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

ANÁLISIS DE LA FACTIBILIDAD TÉCNICA Y ECONÓMICA DE LA MIGRACIÓN DE UNA RED METRO ETHERNET A PBB-TE

Ricardo Augusto del Cid Mancio
Asesorado por el Ing. Enrique Edmundo Ruiz Carballo

Guatemala, julio de 2015

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

ANÁLISIS DE LA FACTIBILIDAD TÉCNICA Y ECONÓMICA DE LA MIGRACIÓN DE UNA RED METRO ETHERNET A PBB-TE

TRABAJO DE GRADUACIÓN

PRESENTADO A LA JUNTA DIRECTIVA DE LA
FACULTAD DE INGENIERÍA
POR

RICARDO AUGUSTO DEL CID MANCIO
ASESORADO POR EL ING. ENRIQUE EDMUNDO RUIZ CARBALLO

AL CONFERÍRSELE EL TÍTULO DE

INGENIERO EN ELECTRÓNICA

GUATEMALA, JULIO DE 2015

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA

FACULTAD DE INGENIERÍA

NÓMINA DE JUNTA DIRECTIVA

DECANO	Ing. Pedro Antonio Aguilar Polanco
VOCAL I	Ing. Angel Roberto Sic García
VOCAL II	Ing. Pablo Christian de León Rodríguez
VOCAL III	Inga. Elvia Miriam Ruballos Samayoa
VOCAL IV	Br. Narda Lucía Pacay Barrientos
VOCAL V	Br. Walter Rafael Véliz Muñoz
SECRETARIA	Inga. Lesbia Magalí Herrera López

TRIBUNAL QUE PRACTICÓ EL EXAMEN GENERAL PRIVADO

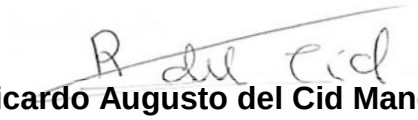
DECANO	Ing. Angel Roberto Sic García
EXAMINADOR	Ing. Julio Rolando Barrios Archila
EXAMINADOR	Ing. Julio César Solares Peñate
EXAMINADORA	Inga. Ingrid Salomé Rodríguez de Loukota
SECRETARIO	Ing. Hugo Humberto Rivera Pérez

HONORABLE TRIBUNAL EXAMINADOR

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

ANÁLISIS DE LA FACTIBILIDAD TÉCNICA Y ECONÓMICA DE LA MIGRACIÓN DE UNA RED METRO ETHERNET A PBB-TE

Tema que me fuera asignado por la Dirección de la Escuela de Ingeniería Mecánica Eléctrica, con fecha 26 de octubre de 2009.



Ricardo Augusto del Cid Mancio

Guatemala, 24 abril de 2013

Ingeniero Carlos Eduardo Guzmán Salazar.

Coordinador del Área de Electrónica.

Escuela de Ingeniería Mecánica Eléctrica.

Facultad de Ingeniería, USAC.

Estimado Ingeniero Guzmán.

Por medio de la presente, me permito informarle que he revisado completamente el trabajo de graduación titulado: "ANÁLISIS DE LA FACTIBILIDAD TÉCNICA Y ECONÓMICA DE LA MIGRACIÓN DE UNA RED METRO ETHERNET A PBB-TE", hecho por el alumno Ricardo Augusto del Cid Mancio, y he encontrado que dicho trabajo cumple con los objetivos propuestos en el anteproyecto de tesis.

Por lo tanto, el autor de este trabajo y yo, como su asesor, nos hacemos responsables por el contenido y las conclusiones del mismo.

Atentamente,

Ing. Enrique Edmundo Ruiz Carballo.

Asesor Nombrado.

Colegiado 2225

Enrique E. Ruiz C.
INGENIERO ELECTRICISTA
COL No 2225

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

Ref. EIME 31. 2015
Guatemala, 9 de MARZO 2015.

Señor Director
Ing. Guillermo Antonio Puente Romero
Escuela de Ingenierìa Mecànica Elèctrica
Facultad de Ingenierìa, USAC.

Señor Director:

Me permito dar aprobación al trabajo de Graduación titulado: ANÁLISIS DE LA FACTIBILIDAD TÉCNICA Y ECONÓMICA DE LA MIGRACIÓN DE UNA RED METRO ETHERNET A PBB-TE, del estudiante Ricardo Augusto del Cid Mancio, que cumple con los requisitos establecidos para tal fin.

Sin otro particular, aprovecho la oportunidad para saludarle.

Atentamente,
ID Y ENSEÑAD A TODOS

Ing. Carlos Eduardo Guzmán Salazar
Coordinador Area Electrónica

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

sro

UNIVERSIDAD DE SAN CARLOS
DE GUATEMALA

FACULTAD DE INGENIERIA

REF. EIME 31. 2015.

El Director de la Escuela de Ingeniería Mecánica Eléctrica, después de conocer el dictamen del Asesor, con el Visto Bueno del Coordinador de Área, al trabajo de Graduación del estudiante; RICARDO AUGUSTO DEL CID MANCIO titulado: ANÁLISIS DE LA FACTIBILIDAD TÉCNICA Y ECONÓMICA DE LA MIGRACIÓN DE UNA RED METRO ETHERNET A PBB-TE, procede a la autorización del mismo.

Ing. Guillermo Antonio Puente Romero

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

GUATEMALA, 16 DE JUNIO 2,015.

Universidad de San Carlos
De Guatemala

Facultad de Ingeniería
Decanato

Ref. DTG.D.359-2015

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: **ANÁLISIS DE LA FACTIBILIDAD TÉCNICA Y ECONÓMICA DE LA MIGRACIÓN DE UNA RED METRO ETHERNET A PBB-TE,** presentado por el estudiante universitario: **Ricardo Augusto del Cid Mancio,** y después de haber culminado las revisiones previas bajo la responsabilidad de las instancias correspondientes, se autoriza la impresión del mismo.

IMPRÍMASE.

Ing. Pedro Antonio Aguilar Polanco
Decano

UNIVERSIDAD DE SAN CARLOS DE GUATEMALA
DECANO
FACULTAD DE INGENIERIA

Guatemala, julio de 2015

/cc

ACTO QUE DEDICO A:

Mis padres	Angel Augusto del Cid Fernández y Juana de Arco Mancio Pimentel, quienes han sido apoyo e inspiración a lo largo de mi vida.
Mis amigos	Especialmente a mis buenos amigos Mario y Kelvin Silvestre, compañeros de estudios y de proyectos.
Mis catedráticos	En especial al Ingeniero Enrique Ruiz, que ha sido fuente de inspiración en la finalización de la carrera.

AGRADECIMIENTOS A:

Mi madre	Por darme su confianza y apoyo, que a lo largo de mi vida me ha demostrado su amor, ha corregido mis faltas y celebrado mis triunfos.
Mi padre	Por su ejemplo de perseverancia y constancia, por su apoyo para salir adelante.
Mi familia	Por ser una fuente de apoyo incondicional.
Mis amigos	Por agregarse a mi vida a lo largo de mi formación académica, con los cuales compartí triunfos y fracasos, alegrías y tristezas.
Universidad de San Carlos De Guatemala	Por ser Alma Mater de la ciencia y la tecnología.
Ing. Enrique Edmundo Ruiz Carballo	Por su orientación, esfuerzo y dedicación.

ÍNDICE GENERAL

ÍNDICE DE ILUSTRACIONES

FIGURAS

TABLAS

LISTA DE SÍMBOLOS

Símbolo	Significado
Q	Cantidad
$	Dólar
%	Porcentaje

GLOSARIO

ASBR Siglas en inglés *Autonomous System Border Router*, en español Routers Fronterizos del AS (Sistema Autónomo) o ASBRs, son *routers* que permiten encaminar paquetes fuera del AS en que se alojen, es decir, a otras redes conectadas al sistema autónomo o resto de internet (*external routing*).

ASIC Siglas en inglés de circuito integrado para aplicaciones específicas (*application specific integrated circuit*) es un circuito integrado hecho a la medida para un uso en particular, en vez de ser concebido para propósitos de uso general.

ATM Siglas en inglés de modo de transferencia asíncrona (*asynchronous transfer mode*). Tecnología de telecomunicación en el que, a fin de aprovechar al máximo la capacidad de los sistemas de transmisión, sean estos cableados o radioeléctricos, la información no es transmitida y conmutada a través de canales asignados en permanencia, sino en forma de cortos paquetes (celdas ATM) de longitud constante y que pueden ser enrutadas individualmente.

B-DA Siglas en inglés de dirección de *backbone* de destino (*backbone destination address*), representa la dirección del Edge Switch de destino de la red PBB.

B-SA Siglas en inglés de dirección de *backbone* de origen (*backbone source address*), representa la dirección MAC del Edge Switch de origen en la red PBB.

B-VID *Backbone* VLAN ID: representa la VLAN ID aplicado al cuadro y es usado para asegurar que los cuadros tomen la ruta apropiada, este campo es opcional.

BGP Siglas en inglés de protocolo de acceso de borde (*border gateway Protocol*) o frontera. Protocolo mediante el cual se intercambia información de encaminamiento entre sistemps autónomos. Por ejemplo, los ISP registrados en Internet suelen componerse de varios sistemas autónomos y para este caso es necesario un protocolo como BGP.

Bit Acrónimo en inglés de *binary digit*, en español dígito binario. Un bit es un dígito del sistema de numeración binario, puede representar uno de esos dos valores, 0 o 1.

Byte Término en inglés que designa una secuencia de 8 bits contiguos. Se usa comúnmente como unidad básica de almacenamiento de datos en combinación con los prefijos de cantidad.

C-DA	Dirección de destino de cliente en una trama PBB (client – *destination address*).
C-SA	Dirección de origen de cliente en la trama de datos del estándar PBB. Siglas en inglés de *customer – source address.*
C-VLAN	Customer-VLANs en inglés, son las VLANs internas de cliente en una red PB.
Campus Network	Red de computadoras hecha a base de la interconexión de redes de área local (LANs) dentro de un área geográfica limitada. Los elementos de red (conmutadores, enrutadores) y los medios de transmisión (fibra óptica, cobre, entre otros.), son por lo general propiedad de la universidad.
Capa 3	También llamada nivel de red o capa de red, según la normalización OSI, es un nivel o capa que proporciona conectividad y selección de ruta entre dos sistemas de hosts que pueden estar ubicados en redes geográficamente distintas. Es el tercer nivel del modelo OSI y su misión es conseguir que los datos lleguen desde el origen al destino aunque no tengan conexión directa.
Carrier Ethernet	Término de mercadeo utilizado para designar a las extensiones de Ethernet que permiten a los proveedores de servicios de telecomunicaciones

	(carriers, tal como se les llama en USA), proveer servicios Ethernet a sus clientes y usar tecnología Ethernet en sus redes.
CBR	*Constraint-based routing*: es un *router* corriendo CSPF.
CCM	Siglas en inglés de mensajes de verificación de continuidad (*continuity check message*), mensaje enviado para mantener una conexión abierta, también llamados "*keep alive".*
CE-VLAN CoS (802.1p)	Definido por MEF como la clase de servicio que utiliza 802.1q para etiquetar las tramas, cuando se utiliza, se pueden indicar hasta 8 clases de servicio. El proveedor de servicio especifica el ancho de banda y los parámetros de desempeño
Ciena	Compañía proveedora de equipos de telecomunicaciones basada en Estados Unidos.
CIR	Siglas en inglés de tasa de información comprometida (*committed information rate*), es la cantidad promedio de información que se ha transmitido, teniendo en cuenta los retardos, pérdidas, entre otros.
Cisco Systems	Es una empresa multinacional con sede en San José, (California), principalmente dedicada a la

	fabricación, venta, mantenimiento y consultoría de equipos de telecomunicaciones.
CLI	Interfaz de línea de comandos, por su acrónimo en inglés de *command line interface* (CLI), es un método que permite a las personas dar instrucciones a algún programa informático, por medio de una línea de texto simple.
Coaxial (cable)	Cable utilizado para transportar señales eléctricas de alta frecuencia que posee dos conductores concéntricos, uno central, llamado vivo, encargado de llevar la información, y uno exterior, de aspecto tubular, llamado malla o blindaje, que sirve como referencia de tierra y retorno de las corrientes. Entre ambos se encuentra una capa aislante llamada dieléctrico, de cuyas características dependerá principalmente la calidad del cable. Todo el conjunto suele estar protegido por una cubierta aislante.
Conmutación de etiquetas	En inglés *label switching*. Técnica de red donde la conmutación ocurre en la capa de enlace de datos en vez de en la tradicional capa de red. A cada paquete se le asigna un número de etiqueta y la conmutación sucede luego de examinar la etiqueta asignada a cada paquete. La conmutación es más rápida que el enrutamiento IP. La conmutación de etiquetas es muy usada en MPLS.

Core	Término en inglés que significa “núcleo”. Se refiere al corazón de una red, nodo donde se encuentran los dispositivos principales.
Cortafuegos	También llamado FW (*firewall*) - Dispositivo o conjunto de dispositivos configurados para permitir, limitar, cifrar, descifrar, el tráfico entre los diferentes ámbitos sobre la base de un conjunto de reglas. Pueden ser implementados en hardware o software, o una combinación de ambos.
CSMA/CD	*carrier sense multiple access with collision detection* siglas en inglés de acceso múltiple con escucha de portadora y detección de colisiones, es un protocolo de acceso al medio compartido. Su uso está especialmente extendido en redes Ethernet. En CSMA/CD, los dispositivos de red escuchan el medio antes de transmitir, es decir, es necesario determinar si el canal y sus recursos se encuentran disponibles para realizar una transmisión.
CSPF	Siglas en inglés de Constrained Shortest Path First – Camino Estrecho Más Corto, es una extensión de los algoritmos de camino más corto (*shortest path*). La ruta o camino calculado con CSPF es el camino más corto que cumple con una serie de restricciones, como puede ser por ejemplo un ancho de banda mínimo requerido, retraso de la señal de punto a punto, número de saltos, entre otros.

DiffServ Servicios diferenciados (DiffServ) son métodos que intentan garantizar la calidad de servicio en redes de gran tamaño, tales como internet. Servicios diferenciados analiza varios flujos de datos en vez de conexiones únicas o reservas de recursos. Esto significa que una negociación será hecha para todos los paquetes que envía una organización. Los contratos resultantes de esas negociaciones son llamados acuerdos de nivel de servicio (SLA), e inevitablemente implican un intercambio oneroso. Estos SLA especifican qué clases de tráfico serán provistos, qué garantías se dan para cada clase y cuántos datos se consideran para cada clase.

DMM *Delay measurement message*, por sus siglas en inglés – mensajes de medición del retardo, son mensajes generados como parte del servicio de CFM y que sirven para medir el retraso de la señal en el canal.

DMR *Delay measurement replay*, por sus siglas en inglés, en CFM, cuando un equipo recibe un DMM, responde con una "respuesta de medición de retardo" o DMR. Los mensajes DMR llevan las etiquetas de tiempo DMM originales en sus propias etiquetas de tiempo.

DTE Siglas en inglés de *data terminal equipment* equipo terminal de datos, es aquel componente de un

	circuito de datos que hace de fuente o destino de la información. Puede ser un terminal, una impresora o también una computadora.
E-LAN	Servicio LAN que proporciona conectividad multipunto a multipunto. Conecta dos o más interfaces UNI (*user network interface*). Los datos enviados desde un UNI llegarán a 1 o más UNI destino. Cada uno de ellos está conectado a un EVC multipunto. Desde el punto de vista del usuario, la E-LAN se comporta como una LAN.
E-Line	Servicio que proporciona un EVC punto a punto entre dos interfaces UNI (*user network interface*). Se utiliza para proporcionar una conexión Ethernet punto a punto.
E-NNI	Siglas en inglés de *external network to network* interface - Interface que sirve como conexión física entre las redes *Carrier Ethernet* de dos operadores donde cada red *Carrier Ethernet* esta bajo el control de una autoridad diferente.
eBGP	Siglas en inglés de “extermal BGP” - BGP externo, es un protocolo usado para el intercambio de información entre sistemas autónomos (ASs).
EIR	Siglas en inglés de *excess information rate* – tasa de información en exceso, especifica la cantidad de

	información mayor o igual que el CIR, hasta el cual las tramas son transmitidas sin pérdidas.
EoMPLS	Siglas en inglés de Ethernet sobre MPLS, es una tecnología que encapsula los cuadros Ethernet en paquetes MPLS y los envía a través de la red MPLS. Cada cuadro es transportado como un único paquete, y los *routers* PE ponen y quitan etiquetas para la encapsulación de paquetes.
Ether type (1)	Campo en la trama que indica que una VLAN de *backbone* está presente en el cuadro PBB y tiene el valor de 0x88A8.
Ether type (2)	Campo en la trama que indica que contenido de la carga o *payload*. En este caso, 0x88E7 indica una carga Ethernet precedida por un I-Tag.
Etiquetas apiladas (*Stacked tags*)	MPLS funciona anexando un encabezado a cada paquete. Dicho encabezado contiene una o más "etiquetas", y al conjunto de etiquetas se le llama pila o "*stack*".
EVC	Siglas en inglés de Ethernet Virtual Circuit (*circuito ethernet virtual*) es la asociación entre una o más interfaces UNIs (*user network interface*). Es un tubo virtual que proporciona al usuario servicios extremo a extremo atravesando múltiples redes MEN (*metro ethernet network*).

EXP field	En MPLS en un campo de 3 bits que puede soportar 8 diferentes clases de servicio, puede llevar etiquetas DiffServ. El campo "EXP" fue luego renombrado como "*Traffic Class Field*".
Fast-forward Switching	Termino en inglés que significa conmutación de reenvío rápido, hace referencia a una técnica de conmutación que ofrece la latencia más baja enviando inmediatamente el paquete luego de recibir la dirección de destino. Debido a que no hace comprobación de errores, algunas veces paquetes con errores son reenviados.
FEC	Siglas en inglés de *forwarding equivalence class - Clase de envío equivalente*. En MPLS es el nombre que se le da al tráfico que se encamina bajo una etiqueta. Subconjunto de paquetes tratados del mismo modo por el conmutador.
Frame relay	Técnica de comunicación mediante retransmisión de tramas para redes de circuito virtual, introducida por la ITU-T a partir de la recomendación I.122 de 1988. Consiste en una forma simplificada de tecnología de conmutación de paquetes que transmite una variedad de tamaños de tramas o marcos (“*frames*”) para datos, perfecto para la transmisión de grandes cantidades de datos.

iBGP Siglas en inglés de “internal-BGP”, hacen referencia al intercambio de información dentro de un sistema autónomo.

IEEE Corresponde a las siglas de Institute of Electrical and Electronics Engineers, en español Instituto de Ingenieros Eléctricos y Electrónicos, una asociación técnico-profesional mundial dedicada a la estandarización, entre otras cosas. Formada por profesionales de las nuevas tecnologías, como ingenieros eléctricos, en electrónica, científicos de la computación, ingenieros en informática, ingenieros en biomédica, ingenieros en telecomunicación y en mecatrónica.

IEEE 802.1ad Estándar Ethernet conocido informalmente como IEEE 802.1QinQ y es una enmienda al estándar IEEE 802.1Q-1998. La técnica también es llamada "*Provider Bridging", "Stacked VLANs*" o simplemente QinQ. La especificación original 802.1Q permite que múltiples encabezados de VLAN sean insertados en un mismo cuadro, una cualidad esencial para implementar redes Metro Ethernet.

IEEE 802.1ag Estándar que define protocolos y prácticas para operación y mantenimiento de túneles en enlaces 802.1 y redes de área local (LANs). Es una enmienda al estándar IEEE 802.1Q-2005 y fue aprobado en 2007. También llamado CFM,

connectivity fault management, siglas en inglés de Administración de fallas de conectividad.

IEEE 802.1p Estándar que proporciona priorización de tráfico y filtrado multicast dinámico. Esencialmente, proporciona un mecanismo para implementar calidad de servicio (QoS) a nivel de MAC (Media access control). Existen 8 clases diferentes de servicios, expresados por medio de 3 bits del campo prioridad de usuario (user_priority) de la cabecera IEEE 802.1Q añadida a la trama, asignando a cada paquete un nivel de prioridad entre 0 y 7.

IEEE 802.1Qay-2009 Estándar aprobado por IEEE para adaptar la tecnología Ethernet a las redes "carrier". Siglas en inglés de PBB-TE: *Provider Backbone Bridge Traffic Engineering* – Puente Backbone de Proveedor con Ingeniería de Tráfico. Está basado en las etiquetas de VLAN escalonadas y en la encapsulación "Mac-in-Mac" definida en IEEE 802.1ah (*Provider Backbone Bridges* - PBB), pero difiere de PBB en que elimina la inundación (en inglés flooding), las tablas de ruteo creadas dinámicamente y el protocolo Spanning Tree. Comparado con PBB y sus predecesores, PBB-TE se comporta de una manera más predecible y su comportamiento puede ser controlado fácilmente por el operador de red, con el inconveniente de que requiere configuración para cada túnel a lo largo de la ruta. La operación,

	administración y mantenimiento está basada en IEEE 802.1ag.
IETF	Siglas en inglés de Internet *Engineering Task Force* - fuerza de tareas de Ingeniería de Internet. Organización internacional abierta de normalización, que tiene como objetivos el contribuir a la ingeniería de Internet, actuando en diversas áreas, como transporte, encaminamiento, seguridad. Fue creada en EE. UU. en 1986. La IETF es mundialmente conocida por ser la entidad que regula las propuestas y los estándares de Internet, conocidos como RFC.
IGP	Siglas en inglés de *interior gateway protocol* - protocolo de acceso interior. Se refiere a los protocolos usados dentro de un sistema autónomo. Un protocolo de pasarela externo determina si la red es accesible desde el sistema autónomo, y usa el IGP para resolver el encaminamiento dentro del propio sistema. Se dividen en dos tipos: "vector-distancia" y "estado del enlace".
Instance tag (I-Tag)	Etiqueta que es sistemáticamente aplicada a todo cuadro PBB y contiene parámetros de QoS así como el identificador de servicio de 24 bits (SID) usado para identificar de forma única a los clientes.

IPsec Siglas en inglés de *internet protocol security* - protocolo de seguridad de internet. Conjunto de protocolos cuya función es asegurar las comunicaciones sobre el Protocolo de Internet (IP) autenticando y/o cifrando cada paquete IP en un flujo de datos. IPsec también incluye protocolos para el establecimiento de claves de cifrado.

IPX Siglas en inglés de *internetwork packet exchange*, en español "intercambio de paquetes interred", es un protocolo de la capa de red de Netware. Se utiliza para transferir datos entre el servidor y los programas de las estaciones de trabajo. Los datos se transmiten en datagramas.

I-SID Siglas en inglés de *Instance Service Identifier*, en español Identificador de Instancias de Servicio, campo en el protocolo PBB con una longitud de 24 bits, es único por cada cliente lo cual permite diferenciar los flujos de tráfico.

I-Tag Campo añadido al paquete por el protocolo PBB, el cual permite al carrier asignar parámetros QoS y define un identificador único por cliente (I-SID).

IS-IS Siglas en inglés de Intermediate System to Intermediate System, en español Sistema Intermedio a Sistema Intermedio. Protocolo de estado enlace, o SPF (*Shortest Path First*), por lo cual, básicamente

	maneja una especie de mapa que se fabrica a medida que converge la red. Es también un protocolo de acceso interior (IGP). Definido por el RFC 1142.
ISP	Siglas en inglés de internet *service provider*, en español proveedor de servicio de internet, es una empresa que brinda conexión a internet a sus clientes.
L2VPN	VPN de capa 2, provee conectividad de punto a punto en Capa 2, lo cual implica no que es necesario el enrutamiento (no intervienen protocolos de capa 3).
LAN	Una red de área local, red local o LAN (del inglés *local area network*) es la interconexión de una o varias computadoras y periféricos. Su extensión está limitada físicamente a un edificio o a un entorno de 200 metros, con repetidores podría llegar a la distancia de un campo de 1 kilómetro. Su aplicación más extendida es la interconexión de computadoras personales y estaciones de trabajo en oficinas, fábricas, entre otros.
LDP	Siglas en inglés de *Label Distribution Protocol*, en español protocolo de distribución de etiquetas. Protocolo mediante el cual un LSR comunica a otros LSRs asignaciones de etiquetas, utilizadas para

enviar tráfico entre ellos. Por medio de este protocolo los LSRs crean caminos de conmutación de etiquetas LSP a través de una red.

LER Siglas en inglés de *label edge router*, en español conmutador frontera de etiquetas. En MPLS es el elemento que inicia o termina el túnel (pone y quita cabeceras). Es decir, el elemento de entrada/salida a la red MPLS. Un *router* de entrada se conoce como "*ingress router*" y uno de salida como "*egress router*". Ambos se suelen denominar *edge label switch router,* ya que se encuentran en los extremos de la red MPLS.

Level Significa “etiqueta” en inglés.

Loopback El término en inglés “*loopback*” designa una interfaz de red virtual. Las direcciones del rango 127.0.0.0/8 son direcciones de *loopback*, de la cual la que se utiliza de forma mayoritaria es la 127.0.0.1 por ser la primera de dicho rango. Esta dirección se suele utilizar cuando una transmisión de datos tiene como destino el propio *host.* También en tareas de diagnóstico de conectividad y validez del protocolo de comunicación.

LSP Siglas en inglés de *label-switched path*, en español camino conmutado de etiquetas. Compuesto por uno o más LSRs dentro de un nivel jerárquico por el que

	un paquete, que pertenece a un determinado FEC, circula en una red MPLS.
LSR	Siglas en inglés de *label switching router*, en español enrutador conmutador de etiquetas. Equipo que realiza el envío de paquetes basándose en la información de la etiqueta del paquete recibido en una red MPLS.
MA	Siglas en inglés de *maintenance association*, en español asociación de mantenimiento.
mBGP	Multicast BGP
MEP	Siglas en inglés de *maintenance end point*, en español punto final de mantenimiento - es un punto en el borde de un dominio, el cual define el límite del dominio. Un MEP envía y recibe cuadros CFM.
MD	Siglas en inglés de *maintenance domain* en español dominio de mantenimiento, es un espacio administrado en una red, típicamente administrado por una sola entidad. Estos son configurados con nombres y etiquetas, las cuales van del 0 al 7. Existe una relación jerárquica entre los dominios basados en etiquetas. Mientras más grande el dominio, más grande la etiqueta.

MEF	Siglas en inglés de Metro Ethernet Forum, es una organización internacional sin fines de lucro fundada en 2001, dedicada a promover la adopción internacional de tecnologías Carrier Ethernet y servicios.
MIP	Siglas en inglés de *Maintenance Intermediate Points*, en español puntos intermedios de mantenimiento, son puntos internos a un dominio, no en el límite. Los cuadros CFM recibidos desde los MEPs y otros MIPs son catalogados y reenviados en este punto, todos los cuadros CFM en un nivel más bajo son descartados. Los MIPs son puntos pasivos que responden solo cuando son disparados por "*trace routes*" CFM y mensajes *loop-back*.
Modelo de servicios Integrados del IETF	Los servicios integrados o Intserv constituyen una arquitectura cuyo cometido es gestionar los recursos necesarios para garantizar calidad de servicio (QoS) en una red de computadores. El concepto que los servicios integrados proponen para cumplir con su cometido, requiere de una nueva arquitectura de protocolos que es difícilmente escalable. Esto se debe a que funciona realizando una reserva extremo a extremo de recursos en los elementos que conforman la red a nivel de aplicación.

MPLS	Siglas en inglés de *multiprotocol label switching,* en español conmutación de etiquetas multiprotocolo. Mecanismo de transporte de datos estándar creado por la IETF y definido en el RFC 3031. Opera entre la capa de enlace de datos y la capa de red del modelo OSI. Fue diseñado para unificar el servicio de transporte de datos para las redes basadas en circuitos y las basadas en paquetes. Puede ser utilizado para transportar diferentes tipos de tráfico, incluyendo tráfico de voz y de paquetes IP.
MSTP	Siglas en inglés de Multiple Spanning Tree Protocol, Protocolo de Espaneo Múltiple, fue definido originalmente en IEEE 802.1s y luego por IEEE 802.1Q-2005, define una extensión a RSTP para avanzar el desarrollo de VLANs. Este protocolo configura un "*spanning tree*" para cada grupo de VLANs y bloquea todas menos una de las posibles rutas dentro de cada *Spanning Tree.*
NNI	Siglas en inglés de *Network-to-Network Interface*, en español Interface red-a-red. Interface que especifica funciones de señalización entre dos redes, las cuales puedes IP, ATM o SS7.
OAM	Siglas en inglés para operación, administración y mantenimiento (operation, administration & maintenance).

OSPF	Siglas en inglés para *Open Shortest Path First,* en español camino más corto primero. Protocolo de enrutamiento jerárquico de pasarela interior o IGP *(Interior Gateway Protocol),* que usa el algoritmo Dijkstra enlace-estado (LSA - *Link State Algorithm*) para calcular la ruta más corta posible. Usa "costo" como su medida de métrica. Además, construye una base de datos enlace-estado (Link-State Data Base, LSDB), idéntica en todos los enrutadores de la zona.
PB	Siglas en inglés de *Provider Bridging*, ver IEEE 802.1ad.
PBCB	Siglas en inglés de PB *Core Bridge.*
PBEB	Siglas en inglés de PB *Edge Bridge.*
PCP	Código de puntos de prioridad, por sus siglas en inglés (*Priority Code Point*). Tabla usada en IEEE 802.1ad *Provider Bridge* para determinar descarte de paquetes.
PIR	Siglas en inglés de *peak Iinformation rate*, en español tasa de información pico, es una tasa fijada en enrutadores y conmutadores que permite una cantidad máxima de información de salida.
Policy map	En inglés mapa de políticas.

Pseudowire En una red de computadoras y telecomunicaciones, un *pseudowire* (también escrito pseudo-wire) es una emulación de una conexión punto a punto sobre una red de conmutación de paquetes, tal como una red MPLS.

PVC Siglas en inglés de *permanent virtual circuit* - circuito virtual permanente. Un circuito virtual permanente es establecido para uso repetido por parte de los mismos equipos de transmisión. Los circuitos permanentes eliminan la necesidad de configuración y terminación repetitivas para cada conexión. Es decir se puede usar sin tener que pasar por la fase de establecimiento ni liberación de las conexiones.

Q-in-Q Ver IEEE 802.1ad.

QoS Siglas en inglés para *quality of service*, en español calidad de servicio. Tecnologías que garantizan la transmisión de cierta cantidad de información en un tiempo dado (*throughput*). Calidad de servicio es la capacidad de dar un buen servicio. Es especialmente importante para ciertas aplicaciones tales como la transmisión de vídeo o voz.

RIP Siglas en inglés de *routing information protocol* (Protocolo de información de enrutamiento). Es un protocolo de puerta de enlace interna o IGP (*Internal Gateway Protocol*) utilizado por los enrutadores,

	aunque también pueden actuar en equipos, para intercambiar información acerca de redes IP.
RSVP	Siglas en inglés de *Resource Reservation Protocol*, en español Protocolo de Reserva de Recursos. Descrito en RFC 2205, es un protocolo de la capa de transporte diseñado para reservar recursos de una red bajo la arquitectura de Servicios Integrados (IntServ).
S-Tag	Source-Tag, etiqueta de origen en inglés. En el protocolo PBB, es una etiqueta que se pone a los paquetes que identifica el origen de estos.
S-VLAN	VLANs de servicio (*service* en inglés). En el protocolo IEEE 802.1ad es posible configurar hasta 4096 S-VLANs, cada una con capacidad de usar hasta 4096 clientes de forma separada.
SFP	Siglas en inglés de *small form-factor pluggable* (insertable de factor de forma pequeño) es un dispositivo insertable compacto, diseñado para aplicaciones de comunicaciones. Sirve de interface entre una tarjeta madre a una fibra óptica o cable de cobre.
Single domain	Término en inglés que describe una red de dominio único, la cual consiste de un dominio maestro o de administración y un cierto número de terminales o computadoras clientes que están sujetas a esta.

SPB Siglas en inglés de *shortest path bridging*, en español puenteo de camino más corto (802.1aq): este es el reemplazo para los antiguos protocolos Spanning Tree (IEEE 802.1D STP, IEEE 802.1w RSTP, IEEE 802.1s MSTP) que bloquean el tráfico en todas las rutas menos una. IEEE 802.1aq permite que todas las rutas en una red estén activas con rutas múltiples de igual valor, lo cual provee más topologías de capa 2 (hasta 16 millones comparadas con 4096 VLANs), tiempos de convergencia más rápidos, y mejora el uso de las topologías de conectividad completa y provee redundancia entre todos los dispositivos, lo cual permite también balancear el tráfico entre todas las rutas posibles de la red. Usa protocolos de estado del enlace para enviar información topológica.

STP Siglas en inglés de Spanning Tree Protocol, en español protocolo de espaneo en árbol, es un protocolo de red de nivel 2 de la capa OSI. Su función es la de gestionar la presencia de bucles en topologías de red debido a la existencia de enlaces redundantes (necesarios en muchos casos para garantizar la disponibilidad de las conexiones). El protocolo permite a los dispositivos de interconexión activar o desactivar automáticamente los enlaces de conexión, de forma que se garantice que la topología está libre de bucles, de forma transparente a las estaciones de usuario.

Topología	La topología (de red) se define como la cadena de comunicación usada por los computadores que conforman una red para intercambiar datos.
ToS	Siglas en inglés de *type of service*, en español, tipo de servicio. Campo en el encabezado de IPv4, puede especificar la prioridad de un paquete.
Traffic engineering	Término en inglés que significa ingeniería de tráfico: en telecomunicaciones se refiere a diferentes funciones necesarias para planificar, diseñar, proyectar, dimensionar, desarrollar y supervisar redes de telecomunicaciones en condiciones óptimas de acuerdo con la demanda de servicios, márgenes de beneficios de la explotación, calidad de la prestación y entorno regulatorio y comercial.
UNI	Siglas en inglés de *user network interface*, en español, interface de usuario de red, es la interfaz estándar Ethernet y el punto de demarcación entre el equipo cliente y el proveedor de servicio MEN, pudiéndolo definir también como un camino virtual que proporciona al usuario servicios extremo a extremo, atravesando múltiples redes MEN (*Metro Ethernet Network*).
VC	Siglas en inglés de virtual channel, en español canal virtual, es una canal diferente del canal de radio en donde viaja la señal.

VID	Siglas en inglés de VLAN ID, en español Identificador de VLAN, campo usado en la trama PB/PBB/PBB-TE para identificar una VLAN.
VPWS	Siglas en inglés de *Virtual private Wire Service*, en español Servicio Cableado Virtual Privado, es una red privada virtual que provee conectividad punto a punto a través de pseudowires sobre una red IP.
VPLS	Siglas en inglés de *virtual private LAN Service*, en español es una red privada virtual (VPN). En contraste con L2TPv3, que sólo permite la capa de punto a punto dos túneles, VPLS permite a cualquier tipo de conectividad (multipunto).
VPN	Siglas en inglés de *virtual private network*, en español red privada virtual., es una tecnología de red que permite una extensión de la red local sobre una red pública o no controlada.
WAN	Siglas en inglés de *wide area network*, en español red de área amplia, es un tipo de red de computadoras capaz de cubrir distancias desde unos 100 hasta unos 1000 km, proveyendo de servicio a un país o un continente. Un ejemplo de este tipo de redes sería Internet o cualquier red en la cual no estén en un mismo edificio todos sus miembros (sobre la distancia hay discusión posible).

RESUMEN

En el presente trabajo de graduación se investigan las características y funcionalidades de dos áreas de la tecnología Carrier Ethernet:

- Ethernet over MPLS (EoMPLS) del IETF, tal como lo implementan los equipos Cisco.

- *Provider Backbone Bridges* (PBB)/Provider Backbone Bridges Traffic Engineering (PBB-TE) del IEEE, tal como lo implementan los equipos Ciena.

Para ellos, se hicieron pruebas usando la infraestructura de producción de la empresa “Tierra Media”, (se han cambiado los nombres por razones de confidencialidad) que cuenta con presencia en los 5 países de Centro América, y se creó una red de pruebas CORE (núcleo), usando switches Ciena 5305 configurados para soportar PBB-TE. Dichas pruebas se describen en 7 capítulos, de los cuales se da un resumen a continuación.

En el primer capìtulo se presentan los fundamentos de la tecnología Ethernet, base de las redes LAN modernas, y se explica cuáles son sus necesidades de crecimiento.

En el segundo capítulo se presentan los fundamentos de las tecnologías MPLS y Ethernet over MPLS, ambas de uso ampliamente extendido en la actualidad.

En el tercer capítulo se presentan los fundamentos de las tecnologías Provider Backbone Bridging y sus variantes con Ingeniería de Tráfico, las cuales compiten con MPLS para el establecimiento de túneles sobre Ethernet.

En el cuarto capítulo se describe la red MPLS existente, y su adaptación para soportar túneles Ethernet over MPLS, los cuales fueron creados mediante pseudo-wires, con el propósito de transportar VLANs en Capa 3.

En el quinto capítulo se describe la construcción de una red PBB, mediante equipos Ciena, y cómo establecer túneles PBB mediante dicha tecnología, usando línea de comandos.

En el sexto capítulo se describe el despliegue de una red PBB-TE, la configuración de la ingeniería de tráfico, cómo se logró separar los espacios de direcciones IP del cliente y del proveedor, así también cómo interoperar con EoMPLS y PBB.

En el séptimo capítulo se hace un análisis de las características técnicas de cada tecnología, seguido por un análisis de la factibilidad económica de migrar a la tecnología PBB-TE.

OBJETIVOS

General

Realizar el análisis de la factibilidad técnica y económica de la migración de una red metro Ethernet a la tecnología PBB-TE.

Específicos

1. Presentar los fundamentos de la tecnología Ethernet.

2. Presentar los fundamentos de las tecnologías MPLS y EoMPLS.

3. Presentar los fundamentos de las tecnologías Provider Backbone Bridge (PBB).

4. Adaptar una red MPLS en producción para soportar Ethernet sobre MPLS.

5. Construir una red con tecnología Provider Backbone Bridge, para establecer sobre ella túneles PBB.

6. Construir una red PBB con Ingeniería de Tráfico (PBB-TE), para interoperar las redes EoMPLS y PBB.

7. Realizar un análisis técnico y financiero de la factibilidad de migrar una red Metro Ethernet a PBB-TE.

INTRODUCCIÓN

El presente trabajo de graduación trata sobre la evaluación de tecnologías de transporte Carrier Ethernet, tales como *Provider Backbone Bridge y Ethernet* over MPLS, con el propósito de estudiar la factibilidad de la migración de una red metro Ethernet a alguna de dichas tecnologías.

Muchos proveedores y "*carriers*" consideran que las tecnologías Carrier Ethernet son muy prometedoras y son capaces de cambiar la industria de las telecomunicaciones. En vista de esto, se han instalado redes de prueba con equipos capaces de soportar las tecnologías PB/PBB-TE y se han usado redes ya existentes en la empresa Tierra media (se ha cambiado el nombre de la empresa por razones de confidencialidad) que soportan MPLS y EoMPLS con el propósito de comparar ambas tecnologías y estudiar la posibilidad de migración de la infraestructura existente a PB/PBB-TE.

1. FUNDAMENTOS DE LA TECNOLOGÍA ETHERNET

En el presente capítulo se describe brevemente la historia de las redes Ethernet, para abordar luego la formación de las tramas Ethernet y los tipos de arquitectura de red posibles.

En 1970, mientras Norman Abramson montaba la red ALOHA en Hawai, un estudiante recién graduado en el MIT llamado Robert Metcalfe se encontraba realizando sus estudios de doctorado en la Universidad de Harvard trabajando para ARPANET, que era el tema de investigación candente en aquellos días. En un viaje a Washington, Metcalfe estuvo en casa de Steve Crocker (el inventor de los RFCs de Internet) donde este lo dejó dormir en el sofá. Para poder conciliar el sueño Metcalfe empezó a leer una revista científica donde encontró un artículo de Norman Abramson acerca de la red Aloha. Metcalfe pensó cómo se podía mejorar el protocolo utilizado por Abramson, y escribió un artículo describiendo un protocolo que mejoraba sustancialmente el rendimiento de Aloha.

Ese artículo se convertiría en su tesis doctoral, que presentó en 1973. La idea básica era muy simple: las estaciones antes de transmitir deberían detectar si el canal ya estaba en uso (es decir si ya había 'portadora'), en cuyo caso esperarían a que la estación activa terminara. Además, cada estación mientras transmitiera estaría continuamente vigilando el medio físico por si se producía alguna colisión, en cuyo caso se pararía y retransmitiría más tarde. Este protocolo de control de acceso al medio recibiría más tarde la denominación acceso múltiple con detección de portadora y detección de colisiones, o más brevemente CSMA/CD (Carrier Sense Multiple Access / Collision Detection).

En 1972 Metcalf se mudó a California para trabajar en el Centro de Investigación de Xerox en Palo Alto llamado Xerox PARC (Palo Alto Research Center). Allí se estaba diseñando lo que se consideraba la 'oficina del futuro' y Metcalfe encontró un ambiente perfecto para desarrollar sus inquietudes. Se estaban probando unas computadoras denominadas Alto, que ya disponían de capacidades gráficas y ratón y fueron consideradas los primeros ordenadores personales. También se estaban fabricando las primeras impresoras láser. Se quería conectar las computadoras entre sí para compartir ficheros y las impresoras.

La comunicación tenía que ser de muy alta velocidad, del orden de megabits por segundo, ya que la cantidad de información a enviar a las impresoras era enorme (tenían una resolución y velocidad comparables a una impresora láser actual). Estas ideas que hoy parecen obvias eran completamente revolucionarias en 1973.

A Metcalfe, el especialista en comunicaciones del equipo con 27 años de edad, se le encomendó la tarea de diseñar y construir la red que uniera todo aquello. Contaba para ello con la ayuda de un estudiante de doctorado de Stanford llamado David Boggs. Las primeras experiencias de la red, que denominaron 'Alto Aloha Network', las llevaron a cabo en 1972. Fueron mejorando gradualmente el prototipo hasta que el 22 de mayo de 1973, Metcalfe escribió un memorándum interno en el que informaba de la nueva red.

Para evitar que se pudiera pensar que solo servía para conectar computadoras Alto cambió el nombre de la red por el de Ethernet, que hacía referencia a la teoría de la física hoy ya abandonada según la cual las ondas electromagnéticas viajaban por un fluido denominado éter que se suponía llenaba todo el espacio (para Metcalfe el 'éter' era el cable coaxial por el que iba

la señal). Las dos computadoras Alto utilizadas para las primeras pruebas de Ethernet fueron rebautizadas con los nombres Michelson iy Morley, en alusión a los dos físicos que demostraron en 1887 la inexistencia del éter mediante el famoso experimento que lleva su nombre.

La red de 1973 ya tenía todas las características esenciales de la Ethernet actual. Empleaba CSMA/CD para minimizar la probabilidad de colisión, y en caso de que esta se produjera se ponía en marcha un mecanismo denominado retroceso exponencial binario para reducir gradualmente la ‘agresividad’ del emisor, con lo que este se adaptaba a situaciones de muy diverso nivel de tráfico. Tenía topología de bus y funcionaba a 2,94 Mb/s sobre un segmento de cable coaxial de 1,6 km de longitud. Las direcciones eran de 8 bits y el CRC de las tramas de 16 bits. El protocolo utilizado al nivel de red era el PUP (Parc Universal Packet) que luego evolucionaría hasta convertirse en el que luego fue XNS (Xerox Network System), antecesor a su vez de IPX (Netware de Novell).

En vez de utilizar el cable coaxial de 75 ohms de las redes de televisión por cable se optó por emplear cable de 50 ohms que producía menos reflexiones de la señal, a las cuales Ethernet era muy sensible por transmitir la señal en banda base (es decir sin modulación). Cada empalme del cable y cada 'pincho' vampiro (*transceiver*) instalado producía la reflexión de una parte de la señal transmitida. En la práctica el número máximo de 'pinchos' vampiro, y por tanto el número máximo de estaciones en un segmento de cable coaxial, venía limitado por la máxima intensidad de señal reflejada tolerable.

En 1975, Metcalfe y Boggs describieron Ethernet en un artículo que enviaron a Communications of the ACM (Association for Computing Machinery), publicado en 1976. En él ya describían el uso de repetidores para aumentar el alcance de la red. En 1977 Metcalfe, Boggs y otros dos ingenieros de Xerox

recibieron una patente por la tecnología básica de Ethernet, y en 1978, Metcalfe y Boggs recibieron otra por el repetidor. En esta época todo el sistema Ethernet era propiedad de Xerox.

Conviene destacar que David Boggs construyó en 1975 durante su estancia en Xerox PARC el primer *router* y el primer servidor de nombres de la Internet.

La primera versión fue un intento de estandarizar Ethernet aunque hubo un campo de la cabecera que se definió de forma diferente, posteriormente ha habido ampliaciones sucesivas al estándar que cubrieron las ampliaciones de velocidad (Fast Ethernet, Gigabit Ethernet y el de 10 Gigabits), redes virtuales, hubs, conmutadores y distintos tipos de medios, tanto de fibra óptica como de cables de cobre (tanto par trenzado como coaxial).

Los estándares de este grupo no reflejan necesariamente lo que se usa en la práctica, aunque a diferencia de otros grupos este suele estar cerca de la realidad.

1.1. Formación de un cuadro Ethernet

La siguiente figura ilustra un ejemplo del camino que sigue la información desde la aplicación que la produce, a través de los distintos niveles o capas de cada protocolo.

Nota: este ejemplo es una simplificación de la realidad. Se han omitido muchos otros datos que forman parte de cada protocolo (controles de error, delimitadores, indicadores de longitud, entre otros.).

Estas son las etapas o capas:

- Capa aplicación: en este caso, el programa cliente, escribe la cadena de datos de salida.

- Capa de transporte: el protocolo TCP forma un paquete agregando el número de secuencia (Sequence), puerto de origen (S-PORT) y puerto de destino (D-PORT).

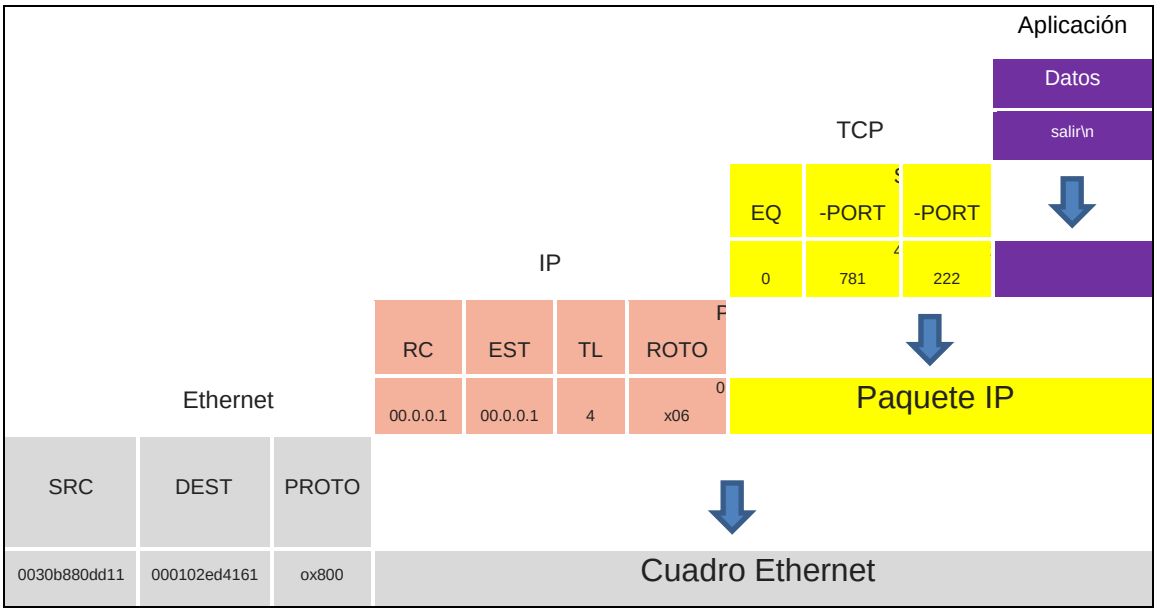
- Capa de red: el protocolo IP forma un paquete añadiendo la dirección IP origen (SRC), destino (DEST), el tiempo de vida del paquete (TTL) y un valor que identifica el protocolo del paquete encapsulado (0×06 en este caso, valor hexadecimal que representa al protocolo TCP).

- Capa de enlace: el protocolo Ethernet forma un cuadro *(frame*) agregando las direcciones Ethernet de origen (SRC: 00:30:b8:80:dd:11) y destino (DEST: 00:01:02:ed:41:61) en hexadecimal. Se añade además el identificador del tipo de protocolo del paquete contenido (el valor 0×800 corresponde al protocolo IP).

- Capa física: el cuadro formado es enviado a través del medio físico que vincula los hosts de la red local (típicamente, cable de par trenzado, UTP).

Como puede verse, tanto IP como Ethernet “encapsulan” a otros protocolos. Esto permite realizar distintas combinaciones, creando “túneles”, que se verán más adelante.

Figura 1. **Formación de un cuadro Ethernet**

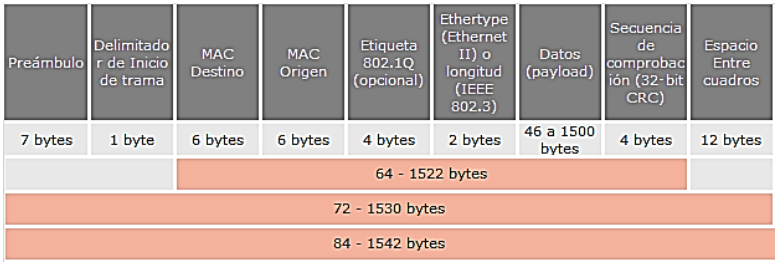


Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software.* p. 22.

1.2. Estructura del cuadro Ethernet 802.3

El cuadro Ethernet también es conocido con el nombre de “trama”.

Figura 2. **Estructura del cuadro 802.3 Ethernet**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 25.

- El primer campo es el preámbulo que indica el inicio de la trama y tienen el objeto de que el dispositivo que lo recibe detecte una nueva trama y se sincronice.
- El delimitador de inicio de trama indica que el cuadro empieza a partir de él.
- Los campos de MAC (o dirección) de destino y origen indican las direcciones físicas del dispositivo al que van dirigidos los datos y del dispositivo origen de los datos, respectivamente.
- La etiqueta es un campo opcional que indica la pertenencia a una VLAN o prioridad en IEEE 802.1Q.
- Ethernetype indica con qué protocolo están encapsulados los datos que contiene la "Payload", en caso de que se usase un protocolo de capa superior.
- La Payload es donde van todos los datos y, en el caso correspondiente, cabeceras de otros protocolos de capas superiores del Modelo OSI,que pudieran formatear a los datos que se tramiten (IP, TCP, etc). Tiene un mínimo de 46 bytes (o 42 si es la versión 802.1Q) hasta un máximo de 1 500 bytes.
- La secuencia de comprobación es un campo de 4 bytes que contiene un valor de verificación CRC (control de redundancia cíclica). El emisor calcula el CRC de toda la trama, desde el campo destino al campo CRC suponiendo que vale 0. El receptor lo recalcula, si el valor calculado es 0 la trama es válida.
- El espacio entre cuadros al final de trama son 12 bytes vacíos con el objetivo de espaciado entre tramas.

1.3. Tecnología y velocidad de Ethernet

Hace ya mucho tiempo que Ethernet consiguió situarse como el principal protocolo del nivel de enlace. Ethernet 10Base2 consiguió, ya en la década de los 90s, una gran aceptación en el sector. Hoy por hoy, 10Base2 se considera como una "tecnología de legado" respecto a 100BaseT. Hoy los fabricantes ya han desarrollado adaptadores capaces de trabajar tanto con la tecnología 10baseT como la 100BaseT y esto ayuda a una mejor adaptación y transición.

Las tecnologías Ethernet que existen se diferencian en estos conceptos:

- Velocidad de transmisión.
- Tipo de cable: tecnología del nivel físico.
- Longitud máxima que puede haber entre dos nodos adyacentes (sin estaciones repetidoras).
- Topología: determina la forma física de la red.

A continuación se especifican los anteriores conceptos en las tecnologías más importantes.

Tabla I. **Tecnologías Ethernet**

Tecnología	Velocidad	Tipo de Cable	Distancia Máxima	Topología
10Base2	10 Mbps	Coaxial	185 m	Bus (Conector T)
10BaseT	10 Mbps	Par Trenzado	100 m	Estrella (hub o switch)
10BaseF	10 Mbps	Fibra óptica	2 000 m	Estrella (hub o switch)
100BaseT4	100 Mbps	Par trenzado (cat 3UTP)	100 m	Estrella half y full
100BaseTX	100 Mbps	Par trenzado (cat 5UTP)	100 m	Estrella half y full
1 00BaseFX	100 Mbps	Fibra óptica	2 000 m	No permite hubs
1 000BaseT	1 000 Mbps	4 pares trenzados (5e o 6UTP)	100 m	Estrella full duplex
1 000BaseSX	1 000 Mbps	Fibra óptica multimodo	550 m	Estrella full duplex
1 000Base LX	1 000 Mbps	Fibra óptica monomodo	5 000 m	Estrella full duplex

Fuente: elaboración propia.

1.4. Hardware comúnmente usado en una red Ethernet

Los elementos de una red Ethernet son: tarjetas de red, repetidores *(repeaters*), concentradores (*hubs*), puentes (*bridges*), conmutadores *(switches),* enrutadores (*routers)*, los nodos de red y el medio de interconexión. Los nodos de red pueden clasificarse en dos grandes grupos: equipo terminal de datos (DTE) y equipo de comunicación de datos (DCE).

Los DTE son dispositivos de red que generan el destino de los datos: los PC, las estaciones de trabajo, los servidores de archivos, los servidores de impresión; todos son parte del grupo de las estaciones finales. Los DCE son los dispositivos de red intermediarios que reciben y retransmiten las tramas dentro

de la red; pueden ser: conmutadores, concentradores, repetidores o interfaces de comunicación. Por ejemplo: un módem o una tarjeta de red.

- NIC, o tarjeta de interfaz de red: permite que una computadora acceda a una red local. Cada tarjeta tiene una única dirección MAC que la identifica en la red. Una computadora conectada a una red se denomina nodo.

- Repetidor: aumenta el alcance de una conexión física, recibiendo las señales y retransmitiéndolas, para evitar su degradación, a través del medio de transmisión. Usualmente se usa para unir dos áreas locales de igual tecnología y solo tiene dos puertos. Opera en la capa física del modelo OSI.

- Concentrador o hub: funciona como un repetidor pero permite la interconexión de múltiples nodos. Su funcionamiento es relativamente simple pues recibe una trama de Ethernet, por uno de sus puertos, y la repite por todos sus puertos restantes sin ejecutar ningún proceso sobre las mismas. Opera en la capa física del modelo OSI.

- Puente o *bridge:* interconecta segmentos de red haciendo el cambio de frames (tramas) entre las redes de acuerdo con una tabla de direcciones que le dice en qué segmento está ubicada una dirección MAC dada. Se diseñan para uso entre LAN que usan protocolos idénticos en la capa física y MAC (de acceso al medio). Aunque existen bridges más sofisticados que permiten la conversión de formatos MAC diferentes (*Ethernet-Token Ring*, por ejemplo). Opera en la capa física del modelo OSI.

- Conmutador o *switch*: funciona como el *bridge*, pero permite la interconexión de múltiples segmentos de red, funciona en velocidades más rápidas y es más sofisticado. Los *switches* pueden tener otras funcionalidades, como redes virtuales, y permiten su configuración a través de la propia red. Por esto son capaces de procesar información de las tramas; su funcionalidad más importante es en las tablas de dirección. Por ejemplo, una computadora conectada al puerto 1 del conmutador envía una trama a otra computadora conectada al puerto 2; el *switch* recibe la trama y la transmite a todos sus puertos, excepto aquel por donde la recibió; la computadora 2 recibirá el mensaje y eventualmente lo responderá, generando tráfico en el sentido contrario; ahora el *switch* conocerá las direcciones MAC de las computadoras en los puertos 1 y 2; cuando reciba otra trama con dirección de destino de alguna de ellas, sólo transmitirá la trama a dicho puerto disminuyendo así el tráfico de la red y contribuyendo al buen funcionamiento de la misma. Opera en la capa física del modelo OSI.

1.5. Topologías de red Ethernet

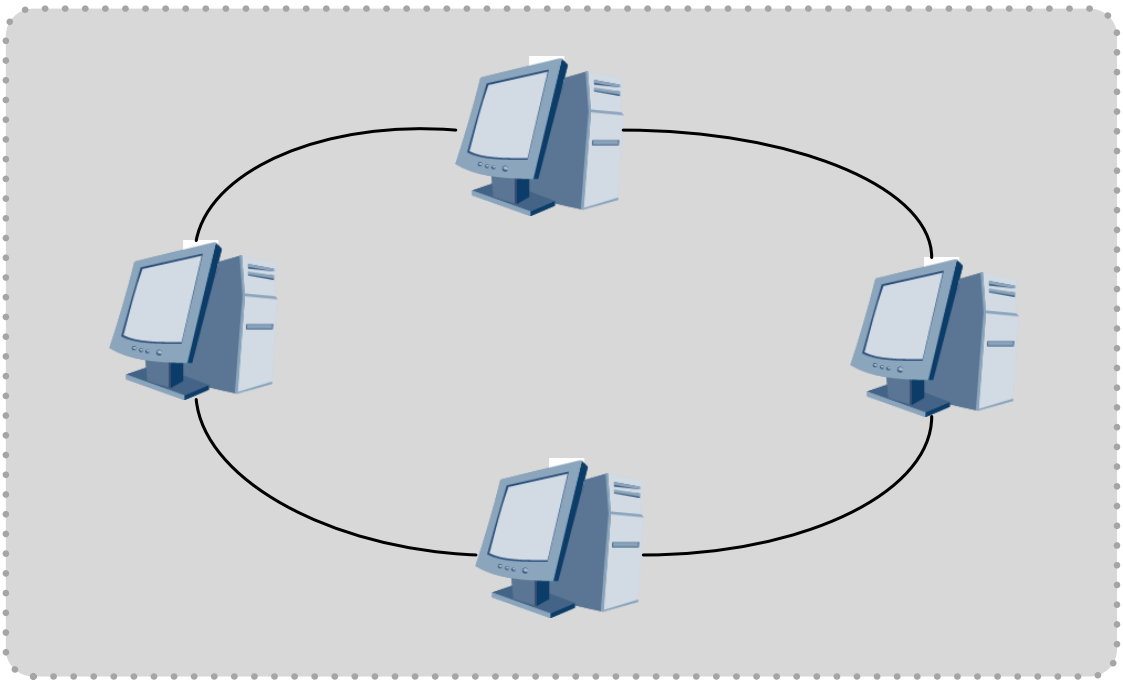
La topología de red es la disposición física en la que se conecta una red de ordenadores. Si una red tiene diversas topologías se la llama mixta.

1.5.1. Red en anillo

Topología de red en la que las estaciones se conectan formando un anillo. Cada estación está conectada a la siguiente y la última está conectada a la primera. En este tipo de red la comunicación se da por el paso de un *token*, de esta manera se evita pérdida de información debido a colisiones.

Cabe mencionar que si algún nodo de la red se cae (término informático para referirse a un mal funcionamiento) la comunicación en todo el anillo se pierde.

Figura 3. **Topología en anillo**

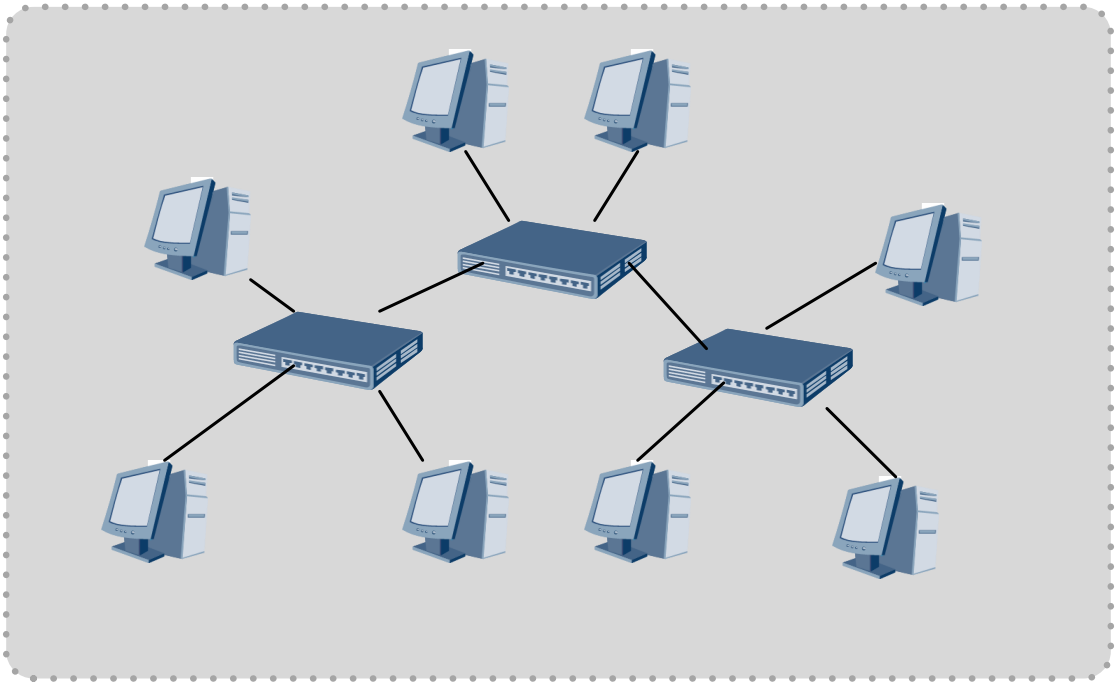


Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 30.

1.5.2. Red en árbol

Topología de red en la que los nodos están colocados en forma de árbol. Desde una visión topológica, la conexión en árbol es parecida a una serie de redes en estrella interconectadas. Es una variación de la red en bus, la falla de un nodo no implica interrupción en las comunicaciones. Se comparte el mismo canal de comunicaciones. Cuenta con un cable principal (*backbone*) al que hay conectadas redes individuales en bus.

Figura 4. **Topología en árbol**

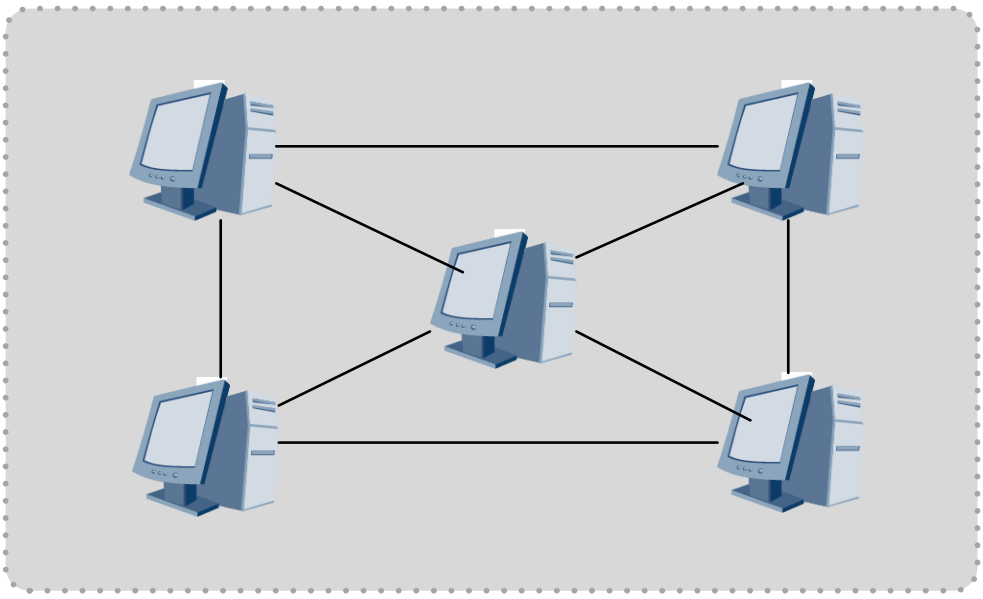


Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 37.

1.5.3. Red en malla

La red en malla es una topología de red en la que cada nodo está conectado a uno o más de los otros nodos. De esta manera es posible llevar los mensajes de un nodo a otro por diferentes caminos. Si la red de malla está completamente conectada no puede existir absolutamente ninguna interrupción en las comunicaciones. Cada servidor tiene sus propias conexiones con todos los demás servidores.

Figura 5. **Topología en malla completa**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 39.

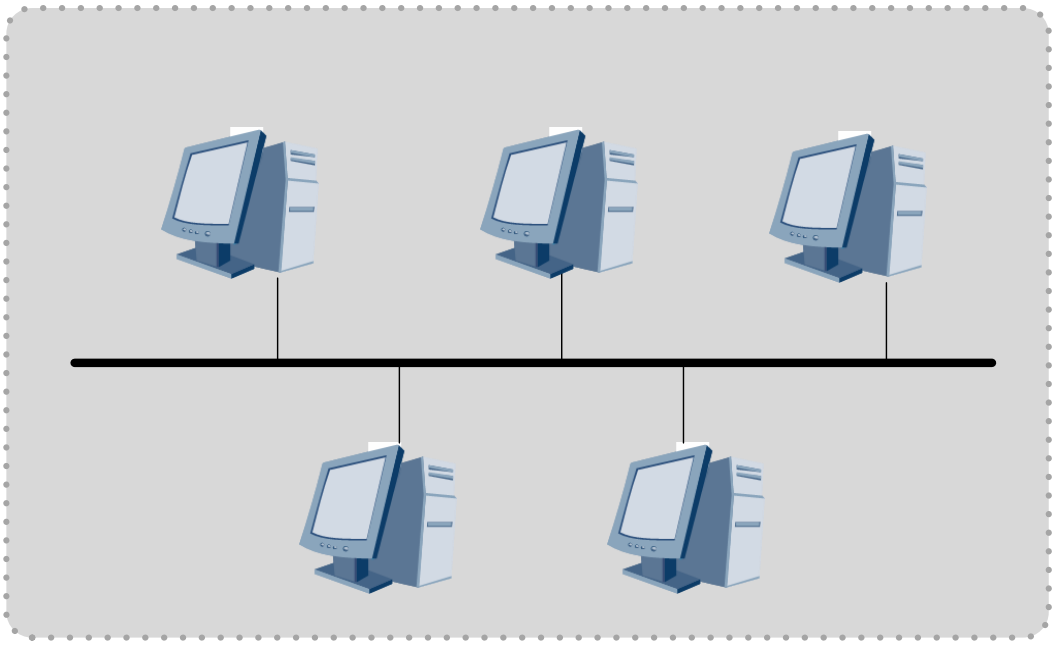
1.5.4. Red en bus

La topología de bus tiene todos sus nodos conectados directamente a un enlace y no tiene ninguna otra conexión entre nodos. Físicamente cada *host* está conectado a un cable común, por lo que se pueden comunicar directamente, aunque la ruptura del cable hace que los *hosts* queden desconectados.

La topología de bus permite que todos los dispositivos de la red puedan ver todas las señales de todos los demás dispositivos, lo que puede ser ventajoso si se desea que dichos dispositivos obtengan esta información. Sin embargo, puede representar una desventaja, ya que es común que se produzcan problemas de tráfico y colisiones, que se pueden paliar

segmentando la red en varias partes. Es la topología más común en pequeñas LAN, con un hub o un *switch* final en uno de los extremos. Ethernet 802.3 es un ejemplo de red en topología de bus, como ya hemos visto.

Figura 6. **Topología de bus**



Fuente: LOBO, Lancy. *MPLS Configuraion Cisco IOS Software*. p. 42.

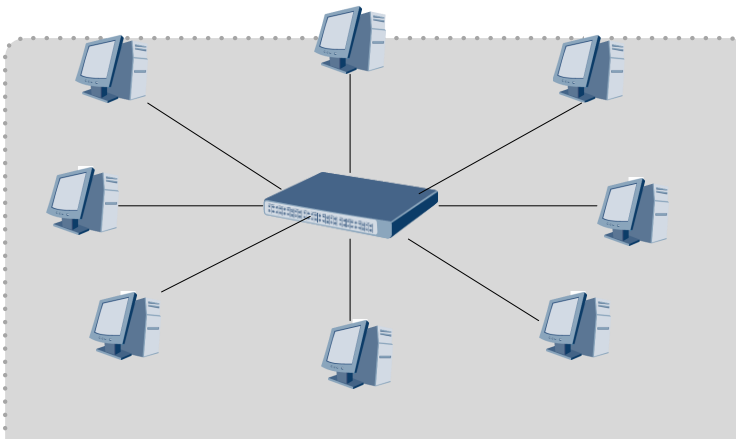
1.5.5. Red en estrella

Red en la cual las estaciones están conectadas directamente al servidor u ordenador y todas las comunicaciones se han de hacer necesariamente a través de él. Todas las estaciones están conectadas por separado a un centro de comunicaciones, concentrador o nodo central, pero no están conectadas entre sí. Esta red crea una mayor facilidad de supervisión y control de información, ya que para pasar los mensajes deben pasar por el hub o

concentrador, el cual gestiona la redistribución de la información a los demás nodos.

La fiabilidad de este tipo de red es que el malfuncionamiento de un ordenador no afecta en nada a la red entera, puesto que cada ordenador se conecta independientemente del *hub,* el costo del cableado puede llegar a ser muy alto. Su punto débil consta en el *hub* ya que es el que sostiene la red en uno.

Figura 7. **Topología en estrella**



Fuente: LOBO, Lancy. *MPLS Configuraion Cisco IOS Software.* p 48.

1.6. Presente y futuro de Ethernet

Ethernet se planteó en un principio como un protocolo destinado a cubrir las necesidades de las redes LAN. A partir de 2001 Ethernet alcanzó los 10 Gbps lo que dio mucha más popularidad a la tecnología. Dentro del sector de las telecomunicaciones se planteaba a ATM como la total encargada de los niveles superiores de la red, pero el estándar 802.3ae (Ethernet Gigabit 10) se

ha situado en una buena posición para extenderse al nivel WAN, y ha permitido la evolución de Ethernet al nivel de redes Metro.

1.7. Metro Ethernet

Una red Metro Ethernet es una red de computadoras que cubre un área metropolitana y está basada en el estándar Ethernet. Es usada comúnmente como una red de acceso metropolitano para conectar suscriptores y negocios a una red más grande o al internet. Las empresas también pueden usar Metro Ethernet para conectar sucursales a su Intranet.

Una interface Ethernet es menos cara que que una interface SONET/SDH o PDH con el mismo ancho de banda. Una ventaja distintiva de una red de acceso basada en Ethernet es que puede ser conectada directamente a la red del cliente, dado que Ethernet es la tecnología más usada en redes corporativas y residenciales. Por lo tanto, llevar Ethernet a la red Metropolitana MAN (también llamada Metro) introduce muchas ventajas tanto al proveedor de servicios como al cliente, sea este residencial o corporativo.

Ethernet en la MAN puede usarse como Ethernet puro, Ethernet sobre SDH, Ethernet sobre MPLS o Ethernet sobre DWDM.

1.8. Ethernet para redes Metro

A continuación se presentan algunas ventajas e inconvenientes que aporta Ethernet en redes Metro.

Ventajas:

- Bajo coste: los costes para implementar la infraestructura (cables, conectores, tarjetas, equipos de interconexión, entre otros.) son menores, además los costes de mantenimiento y configuración también lo son, debido a que Ethernet solo requiere conectar los equipos sin más configuración.

- Configuración rápida bajo demanda: Ethernet Ethernet ofrece una gran variedad de velocidades de transmisión, (desde 10 Mbps hasta 10 Gbps), en intervalos de hasta 1 Mbps o incluso menos.

- Fácil de interconectar con otras redes: debido a que el 98 % de las LAN están implementadas sobre Ethernet, no es necesaria una conversión de protocolos entre LAN y MAN, lo que facilita enormemente la integración de redes LAN en la red MAN.

Inconvenientes:

- La distancia: era una gran limitación puesto que las redes Ethernet sobre cobre podían solo cubrir una extensión de 100 metros antes de que el retardo de propagación causara una degradación seria en la comunicación. Para salvar este problema es necesaria la instalación de fibra óptica, la cual es mucho más cara que el cobre.

- La fiabilidad y la redundancia: hasta hace poco, las redes Ethernet no eran consideradas tan fiables como otras redes tales como TDM. De hecho, los mecanismos de redundancia y recuperación ante fallos de Ethernet, como Spaning Tree, eran sumamente lentos e ineficientes.

- La capacidad de crecimiento: hechos como el continuo *broadcast* o la necesidad de aprendizaje de direcciones físicas (MAC) de todos los usuarios ven todos los nodos de la red, ponían en entredicho la capacidad de crecimiento de la tecnología.

- La seguridad: Ethernet se consideraba una tecnología de medio compartido en el que los usuarios fácilmente podían acceder al tráfico de otros.

Hoy en día la tecnología proporciona las herramientas necesarias para superar dichas limitaciones, de esta manera se puede afirmar que:

- La distancia ya no es una limitación, debido a que las tecnologías ópticas nos permiten transportar Ethernet a decenas e incluso centenares de kilómetros.
- La fiabilidad y la redundancia han dejado de ser un problema y hoy en día los fabricantes de equipamiento Ethernet aportan soluciones de alta fiabilidad.
- La capacidad de crecimiento de las redes Ethernet se ha incrementado en varios órdenes de magnitud, gracias a modificaciones de la tecnología.
- La seguridad y la separación entre usuarios se ha reforzado gracias a tecnologías de tunelización.

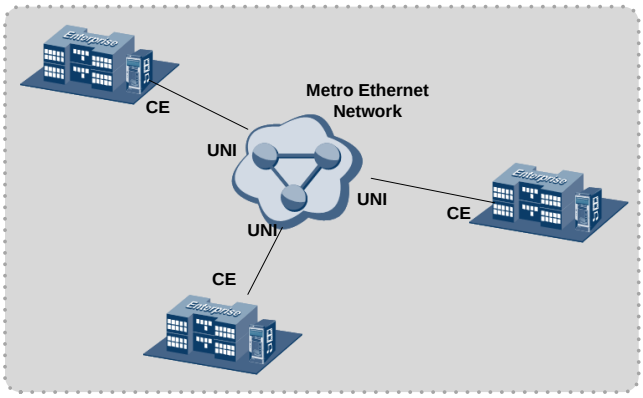
1.9. Componentes de una red Metro Ethernet

El modelo básico de un servicio metropolitano Ethernet consta de tres partes:

- El dispositivo instalado del lado del usuario, por ejemplo *router* o *switch*, llamado Customer Equipment (CE).
- La interfaz de conexión del usuario a la red, por ejemplo puertos RJ45 o de fibra, conocida como User Network Interface (UNI).
- La red metropolitana conocida como Metro Ethernet Network (MEN). Es posible tener múltiples UNIs conectadas a la MEN de una simple localización.

La primera diferencia notable con las típicas conexiones de una empresa hacia una nube metropolitana no basada en Ethernet es el UNI. Atrás quedaron los tiempos en que para conectarse entre las sucursales de una empresa o para conectarse a Internet era necesario utilizar conexiones sincrónicas mediante modems o codecs (usando últimas millas de cobre o radio microondas). El UNI definido por Metro Ethernet es el conocido puerto Ethernet RJ45 (o también un puerto de fibra óptica) usado por la mayoría de redes de área local hoy en día. Es decir que un proveedor de red Metro Ethernet llega hacia sus usuarios con un cable de red, tal como si fuese a conectar otro PC más en su LAN.

Figura 8. **Ubicación del CE, UNI en una Metro Ethernet Network (MEN)**



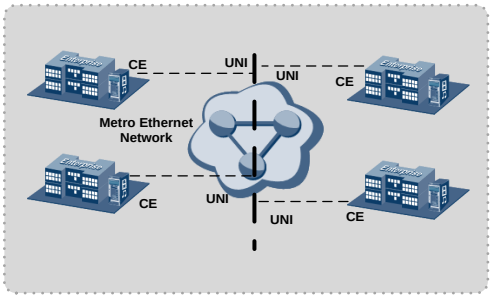
Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 50.

La segunda diferencia respecto de otras redes de área metropolitana es la diversidad del tipo de CE que puede conectarse a la red. Se pueden usar los conocidos enrutadores para conectar las redes LAN entre la casa matriz y las sucursales o se puede simplemente interconectar los *switches* de las respectivas LAN (ubicadas geográficamente en sitios distantes). El proveedor de la red Metro Ethernet debe garantizar en cualquiera de los dos casos que los datos viajen de manera segura e independiente del resto del tráfico de usuarios dentro de la red Metro Ethernet.

1.10. Tipos de servicio en una red Metro Ethernet

En la Red Metro Ethernet se pueden dar dos tipos de servicios diferentes: E-lines y E-LANs. Las E-lines son conexiones punto-a-punto, mientras que las E-LANs son conexiones multipunto-a-multipunto (*any-to-any*). Adicionalmente se ha creado un tercer concepto llamado Ethernet Virtual Connection (EVC) que es definido como la instancia de asociación entre dos o más puntos de la red Metro Ethernet. Los EVC son análogos a las definiciones de circuitos virtuales privados (PVC) en *frame relay* o Virtual Channels (VC) en ATM.

Figura 9. **Servicio E-LAN multipunto – multipunto**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 55.

1.11. Clases de servicio (CoS)

Cuando el objetivo es proporcionar diferentes parámetros de tráfico, cada clase de servicio puede ofrecer diferentes niveles de desempeño, como retardos, *jitter* y tramas perdidas, de ahí que los parámetros de desempeño deben ser los especificados para cada clase. A continuación se muestran las características de dichas clases de servicio.

- Puerto físico: en este caso, una simple clase de servicio es provista por un puerto físico. Todo el tráfico que ingresa o sale del puerto recibe la misma clase de servicio. Si el usuario requiere múltiples clases de servicio para sus tráficos, se separan tantos puertos físicos como sean requeridos, cada uno con su clase de servicio.

- CE-VLAN CoS (802.1p): el MEF (Metro Ethernet Forum) ha definido CE-VLAN CoS como la clase de servicio que utiliza 802.1q para etiquetar las tramas, cuando se utiliza, se pueden indicar hasta 8 clases de servicio. El proveedor de servicio especifica el ancho de banda y los parámetros de desempeño.

- DiffServ/IP TOS Values: pueden ser usados para determinar la clase de servicio IP TOS, en general, se usa para proveer 8 clases de servicio conocidas como prioridad IP. Prioridad IP es muy similar a la definición en 802.1p en IEEE 802.1q cuando la CoS se basa en prioridad de envío. DiffServ se define como PHS (*perhop behaviors*), con una calidad de servicio más robusta cuando se compara con IP TOS y 802.1p. DiffServ provee 64 diferentes valores para determinar las clases de servicio. Casi todos los *routers* y *switches* soportan estas clases de servicio.

2. FUNDAMENTOS DE LAS TECNOLOGÍAS MPLS & EOMPLS

El enorme crecimiento de la red Internet ha convertido al protocolo IP (Internet Protocol) en la base de las actuales redes de telecomunicaciones, contando con más del 80 % del tráfico cursado. La versión actual de IP, conocida por IPv4 y recogida en la RFC 791, lleva operativa desde 1980. Este protocolo de capa de red (Nivel 3 OSI), define los mecanismos de la distribución o encaminamiento de paquetes, de una manera no fiable y sin conexión, en redes heterogéneas; es decir, únicamente está orientado a servicios no orientados a conexión y a la transferencia de datos, por lo que se suele utilizar junto con TCP (Transmission Control Protocol) (Nivel 4 de OSI) para garantizar la entrega de los paquetes.

A mediados de la década de los 90, la demanda por parte de los clientes de los ISP (Internet Service Providers) de aplicaciones multimedia con altas necesidades de ancho de banda y una calidad de servicio o QoS (Quality of Service) garantizada, propiciaron la introducción de ATM (Asyncronous Transfer Mode) en la capa de enlace (Nivel 2 de OSI) de sus redes. En esos momentos, el modelo de IP sobre ATM satisfacía los requisitos de las nuevas aplicaciones, utilizando el encaminamiento inteligente de nivel 3 de los routers IP en la red de acceso, e incrementando el ancho de banda y rendimiento basándose en la alta velocidad de los conmutadores de nivel 2 y los circuitos permanentes virtuales de los *switches* ATM en la red troncal.

Esta arquitectura, no obstante, presenta ciertas limitaciones, debido a: la dificultad de operar e integrar una red basándose en dos tecnologías muy distintas, la aparición de *switches* ATM e IP de alto rendimiento en las redes

troncales, y la mayor capacidad de transmisión ofrecida por SDH/SONET (Synchronous Digital Hierarchy / Syncronous Optical NETwork) y DWDM (Dense Wavelength Division Multiplexing) respecto a ATM.

Durante 1996 empezaron a aparecer soluciones de conmutación de nivel 2 propietarias diseñadas para el núcleo de internet que integraban la conmutación ATM con el encaminamiento IP; como por ejemplo, *Tag Switching* de Cisco o Aggregate Route-Based IP Switching de IBM. La base común de todas estas tecnologías, era tomar el software de control de un router IP, integrarlo con el rendimiento de reenvío con cambio de etiqueta de un switch ATM y crear un router extremadamente rápido y eficiente en cuanto a coste. La integración en esta arquitectura era mayor, porque se utilizaban protocolos IP propietarios para distribuir y asignar los identificadores de conexión de ATM como etiquetas; pero los protocolos no eran compatibles entre sí y requerían aún de infraestructura ATM.

Finalmente en 1997, el IETF (*Internet Engineering Task Force*) establece el grupo de trabajo MPLS (MultiProtocol Label Switching) para producir un estándar que unificase las soluciones propietarias de conmutación de nivel 2. El resultado fue la definición en 1998 del estándar conocido por MPLS, recogido en la RFC 3031. MPLS proporciona los beneficios de la ingeniería de tráfico del modelo de IP sobre ATM, pero además, otras ventajas; como una operación y diseño de red más sencillo y una mayor escalabilidad. Por otro lado, a diferencia de las soluciones de conmutación de nivel 2 propietarias, está diseñado para operar sobre cualquier tecnología en el nivel de enlace, no únicamente ATM, facilitando así la migración a las redes ópticas de próxima generación, basadas en infraestructuras SDH/SONET y DWDM.

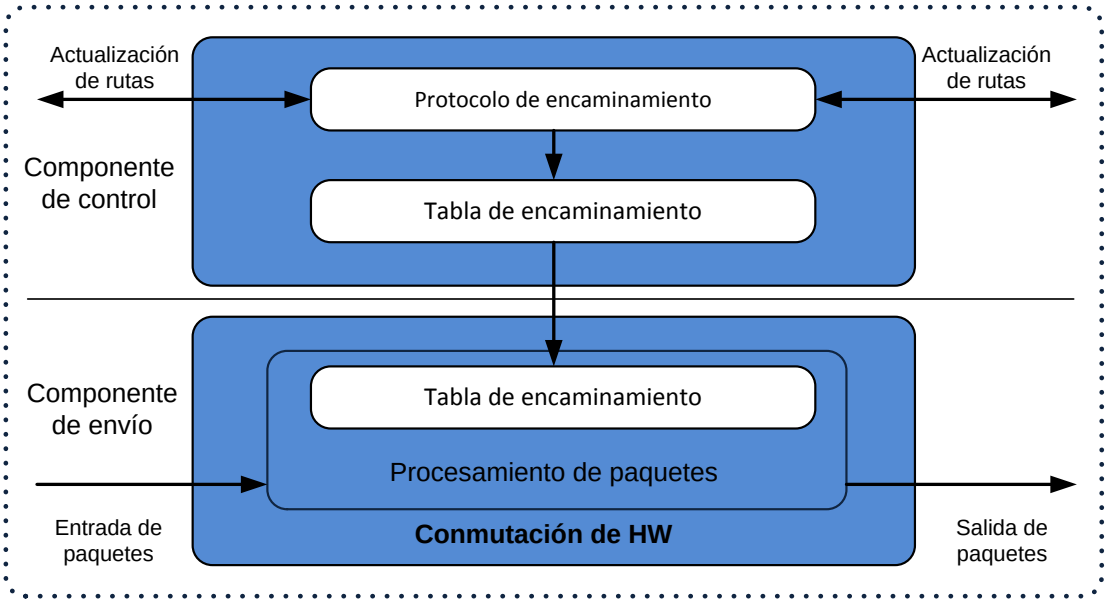
2.1. Conmutación de etiquetas multiprotocolo

MPLS (*Multi Protocol Level Switching*) es un estándar IP de conmutación de paquetes del IETF, que trata de proporcionar algunas de las características de las redes orientadas a conexión a las redes no orientadas a conexión. En el encaminamiento IP sin conexión tradicional, la dirección de destino junto a otros parámetros de la cabecera, es examinada cada vez que el paquete atraviesa un *router*. La ruta del paquete se adapta en función del estado de las tablas de encaminamiento de cada nodo, pero, como la ruta no puede predecirse, es difícil reservar recursos que garanticen la QoS; además, las búsquedas en tablas de encaminamiento hacen que cada nodo pierda cierto tiempo, que se incrementa en función de la longitud de la tabla.

Sin embargo, MPLS permite a cada nodo, ya sea un *switch* o un *router*, asignar una etiqueta a cada uno de los elementos de la tabla y comunicarla a sus nodos vecinos. Esta etiqueta es un valor corto y de tamaño fijo transportado en la cabecera del paquete para identificar un FEC (*Forward Equivalence Class*), que es un conjunto de paquetes que son reenviados sobre el mismo camino a través de la red, incluso si sus destinos finales son diferentes.

La etiqueta es un identificador de conexión que solo tiene significado local y que establece una correspondencia entre el tráfico y un FEC específico. Dicha etiqueta se asigna al paquete basándose en su dirección de destino, los parámetros de tipo de servicio, la pertenencia a una VPN, o siguiendo otro criterio. Cuando MPLS está implementado como una solución IP pura o de nivel 3, que es la más habitual, la etiqueta es un segmento de información añadido al comienzo del paquete. Además de añadir una etiqueta al encabezado de un paquete, MPLS separa los componentes de control (enrutamiento) y de envío (*Forwarding*), tal como se muestra en la figura 10.

Figura 10. **Separación de lo control y de envío**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 63.

La componente de control utiliza los protocolos estándar de encaminamiento (OSPF, IS-IS, BGP, etc.) para el intercambio de información con los otros routers para la construcción y el mantenimiento de las tablas de enrutamiento. Al llegar los paquetes, la componente de envío busca en la tabla de envío, que mantiene la componente de control, para tomar la decisión de encaminamiento para cada paquete. En concreto, la componente de envío examina la información de la cabecera del paquete, busca en la tabla de envío la entrada correspondiente y dirige el paquete desde la interfaz de entrada al de salida a través del correspondiente hardware de conmutación.

Al separar la componente de control (encaminamiento) de la componente de envío, cada una de ella se puede implementar y modificar independientemente. El único requisito es que la componente de

encaminamiento mantenga la comunicación con la de envío mediante la tabla de envío de paquetes y actualice la información. El mecanismo de envío se implementa mediante el intercambio de etiquetas, de modo que lo que se envía por la interfaz física de salida son paquetes "etiquetados".

2.2. Elementos de una red MPLS

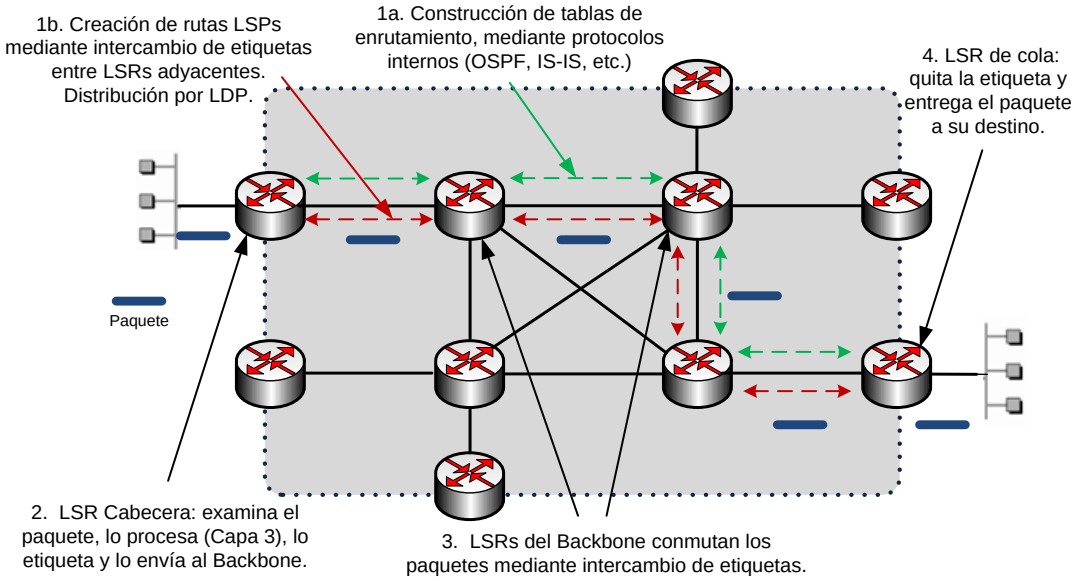
La operación del MPLS se basa en las componentes funcionales de envío y control, aludidas anteriormente, y que actúan ligadas íntimamente entre sí, y por los siguientes componentes físicos:

- LER (*Label Edge Router*): elemento que inicia o termina el túnel (pone y quita etiquetas). Es decir, el elemento de entrada/salida a la red MPLS. Un *router* de entrada se conoce como Ingress *Router* y uno de salida como *Egress Router*. Ambos se suelen denominar *Label Edge Router* ya que se encuentran en los extremos de la red MPLS.
- LSR (*Label Switching Router*): elemento que conmuta etiquetas.
- LSP (*Label Switched Path*): nombre genérico de un camino MPLS (para cierto tráfico o *Forwarding Equivalence Class* - FEC), es decir, el túnel MPLS establecido entre los extremos. Un LSP es unidireccional.
- LDP (*Label Distribution Protocol*): un protocolo para la distribución de etiquetas MPLS entre los equipos de la red.
- FEC (*Forwarding Equivalence Class*): nombre que se le da al tráfico que se encamina bajo una etiqueta. Subconjunto de paquetes tratados del mismo modo por el conmutador.

La arquitectura de una red MPLS es la que se muestra en la figura 11, donde quedan reflejadas las diversas funciones en cada uno de los elementos que integran la red MPLS. Es importante destacar que en el borde de la nube

MPLS se tiene una red convencional de *routers* IP. El núcleo MPLS proporciona una arquitectura de transporte que hace aparecer a cada par de routers a una distancia de un sólo salto. Funcionalmente es como si estuvieran unidos todos en una topología mallada (directamente o por PVCs ATM). Ahora, esa unión a un solo salto se realiza por MPLS mediante los correspondientes LSPs (puede haber más de uno para cada par de *routers*). La diferencia con topologías conectivas reales es que en MPLS la construcción de caminos virtuales es mucho más flexible y que no se pierde la visibilidad sobre los paquetes IP.

Figura 11. **Arquitectura de red MPLS**

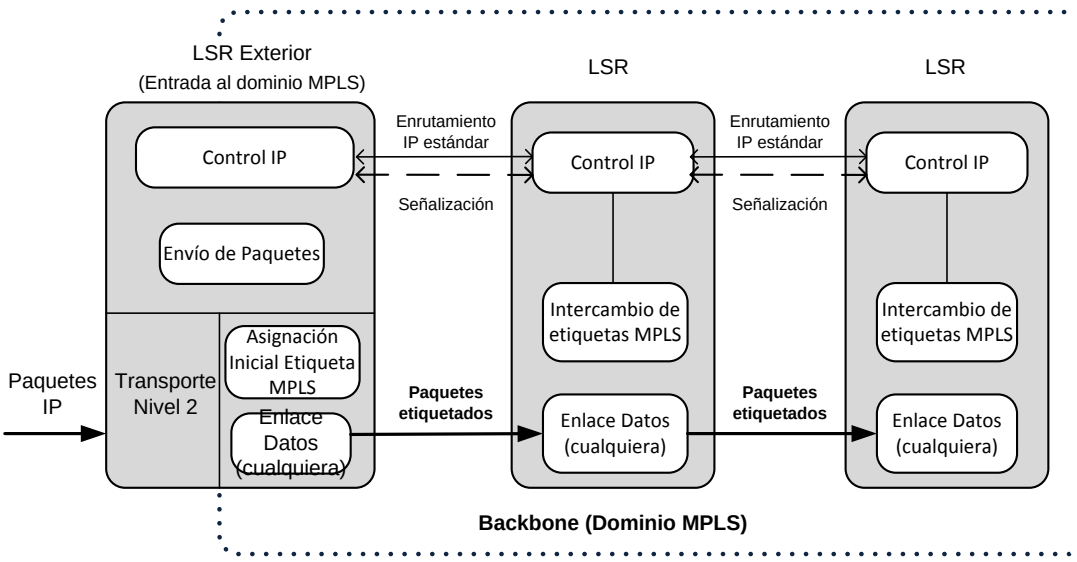


Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p.65.

2.3. Envío de paquetes en MPLS

La base del MPLS está en la asignación e intercambio de etiquetas ya expuesto, que permiten el establecimiento de los caminos LSP por la red. Los LSPs son “simplex” por naturaleza (se establecen para un sentido del tráfico en cada punto de entrada a la red); para el tráfico dúplex requiere dos LSPs, uno en cada sentido. Cada LSP se crea a base de concatenar uno o más saltos (hops) en los que se intercambian las etiquetas, de modo que cada paquete se envía de un "conmutador de etiquetas" (*Label-Swiching Router*) a otro, a través del dominio MPLS.

Figura 12. **Esquema funcional del MPLS**



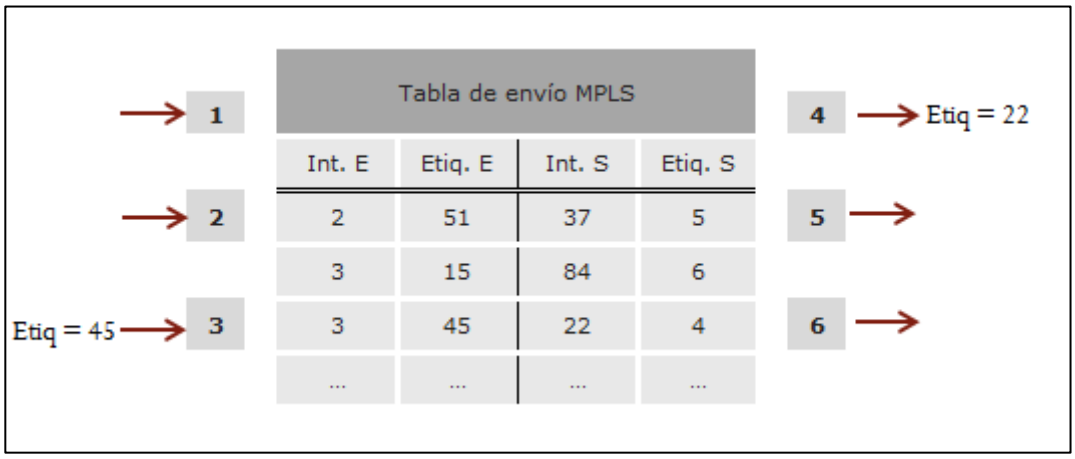
Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 66.

En la figura 12 se puede ver el funcionamiento de una red MPLS. Puede verse la separación de las dos componentes funcionales de control (enrutamiento IP) y de envío (etiquetas MPLS). MPLS utiliza el protocolo RSVP

o bien un nuevo estándar de señalización (el *Label Distribution Protocol*, LDP, del que se tratará más adelante). Pero, de acuerdo con los requisitos del IETF, el transporte de datos puede ser cualquiera.

Si este fuera ATM, una red IP habilitada para MPLS es ahora mucho más sencilla de gestionar que la solución clásica IP/ATM. Ahora ya no hay que administrar dos arquitecturas diferentes acbase de transformar las direcciones IP y las tablas de encaminamiento en las direcciones y el encaminamiento ATM: esto lo resuelve el procedimiento de intercambio de etiquetas MPLS. El papel de ATM o de la tecnología de capa 2 utilizada queda restringido al mero transporte de datos basado en celdas. Para MPLS esto es indiferente, ya que puede utilizar otros transportes como *frame relay*, o directamente sobre líneas punto a punto.

Figura 13. **Detalle de la tabla de envío de un LSR**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Sofware*. p. 67.

Un camino LSP es el circuito virtual que siguen por la red todos los paquetes asignados a la misma FEC. Al primer LSR que interviene en un LSP

se le denomina de entrada o de cabecera y al último se le denomina de salida o de cola. Los dos están en el exterior del dominio MPLS. El resto, entre ambos, son LSRs interiores del dominio MPLS.

Un LSR es como un router que funciona a base de intercambiar etiquetas según una tabla de envío. Esta tabla se construye a partir de la información de encaminamiento que proporciona la componente de control (IP), según se verá más adelante. Cada entrada de la tabla contiene un par de etiquetas entrada/salida correspondientes a cada interfaz de entrada, que se utilizan para acompañar a cada paquete que llega por esa interfaz y con la misma etiqueta (en los LSR exteriores sólo hay una etiqueta, de salida en el de cabecera y de entrada en el de cola). En la figura 13 se ilustra un ejemplo del funcionamiento de un LSR del núcleo MPLS.

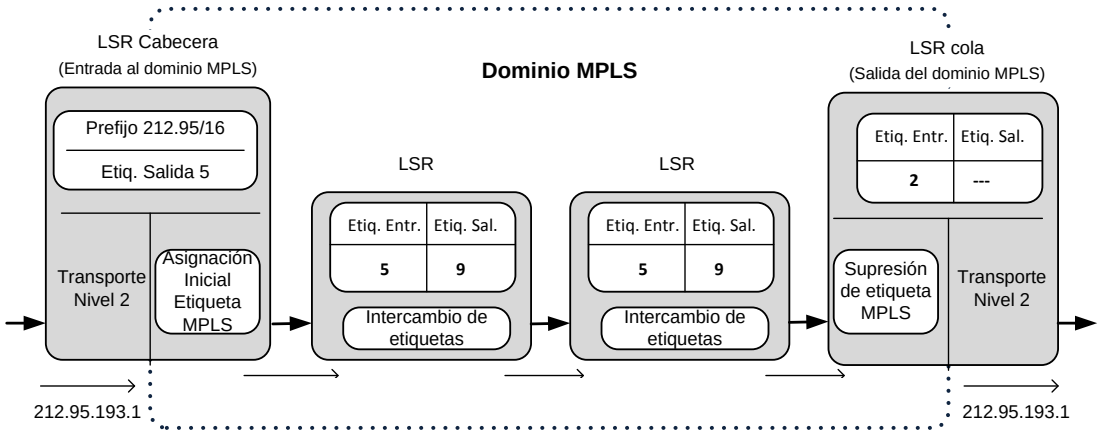
A un paquete que llega al LSR por la interfaz 3 de entrada con la etiqueta 45, el LSR le asigna la etiqueta 22 y lo envía por el interfaz 4 de salida al siguiente LSR, de acuerdo con la información de la tabla.

El algoritmo de intercambio de etiquetas requiere la clasificación de los paquetes a la entrada del dominio MPLS para poder hacer la asignación por el LSR de cabecera. En la figura 14 el LSR de entrada recibe un paquete normal (sin etiquetar) cuya dirección de destino es 212.95.193.1. El LSR consulta la tabla de encaminamiento y asigna el paquete a la clase FEC definida por la red 212.95/16. Asimismo, este LSR le asigna una etiqueta (con valor 5 en el ejemplo) y envía el paquete al siguiente LSR del LSP.

Dentro del dominio MPLS los LSR ignoran la cabecera IP; solamente analizan la etiqueta de entrada, consultan la tabla correspondiente (tabla de conmutación de etiquetas) y la reemplazan por otra nueva, de acuerdo con el

algoritmo de intercambio de etiquetas. Al llegar el paquete al LSR de cola (salida), ve que el siguiente salto lo saca de la red MPLS; al consultar ahora la tabla de conmutación de etiquetas quita esta y envía el paquete por *routing* convencional.

Figura 14. **Ejemplo de envío de un paquete por un LSP**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p.69.

Como se ve, la identidad del paquete original IP queda enmascarada durante el transporte por la red MPLS, que no "mira" sino las etiquetas que necesita para su envío por los diferentes saltos LSR que configuran los caminos LSP. Las etiquetas se insertan en cabeceras MPLS, entre los niveles 2 y 3.

Según las especificaciones del IETF, MPLS debía funcionar sobre cualquier tipo de transporte: PPP, LAN, ATM, Frame Relay, etc. Por ello, si el protocolo de transporte de datos contiene ya un campo para etiquetas (como ocurre con los campos VPI/VCI de ATM y DLCI de Frame Relay), se utilizan esos campos nativos para las etiquetas. Sin embargo, si la tecnología de nivel 2 empleada no soporta un campo para etiquetas p. ej. enlaces PPP o LAN (Ethernet)), entonces se emplea una cabecera genérica MPLS de 4 octetos,

que contiene un campo específico para la etiqueta y que se inserta entre la cabecera del nivel 2 y la del paquete (nivel 3).

En la figura 15 se representa el esquema de los campos de la cabecera generica MPLS y su relación con las cabeceras de los otros niveles. Según se muestra en la figura, los 32 bits de la cabecera MPLS se reparten en:

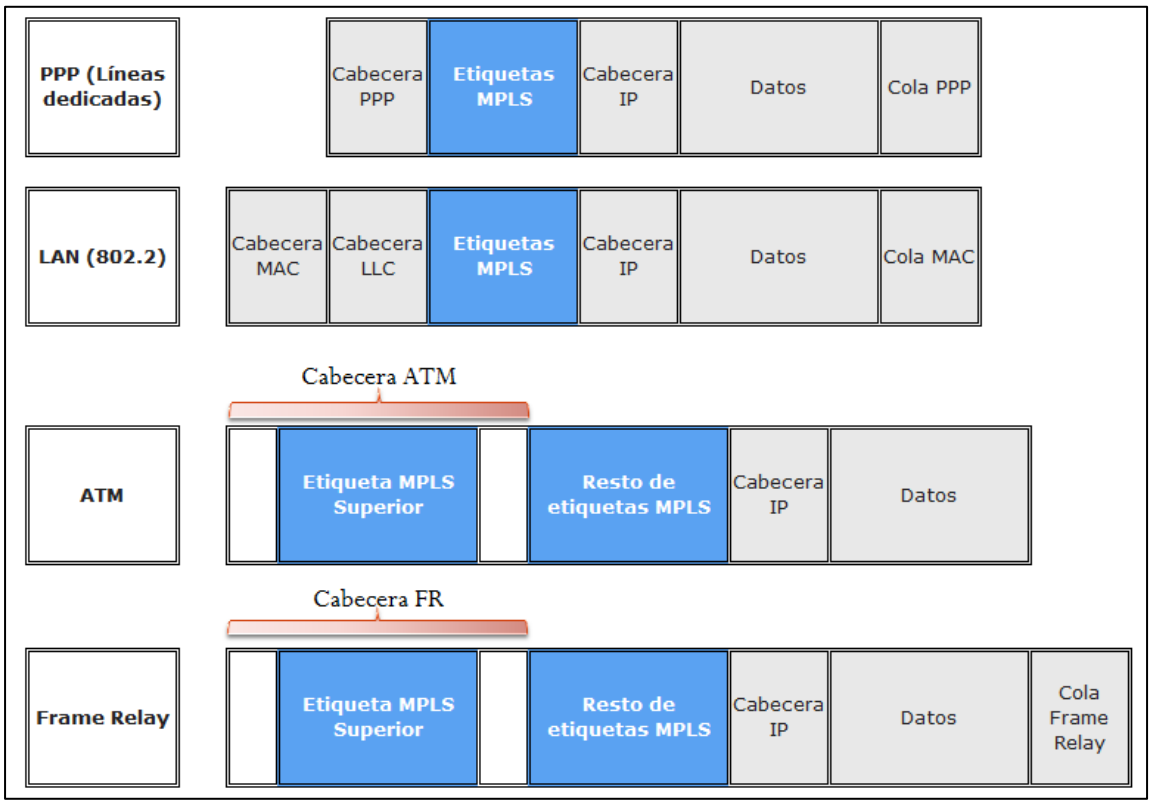
- *Label* (20 bits): es la identificación de la etiqueta.
- EXP (3 bits): también aparece como CoS y como bits experimentales en otros textos, afecta al encolado y descarte de paquetes.
- *Stack (*1 bit): para poder apilar etiquetas de forma jerárquica (S). Cuando S = 0 indica que hay más etiquetas añadidas al paquete. Cuando S = 1 se está en el fondo de la jerarquía.
- TTL (8 bits*): Time-to-live*, misma funcionalidad que en IP, se decrementa en cada enrutador y al llegar al valor de 0, el paquete es descartado. Generalmente sustituye el campo TTL de la cabecera IP.

De este modo, las cabeceras MPLS permiten cualquier tecnología o combinación de tecnologías de transporte, con la flexibilidad que esto supone para un proveedor IP a la hora de extender su red.

Figura 15. **Estructura de la cabecera genérica MPLS**

Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 71.

Figura 16. **Situación de la etiqueta MPLS**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software.* p. 73.

2.4. Control de la información en MPLS

Hasta ahora se ha visto el mecanismo básico de envío de paquetes a través de los LSPs mediante el procedimiento de intercambio de etiquetas, según las tablas de los LSRs. Pero queda por ver dos aspectos fundamentales:

- Cómo se generan las tablas de envío que establecen los LSPs
- Cómo se distribuye la información sobre las etiquetas a los LSRs

El primero de ellos está relacionado con la información que se tiene sobre la red: topología, patrón de tráfico, características de los enlaces, etc. Es la información de control típica de los algoritmos de encaminamiento. MPLS necesita esta información de *routing* para establecer los caminos virtuales LSPs.

Lo más lógico es utilizar la propia información de encaminamiento que manejan los protocolos internos IGP (OSPF, IS-IS, RIP...) para construir las tablas de encaminamiento (recordar que los LSR son *routers* con funcionalidad añadida). Esto es lo que hace MPLS precisamente: para cada "ruta IP" en la red se crea un "camino de etiquetas" a base de concatenar las de entrada/salida en cada tabla de los LSRs; el protocolo interno correspondiente se encarga de pasar la información necesaria.

El segundo aspecto se refiere a la información de "señalización", pero siempre que se quiera establecer un circuito virtual se necesita algún tipo de señalización para marcar el camino, es decir, para la distribución de etiquetas entre los nodos. Sin embargo, la arquitectura MPLS no asume un único protocolo de distribución de etiquetas; de hecho se están estandarizando algunos existentes con las correspondientes extensiones; uno de ellos es el protocolo RSVP del modelo de servicios integrados del IETF (recordar que ese era uno de los requisitos). Pero, además, en el IETF se están definiendo otros nuevos, específicos para la distribución de etiquetas, cual es el caso del Label Distribution Protocol (LDP).

2.5. Aplicaciones de MPLS

Las principales aplicaciones que hoy en día tiene MPLS son:

- Ingeniería de tráfico.
- Diferenciación de niveles de servicio mediante clases (CoS).
- Servicio de redes privadas virtuales (VPN).
- Servicio de tranporte de paquetes 802.1Q (Ethernet) sobre túneles construidos en redes MPLS (EoMPLS).

Brevemente pueden verse las características de estas aplicaciones y las ventajas que MPLS supone para ello frente a otras soluciones tradicionales.

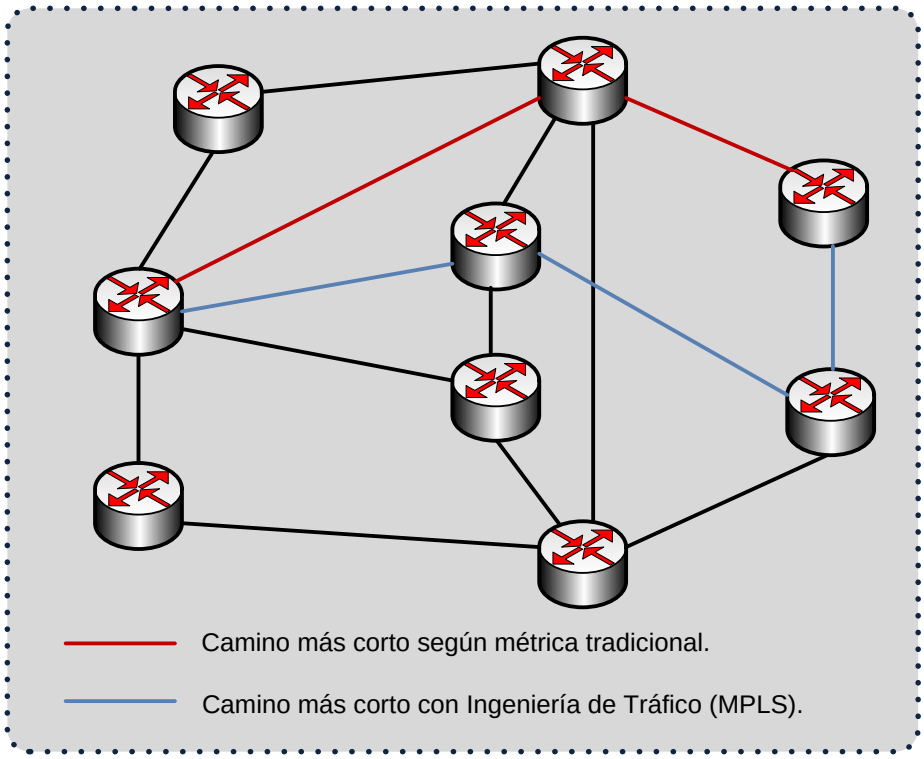
2.5.1. Ingeniería de tráfico

El objetivo básico de la ingeniería de tráfico es adaptar los flujos de tráfico a los recursos físicos de la red. La idea es equilibrar de forma óptima la utilización de esos recursos, de manera que no haya algunos que estén suprautilizados, con posibles puntos calientes y cuellos de botella, mientras otros puedan estar infrautilizados. A comienzos de los 90 los esquemas para adaptar de forma efectiva los flujos de tráfico a la topología física de las redes IP eran bastante rudimentarios. Los flujos de tráfico siguen el camino más corto calculado por el algoritmo IGP correspondiente.

En casos de congestión de algunos enlaces, el problema se resolvía a base de añadir más capacidad a los enlaces. La ingeniería de tráfico consiste en trasladar determinados flujos seleccionados por el algoritmo IGP sobre enlaces más congestionados, a otros enlaces más descargados, aunque estén fuera de la ruta más corta (con menos saltos).

En el esquema de la figura 17 se comparan estos dos tipos de rutas para el mismo par de nodos origen-destino.

Figura 17. **Camino más corto con ingeniería de tráfico**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software.* p. 75.

El camino más corto entre A y B según la métrica normal IGP es el que tiene solo dos saltos, pero puede que el exceso de tráfico sobre esos enlaces o el esfuerzo de los routers correspondientes haga aconsejable la utilización del camino alternativo indicado con un salto más. MPLS es una herramienta efectiva para esta aplicación en grandes Backbones, ya que:

- Permite al administrador de la red el establecimiento de rutas explícitas, especificando el camino físico exacto de un LSP.
- Permite obtener estadísticas de uso LSP, que se pueden utilizar en la planificación de la red y como herramientas de análisis de cuellos de

botella y carga de los enlaces, lo que resulta bastante útil para planes de expansión futura.

- Permite hacer "encaminamiento restringido" (*constraint-based routing, CBR*), de modo que el administrador de la red pueda seleccionar determinadas rutas para servicios especiales (distintos niveles de calidad). Por ejemplo, con garantías explícitas de retardo, ancho de banda, fluctuación, pérdida de paquetes, entre otros.

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

2.5.2. Clases de servicio (CoS)

MPLS está diseñado para poder cursar servicios diferenciados, según el Modelo DiffServ del IETF. Este modelo define una variedad de mecanismos para poder clasificar el tráfico en un reducido número de clases de servicio, con diferentes prioridades. Según los requisitos de los usuarios, DiffServ permite diferenciar servicios tradicionales tales como el WWW, el correo electrónico o la transferencia de ficheros (para los que el retardo no es crítico), de otras aplicaciones mucho más dependientes del retardo y de la variación del mismo, como son las de video y voz IP. Para ello se emplea el campo ToS (*Type of service*), rebautizado en DiffServ como el octeto DS. Esta es la técnica QoS de marcar los paquetes que se envían a la red.

MPLS se adapta perfectamente a ese modelo, ya que las etiquetas MPLS tienen el campo EXP para poder propagar la clase de servicio CoS en el correspondiente LSP.

De este modo, una red MPLS puede transportar distintas clases de tráfico, ya que:

- El tráfico que fluye a través de un determinado LSP se puede asignar a diferentes colas de salida en los diferentes saltos LSR, de acuerdo con la información contenida en los bits del campo EXP.

- Entre cada par de LSR exteriores se pueden provisionar múltiples LSPs, cada uno de ellos con distintas prestaciones y con diferentes garantías de ancho de banda. P. ej., un LSP puede ser para tráfico de máxima prioridad, otro para una prioridad media y un tercero para tráfico "*best-effort*", tres niveles de servicio, primera clase, preferente y turista, que, lógicamente, tendrán distintos precios.

2.5.3. Redes privadas virtuales (VPNs)

Una red privada virtual (VPN) se construye basado en conexiones realizadas sobre una infraestructura compartida, con funcionalidades de red y de seguridad equivalentes a las que se obtienen con una red privada. El objetivo de las VPNs es el soporte de aplicaciones intra/extranet, integrando aplicaciones multimedia de voz, datos y video sobre infraestructuras de comunicaciones eficaces y rentables. La seguridad supone aislamiento, y "privada" indica que el usuario "cree" que posee los enlaces.

Las IP VPNs son soluciones de comunicación VPN basada en el protocolo de red IP de la Internet. En esta sección se van a describir brevemente las ventajas que MPLS ofrece para este tipo de redes frente a otras soluciones tradicionales.

Las VPNs tradicionales se han venido construyendo sobre infraestructuras de transmisión compartidas con características implícitas de seguridad y respuesta predeterminada. Tal es el caso de las redes de datos *frame relay*, que permiten establecer PCVs entre los diversos nodos que conforman la VPN. La seguridad y las garantías las proporcionan la separación de tráficos por PVC y el caudal asegurado (CIR) 9. Algo similar se puede hacer con ATM, con diversas clases de garantías.

El inconveniente de este tipo de solución es que la configuración de las rutas se basa en procedimientos más bien artesanales, al tener que establecer cada PVC entre nodos, con la complejidad que esto supone al proveedor en la gestión (y los mayores costes asociados). Si se quiere tener conectados a todos con todos, en una topología lógica totalmente mallada, añadir un nuevo emplazamiento supone retocar todos los CPEs del cliente y restablecer todos los PVCs.

Además, la popularización de las aplicaciones TCP/IP, así como la expansión de las redes de los NSPs, ha llevado a tratar de utilizar estas infraestructuras IP para el soporte de VPNs, tratando de conseguir una mayor flexibilidad en el diseño e implantación y unos menores costes de gestión y provisión de servicio. La forma de utilizar las infraestructuras IP para servicio VPN (IP VPN) ha sido la de construer túneles IP de diversos modos.

El objetivo de un túnel sobre IP es crear una asociación permanente entre dos extremos, de modo que funcionalmente aparezcan conectados. Lo que se hace es utilizar una estructura no conectiva como IP para simular esas conexiones: una especie de tuberías privadas por las que no puede entrar nadie que no sea miembro de esa IP VPN. No es el objetivo de esta sección una exposición completa de IP VPNs sobre túneles; se pretende tan solo resumir sus características para poder apreciar luego las ventajas que ofrece MPLS frente a esas soluciones.

Los túneles IP en conexiones dedicadas (no se va a tratar aquí de las conexiones conmutadas de acceso) se pueden establecer de dos maneras:

- En el nivel 3, mediante el protocolo IPSec10 del IETF.
- En el nivel 2, mediante el encapsulamiento de paquetes privados (IP u otros) sobre una red IP pública de un ISP.

En las VPNs basadas en túneles IPSec, la seguridad requerida se garantiza mediante el cifrado de la información de los datos y de la cabecera de los paquetes IP, que se encapsulan con una nueva cabecera IP para su transporte por la red del proveedor.

Es relativamente sencillo de implementar, bien sea en dispositivos especializados, tales como cortafuegos, como en los propios routers de acceso del NSP. Además, como es un estándar, IPSec permite crear VPNs a través de redes de distintos NSPs que sigan el estándar IPSec. Pero como el cifrado IPSec oculta las cabeceras de los paquetes originales, las opciones QoS son bastante limitadas, ya que la red no puede distinguir flujos por aplicaciones para asignarles diferentes niveles de servicio. Además, solo vale para paquetes IP nativos, IPSec no admite otros protocolos.

En los túneles de nivel 2 se encapsulan paquetes multiprotocolo (no necesariamente IP), sobre los datagramas IP de la red del ISP. De este modo, la red del proveedor no pierde la visibilidad IP, por lo que hay mayores posibilidades de QoS para priorizar el tráfico por tipo de aplicación IP. Los clientes VPN pueden mantener su esquema privado de direcciones, estableciendo grupos cerrados de usuarios, si así lo desean. (Además de encapsular los paquetes, se puede cifrar la información por mayor seguridad, pero en este caso limitando las opciones QoS). A diferencia de la opción anterior, la operación de túneles de nivel 2 está condicionada a un único proveedor.

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

- Están basadas en conexiones punto a punto (PVCs o túneles).
- La configuración es manual.
- La provisión y gestión son complicadas; una nueva conexión supone alterar todas las configuraciones.
- Plantean problemas de crecimiento al añadir nuevos túneles o circuitos virtuales.

La gestión de QoS es posible en cierta medida, pero no se puede mantener extremo a extremo a lo largo de la red, ya que no existen mecanismos que sustenten los parámetros de calidad durante el transporte.

Realmente, el problema que plantean estas IP VPNs es que están basadas en un modelo topológico superpuesto sobre la topología física existente, basados en túneles extremo a extremo (o circuitos virtuales) entre

cada par de *routers* de cliente en cada VPN. De ahí las desventajas en cuanto a la poca flexibilidad en la provisión y gestión del servicio, así como en el crecimiento cuando se quieren añadir nuevos emplazamientos. Con una arquitectura MPLS se obvian estos inconvenientes, ya que el modelo topológico no se superpone sino que se acopla a la red del proveedor.

En el modelo acoplado MPLS, en lugar de conexiones extremo a extremo entre los distintos emplazamientos de una VPN, lo que hay son conexiones IP a una "nube común" en las que solamente pueden entrar los miembros de la misma VPN.

Las "nubes" que representan las distintas VPNs se implementan mediante los caminos LSPs creados por el mecanismo de intercambio de etiquetas MPLS. Los LSPs son similares a los túneles en cuanto a que la red transporta los paquetes del usuario (incluyendo las cabeceras) sin examinar el contenido, a base de encapsularlos sobre otro protocolo.

Aquí está la diferencia: en los túneles se utiliza el encaminamiento convencional IP para transportar la información del usuario, mientras que en MPLS esta información se transporta sobre el mecanismo de intercambio de etiquetas, que no ve para nada el proceso de routing IP. Sin embargo, sí se mantiene en todo momento la visibilidad IP hacia el usuario, que no sabe nada de rutas MPLS, sino que ve una internet privada (intranet) entre los miembros de su VPN. De este modo, se pueden aplicar técnicas QoS basadas en el examen de la cabecera IP, que la red MPLS podrá propagar hasta el destino, pudiendo así reservar ancho de banda, priorizar aplicaciones, establecer CoS y optimizar los recursos de la red con técnicas de ingeniería de tráfico.

En resumen, las ventajas que MPLS ofrece para IP VPNs son:

- Proporcionan un modelo "acoplado" o "inteligente", ya que la red MPLS "sabe" de la existencia de VPNs (lo que no ocurre con túneles ni PVCs).

- Evita la complejidad de los túneles y PVCs.

- La provisión de servicio es sencilla: una nueva conexión afecta a un solo router por lo que tiene mayores opciones de crecimiento modular.

- Permiten mantener garantías QoS extremo a extremo, pudiendo separar flujos de tráfico por aplicaciones en diferentes clases, gracias al vínculo que mantienen el campo EXP de las etiquetas MPLS con las clases definidas a la entrada.

- Permite aprovechar las posibilidades de ingeniería de tráfico para poder garantizar los parámetros críticos y la respuesta global de la red (ancho banda, retardo, fluctuación...), lo que es necesario para un servicio completo VPN.

2.5.4. Ethernet sobre MPLS (EoMPLS)

Existen soluciones “Cualquier Transponte sobre MPLS” (AToM – Any Transport over MPLS), que permiten a los ISPs usar una red MPLS para proveer conectividad entre sitios que tienen redes en capa 2. Una red MPLS puede usarse para transportar todos tipos de tráfico de diferentes clientes. Una de estas soluciones es EoMPLS (Ethernet over MPLS), el cual usa un mecanismo de tunelización para transportar tráfico Ethernet capa 2.

EoMPLS encapsula los cuadros Ethernet en paquetes MPLS y los envía a través de la red MPLS. Cada cuadro es transportado como un único paquete, y los *routers* PE ponen y quitan etiquetas para la encapsulación de paquetes.

- El *router* PE de ingreso recibe un cuadro Ethernet y encapsula el paquete removiendo el preámbulo, el campo SFD (Start of Frame), y el FCS (Frame Check Sequence). El resto del paquete no es modificado.

- El *router* PE de ingreso añade una etiqueta de conexión punto a punto virtual (VC) y una etiqueta de ruta de conmutación de etiquetas (LSP) para enrutamiento MPLS normal a través del Backbone MPLS.

- Los *routers* del Core MPLS usan el túnel LSP para transportar el paquete a través del Backbone MPLS y no distinguen el tipo de tráfico (Ethernet) que hay dentro de dicho paquete.

- Al final del *Backbone* MPLS, el *router* PE de salida recibe el paquete y lo desencapsula removiendo la etiqueta LSP. También remueve la etiqueta VC del paquete.

- El último *router* PE actualiza el encabezado de ser necesario, y envía el paquete a través de la interface apropiada al conmutador de destino.

El *Backbone* MPLS usa las etiquetas de túnel para transportar los paquetes entre los *routers* PE. El *router* PE de egreso usa la etiqueta VC para seleccionar la interface de salida para el paquete Ethernet. En la implementación EoMPLS de Cisco, los túneles EoMPLS son unidireccionales, para túneles bidireccionales se necesita configurar un túnel en cada dirección.

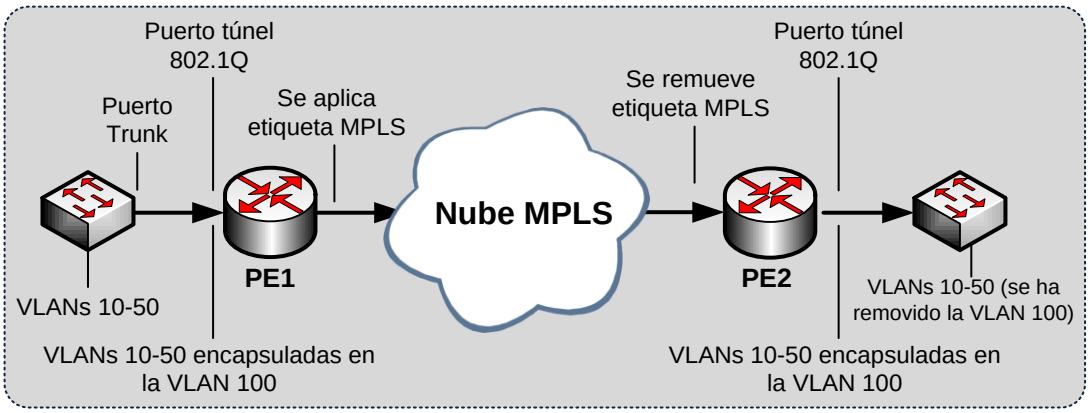
Los VCs punto a punto requieren que se configuren puntos finales *(endpoints)* en los dos *routers* PE. Solo los routers PE en los puntos de ingreso y egreso del *Backbone* MPLS saben sobre los VCs dedicados al transporte del tráfico de capa 2. Los demás *routers* no tienen entradas en sus tablas para estos VCs.

IEEE 802.1Q permite a los proveedores de servicio usar una única VLAN para soportar clientes que tienen múltiples VLANs, mientras se preservan los VLAN IDs de los clientes y el tráfico se segrega en diferentes VLANs.

La figura 18 es un ejemplo donde el tráfico 802.1Q es enviado usando EoMPLS sobre una red MPLS. Para soportar la tunelización 802.1Q en una topología donde un dispositivo de capa 2 se conecta a una red MPLS a través de un conmutador funcionando como PE-CLE, el puerto LAN en el PE-CLE que recibe el tráfico encapsulado 802.1Q (PE1) es configurado como un puerto túnel que acepta tráfico en la VLAN 100. En PE1, la interface es configurada para EoMPLS basado en puerto, con PE2 como la dirección IP de destino.

Cuando los paquetes de las VLANs 10 a 50 llegan al puerto desde CE1, estas son encapsuladas dentro de la VLAN 100 y enviados al puerto de salida de PE1 que está conectado a la red MPLS. En el puerto de salida, una etiqueta MPLS es agregada al encabezado del cuadro antes de que este sea mapeado a un VC y enviado al siguiente PE-CLE (PE2).

Figura 18. **Red EoMPLS**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 76.

En la implementación de Cisco, por medio de los comandos *MPLS l2transport route o xconnect* aplicados a una VLAN para EoMPLS basado en VLAN en un puerto Ethernet para EoMPLS basado en puerto, puede configurarse un túnel para enviar tráfico, basado ya sea en la VLAN cliente o en un puerto Ethernet.

- Para enviar tráfico encapsulado como 802.1Q a través del Core MPLS a un destino específico en el otro lado de la red MPLS, se configura EoMPLS basado en puerto.
- Para enviar tráfico encapsulado como 802.1Q desde un dispositivo de acceso a un router PE, se configura EoMPLS basado en VLAN.

EoMPLS soporta QoS por medio del uso de tres bits experimentales en una etiqueta para determinar la prioridad de los paquetes. Para soportar QoS entre conmutadores de etiquetas de borde (LERs), se usan los bits experimentales tanto en la etiqueta del VC como en la etiqueta de túnel. La clasificación QoS en EoMPLS ocurre en el ingreso, y solo puede hacerse match

con parámetros de capa 3 (tales como IP o DSCP), con parámetros de capa 2 (CoS).

Estas restricciones aplican a EoMPLS:

- En la implementación de Cisco, EoMPLS requiere que al menos uno de los dos puertos ES sea configurado para MPLS. Por lo tanto, si se desea correr EoMPLS en un puerto ES, solo puede configurarse en el puerto ES que no está configurado para MPLS.
- MTU: EoMPLS no soporta la fragmentación y el reensamblado. Por lo tanto, unidad máxima de transmisión (MTU) de todos los *links* intermedios entre los *endpoints* debe de ser suficiente para llevar VLAN Capa 2 más larga recibida. Los routers PE de ingreso y de egreso deben de tener el mismo valor de MTU.
- Formato de la dirección: todas las direcciones *loopback* en los *routers* PE deben de estar configuradas con máscaras de 32 bits para asegurar la operación adecuada del MPLS. OSPF requiere el uso de direcciones *loopback*.
- Formato del paquete: EoMPLS soporta paquetes VLAN 802.1Q. La encapsulación ISL no está soportada entre *routers* PE y CE.
- El número máximo de VLANs usando EoMPLS en un conmutador es 1005.

Restricciones de conexión en capa 2:

  - No puede tenerse una conexión en capa 2 directa entre dos *routers* PE con EoMPLS.
  - No se puede tener más de una conexión capa 2 entre *routers* si esos *routers* están configurados para transportar VLANs Ethernet

a través del *backbone* MPLS. Añadir una segunda conexión capa 2 causa que *el spanning-tree* cambie de estado constantemente si se deshabilita en el enrutador *peer*.

- Restricciones en troncales:

  - Para soportar los BPDUs de *spanning-tree* en Ethernet a través de en un backbone EoMPLS, debe deshabilitarse el *spanning-tree* para la VLAN que lleva EoMPLS. Esto asegura que las VLANs EoMPLS son transportadas únicamente en la troncal que lleva al conmutador del cliente.
  - La VLAN nativa de una troncal no puede ser una VLAN EoMPLS.

- EoMPLS puede habilitarse en interfaces 8021.Q usando los comandos *MPLS l2transport route o xconnect* solo en equipos Cisco.
- No puede configurarse mapeo de VLANs en una interface configurada para EoMPLS.
- No debe configurarse EoMPLS en una interface de VLAN privada.

3. FUNDAMENTOS DE LAS TECNOLOGÍAS PBB

Recientemente han aparecido algunas tecnologías para el transporte de servicios Carrier Ethernet. Una de estas nuevas tecnologías, PBB-TE (*Provider Backbone Bridging – Traffic Engineering*), resuelve varios de los problemas que surgen para la ampliación nativa de los servicios Ethernet en la red de un proveedor. Hasta ahora, otras tecnologías como laconmutación por etiquetas multiprotocolo (MPLS), vista en el capítulo anterior, han sido necesarias para la construcción de redes de gran escala. Sin embargo, muchos operadores están buscando activamente redes Ethernet nativas que reduzcan los costos operativos y de capital y, al mismo tiempo, les permitan ofrecer una amplia gama de aplicaciones y servicios actuales y futuros de forma eficiente.

Debido a su ubicuidad y facilidad de uso, Ethernet, bajo la forma de PBB-TE, se posiciona para capitalizar esta gran oportunidad de suministro y transporte de servicios Carrier Ethernet.

3.1. Servicios Carrier Ethernet

El sector de las telecomunicaciones ha experimentado la continua erosión de tecnologías tradicionales como, por ejemplo, *frame relay* (FR) y la multiplexión por división de tiempo (TDM), que se han visto sustituidas por un nuevo tipo de Ethernet denominado Carrier Ethernet. De acuerdo con la definición de *Metro Ethernet Forum* (MEF), Carrier Ethernet incluye, gracias a la influencia de los proveedores de servicios, cinco atributos específicos que marcan la diferencia respecto del Ethernet tradicional de categoría empresarial. Estos atributos son:

- Servicios estandarizados
- Calidad de servicio (QoS)
- Administración de servicio
- Fiabilidad
- Escalabilidad

La transición de arquitecturas de ruteo y complejos protocolos a un método más fácil de usar basado en conmutadores, tiene ventajas en el suministro de los servicios Carrier Ethernet; pero también tiene algunos inconvenientes, especialmente en el área de la escalabilidad y fiabilidad. PBB-TE se ha desarrollado para resolver estas deficiencias.

3.2. Limitaciones de escalabilidad del Ethernet tradicional

Las redes basadas en conmutadores de Ethernet tradicional tienen dos características definitorias que limitan su tamaño topológico: el aprendizaje *("learning")* y la prevención de bucles. Cuando un conmutador o *switch* recibe un paquete y desconoce si está destinado a una estación terminal (tal como una PC), el conmutador replica el paquete en todos los enlaces a los cuales el paquete está conectado (esto se conoce como *flooding* = inundación). A medida que el conmutador inspecciona cada paquete que recibe, puede recordar o aprender la asociación de las estaciones de envío y los enlaces entrantes. Cada conmutador del dominio de la capa 2 aprende la dirección y el enlace asociado para cada dispositivo de la red.

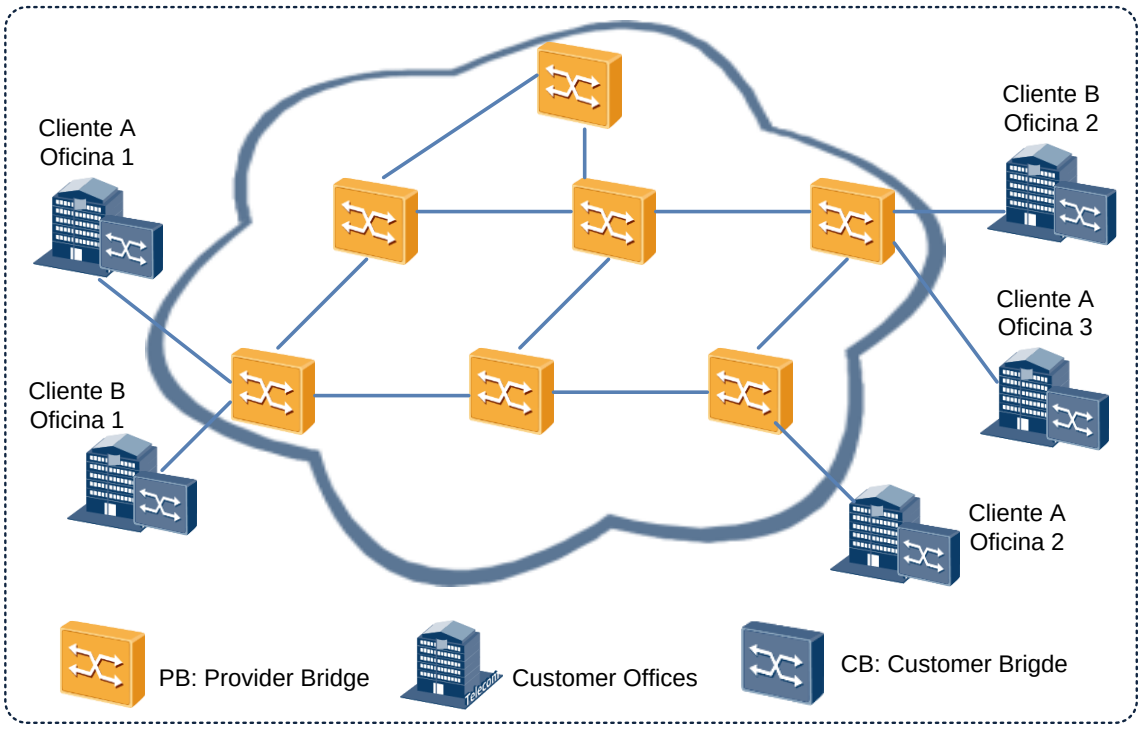
Si bien es cierto que muchos dispositivos de core y metropolitanos pueden soportar centenares de miles de direcciones, esto significaría que si cada dispositivo de la red de un proveedor debe gestionar este número de direcciones, el costo sería prohibitivo y afectaría los modelos de conmutación

de protección. Cuando un enlace o dispositivo experimenta una falla, la red debe reaccionar a este cambio en topología. Comúnmente, a medida que el número de direcciones aumenta, el tiempo de conmutación y restauración de la conectividad de la red también se incrementa.

Una alternativa es instalar routers que segmenten la red de capa 2 en varias subredes (*subnets*). Además de proporcionar un nivel de jerarquía, el enrutamiento también utiliza diversos protocolos complejos y de complicado funcionamiento como, por ejemplo, el Protocolo Border Gateway (BGP). El enrutamiento también requiere una configuración y operación más sofisticada, costoso hardware y procesadores más veloces. Además, el enrutamiento no ofrece el mismo nivel de transparencia de servicios que el transporte de servicios Ethernet basado en conmutadores. Por estas razones, se han dedicado recursos para la mejora de algunos aspectos de las redes Ethernet basadas en la conmutación.

Como se mencionó anteriormente, las redes de capa 2 inundan automáticamente de tráfico los destinos desconocidos. Muchas topologías en malla, estrella o anillo contienen bucles físicos en forma de conexiones redundantes y algunas veces inadvertidas entre dispositivos. Estos bucles se deben prevenir lógicamente para permitir que el tráfico de inundación (*flooding*) se propague inadecuadamente a través de la red. Si los bucles se mantienen, el tráfico de inundación se replicaría y multiplicaría, causando estragos en la red. Por estos motivos, y a fin de detectar y eliminar estos bucles, se inventaron los protocolos STP (*Spanning Tree Protocol*) y sus mejoras posteriores como MSTP (*Multiple STP*) y RSTP (*Rapid STP*).

Figura 19. **Red PB (Provider bridge)**

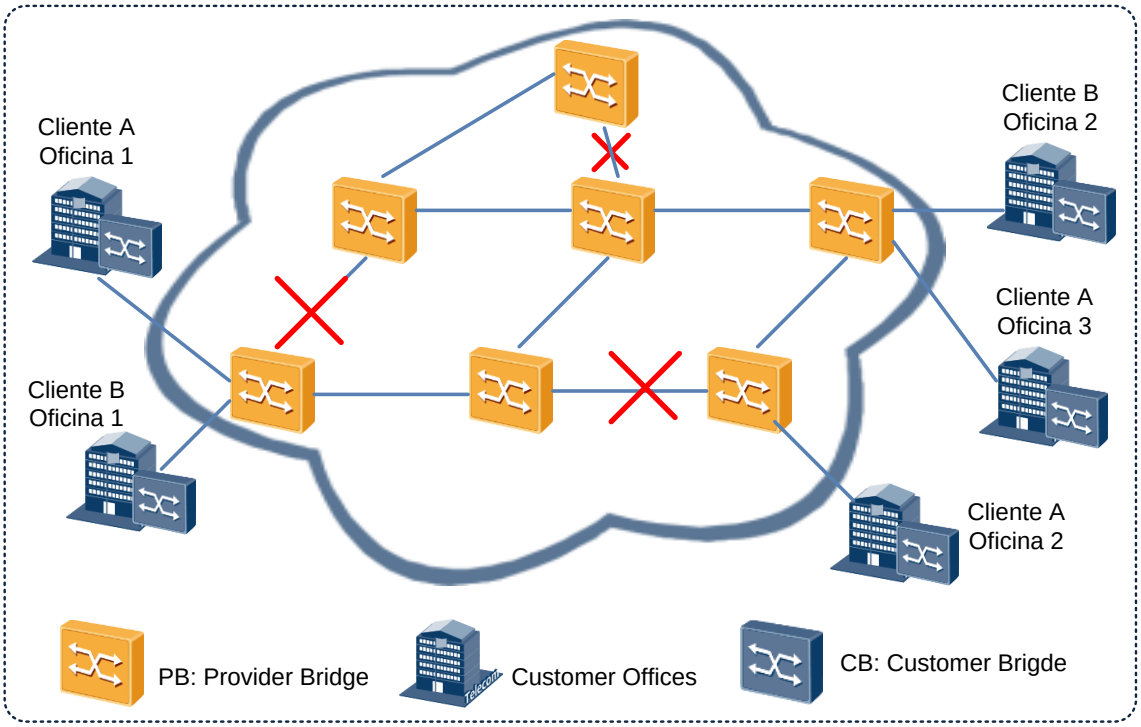


Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 81.

La figura 19 muestra una red de un proveedor en configuración mallada que interconecta varios dispositivos Ethernet basados en conmutadores o *switches*, denominados PB (*Provider Bridges*), y que están bajo control del proveedor. Estos dispositivos admiten una o más tecnologías de transporte de servicios Ethernet, tales como el estándar IEEE 802.1ad PB. Como se muestra en la figura 19, la topología física proporciona cierta redundancia, pero la misma contiene varios bucles. La figura 20 muestra la misma red del proveedor con la facilidad IEEE 802.1w RSTP detectando los bucles y bloqueando de forma lógica algunos enlaces. Ahora ya no hay bucles en la red.

El *flooding* y el *learning* de esta red basada en conmutadores se llevan a cabo de forma normal. Los enlaces bloqueados permanecen en espera en caso de que un enlace o dispositivo activo experimente una falla.

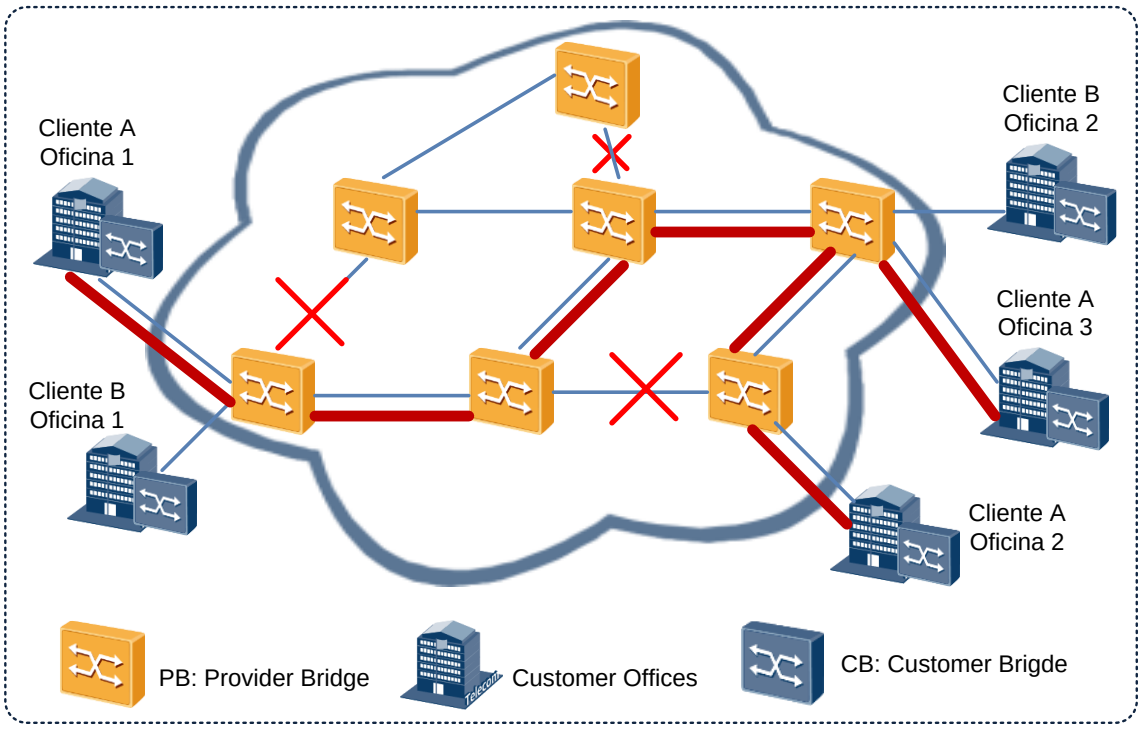
Figura 20. **Red PB con RSTP actuando para evitar bucles**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 82.

La figura 21 muestra la ruta que puede seguir un servicio tipo Carrier Ethernet a través de la red del proveedor. Los enlaces bloqueados RSTP son evitados y todas las ubicaciones del cliente se encuentran interconectadas.

Figura 21. **Carrier Ethernet mediante PB IEEE 802.1ad.**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 83.

En redes de proveedores de una escala moderada es posible usar RSTP y MSTP, pero algunos operadores se muestran escépticos sobre su rendimiento durante situaciones de falla. Las grandes redes deben administrar muchos más enlaces y direcciones MAC (control de acceso a los medios), limitando la capacidad del RSTP y MSTP. Los operadores quieren minimizar (y si es posible, evitar) las fuentes de interrupción de servicio. PBB-TE representa un método para resolver estas preocupaciones.

3.3. Provider Bridge – IEEE 802.1ad

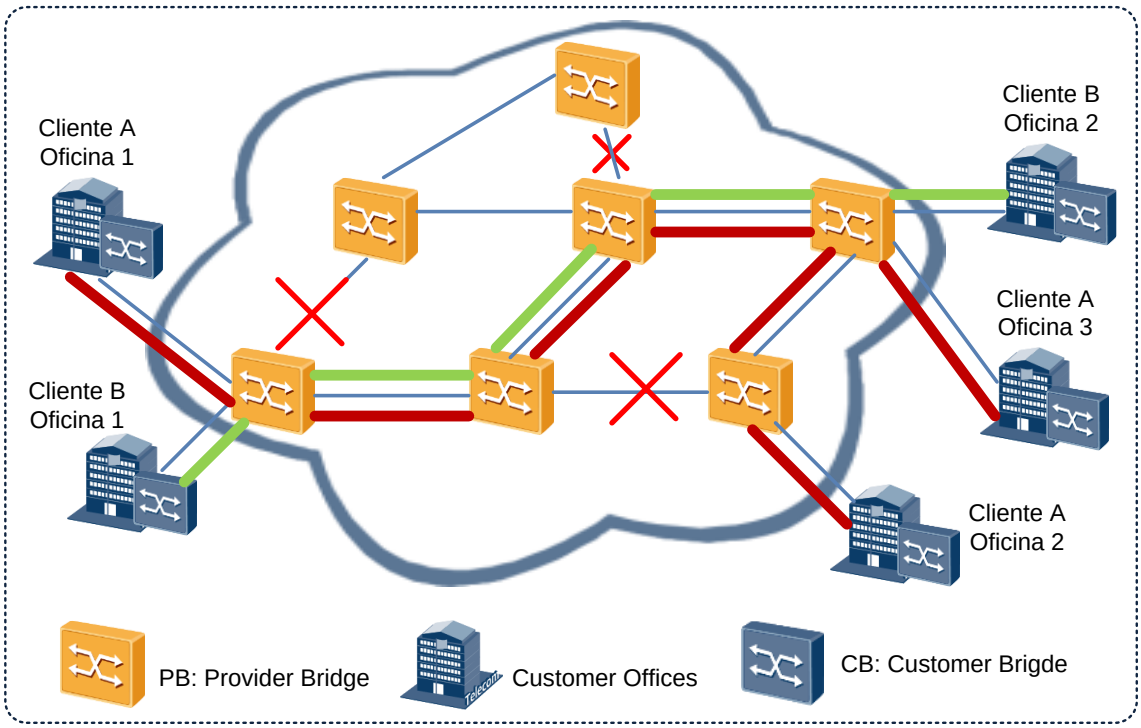
Una motivación para implementar redes privadas virtuales de capa 2 (VPN L2) ha sido la demanda de los clientes para la interconexión de varias ubicaciones. Los clientes quieren servicios de redes de área local (LAN) económicos, transparentes y de alto rendimiento. Además, la mayoría no quiere la complejidad adicional que impone la configuración de *switches* o *routers*. Los clientes también se resisten a intercambiar las tablas de enrutamiento con los proveedores por razones de seguridad y complejidad operativa. Cada vez más, quieren usar Ethernet, en su forma nativa, para interconectar sus ubicaciones.

La conexión de dos ubicaciones crea un servicio Ethernet-Line (E-Line) que utiliza una conexión virtual Ethernet (EVC) punto a punto. Los clientes con más de dos ubicaciones buscan una interconexión de ubicaciones múltiples y podrían elegir un servicio E-LAN que admite circuitos virtuales Ethernet (EVC) multipunto a multipunto.

Finalizado en diciembre de 2005, el IEEE 802.1ad PB es el primer proyecto de bridging Ethernet creado expresamente para las redes de los proveedores de servicios. PB, como normalmente se conoce, estandariza el uso de varias etiquetas de red virtual privada (VLAN) en la misma trama.

Los campos existentes de la trama del cliente son mantenidos, lo que permite que el rango completo de una VLAN 4K de un cliente se transporte de modo transparente a través de una red PB a todas sus otras ubicaciones. Como se muestra en la figura 22, el Cliente A interconecta tres ubicaciones mediante un servicio E-LAN. El Cliente B conecta dos ubicaciones con un servicio E-Line. Ambas técnicas proporcionan VPN L2 seguras y transparentes a través de la red PB.

Figura 22. **VPN L2 mediante una red PB**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software.* p. 85.

Cada VPN L2 permite la separación completa de los clientes. Ambos clientes tienen la libertad de usar VLANs internas de cliente (C-VLAN) a su elección. El proveedor puede configurar hasta cuatro mil VLANs de servicio (S-VLAN) con capacidad para admitir un máximo de cuatro mil clientes de forma separada. A menudo, el máximo de cuatro mil VLANs no es el factor que limita al proveedor. Más bien, el número agregado de direcciones MAC y/o las demandas de la topología física que se plantean a los protocolos RSTP y MSTP, fuerzan al proveedor a segmentar o usar facilidades alternativas de transporte, como puede ser PBB-TE.

3.4. Calidad de servicio de la red PB

Aunque la topología y el escalamiento de direcciones son problemas importantes, un desarrollo crucial en IEEE 802.1ad PB es la inclusión de las capacidades de elegibilidad de descarte y marcado de paquetes. En lugar de la interpretación fija del campo de prioridad de 3 bits que se usa en el estándar anterior IEEE 802.1Q VLAN, PB permite una variedad de codificaciones PCP (*Priority Code Point*). Es posible elegir cuatro distintas interpretaciones de prioridad/descarte. Por ejemplo, 6P2D ofrece seis clases de servicios, con dos de estas clases soportando el marcado elegible de descarte (en amarillo).

La tabla II muestra el uso de PCP y los campos de elegibilidad de descarte.

Tabla II. **IEEE 802.1ad PCP y uso de elegibilidad de descarte**

IEEE 802,1ad Priority Code Point, Uso de elegibilidad de descarte																	
		7	7DE	6	6DE	5	5DE	4	4DE	3	3DE	2	2DE	1	1DE	0	0 DE
PCP, DE	8P8D	7	7	6	6	5	5	4	4	3	3	2	2	1	1	0	0
PCP	8P0D	7	7	6	6	5	5	4	4	3	3	2	2	1	1	0	0
	7P1D	7	7	6	6	5	4	5	4	3	3	2	2	1	1	0	0
	6P2D	7	7	6	6	5	4	5	4	3	2	3	2	1	1	0	0
	5P3D	7	7	6	6	5	4	5	4	3	2	3	2	1	0	1	0

Fuente: elaboración propia.

Este código de colores de la capa 2 permite la aplicación de mecanismos eficientes para gestionar las congestiones sin necesidad de inspeccionar la

información de encabezamiento de la capa 3. La tabla III ofrece un análisis de las ventajas y limitaciones de PB, que se puede usar para hacer una comparación con PBB-TE.

Tabla III. **Ventajas y limitaciones de PB**

Ventajas	Limitaciones
Plano de datos: - Transparencia del rango completo C-VID 4k. - Capacidad para determinar la elegibilidad de descarte de la Capa 2. - PCP de servicio asignado por un proveedor o determinado por C-Tag. - Compatibilidad nativa con servicios E-LAN. **Plano de control:** - Separación de los dominios de control de cliente y proveedor. - Todos los protocolos de la capa 2 de cliente se transportan a través de la red del proveedor.	**Plano de datos:** - Servicios 4K. - Topología restringida por el número de dispositivos conectados agregados. - Los dispositivos PB aprenden todas las direcciones MAC de cliente y proveedor. - Las direcciones MAC de cliente se exponen en la red del proveedor. - Identificador de servicio derivado del puerto entrante y C-VID. **Plano de control:** - Capacidad de la red del proveedor por debajo del nivel óptimo debido a la prevención de bucles RSTP/MSTP.

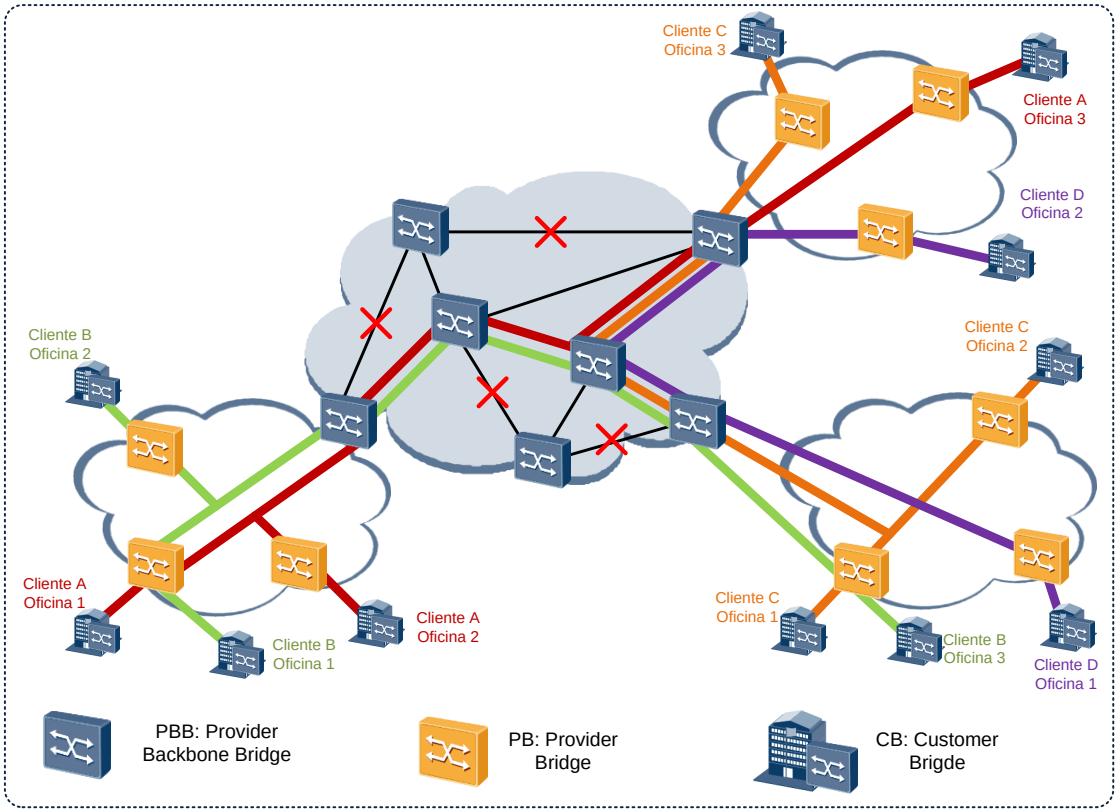
Fuente: elaboración propia.

Las preocupaciones relacionadas con los problemas inherentes a la escalabilidad se están resolviendo mediante las prometedoras técnicas de encapsulado de encabezamiento MAC.

3.5. Provider backbone bridge – PBB

En los últimos años, se ha hecho evidente que Ethernet se impondrá definitivamente en las implementaciones de acceso y metropolitanas. En un principio, MPLS se consideró como la opción más viable para la interconexión de redes PB, pero luego apareció PBB. A diferencia de MPLS, PBB usa el encapsulado de encabezamiento MAC para resolver los posibles problemas de escalabilidad de servicios y direcciones MAC. La figura 23 muestra una red PBB típica.

Figura 23. **Red PBB**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 87.

La trama PB original se mantiene intacta. Cada uno de los campos, empezando con C-DA (dirección de destino de cliente) y C-SA (dirección de origen de cliente), se transportan a través de la red PBB sin modificación. Más importante aún, estas direcciones de cliente no son aprendidas por los dispositivos del core, lo que reduce el costo y la complejidad del equipamiento PBB.

La Tabla IV ofrece un análisis de las ventajas y limitaciones de PBB.

Tabla IV. **Ventajas y limitaciones de PBB**

Ventajas	Limitaciones
Plano de datos: - 16M servicios. - Transparencia de múltiples rangos S-VID 4K. - Las direcciones MAC de cliente se tunelizan en la red del proveedor, mejorando la seguridad y escalabilidad. Plano de control: - Separación de los dominios de cliente, proveedor y backbone. - Los protocolos de control de cliente y PB de capa 2 se transportan a través de la red PBB.	Plano de control: - Los dispositivos PBEB (*Provider Backbone Edge Bridge*) aprenden todos los dispositivos PBB y las direcciones MAC de cliente en tránsito. - Diámetro PBB limitado por restricciones RSTP/MSTP. Plano de control: - Menor capacidad de la red PBB debido a la prevención de bucles RSTP/MSTP.

Fuente: elaboración propia.

3.6. PBB-TE (IEEE 802.1Qay-2009)

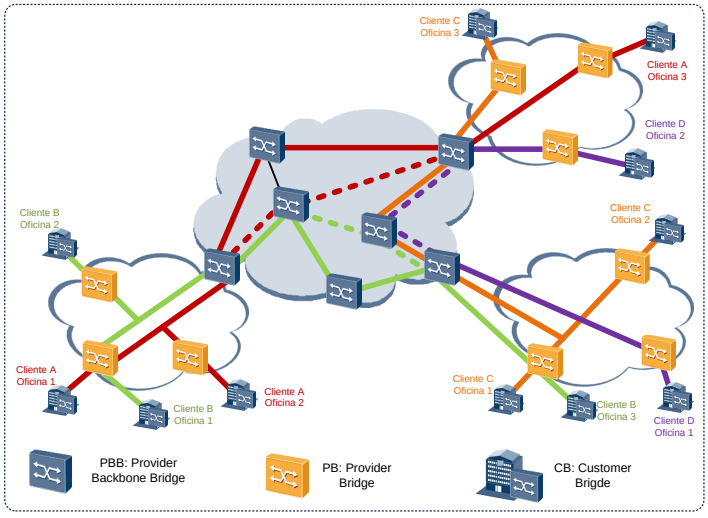
PBB-TE (*Provider Backbone Bridging - Traffic Engineering*) ha llegado para resolver las limitaciones relacionadas con la escalabilidad y la fiabilidad. PBB-TE puede implementarse en lugar de PBB o puede ejecutarse en paralelo. En ambos casos, PBB-TE elimina la necesidad de llevar a cabo el *learning* y el

flooding de los dispositivos de core del backbone. En su lugar, se aprovisionan túneles punto a punto para el transporte de las VPN L2 mediante una sofisticada plataforma de administración. En lugar de usar RSTP/MSTP para prevenir los bucles, la plataforma de administración aplica ingeniería de tráfico a la red PB para utilizar una capacidad considerablemente mayor:

La figura 24 muestra la mayor utilización de la red de backbone con PBB-TE habilitado. Se aprovisionan rutas o túneles principales y de respaldo.

Mediante la IEEE 802.1 se ha iniciado un proyecto para estandarizar esta popular e innovadora tecnología de transporte. Un estándar internacional fomentará el soporte y la interoperabilidad entre los fabricantes. La IEEE 802.1Qay utilizará el actual formato de trama IEEE 802.1ah PBB sin modificaciones, lo que se mostrará más adelante.

Figura 24. **Red de transporte PBB**

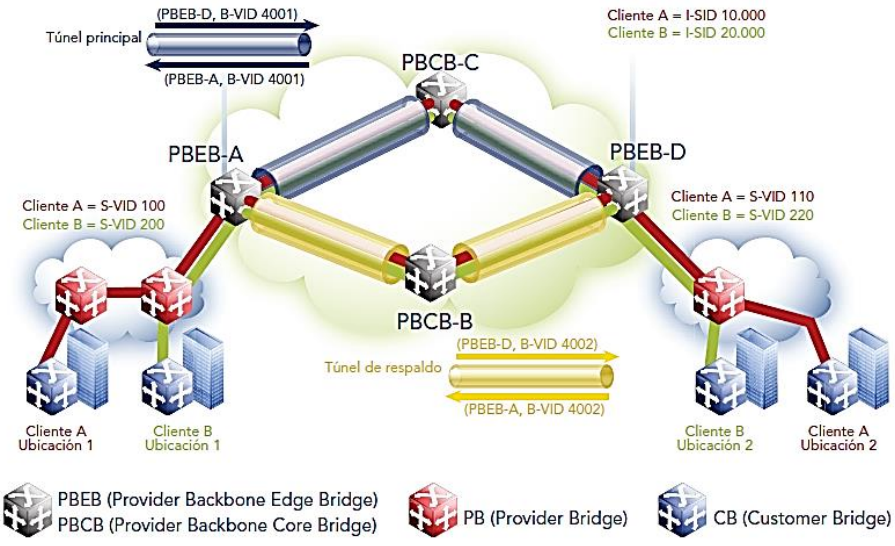


Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 89.

La figura 25 muestra dos redes PB interconectadas con una red PBB-TE. Dos VPN L2 de cliente aparecen atravesando los túneles PBB-TE principal y de respaldo a través de la red de Core.

El tráfico del cliente A (rojo) se origina en la ubicación 1. El PB encapsula el tráfico de cliente agregando una S-Tag que contiene un valor S-VID configurado de 100 reservado para el cliente A dentro de su dominio. El tráfico se envía al PB Edge Bridge A (PBEB-A). El PBEB-A ha sido configurado para asignar al tráfico del cliente A (S-VID=100) un valor I-SID (*Instance Service Identifier*) de 24 bits de 10000. El mismo valor I-SID se asocia con los túneles PBB-TE principal y de respaldo. Cada túnel principal y de respaldo se identifica mediante la combinación de una dirección MAC de destino PBEB y un B-VID (Backbone-VID).

Figura 25. **Túneles principal y de respaldo PBB-TE**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 90.

Esto representa una importante diferencia entre PBB-TE y PBB. Recuerde que con PBB, los B-VID representan los dominios de *flooding* que interconectan varias redes PB. Con PBB-TE, los B-VID junto con los B-DA definen el túnel.

En este caso, el PBEB-A encapsula el tráfico S-VID 100 agregando un valor B-DA de PBEB-D, un valor B-SA de PBEB-A, un valor B-VID de 4001 (túnel principal o púrpura) y el valor I-SID de 10000. Este tráfico con encapsulado de encabezamiento MAC se envía al PB Core Bridge-C (PBCB-C). PBCB-C se ha configurado para que no aprenda o inunde el tráfico en B-VID 4001, que se ha reservado para el uso de PBB-TE. El hecho de que PBB-TE no haga el *learning* o el *flooding* es un punto importante. Cada dispositivo PBCB se debe aprovisionar con entradas de la base de datos de envío a fin de que el tráfico se reenvíe adecuadamente dentro de los túneles.

La tabla de envío PBCB-C contiene una entrada para {PBEB-D, B-VID 4001} y el tráfico se envía al puerto específico en la dirección del PBEB-D.

PBEB-D recibe el tráfico y elimina el encapsulado del encabezamiento MAC. Dado que los valores S-VID sólo son localmente significativos por red PB, un proveedor tiene la flexibilidad de convertir el valor S-VID. En este caso, PBEB-D se ha configurado para asociar I-SID 10000 con S-VID 110. En la ilustración 15, el tráfico del túnel se desencapsula y S-VID se reasigna con el valor de 110. El tráfico se reenvía al PB adjunto al cliente A, ubicación 2. El dispositivo PB elimina la encapsulación S-Tag y la trama de cliente original de la ubicación 1 se suministra a la ubicación 2.

Un sistema de administración preconfigura los túneles PBB-TE principal y de respaldo. Esto permite al operador aplicar ingeniería de tráfico de acuerdo

con la ruta, el ancho de banda y los requerimientos del servicio. Los clientes y los servicios se asocian con los túneles teniendo en cuenta los requerimientos de ancho de banda para la velocidad de información concertada (CIR) y la tasa de información sobrante (EIR). Los túneles se supervisan a través del uso de mensajes de prueba de continuidad (CCM) de administración de errores de conectividad (CFM) IEEE 802.1ag. CCM controlan que las tramas se envíen y reciban cada pocos milisegundos a través de los túneles PBB-TE.

Si el túnel principal experimenta una falla, los extremos del túnel empiezan a usar automáticamente el túnel de respaldo. Las entradas de la base de datos de envío se preconfiguran a lo largo de la ruta de respaldo para minimizar los tiempos de conmutación y restauración en caso de falla.

La tabla V ofrece un análisis de las ventajas y limitaciones de PBB-TE.

De forma ocasional, los servicios se ven afectados por fallas *"soft".* Una falla "*soft"* suele consistir en errores de configuración u otros errores cometidos por el operador. Por ejemplo, es posible que el administrador deshabilite un conjunto de VID en un dispositivo específico o puerto. En una inspección inicial, algunas técnicas de solución de problemas pueden llegar a la conclusión de que el puerto está activo y que otro tráfico pasa normalmente, lo que puede llevar al operador a buscar el problema en el lugar equivocado.

Un proyecto propuesto en IEEE 802.1 resuelve estos errores de configuración. Se denomina CFM dependiente de datos. Estos avances mejorarán aún más la capacidad de las tecnologías de transporte Carrier Ethernet, como PBB-TE, para ofrecer menores costos de operación y una mejor resistencia.

3.7. Formación de la trama PBB-TE

Para aumentar la aceptación de Ethernet como tecnología carrier, fueron necesarios unos cuantos cambios para hacer que el estándar fuera interesante para aplicaciones metropolitanas. A continuación se detallan las varias adiciones que fueron aplicadas a Ethernet para llegar a PBB-TE. Se empieza mostrando nuevamente el formato de trama 802.1Q VLAN para lograr mayor claridad.

Tabla V. **Ventajas y limitaciones de PBB-TE**

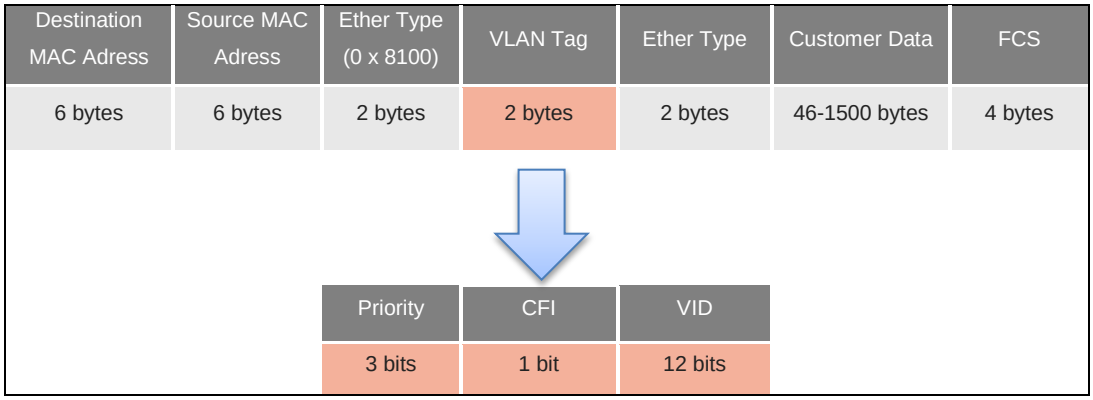
Ventajas	Limitaciones
Plano de datos: - Servicios 16M. - Transparencia de múltiples rangos S-VID 4K. - No hay aprendizaje *("learning")* o inundación (*Flooding*") en la red de Core. - Las direcciones MAC de cliente se tunelizan en la red del proveedor, mejorando la seguridad y la escalabilidad. - Máxima utilización de la red de núcleo con las rutas modeladas por ingeniería. Plano de control: - Separación de los dominios de control de cliente, proveedor y *backbone*. - Los protocolos de control de cliente y PB de capa 2 se transportan a través de la red PBB. - CCM 802.1ag supervisa los túneles principal y de respaldo.	Plano de datos: - Los dispositivos PBEB aprenden todas las direcciones MAC de Backbone y de cliente en tránsito. Plano de control: - Sofisticado sistema de administración para aprovisionar túneles de núcleo.

Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 84.

3.7.1. 802.1Q: VLAN

Virtual Local-Area Network (VLAN), definido en el estándar 802.1Q, usa etiquetas de VLAN (VLAN tags), que son usados por *switches* para diferenciar tráfico con un rango entre 0 y 4095. Esto permite funciones de QoS y de separación de tráfico en un medio compartido.

Figura 26. **IEEE 802.1Q**



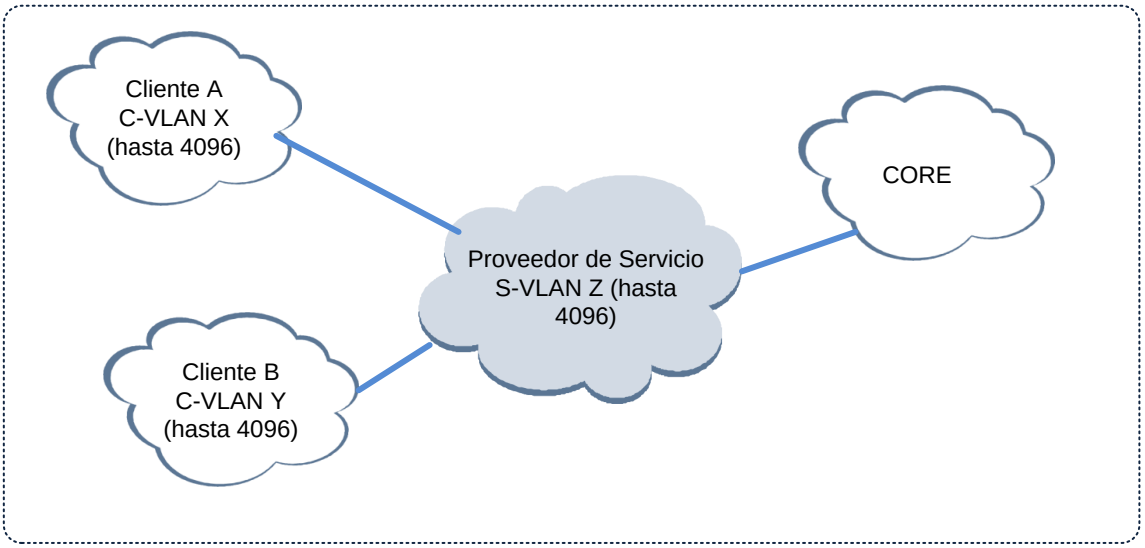
Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 91.

3.7.2. 802.1ad: Provider Bridge

Las etiquetas de VLAN tienen un máximo de 4096 IDs, que es suficiente para LANs, pero no suficiente para carriers con múltiples rutas y clientes. Para mejorar la escalabilidad de VLANs, Provider Bridge (también conocido como Q-in-Q) define etiquetas apiladas (*stacked tags*). Una etiqueta adicional es insertada en un cuadro previamente etiquetado, creando una etiqueta interna y otra externa. Esto permite a los carrier añadir etiquetas específicas a sus redes sin modificar la etiqueta que ya está en el cuadro insertado por el proveedor de servicio.

Figura 27. **IEEE 802.1ad**

Dest. MAC Adress	Source MAC Adress	Ether Type 0x8100 0x9200	S-VLAN	Ether Type 0x8100 0x9200	C-VLAN	Ether Type	Custumer Data	FCS
6 bytes	6 bytes	2 bytes	2 bytes	2 bytes	2 bytes	2 bytes	46-1500 bytes	4 bytes



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 92.

3.7.3. 802.1ah: Provider Backbone Bridge (PBB)

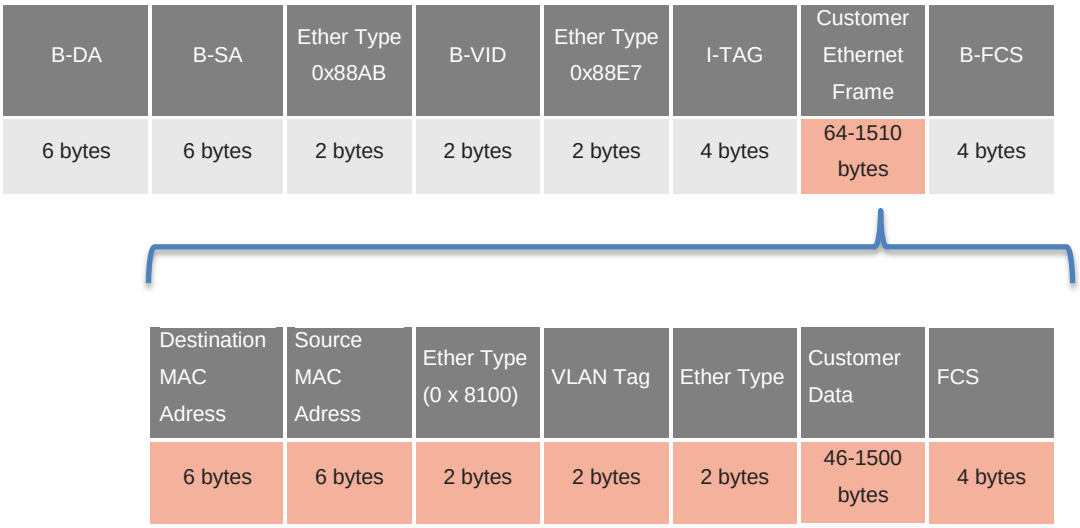
Conforme las redes crecen, los *switches* core necesitan manejar un mayor número direcciones MAC en sus tablas de envío. Combinado con el número limitado de VLANs, esto incrementa la complejidad de las redes.

La propuesta 802.1ah PBB encapsula un cuadro Ethernet de cliente en un cuadro Ethernet de *carrier* o proveedor, completamente con su propio espacio para dirección MAC. Con una red PBB, los paquetes son conmutados de acuerdo a la dirección MAC de destino de *backbone.*

La principal ventaja de esta aproximación es la completa separación de los dominios del carrier y del cliente, permitiendo que los cuadros Ethernet del cliente sean transportados de forma transparente en la red del *carrier*. Esto reduce grandemente la complejidad de las tablas de envío de los *switches*, dado que las entradas están limitadas a los *switches* de la red del *carrier.*

PBB también añade un campo único llamado I-Tag, el cual permite al carrier asignar parámetros QoS y define un identificador único por cliente (I-SID). Por lo tanto, los flujos de tráfico son asignados un I-Tag único por cliente, y el QoS puede hacer por cliente en vez de por VLAN. Además, dado que el I-SID es de 24 bits de longitud, hay hasta dos millones de identificadores de servicio.

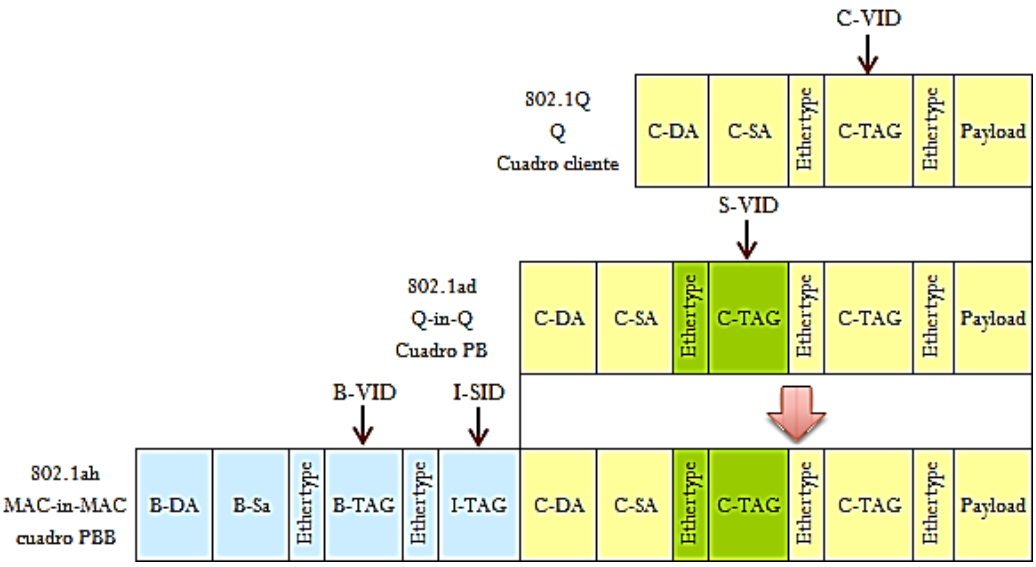
Figura 28. **802.1ah: Provider Backbone Bridge (PBB)**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 93.

La siguiente figura muestra de un modo más explícito el proceso mediante el cual se forma una trama PBB:

Figura 29. **Formación de la trama PBB**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 95.

Los campos usados son los siguientes:

- *Backbone Destination Address* (B-DA): dirección de backbone de destino, representa la dirección del Edge Switch de destino de la red PBB.

- *Backbone Source Address* (B-SA): dirección de *backbone* de origen, representa la dirección MAC del Edge Switch de origen en la red PBB.

- Ether Type (1): indica que una VLAN de *backbone* está presente en el cuadro PBB y tiene el valor de 0x88A8.

- Backbone VLAN ID (B-VID): representa la VLAN ID aplicado al cuadro y es usado para asegurar que los cuadros tomen la ruta apropiada, este campo es opcional.

- Ether type (2): indica el contenido de la carga o *payload*. En este caso, 0x88E7 una carga Ethernet precedida por un I-Tag.

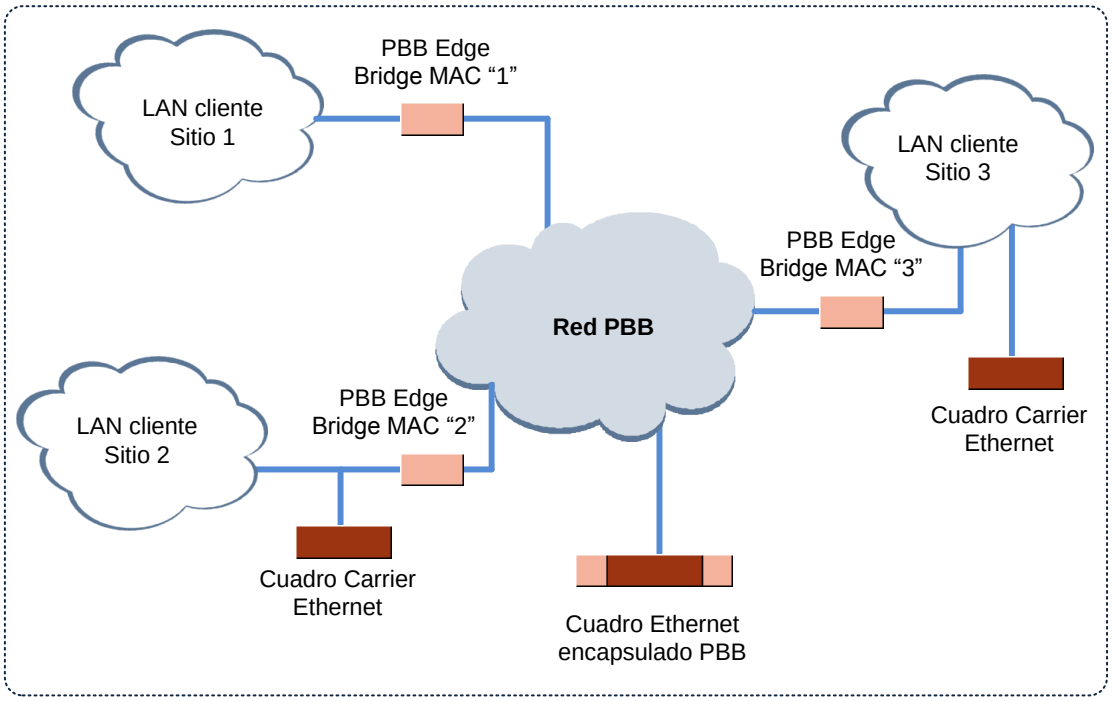
- Instance Tag (I-Tag): es sistemáticamente aplicado a todo cuadro PBB y contiene parámetros de QoS así como el identificador de servicio de 24 bits (SID) usado para identificar de forma única a los clientes.

3.7.4. 801.1Qay: PBB-TE

Este último estándar está basado en la tecnología Nortel conocida como Provider Backbone Transport (PBT). Esencialmente basada en el formato de cuadro PBB, el estándar PBB-TE (*Provider Backbone Bridging - Traffic Engineering*) se concentra en el transporte del cuadro dentro de la red mientras reemplaza el protocolo *Spanning Tree* (*STP*) con un camino orientado a conexión y preestablecido por el usuario mediante ingeniería de tráfico, tal como se discutió previamente en este mismo capítulo.

En el ejemplo de arriba, el *Spanning Tree* está deshabilitado, así que los dispositivos de envío PBB solo necesitan aprender las direcciones MAC en los dispositivos de frontera para transmitir los cuadros apropiadamente.

Figura 30. **Encapsulamiento de una trama Ethernet en una red PBB-TE**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 97.

3.8. Resumen

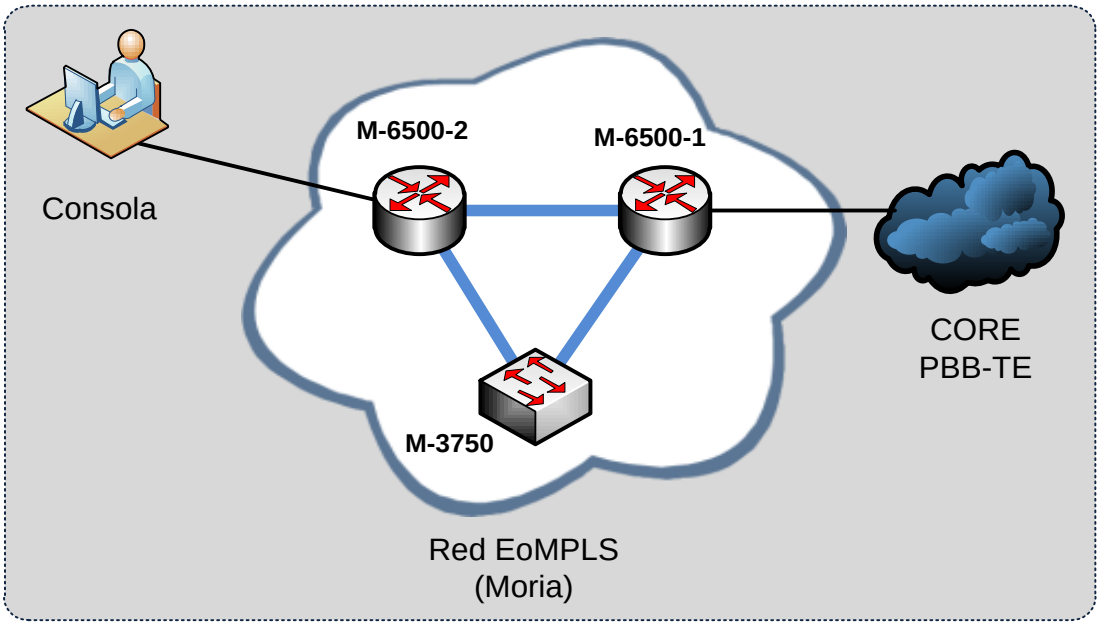
Carrier Ethernet representa una excelente oportunidad en un mercado que se encuentra en una fase de vertiginoso crecimiento. La gran mayoría de proveedores de servicios locales e internacionales y diversos operadores de sistemas están implantando o investigando implementaciones de Carrier Ethernet. A medida que surjan más clientes y servicios, se requerirán tecnologías de transporte de mayor escala. PBB-TE, junto con IEEE 802.1ah PBB, vienen a resolver los retos y superar las limitaciones de las tecnologías tradicionales. PBB-TE y PBB ofrecen alternativas Ethernet nativas a gran escala y alto rendimiento para redes de capa 2 eficientes y transparentes.

4. CONSTRUCIÓN DE UNA RED EOMPLS

4.1. Red MPLS en Moria

A continuación en la figura 31 se muestra un ejemplo de la red de Moria.

Figura 31. **Topología de la red de Moria**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 98.

La red de Moria cuenta con dos *switches* Cisco 6500 con soporte para MPLS, y un Cisco ME3750 con lo cual se configuró una red de pruebas triangular (la red más pequeña que permite probar múltiples trayectorias). Cada Cisco 6500 tenía dos slots SFP (*Small Form-factor Pluggable*) y 4 puertos de 10 Gigabits, mientras que el ME3750 tenía dos puertos GigaEthernet SFP y

2 puertos SFP Enhanced Services (ES) con funcionalidad MPLS. Una computadora portátil se conectó a cada uno de los *switches* para pruebas de ping y análisis de tráfico con *Wireshark.*

El enrutamiento de esta red funciona de modo que:

- iBGP es el protocolo IGP primario.
- iBGP peerings establecidos por medio de direcciones *loopback.*
- OSPF es el protocolo en uso para anunciar estas direcciones *loopback* a través de Core.

Los restantes *routers* y *switches* en la red de Moria (recordemos que esta es una red en producción de una empresa), fueron usados como dispositivos terminales, dado que era posible configurarlos como simples clientes finales (simples dispositivos IP sin etiquetas de VLAN), pero también para actuar, cuando sea necesario, como dispositivos Edge (*Client Edge Devices*).

Se usó el rango de direcciones 10.1.0.0/16, con *loopbacks* de la red 10.1.1.0/24:

Tabla VI. ***Loopbacks***

Loopbacks	10.1.1.0/24
M-3750	10.1.1.1
M-6500-1	10.1.1.2
M-6500-2	10.1.1.3

Fuente: elaboración propia.

Enlaces punto a punto de la red 10.1.2.0/23:

Tabla VII. **Enlaces punto a punto**

Enlaces punto a punto	10.1.2.0/23
M-3750 a M-6500-1	10.1.2.0/30
M-6500-1 a M-6500-2	10.1.2.4/30
M-6500-1 a M-6500-2	10.1.2.8/30
M-6500-2 a M-3750	10.1.2.12/30

Fuente: elaboración propia.

Etiquetas en los siguientes rangos:

Tabla VIII. **Etiquetas**

Switch	Rango
M-3750	101-300
M-6500-1	301-500
M-6500-2	501-700

Fuente: elaboración propia.

4.1.1. Habilitando la conmutación MPLS

En el Cisco 6500 y el ME3750 se habilita globalmente el MPLS usando los siguientes comandos:

```
mpls ip                          ; Habilitada por defecto, pero
                                  ; incluida en caso haya
                                  ; sido deshabilitada previamente

mpls label protocol ldp
```

```
mpls ldp advertise-labels                    ; solo en el ME3750
```

Y luego para cada interface que será parte de la nube MPLS:

```
mpls ip
```

También se usó el comando:

```
mpls label range [X] [Y]              ; X y Y son los valores inferior
                                          ; y superior de las etiquetas
                                          ; usadas por este dispositivo
```

El cual permite asignar rangos únicos a cada *switch* para hacer la depuración (*debugging*) más simple.

Este es un comando opcional:

```
mpls ldp router-id loopback0 force
```

Que se usó para configurar el *router* ID para la interface Loopback0.

Finalmente, se incrementó el tamaño de la MTU de los enlaces entre los routers para lidiar con las etiquetas MPLS añadidas (4 etiquetas por cada nivel de etiquetamiento). Se fijó la MTU de los puertos Giga a 9000 bytes, del siguiente modo:

En el ME3750:

```
system mtu jumbo 9000                    ; después del reinicio
                                             ; aplica a todas las interfaces
```

En los 6500s:

```
system jumbomtu 9000                     ; configurado globalmente para fijar
                                             ; el valor de cuadro jumbo

mtu 9000                                   ; aplicado a todas las interfaces
                                             ; requiere que los cuadros sean jumbo
```

4.1.2. Pruebas locales

Confirmando la configuración MPLS:

```
show mpls ldp neighbor          ; para desplegar que las sesiones
```

```
                                    ; de distribución de etiquetas
                                    ; han sido establecidas y
                                    ; están operativas.

show mpls interfaces                ; para verificar que las
                                    ; interfaces están configuradas
                                    ; para la conmutación de etiquetas

show mpls ldp discovery             ; para desplegar routers
                                    ; descubiertos vía mensajes
                                    ; “hello” de LDP

show mpls forwarding-table          ; para verificar si la tabla
                                    ; de envío de etiquetas
                                    ; ha sido construida correctamente
                                    ; (es decir, para verificar
                                    ; que las etiquetas, redes e interfaces
                                    ; de próximo salto
                                    ; han sido aprendidas como se espera)

ping mpls                           ; para mostrar que
                                    ; los destinos IP están disponibles
                                    ; por medio de conmutación de etiquetas
```

Por ejemplo, en M-6500-1:

```
M-6500-1#  show mpls ldp neighbor

Peer LDP Ident: 10.1.1.3:0; Local LDP Ident 10.1.1.2:0
```

```
        TCP connection: 10.1.1.3.16221 - 10.1.1.2.646
        State: Oper; Msgs sent/rcvd: 49550/49541; Downstream
        Up time: 4w2d
        LDP discovery sources:
                Targeted Hello 10.1.1.2 -> 10.1.1.3, active, passive
                GigabitEthernet3/1, Src IP addr: 10.1.2.10
        Addresses bound to peer LDP Ident:
                10.1.1.3        10.1.2.13       10.1.2.10

Peer LDP Ident: 10.1.1.1:0; Local LDP Ident 10.1.1.2:0
        TCP connection: 10.1.1.1.646 - 10.1.1.2.17038
        State: Oper; Msgs sent/rcvd: 11/12; Downstream
        Up time: 00:01:13
        LDP discovery sources:
                GigabitEthernet1/2, Src IP addr: 10.1.2.1
        Addresses bound to peer LDP Ident:
                10.1.1.1        10.10.9.6       10.1.2.14       10.1.2.1
```

```
M-6500-1# show mpls interfaces

Interface                IP            Tunnel   BGP     Static  Operational
GigabitEthernet1/2       Yes (ldp)     Yes      No      No      Yes
TenGigabitEthernet2/1    Yes           No       No      No      No
GigabitEthernet3/1       Yes (ldp)     Yes      No      No      Yes
```

```
M-6500-1# show mpls ldp discovery

Local LDP Identifier:
```

```
    10.1.1.2:0
    Discovery Sources:
    Interfaces:
        GigabitEthernet1/2 (ldp): xmit/recv
            LDP Id: 10.1.1.1:0
        GigabitEthernet3/1 (ldp): xmit/recv
            LDP Id: 10.1.1.3:0
    Targeted Hellos:
        10.1.1.2 -> 10.1.1.3 (ldp): active/passive, xmit/recv
            LDP Id: 10.1.1.3:0
```

Muestra ambos vecinos como activos pero no envía el enlace de 10 Gbps entre los dos 6500 s (el cual estaba deshabilitado en ese punto).

```
M-6500-1# show mpls forwarding-table

Local  Outgoing    Prefix           Bytes Label   Outgoing    Next Hop
Label  Label       or Tunnel Id     Switched      interface
301    Pop Label   10.1.1.1/32      0             Gi1/2       10.1.2.1
302    Pop Label   10.1.1.3/32      0             Gi3/1       10.1.2.10
305    Pop Label   10.1.2.12/30     0             Gi1/2       10.1.2.1
       Pop Label   10.1.2.12/30     0             Gi3/1       10.1.2.10
```

Finalmente,

```
M-6500-1# ping mpls ipv4 10.1.1.1/32
```

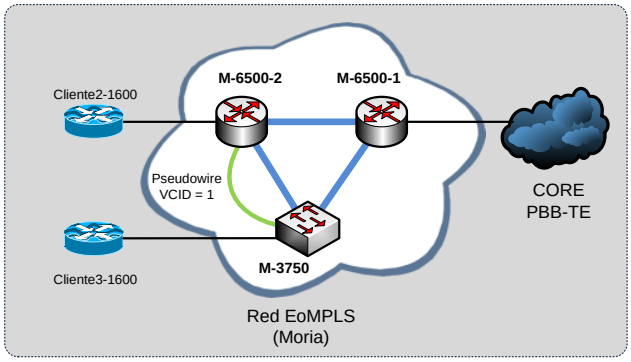
```
        Sending 5, 100-byte MPLS Echos to 10.1.1.1/32,
                timeout is 2 seconds, send interval is 0 msec:

        Codes:      '!' - success, 'Q' - request not transmitted,
                    '.' - timeout, 'U' - unreachable,
                    'R' - downstream router but not target,
                    'M' - malformed request

        Type escape sequence to abort.
        !!!!!
        Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

M-6500-1# ping mpls ipv4 10.1.1.3/32

        Sending 5, 100-byte MPLS Echos to 10.12.1.3/32,
                timeout is 2 seconds, send interval is 0 msec:

        Codes:      '!' - success,  'Q' - request not transmitted,
                    '.' - timeout, 'U' - unreachable,
                    'R' - downstream router but not target,
                    'M' - malformed request

        Type escape sequence to abort.
        !!!!!
        Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

Muestra que la dirección *loopback* de los otros dos *switches* era alcanzable mediante conmutación de etiquetas (*label switching* – esta misma prueba se repitió exitosamente en los otros *swiches)*.

4.1.3. Prueba 1: Pseudowire EoMPLS

Para esta primera prueba, un *router* cliente fue conectado a cada uno de los *switches* M-6500-2 (Gi 3/48) y M-3750 (Fe 1/0/1) de modo que cada uno de los clientes tuviera una única dirección IP sin etiquetado de VLAN de los cuadros en el lado del cliente.

Figura 32. **Pseudowire EoMPLS**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 101.

Del lado del Core, cada una de las interfaces que ven hacia los clientes fue configurada con el comando siguiente:

```
xconnect <IP_ADDRESS> <PSEUDOWIRE_ID> encapsulation mpls
```

En donde IP_ADDRESS era la dirección *loopback* del *switch* en el otro extremo del *pseudowire* EoMPLS y PSEUDOWIRE_ID un entero positivo para identificar el *pseudowire* de forma única para los dos *switches* en cuestión.

Por lo tanto, para esta prueba tiene la configuración:

```
interface GigabitEthernet3/48
      description cliente2-1600 EoMPLS prueba_1
      no switchport
      xconnect 10.1.1.1 1 encapsulation mpls
```

En el *switch* M-6500-2 (donde cliente 2-1600 era un *router* Cisco 1600 conectado a este puerto actuando como cliente),

```
interface FastEthernet1/0/1
      description cliente3-1600 EoMPLS prueba_1
      no switchport
      xconnect 10.1.1.3 1 encapsulation mpls
```

En el *switch* M-3750 (donde cliente3-1600 era un *router* Cisco 1600 conectado en este puerto actuando como cliente).

Una vez configurado primero confirmamos que el *pseudowire* está arriba con los siguientes comandos:

```
show mpls l2transport vc              ; para verificar que el
                                          ; VC ID ha sido usado
                                          ; correctamente y cuál es su estatus

show mpls l2transport binding      ; para ver los detalles
```

```
                                        ; de VC ID
                                        ; para ambos extremos

show mpls forwarding-table          ; para ver que el túnel EoMPLS
                                        ; está arriba, que el LFIB
                                        ; ha sido llenado
                                        ; apropiadamente y que el
                                        ; tráfico está atravesando el
                                        ; pseudowire
                                        ; EoMPLS viendo
                                        ; el incremento del
                                        ; conteo de
                                        ; "Bytes Label Switched"
                                        ; a la entrada del pseudowire

ping mpls pseudowire                 ; ping basado en LSP
                                        ; para confirmar conectividad
                                        ; a través de un pseudowire
                                        ; EoMPLS.
```

Estos comandos dieron las siguientes salidas:

```
M-6500-2# sh mpls l2transport vc

Local intf      Local circuit          Dest address          VC ID          Status
--------------- ---------------------- --------------------- -------------- ----------
Gi3/48          Ethernet               10.1.1.1              1              UP
```

```
M-3750# sh mpls l2transport vc

Local intf      Local circuit          Dest address            VC ID             Status
--------------- ---------------------- ------------------------- ---------------- ----------
Fa1/0/1         Ethernet               10.1.1.3                1                 UP
```

```
M-6500-2#  sh mpls l2transport binding

     Destination Address:  10.1.1.1,       VC ID: 1
          Local Label:  504
               Cbit: 0,       VC Type:  Ethernet,       GroupID: 0
               MTU: 1500,       Interface Desc: cliente2-1600 EoMPLS prueba_1
               VCCV:   CC Type:  RA [2]
                       CV Type:  LSPV [2]

          Remote Label:  101
               Cbit: 0,       VC Type:  Ethernet,       GroupID: 0
               MTU: 1500,       Interface Desc: cliente3-1600 EoMPLS prueba_1
               VCCV:    CC Type:  RA [2]
                       CV Type:  LSPV [2]
```

```
M-3750# sh mpls l2transport binding

     Destination Address:  10.1.1.3,       VC ID: 1
          Local Label:  101
               Cbit: 0,        VC Type: Ethernet,       GroupID: 0
               MTU: 1500,       Interface Desc: cliente3-1600 EoMPLS prueba_1
               VCCV:    CC Type: RA [2]
```

```
                    CV Type: LSPV [2]

          Remote Label:  504
               Cbit: 0,        VC Type: Ethernet,       GroupID: 0
               MTU: 1500,      Interface Desc: cliente2-1600 EoMPLS prueba_1
               VCCV:   CC Type: RA [2]
                       CV Type: LSPV [2]
```

M-6500-2# sh mpls forwarding-table

Local Label	Outgoing Label	Prefix or Tunnel Id	Bytes Label Switched	Outgoing interface	Next Hop
502	Pop Label	10.1.1.1/32	0	Gi1/2	10.1.2.14
503	Pop Label	10.1.1.2/32	0	Gi3/1	10.1.2.9
504	No Label	l2ckt(1)	19462651	none	point2point
506	Pop Label	10.1.2.0/30	0	Gi3/1	10.1.2.9
	Pop Label	10.1.2.0/30	0	Gi1/2	10.1.2.14

M-3750# sh mpls forwarding-table

Local Label	Outgoing Label or VC	Prefix or Tunnel Id	Bytes Label Switched	Outgoing interface	Next Hop
101	No Label	l2ckt(1)	74782997	Fa1/0/1	point2point
104	Pop Label	10.1.1.3/32	4968	Gi1/1/1	10.1.2.13
106	Pop Label	10.1.2.8/30	0	Gi1/1/2	10.1.2.2
	Pop Label	10.1.2.8/30	0	Gi1/1/1	10.1.2.13
107	Pop Label	10.1.1.2/32	0	Gi1/1/2	10.1.2.2

```
M-6500-2# ping mpls pseudowire 10.1.1.1 1

    Sending 5, 100-byte MPLS Echos to 10.1.1.1,
            timeout is 2 seconds, send interval is 0 msec:

    Codes:   '!' - success, 'Q' - request not transmitted,
                '.' - timeout, 'U' - unreachable,
                'R' - downstream router but not target,
                'M' - malformed request

    Type escape sequence to abort.
    !!!!!
    Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
M-3750# ping mpls pseudowire 10.1.1.3 1

      Sending 5, 100-byte MPLS Echos to 10.1.1.3,
            timeout is 2 seconds, send interval is 0 msec:

      Codes: '!' - success, 'Q' - request not sent, '.' - timeout,
                'L' - labeled output interface, 'B' - unlabeled output interface,
                'D' - DS Map mismatch, 'F' - no FEC mapping, 'f' - FEC mismatch,
                'M' - malformed request, 'm' - unsupported tlvs, 'N' - no label entry,
                'P' - no rx intf label prot, 'p' - premature termination of LSP,
                'R' - transit router, 'I' - unknown upstream index,
                'X' - unknown return code, 'x' - return code 0

      Type escape sequence to abort.
      !!!!!
      Success rate is 100 percent (5/5), round-trip min/avg/max = 1/5/9 ms
```

Lo cual indica que el *pseudowire* está arriba y corriendo.

4.1.3.1. Conectividad hacia el borde

Para la primera prueba, se verificó la conectividad mutua de los dos clientes en el borde por medio de los siguientes comandos:

```
show cdp neighbors          ; para mostrar que los dispositivos
                            ; pueden verse en Capa 2

ping <IP ADDRESS>           ; para verificar que los dispositivos
                            ; pueden intercambiar tráfico ICMP

show ip arp                 ; para verificar que la dirección a la que
                            ; se hace ping está en el otro extremo
                            ; del pseudowire EoMPLS en vez de
                            ; conectada directamente al
                            ; dispositivo fuente del ping
                            ; verificando la dirección
                            ; MAC correcta
```

Estos comandos ejecutados en los clientes en el borde mostraron que el *pseudowire* EoMPLS está funcionando:

```
cliente3-1600# show cdp neighbors

Capability Codes:   R - Router, T - Trans Bridge, B - Source Route Bridge
                    S - Switch, H - Host, I - IGMP, r - Repeater
```

```
Device ID                 Local Intrfce     Holdtme    Capability  Platform  Port
ID
cliente2-1600             Fas 0/0           178           R            2621       Fas
0/0
```

```
cliente2-1600# show cdp neighbors

Capability Codes:    R - Router, T - Trans Bridge, B - Source Route Bridge
                              S - Switch, H - Host, I - IGMP, r - Repeater

Device ID                 Local Intrfce     Holdtme    Capability  Platform
Port ID
cliente3-1600             Fas 0/0           136           R            1760
Fas 0/0
```

```
cliente2-1600# ping 192.168.0.1

    Type escape sequence to abort.
    Sending 5,  100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
    !!!!!
    Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms

cliente2-1600# sh ip arp
    Protocol  Address          Age (min)  Hardware Addr   Type   Interface
    Internet  192.168.0.1            19   0014.a81f.e924  ARPA   FastEthernet0/0
    Internet  192.168.0.2             -   0030.85e7.c0a0  ARPA   FastEthernet0/0
```

```
cliente3-1600# ping 192.168.0.2

    Type escape sequence to abort.
    Sending 5, 100-byte ICMP Echos to 192.168.0.2, timeout is 2 seconds:
    !!!!!
    Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

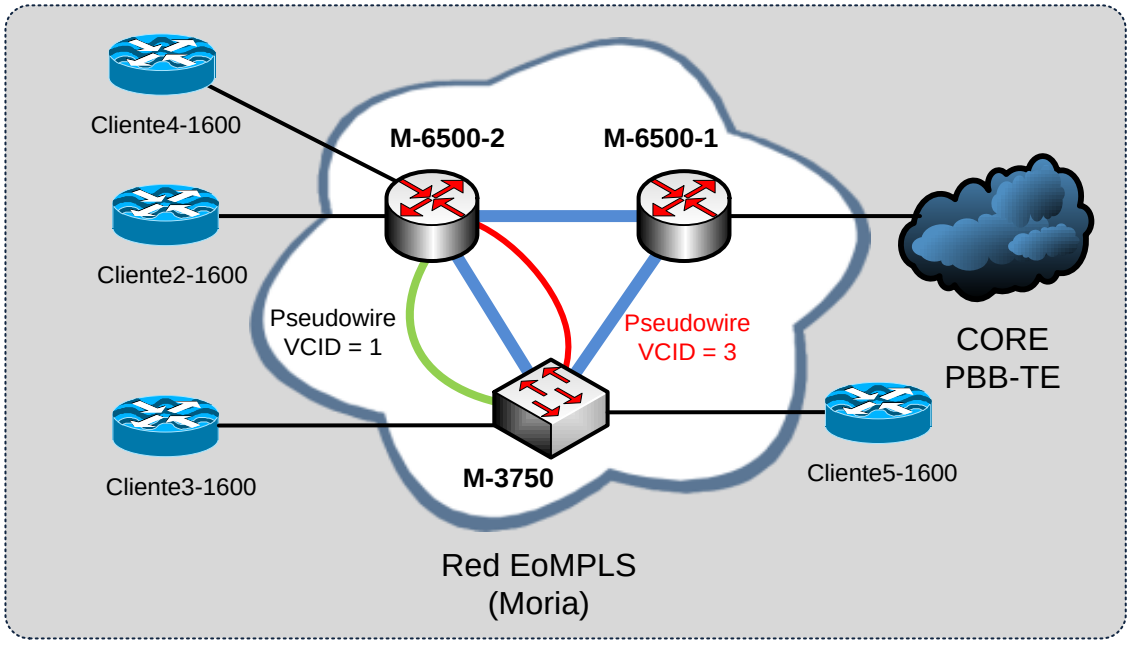
```
cliente3-1600# sh ip arp

    Protocol  Address          Age (min)  Hardware Addr   Type   Interface
    Internet  192.168.0.1            -   0014.a81f.e924  ARPA   FastEthernet0/0
    Internet  192.168.0.2           20   0030.85e7.c0a0  ARPA   FastEthernet0/0
```

Nótese que usando el comando *show mpls forwarding-table* pudo verificarse que el tráfico de *ping* estaba usando el *pseudowire* y mostrando que los pines estaban aumentando los contadores para las entradas EoMPLS por el número correcto de bytes.

4.1.4. Prueba 2: separación de capa 2

A continuación en la figura 33 se muestra un ejemplo de la separación de la capa 2.

Figura 33. **Confirmando la separación en capa 2**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 103.

Una vez que se estableció que el *pseudowire* estaba arriba y funcionando, se añadió un segundo *pseudowire* entre los mismos *routers Provider Edge* que el original (es decir, entre los M-6500-2 y M-3750), de modo de verificar que el tráfico entre estos dos *pseudowires* estaba aislado uno del otro. El segundo *pseudowire* fue configurado de forma idéntica al primero pero con un identificador único, tal como puede verse en M-6500-2:

```
M-6500-2# show mpls l2transport binding

     Destination Address: 10.1.1.1,      VC ID: 1                    ; primer pseudowire
          Local Label: 504
```

```
                Cbit: 0,        VC Type: Ethernet,        GroupID: 0
                MTU: 1500,        Interface Desc: cliente2-1600 EoMPLS prueba_1
                VCCV:      CC Type: RA [2]
                                CV Type: LSPV [2]
          Remote Label: 105
                Cbit: 0,        VC Type: Ethernet,        GroupID: 0
                MTU: 1500,        Interface Desc: cliente3-1600 EoMPLS prueba_1
                VCCV:      CC Type: RA [2]
                                CV Type: LSPV [2]
     Destination Address: 10.1.1.1,        VC ID: 3                        ; segundo
pseudowire
           Local Label: 501
                Cbit: 0,        VC Type: Ethernet,        GroupID: 0
                MTU: 1500,        Interface Desc: cliente4-1600
                VCCV:      CC Type: RA [2]
                                CV Type: LSPV [2]
           Remote Label: 103
                Cbit: 0,        VC Type: Ethernet,        GroupID: 0
                MTU: 1500, Interface Desc: cliente5-1600
                VCCV:      CC Type: RA [2]
                                CV Type: LSPV [2]
```

```
M-3750# sh mpls l2transport binding

     Destination Address: 10.1.1.3,        VC ID: 1
          Local Label: 105
                Cbit: 0,        VC Type: Ethernet,        GroupID: 0
                MTU: 1500,        Interface Desc: cliente3-1600 EoMPLS prueba_1
                VCCV:      CC Type: RA [2]
                                CV Type: LSPV [2]
          Remote Label: 504
```

```
                Cbit: 0,        VC Type: Ethernet,        GroupID: 0
                MTU: 1500,        Interface Desc: cliente2-1600 EoMPLS prueba_1
                VCCV:       CC Type: RA [2]
                                CV Type: LSPV [2]
    Destination Address: 10.1.1.3, VC ID: 3
          Local Label: 103
                Cbit: 0,        VC Type: Ethernet,        GroupID: 0
                MTU: 1500,        Interface Desc: cliente5-1600
                VCCV: CC Type: RA [2]
                                CV Type: LSPV [2]
          Remote Label: 501
                Cbit: 0,        VC Type: Ethernet,        GroupID: 0
                MTU: 1500,        Interface Desc: cliente4-1600
                VCCV: CC Type: RA [2]
                                CV Type: LSPV [2]
```

Se conectó en las siguientes interfaces:

- M-6500-2: puerto Gi3/46.
- M-3750: puerto Fa1/0/23.

En la primera prueba, a los dispositivos clientes (cliente2-1600 y cliente3-1600) se les asignaron direcciones IP 192.168.0.0 y 192.168.0.2 con máscaras de subred 255.255.255.0. Para la segunda prueba, se les dio a los dispositivos clientes usando el segundo *pseudowire* (cliente4-1600 y cliente5-1600) direcciones IP en el mismo rango, 192.168.0.3 y 192.168.0.4 con la misma máscara. Luego se intentó hacer ping a las otras tres direcciones IP desde cada uno de los tres dispositivos cliente para asegurarse de que no existía cros-conectividad entre los dos *pseudowires* EoMPLS y usar el comando *show ip arp* para verificar la separación en capa 2.

```
cliente2-1600# ping 192.168.0.1

      Type escape sequence to abort.
      Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
      !!!!!
      Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
```

```
cliente2-1600# ping 192.168.0.3

      Type escape sequence to abort.
      Sending 5, 100-byte ICMP Echos to 192.168.0.3, timeout is 2 seconds:
      .....
      Success rate is 0 percent (0/5)
```

```
cliente2-1600# ping 192.168.0.4

      Type escape sequence to abort.
      Sending 5, 100-byte ICMP Echos to 192.168.0.4, timeout is 2 seconds:
       .....
      Success rate is 0 percent (0/5)
```

```
cliente2-1600# show ip arp

      Protocol  Address        Age (min)  Hardware Addr   Type   Interface
      Internet  192.168.0.1           15  0014.a81f.e924  ARPA
```

```
FastEthernet0/0
      Internet  192.168.0.2             -   0030.85e7.c0a0  ARPA
FastEthernet0/0
      Internet  192.168.0.3             0   Incomplete      ARPA
      Internet  192.168.0.4             0   Incomplete      ARPA
```

```
cliente3-1600# ping 192.168.0.2

      Type escape sequence to abort.
      Sending 5, 100-byte ICMP Echos to 192.168.0.2, timeout is 2 seconds:
      !!!!!
      Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
cliente3-1600# ping 192.168.0.3

      Type escape sequence to abort.
      Sending 5, 100-byte ICMP Echos to 192.168.0.3, timeout is 2 seconds:
      .....
      Success rate is 0 percent (0/5)
```

```
cliente3-1600# ping 192.168.0.4

      Type escape sequence to abort.
      Sending 5, 100-byte ICMP Echos to 192.168.0.4, timeout is 2 seconds:
      .....
      Success rate is 0 percent (0/5)
```

```
cliente3-1600# show ip arp

      Protocol  Address          Age (min)  Hardware Addr   Type   Interface
      Internet  192.168.0.1              -  0014.a81f.e924   ARPA
FastEthernet0/0
      Internet  192.168.0.2              2  0030.85e7.c0a0   ARPA
FastEthernet0/0
      Internet  192.168.0.3              0  Incomplete       ARPA
      Internet  192.168.0.4              0  Incomplete       ARPA
```

```
cliente4-1600# ping 192.168.0.4

      Type escape sequence to abort.
      Sending 5, 100-byte ICMP Echos to 192.168.0.4, timeout is 2 seconds:
      !!!!!
      Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
cliente4-1600# ping 192.168.0.1

      Type escape sequence to abort.
      Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
      .....
      Success rate is 0 percent (0/5)
```

```
cliente4-1600# ping 192.168.0.2
```

```
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

```
cliente4-1600# sh ip arp

Protocol  Address      Age (min)  Hardware Addr   Type   Interface
Internet  192.168.0.1         0  Incomplete      ARPA
Internet  192.168.0.2         0  Incomplete      ARPA
Internet  192.168.0.3         -  0013.8064.1213  ARPA
FastEthernet0/0
Internet  192.168.0.4        42  000c.ce05.d717  ARPA
FastEthernet0/0
```

```
cliente5-1600# ping 192.168.0.3

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.3, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/2/4 ms
```

```
cliente5-1600# ping 192.168.0.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.1, timeout is 2 seconds:
```

```
.....
Success rate is 0 percent (0/5)
```

```
cliente5-1600# ping 192.168.0.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.2, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
```

```
cliente5-1600# sh ip arp

Protocol  Address      Age (min)  Hardware Addr   Type   Interface
Internet  192.168.0.1         0  Incomplete      ARPA
Internet  192.168.0.2         0  Incomplete      ARPA
Internet  192.168.0.3         2  0013.8064.1213  ARPA
FastEthernet0/0
Internet  192.168.0.4         -  000c.ce05.d717  ARPA
FastEthernet0/0
```

Esta segunda prueba demuestra que el tráfico en un *pseudowire* EoMPLS está aislado del tráfico en otros *pseudowires* EoMPLS, inclusive si estos *pseudowires* comparten los mismos puntos terminales (*End points*).

4.1.5. Calidad de servicio (QoS) y EoMPLS

En los Cisco 6500s, el QoS para un *pseudowire* EoMPLS es implementado por medio del uso del campo TC de MPLS (*Traffic Class Field* – campo de clase de tráfico), el cual permite 3 bits para definir la calidad del tráfico del mismo modo que la precedencia IP (IP Precedence), tal como se vio en el capítulo 2. El campo TC puede cambiarse de una de cuatro formas:

- La primera es cuando un paquete entra a la red MPLS y se añade una etiqueta MPLS, los bits de precedencia IP en el campo IP TOS (*Type of Service*) son copiados dentro del campo TC.
- El segundo es cuando la etiqueta es cambiada dentro de la nube MPLS, el campo TC es copiado de la etiqueta original a la nueva.
- El tercero es cuando la etiqueta superior (*top label)* es removida de un *stack* de etiquetas (*popped*), el campo TC de la etiqueta superior es copiado en la nueva etiqueta superior.
- El cuarto modo es cuando la etiqueta superior es alterada dentro de la nube MPLS por un "*policy map*" (mapa de políticas, útil cuando el administrador de la red quiere controlar la clasificación del tráfico).

Aparte del hecho de que la clasificación de los datos es almacenada en una etiqueta en vez de ser en el campo TOS de un paquete IP, cada aspecto de QoS en EoMPLS es el mismo que cualquier otro QoS en el 6500.

En las tarjetas de línea usadas con los 6500s, las políticas (*policing*) solo están disponibles para una interface en la dirección entrante lo cual significa que el tráfico puede ser politizado o clasificado, ya sea en el borde de la red (antes de que entre a la nube MPLS) o a la salida de esta (una vez el tráfico la

ha atravesado y ya es demasiado tarde para proteger otras clases de tráfico en ese enlace).

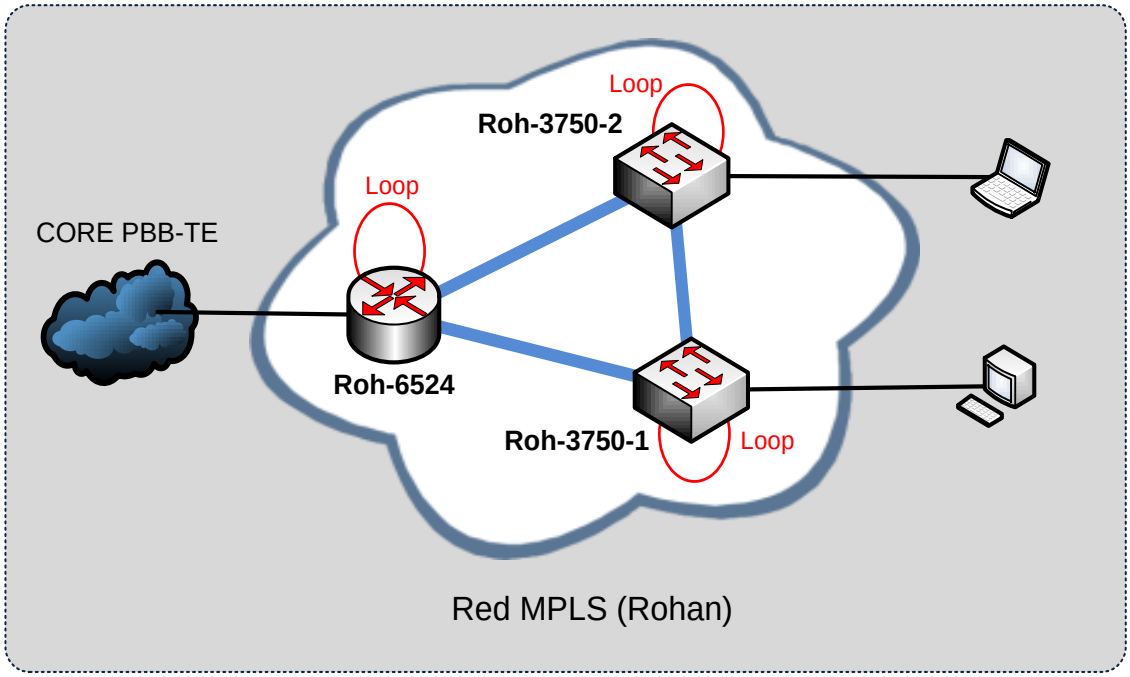
No es apropiado el "*traffic shaping*" (que es todo lo que se puede hacer en las interfaces de salida LAN de los 6500s) dado que esto solo toma efecto cuando el enlace se aproxima a la saturación (lo cual no permite que el tráfico sea limitado a un ancho de banda específico, que es lo que se desea lograr). Además, el "*shaping"* introduce latencia y "*jitter*" (dado que el tráfico es encolado), lo cual no es deseable en los tipos de escenarios donde se desea usar *pseudowires* EoMPLS.

Por estas razones, QoS para EoMPLS en los 6500s, con la tarjeta de LAN que se uso, no era adecuado para *pseudowires* EoMPLS que restringen el ancho de banda en un ISP, tal como lo es la Tierra Media. Por lo tanto se decidió que ya no había nada más que aprender aparte de las pruebas que ya se han realizado.

4.2. Red MPLS en Rohan

Rohan tenía una red de pruebas de tres dispositivos: dos Cisco 3750 Metro y un Cisco 6524. Estaban conectados en una topología triangular y el 6524 se conecta a la red de Tierra Media.

Figura 34. **Topología de la red Rohan**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 104.

Antes de que se configuraran los *pseudowires* EoMPLS los protocolos BGP y LDP ya estaban corriendo y habían establecido relaciones de vecindad exitosas (*neighboring*). Se usaron los siguientes comandos para confirmar que el "MPLS LDP *discovery*" estaba activo en las interfaces y que desde cada *router* se tuviera "*peering*" con los otros dos *routers:*

```
roh-6524# show mpls ldp neighbor
    Peer LDP Ident: 10.100.1.20:0; Local LDP Ident 10.100.1.30:0
        TCP connection: 10.100.1.20.646 - 10.100.1.30.11029
        State: Oper; Msgs sent/rcvd: 62/62; Downstream
```

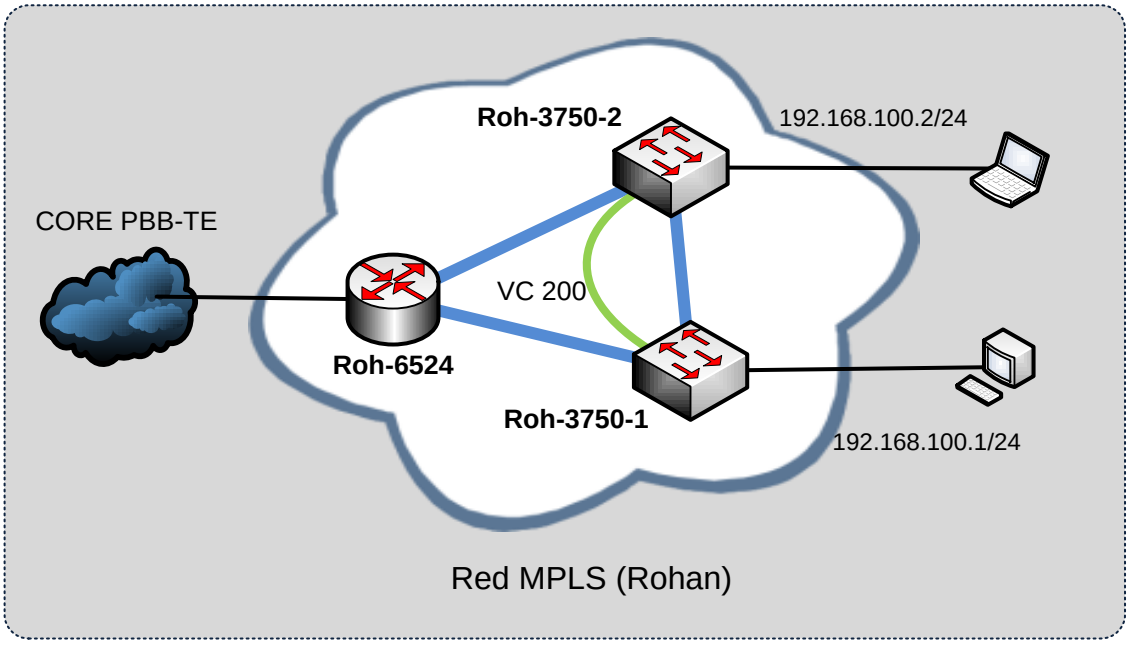
```
            Up time: 00:49:54
            LDP discovery sources:
                GigabitEthernet1/2, Src IP addr: 10.100.2.5
            Addresses bound to peer LDP Ident:
                10.100.1.20 10.100.2.10 10.100.2.5
      Peer LDP Ident: 10.100.1.10:0; Local LDP Ident 10.100.1.30:0
            TCP connection: 10.100.1.10.646 - 10.100.1.30.11028
            State: Oper; Msgs sent/rcvd: 63/63; Downstream
            Up time: 00:49:53
            LDP discovery sources:
                GigabitEthernet1/1, Src IP addr: 10.100.2.1
             Addresses bound to peer LDP Ident:
                10.100.1.10 10.100.99.10 10.100.2.9 10.100.2.1

roh-6524# show mpls ldp discovery
      Local LDP Identifier:
            10.100.1.30:0
            Discovery Sources:
            Interfaces:
                GigabitEthernet1/1 (ldp): xmit/recv
                    LDP Id: 10.100.1.10:0
                GigabitEthernet1/2 (ldp): xmit/recv
                    LDP Id: 10.100.1.20:0

roh-6524# show mpls interfaces
Interface                IP            Tunnel      Operational
GigabitEthernet1/1       Yes (ldp)     No          Yes
GigabitEthernet1/2       Yes (ldp)     No          Yes

roh-6524# show mpls forwarding-table
Local     Outgoing      Prefix            Bytes tag     Outgoing      Next Hop
tag       tag or VC     or Tunnel Id      switched      interface
901       Untagged      10.100.2.8/30     0             Gi1/2         10.100.2.5
          Untagged      10.100.2.8/30     0             Gi1/1         10.100.2.1
902       0             10.100.1.10/32    0             Gi1/1         10.100.2.1
```

903	0	10.100.1.20/32	0	Gi1/2	10.100.2.5
904	Untagged	10.100.99.0/24	0	Gi1/1	10.100.2.1

4.2.1. Prueba 1: *pseudowire* EoMPLS de un solo salto

A continuación, en la figura 35, se muestra un ejemplo de la prueba de Pseudowire de un solo salto.

Figura 35. **Pseudowire EoMPLS de un solo salto (*single hop*)**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 106.

La primera prueba consistió en conectar los 3750s en la topología mostrada arriba, de modo que cada uno pudiera accesar las interfaces *loopback* del otro (usadas como el target para EoMPLS). Nótese que se usaron las

interfaces GigaEthernet para los enlaces entre estos *switches* dado que estas soportan MPLS.

Para cada uno de los *routers* se estableció una sesión LDP hacia el otro. El “Circuit ID” (identificador de circuito) es usado para diferenciar el *pseudowire.*

Con un Circuit ID de 200 y usando el puerto FA1/0/24 en cada dispositivo para conectar los *servers* roh-cliente-1 y roh-cliente-2:

```
roh-3750-1(config)# int fa1/0/24
roh-3750-1(config-if)# no switchport
roh-3750-1(config-if)# xconnect 10.100.1.20 200 encapsulation mpls
roh-3750-1(config-if)# no shutdown

roh-3750-2(config)# int fa1/0/24
roh-3750-2(config-if)# no switchport
roh-3750-2(config-if)# xconnect 10.100.1.10 200 encapsulation mpls
roh-3750-2(config-if)# no shutdown
```

Las direcciones IP en la configuración son las *loopbacks* de los *routers* en los lados opuestos del circuito. El valor 200 es un ID de circuito virtual (VC ID), el cual es escogido arbitrariamente pero debe de ser el mismo a ambos lados del circuito.

El circuito levanta cuando las interfaces fisicas están arriba y las MTUs son consistentes a lo largo de cada salto de la ruta, igual que en la red Moria. Antes de que el circuito este activo, el estatus es DOWN:

```
Local intf      Local circuit         Dest address        VC ID       Status
--------------  --------------------  ------------------  ----------  ----------
Fa1/0/24        Ethernet              10.100.1.10         200         DOWN
```

Luego de que el circuito está activo:

```
roh-3750-2# show mpls l2transport vc

Local intf      Local circuit         Dest address        VC ID       Status
--------------  --------------------  ------------------  ----------  ----------
Fa1/0/24        Ethernet              10.100.1.10         200         UP
```

Y la salida detallada:

```
roh-3750-1# show mpls l2transport vc detail
Local interface: Fa1/0/24 up, line protocol up, Ethernet up
    Destination address: 10.100.1.20, VC ID: 200, VC status: up
        Output interface: Gi1/1/2, imposed label stack {0 805}
        Preferred path: not configured
        Default path: active
        Next hop: 10.100.2.10
    Create time: 00:34:52, last status change time: 00:34:51
    Signaling protocol: LDP, peer 10.100.1.20:0 up
        Targeted Hello: 10.100.1.10(LDP Id) -> 10.100.1.20
        Status TLV support (local/remote) : enabled/not supported
            Label/status state machine : established, LruRru
            Last local dataplane status rcvd: no fault
```

```
                Last local SSS circuit status rcvd: no fault
                Last local SSS circuit status sent: no fault
                Last local LDP TLV status sent: no fault
                Last remote LDP TLV status rcvd: not sent
        MPLS VC labels: local 704, remote 805
        Group ID: local 0, remote 0
        MTU: local 1534, remote 1534
        Remote interface description:
    Sequencing: receive disabled, send disabled
    VC statistics:
        packet totals: receive 25, send 25
        byte totals: receive 13409, send 13409
        packet drops: receive 0, send 0
```

Esto muestra que la etiqueta de apilamiento *(label stack)* para este VC es (0 805), lo cual es una nulidad implícita y 805 lo cual es la etiqueta asignada remotamente para este circuito.

Una prueba de *ping* entre *roh-cliente*-1 y roh-cliente-2 usando 192.168.100.0/24:

```
ricardo@roh-cliente-1:~$ ifconfig eth1 | grep 192
          inet addr:192.168.100.1 Bcast:192.168.100.255 Mask:255.255.255.0
ricardo@ roh-cliente-2:~$ ifconfig eth4 | grep 192
          inet addr:192.168.100.2 Bcast:192.168.100.255 Mask:255.255.255.0
ricardo@roh-cliente-1:~$ ping -M do -c 5 -i 0.2 192.168.100.2
PING 192.168.100.2 (192.168.100.2) 56(84) bytes of data.
64 bytes from 192.168.100.2: icmp_seq=1 ttl=64 time=0.265 ms
64 bytes from 192.168.100.2: icmp_seq=2 ttl=64 time=0.397 ms
64 bytes from 192.168.100.2: icmp_seq=3 ttl=64 time=0.267 ms
```

```
64 bytes from 192.168.100.2: icmp_seq=4 ttl=64 time=0.391 ms
64 bytes from 192.168.100.2: icmp_seq=5 ttl=64 time=0.269 ms

--- 192.168.100.2 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 800ms
rtt min/avg/max/mdev = 0.265/0.317/0.397/0.066 ms
```

No se hace aprendizaje de direcciones MAC entre los puertos EoMPLS:

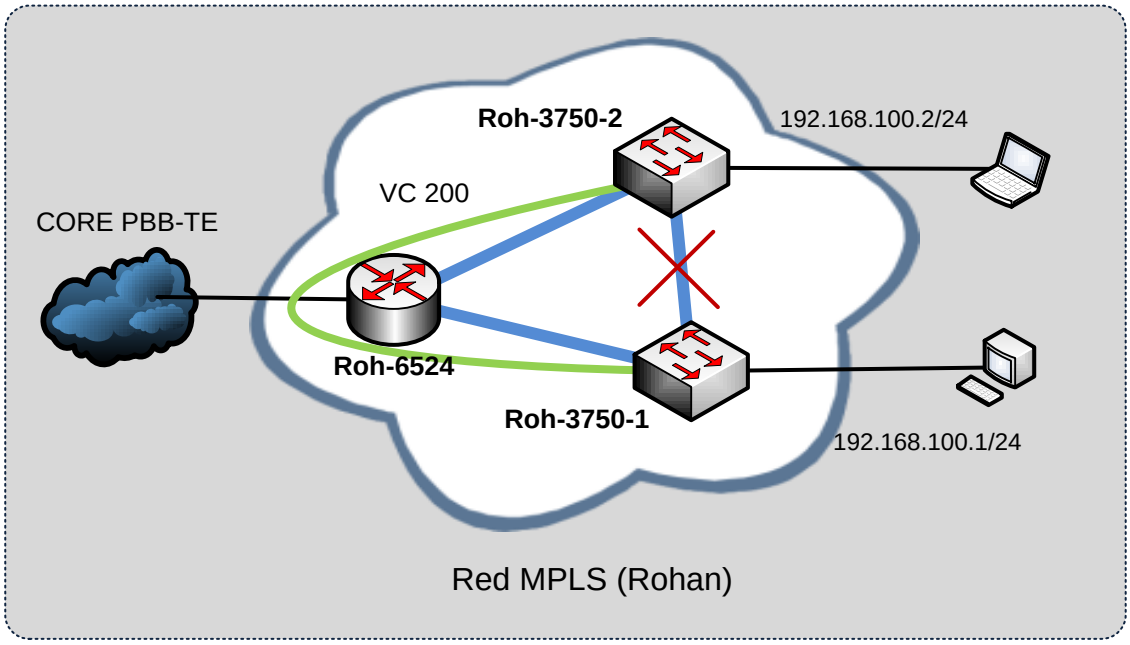
```
roh-3750-1# show mac address-table dynamic interface fa1/0/24
        Mac Address Table
-----------------------------------------------------------
Vlan Mac        Address        Type        Ports
------------        -----------        ------        -------
roh-3750-1#
```

Además, ninguno de los *switches* ha aprendido la dirección MAC o IP de los servers conectados.

4.2.2. Prueba 2: conmutación en caso de falla

A continuación, en la figura 36, se muestra un ejemplo de la prueba de conmutación en casos de fallas.

Figura 36. **Conmutación del *pseudowire* en caso de falla.**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 108.

Si se cae el enlace entre los dos 3750 el circuito debería de restablecerse vía el 6524, tal como sucedió en efecto:

Puede verse que la etiqueta de apilamiento y el próximo salto *(next hop),* han cambiado (subrayado):

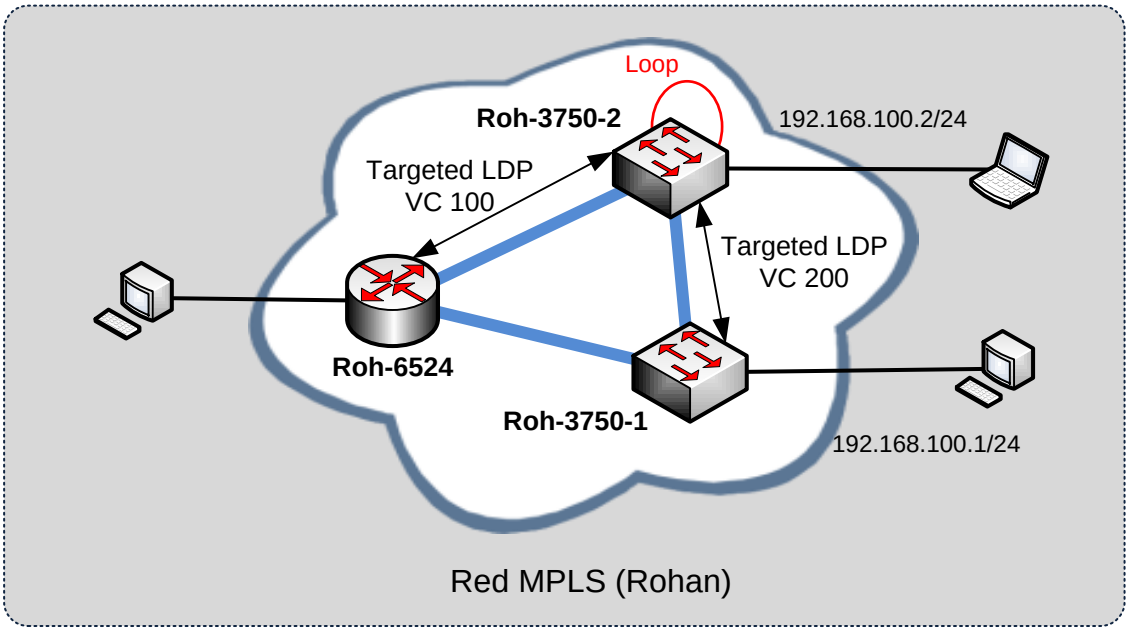
```
roh-3750-1# show mpls l2 vc detail
Local interface: Fa1/0/24 up, line protocol up, Ethernet up
      Destination address: 10.100.1.20, VC ID: 200, VC status: up
            Output interface: Gi1/1/1, imposed label stack {903 805}
            Preferred path: not configured
            Default path: active
```

```
        Next hop: 10.100.2.2
    Create time: 01:38:13, last status change time: 00:00:03
    Signaling protocol: LDP, peer 10.100.1.20:0 up
        Targeted Hello: 10.100.1.10(LDP Id) -> 10.100.1.20
        Status TLV support (local/remote) : enabled/not supported
            <snip>
        MPLS VC labels: local 704, remote 805
        Group ID: local 0, remote 0
        MTU: local 1534, remote 1534
        Remote interface description:
    Sequencing: receive disabled, send disabled
    VC statistics:
        packet totals: receive 53, send 56
        byte totals: receive 31651, send 31843
        packet drops: receive 0, send 0
```

4.2.3. Prueba 3: *pseudowire* con múltiples saltos

El próximo paso es crear dos *pseudowires* para utilizar los tres *switches* de la red de pruebas. Se crea un circuito entre roh-3750-1 y roh-3750-2, y otro entre roh-6524 y roh-3750-2. En el dispositivo común roh-3750-2 se conecta un cable en lazo (*loop)* con el propósito de crear un punto final para los circuitos entre una máquina conectada a 6524-01 y otra conectada a 3750-01.

Figura 37. **Pseudowire EoMPLS de múltiples saltos.**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 110.

La configuración del *pseudowire* básica es idéntica a la de la prueba 1, con excepción de que ahora se tiene dos circuitos virtuales (100 y 200), y el servidor roh-cliente-2 está ahora en el puerto Gi 1/32 del roh-6524. Ahora se tiene un servidor conectado a cada extremo de los *pseudowires* y los dos circuitos están conectados con el cable de *loopback,* tal como se muestra en la imagen de arriba.

Para la verificación, nicialmente, se tuvo problemas habilitando el circuito 100 en el roh-6524:

```
roh-3750-2#show mpls l2 vc
```

```
Local intf      Local circuit          Dest address           VC ID       Status
--------------  ---------------------  ---------------------  ---------  ---------
Fa1/0/2         Ethernet               10.100.1.10            200        UP
Fa1/0/1         Ethernet               10.100.1.30            100        DOWN
```

Sin embargo, se encontró que era el MTU. En el 3750, el MTU puede tener un valor máximo de 1534:

```
roh-3750-2# show mpls l2 vc 100 detail
Local interface: Fa1/0/1 up, line protocol up, Ethernet up
    Destination address: 10.100.1.30, VC ID: 100, VC status: down
        Output interface: none, imposed label stack {}
        Preferred path: not configured
        Default path: no route
        No adjacency
    Create time: 00:05:57, last status change time: 00:00:35
    Signaling protocol: LDP, peer 10.100.1.30:0 up
        Targeted Hello: 10.100.1.20(LDP Id) -> 10.100.1.30
        Status TLV support (local/remote)     :  enabled/not supported
            Label/status state machine        :  remote invalid, LruRnd
            Last local dataplane     status rcvd:   no fault
            Last local SSS circuit   status rcvd:   no fault
            Last local SSS circuit   status sent:    PW DOWN(rx,tx faults)
            Last local LDP TLV       status sent:    no fault
            Last remote LDP TLV      status rcvd:   not sent
        MPLS VC labels: local 804, remote 904
        Group ID: local 0, remote 0
        MTU: local 1534, remote 1500
        Remote interface description:
    Sequencing: receive disabled, send disabled
    VC statistics:
        packet totals:       receive 0,       send 0
```

```
    byte totals:          receive 0,      send 0
    packet drops:         receive 0,      send 0
```

En el 6524 el MTU no había sido fijado en el puerto Gi1/32, de modo que estaba a 1500, pero una vez que esto se incrementó para igualar al del otro dispositivo (igual en vez de simplemente exceder), el circuito levanto en cuestión de segundos.

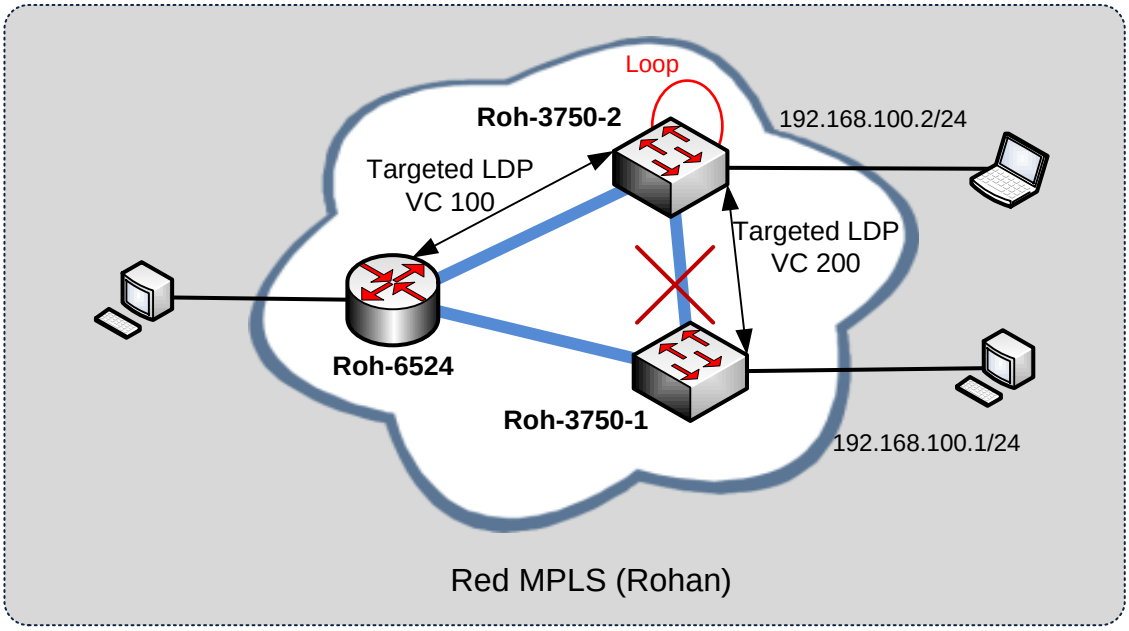
Nuevamente las pruebas de *ping* fueron exitosas entre los servidores, los cuales estaban conectados a los siguientes puertos en los siguientes dispositivos:

roh-cliente-2.rohan	6524-01	Gi1/32	VCID 100
roh-cliente-1.rohan	3750-01	Fa1/0/24	VCID 200

4.2.4. Prueba 4: conmutación de enlace múltiples saltos

Para verificar que los circuitos pueden seguir funcionando después de la falla de un puerto y que usarán el LFIB para localizar una nueva ruta a través de la red, se apagó el puerto Gi1/2 en el 3750-02.

Figura 38. **Conmutación de enlace con múltiples saltos**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 112.

Esto tuvo el efecto de que el VC ID 200 tuvo que ir vía 6524-01, y de hecho una etiqueta extra aparece en el *stack:*

```
roh-3750-1# show mpls l2 vc detail
Local interface: Fa1/0/24 up, line protocol up, Ethernet up
      Destination address: 10.100.1.20, VC ID: 200, VC status: up
            Output interface: Gi1/1/1, imposed label stack {903 806}
            Preferred path: not configured
            Default path: active
            Next hop: 10.100.2.2
      Create time: 02:31:35, last status change time: 00:00:36
      Signaling protocol: LDP, peer 10.100.1.20:0 up
```

```
        Targeted Hello: 10.100.1.10(LDP Id) -> 10.100.1.20
        Status TLV support (local/remote) : enabled/not supported
            Label/status state machine : established, LruRru
            Last local dataplane status rcvd: no fault
            Last local SSS circuit status rcvd: no fault
            Last local SSS circuit status sent: no fault
            Last local LDP TLV status sent: no fault
            Last remote LDP TLV status rcvd: not sent
        MPLS VC labels: local 704, remote 806
        Group ID: local 0, remote 0
        MTU: local 1534, remote 1534
        Remote interface description:
    Sequencing: receive disabled, send disabled
    VC statistics:
        packet totals: receive 65, send 62
        byte totals: receive 32679, send 32379
        packet drops: receive 0, send 0
```

Una prueba de *ping* demostró que el servicio seguía funcionando, y también se verifico que las direcciones MAC de los servidores no estaban siendo aprendidas por ningún dispositivo.

4.3. Conectividad entre ambas redes MPLS

La red PBB-TE que conecta las redes de Moria y Rohan identifica a dónde enviar el tráfico entrante examinando las etiquetas de VLAN, es decir, el tráfico que ingresa a la red PBB-TE en la VLAN 320 (que viene de Moria) fue configurado para ser enviado por la interface hacia Rohan, y el tráfico que ingresa por la VLAN 230 (que viene desde Rohan), fue enviado a la interface que comunica con Moria. Por lo tanto, el tráfico que sale de las redes MPLS necesitaba ser etiquetado apropiadamente, al ingresar a la red PBB-TE. Para

switches/routers Cisco, esto implica configurar el enlace como *trunk*, permitiendo la VLAN necesaria a través del *trunk* y fijando el número de interfaz SVI (Switch Virtual Interface) apropiado, por ejemplo, en Moria (M-6500-1):

```
interface GigabitEthernet1/1
      description Link to ROH PBB-TE Core
      switchport
      switchport trunk encapsulation dot1q
      switchport trunk allowed vlan 320
      switchport mode trunk
      mtu 9000                                        ; agregado para ser consistente
                                                      ; con el resto de la red MPLS.
      !
      vlan 320
            name Rohan_S-VID
      !
      interface Vlan320
            ip address 10.100.3.1 255.255.255.252
      end
```

4.3.1. Prueba 1: conectividad entre ambas redes MPLS

El objetivo era confirmar conectividad básica entre ambas redes MPLS, lo cual se logró haciendo *ping* al *router* en el otro extremo de la red PBB-TE. Inicialmente esto fallo pero luego se descubrió que esto era debido a que los números de VLAN en cada red MPLS eran diferentes (el tráfico de Rohan estaba llegando al dominio PBB-TE con VLAN 230 cuando M-6500-1 estaba esperando VLAN 320, y viceversa).

Si bien las etiquetas de VLAN estaban siendo manejadas e intercambiadas en el dominio PBB-TE, las BPDUs del *switch* Cisco enviadas a través de la red contenían (dentro del payload) el VLAN ID original, el cual no fue alterado.

Por lo tanto, el VLAN ID dentro del BPDU que llego a cada extremo, no coincidía con la etiqueta de VLAN para ese cuadro y por lo tanto los 6500s a cada extremo "concluían" que las dos VLANs se habían unido (creando algún loop) en algún punto, poniendo entonces la VLAN en estado de bloqueo.

Para solucionar este problema, se apagó el Spanning Tree para la VLAN 320 en el lado de Moria (se hizo algo similar en Rohan), entonces la VLAN, ya no fue bloqueada y por lo tanto pudo hacerse *ping* a través del enlace.

```
M-6500-1# ping 10.100.3.2

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.100.3.2, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 4/5/8 ms
```

También se usó el comando *show ip arp* para confirmar que la dirección MAC del dispositivo que responde era la esperada:

```
M-6500-1# show ip arp vlan320

  Protocol  Address          Age (min)  Hardware Addr   Type   Interface
  Internet  10.100.3.2              178  0022.56cf.17ca  ARPA   Vlan320
  Internet  10.100.3.1                -  0021.d8cc.7ac0  ARPA   Vlan320
```

4.3.2. Prueba 2: *pseudowire* con múltiples dominios

Antes de que se pudiera construir un pseudowire EoMPLS entre las dos redes, era necesario que se pudiera hacer el intercambio de etiquetas entre ambas. Uno de los modos en que esto puede lograrse es mediante mBGP L2VPN, lo cual permite que la información de etiquetas sea anunciada entre dominios sin la necesidad de anunciar rutas IP y así mantener la separación de capa 3. Desafortunadamente, L2VPN no era soportada por la plataforma Cisco 6 500, por lo cual hubo que buscar otra solución.

Se intentó tratar los dominios LDP de Rohan y Moria como uno solo. Primero, se agregó una configuración BGP para levantar un *peering* eBGP entre las dos ASBR (*Autonomous System Border Router*) de las dos redes de prueba:

```
router bgp 65000
neighbor 10.100.3.2 remote-as 65200
neighbor 10.100.3.2 description eBGP peering to Rohan
!
address-family ipv4
    neighbor 10.100.3.2 activate
    neighbor 10.100.3.2 soft-reconfiguration inbound
```

Y luego se vio el "*peering*" BGP funcionando por medio del comando:

```
show bgp ipv4 unicast summary
```

El cual dió:

```
M-6500-1# sh bgp ipv4 unicast sum

      BGP router identifier 10.1.1.2, local AS number 65000
      BGP table version is 819, main routing table version 819
      14 network entries using 1638 bytes of memory
      18 path entries using 936 bytes of memory
      5/4 BGP path/bestpath attribute entries using 700 bytes of memory
      1 BGP AS-PATH entries using 24 bytes of memory
      0 BGP route-map cache entries using 0 bytes of memory
      0 BGP filter-list cache entries using 0 bytes of memory
      BGP using 3298 total bytes of memory
      BGP activity 286/272 prefixes, 388/370 paths, scan interval 60 secs

      Neighbor  V    AS      MsgRcvd   MsgSent   TblVer    InQ    OutQ  Up/Down  State/Pfx
Rcd
      10.1.1.1     4    65000  362057    362259     819       0       0       15w4d       4
<-1
      10.1.1.3     4    65000  373443    373599     819       0       0       15w4d       3
<-2
      10.100.3.2  4    65200  201505    200149     819       0       0       1d00h       6
<-3
```

<-1 - *peering* con M-3750.

<-2 - *peering* con M-6500-2.

<-3 - *peering* con Rohan ASBR.

Luego se habilitó MPLS/LDP entre los *links* de los *routers* Core por medio del comando:

```
mpls ip
```

Y luego se confirmó que las etiquetas estaban siendo anunciadas a través del enlace PBB-TE y asociadas con rutas IP con el comando:

```
show mpls ldp bindings
```

El cual dio:

```
M-6500-1# sh mpls ldp bindings

    lib entry: 10.10.9.0/24, rev 411(no route)
        remote binding: lsr: 10.1.1.1:0, label: imp-null
    lib entry: 10.1.1.1/32, rev 408
        local binding: label: 301
        remote binding: lsr: 10.1.1.1:0, label: imp-null
        remote binding: lsr: 10.1.1.3:0, label: 502
    lib entry: 10.1.1.2/32, rev 4
        local binding: label: imp-null
        remote binding: lsr: 10.1.1.3:0, label: 503
        remote binding: lsr: 10.1.1.1:0, label: 104
```

```
lib entry: 10.1.1.3/32, rev 405
        local binding: label: 302
        remote binding: lsr: 10.1.1.3:0, label: imp-null
        remote binding: lsr: 10.1.1.1:0, label: 109
lib entry: 10.1.2.0/30, rev 410
        local binding: label: imp-null
        remote binding: lsr: 10.1.1.1:0, label: imp-null
        remote binding: lsr: 10.1.1.3:0, label: 506
lib entry: 10.1.2.8/30, rev 12
        local binding: label: imp-null
        remote binding: lsr: 10.1.1.3:0, label: imp-null
        remote binding: lsr: 10.1.1.1:0, label: 106
lib entry: 10.1.2.12/30, rev 421
        local binding: label: 304
        remote binding: lsr: 10.1.1.1:0, label: imp-null
        remote binding: lsr: 10.1.1.3:0, label: imp-null
```

Sin embargo, no se aprendieron etiquetas a través del enlace PBB-TE por ninguno de los *routers* ASBR. Esto se debe a que las etiquetas entre ASs deben de ser distribuidas usando BGP y no LDP. Por lo tanto se añadió el comando:

```
neighbor <BGP-NEIGHBOUR_ID> send-label
```

Para cada uno de los *peerings* en ambas redes de prueba, por ejemplo, para Moria:

```
neighbor 10.1.1.1 send-label
```

```
neighbor 10.1.1.3 send-label
neighbor 10.100.3.2 send-label
```

Una vez con esta configuración se usaron los comandos:

```
neighbor <BGP-NEIGHBOUR_ID> send-label
show ip bgp labels
```

Para Moria:

```
M-6500-1# sh mpls ldp bindings

    lib entry: 10.10.9.0/24, rev 411(no route)
        remote binding: lsr: 10.1.1.1:0, label: imp-null
    lib entry: 10.1.1.1/32, rev 408
        local binding: label: 301
        remote binding: lsr: 10.12.1.1:0, label: imp-null
        remote binding: lsr: 10.12.1.3:0, label: 502
    lib entry: 10.12.1.2/32, rev 4
        local binding: label: imp-null
        remote binding: lsr: 10.12.1.3:0, label: 503
        remote binding: lsr: 10.12.1.1:0, label: 104
    lib entry: 10.12.1.3/32, rev 405
        local binding: label: 302
        remote binding: lsr: 10.12.1.3:0, label: imp-null
        remote binding: lsr: 10.12.1.1:0, label: 109
    lib entry: 10.12.2.0/30, rev 410
        local binding: label: imp-null
```

```
        remote binding: lsr: 10.12.1.1:0, label: imp-null
        remote binding: lsr: 10.12.1.3:0, label: 506
    lib entry: 10.12.2.8/30, rev 12
        local binding: label: imp-null
        remote binding: lsr: 10.12.1.3:0, label: imp-null
        remote binding: lsr: 10.12.1.1:0, label: 106
    lib entry: 10.12.2.12/30, rev 421
        local binding: label: 304
        remote binding: lsr: 10.12.1.1:0, label: imp-null
        remote binding: lsr: 10.12.1.3:0, label: imp-null
    lib entry: 10.100.1.10/32, rev 415(no route)                    <---\
        remote binding: lsr: 10.100.1.30:0, label: 902                   |
    lib entry: 10.100.1.20/32, rev 416(no route)                         |
        remote binding: lsr: 10.100.1.30:0, label: 903                   |
    lib entry: 10.100.1.30/32, rev 412(no route)                         |
        remote binding: lsr: 10.100.1.30:0, label: exp-null              |
    lib entry: 10.100.2.0/30, rev 417                                      |
        remote binding: lsr: 10.100.1.30:0, label: exp-null              |
    lib entry: 10.100.2.4/30, rev 413                                      |-recibidas
        remote binding: lsr: 10.100.1.30:0, label: exp-null              |--de la
    lib entry: 10.100.2.8/30, rev 414                                      |--red
        remote binding: lsr: 10.100.1.30:0, label: 901                   |--de pruebas
    lib entry: 10.100.3.0/30, rev 225                                      |--de Rohan.
        local binding: label: imp-null                                     |
        remote binding: lsr: 10.100.1.30:0, label: exp-null              |
    lib entry: 10.100.3.1/32, rev 418                                      |
        remote binding: lsr: 10.100.1.30:0, label: 904                   |
    lib entry: 10.100.3.2/32, rev 369                                      |
        local binding: label: 305                                       <---/
```

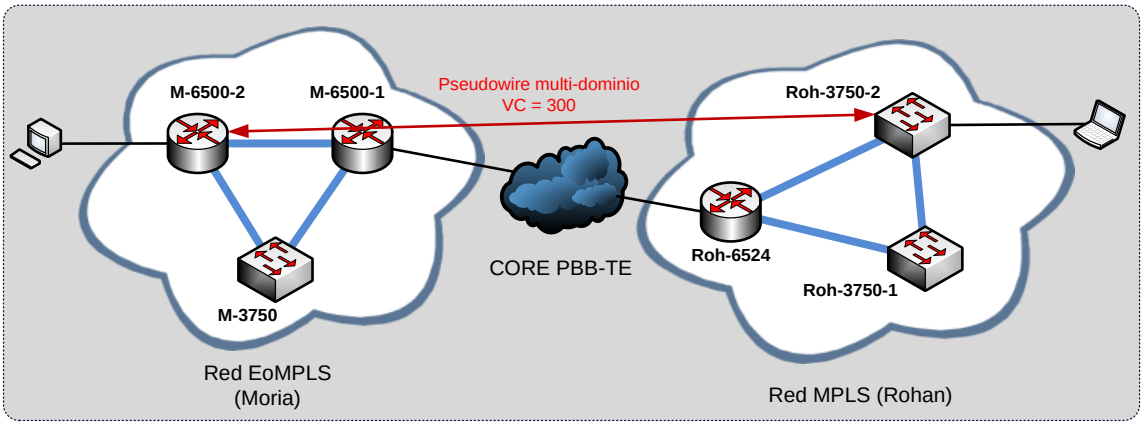
Y:

```
M-6500-1# show ip bgp labels

   Network          Next Hop      In label/Out label
   10.10.9.0/24     10.12.1.1     308/nolabel
   10.12.1.1/32     10.12.1.1     301/nolabel
   10.12.1.2/32     0.0.0.0       imp-null/nolabel
   10.12.1.3/32     10.12.1.3     302/imp-null
   10.12.2.0/30     10.12.1.1     imp-null/nolabel
                    0.0.0.0         imp-null/nolabel
   10.12.2.8/30     10.12.1.3     imp-null/imp-null
                    0.0.0.0         imp-null/nolabel
   10.12.2.12/30    10.12.1.1     304/nolabel
                    10.12.1.3       304/imp-null
   10.100.1.10/32   10.100.3.2    309/902              <---\
   10.100.1.20/32   10.100.3.2    312/903                  |
   10.100.1.30/32   10.100.3.2    313/imp-null           |--recividas
   10.100.3.0/30 1  0.62.3.2      imp-null/imp-null      |--de la
                    0.0.0.0         imp-null/nolabel       |--red
   10.100.3.1/32    10.100.3.2    307/904                  |--de pruebas
   10.100.3.2/32    0.0.0.0       305/nolabel              |--de Rohan
   10.100.99.0/24   10.100.3.2    303/900               <--/
```

Mostraron que ahora se estaba anunciando y recibiendo etiquetas en ambas redes de prueba.

Ahora que todo estaba arriba y corriendo, se creó un *pseudowire* entre los dos dispositivos cliente (Client Edge Devices), uno en la red de Moria y otro en la red de Rohan.

Figura 39. ***Pseudowire* con múltiples dominios (Multidomain)**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 115.

En el extremo Moria se agregó:

```
interface GigabitEthernet3/47
      description EoMPLS test to Rohan
      no ip address
      xconnect 10.100.1.20 300 encapsulation mpls
end
```

En M-6500-2 y se conectó a cliente1-1600 a este puerto para que actuara como dispositivo Client Edge (dirección IP 192.168.100.1 con el dispositivo cliente en Rohan usando la 192.168.100.2). Usando:

```
show mpls l2transport vc
```

Se confirmó que el *pseudowire* estaba arriba:

```
M-6500-2# show mpls l2transport vc 300

     Local intf     Local circuit     Dest address    VC ID      Status
     -------------  ----------------  --------------  ---------  ----------
     Gi3/47         Ethernet          10.100.1.20        300        UP
```

Esta es una prueba de *ping* con un vistazo a la tabla de ARP para asegurarse de que era el dispositivo en Rohan respondiendo:

```
cliente1-1600# ping 192.168.100.2

     Type escape sequence to abort.
     Sending 5, 100-byte ICMP Echos to 192.168.100.2, timeout is 2 seconds:
     !!!!!
     Success rate is 100 percent (5/5), round-trip min/avg/max = 4/8/16 ms
```

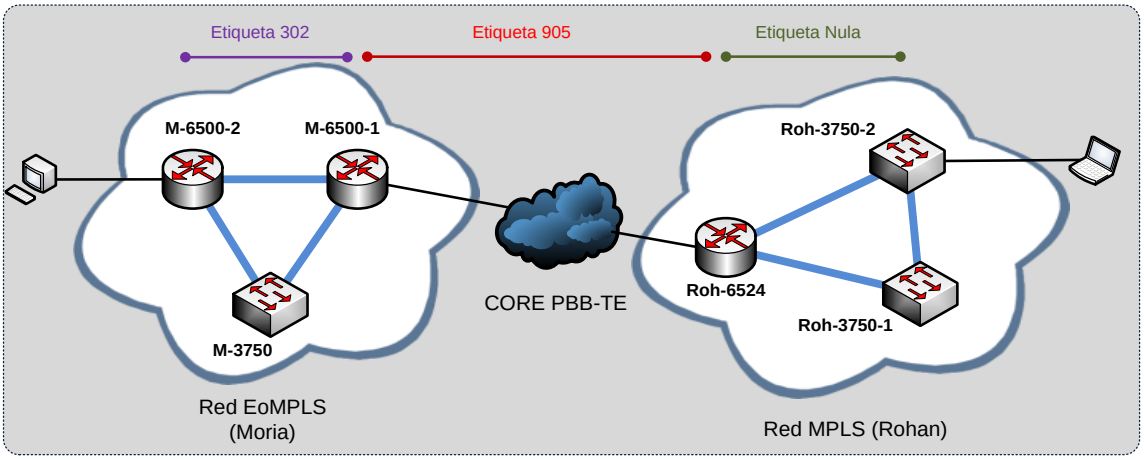
Y,

```
cliente1-1600# show ip arp

     Protocol  Address          Age (min)  Hardware Addr   Type   Interface
     Internet  192.168.100.2          0   0016.0a19.670b  ARPA
FastEthernet0/0
     Internet  192.168.100.1          -   0004.4d56.a080  ARPA
FastEthernet0/0
```

Lo cual confirma que el *pseudowire* EoMPLS multi-hop estaba arriba y funcionando.

La topología del *pseudowire* multidominio es la mostrada a continuación:

Figura 40. **Topología del *pseudowire* multidominio**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 117.

4.3.2.1. Verificación

Circuito en Rohan:

```
roh-3750-2#show mpls l2 vc 300
Local intf      Local circuit      Dest address       VC ID      Status
--------------  -----------------  -----------------  ----------  ----------
Fa1/0/23        Ethernet           10.12.1.3          300         UP

roh-3750-2#show mpls l2 binding 300
      Destination Address: 10.12.1.3, VC ID: 300
```

```
            Local Label: 802
                Cbit: 0, VC Type: Ethernet, GroupID: 0
                MTU: 1500, Interface Desc: EoMPLS test from roh-3750-2/23 to Moria
                VCCV:    CC Type: RA [2]
                         CV Type: LSPV [2]
            Remote Label: 507
                Cbit: 0, VC Type: Ethernet, GroupID: 0
                MTU: 1500, Interface Desc: EoMPLS test to Rohan
                VCCV:    CC Type: RA [2]
                         CV Type: LSPV [2]

roh-3750-2#show mpls l2 vc 300 det
Local interface: Fa1/0/23 up, line protocol up, Ethernet up
    Destination address: 10.12.1.3, VC ID: 300, VC status: up
        Output interface: Gi1/1/2, imposed label stack {0 905 302 507}
        Preferred path: not configured
        Default path: active
        Next hop: 10.100.2.5
    Create time: 18:27:57, last status change time: 13:52:01
    Signaling protocol: LDP, peer 10.12.1.3:0 up
        Targeted Hello: 10.100.1.20(LDP Id) -> 10.12.1.3
        Status TLV support (local/remote) : enabled/not supported
            Label/status state machine : established, LruRru
            Last local dataplane        status rcvd:       no fault
            Last local SSS circuit      status rcvd:       no fault
            Last local SSS circuit      status sent:       no fault
            Last local LDP TLV          status sent:       no fault
            Last remote LDP TLV status rcvd: not sent
        MPLS VC labels: local 802, remote 507
        Group ID: local 0, remote 0
        MTU: local 1500, remote 1500
        Remote interface description: EoMPLS test to Rohan
    Sequencing: receive disabled, send disabled
    VC statistics:
```

```
        packet totals: receive 9390, send 0
        byte totals: receive 1789114, send 0
        packet drops: receive 0, send 0
```

En el circuito de Moria:

```
M-6500-2#show mpls l2transport vc 300
Local intf Local circuit Dest address VC ID Status
------------ -------------------- --------------- ---------- ----------
Gi3/47 Ethernet 10.100.1.20 300 UP

M-6500-2#show mpls l2transport binding 300
    Destination Address: 10.100.1.20, VC ID: 300
        Local Label: 507
        Cbit: 0, VC Type: Ethernet, GroupID: 0
        MTU: 1500, Interface Desc: EoMPLS test from cliente1-1600 to Rohan
        VCCV: CC Type: RA [2]
        CV Type: LSPV [2]
    Remote Label: 802
        Cbit: 0, VC Type: Ethernet, GroupID: 0
        MTU: 1500, Interface Desc: EoMPLS test from roh-3750-2/23 to Moria
        VCCV: CC Type: RA [2]
        CV Type: LSPV [2]

M-6500-2#show mpls l2transport vc 300 detail
Local interface: Gi3/47 up, line protocol up, Ethernet up
    Destination address: 10.100.1.20, VC ID: 300, VC status: up
        Output interface: Gi3/1, imposed label stack {312 802}
        Preferred path: not configured
        Default path: active
        Next hop: 10.12.2.9
    Create time: 13w1d, last status change time: 00:00:09
```

```
Signaling protocol: LDP, peer 10.100.1.20:0 up
    MPLS VC labels: local 507, remote 802 Group ID: local 0, remote 0
    MTU: local 1500, remote 1500
    Remote interface description: EoMPLS test from roh-3750-2/23 to Moria
Sequencing: receive disabled, send disabled
VC statistics:
    packet totals: receive 88191, send 557888
    byte totals: receive 8991984, send 106288187
    packet drops: receive 0, send 0
```

4.3.3. Prueba 3: QoS

Para esta prueba, el papel de Moria era servir como origen del tráfico usado por Rohan para probar su configuración QoS para clasificar el tráfico entrante usando el valor EXP.

La primera parte de prueba consistía en establecer que el campo EXP estaba siendo reservado en las etiquetas enviadas desde Moria a Rohan. Se usó Wireshark para establecer que, por *default,* todos los valores EXP en las etiquetas estaban a cero. Luego, se configuró un *policy-map* en el ME3750 en que terminaba el *pseudowire* EoMPLS en la red de Rohan (3750-02), fijando el valor EXP a 4 y Moria envió tráfico ICMP por el *pseudowire* (desde M-6500-2, que es donde termina el *pseudowire* en Moria) usando el comando:

```
ping mpls pseudowire 10.100.1.20 300 exp 4 repeat 1000
```

Para mandar 1000 paquetes ICMP a través del *pseudowire* con el valor EXP fijado a 4. El resultado mostro que el *policy-map* estaba reservado exitosamente el valor EXP para el *pseudowire.*

4.3.4. Prueba 4: *Streaming* a través de un *pseudowire*

El objetivo de esta prueba era ver una aplicación real corriendo a través del *pseudowire* y se optó por mandar video por "*streaming*" usando el reproductor VLC, con Rohan haciendo el papel de servidor y Moria como cliente.

Desde Rohan se envió un video con un tamaño de 8 Mbps. El video y el audio se recibieron perfectamente.

4.3.5. Prueba 5: Bit EXP punto a punto

En Moria se fijó la etiqueta MPLS EXP a 4. En Rohan se configuró un *policy-map* para encajar con esto. Luego de generar tráfico desde Moria, se pudo verificar que los bits EXP estaban en el modo deseado a través del *pseudowire*. Esta es la salida luego de haber fijado el EXP a 4 y de haber puesto el *policy-map*:

```
roh-3750-2#show policy-map interface gig 1/1/2
    GigabitEthernet1/1/2
        Service-policy input: Moria-PARENT
            Class-map: class-default (match-any)
                81588 packets, 10593105 bytes
                5 minute offered rate 122000 bps, drop rate 0 bps
                Match: any
```

```
                Service-policy : Moria-CHILD
                    Class-map: MATCH-Moria-EXP (match-all)
                        81378 packets, 10579140 bytes
                        5 minute offered rate 122000 bps
                        Match: mpls experimental topmost 4
                    Class-map: class-default (match-any)
                        210 packets, 13965 bytes
                        5 minute offered rate 0 bps, drop rate 0 bps
                        Match: any
```

Se resetearon los contadores y ahora pueden verse únicamente los paquetes que hacen *match:*

```
roh-3750-2#clear counters gigabitEthernet 1/1/2
Clear "show interface" counters on this interface [confirm]
roh-3750-2#show policy-map interface gig 1/1/2
044763: *Aug 2 20:43:26.000 UTC: %CLEAR-5-COUNTERS: Clear counter on interface
GigabitEthernet1/1/2 by console
roh-3750-2#show policy-map interface gig 1/1/2
GigabitEthernet1/1/2
    Service-policy input: Moria-PARENT
        Class-map: class-default (match-any)
            229 packets, 29770 bytes
            5 minute offered rate 0 bps, drop rate 0 bps
            Match: any
            Service-policy : Moria-CHILD
                Class-map: MATCH-Moria-EXP (match-all)
                    229 packets, 29770 bytes
                    5 minute offered rate 0 bps
```

```
                    Match: mpls experimental topmost 4
                Class-map: class-default (match-any)
                    0 packets, 0 bytes
                    5 minute offered rate 0 bps, drop rate 0 bps
                    Match: any
roh-3750-2#show policy-map interface gig 1/1/2
GigabitEthernet1/1/2
Service-policy input: Moria-PARENT
    Class-map: class-default (match-any)
        818 packets, 106340 bytes
        5 minute offered rate 6000 bps, drop rate 0 bps
        Match: any
        Service-policy : Moria-CHILD
            Class-map: MATCH-Moria-EXP (match-all)
                818 packets, 106340 bytes
                5 minute offered rate 6000 bps
                Match: mpls experimental topmost 4
            Class-map: class-default (match-any)
            0 packets, 0 bytes
            5 minute offered rate 0 bps, drop rate 0 bps
            Match: any
roh-3750-2#show policy-map interface gig 1/1/2
GigabitEthernet1/1/2
    Service-policy input: Moria-PARENT
        Class-map: class-default (match-any)
            1293 packets, 168090 bytes
            5 minute offered rate 6000 bps, drop rate 0 bps
            Match: any
            Service-policy : Moria-CHILD
                Class-map: MATCH-Moria-EXP (match-all)
                    1293 packets, 168090 bytes
                    5 minute offered rate 6000 bps
                    Match: mpls experimental topmost 4
                Class-map: class-default (match-any)
                    0 packets, 0 bytes
```

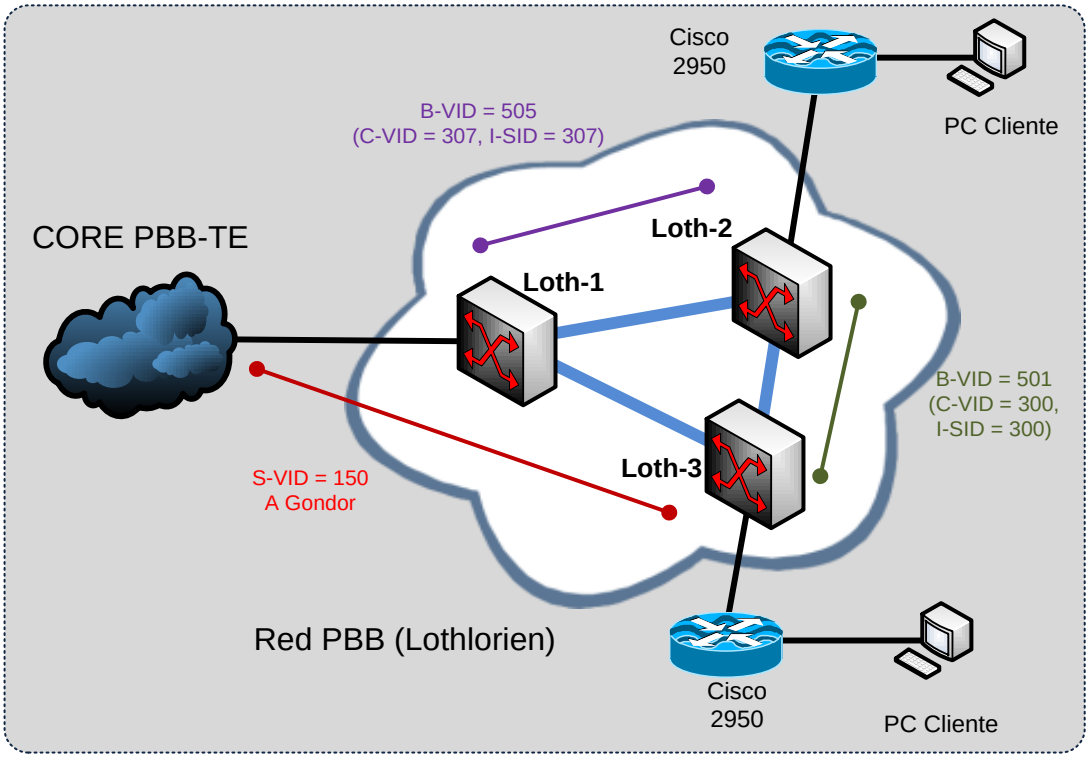
```
                    5 minute offered rate 0 bps, drop rate 0 bps
                    Match: any
roh-3750-2#
```

5. CONSTRUCCIÓN DE UNA RED PBB

5.1. Red PB en Lothlórien

A continuación en la figura 41 se muestran algunas pruebas de la red PB en Lothlórien.

Figura 41. **Red de pruebas PBB de Lothlórien**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 120.

La red usada para estas pruebas se componía de 3 Switches Ciena LE-311v (LOTH-1, LOTH-2 y LOTH-3), los cuales fueron usados para establecer túneles PBT (Ciena usa el acrónimo de Nortel PBT en vez de PBB, el cual es el equivalente de IEEE) y circuitos dentro de ellos. Fueron conectados en una topología de triángulo usando puertos ópticos de 1GE. Se usó una vez más una topología de triángulo, ya que es la más pequeña que permite pruebas establecer múltiples rutas de punto a punto para probar las redundancias y él TE. Todos los *switches* tenían software LEOS v4.6.

Dos *switches* Cisco 2950 y dos servidores Dell fueron usados para emular las redes de clientes. Cada 2950 soportaba dos VLANs cliente con C-VID (Costumer VLAN ID) 300 y con C-VID 307.

Cada servidor Dell tenía dos interfaces Ethernet, una de las cuales fue usada como nodo cliente en la subred 10.1.0.0. La segunda interfaz fue usada para administración, con la subred 193.63.63.128/26, accesable desde fuera de Tierra Media.

Se instaló el Ethernet Service Manager de Ciena en un servidor (servidor WWP en la Figura 41). El servidor de administración también se usó para hacer capturas de tráfico en los puertos espejo de los LE-311v usando Wireshark.

5.1.1. Prueba 1: dos túneles sin protección

A continuación se muestra el objetivo principal de túneles sin protección.

5.1.2. Objetivo

El objetivo de esta prueba es establecer dos túneles PBT sin protección entre los puertos de los *switches* y usarlos para conectar servicios de clientes (VLANs 300 y 307), con el fin de ganar experiencia básica en la configuración y administración de túneles PBT.

5.1.3. Escenario

Se levantaron dos túneles PBT:

- Un túnel indirecto con B-VID 505 entre LOTH-2 y LOTH-3, que pasa a través de LOTH-1.
- Un túnel directo con B-VID 501 entre LOTH-2 y LOTH-3.

El túnel 505 se usó para transportar la VLAN 507 de cliente mientras que el túnel 501 se usó para transportar la VLAN 300. Solo los puertos 25 a 28 pueden usarse para establecer los túneles PBT.

5.1.3.1. Configuración

Un túnel PBT consiste de dos rutas unidireccionales:

- Encap, lo cual encapsula los cuadros Ethernet que entran al túnel usando encapsulación 802.1ah MAC-in-MAC y los manda por el túnel.
- Decap, el cual desencapsula los cuadros Ethernet saliendo del túnel.

La configuración del túnel en LOTH-2 es como sigue:

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! TUNNEL CONFIG:
!
tunnel encap create static-pbt a_loth-3 b-vid 505 dest-bridge-name loth-3 port 26
tunnel encap create static-pbt 501_a_loth-3 b-vid 501 dest-bridge-name loth-3 port 25
tunnel decap create static-pbt desde_loth-3 b-vid 505 src-bridge-name loth-3 port 26
tunnel decap create static-pbt 501_desde_loth-3 b-vid 501 src-bridge-name loth-3 port 25
!
tunnel pair create tnl-pair loth-3 encap-pbt a_loth-3 decap-pbt desde_loth-3
tunnel pair create tnl-pair 501_tunnel encap-pbt 501_a_loth-3 decap-pbt 501_desde_loth-3
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Los nombres de las partes del túnel tal como a_loth-3 fueron escogidos arbitrariamente, mientras que los destinos de los túneles (tales como loth-3) fueron especificados configurando las direcciones MAC de las *loopbacks* de los equipos en cuestión y luego asociando estas direcciones MAC al nombre del equipo correspondiente.

Por ejemplo, en LOTH-3 se ingresó el siguiente comando para especificar su dirección MAC de su *loopback:*

```
pbt set bridge-mac 04:00:00:00:00:03
```

En LOTH-2 el comando:

```
pbt remote-bridge create bridge-name loth-3 bridge-mac 04:00:00:00:00:03
```

Asocia la dirección loopback de LOTH-3 al nombre loth-3.

El comando *"tunnel pair create"* no es mandatorio pero si es útil dado que acopla las partes de encapsulación y desencapsulación de un túnel en una única entidad que es útil en algunos casos, por ejemplo, cuando una parte del túnel se cae y la otra no, un túnel acoplado declara ambas partes como caídas.

Un Switch Virtual (Virtual Switch, VS) y un Circuito Virtual (Virtual Circuit, VC) son elementos que los equipos Ciena usan para crear un servicio para un cliente dentro de un túnel PBT para llevar el tráfico de un cliente.

Un circuito virtual es lo que el IEEE llama un "Service Instance", cual está especificado por la etiqueta I-SID (*Backbone service instance identifier*) con encapsulación 802.1ah. Es de hecho una conexión lógica entre las interfaces de usuario (ya sean estas físicas o basadas en VLAN), y viaja a través de un túnel PBT. Cada túnel PBT puede llevar hasta 16 millones de conexiones de clientes dado que el I-SID es de 24 bits. Sin embargo, en las pruebas realizadas se usó una conexión I-SID por cada túnel PBT. Una conexión I-SID puede ser imaginada como el equivalente de un *pseudowire* EoMPLS.

Un *switch* virtual selecciona tráfico de un usuario específico que entra a un puerto de un *switch.*

La configuración LOTH-2 para especificar *switches* virtuales y circuitos virtuales es como sigue:

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! VIRTUAL-CIRCUIT CONFIG: virtual circuits
!
virtual-circuit pbt create static-vc vs_307 egress-isid 307 ingress-isid 307 tunnel a_loth-3
virtual-circuit pbt create static-vc 501_vc egress-isid 300 ingress-isid 300 tunnel
      501_a_loth-3
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! VIRTUAL-SWITCH CONFIG:
!
virtual-switch add reserved-vlan 4090-4094
!
virtual-switch ethernet create vs vs_307 vc vs_307
virtual-switch ethernet create vs vs_300_501 vc 501_vc
!
virtual-switch ethernet add vs vs_307 port 10 vlan 307
virtual-switch ethernet add vs vs_300_501 port 10 vlan 300
!!!!!!!
```

Ambos *switches* virtuales seleccionan tráfico de usuario del puerto 10 de LOTH-2 pero con diferentes valores de C-VIDs.

Un comando para crear un *switch* virtual asocia un switch a un circuito virtual mientras que la creación de un circuito virtual asocia este circuito con un túnel PBT en particular (la parte de encap) y le da un valor de I-SID.

En las pruebas el valor de I-SID escogido coincide con el C-VIDs. Si bien los WWP pueden traducir los I-SID de ingreso y de egreso, se hizo de este modo por simplicidad.

Un *switch* virtual en la implementación WWP necesita un VLAN ID para llevar a cabo sus operaciones internas. Un *switch* usa este VLAN ID para la encapsulación intermedia 802.1ah (entiéndase QinQ) de un cuadro Ethernet; ese encapsulación es luego removida en el túnel PBT por un encap de modo tal que un cuadro de cliente (customer frame) dentro de un túnel PBT tiene su encabezado original más un encabezado 802.1ah pero no un encabezado QinQ entre ellos.

5.1.4. Resultados

Los túneles PBT y dos conexiones cliente se probaron periódicamente por medio de pines al servidor 10.1.0.2 desde el servidor 10.1.0.1 y viceversa.

Los pines mostraron un desempeño de 100% (sin paquetes perdidos) en ambas C-VID 300 y 307.

El comando "*tunnel show*" refleja el estado de los túneles:

```
loth-2> tunnel show
+---------------------------------------- ENCAP TUNNEL TABLE ----------------------------------------+
|Name                |Type          |Oper    |Admin  |Destination  |B-VID   |Role    |Active |
```

```
+--------------------+-----------------+----------+----------+----------------+----------+---------+----------+
|a_loth-3            |encap-pbt     |En       |En       |loth-3          |505       |pri      |Yes     |
|501_a_loth-3     |encap-pbt     |En       |En       |loth-3          |501       |pri      |Yes     |
+--------------------+-----------------+----------+----------+----------------+----------+---------+---------+
+----------------------------------------- DECAP TUNNEL TABLE ---------------- ----------------------------+
|                                |                     | Oper       |
| Name                         | Type                | State      | B-VID
|
+----------------------------+--------------------+------------+-------------------------------------------------+
| desde_loth-3             | decap-pbt        | En          | 505
|
| 501_desde_loth-3      | decap-pbt        | En          | 501
|
+----------------------------+--------------------+------------+-------------------------------------------------+
```

Cuadros capturados por el software Wireshark en el puerto 28 de LOTH-1 mostraron que el tráfico estaba siendo encapsulado de acuerdo al estándar 802.1ah.

5.1.5. Problemas encontrados

- En los *switches* LE-311v solo es posible crear túneles PBT en puertos Gigabit, y los LE-311v solo tienen 4 puertos GE. Intentos de crear túneles PBT en puertos Fast Ethernet dan error.

5.1.5.1. Prueba 2: monitoreo del estado del enlace

A continuación se muestra el objetivo principal del monitoreo del estado del enlace.

5.1.6. Objetivo

El objetivo de esta prueba era determinar cómo los “mensajes de continuidad de conectividad” (CCM – Continuity Check Messages) de CFM pueden ser usados para monitorear el estado de los túneles PBT y las conexiones I-SID entre *switches* virtuales. CFM envía “*heart beats*” o latidos, de modo que el lado A asume que el lado B está vivo si A recibe regularmente de B los *heartbeats.*

5.1.7. Escenario

Se establecieron sesiones CFM para dos túneles PBT y para dos conexiones I-SID entre ellas.

5.1.7.1. Configuración

En los LE-311v solo está disponible la función CCM para monitorear el estado de los túneles PBT y las conexiones entre switches virtuales. El CFM también incluye las funciones *“linktrace*” y “*loopback*” las cuales son útiles para resolver fallas *(“troubleshooting”*), y están disponibles en los *switches* LE-311v pero solo para otro tipo de servicios, tales como VLANs.

Los CCMs son generados en cada extremo de un túnel PBT o de un switch virtual de forma independiente, sin embargo, ambos deben de tener un nombre en común y el mismo “dominio de mantenimiento” (MD – Maintenance Domain) para que sean reconocidos al otro extremo del túnel PBT. También deben de establecer una “asociación de mantenimiento” (MA – Maintenance Association) entre los extremos de una conexión.

El valor MD para los *switches* virtuales debe de ser más grande que el valor MD para los túneles PBT a través de los cuales se comunican los *switches* virtuales, lo cual refleja la posición de estas entidades en la jerarquía de la red. El valor por defecto de un MD es 3, y fue así como se usó en los túneles PBT durante las pruebas, para *switches* virtuales se usó un MD de 4.

Cada extremo de un túnel PBT o de una conexión de switch virtual debe de tener un número único de “punto final de mantenimiento” (MEP – Maintenance End Point). Establecer “puntos intermedios de mantenimiento” (MIP – Maintenance Intermediate Point) para un túnel PBT y un switch virtual no es necesario debido a que ambos son tratados como una sola entidad.

La configuración de CCM en LOTH-2 es como sigue:

```
loth-3> cfm remote-mep show
+------------------------------------------ CFM REMOTE MEPS -----------------------------------------+
|                    |           |                          |State    |Total      |Seq    |Last          |Fault    |
|Service             |Mepid |Mac Address          |Ad |Op |Rx CCM   |Error |Seq Num  |F |P |R |

+------------------+--------+-------------------------+----+----+-------------+------+-------------+---+---+---+

|pbt_505_cfm   |100     |04:00:00:00:00:02  |en |en |3474064  |0      |3474064   |X  |   |   |
+----------------+-----+----------------+--+--+---------+-----+---------+-+-+-+-+
|pbt_501_cfm   |101     |04:00:00:00:00:02  |en |en |3473941  |0      |3473941   |X  |   |   |
+------------------+--------+-------------------------+----+----+-------------+------+-------------+---+---+---+
```

Se establecieron 4 MAs:

- ‘pbt_505_cfm’ para el túnel ‘a_loth-3’ con B-VID 505.
- ‘pbt_501_cfm’ para el túnel ‘501_a_loth-3’ con B-VID 501.
- ‘cfm_300’ para el switch virtual vs_300_501 (la instancia de servicio va a traves del túnel PBT ‘a_loth-3’).
- ‘vs_307_b’ para el switch virtual vs_307 (la instancia de servicio va a través del túnel PBT ‘501_a_loth-3’).

El intervalo entre CCMs era de 1 segundo.

5.1.8. Resultados

El monitoreo CCM reflejo de forma correcta los cambios en el estado de los túneles PBT y de la conexión de los *switches* virtuales cuando los puertos de los LE-311v en cuestión eran desconectados.

Por ejemplo, cuando los puertos estaban conectados el CLI mostraba ambos túneles en “*enable”* (habilitados), sin indicar ninguna falla:

```
loth-3> cfm remote-mep show
+------------------------------------------ CFM REMOTE MEPS -------------------------------------------+
|                     |           |                          |State     |Total      |Seq   |Last         |Faul  |
|Service              |Mepid  |Mac Address           |Ad |Op  |Rx CCM  |Error|Seq Num |F|P|R|
+--------------------+-----------+-------------------------+-----+-----+------------+------+-------------+-+--+--+
|pbt_505_cfm     |100       |04:00:00:00:00:02  |en  |en  |3463227 |0      |3463227  | |  | |
+--------------------+-----------+-------------------------+----+-----+------------+------+-------------+-+--+--+
|pbt_501_cfm     |101       |04:00:00:00:00:02  |en  |en  |3463226 |0      |3463226  | |  | |
+--------------------+-----------+-------------------------+----+-----+------------+------+-------------+-+--+--+
```

Cuando se desconectaron los puertos de ambos túneles, el CLI mostro las MAs en estado de falla:

```
loth-3> cfm remote-mep show
+------------------------------------------ CFM REMOTE MEPS ------------------------------------------+
|                    |          |                          |State    |Total      |Seq    |Last          |Fault    |
|Service             |Mepid |Mac Address          |Ad |Op |Rx CCM   |Error |Seq Num  |F |P |R |

+------------------+--------+-------------------------+----+----+-------------+------+-------------+---+---+---+

|pbt_505_cfm   |100     |04:00:00:00:00:02  |en |en |3474064  |0      |3474064   |X  |   |    |
+----------------+-----+----------------+--+--+---------+-----+---------+-+-+-+-+
|pbt_501_cfm   |101     |04:00:00:00:00:02  |en |en |3473941  |0      |3473941   |X  |   |    |
+------------------+--------+-------------------------+----+----+-------------+------+-------------+---+---+---+
```

Los pines mutuos entre los servidores 10.1.0.1 y 10.1.0.2 confirmaron la información presentada en el CLI del CFM.

5.1.8.1. Problemas encontrados

El CFM para *switches* virtuales deja de trabajar después de un reinicio a pesar del hecho de que fue configurado adecuadamente y estaba trabajando antes del reinicio. El único modo de arreglar esto es removiendo el CFM CONFIG del *switch* virtual, reiniciar la unidad y luego ingresar una vez más el CFM CONFIG, después de lo cual empieza a funcionar, solo que después de que la unidad se reinicia. Se sospecha que se trate de un *bug* en el equipo de Ciena. El caso fue reportado al proveedor.

5.1.9. Prueba 3: calidad del servicio

A continuación se muestra el objetivo principal de la calidad de servicio.

5.1.9.1. Objetivo

El objetivo de esta prueba era evaluar la funcionalidad Y.1731 para monitorear la calidad del servicio (midiendo el retraso en los cuadros – *frame delay* – y el *jitter)* en los *switches*.

5.1.9.2. Escenario

Iniciar el monitoreo de retraso de cuadros y *jitter* para dos túneles PBT en producción.

5.1.9.3. Configuración

Se configuraron funciones de monitoreo de desempeño en los LE-311v por medio de estándar Y.1731.

Para monitorear el retraso y el *jitter* experimentado por los servicios en los túneles PBT, las siguientes líneas de comando se agregaron a la configuración en el *switch* loth-2:

```
! CFM CONFIG: meps
cfm delay send service pbt_505_cfm port 26 mepid 200 repeat 1
cfm delay send service pbt_501_cfm port 25 mepid 201 repeat 1
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

La primera línea de la configuración inicia la generación de mensajes DMM (Delay Measurement Message – Mensajes de medición del retardo) para el servicio CFM pbt_505_cfm (la cual fue habilitada para el túnel PBT con B-VID 505) a través del puerto 26. El MEP fue definido como MEPID 200. El intervalo entre mensajes DMM era de 100 ms y el intervalo de repetición entre series se especificó a 1 minuto. Los mensajes DMM llevan etiquetas de tiempo (*timestamps*) para permitir calcular el retraso y el *jitter.*

De acuerdo con esta configuración, MEP 200 (localizado en el *switch* loth-3) debe de recibir mensajes DMM y generar mensajes DMR (Delay Measurement Replay). Los mensajes DMR llevan marcas de tiempo DMM en sus propias marcas de tiempo.

La segunda línea de configuración hace el mismo trabajo para monitorear el servicio CFM pbt_502_cfm, el cual es para el túnel con B-VID 501.

5.1.9.4. Resultados

El comando "cfm *delay show*" reporta resultados instantáneos de medición de retraso/*jitter* de acuerdo a los últimos mensajes de DMR recibidos.

El resultado de dos comandos "cfm *delay show*" sucesivos en el *switch* loth-2 se muestra a continuación:

```
loth-2> cfm delay show
+----------------------- MEP DELAY MEASUREMENT MESSAGE INFORMATION ----------------------+
|                    |        |Remote            |Remote|          |          Delay  | Jitter |Rep    |
```

```
|Service             |Port   |Mac Address         |Mepid  |DMM's |DMR's | in us  | in us  |Time  |
+--------------------+-------+--------------------+-------+------+------+--------+--------+------+
|pbt_505_cfm    |26     |04:00:00:00:00:03| 200      |10        |10        |3759  |81      |1      |
|pbt_501_cfm    |25     |04:00:00:00:00:03| 201      |10        |10        |1043  |231     |1      |
+--------------------+-------+--------------------+-------+------+------+--------+--------+------+
```

```
loth-2> cfm delay show
+------------------------ MEP DELAY MEASUREMENT MESSAGE INFORMATION ----------------------
--+
|                    |         |Remote              |Remote|           |            Delay  | Jitter |Rep   |
|Service             |Port   |Mac Address         |Mepid  |DMM's |DMR's | in us  | in us  |Time |
+--------------------+-------+--------------------+-------+------+------+--------+--------+------+
|pbt_505_cfm    |26     |04:00:00:00:00:03 | 200      |10        |10        |3787  |252     |1      |
|pbt_501_cfm    |25     |04:00:00:00:00:03 | 201      |10        |10        |853   |136     |1      |
+--------------------+-------+--------------------+-------+------+------+--------+--------+------+
```

La salida muestra que los promedios de retraso y *jitter* cambiaron ligeramente de un tiempo al otro.

La medición basada en DMM/DMR de los *switches* LE-311v es precisa solo hasta los milisegundos, dado que es una implementación de software de relativamente baja precisión. Existen implementaciones en hardware con precisiones de microsegundos.

5.1.9.5. Problemas encontrados

No se encontró ningún problema.

5.1.10. Prueba 4: protección en caso de falla

A continuación se muestra el objetivo principal de la protección en caso de que hubiera fallas.

5.1.10.1. Objetivo

El objetivo de esta prueba era verificar si PBT soporta la conmutación rápida del primario al túnel de respaldo, en caso de que el túnel primario falle. La protección de conmutación en PBT es la característica que distingue a PBT de PBB, el cual puede soportar ingeniería de tráfico como PBT, pero no soporta la protección de conmutación.

5.1.10.2. Escenario

Se configuró un túnel de respaldo para el túnel primario “loth-2-loth-1-loth-3” y se creó una sesión CFM/CCM para ello.

Se ocasionó una falla del enlace por medio de la desconexión física de un puerto del túnel principal.

Se verificó el estado de ambos túneles por medio de:

- Pines entre los servidores 10.1.0.1 y 10.1.0.2 en ambas direcciones.
- Verificando el estado de ambos túneles por medio del comando *“tunnel-show”.*

5.1.10.3. Configuración

La configuración de un túnel PBT de respaldo es muy similar a la configuración del primario. Un túnel de respaldo debe de ser configurado en los *switches* de ambos extremos y debe de tener el mismo B-VID que el túnel primario, así como el mismo nombre.

A continuación se muestra la configuración de los *switches* loth-2 y loth-3:

```
loth-2> config show
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! TUNNEL CONFIG:
!
tunnel encap create static-pbt a_loth-3 b-vid 505 dest-bridge-name loth-3 port 26
tunnel encap create static-pbt 501_a_loth-3 b-vid 501 dest-bridge-name loth-3 port 25
tunnel encap create static-backup-pbt a_loth-3 b-vid 605 dest-bridge-name loth-3 port 25
tunnel decap create static-pbt desde_loth-3 b-vid 505 src-bridge-name loth-3 port 26
tunnel decap create static-pbt 501_desde_loth-3 b-vid 501 src-bridge-name loth-3 port 25
tunnel decap create static-pbt bkp-from-loth-3 b-vid 605 src-bridge-name loth-3 port 25 !
tunnel pair create tnl-pair loth-3 encap-pbt a_loth-3 decap-pbt desde_loth-3
tunnel pair create tnl-pair 501_tunnel encap-pbt 501_a_loth-3 decap-pbt 501_desde_loth-3
tunnel pair create tnl-pair loth-3-backup encap-backup-pbt a_loth-3 decap-pbt bkp-from-
    loth-3
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
loth-3> config show
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! TUNNEL CONFIG:
```

```
!
tunnel encap create static-pbt a_loth-2 b-vid 505 dest-bridge-name loth-2 port 25
tunnel encap create static-pbt 501_a_loth-2 b-vid 501 dest-bridge-name loth-2 port 26
tunnel encap create static-backup-pbt a_loth-2 b-vid 605 dest-bridge-name loth-2 port 26
tunnel decap create static-pbt from_loth-2 b-vid 505 src-bridge-name loth-2 port 25
tunnel decap create static-pbt 501_from_loth-2 b-vid 501 src-bridge-name loth-2 port 26
tunnel decap create static-pbt bkp_from_loth-2 b-vid 605 src-bridge-name loth-2 port 26 !
tunnel pair create tnl-pair loth-2 encap-pbt a_loth-2 decap-pbt from_loth-2
tunnel pair create tnl-pair 501_tunnel encap-pbt 501_a_loth-2 decap-pbt 501_from_loth-2
tunnel pair create tnl-pair a_loth-2_backup encap-backup-pbt a_loth-2 decap-pbt-
    bkp_from_loth-2
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

El intervalo fijado para los mensajes CCM juega un papel crucial en la conmutación al túnel de respaldo ya que esta empieza después de que se pierde el tercer mensaje CCM sucesivo. En la prueba se dejó este intervalo a 1 segundo, que es el valor por defecto.

5.1.10.4. Resultados

El mecanismo de protección funciono tal como se esperaba. Cuando se deshabilito el puerto 28 de loth-1 el estatus del túnel primario cambio a “Active-No”, mientras que el estatus del túnel de respaldo cambio a “Active-Yes”, de acuerdo con la salida del comando “*tunnel-show”.*

Los pines con un intervalo de 0,1 segundos mostraron una corta interrupción de la conectividad. La conmutación al túnel secundario causo un 5 % de pérdidas o 22 paquetes, lo cual corresponde a aproximadamente 2,2

segundos de tiempo de conmutación, lo cual es menos de los 3 segundos esperados.

A continuación los datos del ping:

```
10.1.0.2 ping statistics ---
420 packets transmitted, 398 received, 5% packet loss, time 45117ms
rtt min/avg/max/mdev = 0.194/0.211/0.235/0.014 ms, pipe 2
```

5.1.10.5. Problemas encontrados

No se encontró ningún problema en esta prueba.

5.1.11. Prueba 5: políticas de tráfico

En función del análisis de tráfico realizado en la sección anterior se establecerán políticas de calidad de servicio que permitan priorizar algunas aplicaciones y administrar la congestión en la red.

5.1.11.1. Objetivo

El objetivo de esta prueba era probar la capacidad de los *switches* LE-311v para aplicar políticas por VLAN.

5.1.11.2. Escenario

Configurar políticas de ingreso para el tráfico por puertos y por VLANs. Se uso el generador de tráfico N2X de Agilent para enviar paquetes Ethernet a

un puerto de usuario, empezando en un nivel abajo del límite impuesto por la política y aumentándolo gradualmente hasta excederlo. El segundo puerto Agilent fue usado para recolectar paquetes que iban a través del "policer" y de los túneles PBT.

5.1.11.3. Configuración

La configuración de las políticas (o del "*policer*") incluye:

- Creación de una política ("*policing profile"*) basada en el CIR (Committed Information Rate – Rata de información comprometida) y el PIR (Peak Information Rate – Rata de Información Pico) para un puerto y para un VLAN ID.
- Habilitar dicha política o perfil.

La configuración en loth-2 es como sigue:

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! TRAFFIC PROFILING CONFIG:
!
traffic-profiling Estándar-profile create port 10 profile 1 cir 2048 pir 4032 name tp_307
    vlan307
!
traffic-profiling set port 10 mode Estándar-vlan
traffic-profiling enable port 10
!
traffic-profiling enable
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

Se aplicó el *policing* al tráfico entrante por el puerto 10 de loth-2 con un CIR de 2048 Kbits/s y un PIR de 4032 kbits/s. El tráfico generado por el Agilent era de 64 octetos de largo (incluyendo encabezado) con 26 octetos de carga útil IP (IP Payload).

La política se aplicó en el modo de VLAN, lo cual significa que el tráfico entrante fue clasificado tomando el número de VLAN de cliente como criterio de selección; esta modalidad funciona solo si el puerto de entrada hace encapsulación MAC-in-MAC.

5.1.11.4. Resultados

Cuando el volumen de tráfico inyectado por el Agilent (eth1) subió de 1Mbit/s a 4Mbit/s todo el tráfico paso sin problemas tal como lo mostró la captura del Wireshark y del Agilent.

Cuando el tráfico inyectado excedió el límite PIR de 4Mbit/s el descarte de paquetes se inició. La rata de tráfico que llegaba al *switch* loth-1 (capturado por Wireshark) y la tasa de tráfico recibida por el Agilent eth2 permanecieron ambas sin cambio.

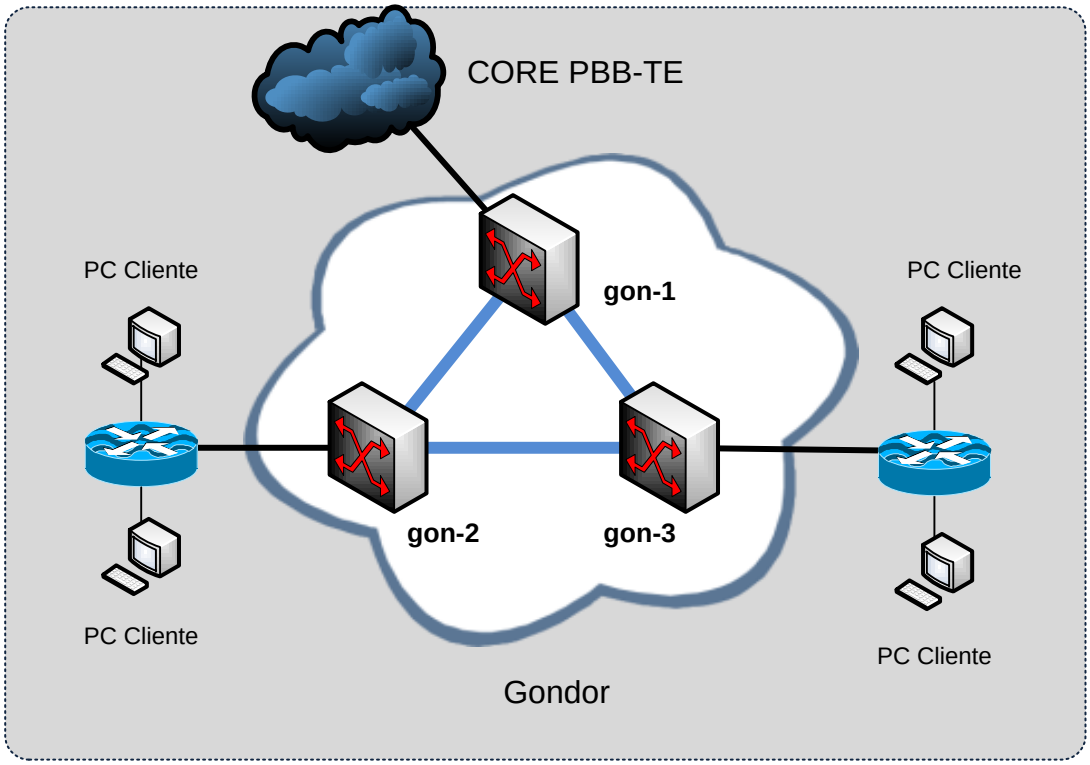
Los cálculos muestran que:

- Los parámetros CIR y PIR cuentan todos los bytes de los cuadros Ethernet, es decir, encabezado y carga útil.
- Siendo aplicado en modo de VLAN, un policer trabaja con los paquetes encapsulados de modo que toma en cuenta una jerarquía completa de encabezados (es decir, todos los campos en un encabezado MAC-in-MAC).

5.2. Pruebas en Gondor

Nuevamente la red de pruebas consiste en tres dispositivos en triángulo, ya que es la configuración mínima que permite probar múltiples trayectorias. En este caso también se tiene LE-311v. Adicionalmente a los switches del triángulo principal existen otros dos Cisco 2950 y 4 nodos de prueba con interfaces Ethernet duales para permitir la administración simultánea.

Figura 42. **Topología de la red de Gondor**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 122.

Los túneles PBT solo pueden crearse en los puertos GE (25 a 28) de los Ciena LE-311v, dado que solo estos puertos están equipados con FPGA (Field-Programmable Gate Array), necesario para soportar PBT.

Se requiere también de licencias de software para permitir la funcionalidad PBT en los LE-311v. Con el siguiente comando pueden verse qué características están habilitadas en los LE-311v:

```
LE311> software license show
```

Con el siguiente comando se puede instalar una licencia:

```
LE311> software license install licence-key <licence key>
```

Nombre del sistema:

```
LE311> System set hostname gon-2
```

IP de administración:

```
gon-2> Interface local set ip 192.168.0.2
```

Aumentando el tiempo de espera del sistema para cerrar la sesión:

```
gon-2> system shell set global-login-timeout 300
```

5.2.1. Prueba 1: 2 túneles sin protección

En el modo túnel, todo el paquete IP es cifrado o autenticado. Debe ser entonces encapsulado en un nuevo paquete IP para que funcione el enrutamiento. El modo túnel se utiliza para comunicaciones red a red (túneles seguros entre *routers*, p.e. para VPNs) o comunicaciones ordenador a red u ordenador a ordenador sobre internet.

5.2.1.1. Objetivo

El objetivo de esta prueba es crear dos túneles PBT entre los LE-311v de modo que se pueda proveer dos servicios completamente separados (C-VIDs 300 y 307).

5.2.1.2. Escenario

La topología de triangulo nos permitió crear un túnel directo entre gon-2 puerto 26 y gon-3 puerto 26 usando la B-VID *(Backbone* VLAN ID) 501, la cual transporta la C-VID 300. También se creó un túnel indirecto con B-VID 505 ente puerto 25 de gon-2 y el puerto 25 de gon-3, pasando por gon-1 puertos 25 y 26.

5.2.1.3. Configuración

Los B-VIDs son configurados así:

```
pbt reserve bvid 501
pbt reserve bvid 505
```

Nuevemante, se crean los componentes “encap” y “decap”.

Configuración de gon-2:

```
tunnel encap create static-pbt a_gon-3 b-vid 505 dest-bridge-name gon-3 port 25
tunnel encap create static-pbt 501_a_gon-3 b-vid 501 dest-bridge-name gon-3 port 26
tunnel decap create static-pbt cs- desde_gon-3 b-vid 505 src-bridge-name gon-3 port 25
tunnel decap create static-pbt 501_from_3 b-vid 501 src-bridge-name gon-3 port 26
tunnel pair create tnl-pair gon-3 encap-pbt a_gon-3 decap-pbt desde_gon-3
tunnel pair create tnl-pair 501_tunnel encap-pbt 501_a_gon-3 decap-pbt 501_desde_gon-3
```

Los nombres de los puentes remotos (“*remote bridges*”) que se ven en la configuración de arriba son creados usando el siguiente comando:

```
pbt remote-bridge create bridge-name gon-3 bridge-mac 02:00:11:00:00:13
```

Para establecer las direcciones MAC de los *remote bridges* se usa el siguiente comando:

```
gon-3> pbt show
+---------------------------------------------- PBT Attributes ----------------------------------------------+
| PBT Bridge MAC                                 | 00:03:18:67:4d:c0
|
```

La dirección MAC de los puentes PBT puede ser sobre-escrita usando el siguiente comando:

```
pbt set bridge-mac 02:00:11:00:00:13 service-tag-ethertype 0x88b5
```

En PBT se crean circuitos y *switches* virtuales para llevar y seleccionar los servicios de los clientes. Un circuito virtual es lo que el IEEE llama un *"service instance",* el cual es especificado por una etiqueta I-SID (*Backbone Service Instance Identifier*) con encapsulación 802.1ah. Un circuito virtual selecciona tráfico de un usuario en particular que entra al puerto del LE-311v.

Configuración de gon-2:

```
virtual-circuit pbt create static-vc vs_307 egress-isid 307 ingress-isid 307 tunnel a_gon-3
virtual-circuit pbt create static-vc 501_vc egress-isid 300 ingress-isid 300 tunnel 501_a_gon-3
virtual-switch add reserved-vlan 4090-4094
virtual-switch ethernet create vs vs_307 vc vs_307
virtual-switch ethernet create vs vs_300_501 vc 501_vc
virtual-switch ethernet add vs vs_307 port 10 vlan 307
virtual-switch ethernet add vs vs_300_501 port 10 vlan 300
```

El rango de VLAN de 4091 a 4094 fue reservado para uso de los *switches* virtuales. No es necesario que los valores de I-SID coincidan con los valores de C-VID.

El *switch* gon-1 que conecta los *switches* gon-2 y gon-3 requiere de configuración adicional para que funcione el túnel indirecto:

```
vlan create vlan 505
vlan add vlan 505 port 25
vlan add vlan 505 port 26
```

5.2.1.4. Resultados

Los dos túneles PBT fueron probados enviando 10,000 pines entre los nodos PC-1 (10.10.1.1/8) y PC-2 (10.10.1.2/8) para la C-VID 300, y entre PC-3 (10.20.1.1/8) y PC-4 (10.20.1.2/8) para la C-VID 307.

No se encontró ningún descarte de paquetes para las C-VID 300 o 307.

El comando *"tunnel show"* refleja el estado de los túneles:

```
gon-2> tunnel show

+---------------------------------------- ENCAP TUNNEL TABLE ----------------------------------------+
|                        |                 |       State       |                 |         |         |         |
|Name                    |Type             |Oper   |Admin|Destination  |B-VID  |Role     |Active |
+------------------------+-----------------+---------+---------+-----------------+---------+--------+---------+
|501_a_gon-3             |encap-pbt     |En      |En       |gon-3           |501     |pri      |Yes      |
```

```
|a_gon-3                |encap-pbt    |En      |En       |gon-3          |505     |pri     |Yes     |
+-----------------------+-------------+--------+---------+---------------+--------+--------+--------+

+---------------------------------------DECAP TUNNEL TABLE ----------------------------------------+
|                            |                      | Oper     |
|
|Name                        |Type                  | State    | B-VID
|
+----------------------------+----------------------+----------+-------------------------------------------+
|501_desde_gon-3     |decap-pbt          | En          | 501                                          |
|desde_gon-3             |decap-pbt          | En          | 505                                           |
+----------------------------+----------------------+----------+-------------------------------------------+
```

5.2.2. Prueba 2: monitoreo del estado del enlace

A continuación se muestra el objetivo principal del monitoreo del estado de enlace.

5.2.2.1. Objetivo

Monitorear el estado de los túneles PBT usando CFM CCMs (Continuity Check Messages).

5.2.2.2. Escenario

Establecer sesiones para los dos túneles PBT y para las dos conexiones I-SID entre ellos.

5.2.2.3. Configuración

Configuración en gon-2:

```
cfm enable
cfm service create static-pbt 501_a_gon-3 name cfm_test level 4 next-mepid 100
cfm service enable service cfm_test
cfm service create static-pbt a_gon-3 name cfm_test_2 level 4 next-mepid 400
cfm service enable service cfm_test_2
```

5.2.2.4. Resultados

El monitoreo CCM reflejo apropiadamente los cambios en el estado de los túneles PBT y de las conexiones de *switch* virtuales cuando los puertos de los LE-311v en cuestión fueron desconectados.

```
gon-2> cfm remote-mep show
+---------------------------------------- CFM REMOTE MEPS ----------------------------------------+
|                    |          |                        |State      |Total     |Seq  |Last          |Fault    |
|Service             |Mepid |MAC Address        |Ad  |Op  |Rx CCM |Error|Seq Num   |F |P |R |
+--------------------+------+-------------------+----+----+-------+-----+----------+--+--+--+
|cfm_test            |200   |02:00:11:00:00:13 |en  |en  |73060  |0    |73060     |  |  |  |
+--------------------+------+-------------------+----+----+-------+-----+----------+--+--+--+
|cfm_test_2          |300   |02:00:11:00:00:13 |en  |en  |73057  |0    |73057     |  |  |  |
+--------------------+------+-------------------+----+----+-------+-----+----------+--+--+--+
```

```
gon-2> cfm remote-mep show
+------------------------------------------ CFM REMOTE MEPS ------------------------------------------+
|                    |          |                          |State      |Total     |Seq  |Last          |Fault    |
|Service             |Mepid |MAC Address         |Ad  |Op  |Rx CCM |Error|Seq Num  |F |P |R |
+--------------------+---------+------------------------+-----+-----+-----------+-------+--------------+--+--+---+
|cfm_test            |200      |02:00:11:00:00:13 |en   |en   |72327   |0       |72327       |X |   |   |
+--------------------+---------+------------------------+-----+-----+-----------+-------+--------------+--+--+---+
|cfm_test_2          |300      |02:00:11:00:00:13 |en   |en   |73198   |0       |73198       |X |   |   |
+--------------------+---------+------------------------+-----+-----+-----------+-------+--------------+--+--+---+
```

5.2.3. Prueba 3: confiabilidad del túnel PBT

A continuación se mustra el objetivo principal de la confiabilidad del túnel PBT.

5.2.3.1. Objetivo

Confirmar que los túneles PBT pueden conmutar rápidamente del primario al secundario en caso de que falle el primario.

5.2.3.2. Escenario

Configurar un túnel de respaldo para el túnel primario que va de gon-2 a gon-3 vía gon-1 y luego crear a través de él una sesión CFM.

En enlace entre gon-2 y gon-3 puede ser deshabilitado ya sea por línea de comandos o por medio de la desconexión física del cable de un puerto.

5.2.3.3. Configuración

La configuración es muy similar a la de los túneles primarios que se han creado.

```
tunnel encap create static-pbt a_gon-3 b-vid 505 dest-bridge-name gon-3 port 25
tunnel encap create static-pbt 501_a_gon-3 b-vid 501 dest-bridge-name gon-3 port 26
tunnel encap create static-backup-pbt to_gon-2 b-vid 605 dest-bridge-name gon-3 port 26
tunnel decap create static-pbt desde_gon-3 b-vid 505 src-bridge-name gon-3 port 25
tunnel decap create static-pbt 501_desde_gon-3 b-vid 501 src-bridge-name gon-3 port 26
tunnel decap create static-pbt bkp_desde_gon-3 b-vid 605 src-bridge-name gon-3 port 26
tunnel pair create tnl-pair gon-3 encap-pbt a_gon-3 decap-pbt desde_gon-3
tunnel pair create tnl-pair 501_tunnel encap-pbt 501_a_gon-3 decap-pbt 501_desde_gon-3
tunnel pair create tnl-pair a_gon-3_backup encap-backup-pbt a_gon-3 decap-pbt
bkp_from_cs-
    3
virtual-circuit pbt create static-vc vs_307 egress-isid 307 ingress-isid 307 tunnel a_gon-3
virtual-circuit pbt create static-vc 501_vc egress-isid 300 ingress-isid 300 tunnel 501_a_gon-3
```

El intervalo entre los mensajes CCM es muy importante dado que la conmutación toma lugar solo después de que se pierden 3 mensajes CCM sucesivos. El intervalo CCM fue dejado a l segundo, que es el valor por defecto.

5.2.3.4. Resultados

El comando *"tunnel show*" muestra una vez más el estado de los túneles:

```
gon-2> tunnel show
```

```
+-------------------------------------- ENCAP TUNNEL TABLE ----------------------------------------+
|                     |                  |State             |                    |          |         |
|Name               |Type              |Oper  |Admin |Destination     |B-VID   |Role   |Active |
+-------------------+------------------+------------------+------------------+----------+--------+ --------+
|501_a_gon-3    |encap-pbt      |En      |En         |gon-3              |501      |pri      |Yes      |
|501_a_gon-3    |encap-pbt      |Dis     |En         |gon-3              |505      |pri      |No       |
|a_gon-3           |encap-pbt      |En      |En         |gon-3              |605      |bkp     |Yes     |
+-------------------+------------------+------------------+------------------+----------+--------+ --------+
+-----------------------------------------DECAP TUNNEL TABLE -------------------------------------+
|                              |                        | Oper      |                                          |
|Name                        |Ty                      | State     | B-VID                                     |
+----------------------------+--------------------+-------------+---------------------------------- ----------+
|501_desde_gon-3       |decap-pbt          | En          | 501                                      |
|desde_gon-3              |decap-pbt          | Dis         | 505                                       |
|bkp_desde_gon-3       |decap-pbt          | En          | 605                                      |
+----------------------------+--------------------+-------------+---------------------------------- ----------+
```

Resultados del *ping*: solo se perdió un paquete:

```
Ping statistics for 10.10.1.1:
Packets: Sent = 18, Received = 17, Lost = 1 (5% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

5.2.4. Prueba 4: políticas de tráfico

A continuación se muestra el objetivo principal de las políticas de tráfico.

5.2.4.1. Objetivo

Investigar la capacidad de los LE-311v de aplicar políticas de tráfico por VLAN.

5.2.4.2. Escenario

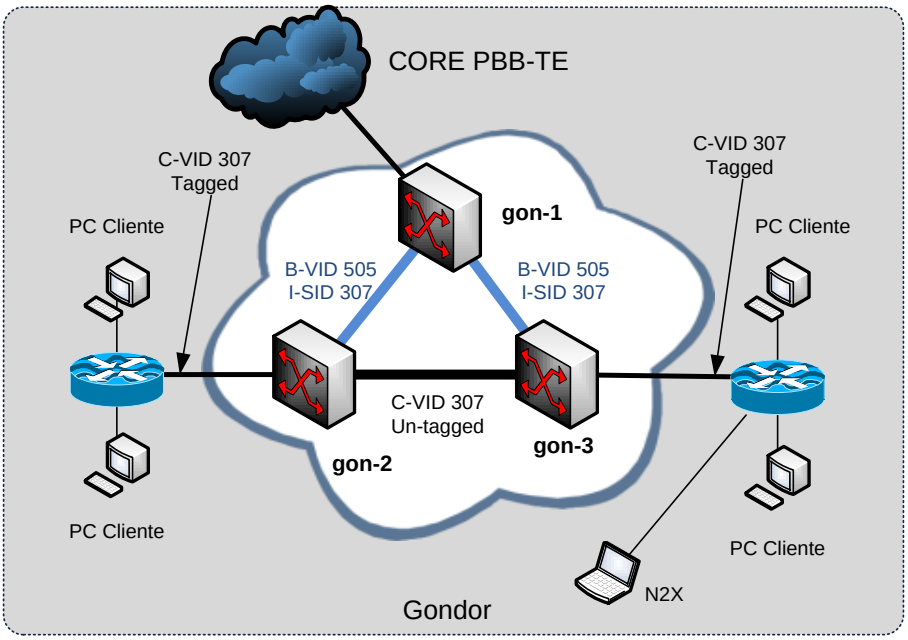
Un generador de tráfico N2X Agilent fue usado para enviar paquetes de Ethernet desde la VLAN 307 en un Cisco 2950 a través del túnel PBT indirecto con B-VID 505 (pasando por el gon-2 puerto 25 al gon-3 puerto 25, vía el gon-1 puerto 25 y 26), terminando en la VLAN 307 en el otro Cisco 2950.

Las políticas fueron definidas para el tráfico de ingreso basando en el puerto de ingreso y el número de VLAN. El generador de tráfico Agilent N2X fue usado para enviar cuadros Ethernet a un puerto de usuario, empezando por un nivel por debajo del límite impuesto por la política y aumentando gradualmente para exceder este límite. El segundo puerto del Agilent fue usado para el tráfico de la B-VID 505.

El policer incluye la creación de un perfil que define un CIR y un PIR por puerto y por VLAN:

```
traffic-profiling Estándar-profile create port 10 profile 1 cir 25600 pir 51200 name policer_307
vlan 307
traffic-profiling set port 10 mode Estándar-vlan
```

Figura 43. **Red de pruebas para políticas de tráfico**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 124.

Luego hay que habilitar la política:

```
traffic-profiling enable port 10
traffic-profiling enable
```

La política de arriba fue aplicada a gon-3 para el tráfico de ingreso al puerto 10 con CIR = 25600 kbit/s y PIR 51200 kbit/s. Se aplicó en modo de VLAN lo que significa que los cuadros de usuario son seleccionados basándose en la etiqueta de VLAN; esto solo funciona si el puerto de ingreso hace encapsulación MAC-in-MAC.

5.2.4.3. Resultados

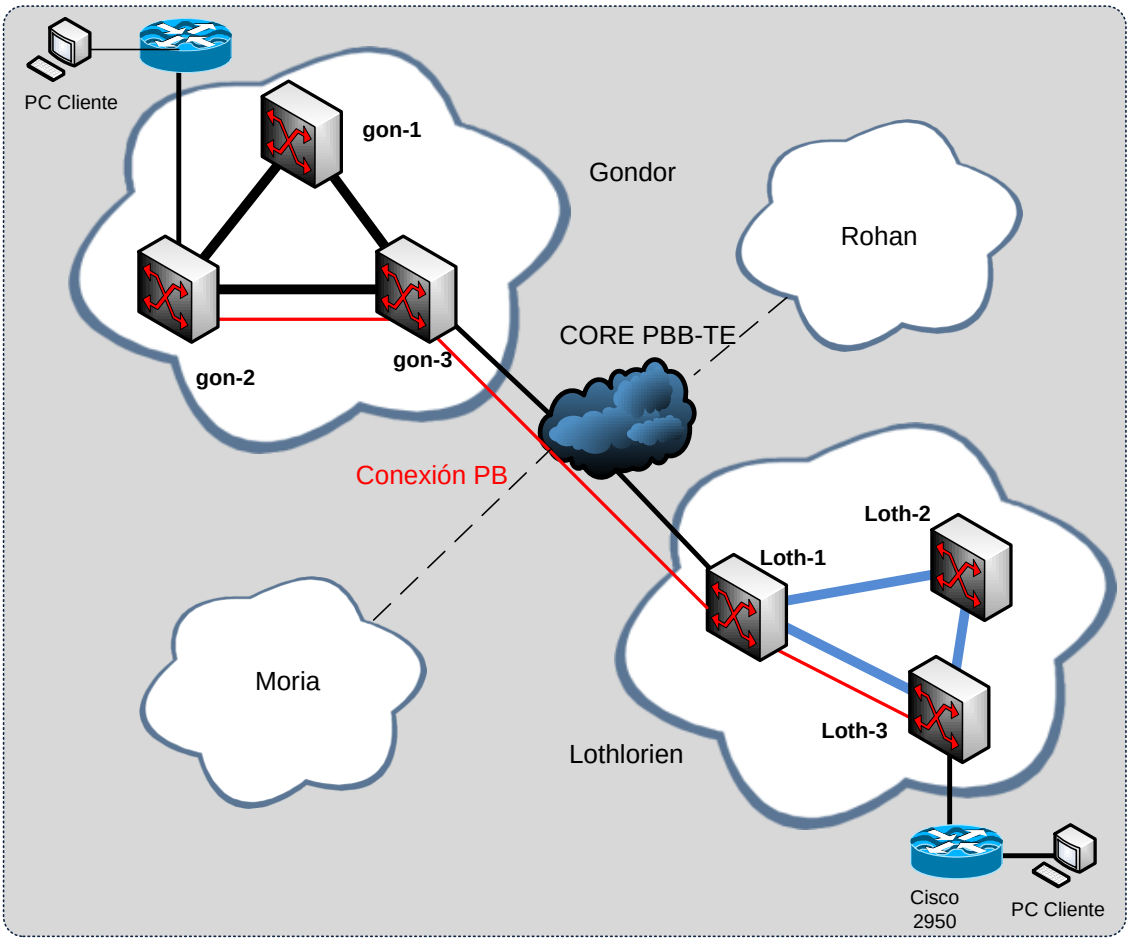
El tráfico de entrada desde el puerto 102/1 fue incrementado hasta el 100 % en la interface de 100 Mb/s, el policer hizo caer el tráfico a 37 Mb/s.

El CIR y el PIR cuentan todos los bytes de los cuadros Ethernet, es decir, encabezado y carga útil. Siendo aplicado en modo de VLAN, un policer trabaja en los paquetes encapsulados de modo que toma en cuenta la jerarquía de encabezados completa (todos los campos en el encabezado MAC-in-MAC).

5.3. Pruebas Lothlórien – Gondor

La idea inicial de esta prueba era usar túneles PBB-TE dentro de cada red local y dentro de la red Core y usar encapsulación PB en las interfaces con la red Core tal como se muestra en la figura 44.

Figura 44. **Red PB/PBB-TE/PB Lothlórien-Gondor**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 126.

Este escenario de pruebas es preferible por varias razones. Primero, es compatible con la especificación MEF E-NNI dado que la encapsulación PB lleva un delimitador de servicio S-VID en la VLAN externa. Segundo, usa PBB-TE con soporte de ingeniería de tráfico y (potencialmente) soporte de "*fast protection switching*". Tercero, los túneles PBB-TE de cada red de pruebas son independientes entre sí,de modo que no se necesita ninguna coordinación, tal como el aprendizaje mutuo de direcciones MAC.

Sin embargo, este escenario no fue posible de implementar debido a que los LE- 311v usados en ambas redes Lothlórien y Gondor tienen una flexibilidad muy limitada. El origen de este problema reside en el mecanismo PBB-TE: cuando un *switch* LE-311v acepta un cuadro de cliente y lo encapsula en el túnel PBB-TE, hace una operación interna intermedia: mapea el C-VID (o el nombre de una interface si el mapeo en el número de interface y no en el valor de C-VID) dentro de la S-VID y luego mapea el S-VID dentro del I-SID de la conexión PBB-TE.

En otras palabras, un *switch* LE-311v usa una encapsulación PB interna antes de encapsular un cuadro de cliente en el formato PBB-TE. Esta encapsulación PB intermedia es lo que se necesita en el extremo lejano de un túnel PBB-TE para tener un cuadro con S-VID como delimitador de servicio. Sin embargo, en el extremo lejano de un túnel PBB-TE un *switch* LE-311v extrae un cuadro de cliente de la encapsulación PBB-TE y lo manda más lejos. Así, en un cuadro que sale del túnel PBB-TE encontramos un C-VID y no un S-VID.

Por lo tanto, no hay modo de producir un cuadro en formato PB después de haber usado un túnel PBB-TE dentro de un *switch* LE-311v. El único modo de tener S-VID como un delimitador de servicio entre dominios LE-311v es usar la encapsulación PB dentro de los dominios también. Este es el escenario que se probó en Lothlórien y Gondor.

El valor 150 fue escogido para la S-VID en la dirección de Lothlórien a Gondor y el valor de 150 fue escogido para la dirección contraria.

El valor C-VID en ambas direcciones es de 700.

5.3.1. Lothlórien

Configuración de LOTH-1:

```
vlan create vlan 150

system set host-name loth-1

vlan add vlan 150 port 25
vlan add vlan 150 port 27

vlan rename vlan 150 name Gondor
vlan set vlan 150 statistics enable

pbt set bridge-mac 04:00:00:00:00:01

virtual-switch add reserved-vlan 4090-4094

cfm enable

cfm mip create vlan 150 port 25 level 3
cfm mip create vlan 150 port 27 level 3
```

Configuración de LOTH-3:

```
vlan create vlan 150

system set host-name loth-3
```

```
vlan add vlan 150 port 25

vlan rename vlan 150 name QinQ-Gondor

virtual-circuit ethernet create vc Gondor vlan 150

virtual-switch add reserved-vlan 4090-4094

virtual-switch ethernet create vs Gondor vc Gondor

virtual-switch ethernet add vs Gondor port 10 vlan 700

cfm enable

cfm service create vs Gondor name Gondor_150 next-mepid 500

cfm service enable service Gondor_150
```

5.3.2. Gondor

Configuración de GON-1:

```
vlan create vlan 505,510

system set host-name gon-1
vlan add vlan 505 port 25
vlan add vlan 505,510 port 26
vlan add vlan 510 port 28

vlan rename vlan 510 name QinQ-Gondor
```

```
cfm enable

cfm mip create vlan 510 port 26 level 4
cfm mip create vlan 510 port 28 level 4
```

Configuración de GON-3:

```
vlan create vlan 510

system set host-name gon-3

vlan remove vlan 127,1 port 1
 vlan remove vlan 127,1 port 2
vlan remove vlan 127,1 port 10
vlan add vlan 510 port 25

vlan rename vlan 510 name QinQ-Gondor

pbt reserve bvid 501
pbt reserve bvid 505

pbt remote-bridge create bridge-name gon-2 bridge-mac 00:03:18:67:4d:60

b-vid 505 dest-bridge-name gon-2
port 25
tunnel encap create static-pbt 501_to_gon-2 b-vid 501 dest-bridge-name gon-2 port 26
tunnel decap create static-pbt from_gon-2 b-vid 505 src-bridge-name gon-2 port 25
tunnel decap create static-pbt 501_from_gon-2 b-vid 501 src-bridge-name gon-2 port 26

encap-pbt to_gon-2
decap-pbt from_gon-2
```

```
tunnel pair create tnl-pair 501_tunnel encap-pbt 501_to_gon-2 decap-pbt 501_from_gon-2

virtual-switch add reserved-vlan 4090-4094

virtual-switch ethernet create vs vs_307 vc vs_307
virtual-switch ethernet create vs vs_300_501 vc 501_vc
virtual-switch ethernet create vs Gondor vc Gondor

virtual-switch ethernet add vs vs_307 port 1 vlan 307
virtual-switch ethernet add vs vs_300_501 port 2 vlan 300
virtual-switch ethernet add vs Gondor port 10 vlan 700

cfm enable

cfm service create vs Gondor name Gondor_150 level 4 next-mepid 601
cfm service enable service Gondor_150

cfm mep create service Gondor_150 port 10 vlan 700 type up mepid 600
```

5.3.3. Resultados

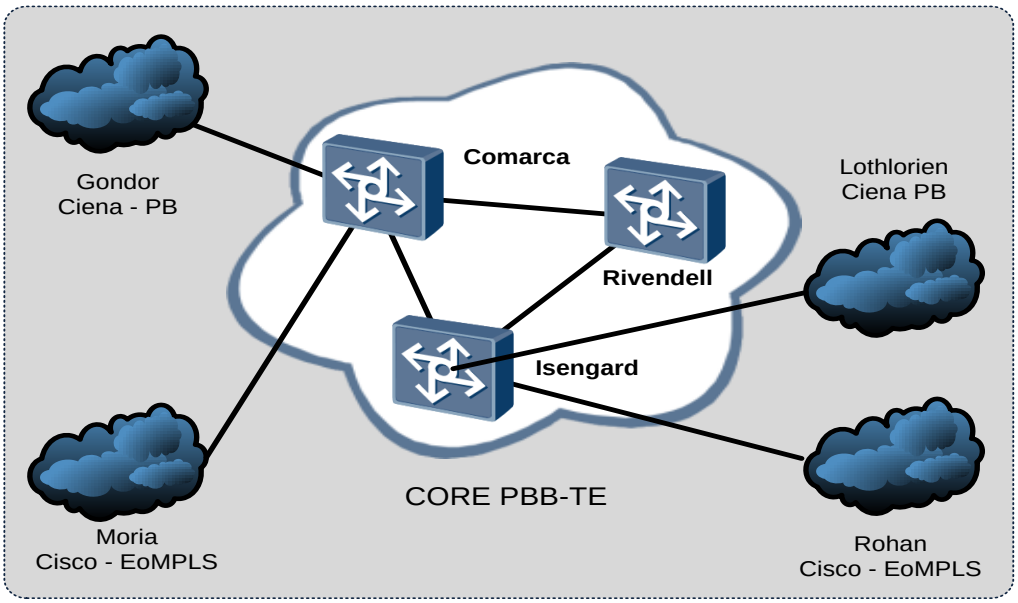
No hubo problemas con el establecimiento de las conexiones PB entre las redes de Lothlórien y Gondor. De hecho, fue una operación muy simple dado que los *switches* en cuestión era todos de la misma marca – Ciena.

Se estableció una sesión CCM para la conexión y está mostró el estado de la conexión. Se hicieron pruebas de *ping* y *telnet* entre las computadoras cliente conectadas a cada extremo, todas fueron exitosas.

6. CONSTRUCCIÓN DE UNA RED PBB-TE

La red Core se hizo con tres *switches* Ciena 5305 conectados por enlaces de 1 Gbps. El diagrama se muestra a continuación:

Figura 45. **El Core Carrier Ethernet**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 127.

Los *switches* Core están localizados en Rivendell, Isengard y La Comarca.

Los *switches* Core fueron conectados por enlaces de 1 Gbps a las 4 redes locales en Moria, Rohan, Lothlórien y Gondor.

Las redes de Moria y Rohan son EoMPLS, mientras que las redes en Gondor y Lothlórien son PB.

La configuración de los *switches* Core (túneles PBB-TE, grupos de túneles, puertos, sub-puertos, entre otros.), usan la siguiente convención de nombres:

- Switch Isengard: isen, o 1
- Switch La Comarca: com, o 2
- Switch Rivendell: riv, o 3

Redes locales:

- Lothlórien: 1
- Rohan: 2
- Moria: 3
- Gondor: 4

6.1. Túneles PBB-TE

Tres pares de túneles PBB-TE se usaron para pasar el tráfico de las redes locales a través del Core, y tres pares de túneles PBB-TE se establecieron para proporcionar redundancia.

Considérense los túneles isen-1 a riv-3 como ejemplo. En el *switch* ‘isen-1’, los túneles ‘isen-riv-group” fueron establecidos para proveer conectividad redundante al *switch* ‘riv-3’.

Para este grupo de túneles se establecieron dos túneles PBB-TE:

- “130-encap-isen-riv” – túnel primario
- “1230-encap-isen-riv” – túnel secundario

El segundo nombre es el resultado de conectar los *switches* 1 y 3 a través del *switch* intermedio 2.

Como se verá, los valores B-VID de los túneles coinciden con los partes numéricas de los nombres, por ejemplo el túnel ‘130-encap-isen-riv’ tiene B-VID 130.

El papel de los túneles dentro de un tunnel-group está determinado por sus pesos, mientras más pesado es el túnel, más alta prioridad se ha usado para la conectividad del grupo. Debido a esto el túnel ‘130-encap-isen-riv’ recibió peso 8 mientras que el túnel ‘1230-isen-riv’ recibió peso 1, de modo que ‘130-encap-isen-riv’ siempre es usado mientras este arriba mientras que “1230-isen-riv” es usado solo si el primero esta caído.

La configuración del grupo “isen-riv” fue como sigue:

```
pbt tunnel-group create group isen-riv group tunnel-sync on logical-id 1

pbt encap-tunnel create static-encap 130-encap-isen-riv dest-bridge-name riv-3 port 7/1 bvid 130 logical-id 1 tunnel-group isen-riv-group pair-index 1 weight 8

pbt encap-tunnel create static-encap 1230-encap-isen-riv dest-bridge-name riv-3 port 7/2 bvid 1230 logical-id 4 tunnel-group isen-riv-group pair-index 4 weight
```

```
1

pbt decap-tunnel create static-decap 130-decap-isen-isen port 7/1 bvid 130
logical-id 1 tunnel-group isen-riv-group pair-index 1

pbt decap-tunnel create static-decap 1230-decap-isen-riv port 7/2 bvid 1230
logical-id 4 src-bridge-name isen-1 tunnel-group isen-riv-group pair-index 4
```

Los túneles usan B-VIDs. La configuración de la contraparte del túnel en el *switch* isen-1 es similar, por lo cual no se muestra.

La configuración del túnel secundario es específica debido a que no es un túnel directo entre dos *switches* adyacentes. En vez de eso, el túnel secundario pasa por un *switch* intermedio com-2 (el cual provee redundancia en caso de que falle el enlace principal 7/1).

La configuración del *switch* com-2 para soportar un túnel secundario usa una técnica de Ciena para túneles PBB-TE:

```
pbt transit create pbt-transit TRANSIT-1230-702 parent-port 7/2 logical-id 3

pbt transit add pbt-transit TRANSIT-1230-702 class-element 1 bvid 1230

pbt transit create pbt-transit TRANSIT-1230-701 parent-port 7/1 logical-id 4

pbt transit add pbt-transit TRANSIT-1230-701 class-element 1 bvid 1230
```

Los túneles de tránsito conectan los puertos con sus respectivos B-VIDs.

En la figura 45, solo se muestra un túnel secundario, entre riv-3 y isen 1 – solo para que el diagrama siga siendo legible. Los otros dos túneles secundarios se establecen del mismo modo.

6.2. Conectividad NNI (Network to Network Interface).

A continuación se muestra el objetivo principal de la conectividad NNI.

6.2.1. Objetivo

La función principal del Core es soportar las conexiones entre las redes locales. Por lo tanto, el objetivo de esta prueba es verificar si el Core es capaz de conectar las redes locales que usan diferentes tecnologías (como EoMPLS y PBB-TE) y transportar el tráfico de forma transparente.

6.2.2. Escenario

Se escogió el valor de VLAN ID como delimitador común para ambas tecnologías. En la figura 45 estos VLAN IDs son mostrados como S-VIDs (Service VLAN ID) de acuerdo a la terminología Ethernet. El escenario escogido para el Core cumple con el estándar E-NNI (External Network to Network Interface) de MEF.

Los valores de VLAN ID para conectividad entre las redes locales fueron asignados de acuerdo con los números previamente asignados a estas redes locales, tal como se verá más adelante.

Se probó la capacidad de Core de traducir las S-VIDs de los clientes (que le da a los clientes la libertad de usar sus propias S-VID, lo cual simplifica la interoperabilidad). Por lo tanto, diferentes valores de S-VID fueron asignados para cada dirección de la conexión entre dos redes locales.

El Core traduce los S-VID a la salida, es decir, acepta tráfico desde Lothlórien con S-VID X y lo envía a Gondor con S-VID Y.

La indicación de éxito fue entonces que ambos extremos pudieran comunicarse exitosamente.

6.2.3. Configuración

La configuración de los *switches* Core para seleccionar tráfico de cliente y traducir S-VIDs está basada en la técnica de sub-puertos de Ciena.

Considérese el *switch* “riv-3”. Para soportar una conexión entre Lothlórien y Gondor se usó la siguiente configuración:

```
sub-port create sub-port lothlorien -gondor-subport parent-port 7/24 classifier-precedence 2 logical-id 2 egress-l2-transform stamp-*.450.*

sub-port add sub-port lothlorien-gondor-subport class-element 1 vtag-stack 450
```

La primera declaración crea un subpuerto llamado “lothlorien-gondor-subport” para el puerto físico 7/24, el cual está conectado al enlace con

Lothlórien. La declaración instruye al *switch* a poner S-VID 450 en la etiqueta de VLAN exterior. Esto significa que los cuadros que van de Gondor a Lothlórien tendrán valor S-VID = 450 sin importar el valor original.

La segunda declaración añade un selector al subpuerto “lothlorien-gondor-subport”, el cual dice al sub-puerto que el tráfico con S-VID = 450 debería de detectarse en la interface física 7/24 para este sub-puerto lógico.

Para transferir tráfico seleccionado por un subpuerto a través de un túnel PBB-TE es necesario crear un “*customer* I-SID” (I-SID de cliente, análogo a una conexión *pseudo-wire* en MPLS) para este túnel PBB-TE y un *switch* virtual para conectar un sub-puerto y una conexión I-SID.

Esto se logra con las siguientes declaraciones:

```
pbt service create service lothlorien-gondor-conn-1 ingress-isid 450 egress-isid 540 logical-id 2 tunnel-group lond-warr-group

virtual-switch create vs lothlorien-gondor-vs logical-id 2

virtual-switch interface attach sub-port lothlorien-gondor-subport vs lothlorien-gondor-vs

virtual-switch interface attach pbt-service lothlorien-gondor-conn-1 vs lothlorien-gondor-vs
```

6.2.4. Resultados

Los resultados de la prueba fueron positivos, el Core manejo exitosamente la conexión entre las redes locales (el resultado de estas pruebas exitosas es descrito más adelante).

Se interconectaron las siguientes redes locales, en pares:

- Lothlórien - Gondor (conexión de tipo PB/PBB-TE/PB).
- Rohan - Moria (conexión de tipo EoMPLS/PBB-TE/EoMPLS).

El Core paso el tráfico entre las redes locales de modo transparente, no se detectó ningún problema con el filtrado de ningún tipo de tráfico.

La primera conexión fue del tipo PB/PBB-TE/PB, lo que significa que los cuadros llegaron a las interfaces de ingreso del Core (E-NNIs) como cuadros encapsulados como QinQ (PB), con un S-VID en la etiqueta de VLAN exterior. Luego fueron encapsulados en cuadros PBB-TE y transferidos a través del Core en ese formato. En la interface de salida del Core, se removieron los encabezados PBB-TE de los cuadros y estos fueron enviados a sus redes de destino en el formato PB original con el S-VID cambiado en el valor asignado para la red de destino.

La segunda conexión (Rohan - Moria) era del tipo EoMPLS/PBB-TE/EoMPLS. El trabajo de los *switches* del Core en transferir cuadros EoMPLS a través del Core fue similar al caso anterior. Mientras ambas redes Rohan y Moria producen cuadros EoMPLS con valores S-VID en la etiqueta de VLAN exterior, los *switches* del Core se las arreglaron para seleccionar esos cuadros y dirigirlos a sus respectivas conexiones I-SID en el Core. La existencia de dos

encabezados MPLS (para un túnel MPLS y un *pseudo-wire*) fue transparente para los *switches* del Core, dado que ellos solo prestan atención a la etiqueta de VLAN exterior en los bordes y a los encabezados PBB-TE en las interfaces de tránsito.

6.2.5. Problemas encontrados

No se encontró ningún problema.

6.3. Conmutación de los túneles en caso de falla

A continuación, se describe el objetivo principal de la conmutación de túneles en caso de que se presentara una falla.

6.3.1. Objetivo

Probar la capacidad de los *switches* Core para proteger los *tunnel-groups* conmutando de un grupo de túneles primario a uno secundario cuando el primario esta abajo (como sucedería después de una falla).

6.3.2. Escenario

Se dejó un ping extendido (en ambas direcciones), entre Lothlórien y Gondor con el intervalo de *ping* ajustado a 100 ms. Después de cierto tiempo, el puerto 7/1 del *switch isen*-1 fue desconectado por línea de comandos, y tiempo después las secciones de *ping* fueron detenidas para ver el número de pines perdidos. El estado de los túneles del grupo “isen-com” también fue grabado. A continuación, las sesiones de ping fueron resumidas y el puerto 7/1

fue activado de nuevo. Este procedimiento se repitió y el número de pines perdidos y el estado de los túneles fue grabado de nuevo.

6.3.3. Configuración

La configuración de los grupos de túneles protegidos y las sesiones CCM (Connectivity Check Management), que monitorean el estado del túnel son como se describe arriba.

6.3.4. Resultados

Los resultados fueron grabados en ambos lados – Lothlórien y Gondor. Los resultados muestran que la conmutación de protección funciona correctamente en todos los casos (el test fue repetido 5 veces), y en el intervalo esperado de 300 ms (3 veces el intervalo CCM, dado que la pérdida de 3 CCMs consecutivos dispara la protección). El número de pines perdidos durante la conmutación del túnel primario al secundario fue en todos los casos entre 0 y 2.

Cuando se restableció el Puerto 7/1, sucedió la protección inversa de conmutación (con un retraso de aproximadamente 10 segundos después de restaurar el estado del puerto). El número de pines perdidos fue el mismo que cuando la conmutación se hizo directamente (entre 0 y 2). Después de consultar con el proveedor Ciena, la razón por el retraso en la conmutación inversa es que existe una característica de diseño para prevenir que la red oscile entre túneles cuando un puerto está experimentando conectividad errática.

6.3.5. Problemas encontrados

No se encontró ningún problema.

6.4. Operación y mantenimiento (OAM)

A continuación se muestra el objetivo principal de operación y mantenimiento.

6.4.1. Objetivo

Probar la capacidad jerárquica de OAM (Operation and Maintenance) Ethernet de monitorear el estado de los túneles del Core sin interferir con el tráfico del cliente y con las sesiones de OAM del mismo. El monitoreo del túnel Core se llevó a cabo por medio de 802.1ag/Y.1731 soportado por los switches Ciena 5305.

6.4.2. Escenario

Se establecieron sesiones CCM para los túneles primarios y secundarios de todos los "*tunnel-groups*" que conectan los *switches* Core. Para cada túnel, dos MEP (Maintenance Endpoints) fueron creados, uno a cada extremo del túnel. Cada MEP envía continuamente cuadros CCM hacia su contraparte al otro extremo a intervalos de 100 ms. Para prevenir interferencia con los CCMs de los clientes, las sesiones CCM del Core trabajan en la capa 3 dejando las capas 4 y 5 para el tráfico de los clientes.

Se usaron comandos "*show"* en los *switches* Ciena 5305 para verificar manualmente el estado de los túneles Core. El mecanismo CCM también fue

configurado y usado en la prueba de confiabilidad del Core, como el mecanismo principal para disparar la conmutación de protección (es decir, conmutación entre un túnel primario y otro secundario o bien entre un grupo de túneles).

Como los *switches* Ciena 5305 no soportan MIPs (Maintenance Intermediate Points) para los túneles PBT, este elemento del estándar CFM (IEEE 802.1ag Connectivity Fault Management) no pudo ser probado.

6.4.3. Configuración

La configuración siguiente es un ejemplo tomado del *switch* “riv-3”, ilustra el modo en que se monitoreó el grupo de túneles *“lond-read”:*

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
! CFM GLOBAL CONFIG:
!
cfm enable
!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!
CFM SERVICE CONFIG: ! cfm service create static-encap 130-encap-riv-isen name cfm-130-isen-riv next-mepid 311 ccm-interval 100msecCCM logical-id 1
cfm service enable service cfm-130-isen-riv
cfm service create static-encap 1230-encap-riv-isen name CFM-1230 next-mepid 2101 ccm- interval 100msecCCM logical-id 4
cfm service enable service CFM-1230
```

CCM nivel 3 es el nivel por defecto para las sesiones CCM de los *switches* Ciena 5305 (por eso es que esto no aparece en la configuración de arriba).

6.4.4. Resultados

Todas las pruebas Ethernet CCM dieron resultados positivos. Las sesiones entre los MEPs fueron establecidas sin problemas y mostraron el estado de los túneles correctamente.

Por ejemplo, el comando "cfm *remote show"* en riv-3 mostro lo siguiente:

```
riv-3 > cfm rem show

+------------------------------------------ CFM REMOTE MEPS -------------------------
--------------+
|                                |Mep   |                          |    State   |
|Total                                                                            |
|Service                    |ID      |Mac Address         |Ad  |Op  | Fault(s)   |
RX                                                                                |
+---------------------------+--------+-----------------------+-----+-----+------------+------
----------+
| cfm-130-isen-riv          |131     |02:00:00:10:00:01  |En  |En   |            |
179381712                                                                         |
| cfm-230-riv-com           |2300 |02:00:00:10:00:02  |En   |En   |            |
167539145                                                                         |
|PBT-1212                     |1212 |02:00:00:10:00:02  |En   |En  |            |
203524943                                                                         |
```

```
|CFM-1230                    |135    |02:00:00:10:00:01  |En   |En  |              |
166267693                                                                          |
+---------------------------+-------+-------------------------+-----+-----+-------------+-----
----------+
```

Cuando todos los túneles estaban en estado operacional y administrativo UP:

```
       riv-3 > pbt encap-tunnel show

       +------------------------------------------- ENCAP TUNNEL TABLE ------------
-------------------------+
       |                              |      State     |         |  Port     |Group    |Pair
|W        |CFM/  |
       |Name                         |Op    |Adm    |Fwd    |B-VID     | Name     |Index
|Index   |t    |y1731 |
       +---------------------------+-----+------+------+---------+----------+------------+-----
---+------+------+
       | 130-encap-riv-isen          |En   |En    |En    |130       |7/1       |1           |1
|8     | Y/N  |
       | 230-encap-riv-com           |En   |En    |En    |230       |7/2       |2           |1
|8     | Y/N  |
       | U_com-cec1                  |En   |En    |En    |1212      |7/2       |3           |1
|6     | Y/N  |
       | 1230-encap-riv-isen         |En   |En    |Dis   |1230      |7/2       |1           |4
|1     | Y/N  |
       +---------------------------+-----+------+------+---------+----------+------------+-----
---+------+------+
```

Cuando surgía un problema con algún túnel, la pantalla se veía como:

```
riv-3 > cfm rem show

+---------- CFM REMOTE MEPS ----------+
|          |Mep  |          | State  |
|Total                                |
|Service   |ID   |Mac Address |Ad |Op| Fault(s) |
RX                                    |
+----------+-------+----------+-----+----+----------+-----+
| cfm-130-isen-riv |131  |02:00:00:10:00:01 |En |En  |          |
179386189|
| cfm-230-riv-com  |2300 |02:00:00:10:00:02 |En |Di  |rMep      |
167543564|
|PBT-1212          |1212 |02:00:00:10:00:02 |En |En  |          |
203529420|
|CFM-1230          |135  |02:00:00:10:00:01 |En |En  |          |
166272170|
+----------+-------+----------+-----+-----+----------+-----+


riv-3 > pbt encap-tunnel show

+---------- ENCAP TUNNEL TABLE ----------+
```

	State		Port	Group	Pair	W
CFM/						
Name	Op	Adm	Fwd	B-VID	Name	Index	Index	t	y1731
130-encap-riv-isen	En	En	En	130	7/1	1	1	8	Y/N
230-encap-riv-com	Dis	En	Dis	230	7/2	2	1	8	Y/N
U_warr-cec1	En	En	En	1212	7/2	3	1	6	Y/N
1230-encap-lond-read	En	En	Dis	1230	7/2	1	4	1	Y/N

Esta situación corresponde a una MEP remota en com-2 caída. La sesión “cfm-230-riv-com” muestra una falla “rMep” y esta cambia el estado de “230-encap-riv-com” a leer “Di” (disable). Esto es específico a los *swiches* Ciena 5305, una falla en la sesión CCM que los túneles respectivos sean reportados como caídos.

6.4.5. Problemas encontrados

No se encontró ningún problema.

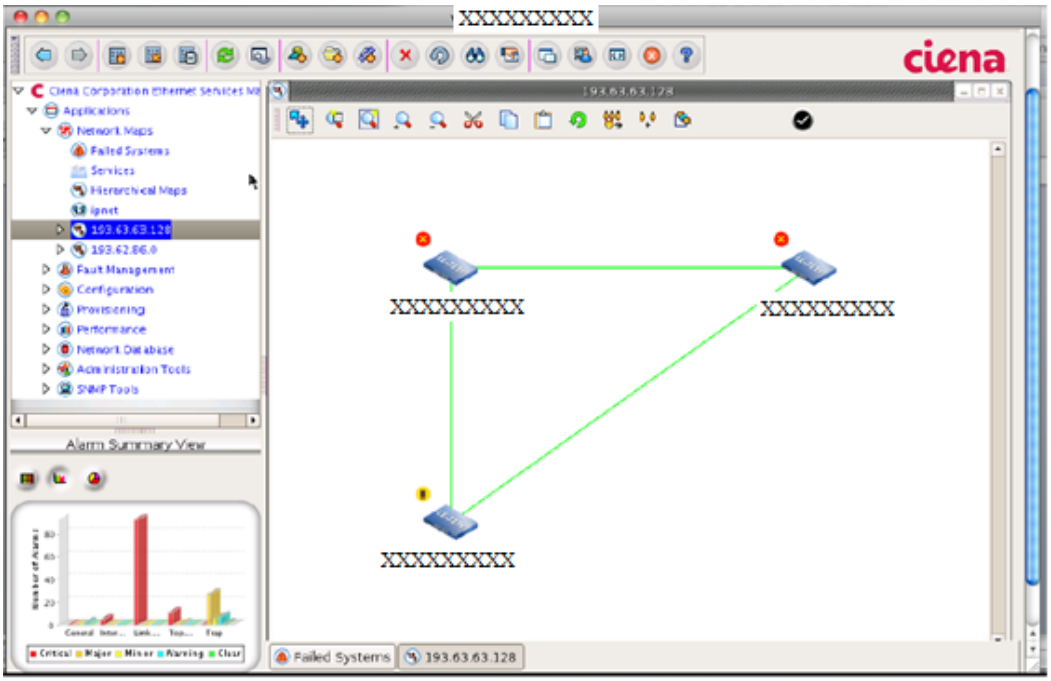
6.5. Administración y aprovisionamiento de la red

La habilidad para manejar y aprovisionar *switches* PBB-TE con un sistema de administración es muy importante dado que, en realidad, PBB-TE es una tecnología sin un plano de control (algunos documentos publicados en Internet describen extensiones GMPLS para PBB-TE pero ninguno ha sido implementado en verdadero equipo PBB-TE). Por lo tanto, los administradores de red tienen dos opciones para administrar redes PBB-TE:

- Aprovisionamiento y administración manual de cada dispositivo vía telnet o ssh.
- Aprovisionamiento y administración automatizada usando algún tipo de "Network Management System" (NMS – Sistema de Administración de la Red).

Durante el desarrollo de las pruebas, se intentó buscar un sistema de administración avanzada que pudiera soportar características de PBB-TE tales como Ingeniería de Tráfico (TE) y confiabilidad de modo automático. El soporte por parte de los distintos proveedores de equipo es también algo muy deseable, dado que la red de Tierra Media cuenta con muchas marcas de equipo.

Figura 46. **Mapa de los *switches* Ciena LE-311v**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 130.

Se escogió el Ethernet Service Manager (ESM) de Ciena como NMS. En Tierra Media ya se tenía alguna experiencia con el ESM, ya que se habían hecho demos con *switches* Ciena LE-311v.

Durante la realización de las pruebas se probó el ESM versión 5.4 manejando las redes del Core y Lothlórien. Los principales resultados de estas pruebas fueron:

- ESM puede descubrir *switches* 5305 y LE-311v en modo automático y visualizarlos en el modo de mapa de red (ver figura 36).

- Los eventos y alarmas generados por los *switches* fueron registrados y visualizados por el ESM, aunque de una forma poco amigable para el usuario.

- ESM soporta el aprovisionamiento de túneles PBB-TE protegidos y no protegidos *("tunnel-resilience"*) por medio de un script de aprovisionamiento. El script de aprovisionamiento puede aceptar la elección de extremos de los túneles haciendo clic en el mapa de red (ver figura 37).

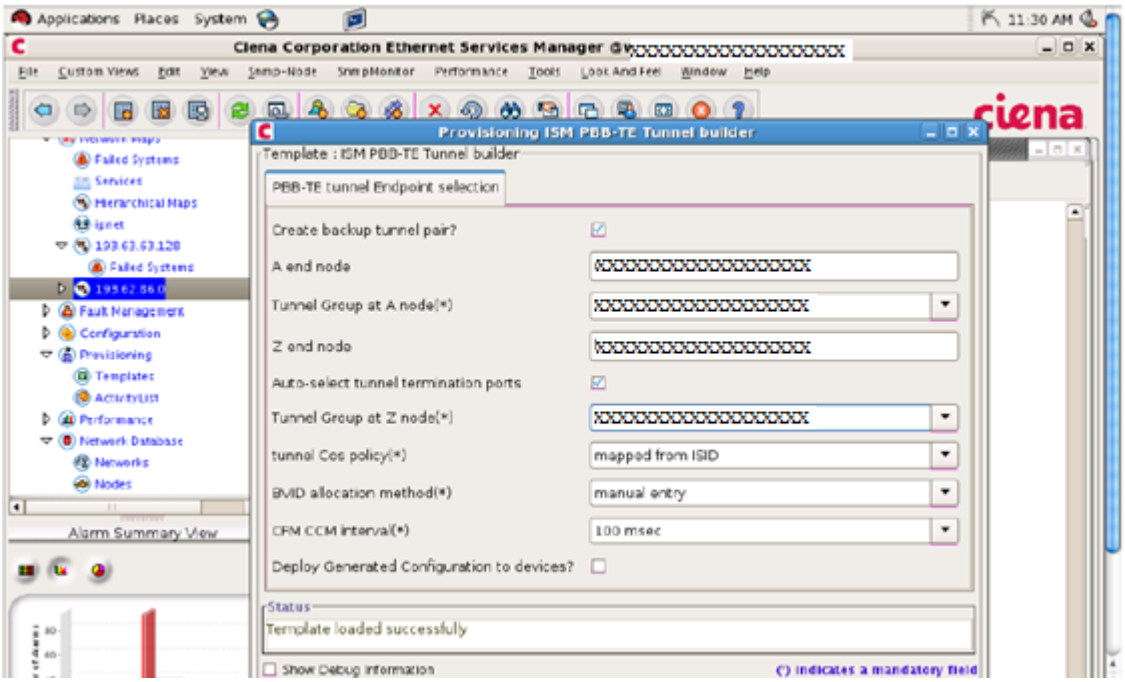
- ESM soporta el aprovisionamiento automático de conexiones I-SID de los clientes a través de los túneles PBB-TE existentes. En el caso de que el túnel entre dos puntos dados no exista, el *script* de aprovisionamiento de conexiones invoca al *script* de aprovisionamiento de túneles, el cual aprovisiona el túnel requerido.

- ESM puede desplegar la información de configuración producida por un script de aprovisionamiento usando telnet o ssh para acceder a los nodos de la red.

- Tanto las conexiones ESM y los scripts de aprovisionamiento de los túneles usan un conveniente método de automatización, el cual permite la intervención del administrador antes de desplegar la información de configuración: la información puede ser verificada por el administrador, el cual puede verla en la familiar CLI antes de confirmar/denegar su aprovisionamiento en los *switches*. Alternativamente, el administrador puede permitir el aprovisionamiento sin verificación si confía en los *scripts.*

- Desafortunadamente, las versiones del *script* de aprovisionamiento de túneles que se usan durante el proyecto no soportan las características de ingeniería de Tráfico (TE) de PBB-TE. De hecho, el *script* de aprovisionamiento solo puede escoger el camino que seguiría la ruta IGP normal. No está soportada la intervención manual en los cálculos de trayectoria, por ejemplo para especificar rutas explicitas e implícitas. Sin embargo, el soporte para la ingeniería de tráfico en ESM será desarrollado en futuras versiones del ESM, según asegura el proveedor Ciena.

Figura 47. **Formato del *script* de configuración de túneles**



Fuente: LOBO, Lancy. *MPLS Configuration Cisco IOS Software*. p. 131.

Abajo un ejemplo del *script* de aprovisionamiento de un túnel sin protección que empieza en isen-1 y termina en riv-3:

```
pbt tunnel-group create group U_ riv-3 tunnel-sync on

port set port 7/1 max-frame-size 2000

pbt encap-tunnel create static-encap U_ riv-3 tunnel-group U_ riv-3 pair-index 1 port 7/1 bvid 3224 dest-bridge-name riv-3 weight 6

pbt decap-tunnel create static-decap U_ riv-3 tunnel-group U_ riv-3 pair-index 1 port 7/1 bvid 3224 src-bridge-name isen-1

cfm service create static-encap U_ riv-3 name PBT-3224 next-mepid 1 level 2 ccm-interval 100ms

cfm service enable service PBT-3224
```

Un servicio CFM fue creado para este túnel como una opción escogida por un administrador.

Abajo un ejemplo de la configuración del *script* de aprovisionamiento de conexión producido para una conexión que empieza en riv-3 con C-VID 777 y S-VID 150 que va desde com-2 usando el *tunnel-group lond-warr-group*:

```
! create service CVID_00007308 on CN 5305 riv-3
```

```
rstp disable port 7/3

aggregation set port 7/3 agg-mode manual

lldp set port 7/3 mode rx-only notification off

virtual-switch create vs CVID_00007308

! add CVID 777 on Sub port 7/3 to CVID_00007308

sub-port create sub-port CVID_00007308 parent-port 7/3 classifier-precedence 777 ingress-l2-transform push-*.150.map egress-l2-transform pop

sub-port add sub-port CVID_00007308 class-element 1 vtag-stack 777

virtual-switch interface attach sub-port CVID_00007308 vs CVID_00007308

cpu-interface sub-interface create cpu-subinterface CVID_00007308 cpu-egress-l2-transform push-8100.777.7:push-8100.150.7

virtual-switch interface attach cpu-subinterface CVID_00007308 vs CVID_00007308

cfm service create vs CVID_00007308 name CVID_00007308 next 1 level 4

cfm service set service CVID_00007308 alarm-priority 1
```

```
cfm service set service CVID_00007308 alarm-time 10

cfm service set service CVID_00007308 reset-time 3000

cfm mep create service CVID_00007308 sub-port CVID_00007308 type up
mepid 1

cfm service enable service CVID_00007308

cfm service set service CVID_00007308 ccm-interval 1s

! add PBB-TE Service CVID_00007308 to CVID_00007308

pbt service create service CVID_00007308 ingress-isid 205278 egress-isid
205278 tunnel-group lond-warr-group

virtual-switch interface attach pbt-service CVID_00007308 vs
CVID_00007308
```

Las configuraciones usadas por los *scripts* de aprovisionamiento ESM fueron desplegadas exitosamente en los *switches* Core 5305 y usadas para transferir el tráfico entre las redes locales.

7. ANÁLISIS TÉCNICO Y FINANCIERO

En esta parte del trabajo de graduación se hace un análisis técnico para evaluar lo presentado en los capítulos anteriores, y un análisis financiero para evaluar la rentabilidad de la migración de una red Metro Ethernet a PBB-TE; para lograr esto último se utiliza el análisis del valor actual neto (VAN) y la tasa interna de retorno (TIR).

7.1. Análisis técnico

Originalmente, Ethernet fue definido como una tecnología de red de área local (LAN), para interconectar computadoras dentro de una pequeña organización o edificio. Con el paso de los años, Ethernet se ha vuelto una tecnología tan popular y tan fácil de implementar, que se ha vuelto la tecnología capa 2 por defecto a utilizar para el transporte de datos; pero tiene la desventaja de que si la red se vuelve demasiado grande (crecimiento al tamaño de un campus universitario o mayor), los dominios de colisión (*broadcast)* se vuelven excesivamente grandes.

Esto ha creado la necesidad de extender el Ethernet del dominio de las LAN al dominio de las redes Metro (redes metropolitanas). En la actualidad, la tecnología más usada en redes Metro es el MPLS (capa 3, IP), su variante EoMPLS y las nuevas tecnologías PBB buscan el modo de extender el dominio de Ethernet (capa 2), a una red metropolitana.

En una red IP tradicional, cada *router* hace una búsqueda en su tabla de enrutamiento, determina en donde está el próximo salto *("next-hope"),* y envía

el paquete a la interface conectada a ese próximo salto. Cada *router* en la ruta repite este mismo proceso (hace sus propias decisiones de enrutamiento independientes), hasta que el destino final es alcanzado. Estas continuas búsquedas en las tablas de enrutamiento (y actualización constante de las mismas), implica tiempos de latencia relativamente grandes y el consumo de grandes recursos de procesador en cada uno de los routers que actualizan sus tablas.

MPLS, en cambio, hace conmutación de etiquetas. El primer *router* en la ruta hace un enrutamiento tradicional, tal como en el caso anterior, pero en vez de encontrar un *router* de próximo salto, se encuentra el *router* de destino final, así como un camino predeterminado desde "acá" hacia ese *router* final. Este primer router encapsula el paquete IP, poniéndole una etiqueta que es usada por otros *routers* en la red MPLS para enrutar dicho paquete, sin necesidad de nuevas búsquedas en su base de datos, ahorrando tiempo (menor latencia) y recursos de procesador. Cuando el paquete llega al *router* final, la etiqueta es removida, y el paquete es enviado por medio de enrutamiento IP normal.

Ethernet over MPLS (EoMPLS para brevedad), es capaz de tomar directamente los cuadros ("*frames")* Ethernet (capa 2, no capa 3 como en el caso del MPLS tradicional), usa un mecanismo de tunelización para enviarlos a través de la red MPLS (la cual si es capa 3), encapsulando cada cuadro Ethernet como un único paquete, y los *routers* en los bordes de la red ponen y quitan las etiquetas, logrando así solucionar el problema de extender la red LAN al dominio de la red MAN o WAN.

Durante las pruebas se establecieron pseudo-wires EoMPLS, con lo que se encontró que la misma VLAN estaba en efecto disponible a ambos lados de la nube en capa 3, sin embargo, se encontró la importante limitación de que

EoMPLS no tiene características de QoS del tipo “ISP” (Internet Service Provider), más allá del QoS estándar basado en PFC, principalmente le falta la capacidad de aplicar políticas en una interface de salida.

Provider Backbone Bridges (PBB. también conocido como "mac-in-mac", o "QinQ", o "Q-tunneling"), es otro medio de extender el dominio de las redes Ethernet (LAN), extendiendo el número de VLANs posibles (solo 4096 en las VLANs Capa 2), la idea es ofrecer transportar las VLANs del cliente en la red de proveedor ("Provider Backbone"), pero ofreciendo separación de los dominios del cliente y del proveedor. Para lograr esto, se definió un nuevo encabezado Ethernet. PBB está definido en el estándar IEEE 802.1ah-2008, y es el fundamento de PBB-TE.

Provider Backbone Bridge Traffic Engineering (PBB-TE), definido en el estándar IEEE 802.1Qay-2009, logra adaptar Ethernet a redes de transporte tipo "Carrier", y difiere de PBB en que elimina la inundación *("flooding"),* e implementa tablas de envío dinámicas, además de protocolos de *Spanning-Tree* y de que es orientado a conexión.

Comparado con PBB, PBB-TE se comporta de modo más predecible, y su comportamiento puede ser más fácilmente controlado por los operadores de red, con el costo de tener que configurar las rutas estáticamente en cada equipo *("bridge")*, a lo largo de la ruta. Además de ofrecer tunelización para Ethernet, puede ser inter operado con MPLS, y ofrece independencia de servicios respecto del transporte (los servicios dentro del túnel pueden ser Ethernet, IP, MPLS, Pseudo-Wires, VPLS).

Se implementó una red usando 3 *switches* Ciena LE-311v, conectados en una topología triangular, se establecieron túneles PBT (Ciena usa el

acrónimo de Nortel PBT en vez de PBB, el cual es el equivalente de IEEE) y circuitos dentro de ellos. Con dichos circuitos, se logró separar los espacios de direcciones MAC del cliente y del proveedor (transporte encCapa 2), y se logró establecer políticas de tráfico por VLAN (QoS, un área donde se encontró debilidad en la tecnología EoMPLS).

Se construyó la red PBB-TE usando tres *switches* Ciena 5305, y se demostró que PBB-TE desplegado en un dominio puede inter operar muy bien con EoMPLS y con PBB desplegados en otros dominio (esta red sirvió para interconectar las redes EoMPLS y PBB), se encontró que esta tecnología está mejor adaptada para aplicaciones "*single domain*". El uso multidominio de túneles PBB-TE contiguos es posible pero no cumple con la especificación MEF del ENNI (External Network to Network Interface) y además necesita conocimiento mutuo de las direcciones MAC a los extremos del túnel, lo cual va más allá de la administración normal de las operaciones entre dominios.

Debido a estas características (la posibilidad de establecer políticas de tráfico y la interoperabilidad con otras tecnologías), la recomendación técnica del autor del presente trabajo de graduación es utilizar PBB-TE para el despliegue/migración de redes Metro Ethernet.

7.2. Análisis financiero

Una matriz financiera incluye los gastos de inversión y los ingresos por los servicios que genera el proyecto. Esta matriz permite encontrar los siguientes parámetros de decisión: el valor actual neto (VAN) y la tasa interna de retorno (TIR). Se ha tomado en cuenta el valor del dinero en el tiempo suponiendo una tasa de ganancia durante cinco años de 7 % no acumulativa que es el porcentaje típico de pago anual por bancos locales.

Para poder decidir si el proyecto es económicamente viable, el criterio de decisión será:

- Que el valor actual neto (VAN) calculado en la matriz financiera deberá ser mayor que cero.
- Que la tasa interna de retorno (TIR) calculada en la matriz financiera sea mayor que la tasa interna aceptable.
- Que la relación beneficio/costo sea mayor que cero.

Si estos criterios se cumplen el proyecto es rentable ya que las ganancias son mayores a cero.

Tabla IX. **Matriz financiera**

Costos	Descripción	Periodos 0	1	2	3	4	5
Construcción	Routers PBB-TE	4 2000					
	Tarjetas Routers PBB-TE	11000					
	Racks	700					
Instalación	Cableado estructurado	1 200					
	Comunicaciones	253 000	253 000	253 000	253 000	253 000	253 000
	Capacitación usuarios	1 100					
	Instalación de equipos	1 100					
	Pruebas	550					
	Migración de servicios	500					
	Gastos imprevistos	600					
Operación y mantenimiento	Mantenimientos preventivos		550	550	550	550	550
	Contrato de Soporte		550	550	550	550	550
	Licencias de Software		300	300	3 300	300	300
	Otras instalaciones		300	300	300	300	300
	Recurso Humano	1 500	1 500	1 500	1 500	1 500	1 500
Total inversión			256 200	256 200	259 200	256 200	256 200
Beneficios	Descripción	0	1	2	3	4	5
Beneficios Tangibles	Ahorro de Ancho de Banda		55 500	55 500	55 500	55500	55 500
	Fácil aprovisionamiento		550	550	550	550	550
	Fácil administración		550	550	550	550	550
	Ahorro en O&M		1 100	1 100	890	800	670
	Ahorro en equipo		5 500	4 400	3 900	3300	3 300
Beneficios Estratégicos	Nuevos Servicios		11 200	8 900	6 700	5500	5 500
	Incursión en nuevos mercados		6 600	4 400	2 200	1100	1 100
	Diversificación de productos		4 400	3 300	3 300	3300	3 300
	Atraer a nuevos clientes		5 500	4 400	3 300	2200	2 200

Continuación de la tabla VI.

Ampliar volumen de operación		11 200	10 000	8 900	8 900	6 700
Proyección de ventas		220 000	280 000	300 000	322 000	345 000
Beneficios totales	0	322 100	373 100	385 790	403 700	424 370
Flujo Neto efectivo	- 313 250	65 900	116 900	126 590	147 500	168 170

Fuente: elaboración propia.

7.2.1. Valor actual neto (VAN)

Tomando como referencia la matriz financiera se calcula el VAN.

Tabla X. **Cálculo del valor actual neto**

Flujo neto de Efectivo suponiendo un 7 % de interés anual	
Año 0	$ 313 250,00
Año 1	$ 65 900,00
Año 2	$ 116 900,00
Año 3	$ 126 590,00
Año 4	$ 147 500,00
Año 5	$ 168 170,00
VAN	$ 194 484,22

Fuente: elaboración propia.

Según este criterio el proyecto es aceptable y factible económicamente.

7.2.2. Tasa interna de retorno (TIR)

Tomando como referencia la matriz financiera se calcula la TIR.

Tabla XI. **Cálculo de la tasa interna de retorno**

Flujo neto de Efectivo suponiendo un 7% de interés anual	
Año 0	$ 313 250,00
Año 1	$ 65 900,00
Año 2	$ 116 900,00
Año 3	$ 126 590,00
Año 4	$ 147 500,00
Año 5	$ 168 170,00
VAN	0,25

Fuente: elaboración propia.

Según este criterio, la tasa interna de retorno es de 25 % mayor que la tasa mínima aceptable (7 %) que se tomó para este proyecto, por lo tanto el proyecto es aceptable y factible económicamente.

7.2.3. Punto de equilibrio

Tomando como referencia la matriz financiera se calcula el punto de equilibrio.

Tabla XII. **Cálculo del punto de equilibrio**

Flujo neto de Efectivo suponiendo un 7% de interés anual	
Año 0	$ 313 250,00
Año 1	$ 65 900,00
Año 2	$ 116 900,00
Año 3	$ 126 590,00
Año 4	$ 147 500,00
Año 5	$ 168 170,00
PE	2,47
	2 años, 6 meses

Fuente: elaboración propia.

Según el cálculo anterior la inversión se recuperará en 2,47 años o en 2 años y 5 meses aproximadamente.

7.2.4. Análisis costo - beneficio

Tomando como referencia la matriz financiera se calcula la relación beneficio/costo:

Tabla XIII. **Cálculo relación beneficio/costo**

Periodo	Inversión suponiendo 7% de interés anual	Ingresos suponiendo 7% de interés anual
Año 0	313 250	0
Año 1	256 200	322 100
Año 2	256 200	373 100
Año 3	259 200	385 790
Año 4	256 200	403 700
Año 5	256 200	424 370
VAN	13 664 410,59	1560 894,88
beneficio/costo		1,14

Fuente: elaboración propia.

Según este criterio la relación beneficio/costo es mayor a cero, o sea que los beneficios del proyecto son mayores que los costos y es económicamente viable.

Se puede ver en los cálculos anteriores que se cumplen los criterios de decisión que se citaron al principio del estudio financiero:

- El valor actual neto $ 194 484,22 es mayor a cero.

- La tasa interna de retorno de 25 % es mayor a la tasa interna aceptable 7 %.
- La relación beneficio/costo 1,14 es mayor a cero.

Con base en lo anterior se puede concluir que el proyecto es económicamente viable y que deja ganancia considerable y la recuperación de la inversión según las ganancias anuales se calcula en 2,47 años o 3 años y 5 meses.

CONCLUSIONES

1. Ethernet es una tecnología que nació para ser usada en redes LAN, si esta red LAN se hace demasiado grande, se encuentra el problema de que el dominio de colisión se vuelve demasiado grande, degradándose el performance de la red, y haciendo difícil su administración.

2. MPLS agrega etiquetas a los paquetes IP (capa 3), de modo que la conmutación de los mismos es más rápida que usando enrutamiento IP tradicional. EoMPLS también usa un sistema de etiquetado, pero lo hace directamente sobre los cuadros Ethernet, logrando así extender el dominio de la red LAN.

3. Las tecnologías Provider Backbone Bridge logran extender el dominio de las LAN, mediante la definición de un nuevo encabezado Ethernet, adaptándolo a las redes tipo Carrier. Además, son interoperables con MPLS y capaces de transportar múltiples servicios.

4. EoMPLS, si bien puede transportar los cuadros Ethernet de un punto a otro en la red Carrier mediante etiquetas, no cuenta con características QoS tipo "ISP", más allá del QoS estándar basado en PFC, la mayor limitación de esto es la falta de soporte para aplicar políticas en una interface de salida.

5. Los equipos PBB se desempeñaron satisfactoriamente en el establecimiento manual de túneles con ingeniería de tráfico (TE), se logró separar los espacios de direcciones MAC del cliente y del

proveedor (transporte en capa 2), y se logró establecer políticas de tráfico por VLAN (QoS, un área donde se encontró debilidad en la tecnología EoMPLS).

6. PBB-TE es una tecnología es capaz de proveer interoperabilidad entre EoMPLS y PBB, por lo cual es adecuada para aplicaciones “single domain”. El uso multidominio es posible pero necesita conocimiento mutuo de las direcciones MAC a ambos extremos del túnel, lo cual va más allá de la administración normal de las operaciones entre dominios.

7. Las tecnologías PBB-TE han demostrado superar a la tecnología EoMPLS en la implementación de políticas QoS, la cual es un área crítica para los proveedores, además de que es económicamente rentable la migración/despliegue de dicha tecnología.

RECOMENDACIONES

1. Es importante saber que el uso de Ethernet debe ser limitado a redes locales (LAN), dadas sus limitaciones de crecimiento.

2. EoMPLS puede implementarse para ampliar el dominio de las redes LAN, si el proveedor ya cuenta con una infraestructura MPLS que soporte dicha tecnología.

3. Debe considerarse que EoMPLS no es la única tecnología que puede extender una LAN a nivel Carrier, las tecnologías PBB también son capaces de lograr esto, además de ser interoperables con MPLS y capaces de transportar múltiples servicios.

4. Considerar que EoMPLS no cuenta con características de QoS sofisticadas, lo cual es una limitación para ciertas aplicaciones tipo Carrier.

5. Tomar en cuenta que el despliegue de PBB tiene ventaja sobre EoMPLS en aplicaciones que requieran políticas de tráfico y/o QoS.

6. PBB-SE TE despempeña mejor en el transporte de aplicaciones "*single domain"* y para interoperar tecnologías EoMPLS y PBB.

7. Considerar que las tecnologías PBB-TE superan a EoMPLS en la implementación de políticas de tráfico, y que su despliegue es económicamente rentable.

BIBLIOGRAFÍA

1. Andersson, L. *Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field.* [en línea]. <http: // tools.ietf.org/html/rfc5462>. [Consulta: 10 de noviembre de 2014].

2. Cisco Systems, Inc. *Configuring PFC3BXL or PFC3B Mode MPLS QoS-Catalyst 6500 Release 12.2SXH and Later Software Configuration Guide. Understanding MPLS QoS Section.* [en línea]. <http: // www. cisco.com/en /US/docs/switches /lan/ catalys t6500/ios/12.2SX/ configuration/guide/mplsqos.html>. [Consulta: 10 de noviembre de 2014].

3. _____. *MPLS VPN Inter-AS IPv4 BGP Label Distribution.* [en línea]. <http://www.cisco. com/en/US/ docs/ios/12_2s / feature/guide/fsiaslbl.html>. [Consulta: 10 de noviembre de 2014].

4. LOBO, Lancy; LAKSHMAN, *Umesh. MPLS Configuration Cisco IOS Software - A complete configuration manual for MPLS, MPLS VPNs, MPLS TE, QoS, any transport over MPLS (AToM) and VPLS.* Cisco Press, 2009. 210 p.

5. *MEF 26 External Network Network Interface (ENNI)–Phase 1.* [en línea]. <http:// metroetherne tforum. org/PDF_Documents /technical-specifications/MEF26.pdf>. [Consulta: 10 de noviembre de 2014].