Layer 2 VPN experiences over a metro IPoDWDM network

F. Valera, C. García, A. Azcorra (1)
L. Bellido, D. Fernández, J. Berrocal (2)
L.M. Díaz-Vizcaino, J.L. Peña, I. Cabello (3)

Abstract-- **PREAMBULO is a recently finished research project, funded by the Spanish Science and Technology Ministry, whose main objective was to install, configure and operate a metropolitan fiber optic research infrastructure, providing a data transport network using IP over Gigabit Ethernet/DWDM. The first part of this article describes the build up of both the physical and the logical network that involves the three different participating nodes: Universidad Carlos III de Madrid, Technical University of Madrid and Telefónica I+D. The second section of this article describes the different activities that have been carried out over this infrastructure: multi-video conferences, IPv6 experiences, e–learning experiences, layer 2 VPN solutions. The last part of the article will focus on these solutions, describing both the current state of the art and the experiences that have been performed with solutions implemented in commercial equipments over PREAMBULO metropolitan infrastructure.**

Index terms—**VPN, DWDM, network architecture, metropolitan, IP services**

I. Introduction

Although the existence of optical fiber based network infrastructures does not really represent a significant development nowadays, it is also true that in general, data transport solutions over these networks are traditionally dependent on protocol architectures built over SONET or SDH.

PREAMBULO project (*Very High Performance Multiservice Network Prototype based on IPv4/IPv6 Over Wavelength Division Multiplexing* [1]) belongs to the Spanish Science and Technology Ministry Research and Development Program (period 2000-2003), and planed to install, configure and operate a research fiber optic metropolitan network in Madrid in order to provide a data transport service using IP directly over Gigabit Ethernet/DWDM between the three network nodes: University Carlos III of Madrid (UC3M), Technical University of Madrid (UPM) and Telefónica I+D (TID). PREAMBULO project was recently concluded by the end of 2003 and its main results are presented in this paper.

In the first part of this article, section two describes PREAMBULO project, commenting the different objectives that were to be achieved. This section is also including an explanation of the architecture that has been installed and operated since the end of 2002 and focuses on the most important details derived from the physical and the logical configuration. Finally, section three comments the most relevant experiences carried out within the network.

Apart from the high level experiences tested over PREAMBULO (multi-videoconferences, e-learning, etc.), as a metropolitan network PREAMBULO represents a perfect environment in order to perform real experiences with equipment capable of providing low level connectivity solutions.

The second part of the article (beginning with section four) considers the different proposal for virtual private networks (VPN) that have been done during these last years. Although a minor mention will be done to level 3 solutions, the article is focusing on level 2 solutions (VPNL2) that are passing now through a very active developing period. Section five is showing the most important experiences carried out in PREAMBULO regarding to VPNL2 and shows the most important conclusions obtained from these tests.

II. Preambulo Project

A. Objectives

Most of the networks that are deployed at the moment and that are actually offering IP services over optical fibers with WDM, are not usually offering them using two tier protocol architectures (IP over WDM, using a layer 2 encapsulation scheme like Gigabit Ethernet).

The service is normally offered using three tiers so that several functions are done in the optical tier (WDM), some others in the digital layers SDH (SONET) and finally IP datagrams are packed in SDH virtual containers.

(1) Department of Telematic Engineering.
Universidad Carlos III de Madrid (Spain)
(2) Department of Telematic Systems Engineering.
Universidad Politécnica de Madrid (Spain)
(3) Telefónica I+D. Madrid (Spain)

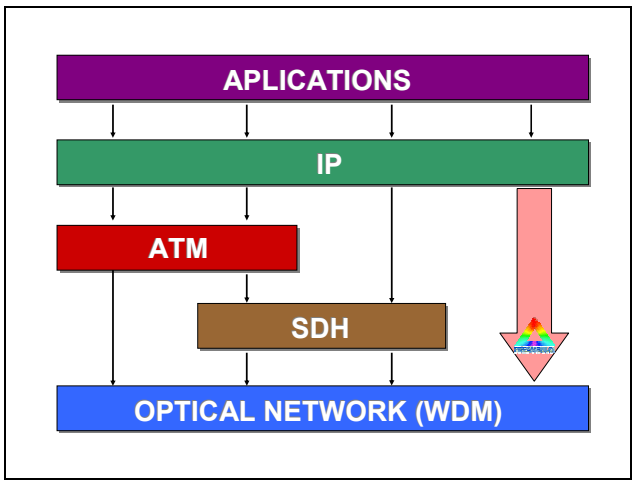

Figure 1. DWDM network

There are some other networks (typically the ones with quality of service requirements) that are offering IP services over ATM, and then over SDH/WDM (using a total of four tiers) or directly over WDM (three tiers).

But despite of the details that are still pending to be solved (traffic control, link recovery and quality of service), the usage of IP directly over WDM is showing notorious advantages and its development is beginning to be considered more and more interesting (less overhead, economical advantages, easier management).

PREAMBULO project assumes that in the short term a massive deployment of DWDM transmission infrastructures is going to be introduced in order to better exploit existing optical networks. Apart from supporting all the existing services, they are also bound to offer an efficient performance and a competitive cost in a technological marketplace that is basically dominated by IP based protocols and applications.

The main objective of PREAMBULO is to deploy the mentioned two tier metropolitan optical network infrastructure and to carry out advanced experiences with IP services:

- IP over DWDM.
- IP version 6 (IPv6).
- Multicast traffic.
- Quality of Service (QoS).
- Traffic engineering.
- GigaSwitch Routers performance.
- Interoperability with other advanced network infrastructures.

B. Architecture

The PREAMBULO network can be divided in two: the core of the network, and the network periphery. The core offers the required interconnectivity to provide a service of Virtual Local Area Networks (VLANs) between the three participating centers. The periphery is composed of different level 2 and level 3 equipment, and is connected in each center to the core of the network to provide IP and IPv6 services to different research projects and experiments using this network infrastructure. The design, implementation and operation of the network core have probably been the main achievement of the PREAMBULO project. In this section the network core architecture is explained in detail.

1) Network Core

The network core can be broken down into three levels: physical level or optical fiber transmission level, DWDM level and link level.

At the physical level, the network is supported by two pairs of single-mode fibers: one between TID and UPM and the other one between TID and UC3M. Over this centralized configuration, a DWDM network with a triangle topology has been established: every center is connected to the other two. The DWDM network configuration is represented in Fig. 2, which shows the three DWDM multiplexers (one in each center) connected by the optical fiber links.

The multiplexer optical equipment used was the Nortel Neworks Optera Metro 5200 Multiservice Platform. UPM and UC3M multiplexers have been deployed as terminal sites where all wavelengths used in the network are terminated, i.e., demultiplexed and converted, and then directed to the access devices. At TID, the multiplexer has been deployed as OADM (optical add/drop multiplexer), so it acts as a terminal for those wavelengths supporting communication to TID, while the other wavelengths, supporting the communication UPM-UC3M, are optically passed through. This configuration makes it possible to have a triangle topology for linking the three centers.

Regarding the connection to the client network, the multiplexer equipment is provided with optical interfaces by means of the OCI cards (optical-channel interface). In the current configuration, Gigabit Ethernet-SX (850 nm) and ATM OCIs have been deployed.

The combination of different OCIs at each center and the use of three different channels or wavelengths, have made it possible to deploy a network in which there were Gigabit Ethernet (GE) links between each pair of centers and an additional ATM link between TID and UPM. The ATM link was required to continue the service which was already being delivered over the fiber between TID and UPM.

In the next level, the link level, the project focused on providing an infrastructure to give a VLAN service between the three participating centers, using the GE links from the lower level. The use of GE links to directly interconnect high performance IP routers that would provide the IP service to the user of the PREAMBULO network was also evaluated in the project. However, the use of level-2 switches was found to have the following benefits:

- Flexibility, versatility. Mainly, the possibility of running different experiments in parallel, and the allocation of the available bandwidth in fragments of 10/100/1000 Mbps.
- Separation, independence between the traffic of different experiments.
- More economical equipment. Ethernet switches, 100 Mbps network cards for routers and terminals (servers) or additional switches connected to PREAMBULO.
- Possibility of connecting servers directly to the level 2 infrastructure.

Other factors were considered, such as the possible reutilization of existing equipment, and the reutilization of the acquired equipment at the end of the project.

The general features of the level 2 network (Fig. 2, bottom) are the following:

- Triangle topology between the Ethernet switches in each center (one or several switches in each center), using the GE links provided by the DWDM network.
- The backbone links were configured as inter-switch links, so they carry all traffic from different VLANs.
- Each port was configured as belonging to a specific VLAN, except the ones used in the backbone. Other possible exceptions were ports that should be used to connect routers or servers simultaneously belonging to different VLANs.

III. EXPERIENCES

After the installation of the network infrastructure that has just been described and the realization of the corresponding connectivity tests both at the physical and at the logical layer between the defined VLANs, the deployment process was considered to be finished, and the trials stage was begun (end of 2002).

A. *Connectivity tests*

In order to test the proper installation of all the DWDM infrastructure a ring model was used. All the optical equipment was connected as a ring that began and finished at TID headquarters, and all the nodes were tested during two days. For this purpose in and out interfaces were connected to a Smartbits 6009, where traffic was being continuously generated. Fig. 3 represents the proposed topology for tests.

After these tests it could be checked that several thousands of Gigabits were properly sent and received, without any error, so it was possible to proceed with the configuration of the VLANs in the switches connected to the optical equipment.

As explained before a set of VLANs were defined between each pair of entities, and different VLANs were created to allow the interconnection of the three entities.

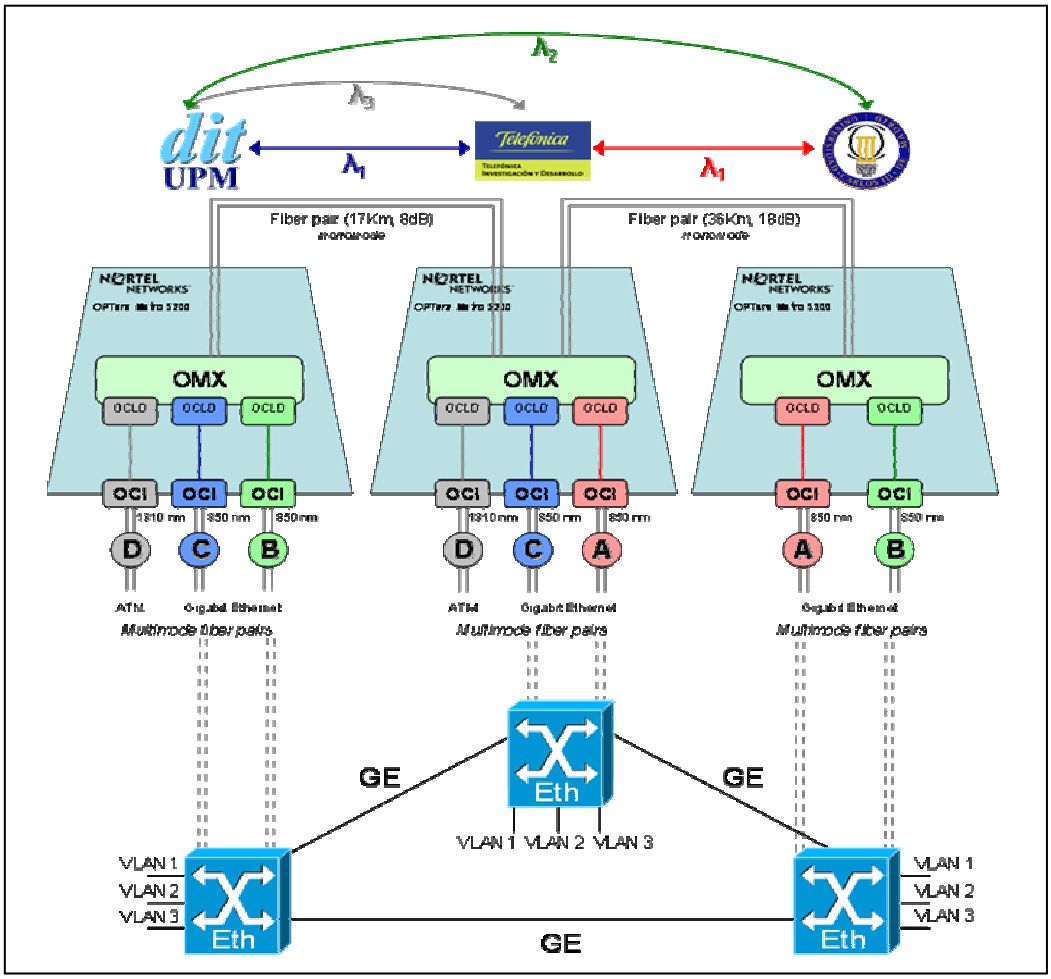

Figure 2. PREAMBULO level 2 and DWDM network configuration

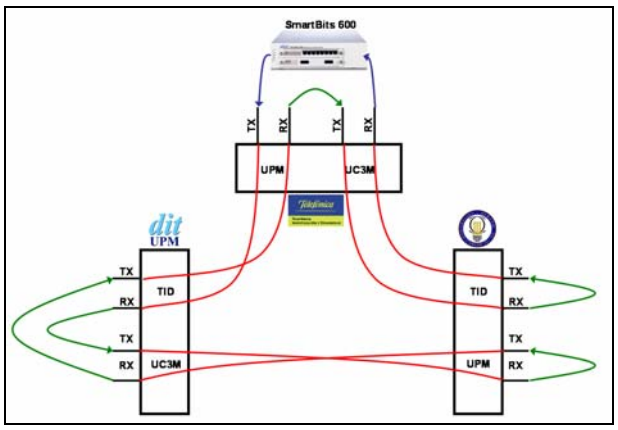

Figure 3. Connectivity test

B. *Video-conferences*

PREAMBULO network has also been used for the transmission of scientific-technological events (meetings, speeches, etc.) between the different nodes of the network. In order to perform this multimedia distribution, a tool developed at UPM, called ISABEL [3] was used.

ISABEL platforms are constructed over standard IP networks using either IP unicast, IP multicast or mixtures of both. A variety of underlying networking technologies can be used to construct the platforms, which may include Internet, GEANT, Internet 2, Canarie, LANs, ATM, ISDN, Frame Relay, satellite, etc. As real time collaboration sessions require some kind of quality of service assurance, network connectivity should assure minimum bandwidth availability for the traffic belonging to the ISABEL session. ISABEL has several unique features compared with standard videoconferencing [3].

PREAMBULO has supported the transmission of the following events to the different nodes:

- IPv6 Forum [4]: this meeting is dedicated to the diffusion of IPv6 technologies and was transmitted using ISABEL over IPv6.
- Telecom I+D 2002 and 2003 [5]: these journals are sponsored by the most relevant businesses and universities in Spain, and summarized the state of research and development at 2002.
- NGN-Ethernet workshop. This distributed event with a great number of participating entities was holding different speeches about new generation networks (optical networks, IPv6, IPv6 mobility, etc.).

C. *IPv6 traffic transport*

One of the first experiences in the network was the migration of the native IPv6 prototype implemented in the European IST project LONG [6], so that connections between UC3M, UPM and TID have notably been improved from IPv6 viewpoint.

LONG (IST-1999-20393), aims to foresee and solve problems related to the design, configuration and deployment of Next Generation Telecommunication networks specially when new services and applications are carried out across them. The new version of the IP protocol, IPv6, will become an integral part of these Next Generation networks. In addition to this, the proliferation of new high bandwidth and asymmetric access technologies, like ADSL and CATV, will also shape the network design of these Next Generation Networks.

Fig. 4 represents the LONG infrastructure at UC3M, and the DWDM cloud represents the support provided by PREAMBULO to this project.

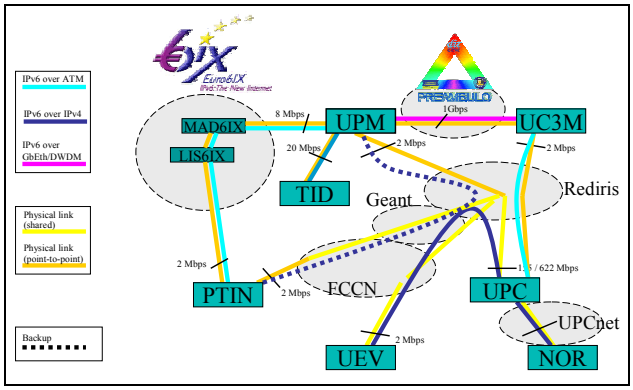

Figure 4. LONG network at UC3M

D. *Multi-video-conferences*

In order to test the network performance and as a tool to support internal meetings a multi-video-conference tool developed at TID was used. This tool runs in a Windows NT system and is supported by the IGMP protocol to perform the distribution of video and audio through multicast.

The video and audio rates are 11 Mbps and 2 Mbps respectively, so each connection generates a rate of 13 Mbps. No compression is used, so video and audio are distributed in a raw and high quality format.

E. *E-learning*

The subject "Broadband Networks", which belongs to the Telecommunication Engineering program (5th year) is taught in a distributed way between the following universities: Technical University of Madrid, Universidad of Valencia, University of Catalunya (Barcelona) and University Carlos III of Madrid. PREAMBULO has supported this subject using ISABEL over IPv4.

F. *Layer 2 VPN*

Besides these experiences, different tests of equipments and technological alternatives to provide virtual private solutions of layer 2 networks (Layer 2 VPN) have been carried out from February of 2003. Such experiences are described in successive sections.

IV. VIRTUAL PRIVATE NETWORKS

Nowadays it is not necessary to stress the requirements for VPN in the existing network environment. The typical private network scenario has usually been based on connecting the different local area networks of a certain company through point-to-point dedicated links, either leased lines or dedicated virtual links, using for example FR/ATM.
This kind of environment has been kept for a long time, but now it is clear that the situation does not fit the current network framework anymore.

Operators are bound to keep a double network infrastructure, one for IP traffic (over a native IP network) and another one for circuit-based applications (over FR/ATM). This situation is becoming more and more expensive and inefficient since network resources are not optimally exploited.

With the appearance of the Multiprotocol Label Switching Technology (MPLS [7]), it seems feasible to join both infrastructures within the same administrative domain, making it possible to operate Internet services, classical circuit services and VPN services over the same network. MPLS allows isolating level 2 technology and merging from the connectivity point of view the best of IP world and the best of the switched circuit world. However, it must also be noted that MPLS does not solve by itself the problems associated with VPNs.

A. Layer 3 VPN

Since IP traffic is the most important one in the networks, it seems to be mandatory to support VPNL3 services (level 3 Virtual Private Networks). The different solutions come from two clearly differentiated groups: the IETF Level 3 Virtual Private Networks (L3VPN) [8] and the IETF Security Area [9]. L3VPN has focused on the usage of MPLS as the main support to provide level 3 VPNs while the IETF Security Area is focusing on IPSec in order to create these VPNs.

1) VPN-IPSec

The security group focused on correcting and/or mitigating the security lacks of IP protocol and so they created IPSec [10]. This protocol allows the establishment of Secure Associations (SA) between entities, obtaining confidentiality and/or authentication from both sides. This secure association can basically be seen as a secure tunnel between both ends, where the two entities know each other (for example through X.501 certificates) and where nobody can listen or capture the information interchange (confidentiality through ciphering techniques).
This is then the basic support in order to create VPNs over the existing Internet infrastructure, since the only thing to be done is to create this security association (SA) or secure tunnel between two entities in different sites of the same VPN (typically between the outgoing firewalls of these sites) and to send IP traffic towards the VPN through this IPSec-IP tunnel. If a full mesh of IPSec tunnels is established between the different sites, a level 3 VPN is then created.

2) BGP/MPLS

On the other hand, there exists the solution proposed by the L3VPN, based on BGP/MPLS [11]. This solution is based on the construction of MPLS tunnels with a double label indexation. The first level (inner label) allows identifying a packet as belonging to a specific VPN, while the second level (outer label) allows the packet traveling through the provider network entry point to the exiting point. BGP is used as signaling mechanism for the inner labels while the outer labels signaling mechanism is independent of VPNs and relies on the mechanism chosen for the provider core network (usually LDP or RSVP).

This is clearly a provider solution where a client only needs to supply the provider with its network prefixes. Security is obtained by splitting the traffic in virtual circuits (the same as it happened in ATM/FR) and avoiding the usage of costly ciphering mechanisms.

B. Layer 2 VPNs

1) Introduction

Layer 2 traffic delivery, just as Ethernet, Frame Relay or ATM, over an MPLS transport network, is currently acquiring special importance, mainly prompted by the interest of service providers, and directed by specific IETF working groups, as well as by the main network transport equipment manufacturers.

This technology would allow the providers to offer the transport of client traffic while the migration to next generation IP networks is being carried out. Traditional services to clients, such as Frame Relay links, would be carried out over an IP core, thus reducing the costs of network maintenance and management. Although there is still not a standard to offer these services, many manufacturers offer support of Martini drafts [12], [13]. Standardization efforts on layer 2 virtual private networks by the IETF are being carried out in two working groups: L2VPN and PWE3 [14] and [15] study the utilization of tunnels based on IP and L2TP, as well as MPLS.

2) Objective

As previously commented, a VPN is just a way to provide private communications over a public network. Companies have traditionally hired layer 2 links to service providers, and have installed their own layer 3 infrastructure.

Layer 2 VPNs are multiprotocol by definition, so they can carry as much IP traffic as well as any other

protocols. Service providers will not have to take part in the management of layer 3 client tasks, which benefits both client and provider.

Layer 2 circuits are usually based on Frame Relay technology although there seems to be a notorious trend towards layer 2 VPNs based on Ethernet. The most important benefits for service providers will be probably coming from these activities but at the moment, there is a significant problem that has to be faced: different infrastructures must be maintained in order to offer different services. The new layer 2 VPNs technology will be able to solve these problems based on a native MPLS transport infrastructure.

3) L2VPN MPLS Tunnels

The main efforts within the IETF are focused on the development of layer 2 VPNs based on MPLS. This way it is possible to create tunnels (LSP) based on label switching instead of using IPSec. Besides, it is possible to use control protocols such as LDP or BGP for the establishment of the virtual circuits (VCs) for the transportation of layer 2 PDUs through the network.

Martini drafts use MPLS 'label stacking' technique in order to separate virtual circuit labels (VC labels) and tunnel labels (TL). The tunnel label identifies the path that packages take through the network, while the virtual circuit label identifies the ingress node and the VPN in the destination. In the core, the routers (LSRs) are able to use tunnel labels in order to forward packages, while the border routers (egress LSRs) use the virtual circuit label to determine how packets must be processed.

There are two Martini drafts, the first one [12] specifies how encapsulation must be carried out on virtual circuits for technologies such as ATM, Ethernet, HDLC and PPP. It also defines a demultiplexing field in order to distinguish different virtual circuits on the same tunnel. In addition, it defines a control word which is used to maintain packet sequence numbers, and to pad small packages according to layer 2 technologies, and to carry certain control bits of this layer. Finally, it allows removing the layer 2 header and its reconstruction in the border router.

The second Martini draft [13] defines the label distribution procedures, so as to allow PDUs delivery through a MPLS network. Although Martini specifies LDP for the establishment of tunnels, other IETF groups are studying the possible use of other protocols (mainly BGP).

4) Extensions to Martini draft

Martini establishes the base for the creation of tunnels on an MPLS network, but it must be taken into account that this mechanism is only able to provide point to point tunnels. A virtual private network needs multipoint to multipoint connectivity, and this requires a full meshed Martini tunnel network.

In order to accomplish this task, the K. Kompella draft [16] specifies the use of BGP for labels blocks distribution, and the mapping of link identifiers, in Frame Relay (DLCIs), ATM (VCIs), and other technologies, on the virtual circuits.

On the other hand, Laserre [17] proposes extensions to Martini to support Ethernet multipoint to multipoint connectivity, allowing delivery of broadcast and multicast traffic through a VPN.

5) VPLS

VPLS (*Virtual Private LAN Service* [16]) specifies how a service provider offers layer 2 connectivity to clients with several sites, in a transparent manner for edge client devices (CE – customer edge). Provider deals with client layer 2 frame transport from one site to another across core networks. MPLS based layer 2 VPNs technology is used to support service provisioning.

Ethernet technology was a good LAN solution, however, due to its wide spread usage, nowadays it is beginning to appear as a MAN/WAN access technology. An Ethernet port allows a client and an edge provider to be connected, so that traffic will be identified as part of one layer 2 VPN due to the port identifier or the VLAN tag.

In order to provide this service, Ethernet broadcast and multicast packet sending must be solved, because it is not natively supported on MPLS. Different client sites, connected over a MPLS network, expect that broadcast, multicast and unicast traffic will be forwarded to the proper site. Thus, the MPLS network must satisfy certain requirements: MAC learning, broadcast and multicast packet replication across LSP tunnels, and unknown destination unicast packet flooding.

The most important purpose of VPLS is then to supply connectivity between geographically distributed clients across a MAN/WAN network, so that clients will perceive the same service as in a LAN connection (MAN/WAN network works as a learning layer 2 bridge).

V. VPLS EXPERIENCES

A. Introduction

Inside the PREAMBULO project, the proposed test-bed meets layer 2 VPNs experiences, and in the following subsections the IETF draft describing Logical Provider Edge architecture is shown. Based on GVPLS (GVPLS, [18]), it provides (as will be seen) certain improvements over the basic mechanism of VPLS shown before.

B. *Distributed VPLS*

As seen in the previous section, the PE (Provider edge) is the key equipment for a correct VPLS service working. This equipment must have all VPNs information to which its clients belong to, interchange Virtual Circuit labels (VC labels) with other PE (typically by means of BGP or LDP), interchange Tunnel labels with core network neighbors (by means of RSVP or LDP, depending on the existence of traffic engineering operations or not) and accomplish MAC learning.

However, from a technological point of view it is very difficult to keep all this functionality together in the same equipment. First of all, this kind of equipment will obviously be complex, and therefore very expensive. Besides, this equipment must do MAC learning of all the machines that are members of the VPNs which it supports, so scalability will be limited to the maximum number of storable MAC addresses in memory. From this point of view, it is reasonable to consider that the stand-alone PE solution could be improved.

Generalized VPLS [18] proposes a solution to PE's scalability and complexity problem. This solution is based on disaggregation of functionality into two entities: PE-core and PE-edge. The former is intended to manage and maintain MPLS tunnels (VC and Tunnel Labels) and to distribute VPNs information to another PEs. The latter is intended for the MAC learning function and for service delimitation (when a client MAC frame arrives, it is capable of identifying the VPN to which it belongs, and the destination PE). With this architecture, we set aside the whole MPLS process complexity from the VPLS service operation into two different kinds of equipment, and since every PE-core will have several PE-edge, the whole scalability is substantially improved without increasing either the complexity nor the solution cost.

C. *LPE solution*

The solution addressed by GVPLS is based on the "Logical Provider Edge" (LPE) architecture (defined by Nortel Networks). This architecture allows reducing the complexity of the PE´s, separating their functionality in two entities and so allowing a cheaper solution, and increasing services scalability and clients aggregation.

Nortel Networks, in their Optical Ethernet (OE), distribute the PE functionality between two devices: PE-edge and PE-core. In their portfolio, PE-edge is represented in the OM1000 series, while for PE-core the OM8000 series devices are used.

PE-edge is the border between the client and the provider, aggregates clients, maintains the forwarding tables for each VPN service defined, signals to PE-core the addition of new members of a VPN and applies QoS policies if necessary.

PE-core distributes and maintains MPLS labels, exchange information about VPNs with other PE-core, encapsulates frames following Martini draft, maintains register information of VPNs clients and participates in routing processes.

After detecting the addition of a new client to the VPN,

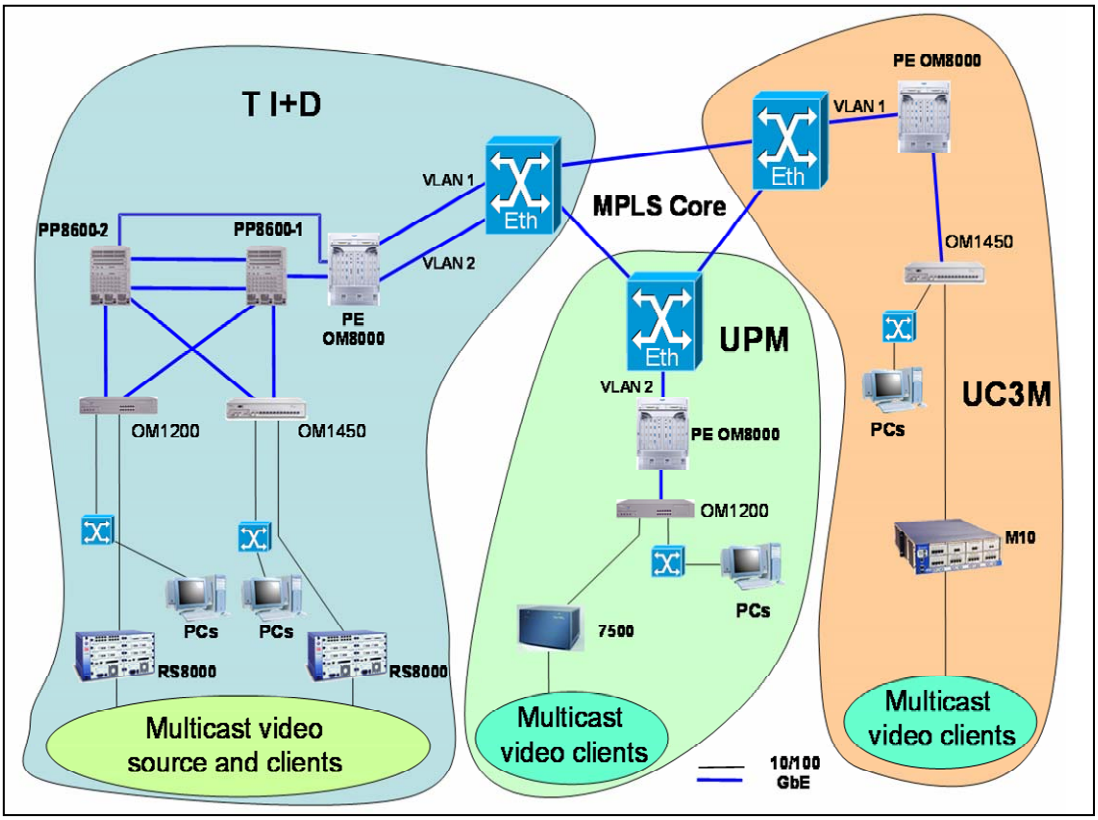

Figure 5. Network configuration installed in PREAMBULO in order to test LPE solution

the PE-edge, using a proprietary protocol called OE-AD (OE-Autodiscovery Protocol), informs to the PE-core of the new membership, and the PE-core propagates this information through the MPLS backbone to all the PE-core in the network. This leads to a very easy and quick provisioning.

PE-edge devices separate user traffic from provider traffic by defining UNI (User Network Interfaces) ports. These ports provide the connection to the VPN level 2 services configured in the network. Any instability produced by the client traffic does not affect the provider's network. This is achieved by adding a new layer 2 header (Service Provider Ethernet Header) and a new layer 3 header (OE/L2 Header).

Once the client traffic reaches the PE-core, the OE-L2 header is analyzed to know what VPN a packet belongs to, in order to send it through the appropriate MPLS tunnel. When the traffic reaches the remote PE-core, it is deencapsulated and encapsulated again using the Service Provider and OE/L2 headers until it reaches the remote PE-edge. The added headers are deencapsulated, and the plain frame is transmitted through the output UNI port.

Figure 5 shows the MPLS backbone used in PREAMBULO. To summarize, LPE highlights are:

- Simple end-point provisioning.
- UNI and encapsulation concepts: separation between client and provider traffic.
- Auto discovery of clients in the network, thanks to OE-AD.
- Scalable solution.

VI. CONCLUSIONS

This article has presented the optical network infrastructure to support IP over DWDM that is provided by the recently concluded project PREAMBULO, describing it both at the physical and at the logical level, and commenting the most important possibilities that were considered before choosing the definitive solution to connect the three participating entities.

This solution was based on the maintenance of level two connectivity with switches (disabling the Spanning Tree algorithm) and the usage of VLANs in order to directly split at this level the traffic passes through the optical network.

After presenting the most relevant experiences done in the project, the article is focusing in one of them: level 2 virtual private networks.

From this point of view, the main research lines regarding VPN have been reviewed, including some comments about level 3 VPNs, but mostly stressing level 2 solutions. These solutions are based on still emerging proposals (most of them under development) that are now beginning to appear in commercial equipments. Although it seems that nearly all of them depend on Martini tunnels, there are different suggestions about the establishment of the virtual circuits.

Finally, the article analyses the configuration that has been tested in PREAMBULO, including real solutions (commercial equipment provided by Nortel Networks) to support layer 2 VPN (based on a GVPLS/LPE implementation).

VII. ACKNOWLEDGMENTS

This article has been partially granted by the Spanish Science and Technology Ministry research and development program (period 2000-2003) through project PREAMBULO.

Layer 2 VPN trials were possible thanks to Nortel Network who provided both the necessary equipment and the required training.

VIII. REFERENCES

[1] *Prototype of high performance multiservice network, based on IPv4/IPv6 over wavelength division multiplexing* (TIC2000-0268-P4-C03-01). http://www.it.uc3m.es/preambulo

[2] J. Clerk Maxwell, *A Treatise on Electricity and Magnetism,* 3rd ed., vol. 2. Oxford: Clarendon, 1892, pp.68-73.

[3] ISABEL: group communication tool. http://isabel.dit.upm.es

[4] IPv6 Forum. http://www.ipv6forum.com

[5] Telecom I+D. http://www.telecom-id.com

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

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

[8] IETF Layer 3 Virtual Private Network (l3vpn). http://www.ietf.org/html.charters/l3vpn-charter.html

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

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

[11] RFC2547bis. BGP/MPLS IP VPNs . http://www.ietf.org/internet-drafts/draft-ietf-l3vpn-rfc2547bis-01.txt

[12] Encapsulation Methods for Transport of Ethernet Frames Over IP/MPLS Networks. http://www.ietf.org/internet-drafts/draft-ietf-pwe3-ethernet-encap-05.txt

[13] Pseudowire Setup and Maintenance using LDP. http://www.ietf.org/internet-drafts/draft-ietf-pwe3-control-protocol-05.txt

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

[15] IETF Layer 2 Virtual Private Network (l2vpn). http://www.ietf.org/html.charters/l2vpn-charter.html

[16] Virtual Private LAN Service. http://www.ietf.org/internet-drafts/draft-ietf-l2vpn-vpls-bgp-01.txt

[17] Virtual Private LAN Service over MPLS. http://www.ietf.org/internet-drafts/draft-ietf-l2vpn-vpls-ldp-02.txt

[18] GVPLS/LPE - Generalized VPLS Solution based on LPE Framework. http://www.ietf.org/internet-drafts/draft-radoaca-ppvpn-gvpls-04.txt