Redes Ethernet ópticas para operadores

Luis Velasco Esteban, Jordi Perelló Muntan, Gabriel Junyent Giralt
GRUPO DE COMUNICACIONES ÓPTICAS - UNIVERSITAT POLITÈCNICA DE CATALUNYA (UPC)
Enrique Urrea Mizzi, Pedro J. Lizcano Martín
TELEFÓNICA INVESTIGACIÓN Y DESARROLLO

Ethernet es la tecnología predominante en las redes de área local (LAN) y se está convirtiendo también en una tecnología de referencia en las redes de acceso, concretamente en las redes de área metropolitana (MAN) y de área extensa (WAN). Su objetivo es proporcionar conectividad entre localizaciones de cliente dispersas en la geografía, como si estuviesen conectadas a una misma LAN.

Si a esto se le une el rápido incremento de la demanda de ancho de banda para el transporte de datos y la disponibilidad de interfaces Ethernet ópticas cada vez más veloces y a precios cada vez más bajos, podemos pensar que es posible incorporar la tecnología Ethernet a las redes de los operadores de telecomunicaciones.

Por otra parte, los límites entre las redes de conmutación de paquetes y las redes de conmutación de circuitos están desapareciendo, y es posible proporcionar servicios similares utilizando ambos tipos de redes. Tal es el caso, por ejemplo, de la nueva generación de SDH (con LCAS, GFP y concatenación virtual) que proporciona servicios de circuitos y de datos, de forma flexible y fiable.

Desde el punto de vista económico, parece claro que los costes de implantación (CAPEX) y de operación (OPEX) de la tecnología Ethernet son menores que los de las redes basadas en SDH. Sin embargo, para que la tecnología Ethernet sea utilizada en las redes de los operadores, es necesario dotarla de un conjunto de características imprescindibles que permitan ofrecer servicios de calidad.

Este artículo revisa los mecanismos que permitirán el despliegue de Ethernet en las redes metropolitanas de los operadores de telecomunicaciones. Habitualmente esto se conoce como "Carrier-class optical Ethernet".

INTRODUCCIÓN

Una red Ethernet metropolitana (MEN) es una red que conecta LANs geográficamente separadas de forma directa o a través de una red WAN, utilizando Ethernet como protocolo principal.

Como se puede ver en la **Figura 1**, los nodos de una red MEN pueden ser *switches* o *routers*, dependiendo de su localización en la red, y del servicio que proporcionan y la protección deseada. Los enlaces son punto a punto a cualquier velocidad de Ethernet (desde 10 Mbit/s hasta 10 Gbit/s).

Las redes MEN son mallas del grado necesario para proporcionar la conectividad, los servicios y el nivel de protección deseados, y se interconectan con otras redes MEN mediante enlaces WAN.

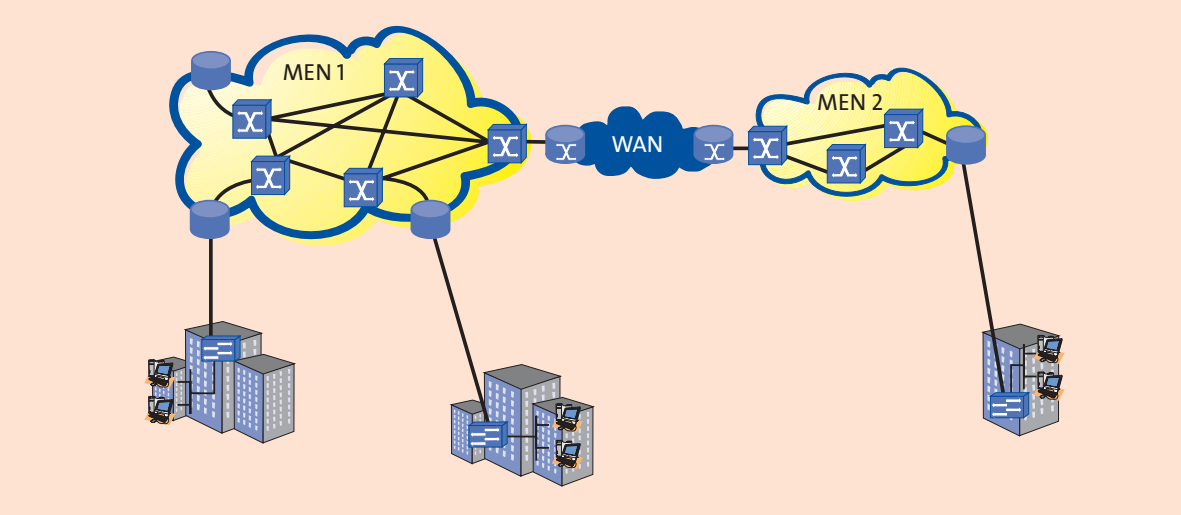

Figura 1. Red Ethernet metropolitana

Los servicios Ethernet [1] [5] pueden clasificarse en punto a punto (E-Line) o multipunto a multipunto (E-LAN), ver la **Figura 2**. En este sentido:

- *El servicio de línea Ethernet (E-Line)* proporciona una conexión virtual Ethernet (EVC) punto a punto. Es análogo a utilizar PVCs Frame Relay, o líneas alquiladas TDM.

- *El servicio de LAN Ethernet (E-LAN)* proporciona conectividad multipunto. La información enviada puede ser recibida por varios puntos. Cada extremo está conectado a un EVC multipunto, y cuando se añade una nueva localización solamente es necesario añadir el nuevo sitio al EVC multipunto.

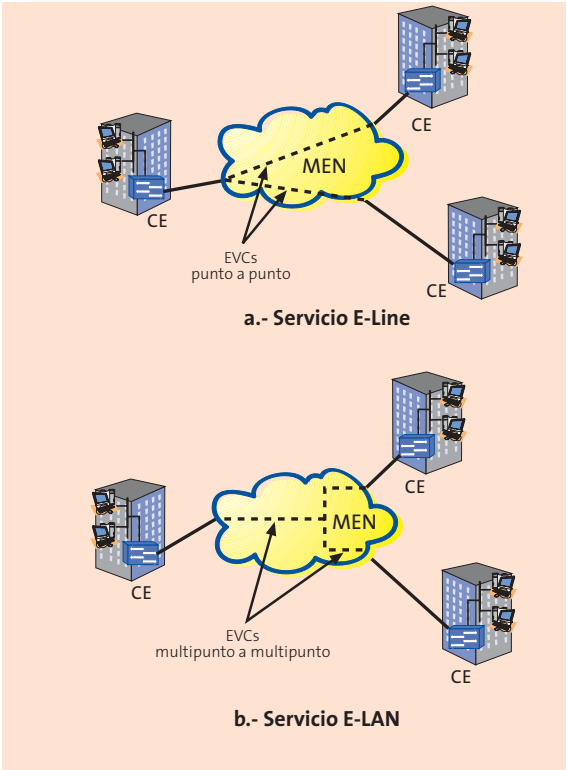

Figura 2. Servicios Ethernet

El despliegue de Gigabit Ethernet (GbE) se basa en razones tales como:

- *Su coste*. El coste de los equipos GbE es significativamente menor que el de Frame Relay o ATM, por su relativa simplicidad técnica y las economías de escala. Además, el coste operacional es significativamente inferior al de TDM (PDH y SDH) y también es menor el coste de implantación [6].

- *Su provisión rápida y bajo demanda*. Los servicios Ethernet ofrecen un amplio rango de velocidades (de 1 Mbit/s a 1 Gbit/s) en incrementos de 1 Mbit/s, y pueden ser provistos de forma rápida y bajo demanda.

- *Su tecnología basada en paquetes*. Ethernet es una tecnología asíncrona basada en tramas que proporciona ventajas, por su flexibilidad sobre sus más rígidos competidores SDH y ATM.

- *Su facilidad de interfuncionamiento*. Se elimina una capa de complejidad (SDH y ATM) del acceso, haciendo más simple la integración de los sistemas de cliente y los de la red, y logrando un transporte más eficiente.

- *Su adopción omnipresente*. Ethernet es la tecnología dominante en las LANs, existiendo interfaces estándar para 10, 100, 1.000 y 10.000 Mbit/s. Respecto a ATM y SDH tiene la ventaja de su facilidad de aprendizaje, entre otras.

Se pueden identificar un conjunto de limitaciones cuando se quiere utilizar Ethernet puro como medio de transporte, respecto de ATM o SDH. La adopción de Ethernet como capa de transporte universal en el área metropolitana dependerá de la resolución de esas limitaciones.

Las limitaciones son las relativas a:

- *La escalabilidad y utilización de los recursos de la red.* Debido a que el campo del identificador de VLAN es de 12 bit, el máximo número de VLANs en un dominio está limitado a 4.096.

- *Los mecanismos de protección.* La pérdida de un enlace se maneja vía STP, que tarda varios segundos en actuar en comparación con los 50 ms de SDH. Este tiempo es crítico en aplicaciones de voz y vídeo. Además presenta una escasa capacidad de aislamiento por fallo, y, al contrario que SDH, no dispone de alarmas como LOS, RDI, etc.

- *El transporte de tráfico TDM.* Si se desea construir una red multiservicio es necesario transportar circuitos TDM, como E1, E3 o STM-1.

- *Las garantías de QoS extremo a extremo.* Para ofrecer un determinado grado de calidad de servicio (*Quality of Service*, QoS)[1] Ethernet necesita de los mecanismos relativos a:

  - La planificación del diseño de recursos, para asegurar que el servicio puede ser garantizado para un determinado volumen de tráfico máximo cursado mediante el dimensionado adecuado de recursos (ancho de banda).

  - El control de admisión de conexión para nuevas peticiones de servicio, en el caso de alcanzar un determinado volumen de tráfico cursado, evitando así la congestión.

  - El establecimiento de un camino óptimo a través de la red. Actualmente se utiliza el protocolo de *spanning tree* (STP).

  - La priorización de los paquetes.

- *La operación, administración y mantenimiento en servicio.* Ethernet no tiene capacidad de monitorizar la tasa de error, tal y como hace SDH con los bytes BIP-8 de la cabecera, ni otros eventos necesarios para realizar el mantenimiento y administración de la red extremo a extremo.

En los siguientes apartados del artículo se revisan los mecanismos que permitirán eliminar las anteriores limitaciones para el despliegue de Ethernet como capa de transporte universal en el área metropolitana.

LOS MECANISMOS DE ENCAPSULACIÓN

Con objeto de soportar tecnologías que permitan ofrecer servicios escalables basados en Ethernet, como es el caso de los servicios de LAN transparente (TLS) para conectar varias localizaciones de cliente mediante una red MEN, es necesario disponer de algún mecanismo de encapsulación, que asegure la independencia de la solución de acceso de la utilizada en la red troncal.

Los aspectos más importantes para el despliegue de Ethernet en las redes metropolitanas son la escalabilidad y separación de los clientes (o para ser más concretos, la segmentación de servicios), y la acotación de las dimensiones de la tabla de direcciones MAC. Con la segmentación de los distintos tipos o clases de servicios se puede intentar asegurar para cada uno el grado de QoS adecuado, utilizando un dimensionado apropiado de los recursos asignados a ese servicio, o utilizando los mecanismos de prioridad correspondientes.

En este sentido, se deben tener en cuenta ciertas limitaciones relacionadas con:

- *La tabla de direcciones MAC*

  Los *switches* Ethernet asimilan las direcciones MAC de las máquinas remotas y las asocian con los puertos desde los que les llegan las tramas Ethernet.

  Si se utilizasen *switches* Ethernet en el núcleo de la red metropolitana, cada *switch* debería asimilar las direcciones MAC de cada máquina remota conectada a cada VLAN de cliente de la red metropolitana. Esto se conoce como *explosión de la tabla de direcciones MAC*, lo que plantea una complejidad innecesaria.

[1] Siendo rigurosos, el protocolo Ethernet (basado en el estándar 802.3, que utiliza el algoritmo CSMA/CD, *Carrier Sense Multiple Access with Collision Detection*) posee, de forma intrínseca, un tiempo de acceso al medio que no es determinista, sino aleatorio, y que depende del número de colisiones (que a su vez depende del tráfico cursado y del número de usuarios que compiten por el acceso al medio). Con un dimensionado adecuado (limitar el número de usuarios, mediante el control de admisión, y el tamaño de los paquetes cursados por usuario) puede estimarse una cota superior del tiempo de acceso y del tráfico a cursar, lo que permite "garantizar", dentro de esos límites, un determinado nivel de QoS.

■ *El identificador de VLAN.*

Una VLAN es una LAN lógica sobre una red Ethernet física compartida, tal y como se establece en el estándar IEEE 802.1Q.

En este estándar se define una etiqueta Q, el identificador de VLAN (VID), que se inserta en las tramas Ethernet. El VID tiene 12 bits, por lo que el máximo número de VLANs diferentes en un dominio es de 4.096. Puesto que la red es utilizada por diferentes clientes, se debe gestionar el identificador de las VLAN de cada cliente, de forma que no existan VID duplicados.

A continuación se describen los tres mecanismos de encapsulación que han sido propuestos hasta la fecha, con indicación de sus efectos. Los mecanismos de encapsulación insertan campos o etiquetas adicionales en las tramas Ethernet de cliente en los nodos de borde. Para seleccionar uno de los mecanismos, se debe considerar la compatibilidad hacia atrás, las prestaciones y su complejidad.

El mecanismo de encapsulación "Q-in-Q"

Este mecanismo de apilamiento de etiquetas de VLAN (*VLAN Stacking*) consiste en insertar una etiqueta *Q* adicional en las tramas de cliente que llegan al *switch* de borde de la red MEN (ver la **Figura 3**). Combinando las etiquetas VID de cliente y de la red Ethernet metropolitana, se aumenta el número de VLANs más allá del límite de las 4.096.

Este esquema es compatible hacia atrás y ha sido introducido en la especificación IEEE 802.1ad.

El mecanismo de encapsulación con etiqueta VMAN

Mediante el mecanismo de *VLAN Stacking* se introduce una nueva etiqueta de 24 bits, denominada VMAN (o etiqueta de MAN virtual), aumentando el número de VLANs de cliente sobre la red MAN (ver la **Figura 3**). De esta forma no se tiene que restringir el VID que utilizan los clientes y se aumenta el número de VLAN que se transportan sobre la red de área metropolitana.

Aunque los mecanismos de *forwarding*, pila de protocolos, etc., son básicamente los mismos de la arquitectura IEEE 802.1Q, este esquema no es compatible con los *switches* existentes.

El mecanismo de encapsulación MPLS de capa 2

La encapsulación MPLS de capa 2 (conocida como encapsulación Martini [7]) facilita el transporte de las tramas Ethernet a través de dominios MPLS (ver la **Figura 4**).

El nodo de ingreso (LER, *Label Edge Router*) inserta dos etiquetas MPLS en las tramas Ethernet de cliente, basándose en la información de destino (dirección MAC, puerto y etiqueta *Q*). Estas dos etiquetas son:

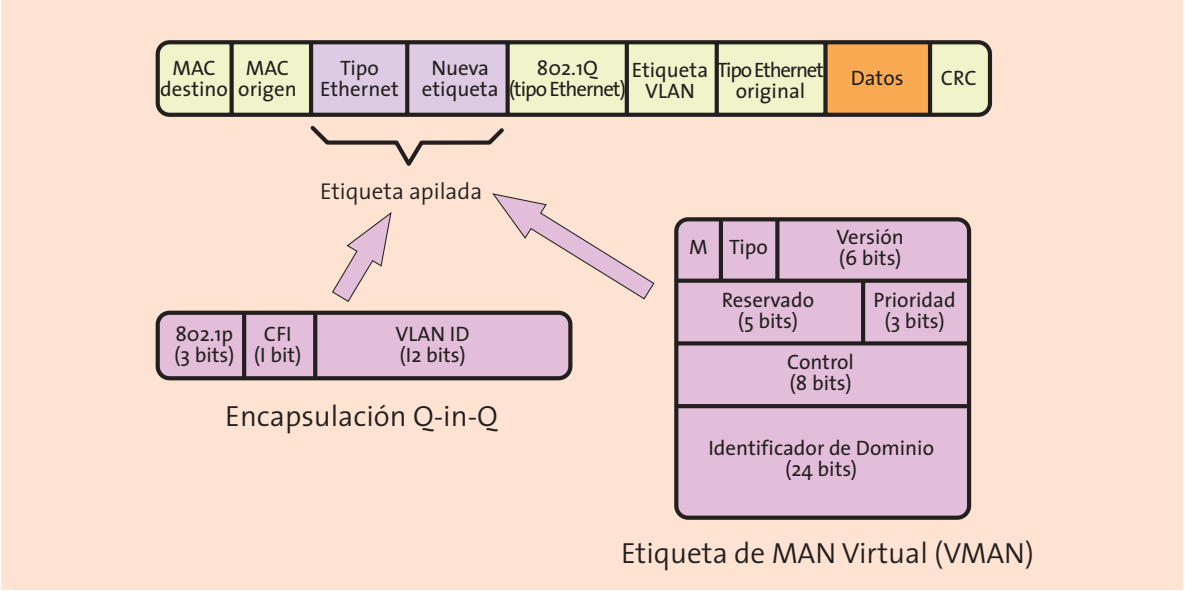

Figura 3. Encapsulación "Q-in-Q"

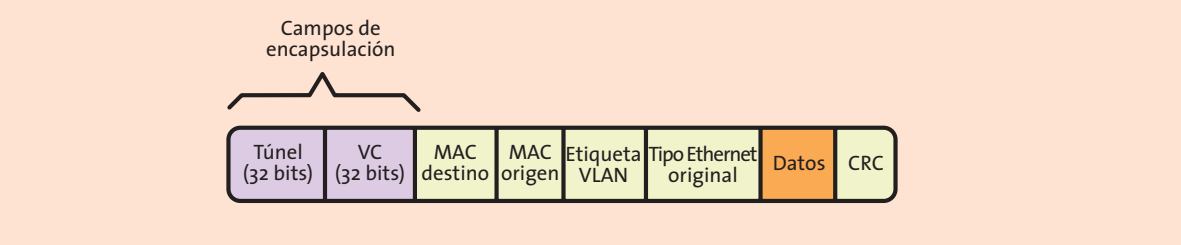

Figura 4. Encapsulación Martini

1. *La etiqueta de túnel*, que se utiliza para transportar la trama a través del dominio MPLS. Esta etiqueta es eliminada por el penúltimo nodo LSR (*Label Switch Router*).

2. *La etiqueta de circuito virtual* (VC). Es utilizada por el LER de salida para determinar cómo procesar la trama y cómo enviarla hacia su destino.

Los LER deben realizar dos funciones: la función de puente Ethernet, para cursar las direcciones MAC de cliente, y la función de envío MPLS, basado en el camino LSP (*Label Switched Path*). Cada LER debe *mapear* las direcciones MAC y/o VID a cursar, en un camino LSP preestablecido que transporta las tramas Ethernet a través del dominio MPLS.

La utilización de MPLS como mecanismo de encapsulación proporciona ventajas adicionales al problema de escalabilidad. Tal es el caso, por ejemplo, de la encapsulación MPLS, donde las tramas Ethernet pueden ser transportadas sobre cualquier tipo de red. Además, se introducen automáticamente todas las características de OAM, así como los mecanismos de protección, la ingeniería de tráfico y las garantías de ancho de banda de MPLS.

Comparación de las técnicas

Puesto que las direcciones MAC solamente deben ser asimiladas en los LER del dominio, utilizando MPLS se evita la explosión de la tabla de direcciones MAC.

Desde la perspectiva de la carga que se introduce, se tiene que:

- *Q-in-Q* introduce 4 bytes de *overhead*.
- VMAN introduce un mínimo de 6 bytes.
- MPLS introduce un mínimo de 8 (2 x 4) bytes, y hasta un máximo de 30 bytes.

Para tramas pequeñas, de unos 64 bytes, se introduce un *overhead* de hasta el 46 por ciento.

La encapsulación *Q-in-Q* proporciona escalabilidad sin añadir una significativa complejidad, sin embargo MPLS proporciona un conjunto de características, como ingeniería de tráfico y fiabilidad, deseables por los operadores de telecomunicaciones. Puesto que ambas tecnologías son complementarias, pueden ser utilizadas conjuntamente: *Q-in-Q* en la red de acceso, y LER y MPLS en el núcleo de la red.

LAS FUNCIONES DE OPERACIÓN, ADMINISTRACIÓN Y MANTENIMIENTO

Con la introducción de un tráfico sensible al tiempo real, como es el generado por los servicios de voz y vídeo, se hace necesario controlar la conmutación y el enrutamiento, con objeto de optimizar y limitar ciertos parámetros de QoS relativos a estos servicios, como son la tasa de pérdidas, el tiempo de retardo extremo a extremo, etc. En los últimos tiempos, dentro de la ITU y la IETF se está realizando un esfuerzo importante para reflejar los requisitos de los operadores de telecomunicaciones en las funciones de Operación, Administración y Mantenimiento (OAM) de MPLS [8] [11] [12], lo que ha dado lugar a la aparición de varios estándares con funciones nuevas y mejoradas de OAM.

Los mecanismos impulsados por la ITU y la IETF son los relativos:

- Verificación de la conectividad (*Connectivity Verification*, CV) y detección rápida de fallos (*Fast Failure Detection*, FFD).
- Indicación de defecto hacia adelante (*Forward Defect Indication*, FDI) e indicación de defecto hacia atrás (*Backward Defect Indication*, BDI).

- *MPLS LSP Ping.*
- Detección de fallos bidireccional (*Bidirectional Forwarding Detection,* BFD).
- *LSR Self Test.*

En los apartados siguientes se presentan estos mecanismos.

Verificación de la conectividad y detección rápida de fallos

Los mecanismos de verificación de la conectividad (*Connectivity Verification*, CV) y de detección rápida de fallos (*Fast Failure Detection*, FFD) propuestos por la ITU [9] permiten detectar y diagnosticar defectos de conectividad de un camino LSP extremo a extremo.

El flujo de paquetes CV, con una periodicidad de un paquete por segundo, tiene origen en el nodo LSR de ingreso del camino LSP y va dirigido hacia el LSR de salida de dicho camino. Como se puede observar en la **Figura 5**, su finalidad es el diagnóstico de posibles errores en recepción: pérdida de paquetes, recepción de paquetes con otro destino, etc.

El mecanismo FFD presenta un funcionamiento idéntico a CV, excepto en que permite la variación de la frecuencia de emisión de los paquetes, posibilitando así la detección rápida de fallos. El valor recomendado es de 20 paquetes por segundo (un paquete cada 50 ms).

Indicación de defecto hacia delante y hacia atrás

Los mecanismos de indicación de defecto hacia delante (*Forward Defect Indication*, FDI) e indicación de defecto hacia atrás (*Backward Defect Indication*, BDI) están propuestos por la ITU [9].

El objetivo de FDI es suprimir las alarmas producidas en los caminos LSP clientes de un LSP afectado por un defecto. Los paquetes FDI tienen una periodicidad de un paquete por segundo y se envían hacia delante desde el primer nodo que detecta el defecto: si el error se ha producido en la capa servidora, será el primer nodo siguiente a la avería; si el error se ha producido en la capa MPLS, será el punto de terminación del LSP del nivel en el cual se ha producido el fallo.

El mecanismo BDI informa al extremo origen de un LSP, con una periodicidad de un paquete por segundo, de cualquier defecto que se observe en el destino. BDI exige un camino de retorno, que puede ser un LSP dedicado, un LSP compartido por varios caminos LSP en sentido hacia delante, o un trayecto de retorno no MPLS.

La **Figura 6** esquematiza el funcionamiento de los mecanismos FDI y BDI.

Tanto FDI como BDI pueden ser útiles para medir la disponibilidad de la red o como evento de conmutación en mecanismos de protección.

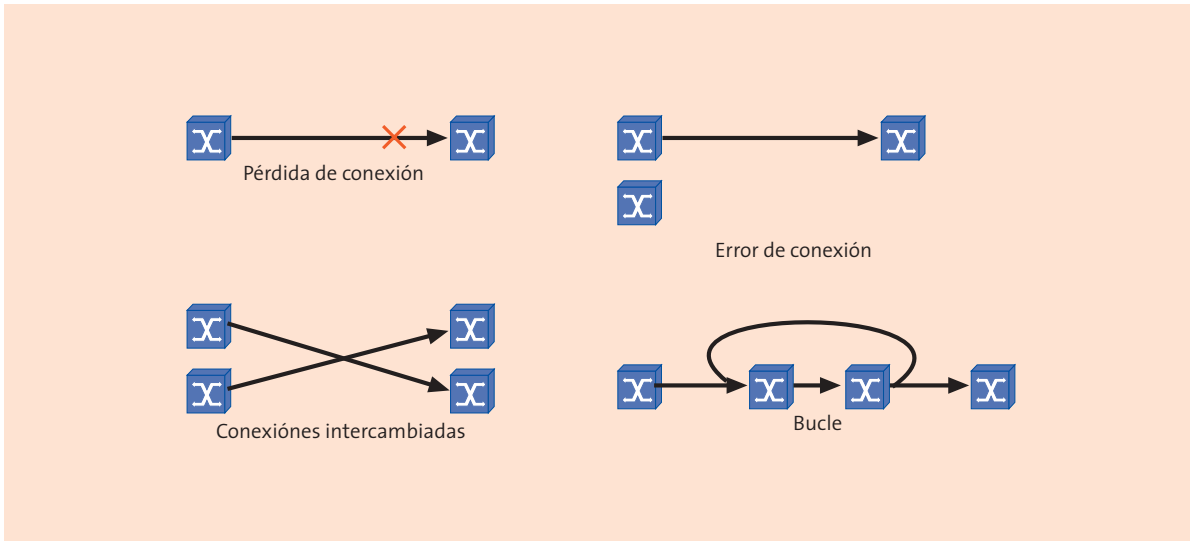

Figura 5. Tipos de defecto de un camino LSP

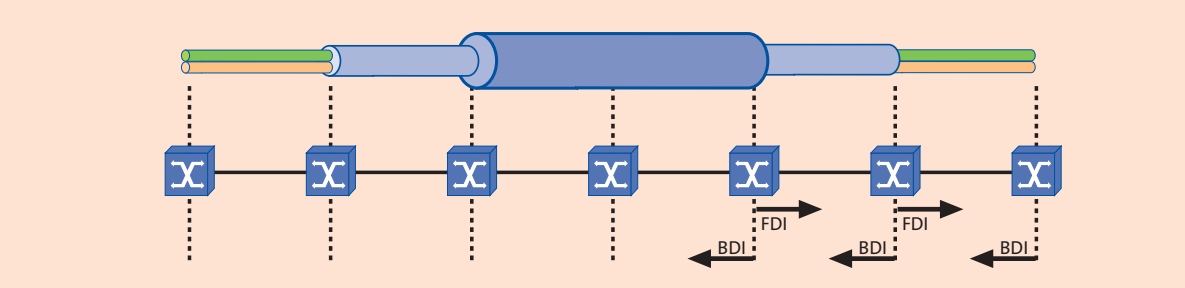

Figura 6. Mecanismos FDI y BDI

El mecanismo MPLS LSP Ping

El mecanismo MPLS LSP Ping, propuesto por la IETF [13], tiene la finalidad de verificar que los paquetes correspondientes a una determinada clase de servicio equivalente (*Forwarding Equivalent Class*, FEC) acaban su camino MPLS en el nodo de salida adecuado para aquella clase. Los paquetes "*MPLS LSP Ping echo request*" son enviados por el nodo de ingreso hacia el nodo de salida, siguiendo el mismo camino que los paquetes correspondientes a la clase de servicio que se desea probar. Este mecanismo presenta dos modos de funcionamiento:

1. En el modo *basic connectivity check,* el paquete *echo request* llega al nodo de salida y allí es enviado al plano de control, que verificará si el LSR es realmente un nodo de salida para aquella clase de servicio. Una vez realizada la verificación, el LSR de salida enviará un "*MPLS LSP Ping echo reply*" reflejando el resultado de dicha verificación.

2. En el modo *traceroute,* el paquete será enviado al plano de control de cada LSR de tránsito, que a su vez verificará que realmente es un LSR de tránsito para aquella clase de servicio.

Detección de fallos bidireccional

Tal como se ha descrito anteriormente, MPLS LSP Ping es un mecanismo capaz de detectar fallos en el plano de datos y de realizar, a su vez, el análisis de este plano frente al plano de control. En cambio, el mecanismo de detección de fallos bidireccional (*Bidirectional Forwarding Detection*, BFD), también propuesto por la IETF [14] [15], está diseñado sólo para detectar fallos del plano de datos a cambio de un coste computacional menor al de MPLS LSP Ping, permitiendo una detección rápida de fallos (menos de un segundo frente a los varios segundos de MPLS LSP Ping) y un soporte para la detección de fallos a un número mayor de caminos LSP. Además, gracias a su formato fijo de paquete, su implementación hardware es más fácil.

El mecanismo LSR Self Test

El mecanismo LSR Self Test, propuesto por la IETF [16], define un procedimiento para que un LSR pueda realizar una prueba de sus asociaciones de etiquetas, así como de la conectividad entre éste y los LSRs a los que está directamente conectado. LSR Self Test puede ser usado tanto en túneles *unicast* LDP como en túneles basados en RSVP.

LOS MECANISMOS DE PROTECCIÓN

Las redes de transporte basadas en SDH proporcionan mecanismos de protección de tráfico con tiempos de restauración inferiores a 50 ms. Esta característica permite que las pérdidas de conectividad en los enlaces, que sean debidas por ejemplo a la rotura de una fibra óptica o a fallos en una tarjeta, no tengan impacto sobre el servicio que se proporciona a los clientes.

Por el contrario, las soluciones tradicionales de Ethernet puro proporcionan protección mediante el mecanismo estándar basado en el protocolo STP (*Spanning Tree Protocol*), que fue diseñado originalmente para recuperar fallos en 30 segundos.

En la referencia [2] se describen los requisitos y objetivos de los mecanismos de protección propuestos para las redes Ethernet metropolitanas.

Protección mediante STP

Alcanzar una alta disponibilidad es difícil utilizando el *bridging* tradicional mediante el protocolo STP (*Spanning Tree Protocol*), definido en la especificación IEEE 802.1d.

Este protocolo previene la aparición de bucles y proporciona un mecanismo de recuperación en caso de fallo en un enlace o puerto (ver la **Figura 7**). Sin embargo, el tiempo lento de convergencia de STP lo hace inadecuado para soportar servicios de calidad. En este sentido, dependiendo de la topología de la red, puede tardar entre 30 segundos y varios minutos en actuar frente a un fallo.

Aunque existen versiones rápidas de STP, este protocolo es incapaz de proporcionar protección por debajo de los 50 ms, el umbral utilizado por los operadores. Sin embargo, como se puede observar en la **Figura 7**, sí puede ser soportado en el acceso.

Protección mediante enlaces redundantes

Para proporcionar tiempos de protección por debajo de los 50 ms, se han definido dos modos de protección (ver la **Figura 8**):

1. *El modo enlace agregado y protección de nodo (ALNP).* Utiliza un camino LSP de desvío para evitar el recurso con fallo.

2. *El modo protección de camino extremo a extremo.* Utiliza un camino de protección extremo a extremo.

La detección de pérdida de señal (*Loss of Signal*, LOS), pérdida de enlace (*Loss of Link*, LOL), pérdida de trama (*Loss of Frame*, LOF) y pérdida de sincronismo (*Loss of Sync*) en el enlace Ethernet, puede utilizarse para lanzar eventos de protección.

Además, Ethernet utiliza el código de línea 8B/10B para recuperación de reloj y balanceo de potencia. Este código también se utiliza para detectar la degradación del enlace físico, midiendo la tasa de error (BER). En este sentido, pueden establecerse umbrales de BER que al ser superados generen eventos de protección.

Cuando se detecta un fallo se protegen, con una única invocación, todos los enlaces y nodos agregados.

Enlace agregado y protección de nodo (ALNP)

ALNP proporciona protección local de múltiples enlaces o nodos a través de la red, utilizando caminos

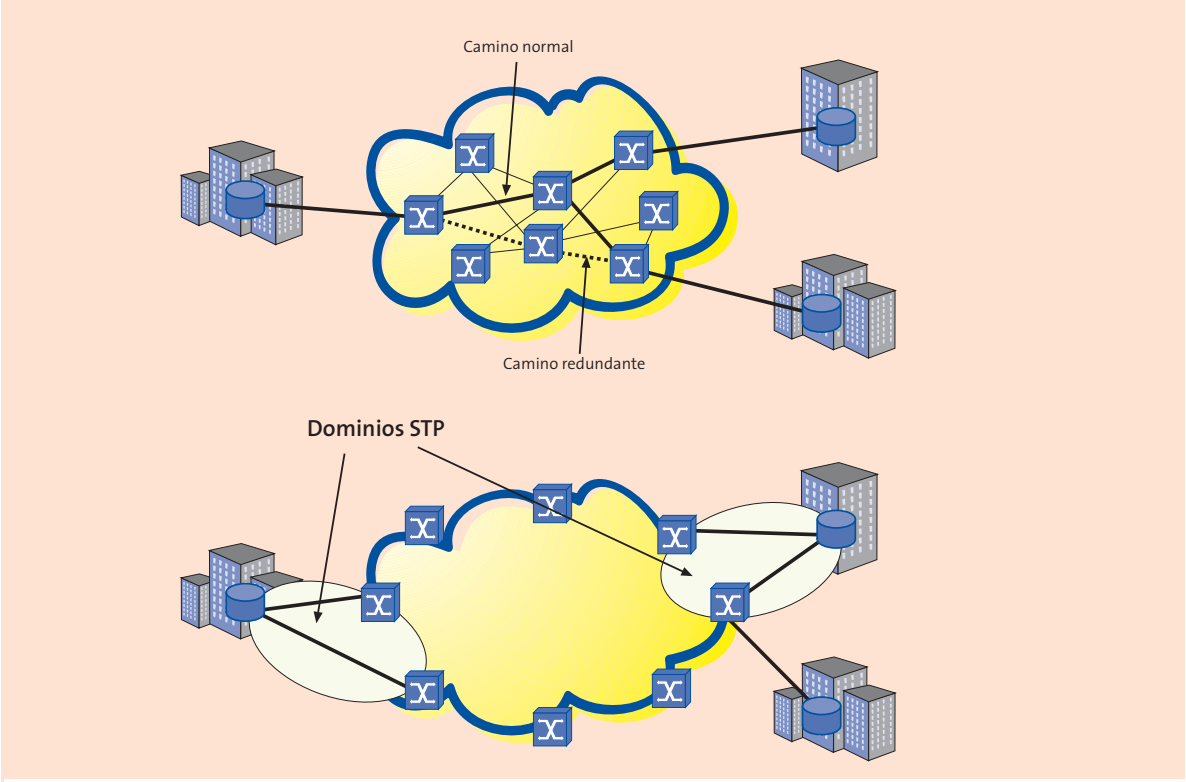

Figura 7. Protocolo STP

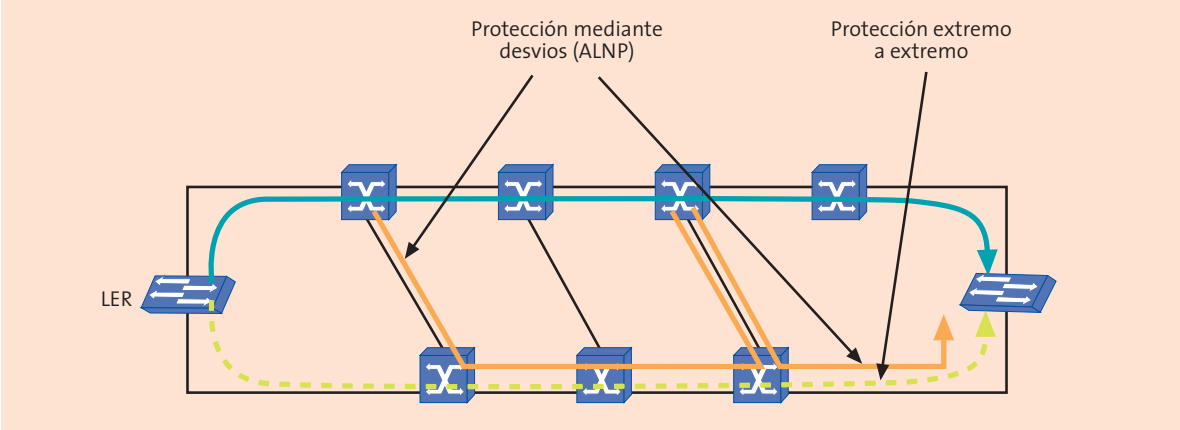

Figura 8. Protección mediante enlaces redundantes

LSP de desvío, que son creados utilizando recursos disjuntos de los que utiliza el camino principal. En este sentido, cuando se detecta un fallo el mecanismo de protección actúa de la siguiente forma (ver la **Figura 9**):

1. El último elemento en el camino antes del recurso con fallo pone una etiqueta adicional para reencaminar el tráfico del LSP primario al LSP de desvío.

2. Una vez que se ha evitado el recurso con fallo, se alcanza el siguiente elemento en el camino principal posterior al recurso con fallo.

3. El siguiente elemento elimina la etiqueta adicional y envía el tráfico por el camino principal.

El ancho de banda reservado para los LSP de desvío se puede utilizar para tráfico extra en arquitecturas de protección dedicada (1:1) o compartida (1:n), cuando no se utilizan para protección.

Protección de camino extremo a extremo

La protección de camino extremo a extremo crea dos o más caminos extremo a extremo redundantes entre el nodo de entrada y el de salida [10]. Estos nodos de entrada y de salida se envían entre ellos mensajes de verificación de conectividad (CV) o de detección rápida de fallos (FFD) para detectar posibles defectos de conectividad.

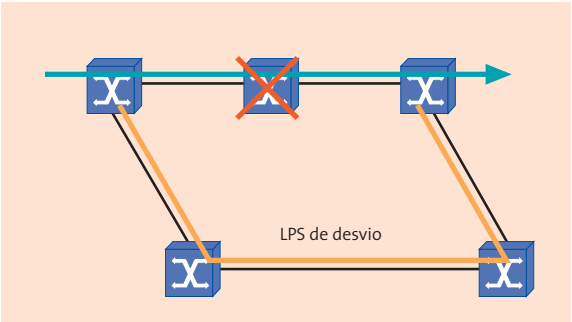

Figura 9. Protección mediante ALNP

En la arquitectura de protección "1:1", el nodo de entrada envía el tráfico a través del camino principal. Cuando se detecta un defecto, el extremo de recepción envía un paquete de indicación de defecto hacia atrás (BDI) al extremo de transmisión, para que éste conmute al LSP de protección.

Por otro lado, en la arquitectura de protección "1+1" el nodo de entrada envía el tráfico por ambos caminos de forma simultánea, para lograr que el tiempo de conmutación sea inferior a 50 ms.

EMULACIÓN DE CIRCUITOS

Los servicios de emulación de circuitos (CES) permiten el transporte de circuitos plesiócronos de velocidad constante, como E1 (2 Mbit/s) o E3 (34 Mbit/s), o síncronos como STM-1 o STM-4, sobre redes asíncronas de velocidad variable[2]. Estos servicios de emulación proporcionan soporte a las aplicaciones de voz TDM tradicional y al transporte de circuitos alquilados punto a punto.

El Metro Ethernet Forum [3] ha definido cuatro tipos generales de servicio, denominados:

1. *Servicio de línea de acceso* TDM (TALS). En este tipo de servicio, al menos uno de los puntos extremos

[2] Este servicio de transporte de tramas SDH sobre redes asíncronas precisa de un mayor estudio, sobre todo en lo relativo a la potencial degradación que el nivel de *jitter* asociado a la transmisión asíncrona puede ocasionar en los márgenes de las señales de sincronización transportadas sobre tramas SDH, debido fundamentalmente a la influencia del *jitter* en una actividad anormal de los punteros SDH.

termina en la red telefónica y permite el transporte de circuitos para voz, Frame Relay y ATM sobre redes Ethernet. El servicio lo provee y gestiona el proveedor de la red Ethernet metropolitana.

2. *Servicio de línea TDM (T-Line)*. En este tipo de servicio los puntos extremos pertenecen a una empresa. Al igual que en el caso anterior, el servicio lo provee y gestiona el proveedor de la red MEN.

3. *Servicio operado por el cliente*. En este caso el servicio lo gestiona el cliente.

4. *Servicio mixto*. Es el formado por la mezcla de cualquiera de los tres anteriores.

La **Figura 10** muestra un ejemplo de los servicios T-Line y TALS.

Modos de operación de un servicio T-Line

En los servicios T-Line es posible proporcionar servicios de multiplexación, como, por ejemplo, la agregación de varios E1 en un enlace E3, o STM-1, creando configuraciones punto a multipunto o multipunto a multipunto. Este servicio de multiplexación lo realiza el bloque opcional TSP, que procesa el servicio TDM [3] [4].

Hay tres posibles modos de operación (los dos primeros son punto a punto y el tercero permite configuraciones multipunto):

1. *El modo no estructurado*. En este caso el servicio se proporciona entre puntos con el mismo tipo de interfaz y el tráfico se transporta de forma transparente de un extremo al otro. Un ejemplo de este modo de operación lo constituyen las líneas alquiladas.

2. *El modo estructurado*. Al igual que el anterior, el servicio se proporciona entre puntos con el mismo tipo de interfaz, pero en este caso el tráfico se trata como cabecera y carga. La cabecera se termina y se crea en los extremos, y la carga se transporta de forma transparente de un extremo al otro. Un ejemplo podría ser un STM-1 conteniendo un VC-3.

3. *El modo multiplexado*. En este caso se multiplexan varios servicios de menor velocidad en una interfaz de nivel superior. La multiplexación se realiza normalmente en el dominio TDM, sin embargo, el servicio de emulación es estructurado.

Modos de operación de un servicio TALS

El servicio TALS es muy parecido al servicio T-Line multiplexado. Ambos utilizan la red Ethernet metropolitana de igual forma, excepto que en el caso de TALS, el servicio de multiplexación final es manejado por otra red en vez de por el usuario final. Por ello tiene algunos requisitos de rendimiento adicionales.

La red Ethernet debe mantener la integridad de bit, el reloj, así como otras características específicas del formato de tráfico transportado, sin causar una degradación que exceda los requisitos del servicio proporcionado. Además, todas las funciones de ges-

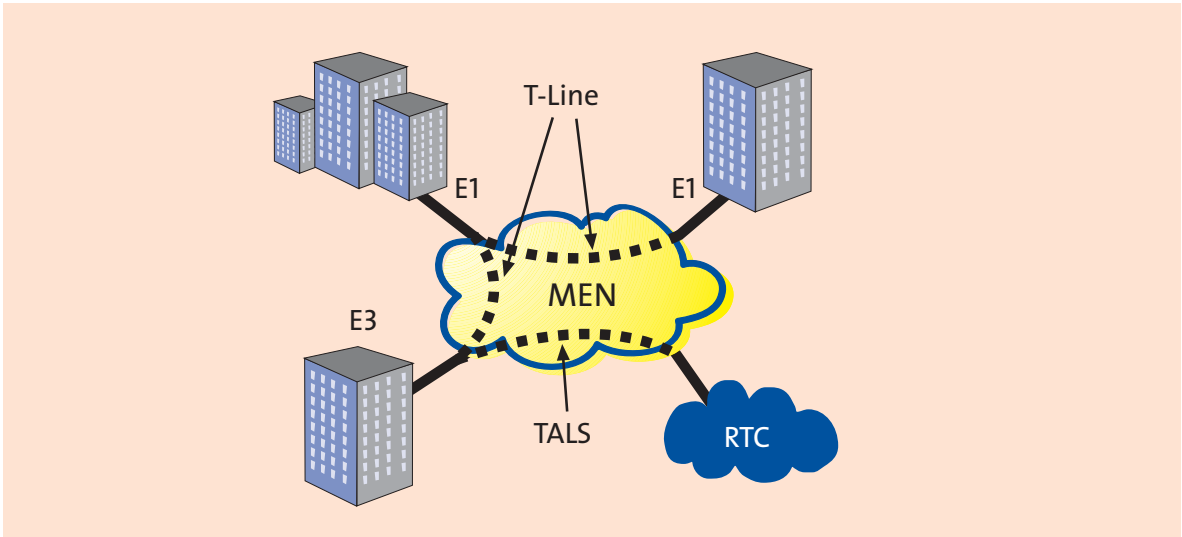

Figura 10. Servicios de emulación de circuitos

tión, monitorización, etc., deben ser realizadas sin afectar al servicio transportado.

Requisitos de los servicios de emulación de circuitos

Los requisitos principales de los servicios de emulación de circuitos son:

- *La paquetización*, que es el proceso de convertir un flujo síncrono de tráfico en tramas Ethernet. Se requiere que el retardo introducido sea constante y lo menor posible. También es posible encapsular tramas de múltiples flujos síncronos para reducir la latencia del proceso.

- *La latencia*. Se define como el retardo desde el punto de entrada del flujo TDM en la red Ethernet metropolitana, hasta el punto de salida. Si es muy elevada implica la necesidad de introducir cancelación de eco en las aplicaciones telefónicas. En las aplicaciones emergentes de vídeo interactivas, el retardo máximo también es limitado, obligando a añadir algoritmos predictivos a los algoritmos de codificación cuando este tiempo se excede. Las redes MEN son capaces de proporcionar latencias inferiores a 10 ms, por lo que es posible proporcionar emulación de circuitos sin necesidad de estos mecanismos compensatorios.

- *La variación del retardo (jitter)*. Se refiere al retardo variable introducido por la red MEN debido a su naturaleza asíncrona de conmutación Ethernet y por la variedad de longitudes de las tramas que la atraviesan. La variación del retardo puede ser compensada utilizando *buffers (jitter buffers)* en el destino, a costa de incrementar la latencia, lo que podría constituir un problema en ciertas aplicaciones de tiempo real como las citadas anteriormente.

- *La pérdida de trama y resecuenciamiento*. Ello se debe a que las tramas pueden no llegar en el mismo orden en que fueron enviadas. El nodo de destino debe reordenar las tramas, utilizando el campo de número de secuencia presente en la cabecera de la trama. A su vez, el *jitter buffer* debe comprobar el número de secuencia de las tramas que llegan y reordenarlas en caso necesario. Todo esto se realiza manteniendo el tamaño del *buffer* lo más pequeño posible para minimizar la latencia.

- *La recuperación de reloj y la sincronización*. Los circuitos transportan información de reloj que se utiliza para sincronizar el emisor con el receptor. Si existen diferencias de reloj entre el transmisor y el receptor se perderá información, reduciéndose la calidad del circuito. Para evitar estas diferencias se debe utilizar un mecanismo de recuperación de reloj, que resista la latencia, el *jitter* y la pérdida de tramas, dentro de unos determinados límites[3].

CONCLUSIONES

La combinación de Ethernet de alta velocidad a precios reducidos con la conmutación óptica puede cumplir con los requisitos de crecimiento de la demanda de ancho de banda, y puede representar una alternativa en el ámbito metropolitano a la tecnología SDH, que tradicionalmente han utilizado los operadores de telecomunicaciones.

La Ethernet óptica proporciona una plataforma para construir grandes redes Ethernet metropolitanas que ofrezcan servicios de calidad incurriendo en unos costes totales (costes de implantación, CAPEX, más costes de operación, OPEX) mucho menores que los de las tecnologías alternativas, como es el caso de la nueva generación SDH o la Ethernet sobre WDM.

Para ello, se debe dotar a la tecnología Ethernet pura de un conjunto de mecanismos (de protección, funciones OAM, emulación de circuitos, ingeniería de tráfico, garantías de calidad de servicio, etc.) que permita cumplir los estrictos requisitos de los operadores de telecomunicaciones.

Estos requisitos han sido especificados por los organismos de estandarización, principalmente la ITU y la IETF, si bien otros aspectos requerirán un mayor estudio. En breve tiempo presenciaremos la aparición de equipos capaces de cumplir todos esos requisitos.

[3] Hay que tener en cuenta que en ciertos servicios, como en el transporte de tramas SDH, la recuperación de reloj está intrínseca en la propia trama SDH, por lo que el *jitter* y la tasa de pérdidas no deberán superar ciertos límites, aspecto éste que precisa mayor estudio, como se indica en la nota número 2.

Glosario de Acrónimos

ALNP *Aggregated Line and Node Protection*. Enlace agregado y protección de nodo
ATM *Asynchronous Transfer Mode*. Modo de transferencia asíncrono
BDI *Backward Defect Indication*. Indicación de defecto hacia atrás
BER *Bit Error Rate*. Tasa de errores de bit
BFD *Bidirectional Forwarding Detection*. Detección de fallos bidireccional
CAPEX *Capital Expenditure*. Gasto de capital en la compra de bienes
CES *Circuit Emulation Service*. Servicio de emulación de circuitos
CV *Connectivity Verification*. Verificación de la conectividad
EVC *Ethernet Virtual Connection*. Conexión virtual Ethernet
FDI *Forward Defect Indication*. Indicación de defecto hacia adelante
FEC *Forwarding Equivalent Class*. Clase de servicio equivalente
FFD *Fast Failure Detection*. Detección rápida de fallos
GbE *Gigabit Ethernet*
GFP *Generic Frame Procedure*. Procedimiento de entramado genérico
IETF *Internet Engineering Task Force*
ITU *International Telecommunication Union*. Unión Internacional de Telecomunicaciones
LAN *Local Area Network*. Red de área local
LCAS *Link Capacity Adjustment Scheme*. Esquema de ajuste de la capacidad del enlace
LDP *Label Distribution Protocol*. Protocolo de distribución de etiquetas
LER *Label Edge Router*. Encaminador de borde
LOF *Loss of Frame*. Pérdida de trama
LOL *Loss of Link*. Pérdida de enlace
LOS *Loss of Signal*. Pérdida de señal
LSP *Label Switched Path*. Camino MPLS
LSR *Label Switch Router*. Encaminador MPLS
MAC *Medium Access Control*. Control de acceso al medio
MAN *Metropolitan Area Network*. Red de área metropolitana
MEN *Metropolitan Ethernet Network*. Red Ethernet metropolitana
MPLS *Multiprotocol Label Switching*. Conmutación de etiquetas multiprotocolo
OAM Operación, Administración y Mantenimiento
OPEX *Operating Expenditures*. Gastos de operación
PDH *Plesiochronous Digital Hierarchy*. Jerarquía digital plesiócrona
QoS *Quality of Service*. Calidad de servicio
RDI *Remote Defect Indication*. Indicación de defecto remoto
RSVP *ReSerVation Protocol*. Protocolo de reserva de recursos
SDH *Synchronous Digital Hierarchy*. Jerarquía digital síncrona
STM *Synchronous Transport Module*. Módulo de transporte síncrono
STP *Spanning Tree Protocol*. Protocolo de *spanning tree*
TALS *TDM Access Line Service*. Servicio de línea de acceso TDM
TDM *Time Division Multiplexing*. Multiplexación por división en el tiempo
TLS *Transparent LAN Services*. Servicios de LAN transparente
TSP *TDM Service Processor*. Procesador de servicio TDM
VC *Virtual Circuit*. Circuito virtual
VID *VLAN Identifier*. Identificador de VLAN
VLAN *Virtual LAN*. Red de área local virtual
VMAN *Virtual MAN*. Red de área metropolitana virtual
WAN *Wide Area Network*. Red de área amplia
WDN *Wavelength Division Multiplexing*. Multiplexación por división de longitud de onda.

Referencias

1. Metro Ethernet Forum: *Technical Specification MEF 1, "Ethernet Services Model, Phase 1". November 2003.*
2. Metro Ethernet Forum: *Technical Specification MEF 2, "Requirements and Framework for Ethernet Service Protection in Metro Ethernet Networks".* February 2004.
3. Metro Ethernet Forum: *Technical Specification MEF 3, "Circuit Emulation Service Definitions, Framework and Requirements in Metro Ethernet Networks".* April 2004.
4. Metro Ethernet Forum: *Technical Specification MEF 4, "Metro Ethernet Network Architecture Framework - Part 1: Generic Framework".* May 2004.
5. Metro Ethernet Forum: *Technical Specification MEF 6, "Ethernet Services Definitions - Phase I".* June 2004.
6. Metro Ethernet Forum: *Comparison to Legacy SONET/SDH MANs for Metro Data Service Providers.* July 2003.
7. Martini et al: *Encapsulation Methods for Transport of Ethernet Frames Over IP/MPLS Networks*. September 2004, *www.ietf.org/internet-drafts/draft-ietf-pwe3-ethernet-encap-08.txt*
8. ITU-T Y-1710: *Requisitos de la funcionalidad de Operación y Mantenimiento para redes MPLS.* Noviembre 2002.
9. ITU-T Y-1711: *Mecanismos de Operación y Administración para redes MPLS*. Febrero 2004.
10. ITU-T Y-1720: *Conmutación de protección para redes MPLS.* Septiembre 2003.
11. ITU-T Y-1730: *Requisitos de las funciones de Operación, Administración y Mantenimiento en redes basadas en Ethernet y en servicios Ethernet*. Enero 2004.
12. T. D. Nadeau et al: *OAM Requirements for MPLS Networks. IETF Internet Draft, draft-ietf-mpls-oam-requirements-05.txt*. December 2004.
13. Kompella et al: *Detecting MPLS Data Plane Failures*. IETF Internet Draft, ***draft-ietf-mpls-lsp-ping-07.txt***, October 2004.
14. R. Aggarwal et al: *BFD for MPLS LSPs*. IETF Internet Draft, ***draft-ietf-bfd-mpls-00.txt***, July 2004.
15. D.Katz and D.Ward: *Bidirectional Forwarding Detection*. IETF Internet Draft, ***draft-ietf-bfd-base-00.txt,*** July 2004.
16. G. Swallow, K. Kompella and D. Tappan: *Label Switching Router Self-Test*. IETF Internet Draft, ***draft-ietf-mpls-lsrself-test-03.txt,*** October 2004.
17. V. Sharma and F. Hellstrand: *Framework for Multi-Protocol Label Switching (MPLS)-based Recovery*. IETF RFC 3469, February 2003.