Interdomain VPLS and deployment experiences

Laura Serrano and Miguel Angel Sotos

RedIRIS Network Engineer, C/ Plaza Manuel Gómez Moreno s/n , Madrid, Spain
e-mail: {laura.serrano|miguel.sotos}@rediris.es

Abstract: The main objective of emergent standard Virtual Private LAN Service (VPLS) is the interconnection of users located in different geographic points as if they were in the same local area network. In this sense, the investigations and tests that have been done are mainly focused on point to point interconnection scenarios using Virtual Private Networks (VPNs), being few the tests that until the moment have been done in academic and research networks with multipoint scenarios and they have been done mainly in the same domain, but not between different domains. With this paper we describe the process to put in production VPLS service for testing purpose in interprovider environment, doing initial tests on a real scenario. With it, one hopes to verify its behaviour in a real production network, analyzing the benefits can be provided to the customers specially with respect to advanced applications and distributed computing, as it is the case of Grid applications.

Key words: Virtual Private LAN Service, Virtual Private Networks, Grid applications

1. INTRODUCTION

Nowadays, the use of *Mutiprotocol Label Switching* (MPLS) to provide layer 3 and even layer 2 VPNs is common, but the majority are point to point VPNs. One step forward is to provide multipoint connectivity using this kind of technology. To provide this layer 2 multipoint connectivity over an IP network the only choice is VPLS.

VLPS is one of the most innovative ways to provide *Multiprotocol Label Switching* (MPLS)/Ethernet VPNs allowing multiple sites to be connected in a single bridged domain over a provider managed network with MPLS support. All the clients using a VPLS instance, seems to be on the same *Local Area Network* (LAN), even if they are in different locations. VPLS uses Ethernet interfaces with the customer, which allows rapid and flexible service provisioning. The main devices involved in the configuration of VPLS are described in the Fig. 1.

The *Customer Edge* (CE) device represent the border equipment in the customer network and it used to be one router or switch directly connected to the provider network through the *Provider Edge* device (PE).

Due to the fact that we use MPLS to transport the *layer 2* (L2) frames over the provider network, the layer 2 technology used in the PE router is independent from the technology used in the rest of the core. However, this technology must be the same in both ends of the L2 VPN, so we must have in both ends Ethernet or Ethernet with vlantagging.

There are no requirements for CE device in order to map the logical connection to the remote site, they are configured as if they were connected to a single bridge.

The CE will be connected to the PE, located in provider premises. In the case of VPLS, it is assumed that the interface between CE and PE is Ethernet.
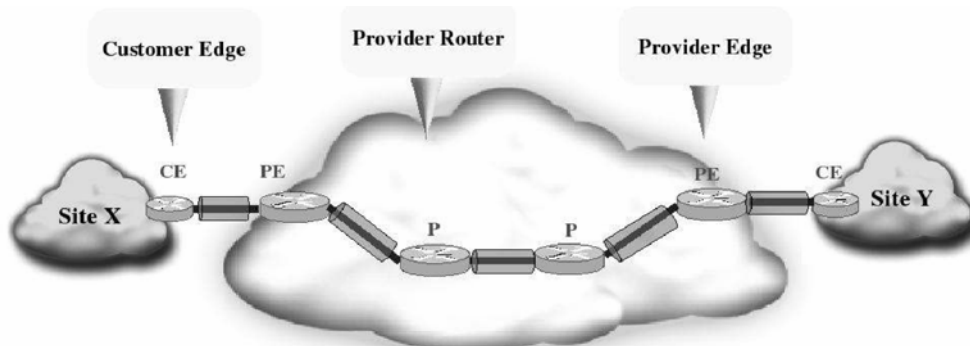

Fig. 1. VPLS connection. Devices involved

All the VPN intelligence is located in the PE. It is where the VPLS connection originates and terminates, and where all the necessary tunnels are set up to connect to all the others PEs.

Finally, the *Provider Router* (P) represent the devices in the core. They do not have any information related to the VPN and only transfer the labeled packets from one PE to another in a transparent way. For this reason, the network must support MPLS to switch the traffic based in the MPLS labels.

In the case where the customer service provider's sites are located in different *Autonomous Systems* (ASs), with different providers, the VPN will transit through several domains. This is what is called VPLS interdomain.

There are two different drafts to implement VPLS, *l2vpn-vpls-bg*p [1] and *ppvpn-vpls-ld*p [7]. The mainly different between them is that the first one uses *Border Gateway Protocol* (BGP) as signaling protocol (supported by Juniper vendor) while the other uses *Label Distributed Protocol* (LDP) to this purpose (supported by Cisco vendor).

Some of the benefits to use BGP as signaling protocol is that it allows for the autodiscovery of new sites, so if we use BGP, when we add new sites we will only need to configure the PE connected to the new site.

As BGP is an scalable protocol, we can use *route reflector* (RR) or *confederations* and of course, note it that BGP have been designed to advertise routes between different *Autonomous Systems* (AS).

Anyway, both drafts, have a common objective; to exchange VPN local routes generated inside our AS with the remote ASs. The MAC addresses and connection ports of the users in the local sites will be known by the remote users.

In this article we describe the use of *Multiprotocol Border Gateway Protocol* (MP-BGP) to distribute labeled VPN-IPv4 (*Internet Protocol version* 4) routes to one AS border router or to one RR, taking advantage of the benefits of using BGP as signaling protocol to reach this purpose.

VPLS is especially useful for users located in different *National Research and Education Networks* (NREN) or in the same NREN but in different regions which are not in the same AS (and in the most common cases, connected to different providers). Today, we can see sparse research groups accessing to sparse research resources. The collaboration of this researchers and their needs can be solved using the GEANT[1] network and VPLS possibilities.

Considering this, it is obvious that VPLS could be extremely useful for advanced applications and distributed computing over *Layer* 3 (L3) networks (inside and outside of the own domain) as it is the case of client-server applications for remote data storage or calculation or Grid applications.

But, in which way can VPLS be beneficial for Grid applications? Firstly, to remind that Grid systems are very sensitive to delay variations so routing changes can be dangerous for the system stability which are some of the most common problems in L3 networks. But moreover, VPLS allows to have multiple supercomputing resources connected between them acceded ones to others without any possible access from untrusted machines. So, with respect to security point of view, VPLS provides a great mechanism to minimize the risk of the Grid resources.

In this sense the content of the article is to speak about our own experiences in RedIRIS[2] with VPLS in intra and interdomain environment, explaining in detail the configuration steps, the most common problems we have found along this process and the benefits of this new technology can provide to the customer. For this purpose we are describing two cases of study.

2. CASES OF STUDY

The goal of the first case of study is to connect three customer sites located in different autonomous region in Spain but in the same AS, through one VPLS connection. In the Fig. 2, you can see a map with the topology of the RedIRIS backbone and the location of these three sites.

Assuming we have an *Interior Gateway Protocol* (IGP) operative between PE and P, we can summarize the configuration steps as following:

• Establish one MP-IBGP session between loopback addresses of the PE routes. This session is used to advertise the VPN route.

• Configure *Label Switching Paths* (LSPs) between all PE routers. For this purpose, we need MPLS support and one signaling protocol, which can be LDP or *ReSerVation Protocol* (RSVP). In case we use RSVP we will have to configure manually each LSP in the ingress router. In contrast, with LDP we will have LSP connectivity among all routers.

• And finally, we need one routing instance for each site we want to connect.

The Figure 3 shows a general diagram with all devices involved in this case of study and the protocols and sessions needed to establish one VPLS connection.

After configuring all the MP-BGP sessions needed, MPLS support one routing instance for each site, the result is that we have three final customer sites, which are physically connected through one L3 network, as if they were in the same LAN, as you can see in the Fig. 4.

The next case of study consists in connecting three customer sites through one VPLS, but in this case they are located in different ASs, concretely, two of them are in

---

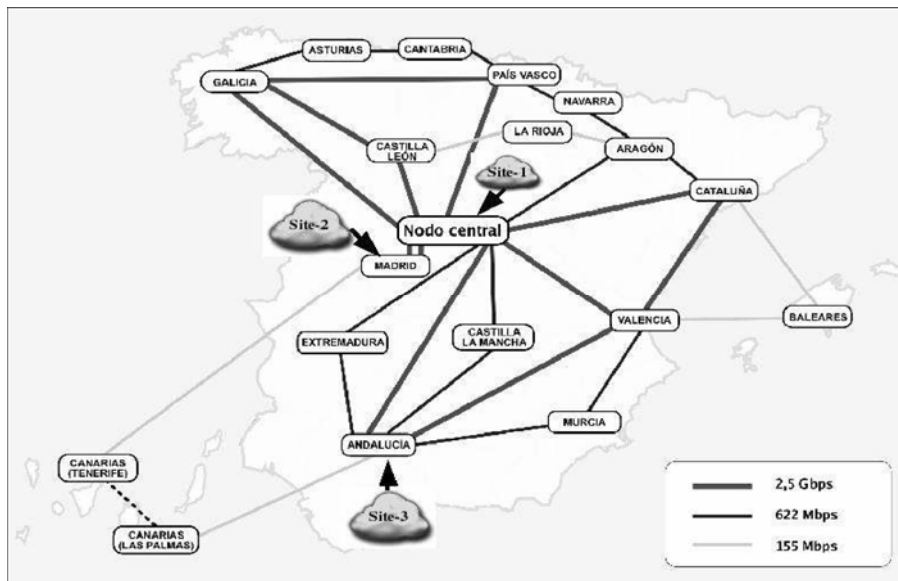[1] Paneuropean research and education network.

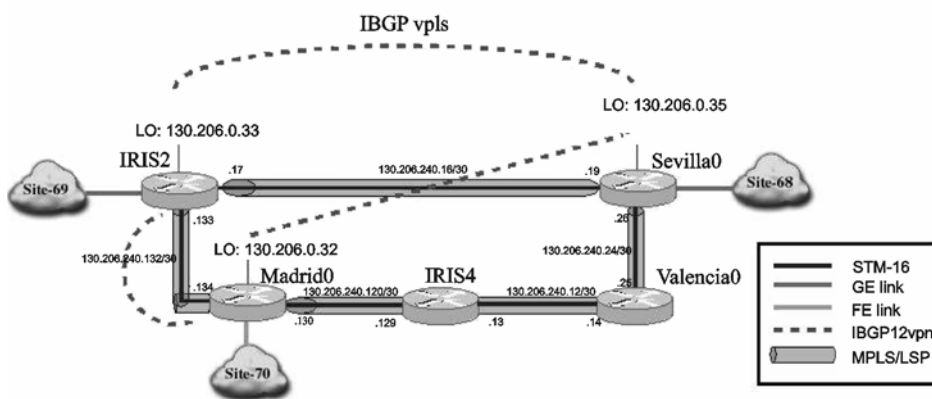Fig. 2. Intraprovider environment case of study

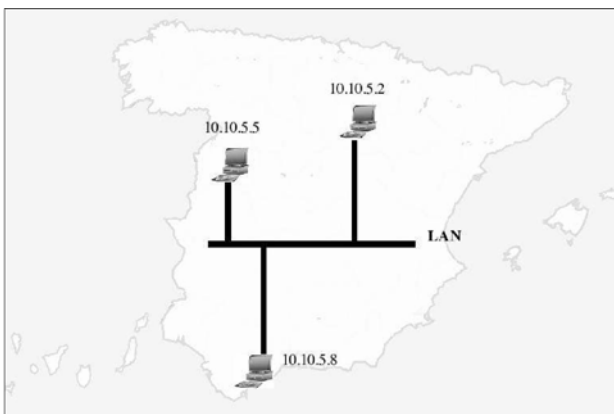Fig. 3. VPLS configuration for intraprovider environment
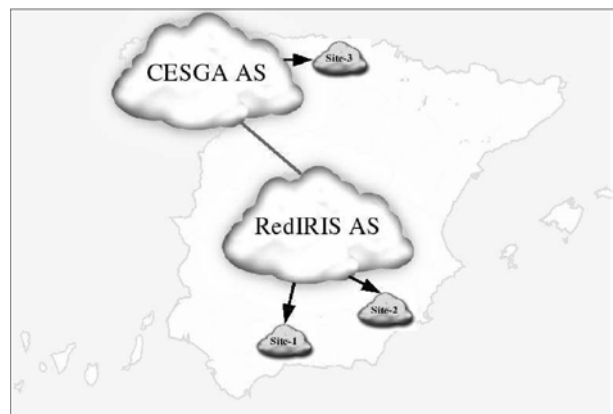

Fig. 4. Intraprovider environment behaviour
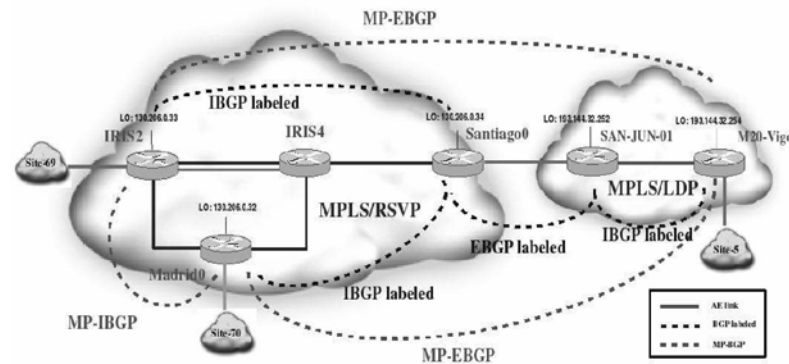

Fig. 5. Interprovider environment case of study

Fig. 6. VPLS configuration steps for interprovider environment

Fig. 7. Concrete configuration statements for PE router

RedIRIS AS, and the last one in CESGA[3] domain. So we have now a real interprovider environment.

The Fig. 5 have a diagram of the testing scenario defined to this case of study.

One first approach to get this result is described in the next general configuration steps (Fig. 6)[4] :

• Firstly, we need to advertise the VPN route from one PE to the others, so we will configure one MP-BGP session from each PE to the rest of PEs. Note that some of these sessions will be *external* and others *internal BGP sessions*.

Fig. 8. Interprovider environment result

• Moreover, it is needed to advertise the internal routes, that is the PE loopback addresses from one domain to the
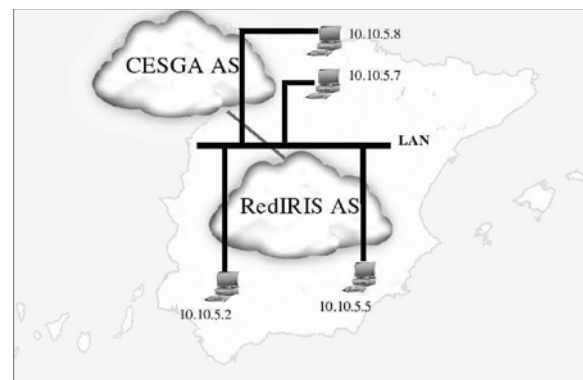
---

[3] CESGA is the Supercomputing Center of Galicia which manages the regional research network in Galicia providing supercomputing and net-working facilities to all the research centers in this autonomous region.

[4] We will explain how you can reduce the effort to expand VPLS too other domains with only one external MP-BGP using route reflectors.
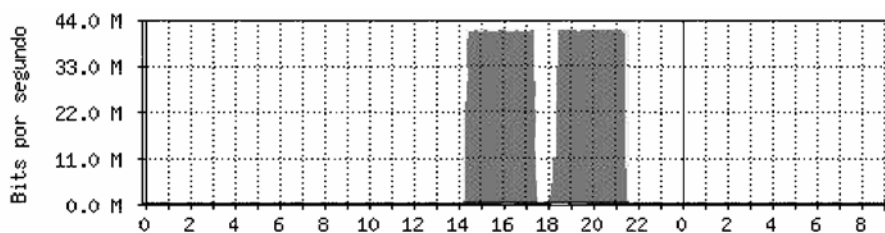
Fig. 9. Transfer of information between two hosts connected through VPLS

others. For this purpose, we could configure one normal BGP session between the AS border routers and extend the LSP from each PE to the others PEs through domains using LDP or RSVP, but there is another possible solution, this is, a new NLRI family called *labeled-unicast* that results in labeled route exchanges between providers *AS Border Routers* (ASBRs) which establishes MPLS LSPs between the providers's PE routers.

• The next steps allow us to associate the packets received for the border router with the LSP, connecting PE and ASBR and is assigned by RSVP or LDP, so we will configure LSPs between PEs and ASBR.

• And finally, we require one routing instance for each site.

In the Fig. 7 you can see the concrete configuration statements for one of the PE routers from the example described in Fig. 6 (IRIS2)[5].

When the multipoint to multipoint VPN and the BGP sessions (they are necessary to exchange the local client and PE routes to the remote AS[6]) are established, the behaviour of the final users will be as if they are in the same LAN and the transit networks from one user to others are completely transparent to them (see next Fig. 8).

From the provider pointof view, we would have one production provider network with IPv4/IPv6/IP multicast and VPLS traffic using the same infrastructure. With respect to customer point of view, he gets a trusted network, because only trusted hosts are include in the VPLS connection and moreover, he manages his network without provider control. And finally, for the final hosts, they have full-connectivity between them as before and they see to the other hosts as they were in the same LAN.

Figure 9 shows a graph with a real transfer of information between two final hosts connected through VPLS technology.

At this moment we would have a VPLS connection completely operative, but what does it happen if we want to add more sites? In the last case of study, we configured one MP-BGP session between each PE pairs, we had a full-mesh MP-BGP between PEs. So, following the same process to add one new site we should configure one new MP-BGP session from the new PE to the others.

At the beginning of the article we spoke about the benefits to use BGP with respect to scalability properties using RRs.

In case we use RRs in the final domains, we will only need to configure *one external* MP-EBGP session between RRs so, for adding a new site, we will only need to configure *one internal* MP-IBGP session inside our domain from the new PE to the RR.

3. GENERAL INTERDOMAIN CONFIGURATION

Summarizing, in an interdomain environment we have to consider 3 label stacking:
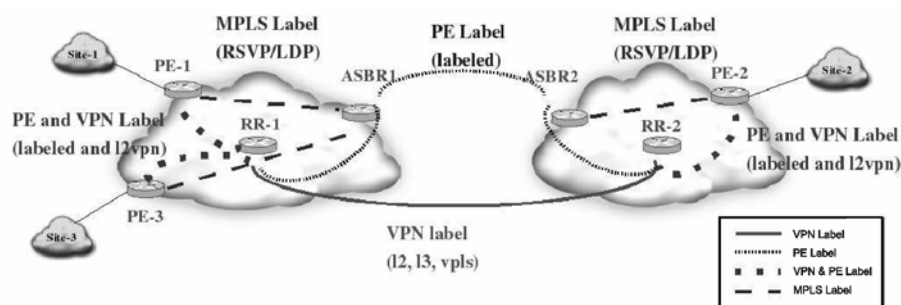

Fig. 10. Process to configure interdomain VPNs

---

[5] IRIS2 is a T-320 Juniper router with Junos 6.4R3.4

[6] This because one Multi-hop EBGP session will be used between the two remote PE (actually the two RR), and one between the ASBR will be used to exchange PE routes between the two AS.

• The first one, or bottom label, is the VRF (virtual route forwarding) label assigned using MP-BGP. This label does not change as the packet is forwarded.

For this label stacking we need one MP-BGP session between RRs for the appropriated family, depending on what kind of VPN we want to configure, layer 2 or layer 3.

• The middle label is assigned by the downstream ASBR and is used by the ASBR to associate the packet with the LSP leading to the next ASBR in the path.

For this label stacking we use the family `labeld--unicast` in the BGP sessions.

At this moment, we would have the general interdomain VPN configuration so, to add new sites we only need to extend the current label stacking from RRs to the new Pes.

• The top label associates the packet with the LSP connecting PE and ASBR and is assigned by RSVP or LDP.

In Fig. 10 you can see the complete process to configure an interdomain environment to support VPNs.

4. APPLICATIONS

With respect to the application of VPLS, it seem that there are some benefits it can provide to the customers but, in which way VPLS can help to the customers?

In the following lines you can see two concrete applications examples, highlighted the benefits provided by VPLS for each of them.

4.1. Grid applications

Let we analyze the most important problems of Grid application and how to solve them with VPLS.

• Grid uses the IP network

Considering we are working over an IP network and that Grid systems are very sensitive to delay variations, the routing itself can be a problem in case we have a complex topology (even routing changes can be dangerous for the stability).

• Security problems

Joining multiple computers to get a single machine, if each of these nodes can be reached from external links, the new system can be attacked from a lot of access points.

• Efficiency and performance

When you want to configure a set of computers as a single machine, you need a link between us as transparent as possible in order to achieve a stable systems.

• Layer 2 tools

To have a layer 2 infrastructure allow you to do a remote management and booting using tools such as bootp, pxe or wake on lan.

4.2. Opera Oberta project [12]

The opera project is an international project to high definition retransmission of opera by multicast. In this sense, there are several retransmission from Liceu in Bar-

celona (Spain) which are received from more than 50 institutions along the world.

The opera is retransmitted by Ipv4 and Ipv6 multicast.

• Security problems

Considering the private key to encrypt the opera retransmission are sending through IP network, the use of VPLS for this purpose can provide more security, because only trusted network are include in the VPLS connection.

• Avoid common network problems

It is well know from every people the complexity to debug and to solve multicast problems, especially with respect to the Ipv6. In this sense, having a VPLS infrastructure connected to the participant institutions, we will take advantage of it to use it to retransmit the opera avoided a lot of routing problems.

5. SUMMARY

As we mentioned at the beginning of the article, VPLS is one of the most innovative ways to provide MPLS/Ethernet VPNs, allowing to connect hosts located in different geographic points as if they were in the same LAN.

Along this pages, we have briefly reviewed the configuration steps needed to put in production this new technology in an intra and interdomain environment, explaining a real configuration example done over a production network, RedIRIS backbone.

All examples and configuration statements described in this document are related to a Juniper platform using BGP as signaling protocol, which is supported by this vendor. This fact allows us to take advantage of the scalability benefits provided by BGP, as it is the use of RRs.

With VPLS, we provide an exceptional environment for computing applications, such as grids, in terms of network resources, security, and network management.

References

[1] K. Kompella, et al, *Virtual Private LAN Service*, draft-ietf-l2vpn-vpls-bgp- 02, Work in Progress.

[2] W. Augustyn et al, *Architecture and Model for Virtual Private LAN Services (VPLS)*, draft-augustyn-vpls-arch, Work in Progress.

[3] W. Augustyn et al, *Requirements for Virtual Private LAN Services (VPLS)*, draft-ietf-ppvpn-vpls-requirements, Work in Progress.

[4] P. Knight et al, *Logical PE Auto-Discovery Mechanism*, draft-knight-l2vpn- lpe-ad, Work in Progress.

[5] K. Kompella et al, *Decoupled Virtual Private LAN Services draft-kompella- ppvpn-dtls*, draft-kompella-ppvpn-dtls, Work in Progress.

[6] K. Kompella et al, *Layer 2 VPNs Over Tunnels*, draft-kompella-ppvpn-l2vpn, Work in Progress.

[7] M. Lasserre, V. Kompella et al, *Virtual Private LAN Services over MPLS*, draft-ietf-l2vpn-vpls-ldp, Work in Progress.

[8] L. Martini et al, *Encapsulation Methods for Transport of Layer 2 Frames Over IP and MPLS Networks*, draft-martini-l2circuit-encap-mpls, Work in Progress.

[9] L. Martini et al, *Transport of Layer 2 Frames Over MPLS*, draft-martini-l2circuit- trans-mpls, Work in Progress.

[10] E. Rosen, Y. Rekhter, BGP/MPLS VPNs, RFC2547, Mars 1999.

[11] E. Rosen, Y. Rekhter Y. et. al., *BGP/MPLS IP VPNs*, draft-ietf-l3vpn-rfc2547bis, Work in Progress. *Interdomain VPLS and deployment experiences.*

[12] Opera Oberta Project. The project consists on regular Opera live transmissions from the Liceo Opera theaters in Barcelona. The Operas are transmitted using multicast to the Universities and Research Centers connected to RedIRIS. It's not an open transmission, the centers use special cards for deencription

Laura Serrano is a Network Engineer at the RedIRIS NOC, and her role is focused on research, management and testing of new technologies such as NTP, IPv6, Diffserv, QoS, MPLS, etc. Her current interests are all aspects of Multiprotocol Label Switching, especially related to its applications such as VPNs and QoS. In this sense, she is currently responsible of putting in production the L2 VPN service in the National Research Network in Spain. As member of the RedIRIS NOC, she has involved in several projects whose main goal is the performance and evaluation of new technologies. Laura has a Master of Science in computer Science at the Polythecnic University of Madrid (SPAIN).

Miguel Angel Sotos is currently working in the RedIRIS NOC, as Network Engineer, focused on IPv6, with active participation in TERENA/DANTE European project, to test new network technologies: IPv6, DiffServ, QoS and MPLS. Miguel Angel, collaborated during 1 year in the Languages and Systems University Department, in the Coral Project (ATM high speed networks migration and its coexistence, financed by CICYT – TEL96-1297), working with Ipv6. Before that, he was working for 1 year as an intern in IBM Spain, in the training department, working with token-ring technology. Miguel Angel, has a Master of Science in computer Science at the Polythecnic University of Madrid (SPAIN).