Experiencias con Redes Privadas Virtuales de Nivel 2 sobre una infraestructura óptica metropolitana de IP sobre DWDM

Carlos García[1], Luis M. Díaz[1], José L. Peña[2], Luis Bellido[3]
Francisco Valera[1], David Fernández[3], Arturo Azcorra[1], Julio Berrocal[3], Isidro Cabello[2], Rafael López[2]
[1]Universidad Carlos III de Madrid, [2]Telefónica I+D, [3]Universidad Politécnica de Madrid
Departamento de Ingeniería Telemática, Avda. de la Universidad 30, 28911 Leganés (Madrid)
Teléfono: 916248778 Fax: 916248749
Email: cgarcia@it.uc3m.es

Abstract*. PREAMBULO is a currently running research project, funded by the MCYT, and whose main objective is to install, configure and operate a metropolitan fiber optic research infrastructure, providing a data transport network using IP directly over DWDM. The first part of the article describes the build up of both the physical and the logical network at the three different participating nodes: Universidad Carlos III de Madrid, Universidad Politécnica de Madrid and Telefónica I+D. Over this infrastructure, different activities have been taking place: multi-video conferences, IPv6 experiences, tele-education experiences, etc. The second part of this article describes one of the technologies that are also being tested in the project as well as some of these experiences: level 2 VPN solutions.*

1 Introducción

Pese a que la existencia de infraestructuras de red basadas en fibra óptica no son hoy en día ninguna novedad, lo cierto es que en general las soluciones que se plantean para el transporte de datos sobre dichas infraestructuras vienen derivadas de arquitecturas de protocolos sustentadas normalmente por SONET o SDH.

El proyecto PREAMBULO (*Prototipo de red multiservicio de muy altas prestaciones basada en IPv4/IPv6 sobre multiplexación por longitud de onda*, [1]) es un proyecto perteneciente al plan nacional I+D+I 2000-2003 del MCyT, que plantea la instalación, configuración y operación de una red de investigación de fibra óptica en la Comunidad de Madrid, que proporcione un servicio de transporte de datos utilizando IP directamente sobre DWDM, entre los tres nodos de la red: la Universidad Carlos III de Madrid, la Universidad Politécnica de Madrid y Telefónica I+D.

En la sección dos de este artículo se describe el proyecto PREAMBULO, detallando por un lado la arquitectura que se ha puesto en funcionamiento (finales de 2002) y por otro lado las diferentes experiencias que se han realizado sobre dicha infraestructura y que se seguirán realizando hasta que termine el proyecto a finales del año 2003.

Además de las experiencias de alto nivel realizadas sobre PREAMBULO (multivideoconferencia, tele-educación, etc.), como infraestructura de red metropolitana que es, PREAMBULO se apuntó en su momento como el entorno perfecto para llevar a cabo también experiencias reales con equipamiento capaz de proporcionar soluciones de conectividad a bajo nivel.

Así, la sección tres, se centra en la descripción tecnológica de las diferentes soluciones de redes privadas virtuales que han aparecido durante estos últimos años. Pese a que se hará una breve mención a las soluciones que se plantean a nivel 3, la sección profundizará más en las soluciones de nivel 2 cuya evolución parece estar desarrollándose de forma muy activa de un tiempo a esta parte.

Por último, la sección cuatro comenta las principales experiencias de VPN de nivel 2 que se han realizado sobre la red de PREAMBULO y expone las conclusiones más importantes extraídas hasta el momento.

2 Proyecto PREAMBULO

2.1 Objetivos

La mayoría de las redes desplegadas en la actualidad que ofrecen servicios IP sobre fibras ópticas con WDM, no ofrecen el servicio IP directamente sobre WDM (2 capas), sino que tienen una arquitectura en

Figura 1. Entidades participantes en PREAMBULO [1]

3 capas, de modo que una parte de las funciones se realizan en la capa óptica (WDM), otra parte en la capa SDH (en cada longitud de onda se envían tramas SDH) y a continuación los datagramas IP vienen empaquetados en los contenedores virtuales SDH. También existen redes que ofrecen el servicio IP sobre un servicio ATM, que es ofrecido a su vez o bien sobre SDH (4 capas en total) o bien directamente sobre WDM (predominando sobre todo la primera opción). Pero el uso de IP directamente sobre WDM plantea ventajas (menos sobrecarga, ventajas económicas, gestión) que hacen interesante su desarrollo, a pesar de los temas que quedan todavía por investigar (control del tráfico, recuperación de caídas de enlaces de la red y calidad de servicio).

El proyecto PREAMBULO [1] se fundamenta en la previsión de que a medio plazo se va a producir una implantación masiva de infraestructuras de transmisión WDM que, además de soportar los servicios existentes actualmente, deberán ofrecer una respuesta eficiente en prestaciones y coste a un mercado de servicios dominado claramente por la tecnología IP.

El objetivo principal del proyecto PREAMBULO, es el de desplegar la mencionada infraestructura de red óptica y llevar a cabo experiencias avanzadas con servicios IP entre las que se encuentran:

- Tráfico multicast
- Calidad de servicio (QoS)
- IP sobre WDM
- IP versión 6 (IPv6)
- Ingeniería de tráfico
- Prestaciones de los *GigaSwitch Routers*
- Interoperabilidad con otras infraestructuras de red avanzadas

2.2 Arquitectura

La red de PREAMBULO se puede dividir por un lado en un núcleo de red, que proporciona la interconectividad necesaria para proporcionar un servicio de redes de área local virtuales (VLANs) entre los tres centros participantes, y la periferia de la red, compuesta por los distintos equipos de nivel 2 y 3 que se conectan en cada centro a este núcleo para dar un servicio IP o IPv6 a los distintos proyectos de investigación y experiencias que utilizan la infraestructura de PREAMBULO. En esta sección se detalla la arquitectura del núcleo de la red, cuya puesta en marcha ha constituido uno de los principales hitos del proyecto.

Núcleo de la red

El núcleo de la red de puede descomponer en el nivel físico, o de transmisión por fibra óptica, el nivel DWDM, y el nivel de enlace.

En el nivel físico, la red está soportada por dos pares de fibras monomodo: uno entre TID y UPM, y otro entre TID y UC3M. Sobre esta configuración "en línea", se ha establecido una red DWDM con una

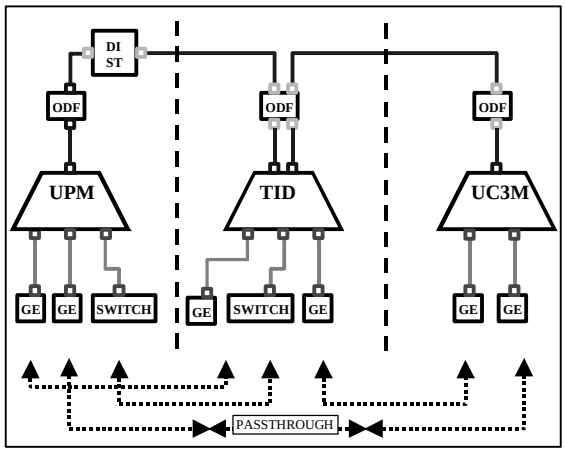

Figura 2: Esquema de la red DWDM

topología en triángulo, en la que los tres centros están conectados dos a dos. La configuración de red en el nivel DWDM se representa en la Figura 2, en la que se muestran los tres multiplexores DWDM conectados entre sí por los enlaces de fibra óptica.

Los equipos multiplexores son Nortel Optera Metro 5200. Los multiplexores en UPM y UC3M se han desplegado como terminales, de manera que todas las longitudes de onda utilizadas tienen su terminación en ellos. En cambio, el multiplexor en TID se ha desplegado como OADM (optical add/drop multiplexer), de manera que actúa como terminal para las longitudes de onda que soportan la comunicación hacia TID, y deja pasar las longitudes de onda para la comunicación UPM-UC3M, permitiendo, por tanto, una topología en triángulo entre los tres centros.

En cuanto a la conexión hacia la red de cliente, los equipos multiplexores proporcionan interfaces ópticas mediante las tarjetas denominadas OCI (optical-channel interface). En la red desplegada las interfaces utilizadas han sido Gigabit Ethernet-SX (850 nm) y ATM.

La instalación de las OCI adecuadas en cada multiplexor y el uso de tres canales o longitudes de onda distintas ha permitido desplegar una red en la que se dispone de enlaces Gigabit Ethernet (GE) dos a dos entre los tres centros y un enlace ATM adicional entre TID y UPM. Este último ha permitido continuar el servicio que ya se estaba dando sobre la fibra entre TID y UPM.

En cuanto al siguiente nivel, el nivel de enlace, el proyecto se ha centrado en proporcionar una infraestructura que proporciona un servicio de VLANs entre los tres centros participantes, utilizando los enlaces GE del nivel inferior. En un principio se evaluó la posibilidad de utilizar los enlaces GE para interconectar directamente routers IP de altas prestaciones, y proporcionar un servicio IP a los usuarios de la red PREAMBULO. Sin embargo, la utilización de conmutadores de nivel 2 ofrece las siguientes ventajas:

- Flexibilidad, versatilidad. Principalmente, la posibilidad de ejecutar diversos experimentos en paralelo y la asignación del ancho de banda disponible en fragmentos de 10/100/1000 Mbps
- Separación, independencia entre tráficos de distintos experimentos.
- Utilización de equipamiento más barato, tanto los conmutadores Ethernet, como las interfaces de nivel 2 a 100 Mbps para routers, sistemas finales (servidores) o conmutadores Ethernet adicionales.
- Posibilidad de conectar servidores directamente a la infraestructura de nivel 2.

En la decisión adoptada, también se consideró la posibilidad de reutilización de equipamiento ya existente y de los equipos adquiridos cuando el proyecto finalice.

Las características generales de la red de nivel 2 (**Figura 3**) son las siguientes:

- Topología en triangulo entre los conmutadores Ethernet de cada centro (uno o varios por centro), a través de los enlaces GE proporcionados por la red DWDM.
- Los enlaces troncales se configuran como enlaces inter-switch ("trunks"), de forma que transporten tráfico de todas las VLANs
- Cada puerto de los conmutadores Ethernet se configura como perteneciente a una determinada VLAN o como "trunk", en caso de conectar routers o servidores que pertenezcan a varias VLANs simultáneamente.

Sobre la infraestructura descrita se implementan distintos tipos de VLAN:

- Según número de participantes:
  - VLANs tipo 1: locales a un centro (sólo incluyen puertos correspondientes a un único conmutador y su tráfico nunca atraviesa el backbone).
  - VLANs tipo 2: en las que participan 2 centros (incluyen puertos en los conmutadores de dos centros y su tráfico se encamina por el enlace directo entre esos dos centros).
  - Tipo 3: VLANs en las que participan los tres centros.
- Según la velocidad de los puertos, de 10 Mbps, de 100 Mbps, de 1 Gbps o mixtas, con puertos a distintas velocidades.

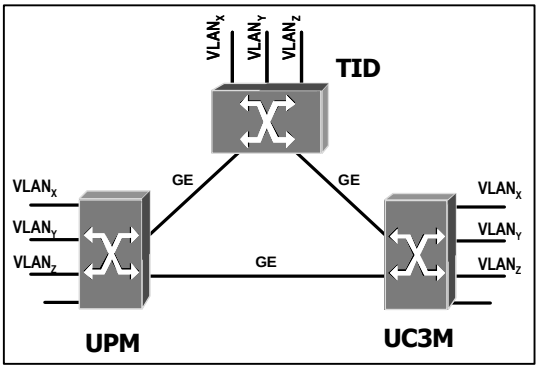

Figura 3: Red Lógica a nivel 2

Uno de los problemas que puede plantear esta topología en triángulo tiene que ver con el algoritmo de encaminamiento utilizado por los bridges: el algoritmo de *Spanning Tree (STP).*

En una topología con bucles, como es el triangulo que forman los conmutadores de la red de PREAMBULO, el algoritmo inhabilita uno de los enlaces para evitar que existan bucles, por lo que el tráfico entre dos de los centros no se encaminaría a través del enlace directo entre los mismos (ej, el tráfico entre UPM y UC3M no se encaminaría a través de su GE directa, o, peor todavía, el tráfico entre UPM y TID sería encaminado a través de UC3M).

Una posible solución a este problema sería el uso de conmutadores que ejecuten el algoritmo de Spanning-Tree por cada VLAN. Esta solución, estandarizada en [2] permitiría que, al menos para las VLAN de tipo 2, se pueda seleccionar mediante configuración (elección del nodo raíz) el enlace deshabilitado, eligiendo para cada VLAN el camino óptimo (enlace directo). Desafortunadamente, esta facilidad no está disponible en muchos de los conmutadores Ethernet que hay en el mercado

Otra alternativa, que finalmente ha sido la solución adoptada en el proyecto, consiste en deshabilitar el algoritmo STP y prohibir determinadas VLAN en cada enlace. Ambas opciones de configuración suelen ser ofrecidas por la mayoría de los fabricantes.

2.3 Experiencias

Después de proceder con la instalación de la infraestructura de red que se acaba de describir y de realizar las correspondientes pruebas de conectividad tanto a nivel físico como a nivel lógico entre las VLANs definidas, se dio por finalizado el proceso de implantación y se inició la fase de experiencias propiamente dicha (finales de 2002).

De entre las experiencias más importantes, realizadas hasta el momento, hay que destacar:

- Transporte de tráfico IPv6: una de las primeras experiencias que se realizaron, fue la migración de la maqueta IPv6 nativa implementada en el proyecto LONG [3], de tal forma que las conexiones entre UC3M, UPM y TID se han visto notablemente mejoradas.

- Vídeo-conferencias: la red de PREAMBULO se ha utilizado también para posibilitar la transmisión de eventos científico-tecnológicos (congresos, charlas, etc.). Las jornadas Telecom I+D 2002 [4], se hicieron llegar por ejemplo a las universidades utilizando PREAMBULO.

- Experiencias de tele-educación: la asignatura "*Redes de Banda Ancha*" perteneciente a la titulación de Ingeniería de Telecomunicación e impartida de forma distribuida ente las Universidades Politécnicas de Madrid, Valencia, Barcelona y la Universidad Carlos III, también se ha visto favorecida por el soporte dentro de las sedes de Madrid que se ha tenido por parte de PREAMBULO.

Además de estas experiencias que se han resaltado, se han llevado a cabo desde Febrero de 2003, diferentes pruebas de equipos y alternativas tecnológicas para proporcionar soluciones de redes privadas virtuales de nivel 2. Dichas experiencias son las que se describen en las siguientes secciones.

3 Redes Privadas Virtuales: VPN

Hoy en día, no es necesario resaltar ya la necesidad de las VPN en el entorno de red actual. Tradicionalmente, las empresas con diversas sedes han unido sus redes locales a través de líneas dedicadas punto a punto, unas veces reales, y otras veces mediante circuitos virtuales dedicados (típicamente, mediante FR/ATM). Esta situación ha perdurado mucho tiempo, pero está claro que estamos ante una solución sub-óptima, que ha provocado que los operadores deban desarrollar y mantener dos infraestructuras totalmente diferenciadas, la de tráfico de Internet (sobre una red puramente IP) y la de circuitos (sobre ATM/FR). Esta situación es, a la vez, más compleja, más cara, y más ineficiente, puesto que no se aprovechan al máximo los recursos de la red.

Actualmente, gracias a la aparición de MPLS [5], parece factible conseguir fusionar ambas infraestructuras en un único dominio administrativo, pudiendo dar el servicio de Internet, el de circuitos clásicos y el de VPN sobre la misma red. MPLS permite el aislamiento de la tecnología de nivel 2, y hacer converger desde el punto de vista de la conectividad lo mejor del mundo IP, con lo mejor del mundo de la conmutación de circuitos. Sin embargo, MPLS no resuelve por sí mismo los problemas asociados a las VPN.

3.1 VPN de nivel 3

En primer lugar, y dado que el tráfico mayoritario en la red es IP, parece obvio intentar soportar un servicio de VPN de nivel 3. Las soluciones planteadas surgen de dos grupos claramente diferenciados: el *IETF Provider Provisioned Virtual Private Networks* [6] y el *IETF Security Area* [7]. El primero se ha centrado en el uso de MPLS como solución para el soporte de VPNs de nivel 3, mientras que el otro se fundamenta en el uso de IPSec para la creación de dichas VPNs.

3.1.1 VPN-IPSec

El grupo de seguridad se centró en corregir y/o paliar las deficiencias de seguridad del protocolo IP, y crearon el protocolo IPSec [8]. Este protocolo permitía crear *Asociaciones Seguras* (SA) entre entidades, consiguiendo así confidencialidad y/o la autenticación de ambas partes. Básicamente, esta asociación segura puede verse como un túnel seguro entre dos entidades, donde ambas saben quién es realmente el otro (por ejemplo, mediante certificados X.501) y donde nadie puede escuchar ni interceptar la conversación (confidencialidad mediante cifrado). Visto así, se proporciona el soporte básico para poder crear una VPN sobre la infraestructura de Internet, pues basta con crear esta asociación segura (SA) o túnel seguro entre 2 entidades en distintas sedes de la misma VPN (típicamente, entre los cortafuegos de salida de dichas sedes) y enviar todo el tráfico IP destinado a la VPN a través de ese túnel IPSec-IP. Si se establece un mallado completo de túneles IPSec entre las distintas sedes, se crea una VPN de nivel 3, aunque esta solución no está exenta de problemas. En primer lugar, esta solución se coloca en el lado del cliente, lo cual no es del todo deseable, ya que muchos clientes prefieren contratar directamente el servicio y no tener que preocuparse de cómo ponerlo en marcha (y mucho menos mantenerlo). Además, la creación y mantenimiento de un mallado completo de túneles IPSec es una tarea compleja (hay que manejar gran cantidad de claves distintas, distribuirlas de forma segura, distribuir los certificados...), y la tarea de cifrar y descifrar exige unos recursos de computación elevados, por lo que la escalabilidad de esta solución es limitada. Finalmente, al ser una solución de cliente soportada sobre la red Internet, no tiene ningún mecanismo de QoS, al contrario de lo que ocurría en las VPN clásicas (ATM/FR).

3.1.2 BGP/MPLS

Por otro lado, aparece la solución propuesta por *Provider Provisioned Virtual Private Network Charter* [6], basada en BGP/MPLS [9]. Esta solución se basa en la construcción de túneles MPLS, mediante una doble indexación de etiquetas. El primer nivel (*inner label*) permite identificar un paquete como perteneciente a una VPN específica, mientras que la segunda etiqueta (*outer label*) permite que el paquete viaje por la red del proveedor desde el punto de entrada al de salida. BGP se usa como mecanismo de señalización de las *inner label* mientras que el mecanismo para señalizar las *outer label* es independiente de las VPN, y depende del mecanismo elegido para señalizar la red troncal del proveedor (normalmente, LDP o RSVP). Esta solución es claramente una solución de proveedor, donde el cliente sólo tiene que suministrar al proveedor el/los prefijos de red que es capaz de alcanzar. La seguridad se consigue gracias a la separación del tráfico en circuitos virtuales (igual que ocurría en ATM/FR), evitando el uso de cifrado, que es un proceso muy costoso. Además, se puede proporcionar QoS e ingeniería de tráfico a través de

los mecanismos básicos de MPLS (creación de túneles RSVP), lo cual es un servicio de valor añadido de incalculable utilidad en las redes actuales. Finalmente, la escalabilidad está asegurada gracias a esta doble indexación de etiquetas, ya que la troncal de la red no tiene que saber nada de VPNs, y los equipos frontera sólo tienen que almacenar la información relevante a las VPN's que cada uno maneje (ningún equipo de la red tiene que conocer todo sobre todas las VPNs).

Eso sí, esta solución también plantea problemas. En primer lugar, es necesario confiar en la información de encaminamiento que proporciona el cliente, lo cual no tiene por qué ser una buena idea. Además, no proporciona ningún soporte para IP Multicast, por lo que sería necesario algún mecanismo externo para soportarlo.

Finalmente, estas soluciones transportan tráfico de nivel 3, pero hace falta algún tipo de mecanismo adicional si lo que se desea es transportar de forma transparente tráfico de nivel 2.

3.3 VPNs de Nivel 2

3.3.1 Introducción

El envío de tráfico de nivel 2, tal como Ethernet, Frame Relay o ATM, sobre una red de transporte MPLS, está cobrando especial importancia en la actualidad, principalmente impulsado por el interés de los proveedores de servicio, y dirigido por determinados grupos de trabajo del IETF, así como por los principales fabricantes de equipos de transporte en la red.

Esta tecnología permitiría a los proveedores ofrecer el transporte de tráfico de los clientes mientras se continúa la migración a las redes IP de próxima generación. Es decir, seguir ofreciendo los tradicionales servicios a clientes, como enlaces Frame Relay, sobre un único núcleo IP, disminuyendo de esta forma los gastos de mantenimiento y gestión de red.

Aunque aún no se dispone de ningún estándar para ofrecer estos servicios, son muchos los fabricantes que ofrecen soporte para los borradores de Martini [10], [11] en el IETF. Como hemos comentado dentro del IETF existen dos grupos de trabajo dedicados a las redes privadas virtuales de nivel 2. Tanto el PPVPN, como el PWE3 [12], estudian la utilización de túneles basados en IP y L2TP, así como MPLS.

3.3.2 Objetivo

Como se ha comentado, una VPN es simplemente una forma de proporcionar comunicaciones privadas sobre una red pública. Tradicionalmente las empresas han contratado enlaces de nivel 2 a los proveedores de servicio, y han montado su propia infraestructura de nivel 3.

Las VPNs de nivel 2 son multiprotocolo por naturaleza, de forma que pueden soportar tanto tráfico de IP como de otros protocolos. De igual forma eliminan la participación del proveedor de servicio en las tareas de configuración de nivel 3 del cliente, beneficiando a ambos.

En la actualidad, la principal demanda de circuitos de nivel 2 se basa en tecnología Frame Relay, y poco a poco ganan terreno las VPN de nivel 2 basadas en Ethernet. En consecuencia, los principales beneficios de los proveedores de servicios vienen derivados de estas actividades. Sin embargo, supone un grave inconveniente el hecho de mantener diferentes infraestructuras para ofrecer diferentes servicios.

La nueva tecnología de VPNs de nivel 2 podría solucionar estos problemas manteniendo una única infraestructura basada en transporte sobre MPLS.

3.3.3 Túneles MPLS L2VPN

Los principales esfuerzos del IETF están dirigidos a la creación de VPNs de nivel 2 basadas en MPLS. De esta forma es posible crear túneles (LSP) basados en conmutación de etiquetas en lugar de usarIPSec. De la misma manera, es posible utilizar protocolos de control como LDP o BGP para el establecimiento de los circuitos virtuales (VCs) para el transporte de PDUs de nivel 2 a través de la red.

El borrador de Martini utiliza la técnica *label-stacking* de MPLS para permitir separar las etiquetas de circuitos virtuales (*VC labels*) y las etiquetas de túneles (*tunnel label*). La etiqueta de túnel identifica el camino que los paquetes tomaran a través de la red, mientras que la etiqueta de circuito virtual identifica la VPN en el destino (y el ingress node). En el núcleo de la red, los routers (LSRs) utilizan la etiqueta de túnel para el reenvío de paquetes, mientras los routers frontera (*egress LSRs*) usan la etiqueta de circuito virtual para determinar como procesar la trama.

Existen dos borradores de Martini, el primero de ellos [11] especifica como debe realizarse la encapsulación sobre circuitos virtuales para tecnologías como ATM, Ethernet, HDLC y PPP. Y define un campo *demultiplexor* para distinguir diferentes circuitos virtuales emulados sobre el mismo túnel. De igual forma se define una *palabra de control* (Control Word), cuya función es mantener el número de secuencia de las tramas, hacer relleno para paquetes pequeños según la tecnología de nivel 2, o llevar ciertos bits de control de este nivel. También permite la eliminación de la cabecera de nivel 2 y su reconstrucción en el router frontera.

El segundo borrador de Martini [10] define los procedimientos para la distribución de etiquetas, lo que permite el transporte de PDUs a través de una red MPLS. Aunque Martini especifica LDP para el establecimiento de túneles, otros grupos del. IETF

están estudiando el posible uso de otros protocolos (principalmente, BGP).

3.3.4 Extensiones al borrador de Martini

Si bien Martini establece la base para la creación de túneles sobre una red MPLS, debemos tener en cuenta que esto solamente proporciona túneles punto a punto. Una red privada virtual necesita de conectividad multipunto-multipunto para lo que se requiere una red mallada de túneles Martini.

En primer lugar el borrador de K. Kompella [13] especifica el uso de BGP para la distribución de bloques de etiquetas, y el mapeo de los identificadores de enlaces, en Frame Relay (DLCIs), ATM(VCIs), y otras tecnologías, sobre los circuitos virtuales.

Por otro lado Laserre [14] propone extensiones a Martini para el soporte de conectividad Ethernet multipunto-multipunto, permitiendo envío de tráfico broadcast y multicast a través de una VPN.

3.3.5 VPLS

VPLS (*Virtual Private LAN Service* [15]) identifica cómo un proveedor de servicios ofrece conectividad a nivel 2 a clientes con múltiples sedes de forma que sea transparente para el dispositivo frontera del cliente (*CE – customer edge*). El proveedor se encarga del transporte de las tramas de nivel 2 del cliente desde una sede hacia otra(s) a través del núcleo de la red. Para la provisión de este servicio se usa la tecnología de VPNs de nivel 2 basadas en MPLS.

Inicialmente la tecnología Ethernet resultaba una buena solución para las redes de área local, sin embargo, debido a su amplia difusión, en la actualidad esta tecnología está comenzando a aparecer como tecnología de acceso en redes MAN y WAN. Un puerto Ethernet permite conectar al cliente con el borde del proveedor (*PE – Provider Edge*), de manera que este tráfico se identificaría con una VPN de nivel 2 a través del identificador de puerto o de la etiqueta VLAN.

Para ofrecer este servicio, es necesario resolver el envío de paquetes en modo broadcast y multicast disponible en tecnología Ethernet, lo cual no se soporta de forma nativa en una red MPLS. Las diferentes sedes de un cliente, conectadas a través de una red MPLS, esperarán que su tráfico broadcast, multicast y unicast sea reenviado a los sitios apropiados. Esto implica ciertos requisitos en la red MPLS: aprendizaje de direcciones MAC, replicación de paquetes a través de túneles LSP para tráfico broadcast y multicast, e inundación para paquetes unicast con destinatario desconocido.

El objetivo principal de la tecnología VPLS es proporcionar de conectividad entre sitios de clientes geográficamente dispersos a través de redes MAN/WAN. De forma que el cliente perciba el mismo servicio como si estuviera conectado a través de una LAN (la red MAN/WAN se comportaría como un Bridge con aprendizaje de nivel 2).

4 Experiencias con VPLS

4.1 Introducción

Dentro del plan de pruebas propuesto en el marco del proyecto PREAMBULO, se encuentra la realización de experiencias con VPNs de nivel 2. A continuación se detalla la solución de Nortel Networks (*"Logical Provider Edge")* basada en DVPLS (Distributed VPLS, [16]), que proporciona como ya veremos ciertas mejoras sobre el mecanismo básico de VPLS visto anteriormente.

4.2 VPLS distribuido

Como se ha visto en el apartado anterior, el equipo clave para el correcto funcionamiento del servicio VPLS es el PE (*Provider Edge*). Este equipo (como mínimo) tiene que tener toda la información de las VPNs a la que pertenecen sus clientes, intercambiar las etiquetas de circuito virtual (*VC Labels)* con los otros PE (típicamente con BGP o LDP), intercambiar las etiquetas de túnel (*Tunnel Label)* con sus vecinos de la red troncal (mediante RSVP o LDP, dependiendo de si se desea hacer ingeniería de tráfico o no) y debe realizar el aprendizaje de direcciones MAC. Juntar toda esta funcionalidad en un único equipo plantea serios problemas.

En primer lugar, es evidente que un equipo de estas características será muy complejo, y por lo tanto muy caro. Además, teniendo en cuenta que el equipo tiene que hacer el aprendizaje de direcciones MAC de todas las máquinas asociadas a las VPNs de las que es miembro, la escalabilidad se ve limitada al número máximo de direcciones que sea capaz de almacenar en memoria. Desde estos puntos de vista es por tanto razonable plantearse que la solución con un único PE es ciertamente mejorable.

VPLS distribuido plantea una solución al problema de la escalabilidad y complejidad del PE. Esta solución se basa en desagregar la funcionalidad del PE en dos entidades: *PE-core* y *PE-edge*. La primera es la encargada de gestionar y mantener los túneles MPLS (*VC* y *Túnel Labels*) y de distribuir la información de VPNs al resto de PE, y la segunda entidad se encarga del aprendizaje de direcciones MAC y de la delimitación del servicio (cuando llega una trama MAC de cliente es capaz de identificar la VPN a la que pertenece y de saber el PE al que debe llegar dicha trama). Con esta arquitectura, separamos toda la complejidad asociada a los procesos MPLS de la mecánica propia del servicio VPLS en dos tipos de equipo diferentes, y como por cada *PE-core* tendremos varios *PE-edge*, se mejora sustancialmente la escalabilidad del conjunto sin aumentar la complejidad ni el coste de la solución.

4.3 Solución LPE

La solución planteada por Nortel Networks para la implementación de VPNs de nivel dos está basada en la arquitectura *"Logical Provider Edge"* (LPE). Esta arquitectura permite reducir la complejidad de los actuales PEs, desagregando sus funciones en varios equipos físicamente separados. Esta separación en entidades independientes permite obtener una solución mucho más rentable en costes y aumentar considerablemente el grado de escalabilidad y agregación de clientes.

Nortel Networks, dentro de su división *Optical Ethernet (OE),* propone dos equipos para realizar las funciones de un PE clásico: PE-edge y PE-core. Dentro de su gama de equipos, la funcionalidad del PE-edge viene implementada con sus equipos de la serie OM1000, mientras que para el PE-Core se utilizan los equipos de la serie OM8000.

El PE-edge es el encargado de separar la demarcación entre el cliente y el proveedor, realizar la agregación de los clientes, mantener las tablas de reenvío para cada servicio VPN definido, informar al PE-core de nuevas incorporaciones y aplicar políticas de calidad de servicio en caso que se necesiten.

Por otra parte, el PE-core es responsable de distribuir y mantener las etiquetas MPLS e información de VPNs entre los PE-core del backbone, realizar la encapsulación Martini, mantener la información de registro de los clientes de las VPNs y controlar los procesos de encaminamiento.

Los equipos de Nortel Networks poseen un mecanismo propietario para detectar de manera automática la incorporación de un nuevo cliente a un servicio VPN y propagar esa información por todo el backbone MPLS a todos los PE-cores. Para ello, el PE-edge utiliza un protocolo llamado OE-AD *(OE-Autodiscovery Protocol)* que informa al PE-core de la nueva incorporación en el PE-Edge. Esto permite que la provisión de nuevos clientes se realice de manera muy sencilla y rápida.

Los PE-edges independizan el tráfico de usuario frente al tráfico de proveedor demarcando el acceso del cliente con puertos UNI *(User Network Interfaces).* Estos puertos proporcionan la conexión con los servicios VPN de nivel 2 configurados en la red. Por esta razón, cualquier inestabilidad producida por el tráfico del cliente no afecta en absoluto a las características de la red del proveedor. Esto se consigue realizando una doble encapsulación del tráfico de cliente añadiendo una cabecera de nivel 2 *(Service Provider Ethernet Header)* y otra de nivel 3 *(OE/L2 Header).* Esta información permite que el paquete sea encaminado por una red de nivel 2 tradicional desde el PE-edge hasta el PE-core ya que las cabeceras introducidas respetan los campos definidos por el estándar 802.3 y de una cabecera IP normal.

Una vez que el tráfico de cliente llega al PE-core, éste analiza la cabecera OE-L2 para saber a que VPN pertenece y lo envía por los túneles MPLS de salida asociados al servicio. Cuando el tráfico llega a los extremos remotos es desencapsulado y vuelto a encapsular con las cabeceras Service Provider Ethernet y OE/L2 hasta que llega al PE-edge remoto. Una vez allí, se desencapsulan las cabeceras y se transmite por el puerto UNI de salida correspondiente del cliente configurado.

La **Figura 4** muestra el backbone MPLS utilizado entre los tres centros participantes.

Además de la implementación LPE, Nortel Networks posee un función propietaria para dar redundancia de equipo y enlace bastante eficiente llamada *Split Multilink Trunking (SMLT).* SMLT permite tener tiempos de convergencia entre 1 y 2 segundos como máximo muy inferiores a los conseguidos por STP. SMLT limita su funcionamiento a entornos de cliente "*dual homing*". Hace uso de varios switches donde se utilizan técnicas de agregación de enlace (MLT) y un protocolo de comunicación entre los switches SMLT llamado IST que es usado para intercambiarse las MACs aprendidas entre ellos.

Por lo tanto como conclusión, la solución de Nortel Networks ofrece:

- Facilidad y rapidez en la provisión de nuevos clientes.
- Una clara demarcación entre cliente y proveedor de servicio (UNI).
- Descubrimiento automático de clientes en toda la red gracias al OE-AD.
- Una gran capacidad de escalabilidad.
- Tiempos de recuperación ante fallos muy rápidos (S-MLT).

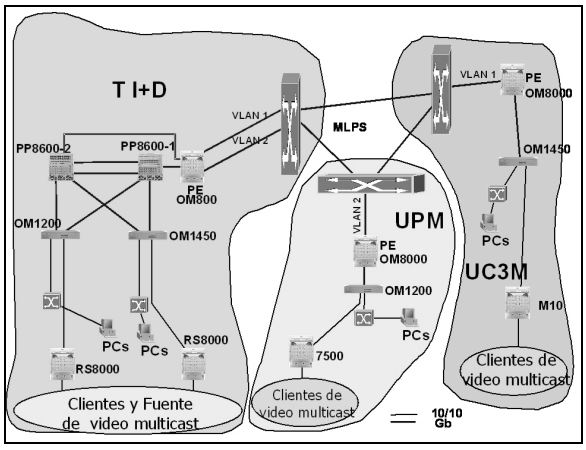

Figura 4. Maqueta LPE de Nortel

5 Conclusiones

En este artículo se ha presentado la infraestructura de red óptica para soporte de IP directamente sobre DWDM del proyecto PREAMBULO, describiéndola tanto a nivel físico como a nivel lógico y comentando las principales alternativas que se dieron antes de optar por una solución definitiva que proporcionase la conectividad deseada entre las tres sedes que participan en el proyecto.

Dicha solución se basa en mantener la conectividad a nivel 2 mediante conmutadores (con el algoritmo *Spanning Tree* deshabilitado), y utilizando VLANs para separar directamente a ese nivel el tráfico que va a circular por la red óptica.

Tras presentar las principales experiencias llevadas a cabo en el proyecto, el artículo se centra en una de ellas, las experiencias con soluciones de redes privadas de nivel 2.

Posteriormente se ha hecho una revisión de las principales líneas de investigación en lo referente a redes privadas virtuales (VPN), comentando la solución para VPNs de nivel 3, y haciendo especial énfasis en las soluciones de nivel 2.

Dichas soluciones se basan en tecnologías que se encuentra actualmente en desarrollo, y para las que han comenzado recientemente a aparecer las primeras implementaciones en equipos comerciales. Si bien casi todas las propuestas se basan en el uso de túneles Martini, existen diferentes propuestas para el establecimiento de los circuitos virtuales.

Finalmente se analiza la infraestructura que se ha probado dentro del proyecto PREAMBULO para dar soporte a una solución concreta VPN de nivel 2, Logical PE, propuesta por el fabricante Nortel Networks. De esta forma se demuestra la viabilidad de esta tecnología de última generación, comprobando las ventajas respecto a soluciones previas que presentaban ciertos problemas de escalabilidad.

Agradecimientos

Este artículo ha sido posible gracias a la financiación del proyecto PREAMBULO por parte del Ministerio de Ciencia y Tecnología, a través de su plan nacional I+D+I 2000-2003.

Las pruebas de VPN de nivel 2 han sido posibles gracias a Nortel Networks, que proporcionó tanto los equipos como la formación necesaria para llevarlas a cabo.

Referencias

[1] PREAMBULO. *Prototipo de red multiservicio de muy altas prestaciones basada en IPv4/IPv6 sobre multiplexación por longitud de onda* (TIC2000-0268-P4-C03-01). http://www.it.uc3m.es/preambulo [Abril 2003]

[2] IEEE 802.1s – Multiple Spannings Trees http://www.ieee802.org/1/pages/802.1s.html

[3] LONG. *Laboratories Over Next Generation Networks.* IST-1999-20393. http://long.ccaba.upc.es/

[4] Jornadas Telecom I+D. www.telecom-id.com

[5] IETF Multi-Protocol Label Switching Charter. http://www.ietf.org/html.charters/mpls-charter.html [Marzo 2003]

[6] IETF Provider Provisioned Virtual Private Networks Charter (ppvpn). http://www.ietf.org/html.charters/ppvpn-charter.html [Marzo 2003]

[7] IETF Security Area. http://sec.ietf.org

[8] IETF IP Security Protocol Charter (IPSec). http://www.ietf.org/html.charters/ipsec-charter.html [Enero 2003]

[9] RFC 2547bis: BGP/MPLS. http://www.ietf.org/rfc/rfc2547.txt [Enero 2003]

[10] Transport of Layer 2 Frames over MPLS. http://www.ietf.org/internet-drafts/draft-martini-l2circuit-trans-mpls-10.txt

[11] Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks. http://www.ietf.org/internet-drafts/draft-martini-l2circuit-encap-mpls-04.txt

[12] IETF Pseudo Wire Emulation Edge to Edge. http://www.ietf.org/html.charters/pwe3-charter.html [Marzo 2003]

[13] Layer 2 VPN Over Tunnels. http://www.ietf.org/internet-drafts/draft-kompella-ppvpn-l2vpn-02.txt

[14] Virtual Private LAN Service over MPLS. http://www.ietf.org/internet-drafts/draft-laserre-vkompella-ppvpn-vpls-03.txt

[15] Virtual Private LAN Service. http://www.ietf.org/internet-drafts/draft-kompella-ppvpn-vpls-01.txt

[16] Decoupled Virtual Private LAN Services http://ietf.org/intenet-drafts/draft-kompella-ppvpn-dtls-02.txt