Universidad de San Carlos de Guatemala
Facultad de Ingeniería
Escuela de Ingeniería Mecánica Eléctrica

DISEÑO DE REDES PRIVADAS EN EQUIPO CISCO UTILIZANDO MULTIPROTOCOLO PARA CONMUTACIÓN DE ETIQUETAS (MPLS)

Selvyn David Reyes Dávila

Asesorado por el Ing. Luis Eduardo Durán Córdoba

Guatemala, abril de 2008

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

DISEÑO DE REDES PRIVADAS EN EQUIPO CISCO UTILIZANDO MULTIPROTOCOLO PARA CONMUTACIÓN DE ETIQUETAS (MPLS)

PRESENTADO A JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR
SELVYN DAVID REYES DÁVILA
ASESORADO POR EL ING. LUIS EDUARDO DURÁN CÓRDOBA
A CONFERÍRSELE EL TÍTULO DE
INGENIERO ELECTRÓNICO

GUATEMALA, ABRIL DE 2008.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Murphy Olympo Paiz Recinos
VOCAL I	Inga. Glenda Patricia García Soria
VOCAL II	Inga. Alba Maritza Guerrero de López
VOCAL III	Ing. Miguel Ángel Dávila Calderón
VOCAL IV	Br. Kenneth Issur Estrada Ruiz
VOCAL V	
SECRETARIA	Inga. Marcia Ivonne Véliz Vaides

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

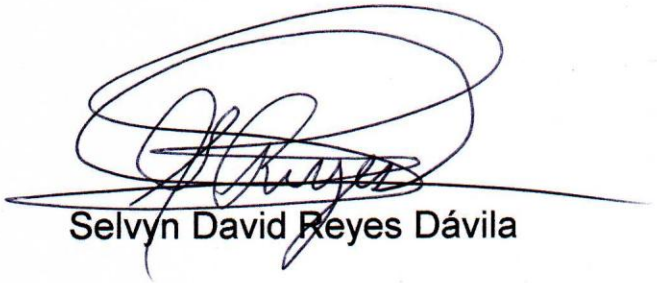
DECANO	Ing. Sydney Alexander Samuels Milson
EXAMINADOR	Ing. Enrique Edmundo Ruiz Carballo
EXAMINADOR	Ing. Manuel Fernando Barrera Pérez
EXAMINADOR	Ing. Marvin Marino Hernández Fernández
SECRETARIO	Ing. Pedro Antonio Aguilar Polanco

HONORABLE TRIBUNAL EXAMINADOR

Cumpliendo con los preceptos que establece la ley de la Universidad de San Carlos de Guatemala, presento a su consideración mi trabajo de graduación titulado:

DISEÑO DE REDES PRIVADAS EN EQUIPO CISCO UTILIZANDO MULTIPROTOCOLO PARA CONMUTACIÓN DE ETIQUETAS (MPLS),

tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, el 7 de abril de 2005.



Selvyn David Reyes Dávila

Guatemala, 21 de agosto de 2,007

Ingeniero
Julio César Solares Peñate
Coordinador de Área
Ingeniería Electrónica
Escuela de Ingeniería Mecánica Eléctrica

Ingeniero Solares,

De la manera más atenta me dirijo a usted para informarle que, satisfactoriamente, he concluído la asesoría y revisión del trabajo de graduación titulado **"Diseño de Redes Privadas en Equipo Cisco Utilizando Multiprotocolo para Conmutación de Etiquetas (MPLS)"**, elaborado por el estudiante Selvyn David Reyes Dávila.

Por lo tanto el autor de este trabajo de graduación y yo, como su asesor, nos hacemos responsables por el contenido y conclusiones de la misma.

Atentamente,

Ing. Luis E. Durán C.
Colegiado No. 5362
Asesor

Cap
c.c.: archivo.

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

Guatemala, 6 de SEPTIEMBRE 2007.

Señor Director
Ing. Mario Renato Escobedo Martìnez
Escuela de Ingenierìa Mecànica Elèctrica
Facultad de Ingenierìa, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado: **Diseño de Redes Privadas en Equipo Cisco Utilizando Multiprotocolo para Conmutación de Etiquetas (MPLS), desarroll**ado por el estudiante; Selvyn David Reyes Dàvila , por considerar que cumple con los requisitos establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,

ID Y ENSEÑAD A TODOS

UNIVERSIDAD DE SAN CARLOS
FACULTAD DE INGENIERIA
DIRECCION ESCUELA DE INGENIERIA
MECANICA ELECTRICA
DE GUATEMALA

Ing. Julio Cèsar Solares Peñate
Coordinador Area de Electrònica

JCSP/sro

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERÍA

El Director de la Escuela de Ingenierìa Mecànica Elèctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Area, al trabajo de Graduación del estudiante; Selvyn David Reyes Dàvila titulado: **Diseño de Redes Privadas en Equipo Cisco Utilizando Multiprotocolo para Conmutación de Etiquetas (MPLS),** procede a la autorización del mismo.

Ing. Mario Renato Escobedo Martínez
DIRECTOR

UNIVERSIDAD DE SAN CARLOS
FACULTAD DE INGENIERIA
DIRECCION ESCUELA DE INGENIERIA
MECANICA ELECTRICA
DE GUATEMALA

GUATEMALA, 11 DE SEPTIEMBRE 2,007.

Universidad de San Carlos
de Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.097.08

El Decano de la Facultad de Ingeniería de la Universidad de San Carlos de Guatemala, luego de conocer la aprobación por parte del Director de la Escuela de Ingeniería Mecánica Eléctrica, al trabajo de graduación titulado: **DISEÑO DE REDES PRIVADAS EN EQUIPO CISCO UTILIZANDO MULTIPROTOCOLO PARA CONMUTACIÓN DE ETIQUETAS (MPLS),** presentado por el estudiante universitario **Selvyn David Reyes Dávila,** autoriza la impresión del mismo.

IMPRÍMASE.

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Ing. Murphy Olympo Paiz Recinos
DECANO

Guatemala, abril de 2008

mestras
/cc

ACTO QUE DEDICO A:

DIOS

MI MADRE	Maura Estela Dávila Marroquón
MI PADRE	Genaro de Jesús Reyes Monzón
MIS HERMANOS	Elsa Argentina Reyes Dávila Rosa Ileana Reyes Dávila Blanca Estela Reyes Dávila Blanca Guissela Reyes Dávila Manolo de Jesús Reyes Dávila Pedro Randolf Reyes Dávila Gloria Maribel Reyes Dávila †

MIS FAMILIARES Y AMIGOS

LA FACULTAD DE INGENIERÍA, DE LA UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
	Enrutador o *Router*
	Enrutador o *Router* LSR
	Conmutador ATM
	Conmutador ATM LSR
	Multiplexor o ADM
	Dispositivo de Acceso para Relevo de Tramas FRAD
	CSU/DSU

GLOSARIO

AAL5 ATM *Adaptation Layer* 5. Adaptación ATM de capa 5. Es usada para adaptar tráfico orientado a la conexión y no orientado a la conexión, por ejemplo IP.

ABR *Available Bit Rate*, o sea, tasa de transferencia de *bits* disponible. Categoría de servicio usada en ATM.

ANSI *American National Standards Institute*. Entidad regulatoria de estándares norteamericana.

AS *Autonomus System*, o sea, sistema autónomo, nombre que se le da al identificador del proceso de BGP.

ATM *Asynchronous Transfer Mode*, modo de transferencia asíncrona.

BECN *Backward Explicit Congestion Notification*. Notificación explícita de congestión reversa. *Bit* utilizado en *Frame*

	Relay para indicar congestión en el sentido reverso de la transmisión de la trama.
BGP	*Border Gateway Protocol*. Protocolo de enrutamiento para intercambio de rutas con otros sistemas BGP.
BISDN	*Broadband* ISDN. ISDN de banda ancha.
Bit	En términos digitales un 0 ó 1 binario.
Byte	Palabra de 8 *bits*.
C	Nombre que se asigna a un enrutador o *Router* propiedad del usuario o cliente.
CBR	*Constant Bit Rate*. Tasa de transferencia de *bits* constante que es usada como categoría de servicio en ATM.
CE	*Customer Edge*. Nombre que se le da al enrutador que se encuentra en el borde de la red del cliente y se conecta a los equipos del proveedor de la red MPLS.

CIR	*Committed Information Rate*. Tasa de transferencia comprometida en una red de *Frame Relay* para un cliente.
CLP	*Cell Lost Priority*. Prioridad de pérdida de celda. *Bit* utilizado en la celda ATM para indicar si la misma debe descartarse.
CoS	*Class of Service*. Característica utilizada para diferenciar diversos tipos de servicio a través de una red.
CPE	*Customer Premises Equipment*. Nombre que se le da al equipo instalado en la casa del cliente.
CRC	*Cyclic Redundancy Check*. Secuencia de chequeo de trama.
Direccionamiento privado	Grupo o rango de direcciones IP asignados para utilizarse en redes privadas.
Direccionamiento público	Grupo o rango de direcciones IP asignados para utilizarse en *Internet*

DLCI *Data Link Connection Identifier*. Identificador de conexión de enlace de datos. Es usado en *Frame Relay* para identificar circuitos virtuales o PVC's.

DS0 *Digital Signal* 0. En jerarquías de señal digital equivale a un canal de 64 kbps.

Ethernet Estándar de transmisión para redes de área local que utiliza una velocidad de transmisión de 10 mega *bits* por segundo.

FasEthernet Estándar de transmisión para redes de área local que utiliza una velocidad de transmisión de 100 mega *bits* por segundo.

FECN *Forward Explicit Congestion Notification*. Notificación explícita de congestión en directa. *Bit* utilizado en *Frame Relay* para indicar congestión en el sentido directo de la transmisión de la trama.

FIB *Forward Information Base*. Tabla que utilizan los *Routers* para el envío de paquetes.

FRAD *Frame Relay Access Device*. Dispositivo de acceso *Frame Relay*.

Frame Relay Relevo de tramas. Modo de transmisión de datos basado en tramas que siguen circuitos virtuales.

FTP *File Transfer Protocol*. Protocolo para la transferencia de archivos que opera en la capa 4 del modelo de referencia OSI.

Fusión de VC VC *Merge*. Técnica que permite enviar celdas que vienen de dos VCI's entrantes, sobre un solo VCI saliente.

GFC *Generic Flow Control*. Campo de 4 *bits* en la celda ATM que es usado para funciones de control de flujo.

Gigabit Ethernet Estándar de transmisión para redes de área local que utiliza una velocidad de transmisión de 1000 mega *bits* por segundo.

HDLC *High Data Link Carrier*. Protocolo de capa 2 usado en *Routers* Cisco para empaquetamiento de datos.

HEC *Header Error Control*. Control de error de cabecera. *Bit* utilizado en la cabecera de ATM para detectar y corregir errores.

Interfase *Loopback* Interfase lógica en un enrutador no asociada a ninguna interfase física.

IP *Internet Protocol*. Protocolo para intercambio de datos a nivel 3 del Modelo OSI basado en direcciones IP.

IPv4 Ip versión 4. Esta versión utiliza direcciones de 32 *bits* y es la usada actualmente en todas las redes de datos.

IPv6 Ip versión 6. Esta es la nueva versión de IP que sustituirá la versión 4 y utilizará 128 *bits*.

ISDN *Integrated Services Digital Network*. Redes de marcado de servicios integrados. Ofrecen servicios de voz y datos a través de marcado.

IS-IS *Intermediate System to Intermediate System*. Protocolo de enrutamiento estandarizado por la ISO y utilizado ampliamente por su robustez y escalabilidad.

ITU-T *Internacional Telecommunication Union Telecomunication Standarization Sector.* Entidad normativa norteamericana para telecomunicaciones.

Kbps Kilo *bits* por segundo.

LAN *Local Area Networks*. Redes de área local.

LC-ATM *Label Controlled* ATM. Interfase que controla la distribución y negociación de las etiquetas o VC's.

LDP *Label Distribution Protocol*. Protocolo que se encarga de distribuir la información de las etiquetas asociadas a trayectorias a los LSR's.

LFIB *Label Forwarding Information Base*. Tabla de datos con la información asociada a la asignación de etiquetas de entrada, salida, FEC's e interfases.

LIB *Label Information Base*. Base de datos con las etiquetas aprendidas de otros LSR's más las etiquetas generadas localmente por el LSR.

Listas de Acceso Comandos de configuración que permiten filtrar tráfico en base a direcciones IP.

LMI *Local Management Interface*. Protocolo cíclico que verifica el estatus de la interfase entre el FRAD y el connmutador de *Frame Relay*.

Loopback Bucle. Puente físico o lógico entre la línea de transmisión y la línea de recepción en un enlace de datos, con el fin de realización de pruebas.

LSC *Label Switch Controlled*. Conmutador para el control y distribución y de las etiquetas o VC's.

LSP *Label Switched Path*. Trayectoria de etiqueta conmutada.

LSR *Label Switching Router*. Equipo o *Router* conmutador de etiquetas.

LSR ATM Conmutador ATM de etiquetas o VC's.

LVC *Label Switch Controlled Virtual Circuit*. Trayectoria de circuito virtual conmutado.

MetroEthernet Red de área metropolitana basada en el estándar de transmisión *Ethernet*.

Modelo OSI Modelo de referencia de 7 capas o niveles para construcción redes de datos.

MPLS *Multiprotocol Label Switching*. Multiprotocolo para conmutación de etiquetas. Arquitectura de envío de paquetes basado en trayectorias de etiquetas conmutadas.

Multicast Protocolo que replica la información que recibe a varios grupos o interfases. Su mejor aplicación es transmisión de video y videoconferencia.

***Multiprotocol* IBGP** Extensión del protocolo BGP que maneja las tablas de enrutamiento de las VRF's con sesiones BGP internas.

Multiplexor Conmutador de circuitos que concatena circuitos de baja velocidad en circuitos de alta velocidad.

Mux Multiplexor.

NNI *Network Node Interface*. Interfase de un equipo que se conecta a la red.

NRP *Node Route Procesor*. Nodo procesador de enrutamiento. Módulo que se encarga del proceso de enrutamiento.

NSP *Node Switching Procesor*. Nodo procesador de conmutación. Módulo que se encarga del proceso de conmutación de circuitos ATM.

OSPF *Open Shortest Path First*. Protocolo de enrutamiento de capa 3 cuya métrica se basa en el estado del link.

P Nombre que se le da al *Router* del Proveedor y que no está conectado al equipo del cliente.

PCM *Pulse Code Modulation*. Modulación por código de pulso. Técnica que transmite una señal de voz por un canal de 64 Kbps en un formato de 8 *bits* a 8,000 muestras por segundo.

PDU *Protocol Data Units*. Unidad de 48 *bytes* usada en las celdas de ATM.

PE *Provider Edge*. Nombre que se le da al *Router* del Proveedor que se conecta al equipo del cliente.

PIM *Protocol Independet Multicast*. Protocolo utilizado para redes *Multicast*.

Prefijos Agrupaciones de direcciones IP o subredes que se tienen en una tabla de enrutamiento.

PVC *Permanent Virtual Circuit*. Circuito configurado permanentemente en tecnologías de capa 2 como ATM o *Frame Relay*.

PVP *Permanent Virtual Path*. Trayectoria configurada permanentemente en una red ATM y que lleva varios VC's.

RD *Route Distinguisher*. Identificador de ruta. Valor de 8 *bytes* concatenado al prefijo de IPv4 para crear una VPN única para dicho prefijo.

RIP *Routing Information Protocol*. Protocolo de información de enrutamiento. Intercambia información de enrutamiento con otros enrutadores que corren el mismo protocolo con el fin de transmitir paquetes.

Router Enrutador, ruteador o encaminador de paquetes de capa 3 referenciado al Modelo OSI. Envía paquetes basándose en la información IP de los mismos y en la tabla de enrutamiento que posee.

Route Reflector Enrutador que maneja sesiones de *Multiprotocol* IBGP centralizadas con el fin de evitar configuraciones de malla a nivel de sesiones.

RT *Route Target*. Ruta objetivo. Comunidad extendida que identifica tablas de enrutamiento de las VPN's.

SVC *Switched Virtual Circuit*. Circuito virtual conmutado que es establecido sólo bajo demanda y una vez terminada la transmisión sobre el mismo es eliminado.

TCP *Transmision Control Protocol*. Protocolo de control de transmisión. Ubicado en el nivel 4 del Modelo Osi,

	controla la transmisión de información de capas superiores y garantiza que las mismas lleguen en correctamente.
TDM	*Time Division Multiplexing*. Técnica que transmite información en varios canales en distinto período de tiempo por el mismo medio.
Time Slot	Canal de determinado ancho de banda por el cual TDM enviará información a la velocidad de dicho canal en cierto período de tiempo.
TTL	*Time To Live*. Campo localizado en el encabezado IP cuyo valor disminuye mientras pasa por cada salto de la red, con el objetivo evitar que un paquete quede circulando por la red en caso de un bucle de enrutamiento.
UBR	*Unspecified Bit Rate*. Tasa de transmisión no especificada que le da la menor prioridad al tráfico sobre una red ATM.
UNI	*User Network Interface*. Interfase en un equipo que se conecta al equipo del cliente.
Unicast	Modo de envío de paquetes hacia un solo destino.

VBR-NRT *Variable Bit Rate Non Real Time*. Categoría de servicio de ATM para tráfico de ráfaga variable y no crítico por no ser en tiempo real.

VBR-RT *Variable Bit Rate Real Time*. Categoría de servicio de ATM para tráfico de ráfaga variable que es crítico debido a que es en tiempo real.

VCI *Virtual Channel Identifier*. Es el identificador del canal o circuito virtual dentro de la trayectoria virtual.

VPI *Virtual Path Identifier*. Identificador Virtual de la trayectoria de un grupo de VCI's.

VPN *Virtual Private Network*. Red privada virtual que puede ser sobre tecnologías tradicionales o sobre MPLS.

VPN V4 Extensión de *Multiprotocol* IBGP para el envío de tablas de enrutamiento virtuales a través de la red MPLS para las distintas VPN's.

VRF	*Virtual Routing and Forwarding*. Enrutamiento virtual y de envío independiente y separado para cada VPN configurada en la red MPLS.
VSI	*Virtual Switch Interface*. Interfase virtual entre el LSC y el conmutador ATM.
WAN	*Wide Area Network*. Red de área extendida.

RESUMEN

En el presente trabajo de graduación se comentan y analizan las características de las redes privadas virtuales, implementadas sobre la nueva tecnología para el envío de paquetes, que es MPLS. Para tener claro dicho panorama, se hace necesario hacer una breve descripción de cómo las tecnologías tradicionales de transmisión han servido de transporte e infraestructura básica, a lo que son las VPN's tradicionales. En cuanto a lo que es MPLS, se da una descripción de su funcionamiento y de su gran versatilidad para el envío de paquetes sobre una red IP.

Para lo que es la descripción y explicación de lo que son las VPN's sobre MPLS, se analizan los dos escenarios más comunes que son, la implementación de VPN's en redes de Modo de Paquetes y la implementación de VPN's en redes de Modo ATM Nativo. De esta descripción anterior se notará la ventaja de la implementación en Modo de Paquetes.

Haciendo entonces una comparación entre las implementaciones tradicionales de VPN's y las implementaciones sobre MPLS. Se nota rápidamente que las VPN's sobre MPLS sobrepasan en ventajas a la implementaciones tradicionales, notándose también la reducción de los costos y la facilidad de implementación. Finalmente, se presenta una propuesta de implementación, basándose dicha propuesta, en las guías de diseño descritas y presentando un escenario bastante común en nuestro medio, de tal forma que

el lector tendrá las herramientas suficientes para diseñar redes VPN sobre MPLS, encontrando propuestas que abarcan todos los escenarios más comunes encontrados en nuestro medio.

HIPÓTESIS

El uso de tecnología MPLS para la implementación de VPN´s por medio de VRF´s en equipo Cisco a partir de la versión 12.0 le permite a los proveedores de servicios de datos reducir sus costos de implementación, obtener una red con mayor escalabilidad, simplificar la configuración, facilitar el manejo y tener una mejor estructura de la red.

OBJETIVOS

GENERAL

Proveer una herramienta de información para el diseño de redes privadas sobre una red MPLS, lo cual permitirá a la persona que lea este trabajo de graduación, obtener el conocimiento básico necesario para poder trabajar sobre la tecnología MPLS.

ESPECÍFICOS

1. Explicar qué es el MPLS y como funciona.

2. Explicar y dar a entender cómo se crea una VRF y cómo se implementa en una Red con MPLS.

3. Establecer una comparación entre una VPN en una red tradicional y una VPN montada sobre MPLS.

4. Proponer Diseños para implementación de VPN´s sobre MPLS en los escenarios de transmisión más comunes de nuestro medio.

INTRODUCCIÓN

En nuestros días puede notarse muy claramente que la era digital está avanzada, que el *Internet* es una necesidad y que las redes de datos se han convertido en una herramienta indispensable para la infraestructura de los países. De aquí la importancia de poder proveer redes de datos confiables y económicas para los distintos sectores que lo requieran en una comunidad. De esta necesidad surgen proveedores de servicios, que construyen infraestructuras digitales para poder soportar estas redes y que con el paso del tiempo se han vuelto costosas y difíciles de ampliar

Esta situación ha impulsado a los fabricantes de equipos a usar técnicas más eficientes en la construcción de redes. Adicionalmente uno de los grandes objetivos es aprovechar la infraestructura existente, ya que el costo no deja de ser importante a la hora de implementar redes y definitivamente el mismo será menor, si la red se actualiza sobre infraestructura existente. De aquí surge la primera opción de desarrollo sobre redes IP, ya que la infraestructura existente en las mismas permite hacer varios desarrollos a nivel de sistemas operativos, haciendo solamente actualizaciones de memoria a los equipos existentes para soportar las nuevas funcionalidades. Es aquí donde surge la tecnología MPLS y una de sus principales aplicaciones que son las VPN's. Iniciaremos entonces el estudio describiendo la evolución tecnológica desde las tecnologías de transmisión tradicionales.

1. INTRODUCCIÓN A LAS TECNOLOGÍAS TRADICIONALES PARA REDES DE ÁREA EXTENDIDA

Desde el momento en que aparece la digitalización de la información, tanto para datos como para la voz, se hace necesario transportar los mismos. Las tecnologías para el transporte de información digital se pueden ubicar en las capas 1 y 2 del Modelo OSI. Comúnmente en nuestro medio se les conoce como tecnologías de Capa 2. Aunque en su momento hubo desarrollos de varias tecnologías para suplir las necesidades de transporte, en Guatemala y a nivel mundial, se popularizaron y se volvieron más comunes tres tecnologías básicas que son TDM, *Frame Relay* y ATM.

Estas tecnologías en su momento se adaptaron para transportar circuitos de voz, como también para interactuar con protocolos de capa 3 para la transmisión específica de datos. El protocolo de capa 3 que predominó sobre otros es IP. Por varios años el campo de las telecomunicaciones basó su transporte en complejas redes que se interconectaban utilizando estándares específicos y adicionalmente formaron la base de transporte para la red IP más grande que hay hasta el momento que es *Internet*.

Es de hacer notar la importancia que tiene el comprender el funcionamiento de estas tres tecnologías, que inicialmente fueron conocidas como tecnologías de transporte para redes de área extendida, WAN, por sus siglas en inglés. Estos tipos de transmisión tendrán la función de transportar la información, tanto por redes públicas como por redes privadas.

1.1 Multiplexación por división de tiempo TDM

Como su nombre los indica, TDM envía una ráfaga de información en un determinado período de tiempo. El objetivo de esto es poder enviar varias ráfagas y en cada una de éstas información distinta. Si se hace lo anterior sobre un mismo canal de transmisión de una manera repetitiva obtendremos, desde el punto de vista del usuario, circuitos virtuales de diferentes velocidades, las cuáles dependerán de cuántos períodos de tiempo (*time slot*) sean asignados a la ráfaga o flujo de datos.

Para modular la información se utiliza PCM, cuyas siglas significan modulación por código de pulso. Generalmente las llamadas de voz necesitan 4 kHz de ancho de banda. Esta señal es muestreada 8,000 veces por segundo y la información es cuantificada dentro de un número binario de 8 *bits*, o sea, dentro de este número tenemos 2 elevado a la 8 que son 256 niveles para registrar la señal inicial. Este tipo de modulación resulta en un canal con una tasa de transferencia constante de 64 kilo *bits* por segundo, es decir, 8,000 muestras por segundo X 8 *bits* por muestra da como resultado un canal o flujo de 64 kbps. Este canal es llamado DS0, Señal Digital 0 por sus siglas en inglés, corresponde a un TS o *Time Slot* que lo llamamos anteriormente período de tiempo. El DS0 es la base para la jerarquía de señal digital, que básicamente tiene 2 normas, la americana y la europea. La tabla I muestra ambas normas. Generalmente el circuito físico sobre el medio de transmisión, ya sea de cobre o óptico, se conoce como T1. Por ejemplo, se habla de habilitar un T1 o T3, que sería DS1 y T3 respectivamente, en la jerarquía de Señal Digital.

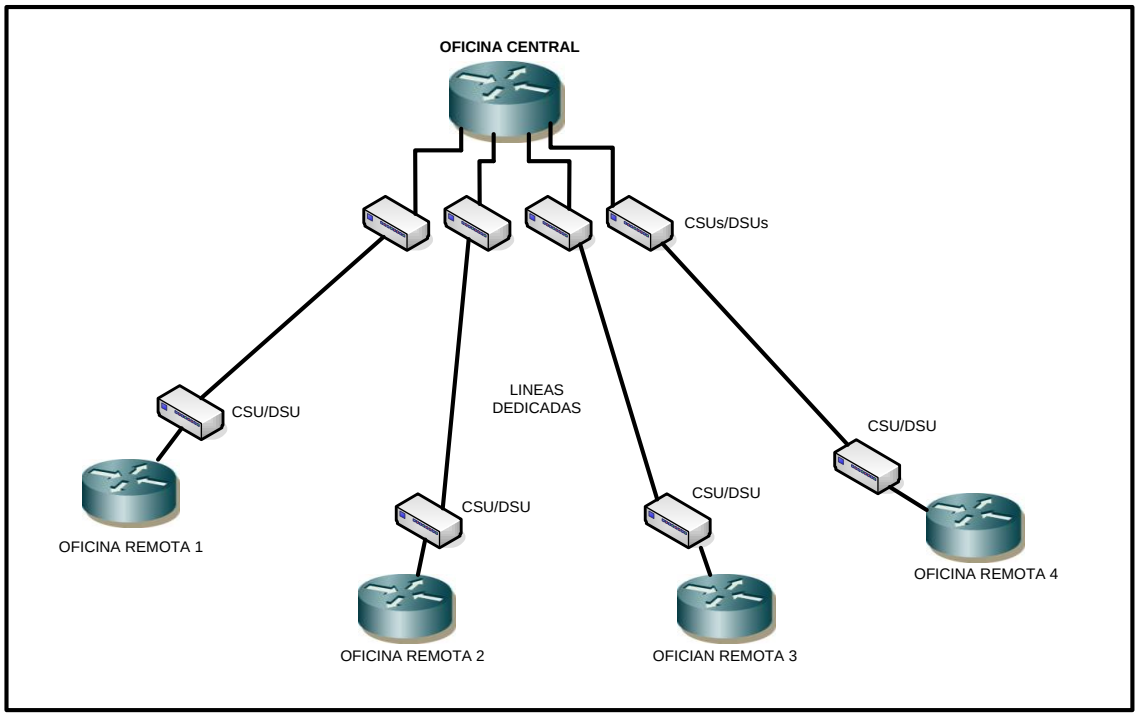
Tabla I. **Jerarquías de señal digital**.

Norma	Nivel de Señal Digital	Número de Canales de 64 kbps	Equivalente	Ancho de Banda
Americana	DS0	1	1 x DS0	64 kbps
Americana	DS1	24	24 x DS0	1.544 Mbps
Americana	DS2	96	4 x DS1	6.312 Mbps
Americana	DS3	672	28 x DS1	44.736 Mbps
Americana (SONET)	OC3	2400	100xDS1	155 Mbps
Americana (SONET)	OC12	9624	401xDS1	622 Mbps
Americana (SONET)	OC48	38544	1606xDS1	2.5 Gbps
Americana (SONET)	OC192	154176	6424xDS1	10 Gbps
Americana (SONET)	OC768	616776	25699xDS1	40 Gbps
Europea	E1	30	30 x DS0	2.048 Mbps
Europea	E3	480	480 x DS0	34 Mbps
Europea (SDH)	STM-1	2400	100xDS1	155 Mbps
Europea (SDH)	STM-4	9624	401xDS1	622 Mbps
Europea (SDH)	STM-16	38544	1606xDS1	2.5 Gbps
Europea (SDH)	STM-64	154176	6424xDS1	10 Gbps
Europea (SDH)	STM-256	616776	25699xDS1	40 Gbps

Los circuitos o grupos de circuitos que hemos mencionado, utilizan multiplexores que son conocidos como Unidades de Servicio de Circuito, o bien, unidades de servicio digital; CSUs y DSUs respectivamente. Estas unidades o equipos se instalan en los puntos donde el cliente requiere el servicio. Para poder interconectar estas unidades existen los sistemas de crosconexión y de acceso digital, DACS por sus siglas en inglés y están instalados en las oficinas del proveedor, o si la red es extensa, en nodos distribuidos geográficamente. Esta estructura le permite al proveedor dar soluciones punto a punto, o lo que se conoce como líneas dedicadas. Las líneas dedicadas se han usado extensamente para proveer las soluciones de redes privadas virtuales a los clientes.

La figura 1 muestra como se vería una VPN tradicional desde el punto de vista de un usuario que quiere interconectar cuatro oficinas remotas a una oficina central.

Figura 1. **VPN Tradicional.**

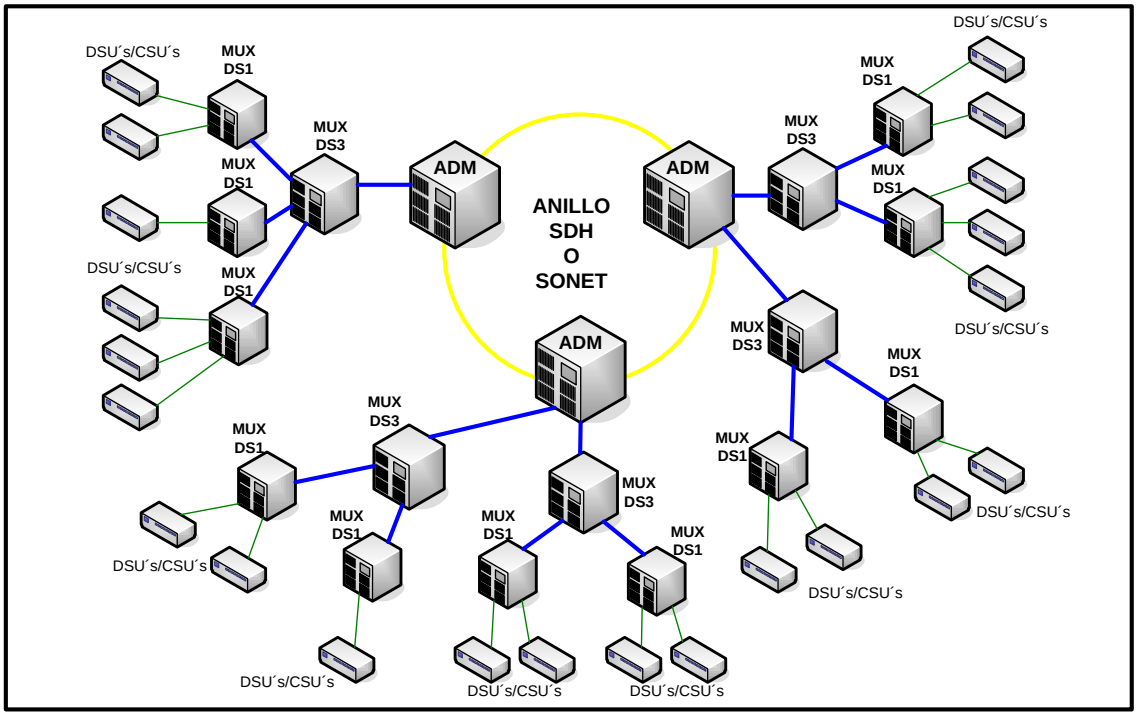


Cuando las redes de este tipo se extienden mucho y tienden a crecer, el proveedor se auxilia de una red de trasporte más robusta, tanto en ancho de banda como en tipo de estructura. Para esto surgen dos tipos de redes de transporte, la primera es en base a los estándares Norteamericanos (ANSI) y llama red óptica síncrona (SONET, por sus siglas en inglés). El estándar europeo se llama jerarquía digital síncrona (SDH, por sus siglas en inglés), este estándar tiende a usarse en el resto del mundo. Los niveles de transporte para estas redes se muestran también en la tabla I. Estas redes utilizan en su

núcleo de red multiplexores de inserción/extracción (ADM, por sus siglas en inglés). Los ADM's suman los circuitos de menor nivel y los montan sobre un solo canal de transporte de mayor nivel.

Por la cantidad de tráfico que manejan, los ADM's suelen interconectarse en topologías que permitan una buena redundancia. Estas topologías son anillo, malla y malla parcial. La más común por su bajo costo es la de anillo. Desde el punto de vista de un proveedor de servicio la red de transporte luciría como en la figura 2.

Figura 2. **Red de transporte.**



En la figura 2 puede observarse claramente como la Jerarquía de Nivel de Señal va aumentando desde el equipo remoto hasta llegar al nodo principal. Por medio de la configuración de circuitos a través de estas redes se obtienen los enlaces o líneas dedicadas que el cliente usa para crear sus VPN's.

Debido a su estructura las líneas dedicadas tienen la ventaja de proveer una buena seguridad y beneficios de control. Por ser líneas dedicadas no se suele tener problemas de disponibilidad de ancho de banda como sucede en un medio compartido, en el cual la disponibilidad de ancho de banda es estadística y representa un problema en algunas ocasiones. El circuito está creado permanentemente y no requiere establecer una conexión para transferir datos, sin embargo esta otra ventaja trae la desventaja inherente de uso ineficiente del ancho de banda. Esto se debe a que se está pagando por un ancho de banda que se usa de un 40 a 70 por ciento del tiempo en el mejor de los casos, lo que trae como consecuencia un gasto excesivo debido a que este tipo de enlaces es muy costoso.

1.2 Relevo de tramas *FRAME RELAY*

El relevo de tramas o *Frame Relay* surge como una tecnología intermedia entre lo que son las tecnologías TDM y ATM. Surge del estándar establecido por la ANSI y la ITU-T, adicionalmente se auxilia del *Frame Relay Forum* para lograr la interoperabilidad entre los distintos proveedores.

Frame Relay opera en el nivel 2 del modelo OSI y reduce considerablemente sus encabezados a nivel de trama ya que asume la no

existencia de errores a nivel de capa 2. Esto quiere decir que básicamente, *Frame Relay* confía en protocolos de capa superior, como lo es TCP, para corregir cualquier error a nivel de capa física. El algoritmo que utiliza *Frame Relay* para la corrección de errores a nivel de trama está basado en el polinomio de 16 *bit* CRC. Este polinomio provee detección de errores para tramas de hasta 4,096 *bytes* de longitud.

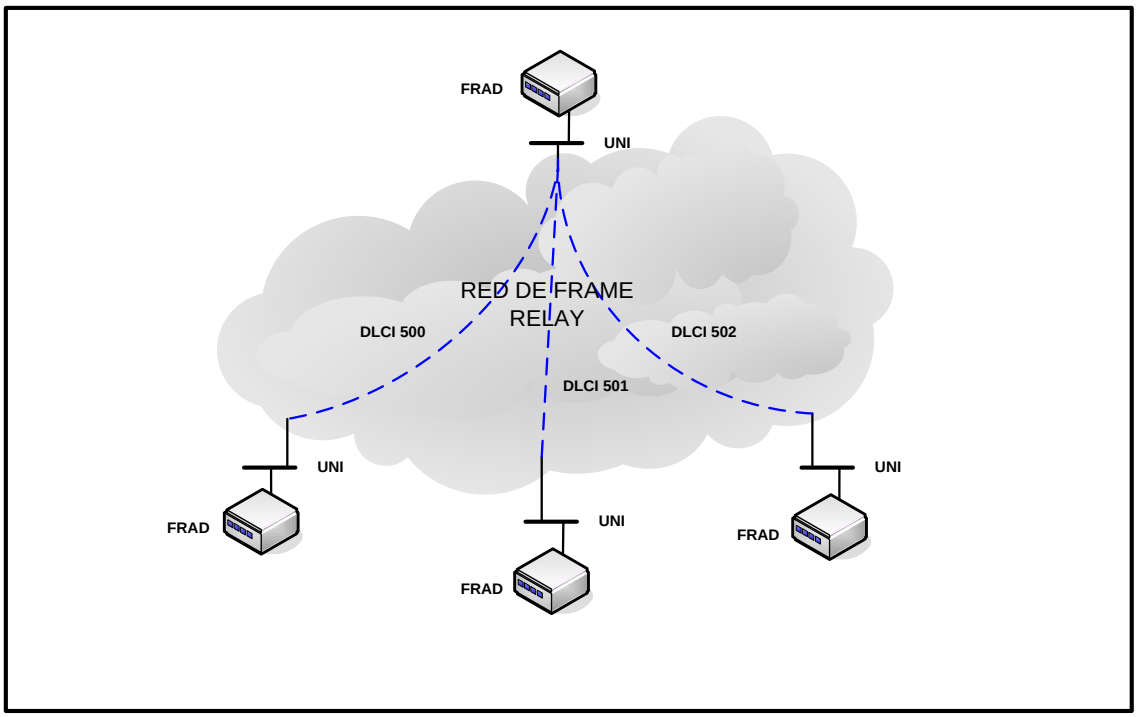
La diferencia básica que tiene *Frame Relay* con las tecnologías que le preceden, es la aparición de Circuitos Virtuales Permanentes o PVC's (por sus siglas en inglés). Estos PVC's son canales lógicos entre los Dispositivos de Acceso de *Frame Relay* (FRAD, por sus siglas en inglés) y la red propia de *Frame Relay*. Otro concepto asociado a los que son los PVC's son los Identificadores de conexión de línea de datos o DLCI's. El DLCI básicamente es la identificación para cada PVC creado. Un DLCI tiene una ruta predeterminada para la trayectoria de las tramas. De esta manera pueden crearse a través de la red de *Frame Relay*, circuitos que interconectan varios sitios o oficinas para los usuarios y de esta manera se construyen las VPN's para los mismos. El DLCI tiene significado local y suele asignársele un valor entre 1 y 1,022. Los PVC's son creados desde la Interfase de Red de Usuario (UNI, por sus siglas en inglés) a través de la red de *Frame Relay*, hasta llegar a su punto remoto que es otra UNI. La interfase UNI es la demarcación entre el FRAD y la red *Frame Relay.*

Otra de las ventajas que posee *Frame Relay* es un mejor aprovechamiento del ancho de banda. Esto se logra por medio del uso de la Rata de Información Comprometida o CIR. Es un parámetro que se aplica en los circuitos virtuales y permite el control de la velocidad de transferencia de los datos.

En un evento de congestión en la red las ráfagas de transferencia que excedan el valor del CIR, serán marcadas y eventualmente descartadas de la red. Para entender un poco mejor como funciona el CIR veamos este ejemplo; tenemos un enlace de 256 kbps, sobre el mismo hay 3 PVC's configurados; el primer PVC lleva el tráfico de datos crítico y se le asigna un CIR de 128 kbps; el segundo PVC lleva tráfico FTP y el tercer PVC lleva el tráfico de aplicaciones no críticas, por lo tanto se le asigna a cada uno un CIR de 32 kbps. Si vemos, la suma del CIR es de 192 kbps, lo que está bien ya que está dentro del rango de la velocidad del enlace. Si en algún enlace la suma del CIR llega a exceder la velocidad del enlace se le conoce con el nombre en inglés de *oversubscription*, que no es más que exceder la capacidad de ancho de banda del enlace con la suma de las tasas de transferencia comprometidas. La mayoría de los proveedores no configuran enlaces con *oversubscription* ya que esto afecta directamente los niveles de calidad de servicio acordados con el cliente. A continuación se muestra en la figura 3, un ejemplo de una red *Frame Relay* que interconecta 4 puntos diferentes e ilustra la creación de circuitos virtuales que interconectan estos puntos simulando una VPN tradicional.

Para que la interacción entre la UNI y el FRAD, el estándar de *Frame Relay* utiliza el protocolo llamado Interfase Local de Gestión o LMI (por sus siglas en inglés). El protocolo LMI básicamente interroga periódicamente a la red sobre su estatus y verifica la integridad del enlace, el estatus de los PVC's y si existen errores en la red.

Figura 3. **Red de *Frame Relay***



Por último, se tiene una de las características innovadoras, que en su tiempo, introdujo *Frame Relay*. Esta es el control de congestión. El control de congestión se logra por medio de el uso de dos *bits* que se llaman FECN y BECN. La función del primero consiste en notificar congestión al nodo de *Frame Relay* que está en la dirección del flujo de tráfico. El segundo hace la notificación en el sentido inverso a la dirección del flujo de tráfico. Adicionalmente de la notificación explícita de congestión, que es la que acabamos de analizar, existe la notificación implícita. La notificación implícita suele ser más compleja y se basa en protocolos que corren entre los FRAD's y una Terminal que es la que controla y monitorea las condiciones de la red.

Como conclusión se puede decir que la tecnología *Frame Relay* fue una muy buena alternativa para los proveedores de servicio debido a sus características de bajo costo y versatilidad para redes de acceso menores a un DS3. La desventaja de estas redes es el constante análisis y monitoreo que se debe hacer sobre el tráfico para que la calidad del servicio no decaiga en determinado momento y se afecte el servicio entregado a los usuarios.

1.3 Modo de transferencia asíncrona ATM

El Modo de Transferencia Asíncrona o ATM, es el último en nuestra lista de tecnologías tradicionales que estamos analizando brevemente antes de entrar al tema principal del presente trabajo. Esta tecnología de transmisión surge como estándar de la ITU-T que fue diseñada para BISDN, o sea, el término en inglés *Broadband* ISDN.

ATM es un tipo de transmisión orientado a la conexión, es decir, se necesita establecer primero una conexión entre dos puntos específicos de la red para que exista una transferencia de tramas. La forma en la que estas tramas están formadas es un poco diferente a las tramas que hemos visto anteriormente, de hecho, tienen hasta un nombre diferente, se les conoce como celdas. Estas celdas tienen como primera característica una longitud constante que es de 48 *bytes*. A estos segmentos se les conoce como Unidades de Protocolo de Datos o PDU's. A estos PDU's se les adiciona un encabezado de 5 *bytes*, conocido como encabezado de ATM. Como resultado tenemos una "celda" de 53 *bytes* de longitud que podemos visualizar como contenedores en donde se toman los datos de capas superiores, se fragmentan (si es necesario) y se acomodan entre estas celdas para su respectiva transmisión en la red

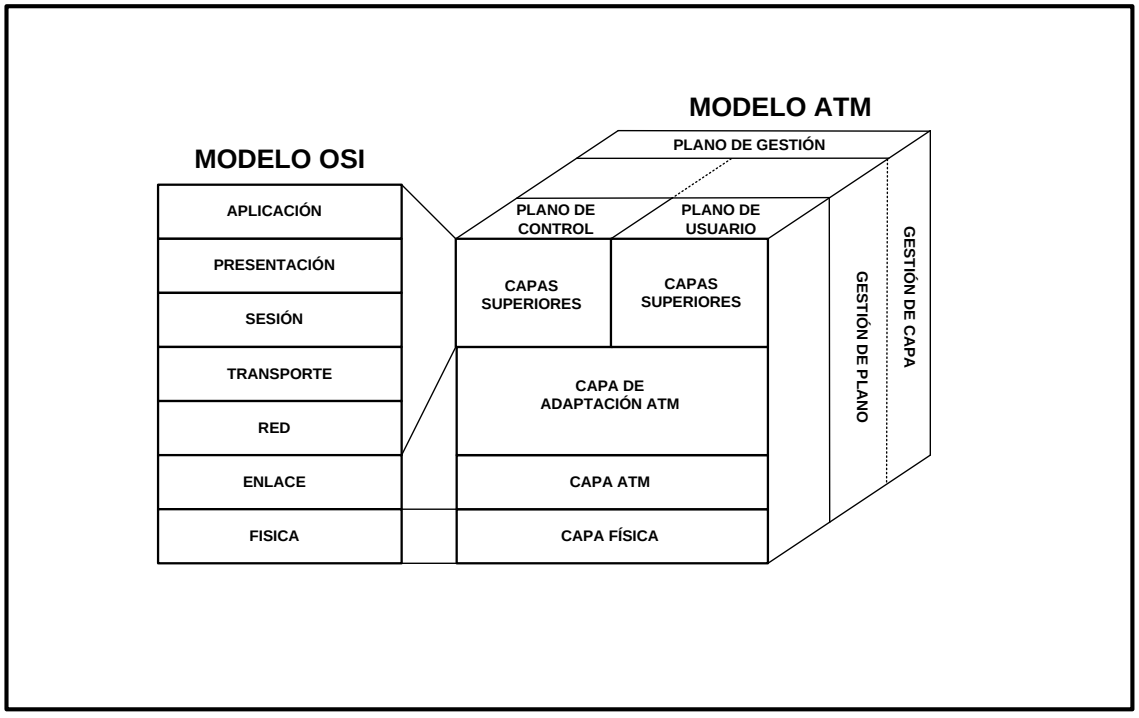
ATM. Para que estas celdas puedan moverse a través de la red, se identifican con dos nombres que son el identificador virtual de trayectoria o VPI y el identificador virtual de canal o VCI; juntos reúnen la información necesaria para el tránsito exitoso de las celdas en la red. El tiempo de llegada o retardo de un grupo particular de celdas no es necesariamente periódico. De ahí entonces el nombre de Transferencia Asíncrona, que denota la particularidad de transferencia asíncrona de las celdas, que es totalmente lo contrario con el transporte sincronizado como TDM, que transmite y recibe en períodos específicos de tiempo.

Inicialmente la tecnología ATM fue creada para ser una solución de extremo a extremo, es decir, se pensaba que la misma sustituiría las tecnologías WAN y LAN a nivel mundial y sería la principal elección de los Proveedores de Servicio para el trasporte de voz, video y datos. Se esperaba que la parte de Emulación de Redes Lan fuera de uso extendido, sin embargo la misma no tuvo éxito y fue sustituida por las tecnologías *Fast Ethernet* y *Gigabit Ethernet*. Estos protocolos son mucho más simples y fáciles de implementar, por lo que la mayoría de Empresas grandes y pequeñas optaron por la implementación de los mismos.

Analicemos entonces, la parte en donde ATM sí tuvo un impacto significativo y debido a su revolucionaria estructura fue por varios años, la tecnología preferida de los países que iban a la vanguardia de la tecnología. Para iniciar debemos destacar el considerable aumento de la “inteligencia” en este modo de transmisión. Tal vez con lo visto hasta ahora no sea evidente la anterior información, pero conforme analicemos brevemente la estructura de esta tecnología entenderemos mejor esta gran ventaja que tiene este modo de

transmisión. Como siempre con una gran ventaja viene una desventaja, que en este caso es el alto nivel de complejidad de una red ATM y que también se ve reflejado en un costo alto. Debido a lo anterior la mayoría de las redes ATM están destinadas a ser sustituidas a mediano plazo por nuevas redes que buscan reducir los costos y facilitar la implementación. Iniciemos entonces por el modelo OSI, es un modelo que nos ha servido de mucho para entender como funcionan las redes de datos. El mismo se representa en un plano de dos dimensiones y se compara al modelo de ATM que como se podrá ver en la Figura 4 es un modelo de 3 dimensiones (empieza la parte compleja).

Figura 4. **Comparación de modelo OSI y modelo ATM**



Analicemos brevemente la función de los Planos y las Capas de ATM, basándonos en la figura 4.

1.3.1 Modelo de planos ATM

Para poder controlar la señalización, la transferencia de datos del usuario y la gestión; ATM utiliza los siguientes Planos:

- **Plano de control**: controla la señalización, tanto generación como los requerimientos.

- **Plano de usuario**: controla la transferencia de los datos.

- **Plano de gestión**: consta de dos componentes, Gestión de Capa y Gestión de Plano. La Gestión de Capa maneja las funciones específicas de la capa como detección de fallas y problemas de protocolo. La Gestión de Plano maneja y coordina las funciones relacionadas con el sistema completo.

1.3.2 Capas ATM

Analicemos ahora la parte que interactúa con transporte de protocolos de capas superiores:

- **Capa Física**: se encarga de manejar el medio de transmisión.

- **Capa ATM**: se encarga de establecer las conexiones y realizar la transferencia de las celdas.

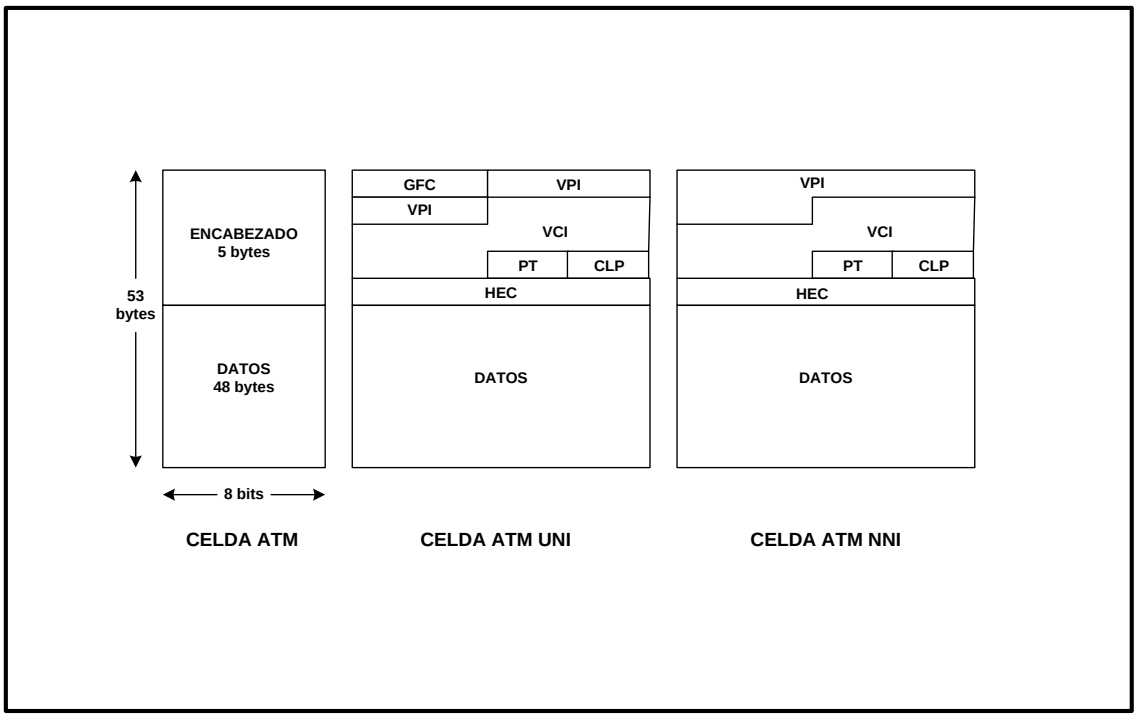
- **Capa de Adaptación ATM**: en conjunto con la Capa ATM, esta capa se encarga de tomar los datos de capas superiores y los adapta al formato de celdas existentes para su envío.

1.3.3 Celdas ATM

Para ver como la complejidad va en aumento, veamos brevemente como está formada la celda ATM. En la figura 5 podemos ver como está constituida la celda ATM.

Como habíamos observado anteriormente, la celda ATM tiene un tamaño de 53 *bytes*, de los cuales 5 *bytes* son de encabezado y 48 son para el transporte de datos. Existen dos tipos de formatos de encabezado. El primero es UNI, o sea, interfase de red de usuario. El segundo es NNI, o sea, interfase de nodo de red. Los anteriores formatos diferencian las celdas que se intercambian, tanto del lado de red, como en las interfases de cara al usuario. A continuación veremos una breve descripción de cada uno de los campos de la celda.

Figura 5. **Celda ATM**



- **Control Genérico de Flujo GFC**: es un campo de 4 *bit* cuya función principal es el control de flujo.

- **Identificador Virtual de Trayectoria VPI**: es un campo de 8 *bit* que identifica la trayectoria que tomará la Celda.

- **Identificador Virtual de Canal VCI**: es un campo de 16 *bit* que identifica un canal específico dentro de una trayectoria (VPI).

- **Tipo de Datos PT**: es un campo de 3 *bit* que identifica el tipo de información contenida en la parte de Datos de la Celda.

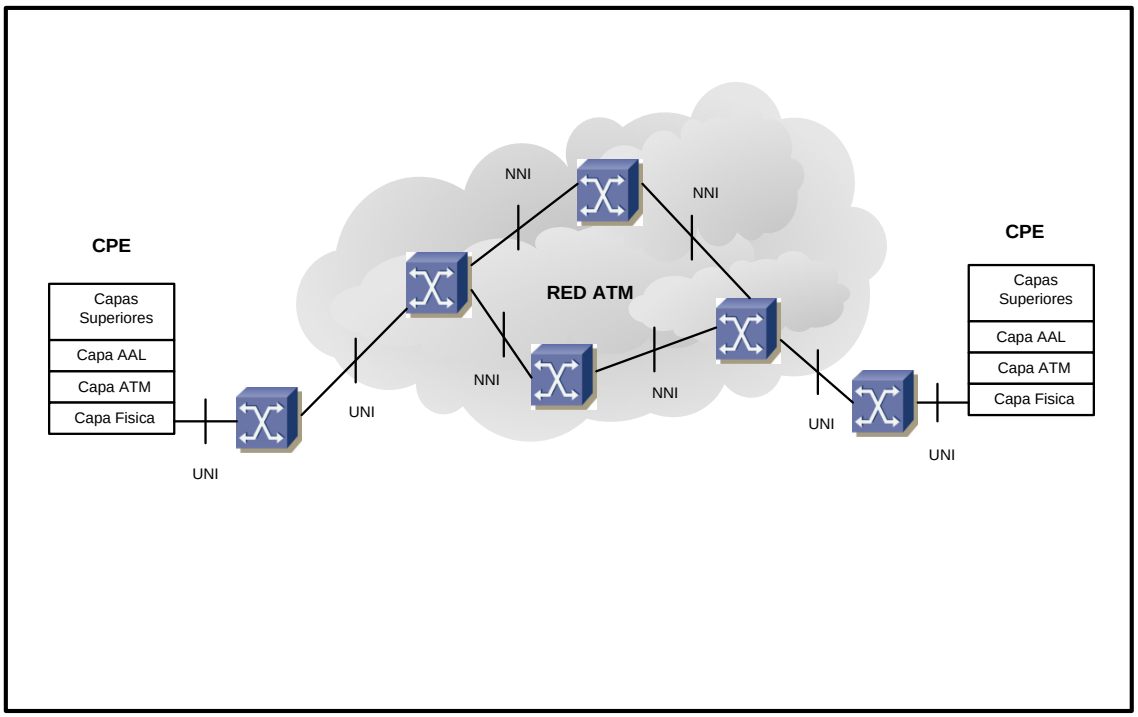
- **Prioridad de Pérdida de Celda CLP**: es un solo *bit* que indica la prioridad para descarte de Celda.

- **Control de Error de Encabezado HEC**: es un campo de 8 *bit* que detecta o corrige errores en el encabezado.

1.3.4 Generación de celdas ATM

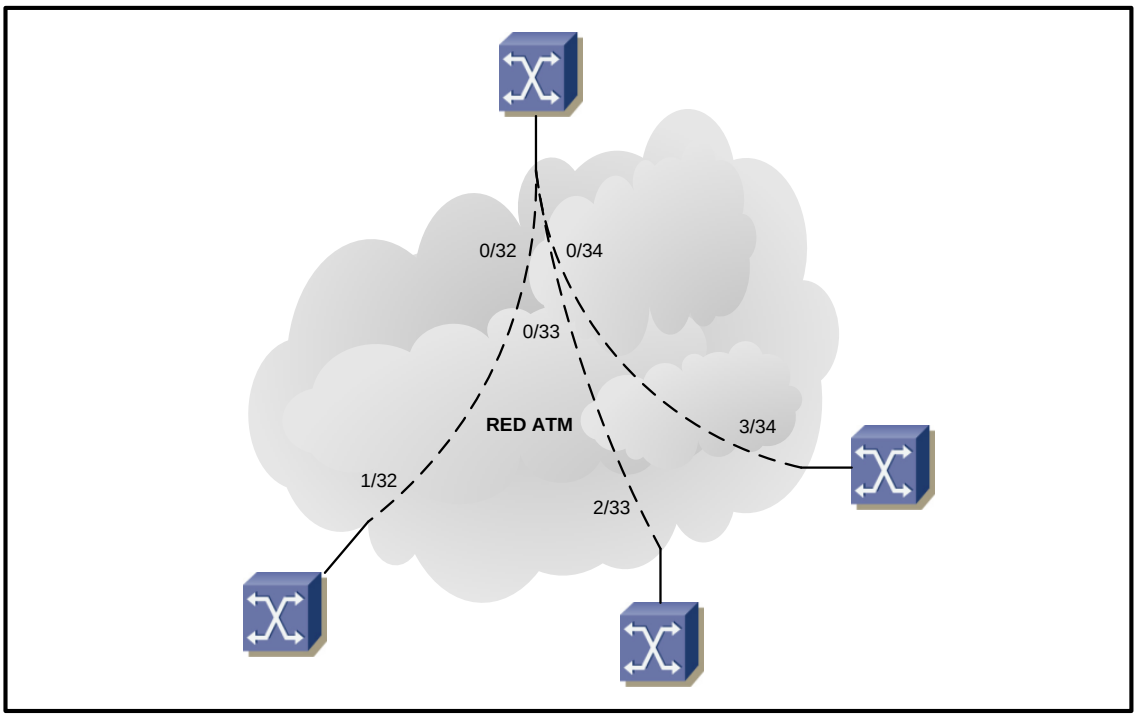
Llegamos al punto en el cual debemos entender cómo se generan las Celdas en una Red ATM. El proceso inicia cuando el CPE toma toda la información de las capas superiores y pasa la información a la capa de adaptación de ATM (AAL), que como recordaremos, es la encargada de adaptar la información que se recibe al formato de celdas ATM. Esta adaptación va a depender del tipo de Datos que se manejen. Una vez hecha la adaptación, la información pasa a la capa ATM, que es la encargada de generar las celdas con el formato de 48 *bytes* e insertar en el mismo la información a transmitir. Por último, la información pasa a la capa física, la cual enviará la información de a cuerdo al protocolo de transmisión que se esté trabajando. En la figura 6 se muestra un diagrama que nos ayuda a ilustrar el proceso anteriormente mencionado y nos da la perspectiva de la red ATM desde el punto de vista del Proveedor de Servicio.

Figura 6. **Red ATM**



Una vez que las celdas están creadas y se están enviando a través del medio físico, es la parte de canales virtuales la que se encarga de llevar las Celdas hasta su destino final basándose en la información que traen las mismas. El par de información VPI/VCI es la clave para poder construir sobre la red física una red virtual que entregue las Celdas generadas en los extremos de la red hacia sus respectivos destinos. Los canales virtuales creados, generalmente se usan para proveer VPN's a los Usuarios. En la figura 7 se ilustra una Red ATM desde el punto de vista del Usuario del Servicio. En esta figura se ilustra la conexión lógica que da origen a la VPN.

Figura 7. **Red ATM lógica**



1.3.5 Calidad de servicio en ATM

La calidad de servicio es una de las cualidades importantes que se introduce en esta tecnología de transmisión. En sí la calidad de servicio es el tratamiento que le damos al tráfico que estamos transportando. Si el equipo nos permite ofrecer una mayor prioridad para tráfico importante, descartar tráfico no crítico en horas de congestión y limitar velocidades en algunas aplicaciones, permitirá al Proveedor de Servicio poder ampliar su carta de servicios hacia el Usuario, teniendo como resultado un beneficio mutuo.

El Foro ATM define las siguientes calidades de servicio, que describiremos brevemente,

- **Clase A, Rata Constante de *Bit* CBR**: esta clasificación se aplica al tráfico considerado como crítico en la red, es decir, no tolera retardos ni descarte de paquetes. Esta configuración simula un canal dedicado, que generalmente se entrega con tecnología TDM.

- **Clase B, Rata Variable de *Bit* Tiempo Real VBR-RT**: es una clasificación para tráfico generado en ráfagas, pero por estarse realizando en tiempo real no tolera los retardos. Los ejemplos de este tipo de tráfico son la voz y el video aplicados por ejemplo a una videoconferencia.

- **Clase C, Rata Variable de *Bit* Tiempo No Real VBR-NRT**: es también una clasificación para tráfico generado en ráfagas, pero con la diferencia de que el retardo no es crítico. Un ejemplo es la descarga de Cursos Virtuales, Videos, etc.

- **Clase D, Rata de *Bit* Disponible ABR**: en esta clasificación está todo el tipo de tráfico que es más tolerante a los retardos y pérdida de paquetes.

- **Clase D, Rata de *Bit* no Especificada UBR**: es similar a la anterior y se utiliza para clasificar el restante de tráfico que no es afectado por los retardos y las pérdidas de paquetes.

Con esta última característica de la red ATM (QoS), terminamos de analizar la tecnología más completa, de las 3 que analizamos, para la transmisión de datos y la construcción de VPN's tradicionales. Como podemos ver la mejor tecnología, desde un punto de vista global, es la ATM; sin embargo, se destaca que la mayoría de las características que la hacen más versátil que sus antecesoras, también la hace más compleja. Conforme el tiempo transcurrió, los fabricantes y desarrolladores de tecnologías de red, empezaron a buscar tecnologías que los hicieran más competitivos en el mercado. Uno de los objetivos para lograr una buena competitividad es disponer de tecnologías baratas y de fácil implementación. Debido a esto, se empezó a desarrollar más soluciones de transmisión en IP ya que es el protocolo de capa 3 más difundido y proporciona mucha flexibilidad para desarrollo ya que es un modelo de paquetes. Como conclusión vemos que las tecnologías tradicionales para la Transmisión y creación de VPN's serán reemplazadas a mediano plazo por redes Ip.

2. ARQUITECTURA MPLS

Las iniciales vienen del nombre en inglés *Multiprotocol Label Switching*. Una traducción bastante aproximada a nuestro idioma sería multiprotocolo para conmutación de etiquetas. De cualquier forma, la manera más común a la que se conoce este protocolo es simplemente con sus iniciales, MPLS. La intención de la palabra Multiprotocolo es tratar de enfatizar que esta arquitectura de conmutación de etiquetas puede ser aplicable a cualquier protocolo de capa de red; sin embargo, este trabajo de graduación se enfoca a la aplicación que ha tenido en el protocolo IP versión 4.

Para entender un poco la aparición de este protocolo es bueno recordar la manera en que funcionan las redes IP. Las redes IP basan su funcionamiento en un modelo de paquetes y direcciones IP. Las direcciones IP son los identificadores de los elementos de red a través de los cuales se envían paquetes con información. Los paquetes son enviados a través de la red en base a una dirección IP origen y una dirección IP destino que van en el encabezado del paquete. Estos paquetes llevan información hacia los equipos, que regularmente son computadoras, con fines diversos (el ejemplo más común e ilustrativo es el acceso a *Internet* y sus diversas aplicaciones). Los equipos encargados de encaminar estos paquetes a través de la red son los enrutadores o como son conocidos comúnmente *Routers*. El *Router* es la columna vertebral de las redes IP debido a la función vital de envío de paquetes. El *Router* se auxilia de la tabla de enrutamiento en donde tiene la información necesaria para poder enviar cualquier paquete que le sea enviado a

su siguiente salto en la red. Por varios años el modelo anteriormente descrito fue la base de las redes IP, que además de *Internet*, son usadas para la creación de VPN's. Sin embargo, con la alta taza de crecimiento de las redes de paquetes, el aumento de tráfico en las mismas, la complejidad de las topologías y la diversificación de aplicaciones; los procesadores de los *Routers* se empezaron a ver afectados y a quedarse sin capacidad para enviar paquetes de una manera eficiente y las redes empezaron a tornarse lentas. Esto es fácil de entender al imaginar que el *Router* tiene que examinar el paquete y buscar en su tabla de enrutamiento y una vez encontrado el siguiente salto enviar el paquete. Si a esto añadimos que en una red grande las tablas de enrutamiento tienden a ser grandes y además se suelen configurar requerimientos especiales a los *Routers*, como listas de acceso, marcaje de paquetes, calidad de servicio, etc. Ante lo anterior, los diversos fabricantes aplicaron diversas técnicas que aliviaron el problema, pero aún así, no existía conformidad con la "lentitud" de envío de paquetes en comparación con los modelos de transmisión y de envío de tramas de capa 2. Por esto varios fabricantes empezaron a trabajar en un modelo más eficiente para enviar los paquetes y que se pudiera acoplar a la infraestructura IP existente. El resultado fue el estándar publicado por la IETF para MPLS.

Con la aparición de los microprocesadores ASIC (circuito integrado de aplicación específica) los *Routers* empezaron a enviar paquetes con la misma velocidad con la que un conmutador de capa 2 envía tramas. Debido a esto, la mejora en la velocidad de envío de paquetes, ya no fue el principal beneficio de las redes MPLS. Sin embargo, la arquitectura MPLS trae otros beneficios a las redes IP, de tal manera, que su aplicación se ha extendido tanto que casi todos los Proveedores de Servicios de Interconexión de Redes IP, tanto para servicios de *Internet*, como para servicios de VPN, utilizan núcleos de red con

arquitectura MPLS. Dentro de los beneficios que adquieren los Proveedores de Servicio al Implementar núcleos de red con tecnología MPLS tenemos los siguientes,

- Integración, ya que MPLS puede funcionar con las tecnologías tradicionales de transmisión.

- Escalabilidad de VPN´s, debido a su fácil implementación y fácil crecimiento.

- Reducción de procesamiento en núcleos de red, como hemos hablado anteriormente, el CPU de los *Routers* se ve altamente aliviado por la forma de envío de paquetes.

- Ingeniería de tráfico, debido a que pueden preestablecerse rutas para diversos tráficos y balancear carga.

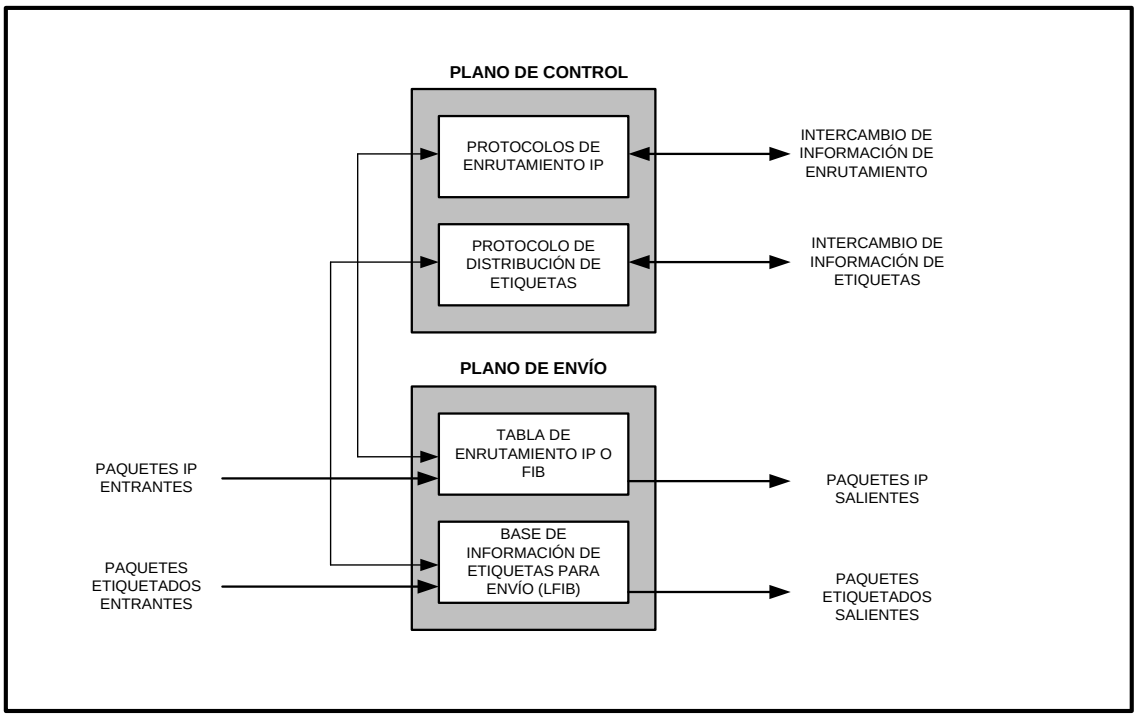
- Calidad de servicio, debido a que puede hacerse una clasificación más eficiente de los distintos tráficos.

2.1 Funcionamiento de MPLS

Ahora bien, en sí, ¿cuál es la gran diferencia que crea la conmutación de etiquetas? La conmutación de etiquetas crea trayectorias predefinidas, por así decirlo, para que los paquetes circulen por la red sin la necesidad de que los *Routers* examinen el paquete a nivel de capa 3. Ahora los *Routers* simplemente envían los paquetes en base a la información de las etiquetas. Para entender mejor, anteriormente los *Routers* tomaban los paquetes, los asignaban a un FEC específico y después asignaban este FEC a un siguiente salto. Esto se hacía cada vez que un paquete arribaba a un *Router* y éstos realizaban estas funciones independientemente. Con el modelo de Etiquetas Conmutadas, la asignación del FEC y la determinación de la ruta se hace sólo una vez y en los *Routers* de borde. La conmutación de etiquetas resume la información y permite conocer todos los destinos posibles y asignar una trayectoria de etiquetas conmutadas permitiendo así el óptimo envío de paquetes.

Para lograr lo anterior, la arquitectura de MPLS se vale de dos planos, el plano de control y el plano de envío. La figura 8 muestra la arquitectura de estos planos.

Figura 8. **Arquitectura de nodo**

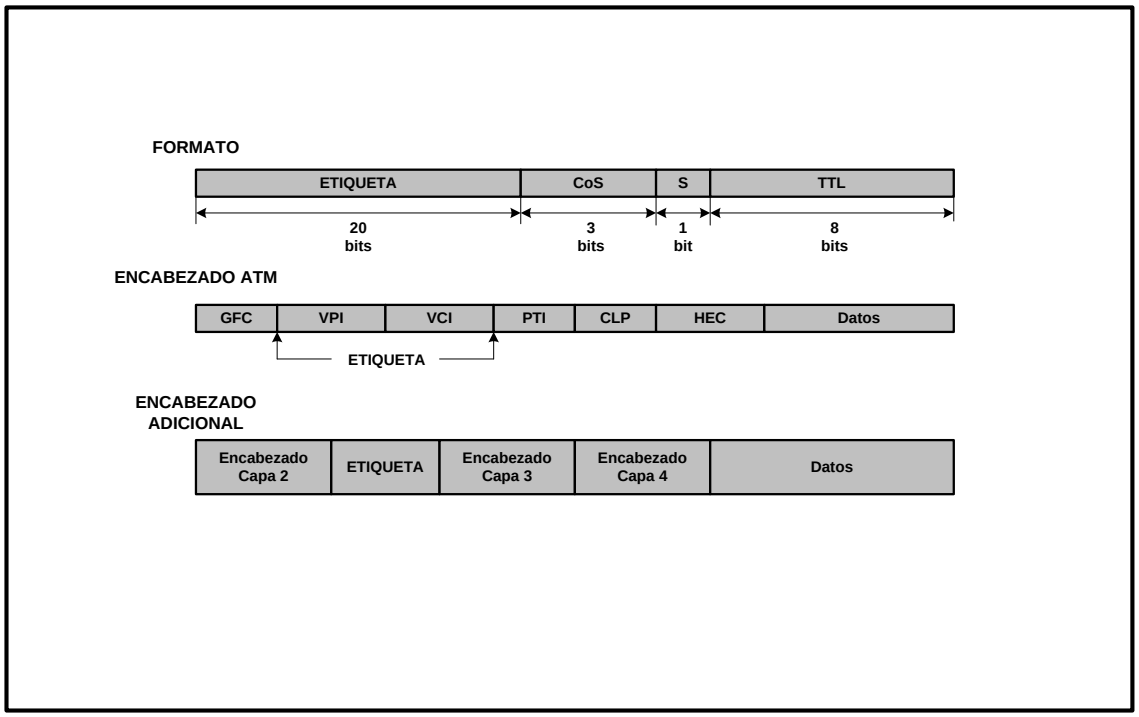


2.1.1 Plano de envío

El Plano de envío de paquetes es el responsable de enviar los paquetes en base a la información que se tenga en las etiquetas. Para realizar dicha tarea se vale de la base de información de envío de etiquetas o LFIB por sus siglas en inglés. Esta base de Información toma los mapeos contenidos en la base de información de etiquetas (LIB, por sus siglas en inglés), que tiene los mapeos de etiquetas tanto locales como los de otros nodos, para asociar los siguientes saltos de los paquetes en la red en base a la etiqueta que se tenga y posteriormente enviar los mismos.

En la figura 9 se muestra la estructura de una Etiqueta de MPLS, tanto para el modelo de paquetes, como para el modelo ATM. La diferencia, como veremos más adelante, se basa propiamente en la diferencia de cómo se maneja el etiquetamiento en ATM. La etiqueta de MPLS identifica el FEC al cual el paquete entrante ha sido asignado.

Figura 9. **Formatos de etiqueta MPLS**



Para el Modelo ATM la asignación de la etiqueta MPLS se hace utilizando el par de datos VPI/VCI. Esto se debe al tamaño fijo que tienen las celdas ATM, a las cuales no se les pueden insertar encabezados como sucede con otras tecnologías de capa 2. El encabezado adicional lleva la información de la etiqueta.

Vamos a ver a continuación la descripción de los campos en una etiqueta MPLS,

- **Campo de etiqueta**: este campo lleva el valor de la etiqueta.

- **Campo CoS**: este campo lleva el valor de Clase de Servicio que se utiliza para marcar los paquetes y priorizar los mismos en las colas de las interfases.

- **Campo de pila**: lleva la información jerárquica de la Etiqueta cuando forma Pilas con otras Etiquetas.

- **Campo TTL**: provee la funcionalidad de tiempo de vida del paquete IP.

La razón de la existencia de la pila de etiquetas es debido a que en algún momento se necesita agregar más de una etiqueta a un paquete. Por ejemplo cuando se configuran VPN´s e Ingeniería de tráfico, se tienen más de una etiqueta, debido a la identificación adicional que se tiene que hacer a la trayectoria de etiquetas conmutadas.

La LFIB consiste en una tabla que contiene principalmente los prefijos o subredes posibles con sus respectivas etiquetas entrantes y por cada una de

estas subredes se tiene una etiqueta que se pondrá a la salida, la interfase del *Router* por donde saldrá y el siguiente salto en la red.

La ventaja esencial del plano de envío es que en lugar de usar múltiples algoritmos para el envío de paquetes, utiliza un solo algoritmo basado en la conmutación de etiquetas, lo que trae como resultado que los dispositivos de red puedan hacer un envío de paquetes de alto desempeño y velocidad.

2.1.2 Plano de control

El plano de control es el encargado de mantener y propagar a través de la red la LFIB. Para lograr esto, existe un protocolo adicional que se encarga de la distribución y el control de la información de la arquitectura del etiquetado. Existen diversos protocolos que realizan dicha función. El más difundido el protocolo de distribución de etiquetas o LDP por sus siglas en inglés. Este protocolo distribuye la información de la arquitectura del etiquetado a través de todos los dispositivos que forman parte de la red MPLS. El plano de control se vale de una segmentación de 5 módulos que se encargan de mantener la arquitectura de etiquetado. Estos módulos son,

- **Módulo de enrutamiento *Unicast***: construye la tabla de FEC usando el protocolo de enrutamiento de la red.

- **Módulo de enrutamiento *Multicast***: construye la tabla de FEC usando el protocolo que utilice la red para el tráfico *Multicast*, por ejemplo PIM.

- **Módulo de ingeniería de tráfico**: permite el manejo de las trayectorias conmutadas de etiquetas con fines de ingeniería de tráfico, es decir, se logran manejos de tráfico de una manera fácil, como por ejemplo, balancear carga en links de diferente ancho de banda, mejorar tiempos de respuesta para recuperación de falla, etc.

- **Módulo de VPN**: este módulo, como su nombre lo indica, es el responsable de la creación de redes privadas sobre la infraestructura MPLS existente.

- **Módulo de calidad de servicio**: permite el marcaje de los distintos FEC para la aplicación modular de calidad de servicio.

2.2 Elementos de una red MPLS

Una red MPLS, como cualquier otra estructura, está formada por elementos que al interactuar entre ellos. Estos tres elementos son:

- Enrutador de etiquetas conmutadas LSR

- Trayectoria de etiquetas conmutadas LSP

- Protocolo de distribución de etiquetas (LDP)

2.2.1 Enrutador de etiquetas conmutadas LSR

El LSR es un equipo que generalmente tiene funciones de *Router* y se configura para que también funcione como LSR. Al activarse la función de LSR el equipo enviará los paquetes, ya no por tabla de enrutamiento IP, sino por conmutación de etiquetas. Las funciones que el LSR realiza a nivel del manejo de etiquetas es la siguiente,

- **Agregación (*Aggregate*)**: remueve la etiqueta y busca en la tabla de enrutamiento en base a información IP.

- **Remoción (*Pop*)**: quita la primera etiqueta de la Pila y transmite el paquete restante, ya sea en base a etiquetas o direcciones IP.

- **Adición (*Push*)**: reemplaza la etiqueta con un arreglo de etiquetas.

- **Conmutación (*Swap*)**: reemplaza una etiqueta por otra.

- **Eliminación (*Untag*)**: quita la etiqueta y envía el paqueta al siguiente salto en la red IP.

Las funciones anteriormente descritas dependen si el LSR está dentro de la red MPLS o en el borde de la misma. Los LSR funcionan de dos maneras distintas, dependiendo si es una red de paquetes o una red ATM.

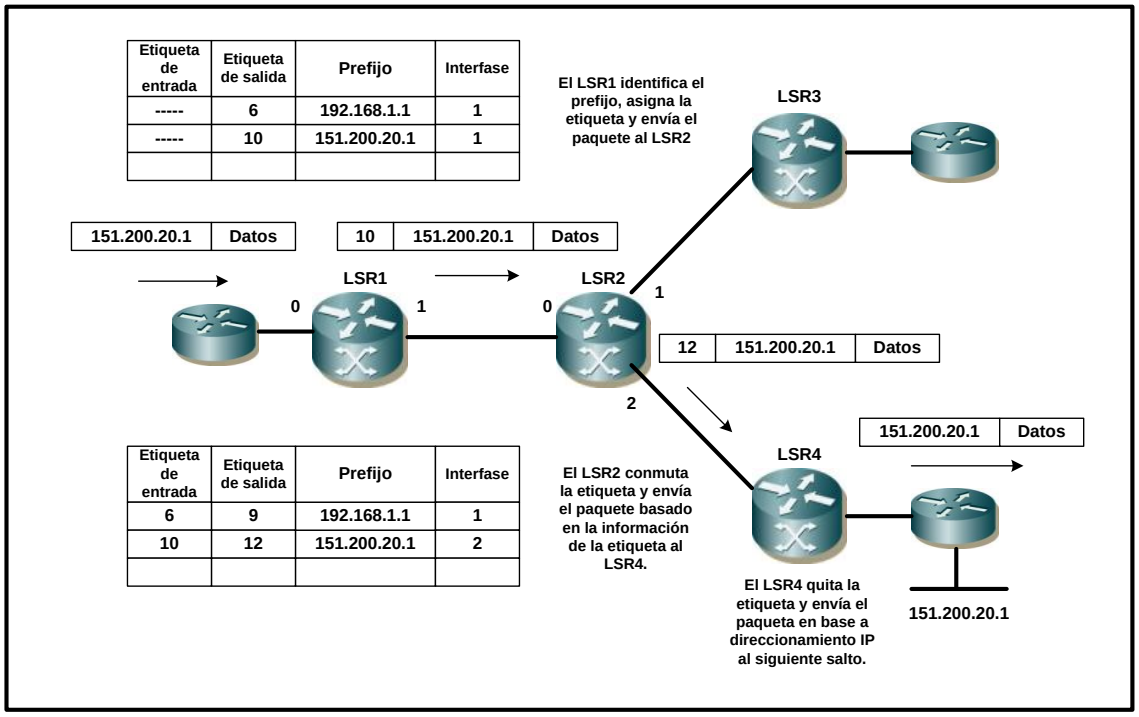
2.2.1.1 Funcionamiento del LSR en una red de paquetes

El funcionamiento básico del LSR se ilustra en la figura 10, en la cual el LSR1 de borde asigna la etiqueta inicial después de aplicar los protocolos convencionales de enrutamiento y escoger el mayor prefijo aplicando el respectivo FEC a dicha subred. Una vez que el LSR2 recibe el paquete, examina la información de la etiqueta, la conmuta por una nueva y envía el paquete al LSR4 basado en la información que traía la etiqueta al ingresar. Al llegar el paquete al LSR4, éste examina la información de la etiqueta, remueve la etiqueta, realiza una búsqueda en la tabla de enrutamiento para determinar cuál será el siguiente salto en la red y una vez lo determina, envía el paquete.

Este proceso se repite para cada paquete que ingresa a la red y que tiene el mismo FEC. Obviamente en una red más grande pueden llegar a ser miles

de prefijos los que formen la LFIB y pueden ser millones los paquetes que cursen a través de la red.

Figura 10. **Funcionamiento del LSR en modo de paquetes**

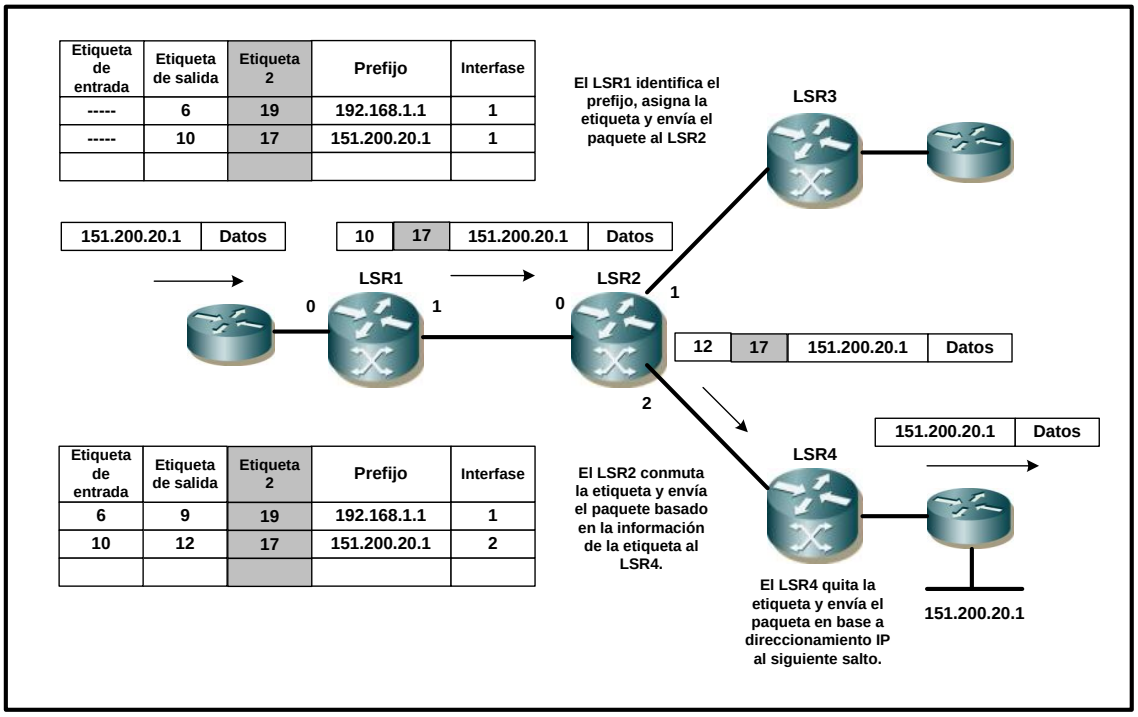


Existen los casos en los cuáles se necesita manejar más de una etiqueta y esto es debido a que en las aplicaciones de VPN's e ingeniería de tráfico se hace necesario aplicar una identificación adicional a la trayectoria de etiquetas conmutadas.

Esta etiqueta adicional, como lo muestra la figura 11, no se conmuta a lo largo de la trayectoria, mantiene su valor cuyo objetivo es identificar esta

trayectoria para que el envío de paquetes de una VPN pueda realizarse, o bien, defina la trayectoria de cierto tipo de tráfico (ingeniería de tráfico).

Figura 11. **Funcionamiento de LSR en modo de paquetes con multietiqueta**



Como el objetivo de una red MPLS es hacer eficiente y rápido el envío de paquetes, se debe optimizar los esquemas anteriormente expuestos. Esto es debido a que los LSR's de frontera deben realizar doble función al eliminar la etiqueta y envía el paquete en base a una búsqueda del siguiente destino en su tabla de enrutamiento. Para solucionar esto, la arquitectura MPLS hace que el LSR anterior al LSR de borde remueva la etiqueta. Esto se logra cuando a través del protocolo LDP (que veremos más adelante) se envía una etiqueta nula implícita, o sea, esta etiqueta tiene un valor de 3 de acuerdo a la tabla de valores reservados de etiquetas.

La figura 12 nos muestra cómo se lleva a cabo la función de remoción de la etiqueta en el penúltimo LSR de la trayectoria.

Figura 12. **Remoción de etiqueta (*pop*)**

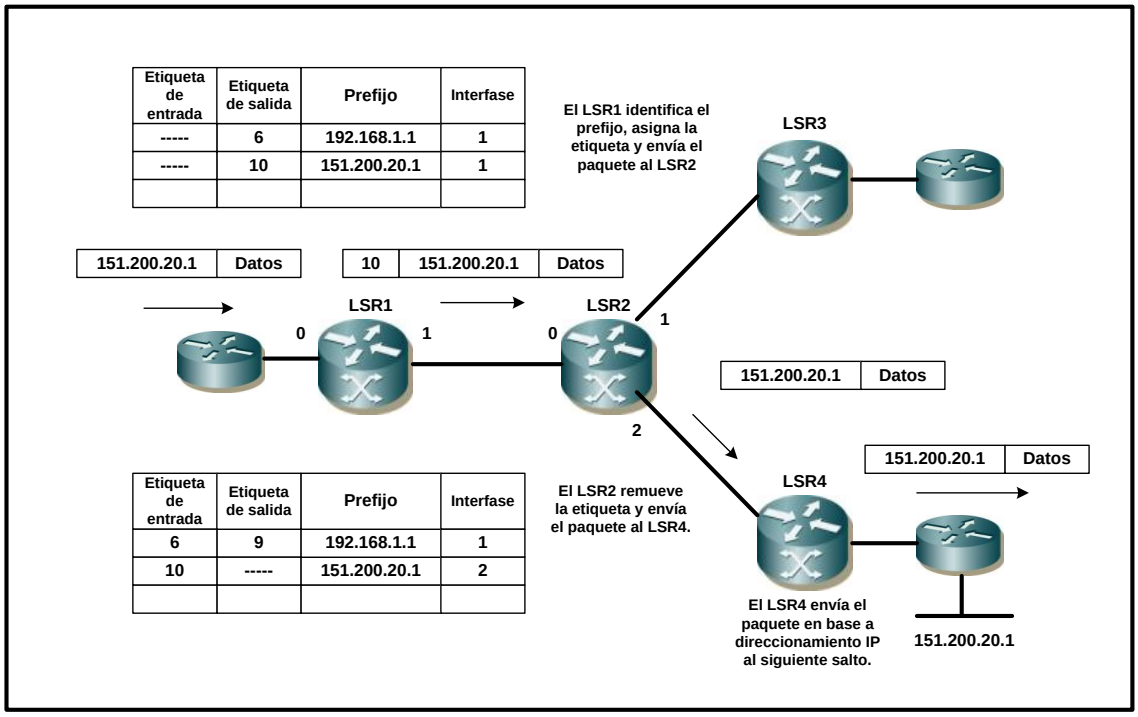


Tabla II. **Valores reservados de etiquetas en MPLS**.

Valor de Etiqueta	Descripción
0	IPv4 etiqueta nula explícita. Indica que la etiqueta debe ser removida y el paquete debe ser enviado en base a la información de Ipv4.
1	Alerta de Etiqueta de *Router*.
2	Ipv6 etiqueta nula explícita. Indica que la etiqueta debe ser removida y el paquete debe ser enviado en base a la información de Ipv6
3	Etiqueta Nula Implícita. Se utiliza para remoción de Etiquetas (Pop).
4 a 15	Reservado para uso futuro.

2.2.1.2 Funcionamiento de un LSR en una red de celdas ATM

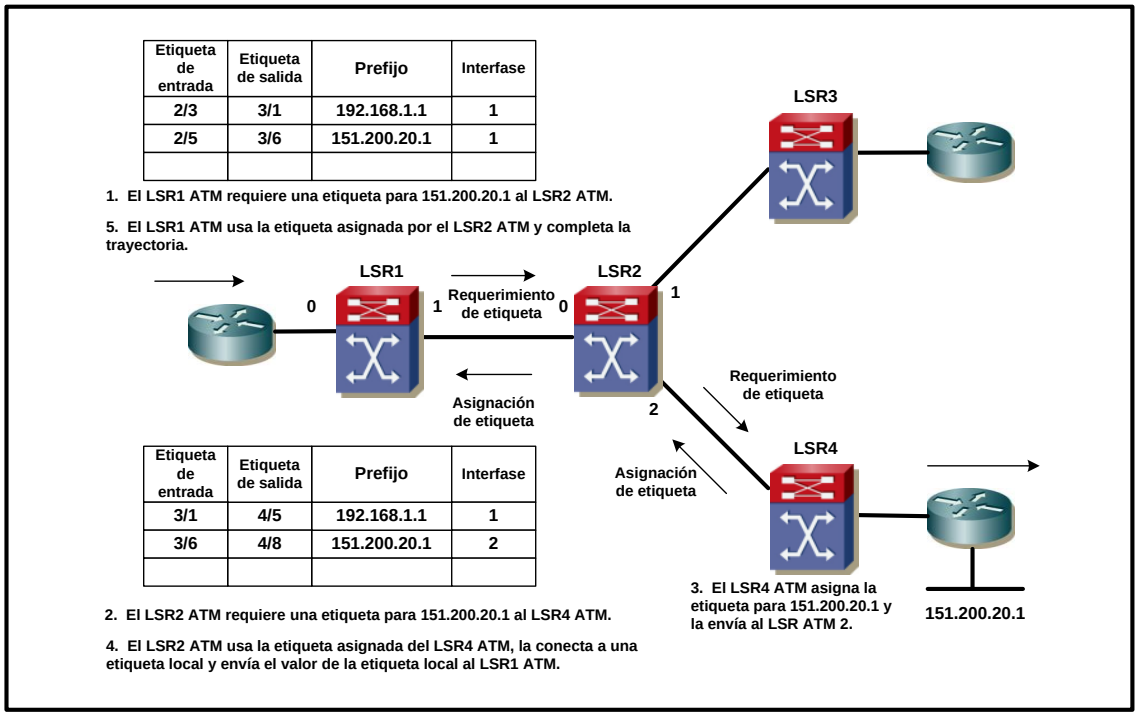
Para el caso de ATM, MPLS funciona de una manera particular. Los conmutadores ATM se convierten en LSR's al añadírseles un componente conocido como control de conmutación de etiquetas o LSC por sus siglas en inglés. Los LSR's de ATM utilizan como etiquetas el par VPI/VCI generado dinámicamente a través de toda la red ATM, emulando las trayectorias de etiquetas conmutadas del modelo de paquetes. De esta forma, la matriz ATM de conmutación se convierte en el análogo de la LFIB.

En los bordes generalmente lo que se tiene es un LSR ATM conectado a un LSR de una red de paquetes, en este punto, el protocolo LDP hace una correspondencia de etiquetas a pares VPI/VCI completando las trayectorias virtuales a través de la red. A diferencia del modelo de paquetes, el modelo de celdas asigna las etiquetas bajo demanda, es decir, una trayectoria de etiquetas en ATM (PVC's) se establece sólo cuando es solicitada por los LSR's. De esta manera, basándonos en la figura 13, el LSR1 requiere una etiqueta al LSR2, el LSR2 se la requiere al LSR4, el LSR4 asigna la etiqueta y se la envía al LSR2, el LSR2 recibe la etiqueta del LSR4 y la conecta a una etiqueta local; después de esto envía el valor de la etiqueta local al LSR1, el LSR1 usa la etiqueta enviada y de esa manera se completa la trayectoria.

El modelo de celdas tiene el inconveniente de que el número de pares VPI/VCI, o sea PVC's, es limitado. Esta limitación se empieza a notar cuando la cantidad de prefijos IP en la red crece y se sobrepasan los límites de PVC´s disponibles en los equipos ATM. Cuando esto sucede, se aplican técnicas de

optimización del uso de los PVC's. De cualquier manera la recomendación en estos casos es migrar las redes con modelo de celdas a modelo de paquetes.

Figura 13. **Funcionamiento del LSR en modo de celdas**



2.2.2 Trayectoria de etiquetas conmutadas LSP

La trayectoria de etiquetas conmutadas, como lo hemos hablado anteriormente, es un camino virtual preestablecido a través de una red MPLS a través de la cual se enviarán los paquetes. Los LSP tienen la característica de ser unidireccionales, es decir, la trayectoria en un sentido no necesariamente es la trayectoria en sentido inverso. Los LSP tienen dos maneras de establecerse que son:

- Control independiente

- Control ordenado

2.2.2.1 Control independiente

En el método de control independiente cada LSR identifica los distintos prefijos como FEC's. Posteriormente a cada FEC se le asigna una etiqueta y una vez formada la tabla de correspondencias, la misma se envía a todos los LSR´s en la red por medio del protocolo LDP. Por último, los LSR´s crean la LFIB usando correspondencias entre los FEC's y sus siguientes saltos en la red. Generalmente los LSR's usan protocolos de enrutamiento como OSPF para la determinación de los siguientes saltos. La figura 14 nos muestra una red de LSR´s y la tabla III nos muestra la LFIB que se forma después de que se propagan todas las etiquetas a través del protocolo LDP.

Como se podrá notar en cada LSR se establece la LFIB que indica el siguiente salto para llegar al prefijo 10.12.20.0/24. La ventaja del Control Independiente es que permite una mejor convergencia ya que establece la LFIB inmediatamente después de que converge el protocolo de enrutamiento.

Figura 14. **Control independiente de establecimiento de LSP**

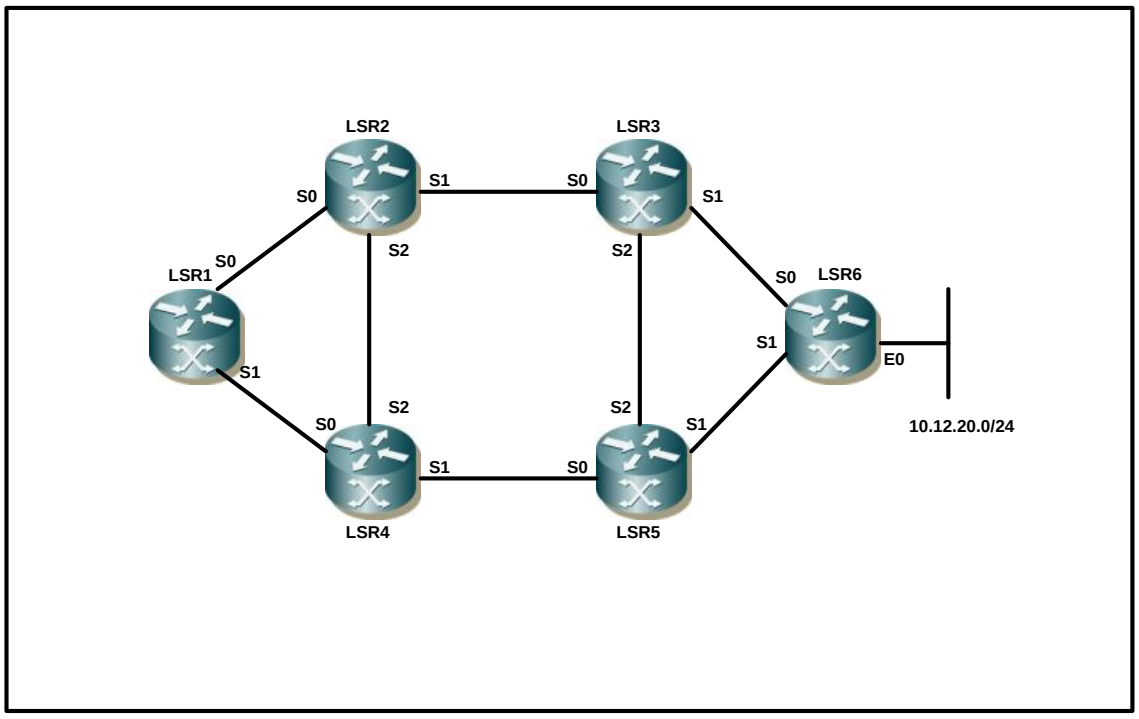


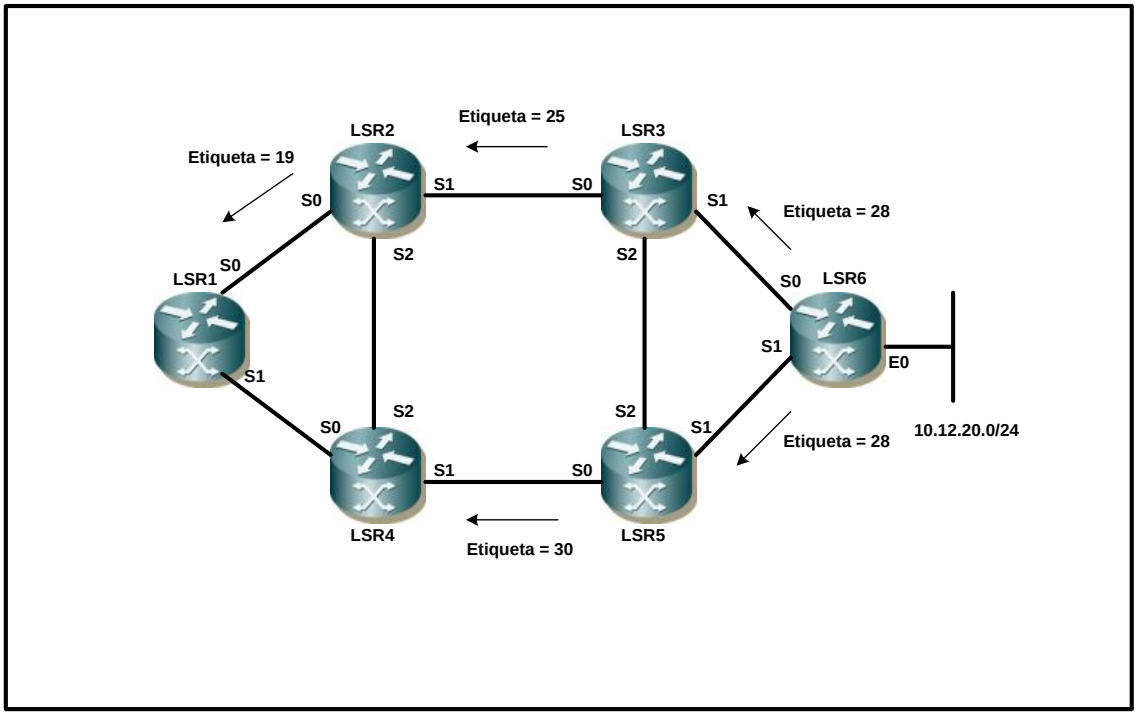
Tabla III. **LFIB después de la distribución de etiquetas**

LSR	Etiqueta Entrante	Etiqueta Saliente	Siguiente Salto	Interfase Saliente
LSR1	22	37	LSR2	S0
LSR2	37	42	LSR3	S1
LSR3	42	51	LSR6	S1
LSR4	72	66	LSR5	S1
LSR5	66	51	LSR6	S1
LSR6	51	----	LSR6	E0

2.2.2.2 Control ordenado

En el control ordenado de establecimiento del LSP, uno de los *Routers* en el borde es el iniciador de los requerimientos de etiquetas. Las etiquetas se asignan de una manera ordenada de extremo a extremo. El LSR iniciador es el que hace la selección de los FEC's y todos los LSR´s de la red usarán los mismos FEC's. El Control Ordenado exige que todas las etiquetas se propaguen antes de que el LSP se establezca. Esto trae como consecuencia que se tenga una convergencia lenta ante cualquier cambio que sufra la red. Sin embargo el control ordenado previene de mejor manera la aparición de bucles en la generación de etiquetas. La figura 15 muestra la manera en que generan las Etiquetas de un extremo a otro de la red.

Figura 15. **Control ordenado de establecimiento de LSP**



2.2.3 Protocolo de distribución de etiquetas LDP

El protocolo LDP provee una estructura robusta para la distribución de las Etiquetas a través de todos los LSR's en la Red MPLS. Utiliza el puerto TCP 646 para la distribución de las etiquetas a los LSR's vecinos. Algo importante de hacer notar es que LDP se vale de los protocolos de enrutamiento configurados a nivel de Capa 3, para lograr la distribución de las Etiquetas.

Existen 4 formas en las cuales LDP asigna y distribuye las etiquetas. A continuación se detalla cada una,

- **Modo LDP por demanda**: consiste en la asignación de etiquetas a través de requerimientos específicos para los FEC's.

- **Modo LDP por asignación no solicitada**: a diferencia del anterior, en este modo las Etiquetas se asignan y distribuyen a los LSR's vecinos, aún cuando estos no lo han solicitado.

- **Modo de retención de etiqueta liberal**: en este caso, se tiene la flexibilidad de poder mantener o borrar Etiquetas recibidas de un LSR vecino aunque este no sea el siguiente salto para alcanzar un prefijo.

- **Modo de retención de etiqueta conservador**: en este caso, las Etiquetas recibidas de un LSR vecino que no sea el siguiente salto para alcanzar un prefijo son descartadas. De esta forma sólo quedan las Etiquetas que identifican a los FEC para el envío directo de paquetes.

2.3 Tópicos avanzados de MPLS

Existen algunas consideraciones que deben ser tomadas en cuenta al momento de la configuración de una red MPLS. Estos tópicos nos permiten hacer un mejor diseño de la red y a la vez nos proporcionan alternativas para solucionar problemas potenciales. Estudiaremos los siguientes:

- Control de distribución de etiquetas.

- Encapsulación de MPLS a través de enlaces *Ethernet*.

- Detección y prevención de bucles en MPLS

- Resumen de rutas dentro de una red MPLS.

2.3.1 Control de distribución de etiquetas

Cuando se utiliza el Control Independiente para la asignación de las Etiquetas, dentro de la configuración normal de MPLS no es posible evitar que se asignen etiquetas a FEC's que probablemente no se deseen. Como sabemos el Control Independiente asigna Etiquetas a todos los posibles FEC's que se tienen en la red MPLS, sin que exista un requerimiento específico de asignación. Suele suceder que en algunos escenarios de migración se desee evitar que algunos FEC's sean asignados con etiquetas. Para casos especiales como este deben aplicarse configuraciones especiales que permitan el filtrado de Etiquetas. El comando *tag-switching advertise-tags* en conjunto con listas de acceso permite controlar la distribución de etiquetas. A continuación se muestra cómo filtrar Etiquetas para el prefijo 192.168.1.0/24 hacia el LSR vecino con la dirección IP 10.10.10.1,

```
!
tag-switching advertise-tags for 1 to 2
!
access-list 1 permit 192.168.1.0 0.0.0.255
access-list 1 deny any
access-list 2 permit 10.10.10.1
¡
```

2.3.2 Encapsulación de MPLS a través de enlaces *Ethernet*

Como es sabido, cuando se configura MPLS en una red de *Routers*, la generación de etiquetas traerá como resultado el incremento en el tamaño de los paquetes. El incremento generalmente supera los 1500 *bytes*, y esto

genera un problema cuando a través de la red cursan paquetes cuyo *bit* pata fragmentación no está activo. Dichos paquetes no pasan a través del enlace *Ethernet*. Para solucionar este problema se utiliza un comando que permite la fragmentación previa del paquete antes que ingrese a la red MPLS. El comando es ***tag-switching mtu***. Este comando debe ser aplicado en todas las interfases que manejen la funcionalidad de MPLS.

2.3.3 Detección y prevención de bucles en MPLS

Con el fin de mantener la estabilidad en la red de MPLS deben existir mecanismos que prevengan el hecho que un paquete se quede circulando por tiempo indefinido en la red. Para esto la arquitectura posee características que previenen dichas situaciones en particular. Existen dos tipos de detección y prevención de bucles, para modo de paquetes y para modo de celdas.

- **Detección y prevención en modo de paquetes**: existen dos formas. La primera utiliza el campo TTL del paquete IP en el plano de envío y de esa manera se descartan los paquetes después de cierto tiempo. La segunda que básicamente es para el plano de control, delega la función de detección y prevención a los protocolos de enrutamiento de capa 3.

- **Detección y prevención en modo de celdas**: para el caso del plano de envío se utiliza el parámetro TLV, que tiene una función similar al TTL sólo que en este caso en lugar de ser un decremento

del valor el equipo incrementa el valor de este campo con cada salto hasta que el mismo llega a su valor máximo y el paquete es descartado. Para el caso del Plano de Control se hace una relación entre el valor del TLV y el TTL. Como resultado se tiene que el valor de saltos es trasladado al campo TTL del paquete IP después de restarle un salto para compensar el paso por la red ATM. De esta manera se tiene un control confiable para los posibles bucles que se presenten.

2.3.4 Resumen de rutas en una red MPLS

El resumen de rutas en una red MPLS debe estudiarse a detalle ya que si se aplica de mala manera puede afectar la operación de la arquitectura MPLS. Para evitar problemas cuando se implemente una red MPLS debe evitarse resumir las rutas de las direcciones que identifican los procesos de LDP (generalmente son direcciones *Loopback*). Esto se debe a que cuando se hace un resumen de rutas el *Router* es obligado a hacer una búsqueda en su tabla de enrutamiento para enviar el paquete y al mismo tiempo genera una etiqueta nula implícita, creando una inconsistencia en la arquitectura de MPLS y rompiendo la trayectoria de etiquetas conmutadas. Esto afectará los servicios que provee la red MPLS.

3. REDES PRIVADAS VIRTUALES BASADAS EN MPLS, MODO DE PAQUETES

Finalmente iniciaremos el análisis de las VPN's sobre MPLS. Como punto de partida podemos decir que una red privada virtual (VPN) es un conjunto de sitios u oficinas remotas que comparten una arquitectura de comunicación en Capa 3, auxiliándose de la red de *Routers* y sus tablas de enrutamiento. Entonces las VPN's sobre MPLS, combinan los beneficios de la velocidad de envío de paquetes que se tiene con la conmutación de etiquetas y la versatilidad, escalabilidad y flexibilidad del Enrutamiento a nivel de Capa 3. Las VPN's basadas en MPLS no son orientadas a la conexión, por lo facilitan su aprovisionamiento o configuración. Adicionalmente, esta arquitectura ofrece una comunicación segura aislando el intercambio de información de la VPN de determinado cliente, del resto de VPN's de Clientes que utilizan el mismo entorno de capa 3.

La VPN de MPLS es un proceso de enrutamiento virtual separado de la tabla de enrutamiento global. Este singular proceso se le conoce como enrutamiento virtual y de envío, VRF por sus siglas en inglés. Una VRF se construye sobre la infraestructura existente, es decir, para el caso de una Red de Paquetes formada por *Routers*, la VRF consistirá en una configuración especial de estos *Routers*, que se asume, ya forman una red MPLS.

3.1 Elementos para construir una VPN basada en MPLS

Existen elementos en una Red MPLS que son necesarios para la construcción de la VPN. A continuación se describen los mismos,

- ***Routers* de núcleo de red del proveedor P**: se caracterizan por no tener conexiones hacia *Routers* de Clientes, se interconectan usando topologías para alta disponibilidad y no tiene configuración ni conocen las VPN's que pasan a través de ellos.

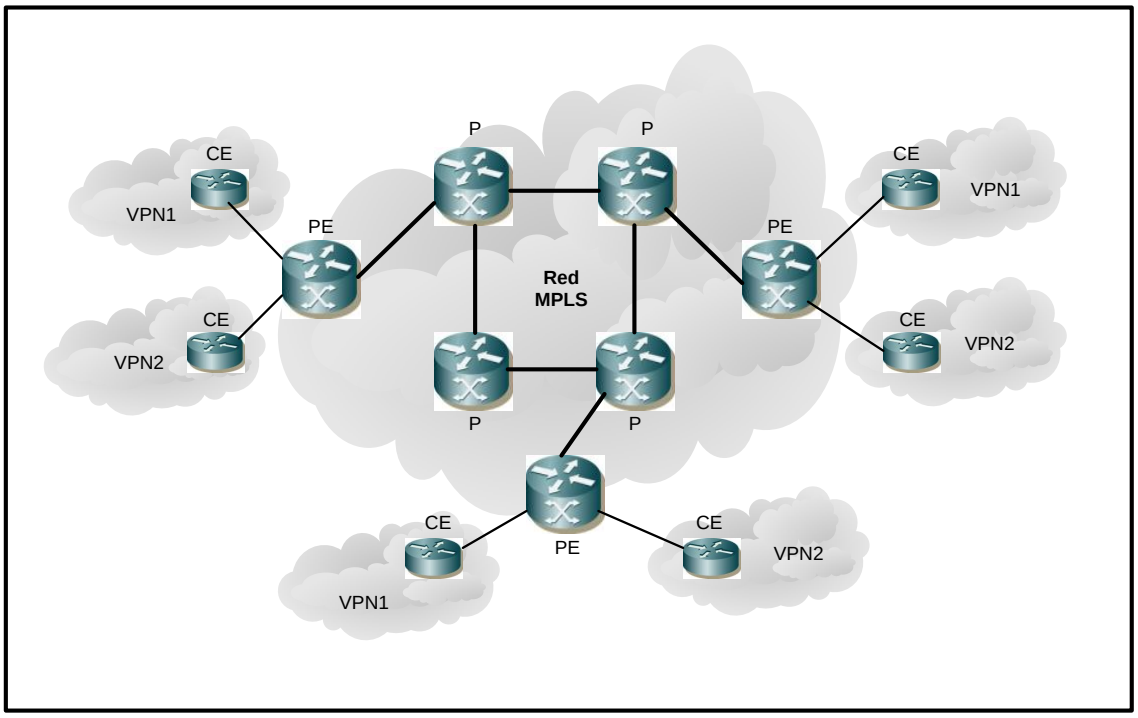
- ***Routers* de borde de red del proveedor PE**: se caracterizan por ser los que tienen las conexiones hacia los Clientes, en ellos se configuran las VPN's. Adicionalmente se conectan a otros PE, o bien, a los *Routers* P.

- ***Routers* de borde de cliente CE**: son los *Routers* del Cliente que se conectan con los PE del proveedor. Como se verá adelante, no necesitan soportar MPLS y sólo necesitan las funciones tradicionales de Capa 3.

- ***Routers* de Cliente C**: son los *Routers* que forman parte de la red iInterna del cliente y nunca se conectan a los *Routers* PE. No necesitan soportar MPLS y sólo necesitan las funciones tradicionales de Capa 3.

En la figura 16 se muestra una Red MPLS de ejemplo, identificando los elementos anteriormente mencionados. Se omite el *Router* de Cliente C, debido a que por ser equipo interno del cliente, no tiene una participación activa en la red MPLS y en la VPN.

Figura 16. **Elementos de una VPN basada en MPLS**



3.2 Estructura lógica de una VRF

Para la creación de la VRF se necesita una estructura lógica a configurar en los *Routers*. Es obvio que en el cuadro anterior queda la incógnita de cómo los PE y los P pueden manejar dos VPN's distintas con seguridad y sin que se puedan ver entre ellas. Analicemos un poco la estructura lógica que se configurará para lograr este fin.

3.2.1 Multiprotocolo IBGP

Anteriormente mencionamos que sólo los *Routers* PE conocerían la información de las VRF´s que se configurarían. Adicionalmente, también se mencionó que estas VRF´s no se podrían ver entre ellas a Nivel 3. Para lograr hacer todo lo anterior se tendría que implementar una estructura muy compleja que, al final del día, resultaría impráctica y engorrosa. La idea para lograr todas las características anteriores es la implementación de un nuevo Protocolo denominado multiprotocolo IBGP. El estándar que lo define es el RFC 2283, que define una extensión del Protocolo BGP que permite el manejo de comunidades extendidas y otras familias de protocolos distintos al ya bien conocido IPv4. Debido a lo anterior, se le denomina a esta extensión de BGP "multiprotocolo". El M-IBGP será el responsable de distribuir la información de enrutamiento para las VRF´s entre los distintos PE.

Se escogió el M-IBGP, ya que es un protocolo muy escalable y robusto para el intercambio de la información de las VRF's. Adicionalmente, debido al

manejo de las comunidades extendidas, soporta los RD's y RT's que veremos más adelante y que son clave para la creación de las VRF's. Por último, la característica que le permite manejar sesiones con *Routers* que no son adyacentes, termina de completar las características por las cuáles se eligió este protocolo para formar la base de intercambio de información para las VRF's. Se necesita que el M-IBGP tenga una estructura de malla en sus conexiones Lógicas hacia sus otros vecinos PE. Esto en una Red que es muy grande, resulta impráctico de configurar. Por lo tanto aparece el término *Router Reflector*. La aparición de este equipo simplifica enormemente la configuración de M-IBGP, ya que sólo se necesita que todos los PE's tengan una sesión de BGP hacia el RR. El RR recibirá la información de uno o varios PE y la distribuirá a los PE's restantes.

3.2.2 Identificadores de ruta RD

Como su nombre lo especifica, se utilizan para identificar las rutas creadas en un CE y enviadas al PE respectivo. Esto permitirá hacer que los prefijos generados por las interfases que estén dentro de la VRF, sean únicos para el resto de la red.

El identificador consiste en 64 *bits* adicionales que se le agregan al paquete de IPv4. El resultado es una dirección de 96 *bits* que se le conoce como dirección VPNv4. Los RD's, permiten que dentro de las VRF's, puedan reutilizarse las direcciones IP que ya se han usado en otros clientes.

3.2.3 Ruta objetivo RT

El RT es un atributo adicional que se agrega a las rutas VPNv4 para indicar la pertenencia de la VPN. Este atributo o comunidad se hace necesario al momento en el que el RD no puede identificar su participación en más de una VPN. La flexibilidad que añade este atributo, permite la configuración de escenarios complejos para VPN's basadas en MPLS.

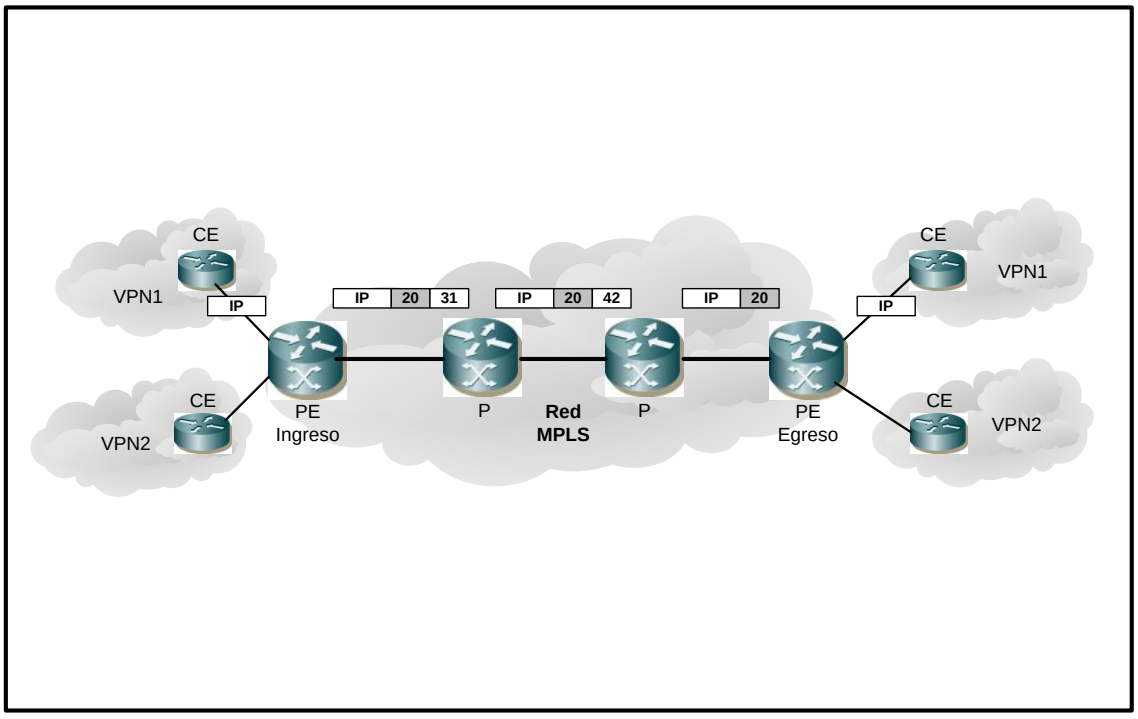
Con este último atributo ya podemos justificar las distintas operaciones que realiza un PE y que permiten la creación de las VRF's. En el siguiente apartado, veremos el ejemplo ilustrativo, de cómo funciona una VRF.

3.3 Funcionamiento de envío de paquetes a través de una VRF

En la figura 17 podemos ver un ejemplo ilustrativo de lo que pasa en los distintos componentes de una Red MPLS para que se lleve a cabo el envío de paquetes a través de la VRF. Inicialmente sabemos que ya existe una trayectoria de etiquetas conmutadas asociada a un FEC que se usará para el envío de paquetes de la VRF en cuestión. Al momento de entrar el paquete proveniente del CE, el PE correspondiente utiliza la característica de pila de etiquetas, para asignar una etiqueta que identificará la VRF y sobre ésta la red manejara la conmutación de etiquetas que llevará el paquete al PE destino. Cómo vemos en la figura 12, el último *Router* P en la trayectoria remueve la etiqueta superior de la pila, dejando ya solamente la etiqueta que identifica la VRF y envía el paquete al *Router* de egreso PE.

Al llegar el paquete al PE, éste sólo hace la revisión de la etiqueta restante, la cual le indica la interfase a la cual debe enviar el paquete. El PE procede entonces a remover la etiqueta y a enviar el paquete por la interfase que lo conecta al CE correspondiente.

Figura 17. **Funcionamiento de envío de paquete en una VRF**

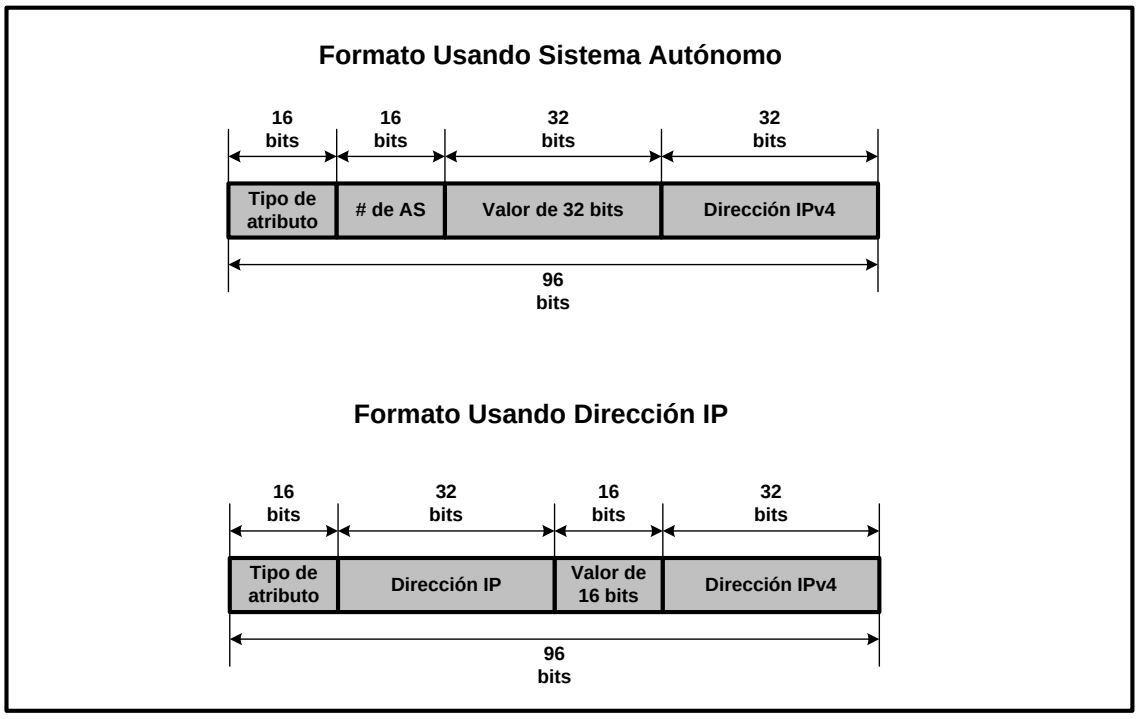


Al momento de ingresar el paquete en el PE de Ingreso, éste comunica la información de la etiqueta asignada al PE de egreso a través de M-IBGP. De esta manera es como todos los elementos, tanto lógicos como físicos, interactúan para que la VRF funcione y por ende la VPN asignada al cliente.

3.4 Formato para comunidad extendida de BGP

En la figura 18 se muestra el formato que se utiliza para la comunidad extendida de BGP. Existen 2 formas en las que se puede presentar dicho formato. La primera consiste en utilizar en los campos en donde se coloca el nombre del atributo, una asociación entre el AS o Sistema Autónomo (de 16 *bits*) de la red más un valor de 32 *bits* que lo asignará el administrador de la Red. La segunda consiste en una asociación de la dirección IP del *Router* PE (generalmente es la dirección *Loopback*) de 32 *bits* más un valor de 16 *bits* que lo asignará el administrador de la red.

Figura 18. **Formatos de comunidad extendida de BGP**



3.5 Enrutamiento dentro de una VRF

Una vez creada la VRF, es necesario hacer el enrutamiento para los equipos del cliente. Existen 4 maneras principales para configurar enrutamiento dentro de la VRF que son:

- Usando rutas estáticas.
- Usando protocolo RIP.
- Usando protocolo BGP.
- Usando protocolo OSPF.

Los ejemplos de configuración de los protocolos mencionados se verán a detalle en el capítulo 6. Al configurar estos protocolos debe tomarse en cuenta las siguientes limitantes,

- Cuando se usa RIP o BGP sólo se puede configurar un proceso por *Router*.

- Cuando se configura OSPF, se debe configurar un proceso diferente por VRF.

- En resumen, el número de Procesos de enrutamiento está limitado a 32 por *Router*.

4. REDES PRIVADAS VIRTUALES BASADAS EN MPLS, MODO DE CELDAS

Existen muchas implementaciones de Redes ATM alrededor del mundo. En algunos casos, el tamaño de estas redes llega a ser considerablemente grande. Adicionalmente, como hemos visto en el capítulo 1, las redes ATM suelen se muy complejas debido al nivel de inteligencia que manejan y por lo tanto el equipo en sí, suele ser muy costoso sin importar el fabricante. Al día de hoy, la estrategia de la mayoría de Proveedores de Servicio es ya no crecer sus redes ATM y sustituir las por redes IP/MPLS. La estrategia que se tome depende de los costos que represente para el proveedor. Por ejemplo, las Redes IP/MPLS *MetroEthernet* representan un menor costo en implementación, operación y mantenimiento; considerando esto, los proveedores hacer inversiones para la sustitución de los equipos ATM en tiempos relativamente cortos y esperando un retorno de la inversión a largo plazo. Otros proveedores por ejemplo, ven que sus costos de migración son sumamente altos si deciden hacer la migración en un período relativamente corto; incluso, los costos siguen siendo altos si se considera una migración a mediano plazo. Por lo tanto existe un gran número de proveedores que prefiere hacer sus ampliaciones de Red usando Redes de Paquetes IP/MPLS, y en los segmentos de red donde aplique, hacer la integración con las redes ATM existentes implementando MPLS sobre ATM.

La implementación de MPLS sobre redes ATM puede realizarse de dos formas,

- Modo ATM nativo

- Modo de paquetes sobre ATM

4.1 Modo ATM nativo

El modo ATM nativo aprovecha la similitud de los LSP's del modo de paquetes con los PVC's para hacer correspondencia de los mismos en los bordes. De esta forma, un LSP al llegar al LSR que se conecta a la red ATM, se conecta a un PVC asignado dinámicamente que lo transporta hacia el LSR correspondiente en el otro extremo de la red ATM.

4.1.1 Elementos del modo ATM nativo

Los elementos necesarios para construir la red MPLS-ATM en modo Nativo se describen a continuación,

- **Enrutador de etiquetas conmutadas LSR**: tiene las características que ya describimos en el capítulo 2, con la diferencia que está en el borde de la red de Paquetes IP y utiliza interfases ATM (obviamente para conectarse al borde de la red ATM).

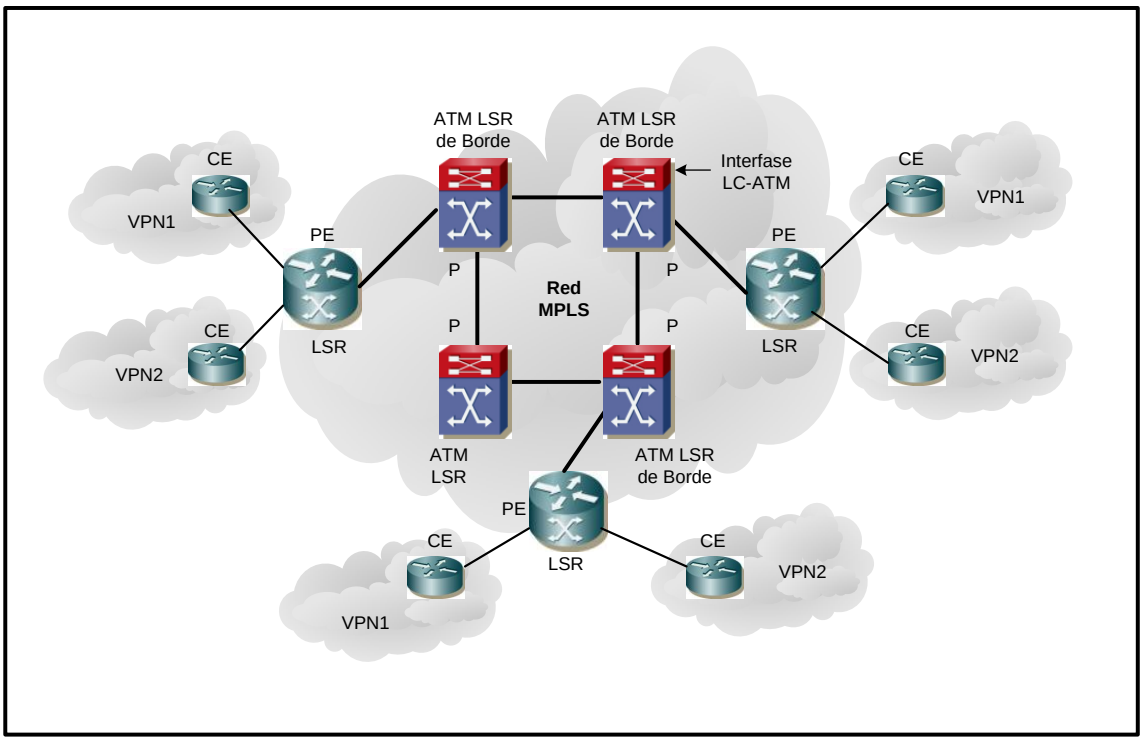
- **Interfase para control de etiquetas ATM o Interfase LC-ATM**: como su nombre lo indica, controla la asignación de las Etiquetas, que en este caso son PVC's dinámicos. Este control puede ser interno en el Conmutador ATM, o bien, un *Router* externo puede proveer dicha funcionalidad.

- **Enrutador de etiquetas conmutadas ATM o ATM LSR**: es el conmutador ATM que asigna de manera dinámica las Etiquetas o PVC's para el envío de paquetes.

- **Enrutador de etiquetas conmutadas ATM de borde o ATM LSR de borde)**: es el mismo dispositivo que el anterior con la diferencia que está en el borde de la red ATM y tendrá las funciones de etiquetar o eliminar etiquetas.

En la figura 19 se muestra la estructura básica del modo ATM nativo y los elementos que lo conforman. Se podrá notar también que la figura muestra una implementación en donde el ATM LSR y la interfase LC-ATM, se encuentran en un mismo equipo.

Figura 19. **Elementos de una VPN basada en MPLS modo ATM nativo**



4.1.2 Intercalado de celdas

El intercalado de celdas le permite a los conmutadores ATM crear 2 trayectorias en puntos de convergencia evitando el descarte de celdas. Por ejemplo, en la operación normal de MPLS en modo de celdas, la asignación de etiquetas se hace bajo demanda; puede ser entonces que en determinado momento un conmutador asigne un solo PVC para dos requerimientos sobre enlaces separados sobre un tercer enlace de salida. Esto causaría, obviamente, el descarte de las celdas. En lugar de eso, el conmutador asigna una etiqueta para cada requerimiento e intercala las celdas en el tercer enlace hacia el LSR destino. Esto a la larga es una desventaja en redes que llegan a tener muchos prefijos, ya que como sabemos, a cada prefijo es asignado una

etiqueta o PVC; en determinado momento los ATM LSR pueden quedarse sin PVC´s y esto traería como consecuencia la no comunicación de las VPN's que estén solicitando los PVC's.

4.1.3 Fusión de VC

La técnica de fusión de VC permite enviar celdas provenientes de 2 PVC's distintos sobre un mismo PVC. Como podemos ver, es el mismo caso analizado anteriormente, solo que en este caso, sólo se asigna un PVC en lugar de dos. La fusión de VC tiene la función de evitar el descarte de Celdas por medio de un encolamiento. Por ejemplo, si se están transmitiendo dos tramas de datos sobre las Celdas ATM simultáneamente, las mismas se colocan en dos colas en la interfase de convergencia del LSR. Una de estas colas se define como primaria y empezará a despachar las celdas hasta que detecte la secuencia de fin de trama, la cual una vez recibida será el indicador para trasladar las celdas de la cola secundaria a la primaria e iniciar a despachar las mismas. De esta manera se hace un ahorro de etiquetas o PVC's aumentando la disponibilidad de los mismos para requerimientos futuros. La desventaja que puede presentar es un aumento en el retardo de envío de paquetes en la red, el cual puede afectar o no la misma, dependiendo del tipo de tráfico que se maneje.

4.1.4 Circuitos virtuales etiquetados (LVC)

Estos circuitos son similares a los SVC's o circuitos virtuales conmutados descritos en el Foro ATM, ya que hasta cierto punto son asignados dinámicamente y no de manera permanente como los PVC's. Sin embargo son muy distintos desde el punto de vista de la manera en que se generan. Los LVC's utilizan señalización LDP para ser creados. Existen dos tipos de LVC's, los LVC's de Señalización y los LVC's Ordinarios.

- **LVC's de señalización**: como su nombre lo indica se utilizan para señalización entre los Controladores de Etiqueta Conmutada (que veremos más adelante). Suelen llevar información de protocolos de enrutamiento como MP-BGP y OSPF; también transportan el protocolo LDP. Está preestablecido que el par VPI/VCI de este LVC sea el 0/32.

- **LVC's ordinarios**: estos LVC's llevan los datos sobre la trayectoria de etiqueta conmutada sin ser reensamblados y generalmente van sobre el mismo VP o grupo de VP's.

En la figura 20 se ilustra la forma en que se interconectan estos tipos de LVC's a lo largo de una trayectoria.

4.1.5 Controladores de etiqueta conmutada (LSC)

Estos dispositivos manejan tanto la parte de control como la de envío de un LSR ATM. El LSC mantiene un conocimiento de la topología de la red MPLS y de esa manera mantiene actualizadas las trayectorias de etiquetas conmutadas emulando, hasta cierto punto, lo que se desarrolla en una Red de Paquetes. La implementación de el LSC puede ser Interna o Externa.

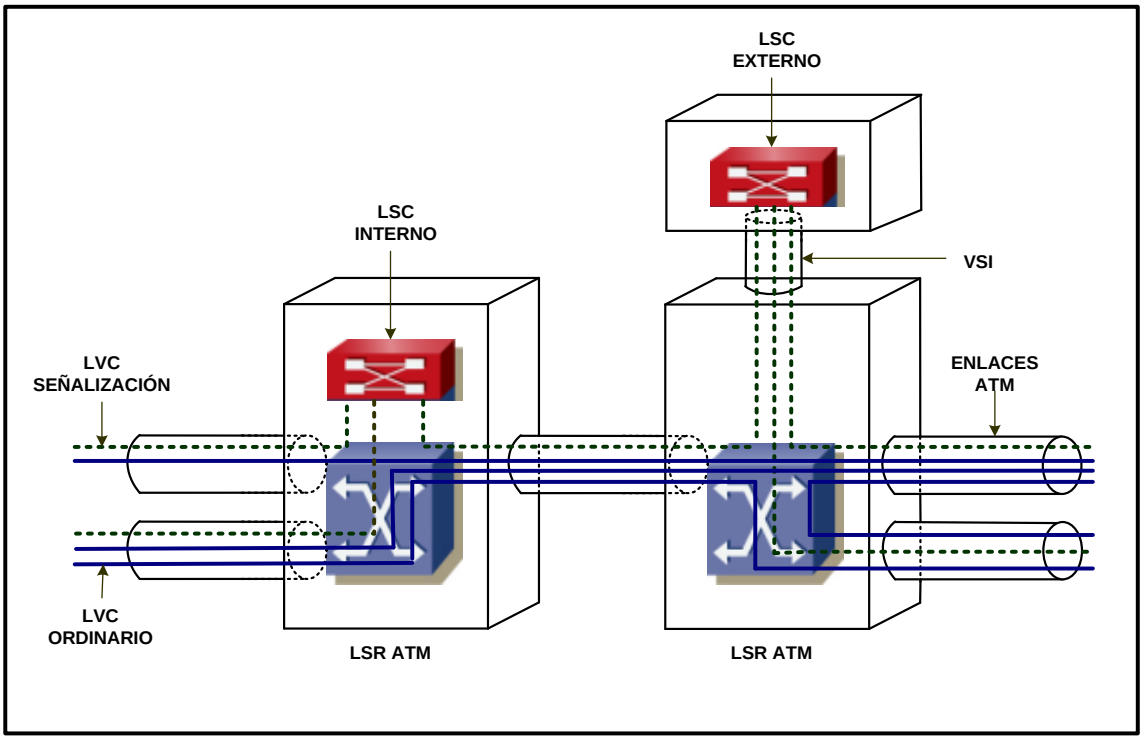
- **Implementación de LSC interna**: como su nombre lo indica, esta función es generada en el mismo Conmutador ATM, generalmente, por una tarjeta electrónica que tiene habilitada dicha funcionalidad.

- **Implementación de LSC externa:** en este caso el Conmutador ATM no puede tener esta funcionalidad interna, generalmente originada por ser un equipo muy antiguo. Para solucionar este inconveniente se realiza una implementación utilizando un *Router* que se conecta al conmutador ATM por medio de interfases ATM. Estas interfases ATM están en el orden de un DS3 hasta un OC3 o STM-1 y se conocen como interfase virtual de conmutación.

En los años recientes se han desarrollado equipos que integran la funcionalidad de enrutamiento con la función de LSR ATM, teniendo como resultado un equipo versátil para las implementaciones de MPLS en modo ATM nativo.

En la figura 20 se muestran las implementaciones que se pueden tener de un LSC.

Figura 20. **Implementaciones de LSC**

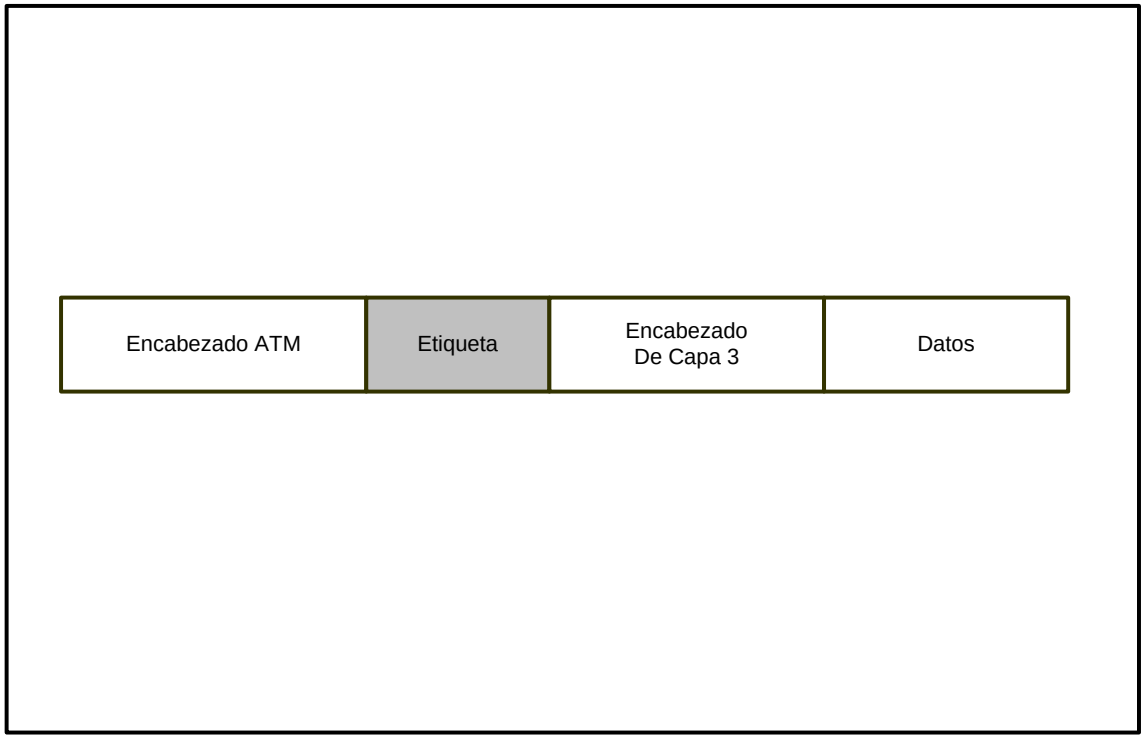


4.2 Modo de paquetes sobre ATM

Existen algunos casos en los que por la disposición de la Red ATM, resulte más sencillo implementar el modo de paquetes. Por ejemplo, en una red en la que los conmutadores ATM están dispersos y ubicados más en la parte de acceso, requeriría la implementación de *Routers* LSR en los bordes para poder configurar el modo ATM nativo; esto resultaría demasiado costoso e innecesario. Otro ejemplo que se puede citar es cuando los segmentos de red

ATM son muy pequeños dentro de una red de paquetes; nuevamente resultaría muy costoso e innecesario configurar el modo ATM nativo. Para los casos vistos anteriormente, resulta más sencillo levantar PVC's permanentes que formen puentes sobre los segmentos de red ATM y de esa manera no se interrumpan los LSP´s. La figura 21 muestra cómo se le agrega el encabezado con la etiqueta a la trama ATM. Prácticamente lo que se obtiene es un empaquetado del modo de paquetes sobre ATM.

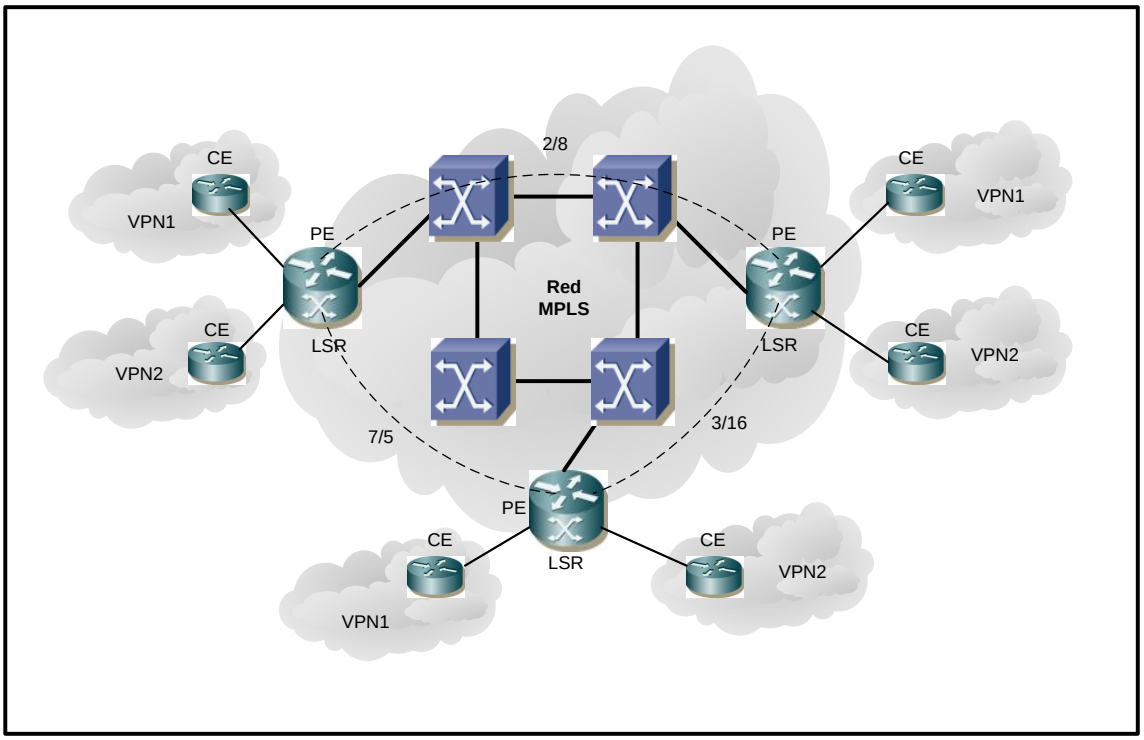
Figura 21. **Celda ATM empaquetando el modo de paquetes sobre ATM**



Para estas implementaciones se obvia totalmente los beneficios de una red ATM, es decir, se utilizan pocos PVC's, la única categoría de servicio aplicada es la de CBR ya que los PVC's se configuran emulando canales dedicados como sucede en TDM y SDH.

La desventaja de esta implementación es que se le agrega demasiado encabezado al paquete IP y no se aproveche de manera eficiente la disponibilidad de ancho de banda total en un enlace como sucede con TDM y SDH. La figura 22 muestra como se implementan las VPN´s en este modelo.

Figura 22. **VPN's sobre modo de paquetes sobre ATM**



Como se puede observar, los conmutadores ATM sólo se utilizan como transporte de capa 2. Generalmente, se configuran los PVC's necesarios para tener una malla y así distribuir el tráfico de manera eficiente.

Para concluir este capítulo podemos resumir que cada una de las implementaciones de VPN's de MPLS tiene un escenario específico en donde

se aplican mejor las cualidades de cada una. De cualquier manera, la visión a futuro debe ser sustituir la red ATM por un modelo de red de paquetes.

5. COMPARACIÓN ENTRE VPN'S TRADICIONALES Y VPN'S SOBRE MPLS

A este punto hemos visto cómo se implementan las VPN's, tanto en las tecnologías tradicionales, como con la tecnología MPLS. Vale la pena entonces que nos detengamos a hacer un resumen de las características principales de cada tecnología y establecer las ventajas que tienen las VPN's sobre MPLS.

5.1 Características de las VPN's tradicionales

Para hacer un mejor resumen de las características vamos a hacer el análisis en base a los tipos y topologías.

5.1.1 Tipos de VPN's

La división principal que se hace de las VPN's Tradicionales es basada en la manera en que se construye la interacción del usuario y proveedor. De esta división tenemos dos estructuras principales que son las VPN's sobre capas y las VPN's extremo a extremo.

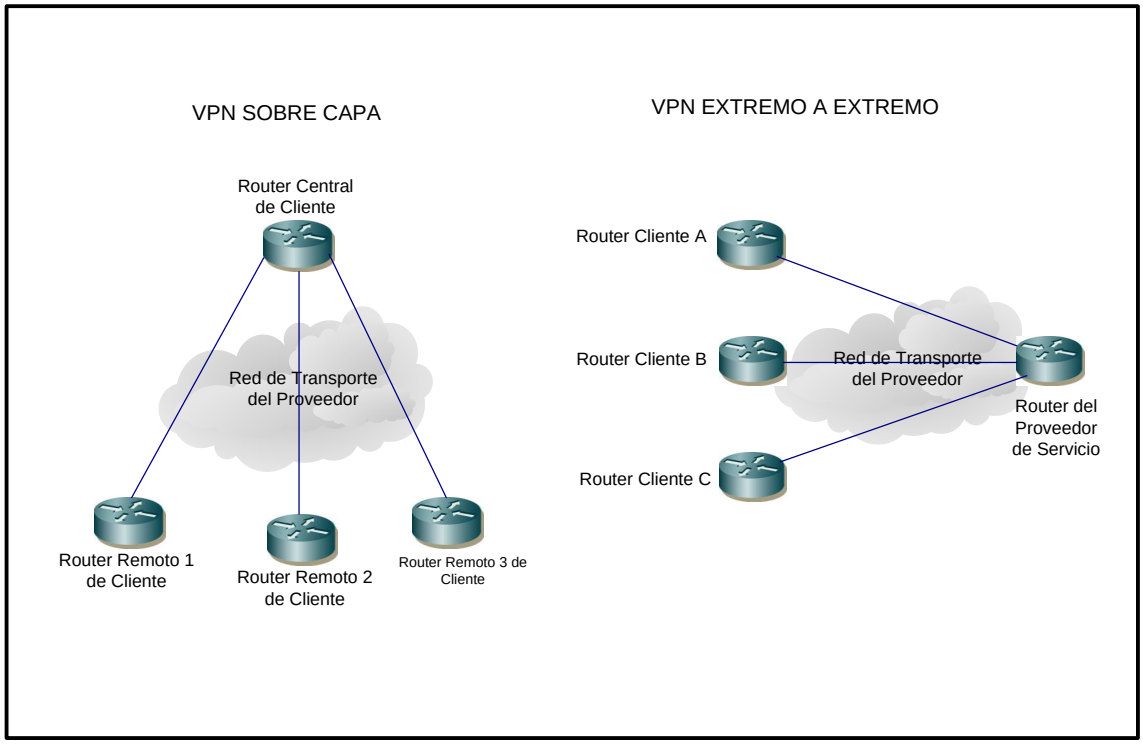
- **VPN's sobre capas (*Overlay* VPN's)**: en este tipo de VPN el usuario configura las conexiones de sus Enrutadores sobre

tecnologías tradicionales de transmisión que le proporciona el proveedor. Estas tecnologías suelen ser TDM, *Frame Relay* y ATM. De esta forma el compromiso del proveedor es proporcionar únicamente la conectividad a nivel de capa 2 y es el cliente quién se encarga de la configuración y el control de los dispositivos de Capa 3. El proveedor de servicio no es responsable de la configuración, operación y mantenimiento de los dispositivos de capa 3. Debido a la estructura de canales dedicados y a que no es un medio compartido esta solución es una de las más usadas por los clientes.

- **VPN's extremo-a-extremo (*Peer-to-Peer* VPN's):** en este caso la estructura se orienta a tener un medio compartido a nivel de capa 3 entre el usuario y el proveedor. Para lograr esto el proveedor utiliza Enrutadores de su propiedad para conectarse a los Enrutadores de cada uno de sus clientes. Esto trae como consecuencia que se tenga una sola tabla de enrutamiento y por lo tanto el proveedor debe asegurarse de configurar las listas de acceso, manejar el direccionamiento y enrutamiento de la red, para que la distintas VPN's de clientes no se mezclen.

En la figura 23 se ilustra la manera en que interactúan los dos tipos de VPN's anteriormente descritos. Para la VPN extremo a extremo, se requiere que el Proveedor tenga un profundo conocimiento sobre enrutamiento y configuraciones a nivel de capa 3. Para el caso de Guatemala este tipo de VPN no existe debido a que los clientes prefieren el modelo de VPN sobre capa por razones de seguridad.

Figura 23. **Tipos de VPN's tradicionales**



5.1.2 Topologías de VPN's tradicionales

Las topologías indican específicamente las características de conexión física para las VPN's. Esto generalmente viene determinado por características de conexión solicitadas por el cliente y por limitaciones en configuración en los equipos de transmisión. Las topologías básicas son tres y se describen a continuación.

- **Topología centralizada**: como su nombre lo indica, esta topología consiste en que todos los *Routers* remotos se conecten al *Router* central y éste último se encarga de enviar los paquetes correspondientes a cada *Router* remoto. Generalmente la configuración de enrutamiento utilizada es el enrutamiento a base de rutas estáticas debido a la simplicidad y al hecho que los *Routers* remotos sólo tienen un enlace hacia la red. Esta es la más simple de las topologías y la más difundida en nuestro medio.

- **Topología en malla**: esta topología tiene como característica que cada uno de los *Routers* se conecte a los otros por medio de un enlace. Esta topología tiene la ventaja de que permitiría la comunicación entre los *Routers* aunque el *Router* Central esté desconectado, ya sea por alguna falla que se haya presentado, o bien, porque se esté realizando algún tipo de mantenimiento en el mismo. Esta topología casi no es usada debido al elevado costo que se tendría al tener que interconectar a todos los enrutadores. Debido a la existencia de más de una conexión a la central o a otros enrutadores, se hace necesario configurar un Protocolo de enrutamiento dinámico para que se haga una mejor distribución del tráfico y se habilite la redundancia en enlaces.

- **Topología mixta**: esta topología es más común que la anterior debido a que sólo se levantan enlaces entre *Routers* que así lo requieran. Esto puede ser por razones de redundancia, ya que por alguna razón, a veces, una de todas las oficinas remotas del cliente resulta ser la más importante y se solicita que la misma tenga enlaces de redundancia para garantizar la disponibilidad, o bien, se tienen enlaces adicionales que le ayudarán a balancear y distribuir el tráfico de una mejor manera. Al igual

que en la topología anterior se hace necesario que se configuren protocolos de enrutamiento dinámico tales como RIP, OSPF, ISIS, etc.

5.2 Desventajas de las VPN's tradicionales

A continuación vamos a describir las desventajas que tienen las VPN's tradicionales en base a su tipo.

5.2.1 Desventajas para VPN's sobre capa

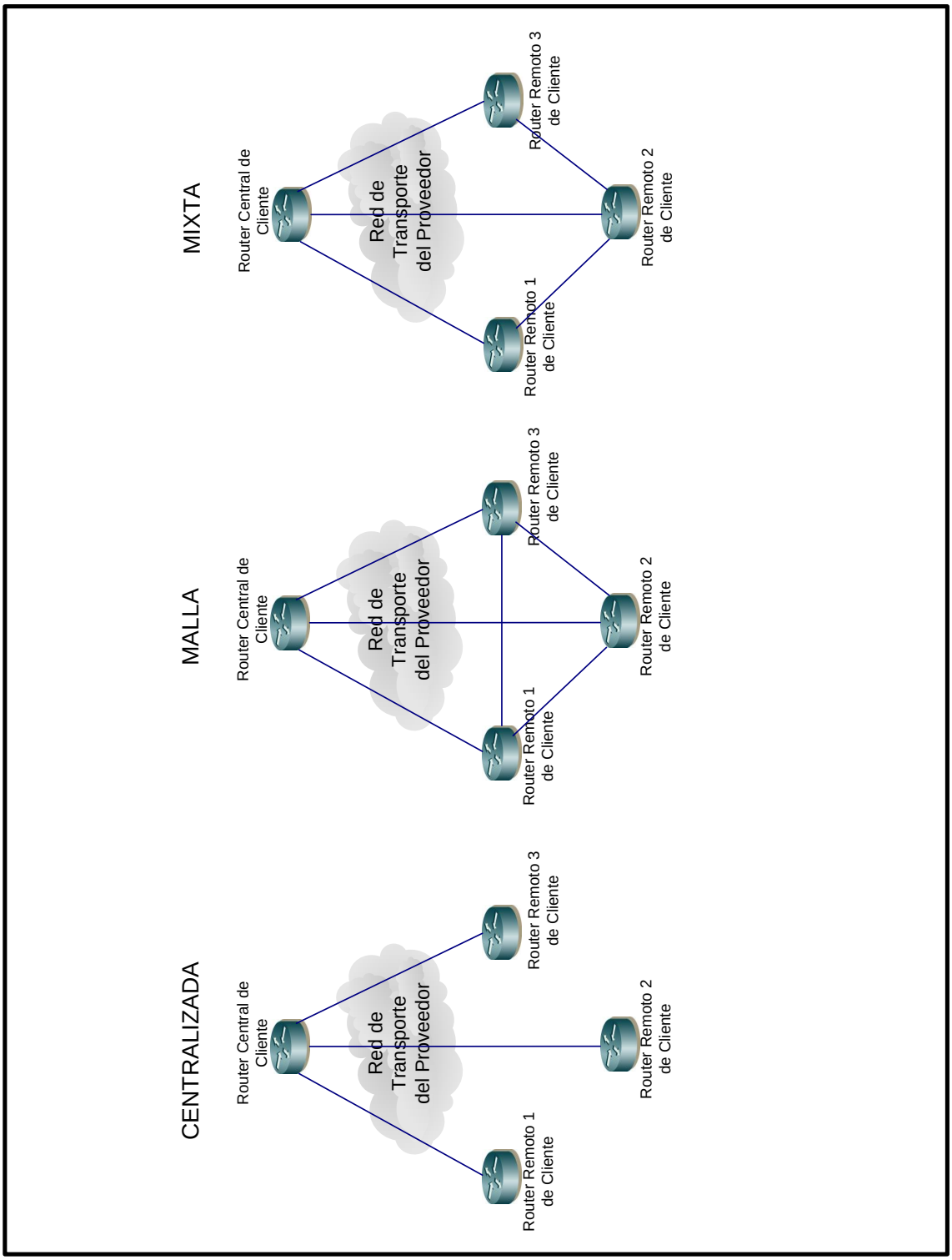
- Para implementar un óptimo enrutamiento se necesita una topología de malla, la cual es muy costosa.

- Los VC's tienen que ser configurados manualmente.

- El ancho de banda debe aprovisionarse por sitio.

- Las VPN´s sobre capa suelen tener demasiado exceso de tráfico por encabezados, especialmente cuando se hacen conexiones seguras.

Figura 24. **Topologías de VPN's tradicionales**



5.2.2 Desventajas para VPN's extremo a extremo

- El proveedor de servicio comparte el medio de enrutamiento con el cliente.

- El proveedor es el responsable por los tiempos de convergencia del cliente, en lo que respecta al enrutamiento de capa tres.

- Los *Routers* de borde llevan todas las rutas de todos los clientes.

- El proveedor de servicio necesita un buen conocimiento y experiencia de enrutamiento IP.

- Todos los clientes comparten el mismo esquema de direccionamiento, ya sea público o privado.

- Resulta complicado el esquema de bloqueos por listas de acceso.

- El desempeño es lento debido a que cada paquete debe pasar por una lista de acceso.

5.3 Características de las VPN's sobre MPLS

A continuación veremos un resumen de las principales características que distinguen las implementaciones de VPN's sobre MPLS.

- **No orientadas a la conexión**: esto significa que no es necesario que esté preestablecido un enlace virtual para que el tráfico fluya a través de la red.

- **Múltiples VPN's**: debido a su estructura y al manejo de comunidades extendidas permite el manejo de miles de VPN's separadas.

- **Seguridad entre VPN's**: las comunidades extendidas permiten que al ser un direccionamiento único, las VPN's puedan separarse del resto de VPN's configuradas y de la tabla de enrutamiento global de los equipos.

- **Bajo requerimiento de CPU**: como lo hemos visto anteriormente, el hecho de que las VPN's se construyan sobre una red MPLS trae como consecuencia que el uso de los CPU's de los *Routers* bajen considerablemente y puedan utilizarse para otras tareas.

5.4 Ventajas de las VPN's sobre MPLS

Al hacer una comparación directa de las características de las VPN's Tradicionales contra las VPN's Sobre MPLS, vemos una clara ventaja por el uso de la arquitectura de VPN's Sobre MPLS. A continuación se describen cada uno de las ventajas por las que la implementación sobre MPLS es mejor.

- **Escalabilidad**: como hemos visto desde un principio, el diseño de MPLS permite que la implementación de VPN's sea altamente escalable gracias al uso de MP-BGP.

- **Seguridad**: como la adición de la etiqueta en el modelo MPLS se realiza en una capa intermedia entre la capa 2 y la capa 3, inherentemente las VPN's sobre MPLS ya son seguras y no se necesita de configuración adicional para habilitarla; cosa que no sucede con las VPN's tradicionales.

- **Fácil configuración**: una vez que toda la infraestructura lógica está lista, la configuración de las VPN's es sumamente sencilla y se requiere solamente en los extremos de la red, específicamente, en los PE, lo que es un gran avance, ya que en las VPN's tradicionales las configuraciones había que hacerlas por cada Nodo donde pasara la trayectoria del circuito.

- **Direccionamiento flexible**: el manejo de tablas de enrutamiento de manera separada gracias a las comunidades extendidas de MP-BGP, permite que usen direccionamientos repetidos sin riesgo que se afecte el funcionamiento de las VPN's.

- **Basado en estándares**: con el fin de hacer fácil la integración con plataformas de distintos proveedores, las VPN's Sobre MPLS son creadas sobre protocolos estándar.

- **Ingeniería de tráfico**: debido a la existencia de los LSP, el administrador de la red puede hacer balanceos de tráfico sobre rutas alternativas. Esto antes no era posible debido a que los protocolos de enrutamiento tenían ciertas limitaciones. Con ingeniería de tráfico, se puede incluso configurar rutas de protección de manera similar a como se hace con SDH con los mismos tiempos de convergencia.

- **Facilidad de aplicación de calidad de servicio**: debido a la etiqueta adicionada a los paquetes, se pueden usar los *bits* experimentales de dicho encabezado para establecer varias clases de servicio y aplicarlas de manera fácil en la red.

6. PROPUESTA DE DISEÑO DE VPN'S SOBRE MPLS

Habiendo terminado el análisis funcional de las VPN's sobre MPLS, en este capítulo vamos a enfocarnos en el diseño de las mismas. Iniciaremos revisando algunas guías básicas para el diseño de dichas redes y posteriormente nos enfocaremos en los diseños particulares.

6.1 Guías para diseño

Existen una serie de recomendaciones y lineamientos para el diseño de redes IP. Adicionalmente existen recomendaciones y guías para diseñar específicamente redes MPLS. Vamos a tratar de recordar fundamentos básicos del diseño de redes IP y adicionarlos a los fundamentos del diseño de redes MPLS. Como es obvio se hace muy difícil abarcar todos los temas del diseño de redes, sin embargo, creo que vamos a llegar a una buena aproximación a los temas esenciales en este capítulo.

6.1.1 Determinar la cantidad de usuarios que tendrá la red

Cuando se va a iniciar la implementación de una Red MPLS, lo que se debe tomar en cuenta son las proyecciones de clientes que se tienen para hacer el diseño inicial de la red.

6.1.2 Determinar los puntos de presencia

El siguiente paso en el cálculo es determinar los puntos de presencia de la red, ya que en base a eso y a la cantidad de tráfico se escogerán los equipos para instalar.

6.1.3 Determinar el tráfico total de la red

En base a la cantidad de usuarios obtenida se obtiene el tráfico total de la red. A dicha cantidad se le aplican factores de crecimiento basados en la proyección de usuarios presentada. Generalmente las proyecciones se realizan a 5 años máximo debido a que la tecnología en equipos de redes cambia constantemente. Por lo tanto, la capacidad total de la red debería ser suficiente para soportar el tráfico que se tendrá en 5 años.

6.1.4 Escoger los equipos a instalar

Con la información obtenida en los apartados anteriores ya podemos proceder a escoger los equipos que se van a Instalar. Lo recomendable es escoger tecnologías basadas en transmisión *Metro Ethernet* ya que es el medio de transporte más utilizado actualmente debido a su bajo costo. En el caso de que la implementación de MPLS vaya a realizarse sobre una red existente, los equipos deberán adaptarse al medio de transmisión que se tenga, aplicando los

criterios vistos en los capítulos anteriores, tanto para redes con modo de celdas, como para redes con modo de paquetes.

6.1.5 Realizar diagrama de conexión de la red

Se debe proceder a realizar el diagrama inicial de la red sobre el cual se adjuntará el resto de información de la misma. El diagrama deberá tener toda la información en cuanto a direccionamiento, interfases y topología.

6.1.6 Asignar el direccionamiento para el núcleo de red

El direccionamiento del núcleo de red es el conjunto de direcciones IP que se utilizarán para la conectividad inicial de la red sobre la cual se configurarán los protocolos OSPF, LDP y MP-BGP. Como hemos visto anteriormente, puede usarse otros protocolos para la conectividad inicial, como por ejemplo IS-IS, sin embargo se menciona OSPF inicialmente por ser el más usado.

6.1.7 Asignar los RD's para las VPN's a configurar

Los RD's identificarán a las VPN's que se configuren. La asignación de dicho parámetro dependerá del formato que se escoja en base a los dos existentes.

6.1.8 Asignar el direccionamiento para las VPN's

Como ya vimos anteriormente, con estos datos no se tendrá mayor problema, ya que pueden ser asignados por el proveedor o por el cliente y dichos bloques de direcciones IP pueden repetirse, siempre y cuando estén en VRF's diferentes.

6.1.9 Establecer el tipo de enrutamiento que se tendrá en las VPN's

Para completar el enrutamiento hacia el cliente, se deberá establecer el protocolo a utilizar, ya sea que lo determine el proveedor según su conveniencia, o bien, que el cliente pida un tipo de protocolo en específico.

6.1.10 Generación de las configuraciones por equipo

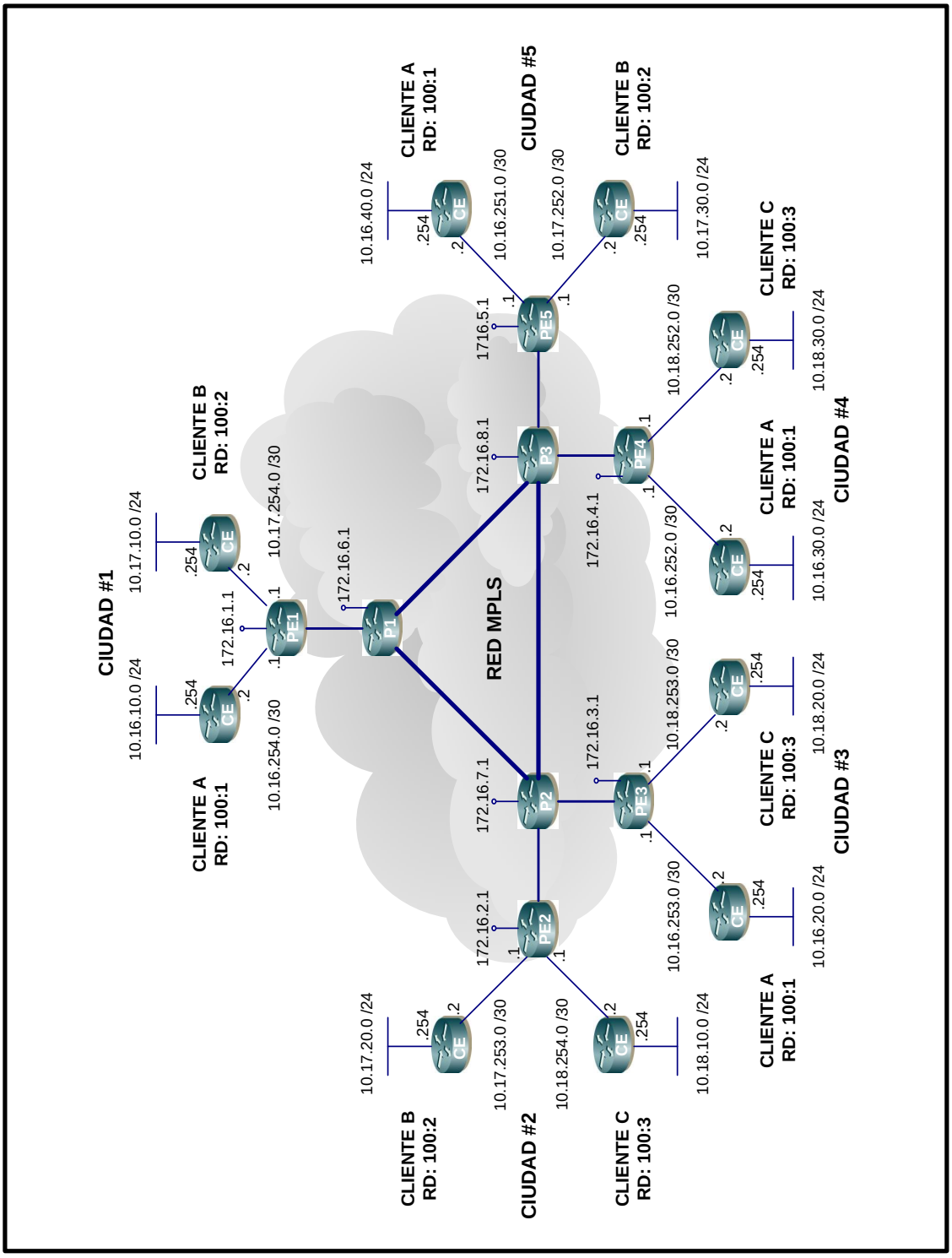
Para finalizar, se generan las configuraciones de todos los equipos para que después sean utilizadas por el personal que configurará los equipos de la red.

6.2 Propuesta de diseño sobre una red de paquetes

Para nuestra primera propuesta se armará una red que requiere *Routers* que puedan manejar MPLS. Para cumplir con este requisito, los *Routers* deben tener versión 12.0 o superior. Los comandos y configuración presentada es generalmente válida para la mayoría de los *Routers* Cisco, sin embargo, pueden haber cambios en ciertos comandos dependiendo la versión de sistema operativo que se utilice.

La figura 25 muestra el diagrama para implementación de una red MPLS sobre la cual se configurarán dos VPN's de clientes. El medio de transmisión es TDM entre todos los PE y el protocolo de empaquetado de capa 2 será PPP. Se utilizan direcciones en interfases *Loopback* para facilitar la gestión de los equipos. Los enlaces entre todos los PE son DS3. Los enlaces de los PE hacia los CE pueden ser de cuatro tipos, TDM, *Frame Relay*, *Ethernet* y ATM. De esta forma se verá como se configuran las interfases para cada tipo de enlace de transmisión.

Figura 25. **Diseño para implementación de VPN's sobre MPLS modo de paquetes**



6.2.1 Configuración de los *Routers* P del proveedor

6.2.1.1 *Router* P1

```
hostname P1
!
ip cef
!
! EL COMANDO CEF ES PRERREQUISITO PARA LA CONFIGURACIÓN DE LDP
!
interfase loopback0
 ip address 172.16.6.1 255.255.255.255
! CONFIGURACIÓN DE LOOPBACK PARA ENRUTAMIENTO
!
interfase Serial2/0/0
 ip unnumbered loopback0
 encapsulation ppp
 framing c-bit
 dsu bandwidth 44210
 clock source internal
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS
!
interfase Serial2/0/1
 ip unnumbered loopback0
 encapsulation ppp
 framing c-bit
 dsu bandwidth 44210
 clock source internal
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS
!
interfase Serial3/0/0
 ip unnumbered loopback0
 encapsulation ppp
 framing c-bit
 dsu bandwidth 44210
 clock source internal
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS
!

router ospf 100
 network 172.16.6.1 0.0.0.0 area 0
!
```

6.2.1.2 *Router* P2

```
!
hostname P2
!
ip cef
!
! EL COMANDO CEF ES PRERREQUISITO PARA LA CONFIGURACIÓN DE LDP
!
interfase loopback0
 ip address 172.16.7.1 255.255.255.255
! CONFIGURACIÓN DE LOOPBACK PARA ENRUTAMIENTO
!
interfase Serial2/0/0
 ip unnumbered loopback0
 encapsulation ppp
 framing c-bit
 dsu bandwidth 44210
 clock source internal
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS
!
interfase Serial2/0/1
 ip unnumbered loopback0
 encapsulation ppp
 framing c-bit
 dsu bandwidth 44210
 clock source internal
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS
!
interfase Serial3/0/0
 ip unnumbered loopback0
 encapsulation ppp
 framing c-bit
 dsu bandwidth 44210
 clock source internal
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS
!
interfase Serial3/0/1
 ip unnumbered loopback0
 encapsulation ppp
 framing c-bit
 dsu bandwidth 44210
 clock source internal
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS
!
router ospf 100
 network 172.16.7.1 0.0.0.0 area 0
!
```

6.2.1.3 *Router* P3

```
!
hostname P2
!
ip cef
!
! EL COMANDO CEF ES PRERREQUISITO PARA LA CONFIGURACIÓN DE LDP
!
interfase loopback0
 ip address 172.16.8.1 255.255.255.255
! CONFIGURACIÓN DE LOOPBACK PARA ENRUTAMIENTO
!
interfase Serial2/0/0
 ip unnumbered loopback0
 encapsulation ppp
 framing c-bit
 dsu bandwidth 44210
 clock source internal
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS
!
interfase Serial2/0/1
 ip unnumbered loopback0
 encapsulation ppp
 framing c-bit
 dsu bandwidth 44210
 clock source internal
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS
!
interfase Serial3/0/0
 ip unnumbered loopback0
 encapsulation ppp
 framing c-bit
 dsu bandwidth 44210
 clock source internal
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS
!
interfase Serial3/0/1
 ip unnumbered loopback0
 encapsulation ppp
 framing c-bit
 dsu bandwidth 44210
 clock source internal
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS
!
router ospf 100
 network 172.16.8.1 0.0.0.0 area 0
!
```

6.2.2 Configuración de los *Routers* PE del proveedor y CE del cliente

6.2.2.1 Ciudad #1 PE1

```
!
hostname Ciudad#1_PE1
!
ip cef
!  EL COMANDO CEF ES PRERREQUISITO PARA LA CONFIGURACIÓN DE LDP
!
ip vrf VRF1
 rd 100:1
 route-target import 100:1
 route-target export 100:1
!  CONFIGURACIÓN DEL RD DE LA VRF Y EL RT PARA IMPORTAR Y EXPORTAR
!
ip vrf VRF2
 rd 100:2
 route-target import 100:2
 route-target export 100:2
!  CONFIGURACIÓN DEL RD DE LA VRF Y EL RT PARA IMPORTAR Y EXPORTAR
!
interfase loopback0
 ip address 172.16.1.1 255.255.255.255
! CONFIGURACIÓN DE LOOPBACK PARA ENRUTAMIENTO
!
interfase Serial2/0/0
 ip unnumbered loopback0
 encapsulation ppp
 framing c-bit
 dsu bandwidth 44210
 clock source internal
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS
!
interfase Ethernet4/0/0
 ip vrf frwarding VRF1
 ip address 10.16.254.1 255.255.255.252
!  CONFIGURACIÓN DE UNA VRF SOBRE UNA INTERFASE ETHERNET CONECTADA A CE CLIENTE A
!
interfase Serial 5/0/0
 encapsulation frame-relay
 frame-relay lmi-type ansi
!  CONFIGURACIÓN DE INTERFASE CON EMPAQUETAMIENTO FRAME RELAY
!
interfase Serial 5/0/0.1 point-to-point
 ip vrf forwarding VRF2
 ip address 10.17.254.1 255.255.255.252
 frame-relay interfase-dlci 101
!  CONFIGURACIÓN DE INTERFASE DE CONEXIÓN A CE CLIENTE B
!  LA CONFIGURACIÓN DE LA SUBINTERFASE LA INSERTA EN LA VRF2 SOBRE EL DLCI 101
!
router ospf 100
 network 172.16.1.1 0.0.0.0 area 0
!
router bgp 65000
```

```
!  CONFIGURACION DE SESIONES BGP
 no synchronization
 no bgp default ipv4-activate
!  ESTE COMANDO DESACTIVA LOS ANUNCIOS POR IPV4
 neighbor 172.16.2.1 remote-as 65000
!  ESTE COMANDO DEFINE LA SESIÓN IBGP CON PE2
 neighbor 172.16.2.1 update-source loopback0
 neighbor 172.16.3.1 remote-as 65000
!  ESTE COMANDO DEFINE LA SESIÓN IBGP CON PE3
 neighbor 172.16.3.1 update-source loopback0
 neighbor 172.16.4.1 remote-as 65000
!  ESTE COMANDO DEFINE LA SESIÓN IBGP CON PE4
 neighbor 172.16.4.1 update-source loopback0
 neighbor 172.16.5.1 remote-as 65000
!  ESTE COMANDO DEFINE LA SESIÓN IBGP CON PE5
 neighbor 172.16.5.1 update-source loopback0
!
 address-family vpnv4 unicast
!  LOS SIGUIETES COMANDOS ACTIVAN EL INTERCAMBIO DE COMUNIDADES VPNV4
 neighbor 172.16.2.1 activate
 neighbor 172.16.2.1 send-community extended
 neighbor 172.16.3.1 activate
 neighbor 172.16.3.1 send-community extended
 neighbor 172.16.4.1 activate
 neighbor 172.16.4.1 send-community extended
 neighbor 172.16.5.1 activate
 neighbor 172.16.5.1 send-community extended
 exit-address-family
!
 address-family ipv4 unicast vrf VRF1
  redistribute static
!  ESTE COMANDO ANUNCIA LAS RUTAS ESTÁTICAS A LOS OTROS PE VIA IBGP
  no auto-summary
  exit-address-family
!
 address-family ipv4 unicast vrf VRF2
  redistribute static
!  ESTE COMANDO ANUNCIA LAS RUTAS ESTÁTICAS A LOS OTROS PE VIA IBGP
  no auto-summary
  exit-address-family
!
ip route vrf VRF1 10.16.10.0 255.255.255.0 e4/0/0
!  ESTE COMANDO DEFINE EL TIPO DE ENRUTAMIENTO PARA LA VRF1
!  QUE EN ESTE CASO ES ENRUTAMIENTO ESTÁTICO
!
ip route vrf VRF2 10.17.10.0 255.255.255.0 s5/0/0.1
!  ESTE COMANDO DEFINE EL TIPO DE ENRUTAMIENTO PARA LA VRF2
!  QUE EN ESTE CASO ES ENRUTAMIENTO ESTÁTICO
!
```

6.2.2.2 Ciudad #1 CE cliente A

```
!
hostname CIUDAD#1_CE_A
!
interfase ethernet 0/0
 ip address 10.16.10.254 255.255.255.0
```

```
!
interfase ethernet 0/1
 ip address 10.16.254.2 255.255.255.252
!
ip route 0.0.0.0 0.0.0.0 10.16.254.1
!
```

6.2.2.3 Ciudad #1 CE cliente B

```
!
hostname CIUDAD#1_CE_B
!
interfase ethernet 0/0
 ip address 10.17.10.254 255.255.255.0
!
!
interfase Serial 5/0/0
 encapsulation frame-relay
 frame-relay lmi-type ansi
!  CONFIGURACIÓN DE INTERFASE CON EMPAQUETAMIENTO FRAME RELAY
!
interfase Serial 5/0/0.1 point-to-point
 ip address 10.17.254.2 255.255.255.252
 frame-relay interfase-dlci 101
!  CONFIGURACIÓN DE INTERFASE DE CONEXIÓN A PE1 DESDE CLIENTE B
!  LA CONFIGURACIÓN DE LA SUBINTERFASE ES SOBRE EL DLCI 101
!
!
ip route 0.0.0.0 0.0.0.0 10.17.254.1
!
```

6.2.2.4 Ciudad #2 PE2

```
!
hostname Ciudad#2_PE2
!
ip cef
!  EL COMANDO CEF ES PRERREQUISITO PARA LA CONFIGURACIÓN DE LDP
!
ip vrf VRF2
 rd 100:2
 route-target import 100:2
 route-target export 100:2
!  CONFIGURACIÓN DEL RD DE LA VRF Y EL RT PARA IMPORTAR Y EXPORTAR
!
ip vrf VRF3
 rd 100:3
 route-target import 100:3
```

```
 route-target export 100:3
!  CONFIGURACIÓN DEL RD DE LA VRF Y EL RT PARA IMPORTAR Y EXPORTAR
!
interfase loopback0
 ip address 172.16.2.1 255.255.255.255
! CONFIGURACIÓN DE LOOPBACK PARA ENRUTAMIENTO
!
interfase Serial9/0/0
 ip unnumbered loopback0
 encapsulation ppp
 framing c-bit
 dsu bandwidth 44210
 clock source internal
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS
!
interfase Ethernet4/0/0
 ip vrf frwarding VRF2
 ip address 10.17.253.1 255.255.255.252
!  CONFIGURACIÓN DE UNA VRF SOBRE UNA INTERFASE ETHERNET CONECTADA A CE CLIENTE B
!
interfase atm1/0/0
!  CONFIGURACIÓN DE INTERFASE CON EMPAQUETAMIENTO ATM
!
interfase atm1/0/0.1 point-to-point
 ip vrf forwarding VRF3
 ip address 10.18.254.1 255.255.255.252
 pvc 3/1
 encapsulation aal5snap
!  CONFIGURACIÓN DE INTERFASE DE CONEXIÓN A CE CLIENTE C
!  LA CONFIGURACIÓN DE LA SUBINTERFASE LA INSERTA EN LA VRF2 SOBRE EL PVC 3/1
!
router ospf 100
 network 172.16.2.1 0.0.0.0 area 0
!
router rip
 version 2
 network 10.17.0.0
 network 10.18.0.0
address-family ipv4 vrf VRF2
 version 2
 network 10.17.0.0
 redistribute bgp 65000 metric 1
 no auto-summary
 exit-address-family
!
address-family ipv4 vrf VRF3
 version 2
 network 10.18.0.0
 redistribute bgp 65000 metric 1
 no auto-summary
 exit-address-family
!  LA CONFIGURACIÓN ANTERIOR MANEJA ENRUTAMIENTO RIP HACIA EL CLIENTE
!  SE REDISTRIBUYE EL PROCESO DE BGP EN CADA VRF
!
router bgp 65000
!  CONFIGURACION DE SESIONES BGP
 no synchronization
 no bgp default ipv4-activate
!  ESTE COMANDO DESACTIVA LOS ANUNCIOS POR IPV4
 neighbor 172.16.1.1 remote-as 65000
!  ESTE COMANDO DEFINE LA SESIÓN IBGP CON PE1
 neighbor 172.16.1.1 update-source loopback0
 neighbor 172.16.3.1 remote-as 65000
!  ESTE COMANDO DEFINE LA SESIÓN IBGP CON PE3
 neighbor 172.16.3.1 update-source loopback0
```

```
 neighbor 172.16.4.1 remote-as 65000
!  ESTE COMANDO DEFINE LA SESIÓN IBGP CON PE4
 neighbor 172.16.4.1 update-source loopback0
 neighbor 172.16.5.1 remote-as 65000
!  ESTE COMANDO DEFINE LA SESIÓN IBGP CON PE5
 neighbor 172.16.5.1 update-source loopback0
!
 address-family vpnv4 unicast
!  LOS SIGUIETES COMANDOS ACTIVAN EL INTERCAMBIO DE COMUNIDADES VPNV4
 neighbor 172.16.1.1 activate
 neighbor 172.16.1.1 send-community extended
 neighbor 172.16.3.1 activate
 neighbor 172.16.3.1 send-community extended
 neighbor 172.16.4.1 activate
 neighbor 172.16.4.1 send-community extended
 neighbor 172.16.5.1 activate
 neighbor 172.16.5.1 send-community extended
 exit-address-family
!
 address-family ipv4 unicast vrf VRF2
  redistribute rip
!  ESTE COMANDO REDISTRIBUYE LAS RUTAS DE RIP HACIA LOS OTROS PE VIA IBGP
  no auto-summary
  exit-address-family
!
 address-family ipv4 unicast vrf VRF3
  redistribute rip
!  ESTE COMANDO REDISTRIBUYE LAS RUTAS DE RIP HACIA LOS OTROS PE VIA IBGP
  no auto-summary
  exit-address-family
!
```

6.2.2.5 Ciudad #2 CE cliente B

```
!
hostname CIUDAD#2_CE_B
!
interfase ethernet 0/0
 ip address 10.17.20.254 255.255.255.0
!
interfase ethernet 0/1
 ip address 10.17.253.2 255.255.255.252
!
router rip
 version 2
 network 10.17.0.0
!
```

6.2.2.6 Ciudad #2 CE cliente C

```
!
hostname CIUDAD#2_CE_C
!
interfase ethernet 0/0
 ip address 10.18.10.254 255.255.255.0
!
interfase atm1/0/0.1 point-to-point
 ip address 10.18.254.1 255.255.255.252
 pvc 3/1
 encapsulation aal5snap
!  CONFIGURACIÓN DE INTERFASE DE CONEXIÓN A PE2 DESDE CLIENTE C
!  LA CONFIGURACIÓN DE LA SUBINTERFASE ES SOBRE EL PVC 3/1
!
router rip
 version 2
 network 10.18.0.0
!
```

6.2.2.7 Ciudad #3 PE3

```
!
hostname Ciudad#3_PE3
!
ip cef
!  EL COMANDO CEF ES PRERREQUISITO PARA LA CONFIGURACIÓN DE LDP
!
ip vrf VRF1
 rd 100:1
 route-target import 100:1
 route-target export 100:1
!  CONFIGURACIÓN DEL RD DE LA VRF Y EL RT PARA IMPORTAR Y EXPORTAR
!
ip vrf VRF3
 rd 100:3
 route-target import 100:3
 route-target export 100:3
!  CONFIGURACIÓN DEL RD DE LA VRF Y EL RT PARA IMPORTAR Y EXPORTAR
!
interfase loopback0
 ip address 172.16.3.1 255.255.255.255
! CONFIGURACIÓN DE LOOPBACK PARA ENRUTAMIENTO
!
interfase Serial9/0/0
 ip unnumbered loopback0
 encapsulation ppp
 framing c-bit
 dsu bandwidth 44210
 clock source internal
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS
!
```

```
interfase Ethernet4/0/0
 ip vrf frwarding VRF1
 ip address 10.16.253.1 255.255.255.252
!  CONFIGURACIÓN DE UNA VRF SOBRE UNA INTERFASE ETHERNET CONECTADA A CE CLIENTE A
!
interfase Serial5/0/0
 ip vrf forwarding VRF3
 ip address 10.18.253.1 255.255.255.252
 encapsulation hdlc
!  CONFIGURACIÓN DE INTERFASE DE CONEXIÓN A CE CLIENTE C
!  CONFIGURACIÓN DE INTERFASE CON EMPAQUETAMIENTO HDLC
!
router ospf 100
 network 172.16.3.1 0.0.0.0 area 0
!!
router bgp 65000
!  CONFIGURACION DE SESIONES BGP
 no synchronization
 no bgp default ipv4-activate
!  ESTE COMANDO DESACTIVA LOS ANUNCIOS POR IPV4
 neighbor 172.16.1.1 remote-as 65000
!  ESTE COMANDO DEFINE LA SESIÓN IBGP CON PE1
 neighbor 172.16.1.1 update-source loopback0
 neighbor 172.16.2.1 remote-as 65000
!  ESTE COMANDO DEFINE LA SESIÓN IBGP CON PE2
 neighbor 172.16.2.1 update-source loopback0
 neighbor 172.16.4.1 remote-as 65000
!  ESTE COMANDO DEFINE LA SESIÓN IBGP CON PE4
 neighbor 172.16.4.1 update-source loopback0
 neighbor 172.16.5.1 remote-as 65000
!  ESTE COMANDO DEFINE LA SESIÓN IBGP CON PE5
 neighbor 172.16.5.1 update-source loopback0
!
 address-family vpnv4 unicast
!  LOS SIGUIETES COMANDOS ACTIVAN EL INTERCAMBIO DE COMUNIDADES VPNV4
 neighbor 172.16.1.1 activate
 neighbor 172.16.1.1 send-community extended
 neighbor 172.16.2.1 activate
 neighbor 172.16.2.1 send-community extended
 neighbor 172.16.4.1 activate
 neighbor 172.16.4.1 send-community extended
 neighbor 172.16.5.1 activate
 neighbor 172.16.5.1 send-community extended
 exit-address-family
!
 address-family ipv4 unicast vrf VRF2
  neighbor 10.16.253.2 remote-as 65100
  neighbor 10.16.253.2 activate
!  ESTOS COMANDOS HABILITAN ENRUTAMIENTO BGP DENTRO DE LA VRF HACIA CLIENTE A
  no synchronization
  no auto-summary
  exit-address-family
!
 address-family ipv4 unicast vrf VRF3
  neighbor 10.18.253.2 remote-as 65200
  neighbor 10.18.253.2 activate
!  ESTOS COMANDOS HABILITAN ENRUTAMIENTO BGP DENTRO DE LA VRF HACIA CLIENTE B
  no synchronization
  no auto-summary
  exit-address-family
!
```

6.2.2.8 Ciudad #3 CE cliente A

```
!
hostname CIUDAD#3_CE_A
!
interfase ethernet 0/0
 ip address 10.16.20.254 255.255.255.0
!
interfase ethernet 0/1
 ip address 10.16.253.2 255.255.255.252
!
router bgp 65100
 neighbor 10.16.253.1 remote-as 65000
 network 10.16.20.0 mask 255.255.255.0
!
```

6.2.2.9 Ciudad #3 CE cliente C

```
!
hostname CIUDAD#3_CE_C
!
interfase ethernet 0/0
 ip address 10.18.20.254 255.255.255.0
!
interfase Serial 0/1
 encapsulation hdlc
 ip address 10.18.253.2 255.255.255.252
!
router bgp 65200
 neighbor 10.18.253.1 remote-as 65000
 network 10.18.20.0 mask 255.255.255.0
!
```

6.2.2.10 Ciudad #4 PE4

```
!
hostname Ciudad#4_PE4
!
ip cef
!  EL COMANDO CEF ES PRERREQUISITO PARA LA CONFIGURACIÓN DE LDP
!
ip vrf VRF1
 rd 100:1
 route-target import 100:1
```

```
 route-target export 100:1
!  CONFIGURACIÓN DEL RD DE LA VRF Y EL RT PARA IMPORTAR Y EXPORTAR
!
ip vrf VRF3
 rd 100:3
 route-target import 100:3
 route-target export 100:3
!  CONFIGURACIÓN DEL RD DE LA VRF Y EL RT PARA IMPORTAR Y EXPORTAR
!
interfase loopback0
 ip address 172.16.4.1 255.255.255.255
! CONFIGURACIÓN DE LOOPBACK PARA ENRUTAMIENTO
!
interfase Serial9/0/0
 ip unnumbered loopback0
 encapsulation ppp
 framing c-bit
 dsu bandwidth 44210
 clock source internal
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS
!
interfase Ethernet4/0/0
 ip vrf frwarding VRF1
 ip address 10.16.252.1 255.255.255.252
!  CONFIGURACIÓN DE UNA VRF SOBRE UNA INTERFASE ETHERNET CONECTADA A CE CLIENTE A
!
interfase Serial5/0/0
 ip vrf forwarding VRF3
 ip address 10.18.252.1 255.255.255.252
 encapsulation ppp
!  CONFIGURACIÓN DE INTERFASE DE CONEXIÓN A CE CLIENTE C
!  CONFIGURACIÓN DE INTERFASE CON EMPAQUETAMIENTO PPP
!
router ospf 100
 network 172.16.4.1 0.0.0.0 area 0
!
router ospf 111 vrf VRF1
 redistribute bgp 65000 subnets metric 10
 network 10.16.0.0 0.0.255.255 area 0
!  ESTOS COMANDOS HABILITAN OSPF DENTRO DE LA VRF
!  Y REDISTRIBUYEN LAS RUTAS DE BGP EN EL PROCESO DE OSPF
!
router ospf 333 vrf VRF3
 redistribute bgp 65000 subnets metric 10
 network 10.18.0.0 0.0.255.255 area 0
!  ESTOS COMANDOS HABILITAN OSPF DENTRO DE LA VRF
!  Y REDISTRIBUYEN LAS RUTAS DE BGP EN EL PROCESO DE OSPF
!
router bgp 65000
!  CONFIGURACION DE SESIONES BGP
 no synchronization
 no bgp default ipv4-activate
!  ESTE COMANDO DESACTIVA LOS ANUNCIOS POR IPV4
 neighbor 172.16.1.1 remote-as 65000
!  ESTE COMANDO DEFINE LA SESIÓN IBGP CON PE1
 neighbor 172.16.1.1 update-source loopback0
 neighbor 172.16.2.1 remote-as 65000
!  ESTE COMANDO DEFINE LA SESIÓN IBGP CON PE2
 neighbor 172.16.2.1 update-source loopback0
 neighbor 172.16.3.1 remote-as 65000
!  ESTE COMANDO DEFINE LA SESIÓN IBGP CON PE3
 neighbor 172.16.3.1 update-source loopback0
 neighbor 172.16.5.1 remote-as 65000
!  ESTE COMANDO DEFINE LA SESIÓN IBGP CON PE5
 neighbor 172.16.5.1 update-source loopback0
```

```
!
 address-family vpnv4 unicast
!  LOS SIGUIETES COMANDOS ACTIVAN EL INTERCAMBIO DE COMUNIDADES VPNV4
 neighbor 172.16.1.1 activate
 neighbor 172.16.1.1 send-community extended
 neighbor 172.16.2.1 activate
 neighbor 172.16.2.1 send-community extended
 neighbor 172.16.3.1 activate
 neighbor 172.16.3.1 send-community extended
 neighbor 172.16.5.1 activate
 neighbor 172.16.5.1 send-community extended
 exit-address-family
!
!
 address-family ipv4 unicast vrf VRF1
  redistribute ospf 111 subnets
!  ESTE COMANDO ANUNCIA LAS RUTAS POR OSPF A LOS OTROS PE VIA IBGP
  no auto-summary
  no synchronization
  exit-address-family
!
 address-family ipv4 unicast vrf VRF3
  redistribute ospf 333 subnets
!  ESTE COMANDO ANUNCIA LAS RUTAS POR OSPF A LOS OTROS PE VIA IBGP
  no auto-summary
  no synchronization
  exit-address-family
!
```

6.2.2.11 Ciudad #4 CE cliente A

```
!
hostname CIUDAD#4_CE_A
!
interfase ethernet 0/0
 ip address 10.16.30.254 255.255.255.0
!
interfase ethernet 0/1
 ip address 10.16.252.2 255.255.255.252
!
router ospf 111
 network 10.16.0.0 0.0.255.255 area 0
!
```

6.2.2.12 Ciudad #4 CE cliente C

```
!
hostname CIUDAD#4_CE_C
!
```

```
interfase ethernet 0/0
 ip address 10.18.30.254 255.255.255.0
!
interfase Serial0/0
 encapsulation ppp
 ip address 10.18.252.2 255.255.255.252
!
router ospf 333
 network 10.18.0.0 0.0.255.255 area 0
!
```

6.2.2.13 Ciudad #5 PE5

```
!
hostname Ciudad#5_PE5
!
ip cef
!  EL COMANDO CEF ES PRERREQUISITO PARA LA CONFIGURACIÓN DE LDP
!
ip vrf VRF1
 rd 100:1
 route-target import 100:1
 route-target export 100:1
!  CONFIGURACIÓN DEL RD DE LA VRF Y EL RT PARA IMPORTAR Y EXPORTAR
!
ip vrf VRF2
 rd 100:2
 route-target import 100:2
 route-target export 100:2
!  CONFIGURACIÓN DEL RD DE LA VRF Y EL RT PARA IMPORTAR Y EXPORTAR
!
interfase loopback0
 ip address 172.16.5.1 255.255.255.255
! CONFIGURACIÓN DE LOOPBACK PARA ENRUTAMIENTO
!
interfase Serial9/0/0
 ip unnumbered loopback0
 encapsulation ppp
 framing c-bit
 dsu bandwidth 44210
 clock source internal
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS
!
interfase Ethernet4/0/0
 ip vrf frwarding VRF1
 ip address 10.16.251.1 255.255.255.252
!  CONFIGURACIÓN DE UNA VRF SOBRE UNA INTERFASE ETHERNET CONECTADA A CE CLIENTE A
!
interfase Serial 5/0/0
 encapsulation frame-relay
 frame-relay lmi-type ansi
!  CONFIGURACIÓN DE INTERFASE CON EMPAQUETAMIENTO FRAME RELAY
!
interfase Serial 5/0/0.1 point-to-point
 ip vrf forwarding VRF2
 ip address 10.17.252.1 255.255.255.252
```

```
 frame-relay interfase-dlci 201
!  CONFIGURACIÓN DE INTERFASE DE CONEXIÓN A CE CLIENTE B
!  LA CONFIGURACIÓN DE LA SUBINTERFASE LA INSERTA EN LA VRF2 SOBRE EL DLCI 201
!
router ospf 100
 network 172.16.5.1 0.0.0.0 area 0
!
router bgp 65000
!  CONFIGURACION DE SESIONES BGP
 no synchronization
 no bgp default ipv4-activate
!  ESTE COMANDO DESACTIVA LOS ANUNCIOS POR IPV4
 neighbor 172.16.1.1 remote-as 65000
!  ESTE COMANDO DEFINE LA SESIÓN IBGP CON PE1
 neighbor 172.16.1.1 update-source loopback0
 neighbor 172.16.2.1 remote-as 65000
!  ESTE COMANDO DEFINE LA SESIÓN IBGP CON PE2
 neighbor 172.16.2.1 update-source loopback0
 neighbor 172.16.3.1 remote-as 65000
!  ESTE COMANDO DEFINE LA SESIÓN IBGP CON PE3
 neighbor 172.16.3.1 update-source loopback0
 neighbor 172.16.4.1 remote-as 65000
!  ESTE COMANDO DEFINE LA SESIÓN IBGP CON PE4
 neighbor 172.16.4.1 update-source loopback0
!
 address-family vpnv4 unicast
!  LOS SIGUIETES COMANDOS ACTIVAN EL INTERCAMBIO DE COMUNIDADES VPNV4
 neighbor 172.16.1.1 activate
 neighbor 172.16.1.1 send-community extended
 neighbor 172.16.2.1 activate
 neighbor 172.16.2.1 send-community extended
 neighbor 172.16.3.1 activate
 neighbor 172.16.3.1 send-community extended
 neighbor 172.16.4.1 activate
 neighbor 172.16.4.1 send-community extended
 exit-address-family
!
 address-family ipv4 unicast vrf VRF1
  redistribute static
!  ESTE COMANDO ANUNCIA LAS RUTAS ESTÁTICAS A LOS OTROS PE VIA IBGP
  no auto-summary
  exit-address-family
!
 address-family ipv4 unicast vrf VRF2
  redistribute static
!  ESTE COMANDO ANUNCIA LAS RUTAS ESTÁTICAS A LOS OTROS PE VIA IBGP
  no auto-summary
  exit-address-family
!
ip route vrf VRF1 10.16.40.0 255.255.255.0 e4/0/0
!  ESTE COMANDO DEFINE EL TIPO DE ENRUTAMIENTO PARA LA VRF1
!  QUE EN ESTE CASO ES ENRUTAMIENTO ESTÁTICO
!
ip route vrf VRF2 10.17.30.0 255.255.255.0 s5/0/0.1
!  ESTE COMANDO DEFINE EL TIPO DE ENRUTAMIENTO PARA LA VRF2
!  QUE EN ESTE CASO ES ENRUTAMIENTO ESTÁTICO
!
```

6.2.2.14 Ciudad #5 CE cliente A

```
!
hostname CIUDAD#5_CE_A
!
interfase ethernet 0/0
 ip address 10.16.40.254 255.255.255.0
!
interfase ethernet 0/1
 ip address 10.16.251.2 255.255.255.252
!
ip route 0.0.0.0 0.0.0.0 10.16.251.1
!
```

6.2.2.15 Ciudad #5 CE cliente B

```
!
hostname CIUDAD#5_CE_B
!
interfase ethernet 0/0
 ip address 10.17.30.254 255.255.255.0
!
!
interfase Serial 5/0/0
 encapsulation frame-relay
 frame-relay lmi-type ansi
!  CONFIGURACIÓN DE INTERFASE CON EMPAQUETAMIENTO FRAME RELAY
!
interfase Serial 5/0/0.1 point-to-point
 ip address 10.17.252.2 255.255.255.252
 frame-relay interfase-dlci 201
!  CONFIGURACIÓN DE INTERFASE DE CONEXIÓN A PE5 DESDE CLIENTE B
!  LA CONFIGURACIÓN DE LA SUBINTERFASE ES SOBRE EL DLCI 201
!
!
ip route 0.0.0.0 0.0.0.0 10.17.252.1
!
```

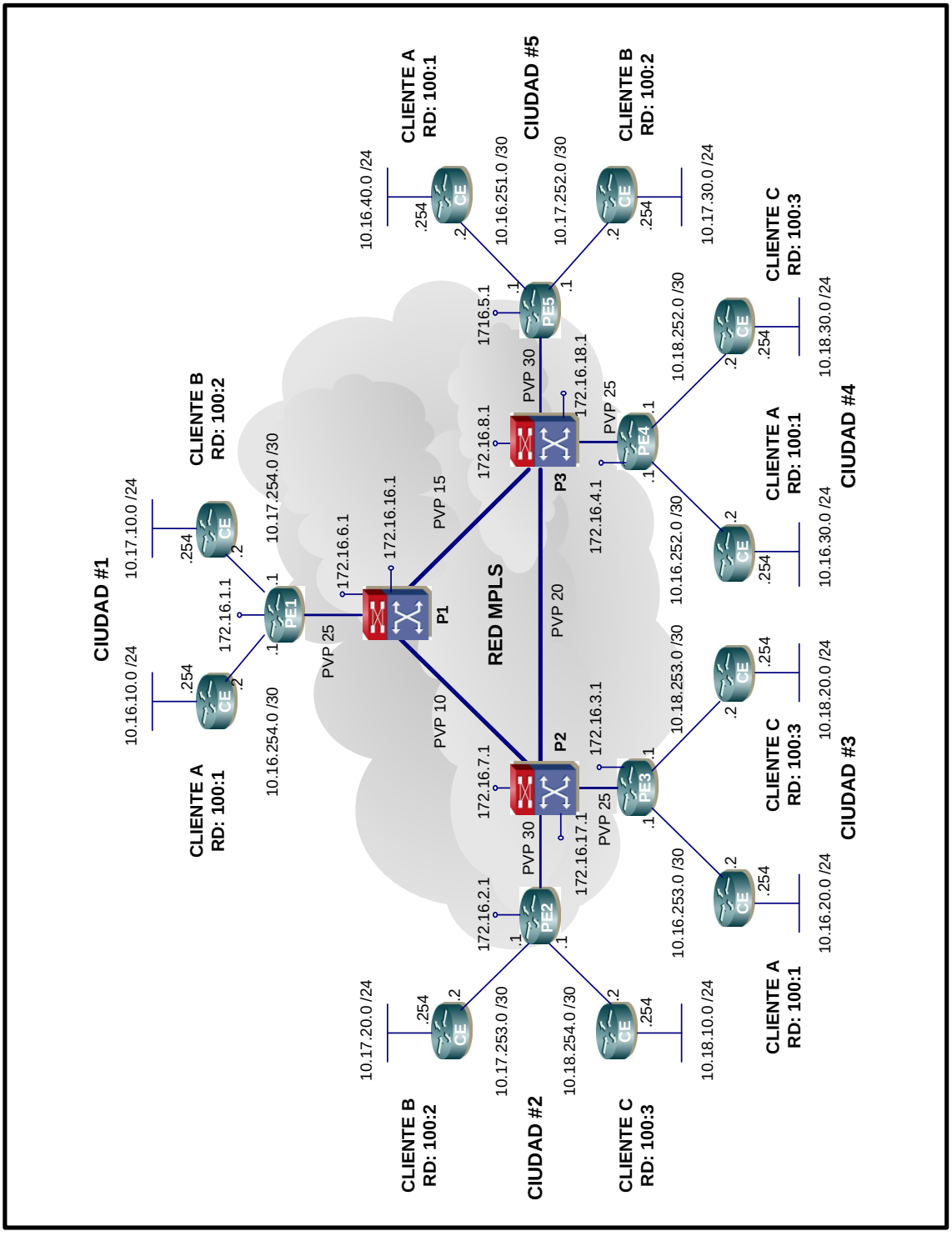
6.3 Propuesta de diseño en red modo ATM nativo

La propuesta de diseño para una red MPLS en modo ATM nativo la vamos a basar en la misma red que se presentó para el modo de paquetes con la diferencia de que ahora las conexiones entre los *Routers* PE y P son con interfases ATM. Para esto se hace necesario que los *Routers* PE posean una interfase STM-1 ATM en lugar de serial.

Los *Routers* P en lugar de ser *Routers* normales ahora se convierten en un equipo que posee funciones de conmutador ATM y de *Router*. Para esta propuesta se está basando la configuración en un equipo Cisco 6400. Este equipo posee tarjetas NSP, o sea, nodo procesador de conmutación, que proporcionan las funciones de conmutación ATM. Adicionalmente el equipo posee tarjetas NRP, o sea, nodo procesador de enrutamiento, este se encarga de todas las funciones de enrutamiento, MPLS y LSC que vimos en el modo ATM nativo. Las interfases de conexión entre todos los *Routers* P son STM-1 ATM.

El modelo de configuración de equipos de *Router* PE a *Router* CE es el mismo que se tuvo para el modo de paquetes, por lo tanto solo se va a mostrar esquemas de configuración de cada uno de los equipos relacionada solamente con la configuración del modo ATM nativo. Nuevamente se hace la aclaración que los comandos y configuraciones propuestas son generalmente válidas en los equipos, sin embargo, pueden haber variaciones debidas a nuevos sistemas operativos o a cambios en las estructuras de los equipos más recientes. La figura 26 nos muestra el esquema base de la propuesta.

Figura 26. **Diseño para implementación de VPN's sobre MPLS modo ATM nativo**



6.3.1 Configuración de los *Routers* P del proveedor

6.3.1.1 *Router* P1 NSP

```
hostname P1_NSP
!
ip cef
!
! EL COMANDO CEF ES PRERREQUISITO PARA LA CONFIGURACIÓN DE LDP
!
interfase loopback0
 ip address 172.16.16.1 255.255.255.255
! CONFIGURACIÓN DE LOOPBACK PARA ENRUTAMIENTO
!
interface ATM0/0/0
 no ip address
! CONFIGURACIÓN DE INTERFASE LSC PARA COMUNICACIÓN HACIA NRP
!
interface ATM0/0/0.1 point-to-point
 mtu 1900
 ip unnumbered Loopback0
 pvc 0/32
  encapsulation aal5snap
 !
! CONFIGURACIÓN DE INTERFASE LSC PARA COMUNICACIÓN HACIA NRP
!
interfase ATM2/0/0
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 sonet stm-1
! CONFIGURACIÓN DE LA INTERFASE FÍSICA DE ATM HACIA PE1
!
interfase ATM2/0/1
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 sonet stm-1
! CONFIGURACIÓN DE LA INTERFASE FÍSICA DE ATM HACIA P2
!
interfase ATM2/1/0
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 sonet stm-1
! CONFIGURACIÓN DE LA INTERFASE FÍSICA DE ATM HACIA P3
!
interface ATM5/0/0
 no ip address
 no atm ilmi-keepalive
 atm pvc 0 32  interface  ATM0/0/0.1 0 32
 atm pvp 25  interface  ATM2/0/0 25
 atm pvp 10  interface  ATM2/0/1 10
 atm pvp 15  interface  ATM2/1/0 15
! CONFIGURACIÓN DE LA INTERFASE ATM HACIA NRP
!
```

```
router ospf 100
 network 172.16.16.1 0.0.0.0 area 0
!
```

6.3.1.2 *Router* P1 NRP

```
!
hostname P1_NRP
!
ip cef
!
! EL COMANDO CEF ES PRERREQUISITO PARA LA CONFIGURACIÓN DE LDP
!
interfase loopback0
 ip address 172.16.6.1 255.255.255.255
! CONFIGURACIÓN DE LOOPBACK PARA ENRUTAMIENTO
!
interface ATM0/0/0
 no ip address
 no atm ilmi-keepalive
! CONFIGURACIÓN DE INTERFASE LSC PARA COMUNICACIÓN HACIA NSP
!
interface ATM0/0/0.1 point-to-point
 description CONEXION HACIA NSP
 ip unnumbered Loopback0
 pvc 0/32
  encapsulation aal5snap
 !
! CONFIGURACIÓN DE INTERFASE LSC PARA COMUNICACIÓN HACIA NSP
!
interface ATM0/0/0.25 tag-switching
 ip unnumbered Loopback0
 no ip directed-broadcast
 tag-switching atm vp-tunnel 25 vci-range 33-65535
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS HACIA PE1
!
interface ATM0/0/0.10 tag-switching
 ip unnumbered Loopback0
 no ip directed-broadcast
 tag-switching atm vp-tunnel 10 vci-range 33-65535
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS HACIA P2
!
interface ATM0/0/0.15 tag-switching
 ip unnumbered Loopback0
 no ip directed-broadcast
 tag-switching atm vp-tunnel 15 vci-range 33-65535
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS HACIA P3
!
router ospf 100
 network 172.16.6.1 0.0.0.0 area 0
!
```

6.3.1.3 *Router* P2 NSP

```
hostname P2_NSP
!
ip cef
!
! EL COMANDO CEF ES PRERREQUISITO PARA LA CONFIGURACIÓN DE LDP
!
interfase loopback0
 ip address 172.16.17.1 255.255.255.255
! CONFIGURACIÓN DE LOOPBACK PARA ENRUTAMIENTO
!
interface ATM0/0/0
 no ip address
! CONFIGURACIÓN DE INTERFASE LSC PARA COMUNICACIÓN HACIA NRP
!
interface ATM0/0/0.1 point-to-point
 mtu 1900
 ip unnumbered Loopback0
 pvc 0/32
  encapsulation aal5snap
 !
! CONFIGURACIÓN DE INTERFASE LSC PARA COMUNICACIÓN HACIA NRP
!
interfase ATM2/0/0
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 sonet stm-1
! CONFIGURACIÓN DE LA INTERFASE FÍSICA DE ATM HACIA PE2
!
interfase ATM2/0/1
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 sonet stm-1
! CONFIGURACIÓN DE LA INTERFASE FÍSICA DE ATM HACIA PE3
!
interfase ATM2/1/0
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 sonet stm-1
! CONFIGURACIÓN DE LA INTERFASE FÍSICA DE ATM HACIA P3
!
interfase ATM2/1/1
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 sonet stm-1
! CONFIGURACIÓN DE LA INTERFASE FÍSICA DE ATM HACIA P1
!
interface ATM5/0/0
 no ip address
 no atm ilmi-keepalive
 atm pvc 0 32  interface  ATM0/0/0.1 0 32
 atm pvp 30  interface  ATM2/0/0 30
 atm pvp 25  interface  ATM2/0/1 25
 atm pvp 20  interface  ATM2/1/0 20
 atm pvp 10  interface  ATM2/1/1 10
! CONFIGURACIÓN DE LA INTERFASE ATM HACIA NRP
```

```
!
router ospf 100
 network 172.16.17.1 0.0.0.0 area 0
!
```

6.3.1.4 *Router* P2 NRP

```
!
!
hostname P2_NRP
!
ip cef
!
! EL COMANDO CEF ES PRERREQUISITO PARA LA CONFIGURACIÓN DE LDP
!
interfase loopback0
 ip address 172.16.7.1 255.255.255.255
! CONFIGURACIÓN DE LOOPBACK PARA ENRUTAMIENTO
!
interface ATM0/0/0
 no ip address
 no atm ilmi-keepalive
! CONFIGURACIÓN DE INTERFASE LSC PARA COMUNICACIÓN HACIA NSP
!
interface ATM0/0/0.1 point-to-point
 description CONEXION HACIA NSP
 ip unnumbered Loopback0
 pvc 0/32
  encapsulation aal5snap
 !
! CONFIGURACIÓN DE INTERFASE LSC PARA COMUNICACIÓN HACIA NSP
!
interface ATM0/0/0.30 tag-switching
 ip unnumbered Loopback0
 no ip directed-broadcast
 tag-switching atm vp-tunnel 30 vci-range 33-65535
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS HACIA PE2
!
interface ATM0/0/0.25 tag-switching
 ip unnumbered Loopback0
 no ip directed-broadcast
 tag-switching atm vp-tunnel 25 vci-range 33-65535
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS HACIA PE3
!
interface ATM0/0/0.20 tag-switching
 ip unnumbered Loopback0
 no ip directed-broadcast
 tag-switching atm vp-tunnel 20 vci-range 33-65535
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS HACIA P3
!
interface ATM0/0/0.10 tag-switching
 ip unnumbered Loopback0
 no ip directed-broadcast
 tag-switching atm vp-tunnel 10 vci-range 33-65535
```

```
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS HACIA P1
!
router ospf 100
 network 172.16.7.1 0.0.0.0 area 0
!
```

6.3.1.5 *Router* P3 NSP

```
hostname P3_NSP
!
ip cef
!
! EL COMANDO CEF ES PRERREQUISITO PARA LA CONFIGURACIÓN DE LDP
!
interfase loopback0
 ip address 172.16.18.1 255.255.255.255
! CONFIGURACIÓN DE LOOPBACK PARA ENRUTAMIENTO
!
interface ATM0/0/0
 no ip address
! CONFIGURACIÓN DE INTERFASE LSC PARA COMUNICACIÓN HACIA NRP
!
interface ATM0/0/0.1 point-to-point
 mtu 1900
 ip unnumbered Loopback0
 pvc 0/32
  encapsulation aal5snap
 !
! CONFIGURACIÓN DE INTERFASE LSC PARA COMUNICACIÓN HACIA NRP
!
interfase ATM2/0/0
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 sonet stm-1
! CONFIGURACIÓN DE LA INTERFASE FÍSICA DE ATM HACIA PE4
!
interfase ATM2/0/1
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 sonet stm-1
! CONFIGURACIÓN DE LA INTERFASE FÍSICA DE ATM HACIA PE5
!
interfase ATM2/1/0
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 sonet stm-1
! CONFIGURACIÓN DE LA INTERFASE FÍSICA DE ATM HACIA P1
!
interfase ATM2/1/1
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
 sonet stm-1
```

```
! CONFIGURACIÓN DE LA INTERFASE FÍSICA DE ATM HACIA P2
!
interface ATM5/0/0
 no ip address
 no atm ilmi-keepalive
 atm pvc 0 32  interface  ATM0/0/0.1 0 32
 atm pvp 25  interface  ATM2/0/0 25
 atm pvp 30  interface  ATM2/0/1 30
 atm pvp 15  interface  ATM2/1/0 15
 atm pvp 20  interface  ATM2/1/1 20
! CONFIGURACIÓN DE LA INTERFASE ATM HACIA NRP
!
router ospf 100
 network 172.16.18.1 0.0.0.0 area 0
!
```

6.3.1.6 *Router* P3 NRP

```
!
!
hostname P3_NRP
!
ip cef
!
! EL COMANDO CEF ES PRERREQUISITO PARA LA CONFIGURACIÓN DE LDP
!
interfase loopback0
 ip address 172.16.8.1 255.255.255.255
! CONFIGURACIÓN DE LOOPBACK PARA ENRUTAMIENTO
!
interface ATM0/0/0
 no ip address
 no atm ilmi-keepalive
! CONFIGURACIÓN DE INTERFASE LSC PARA COMUNICACIÓN HACIA NSP
!
interface ATM0/0/0.1 point-to-point
 description CONEXION HACIA NSP
 ip unnumbered Loopback0
 pvc 0/32
  encapsulation aal5snap
 !
! CONFIGURACIÓN DE INTERFASE LSC PARA COMUNICACIÓN HACIA NSP
!
interface ATM0/0/0.25 tag-switching
 ip unnumbered Loopback0
 no ip directed-broadcast
 tag-switching atm vp-tunnel 25 vci-range 33-65535
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS HACIA PE4
!
interface ATM0/0/0.30 tag-switching
 ip unnumbered Loopback0
 no ip directed-broadcast
 tag-switching atm vp-tunnel 30 vci-range 33-65535
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS HACIA PE5
!
```

```
interface ATM0/0/0.15 tag-switching
 ip unnumbered Loopback0
 no ip directed-broadcast
 tag-switching atm vp-tunnel 15 vci-range 33-65535
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS HACIA P1
!
interface ATM0/0/0.20 tag-switching
 ip unnumbered Loopback0
 no ip directed-broadcast
 tag-switching atm vp-tunnel 20 vci-range 33-65535
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS HACIA P2
!
router ospf 100
 network 172.16.8.1 0.0.0.0 area 0
!
```

6.3.2 Configuración de los *Routers* PE del proveedor

6.3.2.1 Ciudad #1 PE1

```
!
hostname Ciudad#1_PE1
!
ip cef
!  EL COMANDO CEF ES PRERREQUISITO PARA LA CONFIGURACIÓN DE LDP
!
interfase loopback0
 ip address 172.16.1.1 255.255.255.255
! CONFIGURACIÓN DE LOOPBACK PARA ENRUTAMIENTO
!
interfase ATM2/0/0
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
! CONFIGURACIÓN DE LA INTERFASE FÍSICA
!
interfase ATM2/0/0.1 tag-switching
 ip unnumbered loopback0
 no ip directed-broadcast
 tag-switching atm vp-tunnel 25 vci-range 33-65535
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS
!
```

6.3.2.2 Ciudad #2 PE2

```
!
hostname Ciudad#2_PE2
!
ip cef
!  EL COMANDO CEF ES PRERREQUISITO PARA LA CONFIGURACIÓN DE LDP
!
interfase loopback0
 ip address 172.16.2.1 255.255.255.255
! CONFIGURACIÓN DE LOOPBACK PARA ENRUTAMIENTO
!
interfase ATM9/0/0
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
! CONFIGURACIÓN DE LA INTERFASE FÍSICA
!
interfase ATM9/0/0.1 tag-switching
 ip unnumbered loopback0
 no ip directed-broadcast
 tag-switching atm vp-tunnel 30 vci-range 33-65535
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS
!
```

6.3.2.3 Ciudad #3 PE3

```
!
hostname Ciudad#3_PE3
!
ip cef
!  EL COMANDO CEF ES PRERREQUISITO PARA LA CONFIGURACIÓN DE LDP
!
interfase loopback0
 ip address 172.16.3.1 255.255.255.255
! CONFIGURACIÓN DE LOOPBACK PARA ENRUTAMIENTO
!
interfase ATM9/0/0
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
! CONFIGURACIÓN DE LA INTERFASE FÍSICA
!
interfase ATM9/0/0.1 tag-switching
 ip unnumbered loopback0
 no ip directed-broadcast
 tag-switching atm vp-tunnel 25 vci-range 33-65535
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS
!
```

6.3.2.4 Ciudad #4 PE4

```
!
hostname Ciudad#4_PE4
!
ip cef
!  EL COMANDO CEF ES PRERREQUISITO PARA LA CONFIGURACIÓN DE LDP
!
interfase loopback0
 ip address 172.16.4.1 255.255.255.255
! CONFIGURACIÓN DE LOOPBACK PARA ENRUTAMIENTO
!
interfase ATM9/0/0
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
! CONFIGURACIÓN DE LA INTERFASE FÍSICA
!
interfase ATM9/0/0.1 tag-switching
 ip unnumbered loopback0
 no ip directed-broadcast
 tag-switching atm vp-tunnel 25 vci-range 33-65535
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS
!
```

6.3.2.5 Ciudad #5 PE5

```
!
hostname Ciudad#5_PE5
!
ip cef
!  EL COMANDO CEF ES PRERREQUISITO PARA LA CONFIGURACIÓN DE LDP
!
interfase loopback0
 ip address 172.16.5.1 255.255.255.255
! CONFIGURACIÓN DE LOOPBACK PARA ENRUTAMIENTO
!
interfase ATM9/0/0
 no ip address
 no ip directed-broadcast
 no atm ilmi-keepalive
! CONFIGURACIÓN DE LA INTERFASE FÍSICA
!
interfase ATM9/0/0.1 tag-switching
 ip unnumbered loopback0
 no ip directed-broadcast
 tag-switching atm vp-tunnel 30 vci-range 33-65535
 tag-switching ip
! CONFIGURACIÓN DE LA INTERFASE PARA CONMUTACIÓN DE ETIQUETAS
!
```

Siempre que se diseñen redes MPLS Modelo ATM Nativo, se deberá tomar en cuenta que el número de PVC's es limitado, por lo que se recomienda hacer un cálculo previo sobre la cantidad de prefijos que tendrá la red. Deberá también proyectarse a futuro determinado la cantidad de prefijos que tendrá la red. En todo caso se verá que la implementación en modo ATM nativo es más cara y menos escalable. Puede hacerse una implementación de modo ATM nativo en una red ATM existente, sin embargo, la migración de la misma a una red de modo de paquetes se tendrá que hacer tarde o temprano dependiendo del crecimiento de la red y del tiempo de vida de los equipos ATM existentes.

De esta manera concluimos de presentar todas las configuraciones del diseño preliminar, tanto para el modo de paquetes, como para el modo ATM nativo. Como se podrá verificar se han visto todos los escenarios en donde se implementa con tecnologías de transmisión que vimos en el primer capítulo y que son TDM (HDLC, PPP), *Frame Relay*, *Ethernet* y ATM. Igualmente se abarcaron los cuatro posibles enrutamientos que son OSPF, BGP, RIP y rutas estáticas.

Podemos concluir de este capítulo, que la implementación de VPN's sobre MPLS tiene la flexibilidad de poder usar cualquier medio de transmisión.

CONCLUSIONES

1. Las tecnologías tradicionales de transmisión proveen una infraestructura de transmisión necesaria para implementar redes privadas virtuales, sin embargo, dichas infraestructuras son costosas y requieren más recursos para su implementación.

2. MPLS es una tecnología versátil que permite un manejo más eficiente del envío de paquetes de capa 3, todo con base a trayectorias de etiquetas conmutadas.

3. Una red privada virtual sobre una Red MPLS se construye sobre trayectorias específicas de etiquetas conmutadas y creando un enrutamiento virtual para cada VPN.

4. Una VPN sobre MPLS presenta más ventajas que una VPN tradicional debido a que su implementación es menos costosa y presenta más características útiles que las VPN's tradicionales.

5. La tecnología MPLS tiene la flexibilidad suficiente para permitir implementaciones en escenarios de transmisión de datos tradicionales,

tanto en escenarios de migración gradual, como en escenarios donde toda la red de transmisión se convierte en una red MPLS en modo de paquetes.

RECOMENDACIONES

1. Cuando se diseñe una red MPLS es bueno hacer una proyección de crecimiento de 3 a 5 años, esto permitirá instalar equipos y capacidad suficiente para llevar un crecimiento de red fácil sin tener que hacer cambios demasiado grandes en la red.

2. Si ya se posee una red MPLS con VPN's implementadas se debe analizar y comparar el crecimiento del tráfico contra la capacidad actual instalada, ya que existen limitantes tanto del lado de los equipos, como del lado del sistema operativo que pueden afectar el desempeño de la red.

3. Iniciar ampliaciones de red en donde se requiera al alcanzar el 80% de utilización. Iniciar en este punto permite tener suficiente tiempo para que la ampliación esté lista sin afectar el tráfico que cursa por la red.

BIBLIOGRAFÍA

1. Alwayn, Viviek. ***Advanced* MPLS *design and implementation.*** Indianapolis: Cisco Press, 2002.

2. De Ghein, Luc. **MPLS *fundamentals*.** Indianapolis: Cisco Press, 2006.

3. Halabi, Sam. ***Internet routing arquitectures***. Second Edition. Indianapolis: Cisco Press, 2001.

4. Lewis, Christopher S. **Cisco TCP/IP *routing professional reference*.** McGraw-Hill, 1998**.**

5. Pepelnjak Ivan, Jim Guichard; **MPLS *and* VPN *arquitectures*.** Indianapolis: Cisco Press, 2002.

6. Pepelnjak Ivan, Jim Guichard, Jeff Apcar **MPLS *and* VPN *arquitectures*.** (Volumen II). Indianápolis: Cisco Press, 2003.