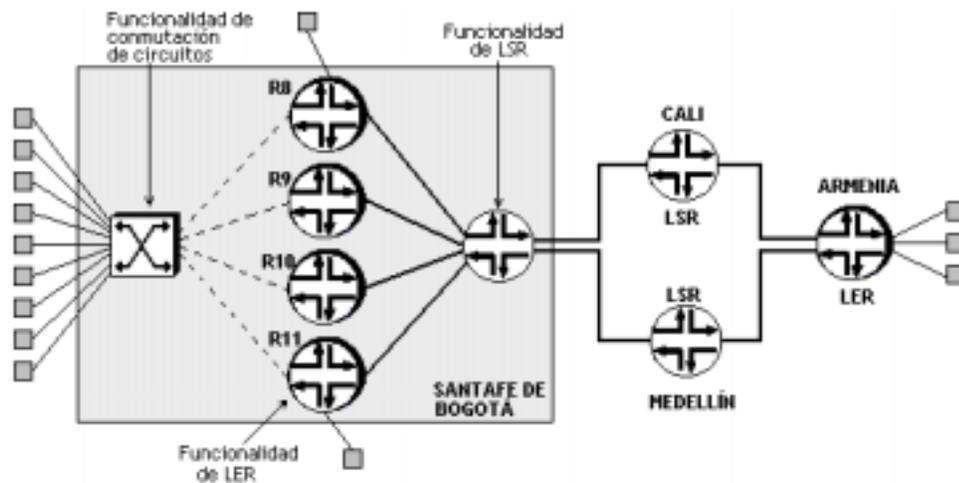


Figura 5.9. Punto de Vista Funcional.

3. Enrutamiento: Presenta la red tal como la ve el protocolo de enrutamiento IP y esta representación se deriva del punto de vista funcional de la siguiente forma:

- Las funciones de circuito virtual permanente son invisibles para el enrutamiento IP. Si un usuario está conectado a un enrutador por un circuito virtual permanente, el circuito virtual es visto por el enrutamiento IP como una conexión directa y los nodos son considerados como enrutadores adyacentes.
- Las funcionalidades de la frontera y del núcleo de la red (LER y LSR respectivamente) son considerados como enrutadores desde este punto de vista.

Usando estas reglas, el punto de vista de enrutamiento del segmento de la red en cuestión es como el que se muestra en la Figura 5.10.

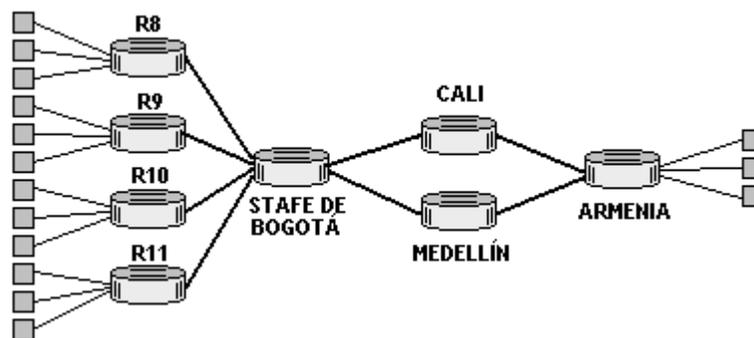


Figura 5.10. Punto de Vista de Enrutamiento.

Hay un número de consideraciones a tener en cuenta en el momento de elegir un protocolo de enrutamiento IP para una red MPLS:

- Específicamente, la ingeniería de tráfico MPLS usa enrutamiento junto con la reservación de recursos y por lo tanto requiere de protocolos de estado de enlace para distribuir información de la carga de tráfico en los enlaces. Los protocolos de vector distancia no pueden ser soportados por TE-MPLS.
- Algunos protocolos IP permiten implementar enlaces no numerados (enlaces sin dirección IP) para propósitos de enrutamiento. El uso de enlaces IP no numerados reduce el número de prefijos de destinos conocidos por los LERs y reduce la cantidad de etiquetas usadas en la red.

Considerando estas especificaciones y las características de los protocolos de enrutamiento IP (ya estudiadas en capítulos anteriores) se elige el algoritmo convencional OSPF por sus características de robustez y estabilidad, que permiten detectar y propagar cambios de topología y de tráfico rápidamente, estableciendo rutas libres de loops. A continuación se ilustra de forma parcial el proceso realizado por el algoritmo OSPF para el descubrimiento de la topología de la red.

Para determinar las rutas a los destinos, OSPF utiliza los costos de los enlaces de la red. Como se mencionó en capítulos anteriores, los costos son asignados administrativamente y dependen de criterios como el número de saltos, el ancho de banda del enlace, la tecnología de la red, etc. Para la red en estudio, los costos de los enlaces han sido definidos según la capacidad de los mismos con el fin de distribuir el tráfico uniformemente (Figura 5.11).

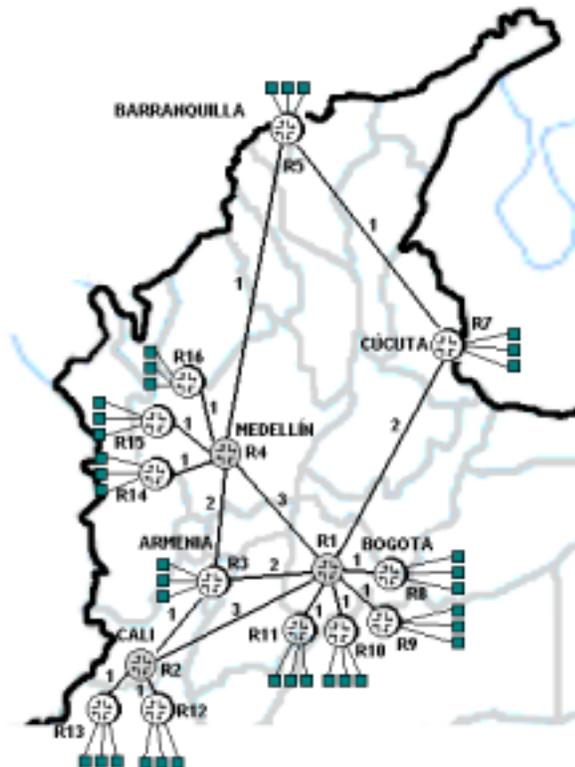


Figura 5.11. Costos de los Enlaces de la Red Colombiana.

El proceso inicia con la inundación de los anuncios de estado de enlace entre todos los enrutadores que conforman la red. Gracias a éstos anuncios, cada enrutador tendrá conocimiento de sus enrutadores adyacentes y el costo de los enlaces que lo conectan a ellos; a partir de esta información se crea la base de datos de estado de enlace. Para la red en estudio, las bases de datos de los enrutadores R1 (Bogotá), R2 (Cali), R4 (Medellín) se muestran en las tablas 5.4.a ,5.4.b y 5.4.c respectivamente.

R1 - Bogotá	
Adyacencia	Costo
R2	3
R3	2
R4	3
R7	2
R8	1
R9	1
R10	1
R11	1

Tabla 5.4.a

R2 - Cali	
Adyacencia	Costo
R1	3
R3	1
R12	1
R13	1

Tabla 5.4.b

R4 - Medellín	
Adyacencia	Costo
R1	2
R3	2
R5	1
R14	1
R15	1
R16	1

Tabla 5.4.c

Tabla 5.4. Bases de Datos de Estado de Enlace para R1, R2, y R4.

Una vez establecidas las bases de datos se aplica el algoritmo Dijkstra para calcular el árbol SPF y así conocer los trayectos de menor costo a cada uno de los posibles destinos. En la Tabla 5.5 y en la Figura 5.12 se muestra un ejemplo para el enrutador R1.

ENRUTADOR DE ORIGEN		SIGUIENTE SALTO		ENRUTADOR DESTINO	COSTO
R1	→			R1	(costo=0)
R1	→			R2	(costo=3)
R1	→			R3	(costo=2)
R1	→			R4	(costo=3)
R1	→	R7	→	R5	(costo=3)
R1	→			R7	(costo=2)
R1	→			R8	(costo=1)
R1	→			R9	(costo=1)
R1	→			R10	(costo=1)
R1	→			R11	(costo=1)
R1	→	R2	→	R12	(costo=4)
R1	→	R2	→	R13	(costo=4)
R1	→	R4	→	R14	(costo=4)
R1	→	R4	→	R15	(costo=4)
R1	→	R4	→	R16	(costo=4)

Tabla 5.5. Tabla de los Trayectos más Cortos.

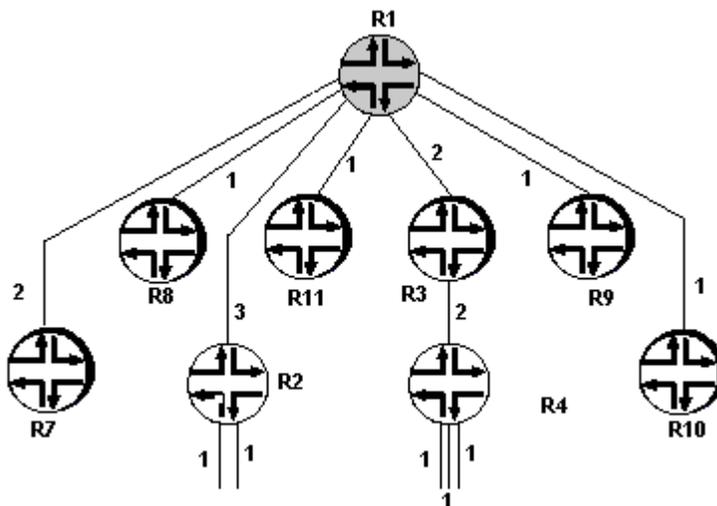


Figura 5.12. Árbol SPF.

Finalmente, a partir del árbol SPF se genera la tabla de enrutamiento, que se muestra en la Tabla 5.6.

DESTINO	CAMINO	COSTO
R2	R2	3
R3	R3	2
R4	R4	3
R5	R7	3
R7	R7	2
R8	R8	1
R9	R9	1
R10	R10	1
R11	R11	1
R12	R2	4
R13	R2	4
R14	R4	4
R15	R4	4
R16	R4	4

Tabla 5.6. Tabla de Enrutamiento para R1.

Este proceso es igual para todos los nodos, y los resultados obtenidos son utilizados por MPLS para conocer la topología de la red, más no para tomar las decisiones de enrutamiento.

5.3.4 Dimensionamiento del Espacio de las Etiquetas MPLS

Una parte importante en el diseño de las redes MPLS es el cálculo de los requerimientos de los espacios de etiquetas sobre cada enlace. En una red MPLS enrutada salto por salto las etiquetas se utilizan para identificar los prefijos de dirección IP conocidos, para lo cual se construye una tabla de enrutamiento con la ayuda de los protocolos de nivel 3, la cual contiene la lista de prefijos de destino conocidos en el área de enrutamiento.

El número de etiquetas requerido depende de:

- El número de destinos IP en la red.
- La relación entre destinos y etiquetas.
- El uso de unión de etiquetas.
- Los trayectos escogidos por el enrutamiento IP.
- Clases de servicio que la red prestará.

Muchos LSRs soportan unión de etiquetas, permitiendo que los LSPs que tienen el mismo destino puedan unirse en un LSR específico, de modo que sólo una etiqueta identifique los enlaces a ese destino. En las redes que usan unión de etiquetas existe un límite sobre el número de etiquetas activas requerido por enlace, el límite es $c*d$, donde c es el número de clases de servicio usadas en la red y d es el número de prefijos de destino en la red. El valor por defecto de c es 1, a menos que se requieran distintas etiquetas para múltiples clases de servicios, en cuyo caso típicamente será de 2 a 5.

Una vez los requerimientos de espacio de etiquetas han sido analizados, estos deben compararse a las capacidades de los equipos de la red y determinar si éstos pueden soportar ese rango de etiquetas.

Para verificar que exista un número suficiente de etiquetas en un LER se analizan las siguientes situaciones y se escoge la más apropiada para el caso de diseño específico:

Dispositivo	Situación	Parámetro Clave	Ecuación
LER	La red usa unión de LSPs	Número de LSPs activos soportados por enlace	$I \leq cd$
LER	La red no usa unión de LSPs; hay un prefijo por cada LSR o LER. No hay enrutadores fuera del área.	Número de LSPs activos soportados por enlace	$I \leq c(d-d_c) + cnd_c$
LER	La red no usa unión de LSPs; todas las otras situaciones se aplican.	Número de LSPs activos soportados por enlace	$I < 2cn$

Donde I = número de etiquetas soportado.

d_c = número de destinos alcanzables a través de un LER.

n = número de LERs en el área.

Para la red colombiana en estudio, se usa unión de etiquetas y una clase de servicio ($c = 1$, mejor esfuerzo). Usando un LER de la Serie 7200 de CISCO que soporta $I = 4096$ etiquetas, y sustituyendo esto en la ecuación $I \leq cd$, se tiene:

$$4096 \leq 1d$$

$$4096 \leq d$$

Esto significa que se garantizan 4069 prefijos de dirección a ser soportados en el área.

Para el caso de los LSRs que soportan unión de LSPs, habrá al menos una etiqueta por destino sobre cada enlace, y los LSRs sin unión de LSPs pueden tener muchos trayectos por destino sobre cada enlace. Para verificar que exista un número suficiente de etiquetas se considera:

Dispositivo	Parámetro clave	Ecuación
LSRs con unión de LSPs	1. Número de LSPs activos soportados por enlace.	$I < cd$
	2. Número de unión de etiquetas soportada por enrutador o por puerto.	$m < cd(k-1)$
LSRs sin unión de LSPs	Hay un prefijo de destino para el LSR o LER, y no hay enrutadores fuera del área	$L \leq c(n^2/2)$

Donde: m = número de etiquetas unidas en el enrutador.

K = número de enlaces en el enrutador.

n = número total de LER en el área.

Para la red en estudio, la cual soporta 1 clase de servicio y usa un LSR 8650 de CISCO con 4 puertos ($k = 4$), una tarjeta activa de 32 Kbps y cuya capacidad m es 32768 (estos datos son suministrados por el proveedor de equipos), tenemos :

$$I < cd$$

$$32768 < 1d$$

$$32768 < d$$

$$m < cd (k-1)$$

$$32768 < 1d(4-1)$$

$$10922 < d$$

Lo cual significa que existen 10922 prefijos de dirección en el área.

En este punto del diseño se tiene una red MPLS con capacidades básicas, donde se han definido los dispositivos físicos a utilizar y los rangos de etiquetas que soportará cada uno de los enrutadores. Con ésta información y la tabla de enrutamiento IP se pueden definir las LIB que usaría cada enrutador. Por ejemplo, para el caso de R1 (Bogotá) su LIB resultante es como se muestra en la Tabla 5.7.

Tabla Enrutamiento			Tabla de Etiquetas			
FEC	Próximo salto	Puerto salida	Entrante		Saliente	
			Etiqueta	Puerto	Etiqueta	Puerto
20.0.x.x	R2	2	809	9	874	45
30.0.x.x	R3	76	959	25	954	24
40.0.x.x	R4	52	963	15	852	14
50.0.x.x	R5	32	847	97	974	18
70.0.x.x	R7	165	947	54	873	95
80.0.x.x	R8	364	854	964	1001	57
⋮	⋮	⋮	⋮	⋮	⋮	⋮

Tabla 5.7. LIB para R1.

El diseño obtenido hasta este momento no es el más óptimo, pues es una infraestructura poco tolerante a fallas y no es muy confiable para la prestación de servicios diferenciados. Si se observa el diseño físico de la red, notará que hay enlaces cuya capacidad no es suficiente para soportar el volumen de tráfico que circularía por él si se presenta una falla en cualquiera de los enlaces o nodos adyacentes, como es el caso del enlace entre Armenia y Bogotá, cuyo enlace es un E3.

Para solucionar estos inconvenientes, en los siguientes pasos del diseño se introducen las funcionalidades de TE y QoS que ofrece la tecnología MPLS.

5.3.5 Diseño del Sistema TE-MPLS para Soporte de QoS

En esta sección se describen las características y pasos a tener en cuenta al introducir aplicaciones como ingeniería de tráfico y calidad de servicio en un dominio MPLS:

1. Alcance geográfico del sistema TE-MPLS y enrutadores participantes.

El alcance geográfico del sistema TE-MPLS es una decisión administrativa y también depende de las características de desempeño de la red. Si un área de la red no tiene la capacidad suficiente para satisfacer la demanda, entonces debe ser incluida dentro del diseño del sistema TE-MPLS .

Por otro lado, la elección de los enrutadores que van a ser parte del sistema TE-MPLS depende de factores como confiabilidad, capacidad de memoria, poder de procesamiento, etc. Es importante tener en cuenta que a mayor número de LERs de entrada y salida, se requerirá un mayor número de LSPs, incrementando la complejidad en los procesos de enrutamiento. Si el ancho de banda de estos LSPs es una cantidad promedio, el enrutamiento restringido tendrá más facilidad de manejar dichos LSPs.

Para el ejemplo que se está siguiendo, el sistema TE-MPLS se implementará en todo el dominio de la red donde los LERs y los LSRs se les adicionarán las capacidades de TE necesarias para cumplir con los objetivos de desempeño.

2. Jerarquía del sistema TE-MPLS

Una vez elegidos los enrutadores que harán parte del sistema TE-MPLS, se decide la jerarquía en el dominio. Una alternativa es una topología con todos los LSRs formando una malla en la cual todos tienen la misma jerarquía. En los casos en que la red sea muy extensa esta aproximación sería muy costosa de implementar y se recomienda el uso de una topología combinada, que divida la red en varias regiones cada una con su propia topología. Este diseño reduce el número de LSPs en la red y por ende se reduce la complejidad del enrutamiento, costos de implementación, etc.

Para nuestro ejemplo, el sistema de ingeniería de tráfico tiene una topología combinada, en la cual los nodos principales son Bogotá, Medellín y Cali.

3. Diseño del backbone de TE-MPLS.

El objetivo de introducir un sistema de TE-MPLS con soporte para QoS es optimizar los recursos de la red y garantizar la continuidad de los servicios y los niveles de QoS en cada clase. Para cumplir con este objetivo se provee un nivel de redundancia aceptable (a nivel de red y de troncales) para contar con múltiples trayectos hacia cada destino.

En el ejemplo se introduce un LSR (en Bucaramanga, departamento de Santander) por contar con la infraestructura necesaria para el soporte de dicho dispositivo, además de ser un punto intermedio entre las ciudades de Bogotá, Medellín, Barranquilla y Cúcuta. Este enrutador provee un mayor número de trayectos alternos, evitando redundancia de troncales y disminuyendo los costos al permitir implementar las capacidades de enrutamiento que provee MPLS.

Como consecuencia de la distribución geográfica, configuración física y al alto nivel de tráfico transportado a través de los enlaces Medellín - Bogotá y Cali - Bogotá, se introducen enlaces redundantes en estos trayectos para garantizar la continuidad del servicio en caso de que uno de ellos falle.

En la Figura 5.13 se puede observar la nueva topología de la red.

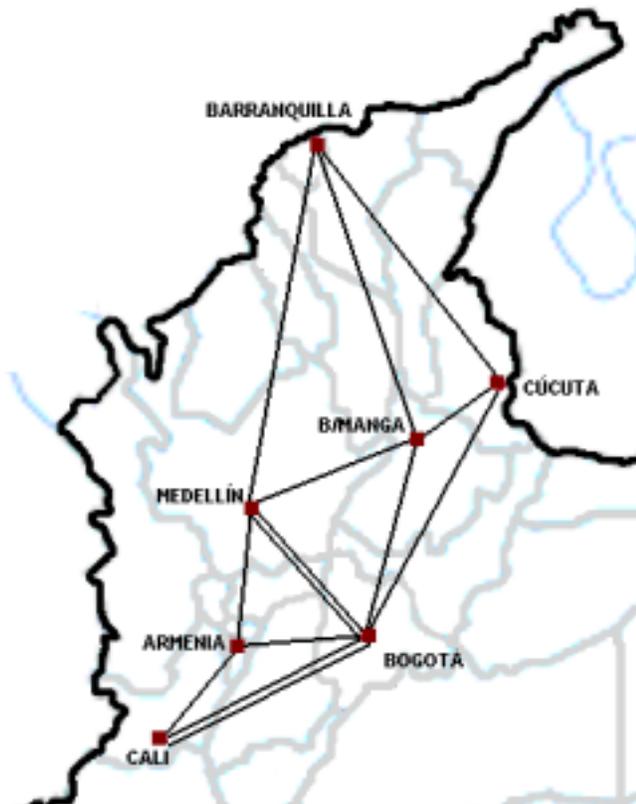


Figura 5.13. Topología de Red MPLS.

- Requerimientos de Ancho de Banda de los LSPs.

Para asegurar que haya suficiente capacidad en la red y se puedan tratar fallas en los enlaces, cumplir con los objetivos de desempeño de ingeniería de tráfico, con las restricciones de QoS acordadas y con futuras demandas; es necesario ajustar la capacidad del ancho de banda de los enlaces inicialmente establecidos.

Antes de definir las nuevas capacidades de los enlaces, se debe tener en cuenta que el propósito de ésta red MPLS es ofrecer varias clases de servicio, las cuales tienen requerimientos de ancho de banda específicos. Estos requerimientos se definen en los Acuerdos de Nivel de Servicio y se determinan de acuerdo a la proporción del número de nodos y servidores de cada sitio de usuario.

En éste ejemplo la red prestará tres clases de servicios: mejor esfuerzo, premium y asegurado. Una posible manera de contratación del ancho de banda para cada una de estas clases de servicio es:

- Los primeros 50 Kbps es para el Servicio Asegurado.
- Los siguientes 32 Kbps son para el Servicio Premium.
- El restante es utilizado para transportar tráfico del Mejor Esfuerzo.

Con base a éstos valores y a la matriz de tráfico bidireccional (Tabla 5.2), se ajusta el ancho de banda asignado a los enlaces siguiendo el mismo proceso realizado en la sección Dimensionamiento de los enlaces del backbone (numeral 5.3.2), en la parte de estimación de los flujos del enlace. Los resultados de este procedimiento se muestran en la Figura 5.14.

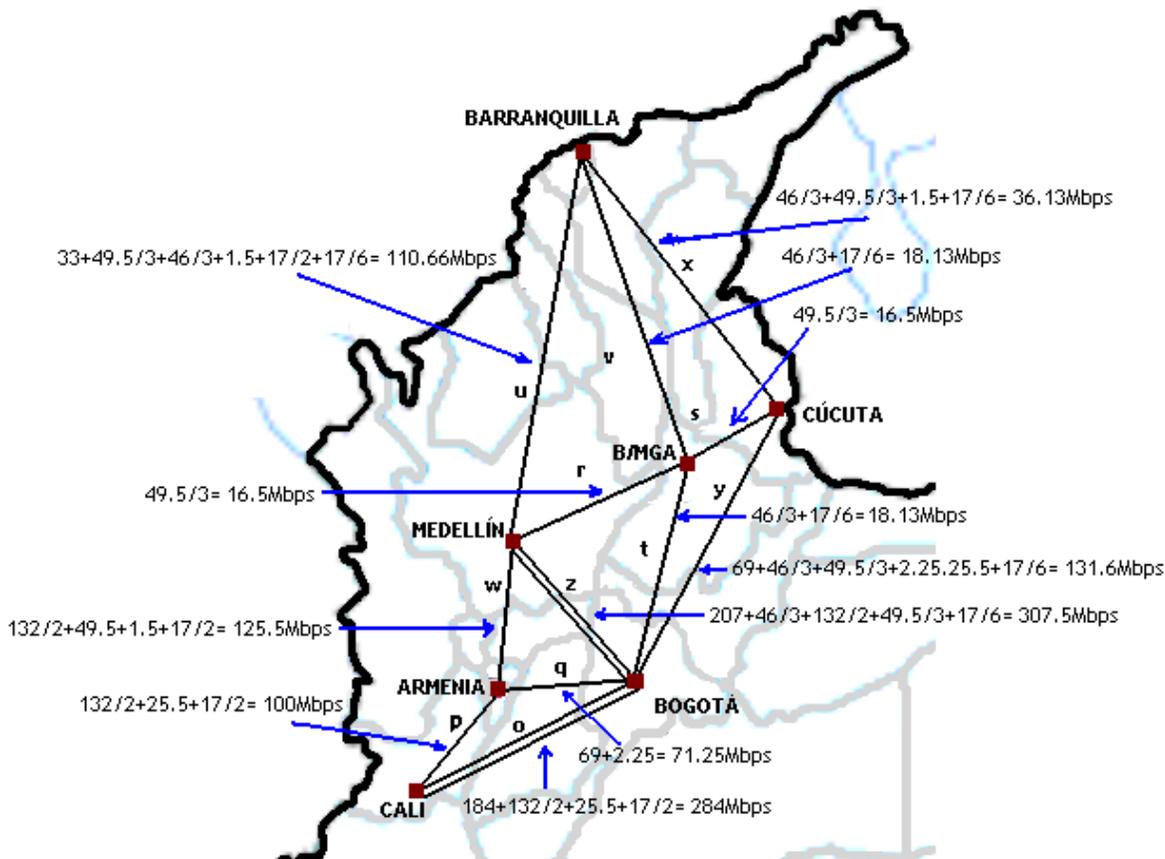


Figura 5.14. Reajuste de los Anchos de Banda de los Enlaces.

La Figura 5.15 muestra los anchos de banda totales después del reajuste.

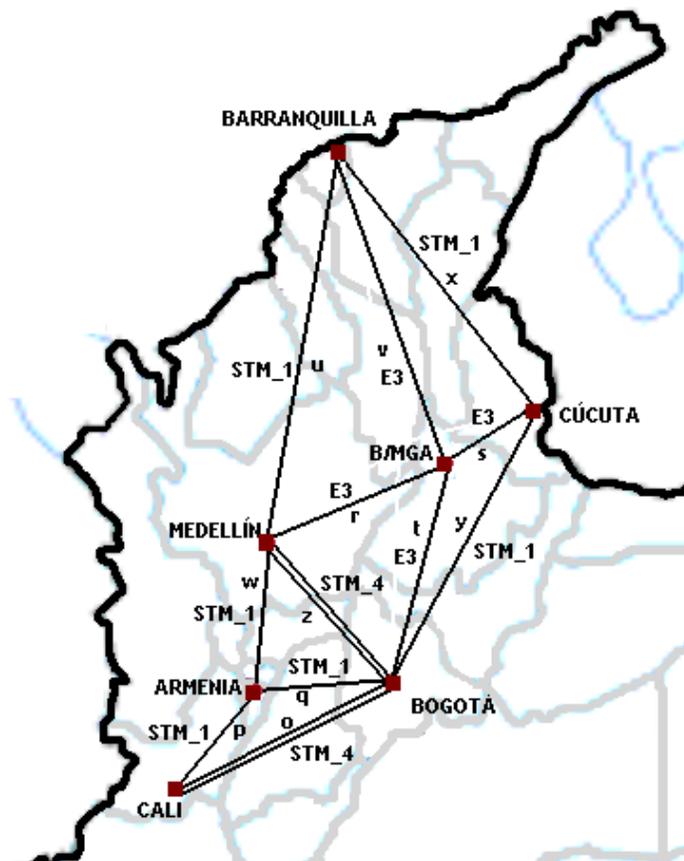


Figura 5.15. Anchos de Banda Totales de los Enlaces después del Reajuste.

En la Tabla 5.8 se resume la capacidad de los enlaces estimada y asignada.

ENLACE	VALOR ESTIMADO (Mbps)	VALOR ASIGNADO
Armenia-Bogotá	71.25	STM_1
Armenia-Medellín	125.5	STM_1
Barranquilla-Bucaramanga	18.13	E3
Bogotá-Bucaramanga	18.13	E3
Bogotá-Cúcuta	131.6	STM_1
Bogotá-Medellín	307.5	STM_4
Cali-Armenia	100	STM_1
Cali-Bogotá	284	STM_4
Cúcuta-Barranquilla	36.13	STM_1
Cúcuta-Bucaramanga	18.13	E3
Medellín-Barranquilla	110.66	STM_1
Medellín-Bucaramanga	16.5	E3

Tabla 5.8. Capacidades Estimadas y Asignadas.

Existen enlaces que no soportarían una carga de tráfico alta y por lo cual se debe incrementar su capacidad y de esta manera asegurar que la red responda adecuadamente a cualquier tipo de anomalía. Por ejemplo, si el enlace u (STM_1) entre Medellín y Barranquilla falla, los

enlaces r (E3) y v (E3) tendrán que transportar todo o una gran parte del tráfico afectado. La carga de éstos enlaces puede exceder la tasa de E3 y por tanto se requieren SMT_1 en los enlaces r y v . Similarmente, si el enlace y falla los enlaces s y t requerirán una capacidad mayor a E3. La asignación final de los anchos de banda se observa en la Figura 5.16.

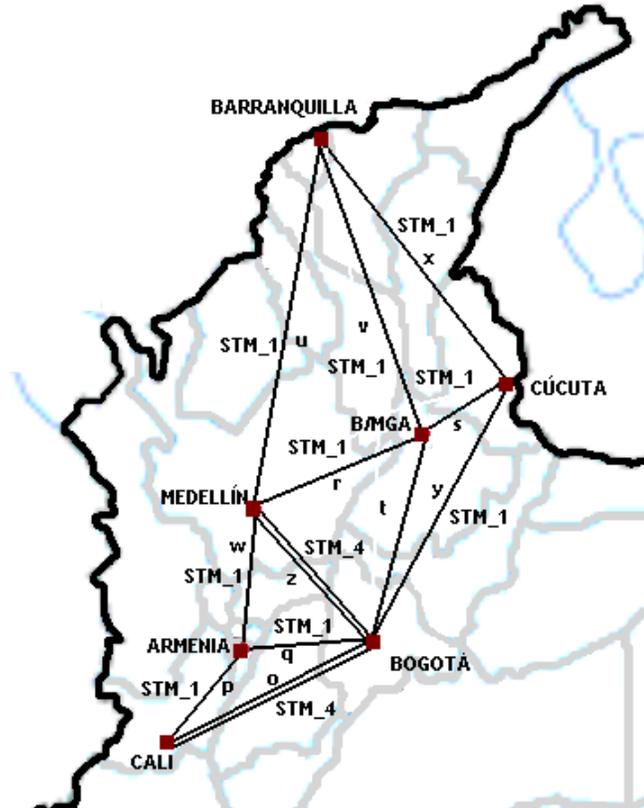


Figura 5.16. Asignación Final de los Anchos de Banda.

4. Verificación de los equipos de red

Por las nuevas características y funcionalidades adicionadas a la red, es indispensable verificar que los equipos seleccionados anteriormente cumplan con estas nuevas especificaciones. Se repite el proceso de dimensionamiento del espacio de las etiquetas MPLS (numeral 5.3.4).

Para la red colombiana en estudio, se usa unión de etiquetas y tres clases de servicio ($c = 3$, mejor esfuerzo, premium y garantizado) y usando el LER de la Serie 7200 de CISCO que soporta $l=4096$ etiquetas, y sustituyendo esto en la ecuación $l \leq cd$, se tiene:

$$4096 \leq 3d$$

$$1365 \leq d$$

Esto significa que se garantizan 1365 prefijos de dirección a ser soportados en el área.

Usando el LSR 8650 de CISCO con 4 puertos ($k = 4$), una tarjeta activa de 32 Kbps y cuya capacidad m es 32768 (estos datos son suministrados por el proveedor de equipos), tenemos :

$$\begin{aligned}l &< cd \\ 32768 &< 3d \\ 10922 &< d\end{aligned}$$

$$\begin{aligned}m &< cd (k-1) \\ 32768 &< 3d(4-1) \\ 5461 &< d\end{aligned}$$

Lo cual significa que existen 5461 prefijos de dirección en el área.

Estos valores indican que los LERs y LSRs definidos en pasos anteriores son adecuados para la implementación de TE-MPLS.

5. Modificaciones en el enrutamiento

Con la nueva topología de la red, el enrutamiento IP debe actualizarse para adaptarse a los cambios realizados en la infraestructura física de la red. Para los enlaces adicionales se definen sus costos y a partir de ellos se repite el proceso de obtención de la tabla de enrutamiento IP. La Figura 5.17 muestra el mapa con los costos adicionales y la Tabla 5.9 muestra la tabla de enrutamiento IP resultante para el enrutador R1 (Bogotá).

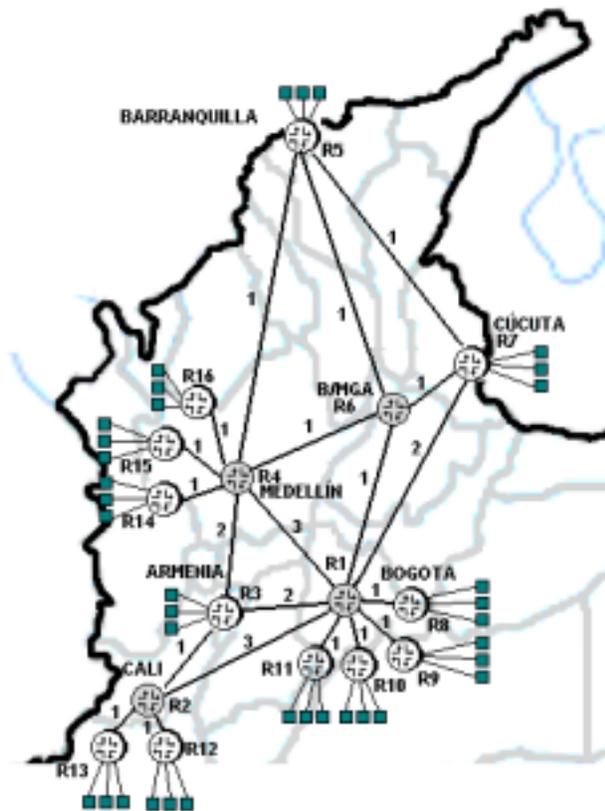


Figura 5.17. Costos Totales.

DESTINO	CAMINO	COSTO
R2	R2	3
R3	R3	2
R4	R4	3
R5	R6	2
R6	R6	1
R7	R7	2
R8	R8	1
R9	R9	1
R10	R10	1
R11	R11	1
R12	R2	4
R13	R2	4
R14	R6	3
R15	R6	3
R16	R6	3

Tabla 5.9. Tabla Final de Enrutamiento IP.

Para prestar las funcionalidades de ingeniería de tráfico, MPLS usa CR para tomar las decisiones de enrutamiento, basándose en la descripción del tráfico y en un conjunto de

restricciones, derivado de los atributos asociados con la demanda de la red y la información local.

El enrutamiento restringido es un mecanismo de control con un conjunto de factores complejos que influyen en sus características de diseño. No todos los factores involucrados en el diseño son controlados por el diseñador, por ejemplo, los factores de demanda y topología de la red son generalmente derivados de otros procesos. Los factores característicos en el diseño de CRs son los siguientes:

- Tipo de restricciones. Con el fin de simplificar los procesos de enrutamiento, el número y tipo de restricciones consideradas para el cálculo de los trayectos es limitado, por ejemplo, el cálculo basado en dos o más métricas adaptativas/multiplicativas (retardo, número de saltos, probabilidad de pérdidas, jitter, etc.) es complejo, además estas métricas son difíciles de determinar con los IGP y son muy cambiantes lo cual conduce a estados inestables de la red. Por estas razones y con el propósito de reducir costos y optimizar los recursos se elige las métricas de TE (número de saltos y métricas IGP), capacidad de enlace (ancho de banda reservable y reservado por cada clase de servicio), la clase de los recursos y el color de los enlaces, como las restricciones a tener en cuenta en la selección de los trayectos.
- Tamaño y estructura de la tabla de enrutamiento. La estructura y tamaño de la tabla de enrutamiento depende directamente de la granularidad y métricas para calcular las rutas. Lógicamente, la tabla es vista como una matriz de dos dimensiones. El número de filas es determinado por la granularidad de enrutamiento y el número de columnas es determinado por las métricas. Por ejemplo, en el enrutamiento basado en el destino con restricciones de ancho de banda y número de saltos, la tabla es organizada como una matriz $K \times H$, donde K es el número de destinos, y H es el número máximo de saltos permitidos para cualquier ruta. La entrada (k,h) contiene uno o más rutas con h saltos para un destino k . Cada ruta también tiene un ancho de banda disponible asociado con él.

Obviamente, el tamaño de una tabla de CR puede ser de mayor tamaño que la de un enrutamiento normal para una misma red. Esto introduce una sobrecarga de almacenamiento e incrementa el tiempo de consulta.

En la red colombiana, para reducir el tamaño de la tabla de enrutamiento CR se tiene en cuenta:

- Usar granularidad de enrutamiento gruesa.
- Usar la cuantización de saltos, dividiendo todos los valores del número de saltos en pocas clases para reducir el número de columnas en la tabla de enrutamiento.

Conforme a la nueva topología de la red y a las características del enrutamiento CR, la estructura de la LIB de MPLS para R1 se define como se muestra en la Tabla 5.10.

Tabla Enrutamiento			Tabla de Etiquetas					
FEC	Próximo salto	Puerto Salida	Entrante		Saliente			
			Etiqueta	Puerto	Etiqueta Asegurado	Etiqueta Premium	Etiqueta Mejor Esfuerzo	Puerto
20.0.x.x	R2	2	809	9	874	923	964	45
30.0.x.x	R3	76	959	25	954	855	937	24
40.0.x.x	R4	52	963	15	852	964	831	14
50.0.x.x	R5	32	847	97	974	811	977	18
60.0.x.x	R6	28	817	53	970	815	999	34
60.0.x.x	R7	165	947	54	873	965	987	95
70.0.x.x	R8	364	854	964	1001	1005	1030	57
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮

Tabla 5.10. LIB de MPLS.

- Distribución de la información de estado de enlace. Para distribuir la información de disponibilidad se extienden los Anuncios de Estado de Enlace (LSA) del protocolo OSPF. A causa de los frecuentes cambios en el ancho de banda residual, se realiza una elección entre tener información actualizada o la necesidad de evitar la frecuencia de propagación de LSAs. Para reducir la frecuencia de propagación de los LSAs, los cambios de ancho de banda disponible se anuncian sólo cuando son significantes (más del 50% ó más de 10 Mbps) ó se define un tiempo de espera usado como límite para la frecuencia de tales anuncios; el valor de tiempo recomendado es 30 segundos.

6. Configuración del sistema de gestión de fallas

Este sistema TE-MPLS facilita los procesos de recuperación de fallas, lo que garantiza la continuidad del servicio y hace más robustos los procesos de enrutamiento. Para el ejemplo de la red colombiana se define una infraestructura de recuperación de fallas que consiste de la combinación de modelos de la conmutación protegida y del reenrutamiento rápido. Este modelo de recuperación se desempeña a nivel local (enlace y nodo) y a nivel global. Por ejemplo, en caso que el R3 (nodo en Armenia) falle, se define un LSP backup constituido por los enlaces **o** y **z** para transmitir el tráfico desde Cali a Medellín, como se muestra en la Figura 5.18. Si el enlace **y** falla, el tráfico de Bogotá a Cúcuta se transmitirá por el LSP backup conformado por los enlaces **t** y **s** (Figura 5.19).



Figura 5.18. Recuperación de Fallas de Nodo.

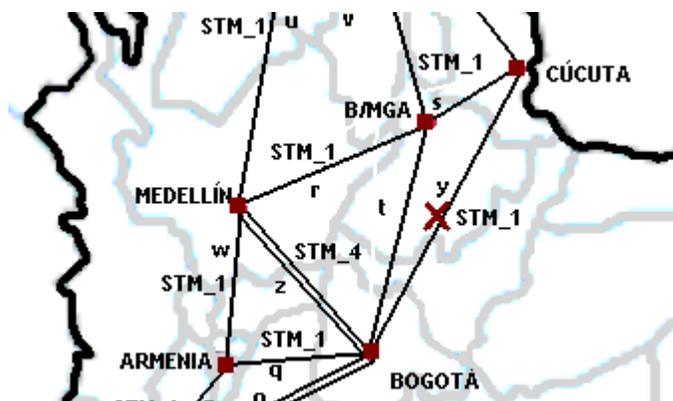


Figura 5.19. Recuperación de Fallas de Enlace.

Para realizar adecuadamente los procesos de detección, notificación y recuperación de fallas, se crea el árbol de notificación inverso, conforme a los requerimientos y características de la red. En la Figura 5.20 se ilustra el RNT y los PSLs establecidos para la red colombiana.

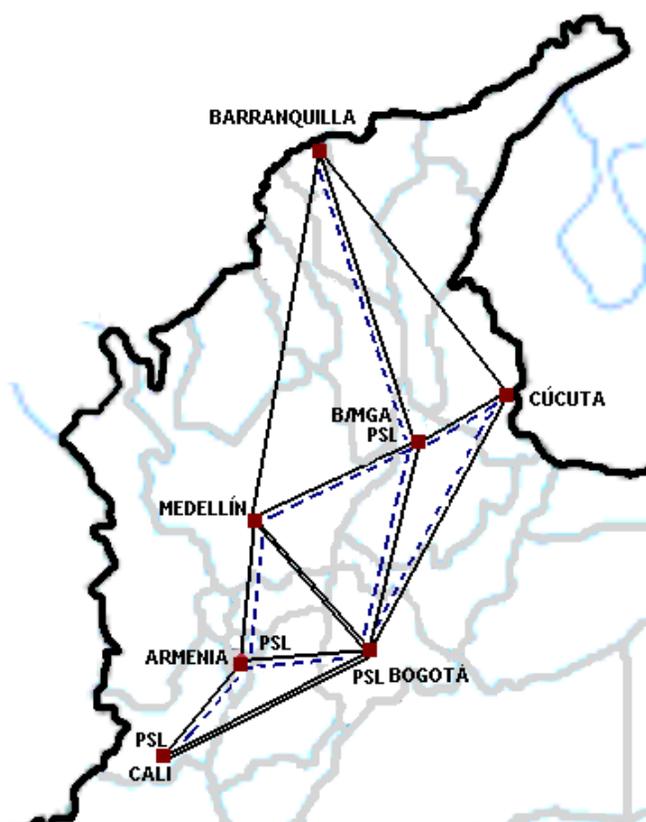


Figura 5.20. Red MPLS con Recuperación de Fallas.

Los enlaces Bogotá-Medellín y Cali-Bogotá no se incluyen en el árbol RNT debido a que cuentan con enlaces redundantes, y en caso de falla el enlace secundarios soporta el tráfico generado entre estos nodos.

7. Configuración de la gestión de red.

La gestión de la red es un aspecto importante del sistema de TE-MPLS. El éxito de la implementación de este tipo de sistemas depende de la facilidad con que la red pueda observarse y controlarse. Generalmente, un sistema de gestión para las redes MPLS incluye un conjunto de funciones para la gestión de configuración, gestión de desempeño y gestión de fallas. Colectivamente, estas funciones obtienen el estado y las características de los objetos MPLS a gestionar. Los flujos de tráfico punto a punto se caracterizan por las estadísticas del monitoreo de tráfico sobre los túneles LSPs. Las características de pérdida de los trayectos, se estiman monitoreando las estadísticas de tráfico de entrada y salida en los extremos del túnel LSP y comparando sus discrepancias. Las características de retardos de trayectos se estiman enviando paquetes de prueba a través de los túneles LSPs y midiendo los tiempos de tránsito. Cualquier notificación es caracterizada cuando el estado de los objetos MPLS gestionados excede los umbrales. El volumen de recuperación de las estadísticas del tráfico

de los túneles LSPs se utilizan para análisis de tiempo y propósitos de planeación de capacidad.

El monitoreo de la red es útil para verificar la calidad del servicio, verificar la conectividad, chequear el estado de posibles trayectos alternos e indicar fallas inminentes o problemas de desempeño. Una manera tradicional y estandarizada de monitorear la red es el Protocolo Simple de Gestión de Red (SNMP - Simple Network Management Protocol). Con SNMP los operadores de red consultan los nodos para verificar su estado, parámetros operacionales o recibir alarmas para indicar problemas específicos. Para el monitoreo de tráfico, el IETF ha extendido las funcionalidades de SNMP para incluir medidores de tráfico que determinen los flujos de tiempo real. Los medidores de tráfico son situados alrededor de la red, con la capacidad de observar los flujos de paquetes que pasan a través de ellos. Un medidor de tráfico se configura para observar un flujo de paquetes específico y sus diferentes atributos definidos por reglas proveídas por el gestor de red. Los atributos específicos del flujo (número de paquetes o bytes observados) son almacenados en una base de datos, la cual puede ser retribuida a los lectores de medida.

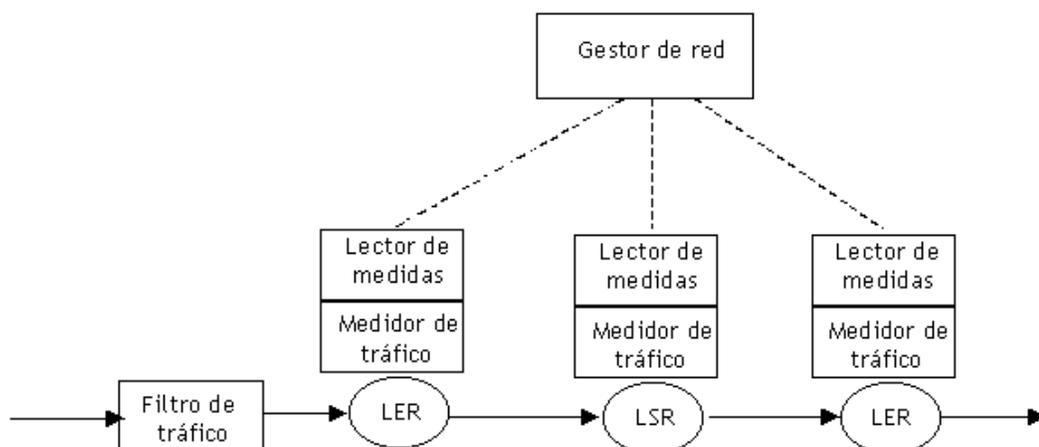


Figura 5.21. Monitoreo de Tráfico en la Red MPLS.

En MPLS, los FEC proveen una definición natural de flujo y los paquetes pertenecientes al mismo FEC pueden identificarse fácilmente por sus valores de etiquetas. Los medidores de tráfico pueden simplemente analizar las etiquetas MPLS para clasificar los paquetes en el dominio. Comparando el rendimiento en cada LSR los gestores de red determinan si están experimentando congestión o pérdidas e identifican la localización de la congestión. El monitoreo de tráfico puede utilizar filtros de tráfico a la entrada del dominio MPLS para monitorear las tasas de flujo de tráfico entrantes (Figura 5.21).

5.3.6 Resultados del Diseño de la Red Colombiana.

El sistema final de TE-MPLS diseñado para la red colombiana, cumple con las funciones de optimización y desempeño de un sistema de ingeniería de tráfico tradicional, que satisface los

requerimientos de los métodos dependiente del estado, offline, online, distribuido, global, local, prescriptivo, bucle cerrado y estratégico; convirtiéndolo en un ente más robusto, eficiente y competitivo.

Para cumplir con las funcionalidades de optimización, la TE usa el CR y el modelo de monitoreo de tráfico a través de los cuales gestiona la planeación, enrutamiento y control de los recursos según los requerimientos de calidad de servicio. Además, cuenta con las capacidades de recuperación de fallas y con el algoritmo Colored Thread que evita la prevención de bucles, y definen acciones que mejoran el desempeño global de la red. En la Figura 5.22 se ilustra la interacción entre los componentes del sistema diseñado.

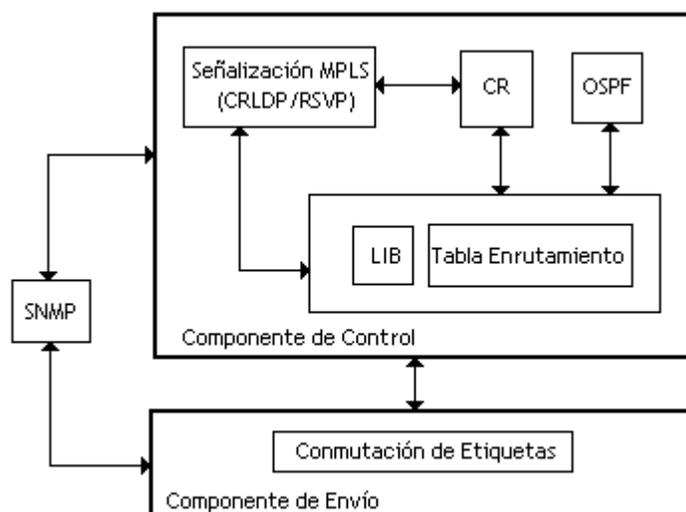


Figura 5.22. Interacción de los Componentes del Sistema TE-MPLS.

5.3.6.1 Descripción de los Enrutadores MPLS

Los enrutadores que forman parte del dominio MPLS diseñado, son tolerantes a fallas y tienen las siguientes funcionalidades:

1. Protocolos de distribución de etiquetas : CR-LDP. Aunque MPLS soporta varios protocolos para distribución de etiquetas, se eligió CR-LDP por su confiabilidad al momento de reportar fallas ya que utiliza TCP para asegurar que el proceso de recuperación pueda iniciarse a tiempo basándose en las políticas especificadas por el operador de la red.
2. Soporte para todos los modos de distribución de etiquetas (downstream, upstream, downstream sobre demanda, upstream sobre demanda). En el proceso de señalización, los enrutadores acuerdan el modo de distribución que van a utilizar.
3. Soporte múltiple para clasificación de FECs en: prefijo de dirección IP, direcciones de nodos y calidad de servicio.
4. Soporte de distribución de cargas.
5. Soporte para modo de retención de etiquetas conservativo y liberal.

6. Soporte para detección de bucles por medio del algoritmo Colored Thread.
7. Soporte para enrutamiento restringido.
8. Soporte para enrutamiento IP, tal como OSPF.
9. Soporte de mecanismos de recuperación de fallas: conmutación protegida y reenrutamiento rápido.
10. Soporte del protocolo de gestión SNMP.

En la Figura 5.23 se ilustra un modelo en bloques de los enrutadores MPLS:

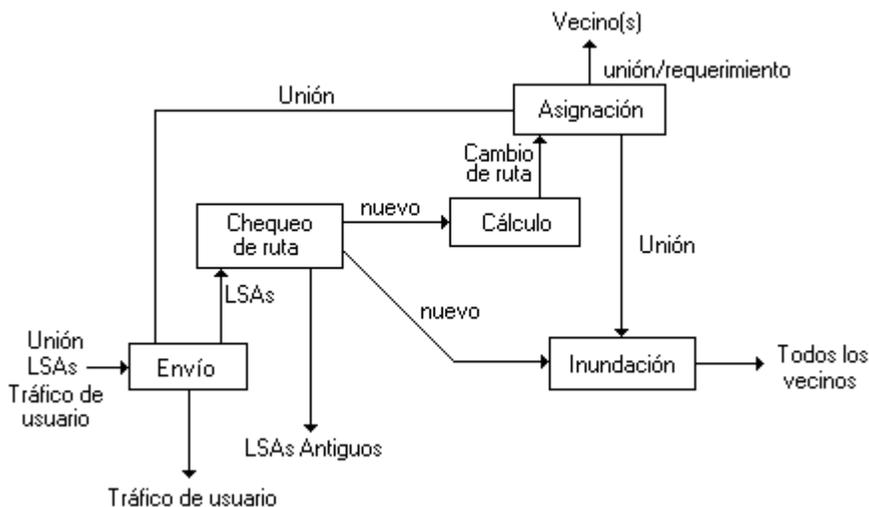


Figura 5.23. Modelo de un LSR.

5.3.7 Evaluación y Optimización de la Red

Una vez la red TE-MPLS ha sido implementada se requiere un proceso de monitoreo constante que tiene mucho en común con las redes IP. Una actividad importante es medir el tráfico actual de los enlaces de los PoP, compararlo con los parámetros asumidos durante la etapa de diseño y realizar las modificaciones o ajustes necesarios, por ejemplo, la distribución del tráfico a través de los nodos puede ser diferente a la determinada inicialmente. Este proceso es repetitivo, ya que debe renovarse a medida que aparecen nuevos usuarios que incrementan la carga en la red, y consta de los siguientes pasos:

1. Adición de nuevos LERs a los PoP, para cubrir el incremento del número de enlaces de los clientes.
2. Adición de nuevos enlaces a la red.
3. Ajuste de los parámetros de ingeniería de tráfico.
4. Chequeo de la existencia del número etiquetas suficientes sobre los enlaces.

5.3.7.1 *Optimización de tiempos de convergencia*

Con la introducción de MPLS a las redes IP se define un conjunto de métricas para cuantificar el comportamiento dinámico del enrutamiento. La cuantificación de estas métricas usa los mecanismos de asignación de etiquetas como base para un análisis comparativo. Los resultados de este análisis desarrollan un mejor entendimiento de la dinámica de enrutamiento e identifican las características de MPLS diseñadas en las redes IP. Las características de la red que intervienen en el comportamiento dinámico son:

- La naturaleza del protocolo en cuestión y la aproximación del control adoptada. Por ejemplo, la distribución de etiquetas puede realizarse a través de mecanismos de control de asignación upstream y downstream.
- Duración del cálculo de la tabla de los trayectos más cortos que es función del tamaño de la red y la capacidad de CPU disponible para este proceso.
- Volumen del tráfico de usuario que compite por los recursos.

El impacto de éstas características son capturadas a través de una serie de eventos que reflejan cambios en la red y en la configuración de los enrutadores. Los parámetros que definen la métrica para la dinámica de enrutamiento y estabilidad que influyen en éstas características son:

- Tiempo de Actualización de la Tabla de Enrutamiento (RTUT - Routing Table Update Time). Es el intervalo de tiempo entre la ocurrencia de un evento y la actualización completa de la tabla de enrutamiento. La actualización es incremental ó es el resultado del cálculo del trayecto más corto. Este parámetro es una métrica base que se relaciona con las características mencionadas.
- Tiempo de Convergencia de la Tabla de Enrutamiento (RTCT - Routing Table Convergence Time). Si ocurre un evento y es necesario actualizar varias tablas de enrutamiento de LSRs al mismo tiempo, el RTCT es el tiempo más largo de tales actualizaciones. Esta métrica es muy importante ya que una de las metas del diseño de la red es minimizar éste tiempo. El RTCT es afectado tanto por los protocolos de señalización como por los protocolos de distribución de etiquetas.
- Tiempo de Asignación de Etiquetas (LAT - Label Allocation Time). Las etiquetas pueden asignarse a una nueva ruta o pueden reasignarse como resultado de un cambio en la ruta. El LAT es el intervalo entre la ocurrencia del evento y la asignación o el cambio de ruta. LAT permite comparar los diferentes mecanismos de distribución de etiquetas ya que es una medida de la respuesta de la red a cualquier cambio de ruta y a la velocidad a la que ella es capaz de hacer el envío basado en etiquetas.

- Tiempo de Convergencia de Asignación de Etiquetas (LACT - Label Allocation Convergence Time). Si ocurre un evento donde es necesaria la asignación de etiquetas en varios LSRs, el LACT es el tiempo mas largo de tales asignaciones.

Gracias a sus procesos de enrutamiento e intercambio de etiquetas MPLS reduce significativamente estos tiempos, mejorando la respuesta de la red a diversos eventos. El LACT es una métrica importante pues indica que tan rápido la red será capaz de hacer el envío de etiquetas inclusive después de un cambio de ruta. La principal meta en el diseño de MPLS es proveer un protocolo de distribución de etiquetas con un LACT mínimo.

5.4 ASPECTOS A TENER EN CUENTA EN LA IMPLEMENTACION DE MPLS

MPLS puede implementarse en una red tradicional IP de forma gradual, iniciando con un simple par de LSRs en el backbone. En el momento de introducir los LSRs se debe considerar que los enrutadores de la red sean compatibles con los protocolos empleados por MPLS; si por factores económicos no es posible adquirir los equipos y se cuenta con dispositivos compatibles con MPLS se puede pensar en adicionar las funcionalidades de MPLS en dichos equipos.

Un buen ejemplo de la migración de una red IP a una MPLS se ilustra en la Figura 5.24 en la cual podemos observar la red con conexiones punto a punto entre cada uno de los enrutadores. Para mejorar la escalabilidad de la red se introduce un LSR en el núcleo lo que permite reducir el número de enlaces punto a punto. A medida que se introduce un mayor número de LSRs, la eficiencia de la red aumenta, la cantidad de enlaces que interconectan los dispositivos disminuye significativamente, los procesos de enrutamiento se simplifican y es posible prestar diferentes clases de servicios.

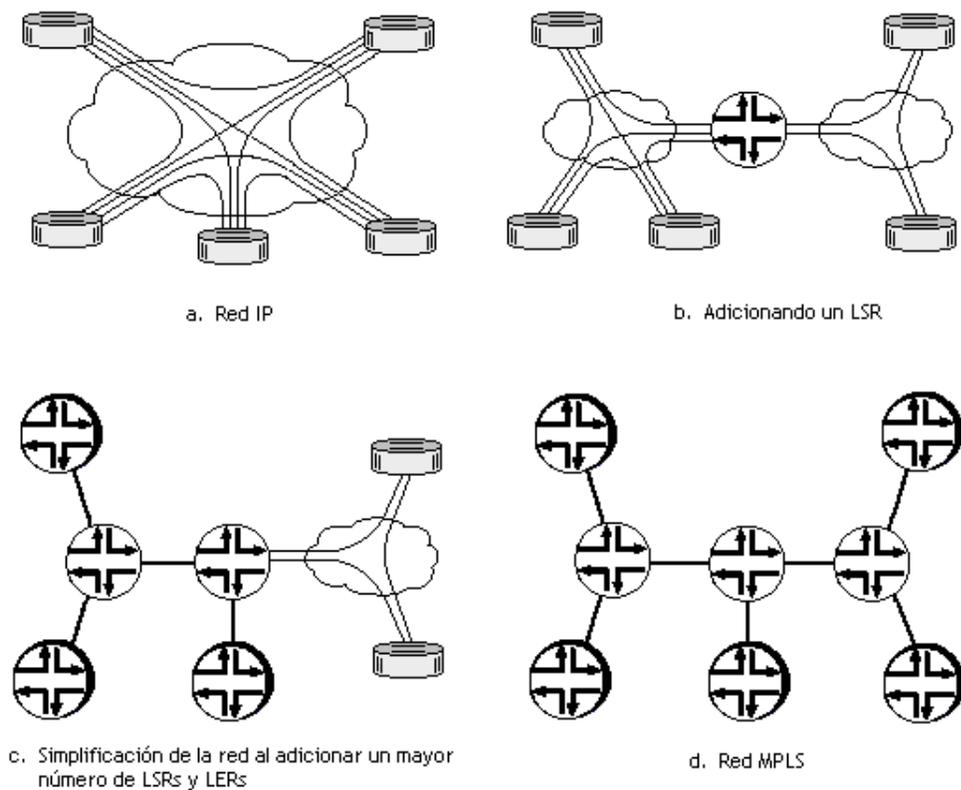


Figura 5.24. Migración hacia MPLS.

La interoperabilidad de MPLS con los diferentes protocolos de nivel de red y de nivel de enlace convergen hacia una misma plataforma de red, que pueda prestar diferentes clases de servicio, cumpliendo con objetivos de desempeño de TE. La participación de MPLS en esta nueva plataforma, extiende las capacidades de las redes IP logrando integrar sus procesos de enrutamiento con tecnologías de nivel 2, sin tratar de reemplazarlas, sino más bien complementando sus funcionalidades. La mayoría de las nuevas consideraciones introducidas por MPLS son la fiabilidad y redundancia en las redes y el asegurar un suficiente espacio de etiquetas.

6. CONCLUSIONES Y RECOMENDACIONES

Actualmente, el mercado de las comunicaciones enfrenta cambios en la demanda de los servicios, pero el bajo rendimiento y confiabilidad de las redes IP convencionales no ha permitido a los ISPs mantenerse al ritmo de esta demanda ni ofrecer niveles de QoS superiores a los del mejor esfuerzo. Con el fin de encontrar soluciones que permitan la prestación de servicios de valor agregado se está evolucionando a redes públicas multiservicio con mayores capacidades para satisfacer las necesidades de los usuarios.

La evolución empezó con el desarrollo del modelo superpuesto, el cual a pesar de sus ventajas de conmutación rápida y establecimiento de circuitos virtuales, no proporcionaba las garantías de nivel de servicio buscadas. Fue entonces cuando se enfocó la atención en las tecnologías de conmutación multinivel, que por sus características brindan la mejor solución a los problemas de operación y rendimiento. Como parte de esta evolución surgió MPLS aportando una serie de funcionalidades importantes, que dieron respuesta a la mayoría de las limitaciones de las tecnologías convencionales.

La introducción de MPLS a la arquitectura de envío de Internet tiene aplicaciones inmediatas en la Ingeniería de Tráfico, en QoS y en Redes Privadas Virtuales, entre otras, afectando la forma en que se transporta el tráfico a través de la red, pues MPLS reemplaza el paradigma de envío salto por salto (basado en la dirección de destino) por un paradigma de intercambio de etiquetas que garantiza una fácil transmisión de paquetes y que permitirá evolucionar las redes a tasas de terabits. Aunque MPLS en un principio fue creada para optimizar el envío de datos en las redes, sus recientes desarrollos han incrementado su campo de acción y han abierto nuevas posibilidades para integrar MPLS a las actuales infraestructuras de red.

MPLS es una tecnología en vía de estandarización, creada por el grupo de trabajo del IETF y cuyo propósito es definir una tecnología base que integre el paradigma de intercambio de etiquetas con el enrutamiento de nivel de red, estandarizar un conjunto de protocolos para la distribución y mantenimiento de etiquetas, y un conjunto de procedimientos para emplear esta tecnología sobre varios protocolos de nivel de enlace; todo esto con el propósito de obtener una estructura unificada e interoperativa que incremente la velocidad, y mejore la escalabilidad y las capacidades de provisión de servicios en las redes IP. Durante el proceso de estandarización (que aun no finaliza), muchas de las empresas del sector de las telecomunicaciones han apoyado esta iniciativa, haciendo parte de los diferentes grupos de desarrollo de MPLS.

MPLS es una solución basada en estándares que promete interoperabilidad multivendedor. No pretende desplazar ninguna tecnología, sino por el contrario lo que busca es complementarlas,

característica que hace a MPLS atractiva a los proveedores de servicio. Entre las propiedades y beneficios más relevantes de MPLS se encuentran:

- Rutas explícitas. Los LSPs enrutados explícitamente especifican el camino físico exacto del trayecto garantizando la reserva de los recursos y niveles específicos de QoS. Además, al conocer las rutas exactas de los LSPs se pueden obtener estadísticas del uso de los recursos utilizadas en la planificación de la red y como herramientas de análisis, de cuellos de botellas y cargas de los enlaces lo que resulta muy útil para planes futuros de expansión.
- Jerarquía de LSPs. Los LSPs pueden encapsularse dentro de otros LSPs, y sin perder su granularidad son transportados transparentemente a través de la red para finalmente entregarlos a su destino. La jerarquía de LSPs minimiza los recursos de las conexiones virtuales y facilita los procesos de enrutamiento solucionando los problemas de escalabilidad de las redes IP.
- Pila de etiquetas. MPLS permite un número arbitrario de etiquetas organizadas en una pila LIFO, en la cual el algoritmo de intercambio de etiquetas se ejecuta sobre la etiqueta superior. La pila de etiquetas permite que múltiples componentes de control actúen sobre un paquete, sin ningún tipo de coordinación facilitando la prestación de múltiples servicios.
- Multiprotocolo. MPLS integra sin discontinuidades las tecnologías de nivel de enlace y nivel de red combinando eficazmente el alto rendimiento, eficiencia y rapidez de la conmutación de nivel 2 con la inteligencia, flexibilidad y escalabilidad del enrutamiento de nivel 3.
- Intercambio de Etiquetas. El intercambio de etiquetas es una técnica robusta, que procesa rápidamente los paquetes y usa de forma más eficiente los recursos de la red. Este algoritmo clasifica sofisticadamente el tráfico que ingresa al dominio MPLS diferenciando cada clase de servicio por medio de su etiqueta, de esta manera, garantiza que cada una de las clases reciba un tratamiento diferencial.

Al trabajar con pequeñas etiquetas de tamaño fijo se optimiza el proceso de envío de paquetes en los enrutadores del núcleo y se reduce el tamaño de las tablas de enrutamiento incrementando la velocidad de la red.

- Fácil evolución. MPLS separa el componente de envío (intercambio de datos entre los elementos de red) y el componente de control (control de la información sobre la topología y tráfico de la red), facilitando que uno de ellos pueda evolucionar sin afectar al otro, lo cual hace la evolución de las redes fácil, a menor costo y menos propensa a errores.

- Fácil gestión. En MPLS, antes de enviar los datos hacia un destino se determinan las rutas explícitas que tomarán los paquetes, permitiendo controlar el consumo de recursos, monitorear los tipos de tráfico transportados, y en general, gestionar toda la red manteniendo información acerca del estado de los dispositivos con la ayuda de herramientas de recuperación de fallas y herramientas de gestión de tráfico online y offline.
- Enrutamiento restringido. Permiten al administrador una gestión mas eficiente de los enlaces y recursos en la red, de modo que las rutas seleccionadas satisfagan políticas administrativas y diferentes requerimientos de QoS.
- Tiempos de convergencia cortos. MPLS disminuye los tiempos de convergencia debido a que los enrutadores ya no examinan toda la cabecera IP para tomar sus decisiones de enrutamiento, sino que usan la etiqueta MPLS (de longitud fija) codificada en los paquetes como índice para decidir el próximo salto a seguir. La reducción en los tiempos de convergencia brinda la posibilidad de prestar servicios de tiempo real en las redes convencionales.
- Redes Privadas Virtuales. MPLS ofrece los servicios de VPNs con la seguridad y los niveles de QoS exigidos por los clientes empresariales. Los enrutadores MPLS tienen la funcionalidad de enrutador virtual que mantiene tablas de enrutamiento individuales para cada VPN formada en el dominio, permitiendo dividir la red física en regiones virtuales. Estas características aseguran que el tráfico entre las VPNs permanezca aislado y que el crecimiento de alguna de ellas no afecte a las demás ni al tráfico de los usuarios externos.
- Ingeniería de Tráfico. MPLS por sus características, hace que la ingeniería de tráfico sea una herramienta esencial en el diseño y operación de las redes IP. La TE abarca muchos aspectos relacionados con el desempeño de la red: control de tráfico, garantías de QoS, optimización de los recursos, provisión de características de recuperación de fallas, etc. Estas funcionalidades han conducido a simplificar la operación y gestión de la red brindando flexibilidad para soportar diferentes clases de servicio.
- Calidad de Servicio. MPLS está diseñada para soportar el modelo de servicios diferenciados diseñado por el IETF, el cual define una variedad de mecanismos para clasificar el tráfico en un reducido número de clases de servicios cada una de ellas con distintas prestaciones y con diferentes garantías de ancho de banda.
- Redes Ópticas. Los proveedores de servicio actuales usan en sus redes medios ópticos permitiéndoles tener mas prestaciones, mas capacidad de transporte de datos y mas velocidad de transmisión. Por esto, Uno de los grupos de trabajo de la IETF vio la necesidad de trabajar en la integración de las tecnologías ópticas con MPLS, formando GMPLS, cuyo objetivo es trasladar las características de simplicidad, gestión, TE y QoS de MPLS a las redes ópticas. GMPLS se ha convertido en una solución extremo a extremo a bajo costo para los proveedores de servicio.

- VoMPLS. MPLS busca integrar el plano de usuario y el plano de señalización de las PSTNs, y las redes de datos en una misma estructura y para esto se ha generado una arquitectura capaz de soportar estas funcionalidades. VoMPLS incluye elementos funcionales para garantizar los niveles de QoS, disminuyendo los tiempos de procesamiento de los paquetes, y controlando la admisión de llamadas de acuerdo a políticas administrativas.

Todas estas características hacen que MPLS extienda las capacidades de las redes de los proveedores de servicio sobre una estructura única, escalable, robusta con un comportamiento predecible y confiable para la prestación de servicios diferenciados.

Viendo el interés de los proveedores de servicio para implementar MPLS en sus redes, en este trabajo se generaron los criterios de diseño y migración como aporte en el proceso investigativo del Grupo I+D de Nuevas Tecnologías en Telecomunicaciones de la FIET. A través de este proceso se constataron los siguientes aspectos de diseño:

- El diseño de MPLS es similar al de las redes IP debido a que usan los mismos protocolos de enrutamiento como OSPF y BGP, facilitando la introducción de MPLS en las redes actuales.
- Muchos de los enrutadores y equipos de red existentes son compatibles con las funcionalidades de MPLS, pero no necesariamente con sus protocolos de señalización y de enrutamiento (especialmente con BGP), lo que impediría implementar satisfactoriamente MPLS.
- Aunque funcionalmente CR-LDP y RSVP proveen capacidades similares, se considera CR-LDP como un protocolo más confiable puesto que usa TCP para proveer un mecanismo de transporte fiable para sus mensajes de señalización y es un protocolo donde la información del estado no se refresca constantemente, mientras que en RSVP los mensajes deben ser refrescados periódicamente para mantener los trayectos, conduciendo a un problema de escalabilidad: si se tiene un gran número de trayectos a través de un nodo los requerimientos de memoria y procesamiento sobre ese nodo se incrementan proporcionalmente con el número de sesiones separadas. Si se disminuye la tasa de los mensajes usados para refrescar el estado de los LSPs podría afectar los procesos de detección de fallas y recuperación.
- En el enrutamiento restringido las restricciones seleccionadas para los procesos de enrutamiento influyen drásticamente en el desempeño y estabilidad de la red. Si se eligen restricciones que no dependen de cambios topológicos (retardo, ancho de banda reservable, etc.) se pueden ocasionar modificaciones constantes en las tablas de enrutamiento, afectando la estabilidad de la red al tener que conmutar continuamente el tráfico de un LSP a otro. En caso de que estas restricciones sean necesarias para garantizar niveles de QoS, se establecen límites en la frecuencia de cálculo, de tal forma que si no hay cambios significativos en el comportamiento de la red, el enrutador

simplemente actualiza su base de datos de estado de enlace y espera hasta el fin del tiempo límite para recalcular su tabla de enrutamiento.

- La introducción de MPLS trae consigo una característica muy importante que es la reducción de los tiempos de procesamiento y convergencia, permitiendo que las redes de datos puedan prestar servicios de tiempo real. Esto se logra gracias a que los enrutadores MPLS usan el algoritmo de intercambio de etiquetas para encaminar los paquetes a través de la red.

Todo este trabajo investigativo condujo al desarrollo de un software educativo que recopila los aspectos de mayor interés y auge en el entorno de MPLS y que cumple con requisitos técnicos y pedagógicos que colaboran en la divulgación de esta tecnología. Las características de un buen software educativo son:

- Facilidad de uso. El estudiante no necesita amplios conocimientos informáticos para utilizar este software. Además en cada momento el estudiante sabe el lugar del programa en donde se encuentra y tiene la posibilidad de moverse según sus preferencias.
- Entorno visual. Un buen software educativo debe tener un diseño general, claro y atractivo, con gran calidad técnica y estética en sus elementos (menús, botones, ventanas, textos, imágenes, barras de navegación, barras de estado, hipertextos, fondos, etc.).
- Enfoque pedagógico. El programa presenta entornos centrados en el estudiante, en los cuales, además de comprender los contenidos, el estudiante puede investigar y buscar nuevas relaciones, siendo así el constructor de su aprendizaje a través del entorno que le ofrece el programa.
- Calidad de los contenidos. Puesto que el software pretende enseñar un nuevo tema al estudiante, los contenidos han sido preparados cuidadosamente y están estructurados de acuerdo con dicha preparación.
- Navegación e interacción. La amabilidad del programa está dada por la facilidad de navegación entre los diferentes temas y por la forma de responder a las interacciones con los estudiantes. Por eso un buen software educativo tiene en cuenta:
 - ✓ Una buena estructuración del mapa de navegación del programa que permita acceder rápido y fácil a los contenidos .
 - ✓ La velocidad del programa debe ser adecuada en cuanto a animaciones, lectura de datos, hipertextos, etc.
 - ✓ El análisis de respuestas debe ser ágil y avanzado.

- Capacidad de motivación. Para que la herramienta sea realmente aprovechada, el programa provee contenidos significativos y el estudiante debe tener la voluntad de aprenderlos.

El estudio de la tecnología MPLS es muy amplio e interesante y se invita a seguir en la investigación de sus conceptos y aplicaciones, pues aún hay muchos campos donde no se ha desarrollado completamente esta tecnología, como es el caso de GMPLS que, aunque necesita cambios en los protocolos de enrutamiento y señalización, ya es parte integral en la evolución de las redes de datos. Existen otros campos en los cuales MPLS está empezando a incursionar, entre los que se encuentran Redes Inalámbricas y Electricidad sobre IP (con un plano de control MPLS) que sería interesante contribuir en su desarrollo.

ACRÓNIMOS

AG	Pasarela de Acceso (<i>Access Gateway</i>)
ARIS	Conmutación IP Basada en Ruta Agregada (<i>Aggregate Route-Based IP Switching</i>)
ARP	Protocolo de Resolución de Direcciones (<i>Addresses Resolution Protocol</i>)
ARs	Enrutador de Acceso (<i>Access Router</i>)
AS	Servicio Asegurado (<i>Assured Service</i>)
ATM	Modo de Transferencia Asíncrono (<i>Asynchronous Transfer Mode</i>)
ATM-LSR	Enrutador Conmutación de Etiqueta ATM (<i>ATM label switching router</i>)
BA	Comportamiento Agregado (<i>Behaviour Aggregate</i>)
BDI	Fallas Emitido hacia Atrás (<i>Backward Defect Identifier</i>)
BEB	Servicios del mejor Esfuerzo (<i>Best Effort Service</i>)
BGP	Protocolo de Pasarela de Frontera (<i>Border Gateway Protocol</i>)
BRs	Enrutador de Frontera (<i>Border Router</i>)
BTT	Troncales de Tráfico Bidireccionales (<i>Bidirectional Traffic Trunk</i>)
CA	Agente de Llamada (<i>Call Agent</i>)
CAR	Tasa de Acceso Negociada (<i>Committed Access Rate</i>)
CoS	Clase de Servicio (<i>Class of service</i>)
CR	Enrutamiento Restringido (<i>Constraint Based Routing</i>)
CRs	Enrutadores del Núcleo (<i>Core Routers</i>)
CR-LDP	Protocolo de Distribución de Etiquetas con CR (<i>Constraint based Routing Label Distribution Protocol</i>)
CSPF	Trayecto más Corto Restringido (<i>Constraint Shortest Path First</i>)
CSR	Enrutador de Conmutación de Celdas (<i>Cell Switching Router</i>)
CV	Verificación de Conectividad (<i>Connectivity Verification</i>)
DARPA	Agencia de Proyectos de Investigación Avanzados del Departamento de Defensa de los EUA (<i>US Defense Advanced Research Projects Agency</i>)
DF	No Fragmentado (<i>Don't Fragment</i>)
DiffServ	Servicios Diferenciados (<i>Differentiated Services</i>)
DLCI	Identificador de Control de Enlace de Datos (<i>Data Link Control Identifier</i>)
DWDM	Multiplexación por División de Onda (<i>Dense Wavelength Division Multiplexing</i>)
ECMP	Multitrayectos de Igual Costo (<i>Equal Cost MultiPath</i>)
EDR	Enrutamiento Dependiente de Eventos (<i>Event-Dependent Routing</i>)
EGP	Protocolos de Enrutamiento Externo (<i>Exterior gateway protocol</i>)
E-LSP	LSP Deducido del campo Exp (<i>Exp Inferred LSP</i>)

ES	Sistemas Terminales (<i>End System</i>)
FDI	Fallas Emitido hacia Adelante (<i>Forward Defect Identifier</i>)
FEC	Clase Equivalente de Envío (<i>Forwarding Equivalence Class</i>)
FIS	Señal de Indicación de Falla (<i>Fault Indication Signal</i>)
FR	Enrutamiento Fijo (<i>Fixed Routing</i>)
FRS	Señales de Recuperación de Fallas (<i>Fault Recovery Signal</i>)
FTN	Mapeo del FEC a un NHLFE (<i>FEC to NHLFE Map</i>)
FTP	Protocolo de Transferencia de Archivos (<i>File Transfer Protocol</i>)
HR	Enrutador de Hosting (<i>Hosting Router</i>)
IAD	Dispositivos de Acceso Integrado (<i>Integrated Access Device</i>)
IBF	Algoritmo Berman-Ford iterativo (<i>Iterative Berman-Ford</i>)
ICMP	Protocolo de Mensajes de Control en Internet (<i>Control Message Protocol</i>)
IETF	Grupo de Trabajo en Ingeniería de Internet (<i>Internet Engineering Task Force</i>)
IHL	Longitud de Cabecera IP (<i>IP Header Length</i>)
IGP	Protocolos de Enrutamiento Interno (<i>Interior gateway protocol</i>)
ILM	Mapeo de la Etiqueta Entrante (<i>Incoming Label Map</i>)
IP	Protocolo Internet (<i>Internet Protocol</i>)
IS-IS	Sistema Intermedio - Sistema Intermedio (<i>Intermedium System Intermedium System</i>)
ISP	Proveedor de Servicio Internet (<i>Internet Service Provider</i>)
L-LSPs	LSP Deducido del valor de Etiqueta (<i>Label Inferred LSPs</i>)
LACT	Tiempo de convergencia de asignación de etiquetas (<i>Label Allocation Convergence Time</i>)
LAT	Tiempo de Asignación de Etiquetas (<i>Label Allocation Time</i>)
LDP	Protocolo de Distribución de Etiquetas (<i>Label Distribution Protocol</i>)
LER	Enrutador de Frontera de Etiquetas (<i>Label Edge Router</i>)
LIB	Base de Información de Etiquetas (<i>Label Information Base</i>)
LIFO	Ultimo en Entrar Primero en Salir (<i>Last In First Out</i>)
LSA	Anuncios de Estado de Enlace (<i>Link State Advertisements</i>)
LSDB	Base de Datos de Estado de Enlace (<i>Link State Data Base</i>)
LSG	Línea del Lado de la Pasarela (<i>Line Side Gateway</i>)
LSP	Trayectos Conmutados de Etiquetas (<i>Label Switched Path</i>)
LSP ID	Identificador de LSP
LSP-LDP	LSP Establecido por LDP
LSP-RSVP	LSP Establecido por RSVP
LSR	Enrutador de Conmutación de Etiquetas (<i>Label Switching Router</i>)
MF	Mas Fragmentos (<i>More Fragments</i>)
MG	Pasarela de Comunicaciones (<i>Media Gateway</i>)
MPLS	Conmutación de Etiquetas MultiProtocolo (<i>MultiProtocol Label Switching</i>)

MTU	Unidad de Transferencia Máxima (<i>Maximum Transfer Unit</i>)
NHLFE	Entrada de Envío de Etiqueta para el Siguiente Salto (<i>The Next Hop Label Forwarding Entry</i>)
NFS	Sistema de Archivos de Red (<i>Network File System</i>)
NP-Complete	Algoritmo de Polinomio no Determinístico de Tiempo Completo (<i>Nondeterministic Poynomia - Time Complete</i>)
OAM	Operación, Administración y Mantenimiento
OSI	Interconexión de Sistemas Abiertos (<i>Open System Interconnection</i>)
OSPF	Abrir Primero el Trayecto más Corto (<i>Open Shortest Path First</i>)
OXCs	Conectores Opticos (<i>Optical Cross-Connect</i>)
PD	Vector Trayecto/ Algoritmo de Difusión (<i>Path Vectors / Diffusion Algorithm</i>)
PHB	Comportamiento por Salto (<i>Per-Hop Behaviour</i>)
PoP	Punto de Presencia (<i>Point of Presence</i>)
PS	Servicio Premium (<i>Premium Service</i>)
PSL	LSR Conmutador de Trayectos (<i>Path Switch LSR</i>)
PSTN	Red Telefónica Pública Conmutada (<i>Public Switched Telephone Network</i>)
QoS	Calidad de Servicio (<i>Quality of Service</i>)
RARP	Protocolo de Resolución de Direcciones Inverso (<i>Reverse Addresses Resolution Protocol</i>)
RED	Detección Aleatoria Preventiva (<i>Random Early Detection</i>)
RIP	Protocolo de Información de Enrutamiento (<i>Routing Information Protocol</i>)
RNT	Árbol de Notificación Inverso (<i>Reverse Notification Tree</i>)
RPC	Llamadas a Procedimientos Remotos (<i>Remote Procedure Call</i>)
RSVP	Protocolo de Reservación de Recursos (<i>Resources reSerVation Protocol</i>)
RTCT	Tiempo de Convergencia de la Tabla de Enrutamiento (<i>Routing Table Convergence Time</i>)
RTUT	Tiempo de Actualización de la Tabla de Enrutamiento (<i>Routing Table Update Time</i>)
SDR	Enrutamiento Dependiente del Estado (<i>State-Dependent Routing</i>)
SG	Pasarela de Señalización (<i>Signaling Gateway</i>)
SLAs	Acuerdos de Nivel de Servicio (<i>Service Level Agreements</i>)
SMTP	Protocolo de Transferencia Simple de Correo (<i>Simple Mail Transfer Protocol</i>)
SNMP	Protocolo Simple de Gestión de Red (<i>Simple Network Management Protocol</i>)
TCP	Protocolo de Control de Transmisión (<i>Transmission Control Protocol</i>)
TDR	Enrutamiento Dependiente del Tiempo (<i>Time-Dependent Routing</i>)
TE	Ingeniería de Tráfico (<i>Traffic Engineering</i>)

TED	Base de Datos de Ingeniería de Tráfico especializada (<i>Traffic Engineering Database</i>)
TE-MPLS	Ingeniería de Tráfico MPLS (<i>Traffic Engineering MPLS</i>)
TF	Tolerancia a Fallas (<i>Fault Tolerance</i>)
TG	Pasarela de Troncales (<i>Trunk Gateway</i>)
TTL	Tiempo de Vida (<i>Time To Live</i>)
ToS	Tipo de Servicio (<i>Type of Service</i>)
UDP	Protocolo de Datagramas de Usuario (<i>User Datagram Protocol</i>)
VoIP	Voz sobre IP
VoMPLS	Voz sobre MPLS
VPI/VCI	Identificador de Trayecto Virtual/Identificador de Circuito Virtual (<i>Virtual Path Identifier/Virtual Circuit Identifier</i>)
VPN	Redes Privadas Virtuales (<i>Virtual Private Network</i>)
WFQ	Atención de Colas Equitativa Ponderada (<i>Weighted Fair Queuing</i>)
WRED	RED Ponderado (<i>Weighted Random Early</i>)
XDR	Representación Externa de Datos (<i>eXternal Data Representation</i>)

BIBLIOGRAFÍA

- [1] Rosen Eric C., Viswanathan Arun, Callon Ross. MPLS Architecture. Internet RFC 3031, IETF. Enero, 2001.
- [2] Rosen Eric C., Tappan Dan, Rekhter Yakov, Fedorkow Guy, Farinacci Dino, Li Tony, Conta Alex. MPLS Label Stack Encoding. Internet RFC 3032, IETF. Enero, 2001.
- [3] Awduche Daniel O., Malcolm Joe, Agogbua Johnson, O'Dell Mike, McManus Jim. Requirements for Traffic Engineering Over MPLS. Internet RFC 2702, IETF. Septiembre, 1999.
- [4] Andersson L., Doolan P., Feldman N., Fredette A., Thomas B. LDP Specification. Internet RFC 3036, IETF. Enero, 2001.
- [5] Ohba Y., Katsube Y., Rosen E., Doolan P. MPLS Loop Prevention Mechanism. Internet RFC 3063, IETF. Febrero, 2001.
- [6] Ash Gerald R. TE & QoS Methods for IP,ATM,TDM-Based Networks. Internet Draft draft-ash-te-qos-routing-01.txt, IETF. Julio, 2000.
- [7] Le Faucheur Francois, Wu Liwen, Davie Bruce, Davari Shahram, Vaananen Pasi, Krishnan Ram, Cheval Pierrick, Heinanen Juha. MPLS Support of Diff-Serv. Internet Draft draft-ietf-mpls-diff-ext-08.txt, IETF. Febrero, 2001.
- [8] Sharma Vishal, Crane Ben-Mack, Makam Srinivas, Owens Ken, Huang Changcheng, Hellstrand Fiffi, Weil Jon, Andersson Loa, Jamoussi Bilel, Cain Brad, Civanlar Seyhan, Chiu Angela. Framework for MPLS-based Recovery. Internet Draft draft-ietf-mpls-recovery-frmwrk-02.txt, IETF. Marzo, 2001.
- [9] Awduche Daniel O., Chiu Angela, Elwalid Anwar, Widjaja Indra, Xiao Xipeng. A Framework for Internet Traffic Engineering. Internet Draft draft-ietf-tewg-framework-02.txt, IETF. Julio, 2000.
- [10] Chen Thomas M., Kennington Jeffery L., Oh Tae(Tom). Fault Restoration Techniques for MPLS with QoS Constraints. Agosto, 2000.
- [11] Cisco Systems. Calidad de Servicios. 1999.
- [12] Ennovate Networks, Inc. Multiprotocol Label Switching (MPLS). 1998.
- [13] Semeria Chuck. Multiprotocol Label Switching ,Enhancing Routing in the New Public Network. Juniper Networks, inc. 2000.
- [14] Brittain Paul, Farrel Adrian. MPLS Traffic Engineering: A Choice of Signaling Protocols - Analysis of the similarities and differences between the two primary MPLS label distribution protocols: RSVP and CR-LDP. Data Connection Limited. Enero 17, 2000.
- [15] Semeria Chuck. Traffic Engineering for the New Public Network. Juniper Networks, inc. 2000.
- [16] Semeria Chuck. RSVP Signaling Extensions for MPLS Traffic Engineering. Juniper Networks, inc. 2000.

-
- [17] Mitra Debasis, Ramakrishnan K. G. Techniques for Traffic Engineering of Multiservice, Multipriority Networks. Abril, 2001.
 - [18] Donnell Annette Kay. Deploying MPLS Traffic Engineering. Juniper Networks, inc. 2000.
 - [19] Cisco Systems. Quality of Service (QoS) Networking. Junio, 1999.
 - [20] Cisco Systems. Cisco MPLS Controller Software Configuration Guide. Mayo, 2001.
 - [21] QoS Forum. White Paper -The Need for QoS. 1999.
 - [22] QoS Forum. White Paper -Introduction to QoS Policies. 1999.
 - [23] QoS Forum. White Paper -QoS protocols & architectures. Julio, 1999.
 - [24] Juniper Networks, Inc. JUNOS™ Internet Software Configuration Guide - MPLS Applications. 2000.
 - [25] Juniper Networks, Inc. JUNOS™ Internet Software Configuration Guide - Routing and Routing Protocols. 2000.
 - [26] Murillo Javier. IP over ATM. Newbridge. Marzo, 2000.
 - [27] Lasserre Marc. Deploying MPLS in Deploying MPLS in MANs. 2000.
 - [28] Armitage Grenville. MPLS: The Magic Behind the Myths. IEE Communications Magazine, p. 124-131. Enero, 2000.
 - [29] Xiao Xipeng. Providing Quality of Service in the Internet. Universidad del Estado de Michigan. 2000.
 - [30] Pulley Robert, Christensen Peter. A Comparison Of MPLS Traffic Engineering Initiatives. NETPLANE Systems, Inc. 2000.
 - [31] Xiao Xipeng, Hannan Alan, Bailey Brook, Ni Lionel M.. Traffic Engineering with MPLS in the Internet. IEEE Network, p. 28-33. Marzo/Abril, 2000.
 - [32] Webb Roderick, Castelli Paolo, Varga Balazs, Geczi Csaba, Telbisz Ferenc, Svinnet Inge, Osterbo Olav, Aarstad Egil. Differentiated Services - Network Configuration and Management. Diciembre, 2000.
 - [33] Xiao Xipeng, Ni Lionel M. Internet QoS: A Big Picture. IEEE Network, p 8-18. Marzo/Abril 1999.
 - [34] Kimbell John P. Multiprotocol Label Switching White Paper. Febrero 2001.
 - [35] Roth Rudolf, Tiemann Jens, Mark Lutz. MPLS Study. Septiembre, 1999.
 - [36] van der Zee Martin, Heijenck Geert. Quality of Service Routing. Julio, 1999.
 - [37] Viswanathan Arun, Feldman Nancy, Wang Zheng, Callon Ross. Evolution of Multi-Protocol Label Switching. 2000.
 - [38] Newbridge Networks. IP Internetworking Transport. Mayo, 1999.
 - [39] Trillium. Multiprotocol Label switching (MPLS). 1999.
 - [40] Newbridge Networks. Technical Paper - The Role of MPLS Technology in IP Networks. Marzo, 2000.
 - [41] Naidu Kiran D., Yi Yang. Multiprotocol Label Switching(MPLS). Diciembre, 1999.
 - [42] Cisco Systems. Internet Protocols. Junio, 1999.
 - [43] Harris & Jeffries, Inc. Layer 3 Switching Using MPLS_White Paper. 1999
 - [44] Cisco Systems. Tag Switching. Junio, 1999.
 - [45] Williams Brian. Quality of Service Differentiated Services and Multiprotocol Label Switching. Australia, Marzo, 2000.

-
- [46] Brittain Paul, Farrel Adrian. Mpls Virtual Private Networks- A review of the implementation options for MPLS VPNs including the ongoing standardization work in the IETF MPLS Working Group. Noviembre, 2000.
- [47] Alerta Corporation. Implementing Multiprotocol Label Switching with Alerta PLDs. Enero, 2001.
- [48] Awduche, Daniel O. MPLS and Traffic Engineering in IP Networks. IEEE Communications Magazine. Diciembre, 1999.
- [49] Riverstone Networks, Inc. QoS: Solutions for ServiceProviders using RiverstoneNetworks' Switch Routers. Santa clara, 2000.
- [50] Nortel Networks. Using CR-LDP or Service Interworking, Traffic Engineering, and Quality of Service in Carrier Networks. Septiembre, 2000.
- [51] Nortel Networks. Traffic Management 101 - An introduction to the essentials of Internet service provisioning from the sponsors of the iBAND4 exhibition and conference. 2000.
- [52] Fischer Philippe Levillain Philippe. Calidad de servicio : una solución global para empresas. 2000.
- [53] Future Software Private Limited. Multi Protocol Label Switching - White Paper. 1999.
- [54] Fisher Sharon. Policy Management: An Introduction. Agosto, 2000.
- [55] Cebrian Pablo, Lin Eric. Support for Differentiated Services in Utl-Protocol Label Switching. Octubre, 2000.
- [56] Chung Ting Wo, Coulter John, Fitchett Jeff Mokbel, Sam, Arnaud Bill St. Architectural and Engineering Issues for Building an Optical Internet. 1999.
- [57] Stephenson Ashley. QoS: The IP Solution Delivering End-to-End Quality of Service for the Future of IP. Diciembre, 1999.
- [58] Nortel Networks. IP Traffic Engineering for Carrier Networks: Using Constraint-Based Routing to Deliver New Services. 1999
- [59] Farrel Adrian, Miller Ben. Surviving Failures In Mpls Networks An examination of the methods for protecting MPLS LSPs against failures of network resources. February 2001.
- [60] Li Tony. MPLS and the Evolving Internet Architecture. IEEE Communications Magazine. Diciembre 199.
- [61] Ghanwani Anoop, Jamoussi Bilel, FedyK Don, Aswood-Smith Peter, Li Li. Traffic Engineering Standars in Ip Networks Using MPLS. IEEE Communications Magazine. Diciembre 199.
- [62] Swallow George, MPLS Advantages for Traffic Engineering. . IEEE Communications Magazine. Diciembre 199.
- [63] Chen Thomas M. Oh Tae H. Reliable Services in MPLS. . IEEE Communications Magazine. Diciembre 199.
- [64] Ohba Yoshihiro. Issues on Loop Prevention in MPLS Networks. . IEEE Communications Magazine. Diciembre 199.
- [65] Fenczik Peter, Jacowitz Dave, Lancaster John Melnick, Ben, Sudduth Michelle. Macromedia Usando Flash 4. Junio 1999.
- [66] Doyle Jeff. Resolving Routes for MPLS Traffic Engineering. 2000.
- [67] Extreme Networks, Inc. Policy Based Quality of Service for enterprise LANs. 1999.

- [68] Extreme Networks, Inc. Leveraging MPLS To Enhance Network Transport Capabilities An Overview of the Key Challenges and Opportunities In Service Provider and Enterprise Environments. 1999.

Referencias Web

- [69] <http://www.mplsrc.com>
- [70] <http://www.atmforum.com>
- [71] <http://www.mplsforum.com>
- [72] <http://www.ietf.org>
- [73] <http://www.juniper.net>
- [74] <http://www.cisco.com>
- [75] <http://www.mplsworld.com>
- [76] <http://www.wandl.com>
- [77] <http://www.cid.alcatel.com>
- [78] <http://www.lucent.com>
- [79] <http://www.nortelnetworks.com>
- [80] <http://www.dataconnection.com>
- [81] <http://www.qosforum.com>
- [82] <http://www.futsoft.com>
- [83] <http://www.alerta.com>
- [84] <http://www.iec.com/tutorials/mpls>
- [85] <http://www.thecguide.com>