METHODS OF ADJUSTING MPLS NETWORK POLICIES

Răzvan RUGHINIŞ[1], Răzvan DEACONESCU[2]

Lucrarea de faţă discută strategii de ajustare a reţelelor bazate pe tehnologia MPLS la cerinţele utilizatorilor. Pornind de la capabilităţile tehnologiei MPLS şi de la evoluţiile recente din domeniu, este propusă o metodă de analiză a ajustărilor posibile în reţea, pe patru dimensiuni: securitate, recuperare din eroare, calitatea serviciilor şi integrarea reţelelor din organizaţii diferite, cu accent pe sistemele Grid. Pentru fiecare dimensiune sunt evaluate două alternative de ajustare: diferenţierea internă şi compensarea între dimensiuni.

This paper discusses adjustment strategies for MPLS networks, taking into account users demands. Recent developments in MPLS technology are used to propose a new method for analyzing network adjustments, on four dimensions: security, error recovery, Quality of Service and network integration - with a special focus on Grid systems. Two options are evaluated for each dimension: internal differentiation and inter-dimension compensation.

Keywords: Multiprotocol Label Switching MPLS, computer networks, security, error recovery, Quality of Service, Traffic Engineering, Grid system

1. Introduction

MPLS (MultiProtocol Label Switching) is an example of a successful project in reforming the information technology. We can safely say that its aims, to increase the fluidity of Internet traffic and to facilitate Traffic Engineering, have been reached. Its increased use is proof for this achievement. As the user community has amplified, so did the interest and resources allocated to improvements in this technology.

MPLS has been developed in a particular direction, under the influence of other technological innovations. The most relevant are the ASIC – Application Specific Integrated Circuits and the CAM – Content Addressable Memory. Both have improved the capacity of routers and switches to search rapidly in routing tables, and they have thus decreased the pressure towards using simplified procedures such as the label switched paths (LSP) that are central to MPLS. On the other hand, MPLS has been increasingly used in configuring level 2 and level

[1] Lecturer, Dept. of Automatic Control and Computer Science, University POLITEHNICA of Bucharest, Romania, razvan.rughinis@cs.pub.ro
[2] Assistant, Dept. of Automatic Control and Computer Science, University POLITEHNICA of Bucharest, Romania

3 virtual private networks (VPNs), as a result of an increased need of secure and high QoS networks. MPLS VPNs have witnessed the same process of an extended user base leading to increased research and improvements in configuration strategies and available options.

This paper discusses adjustment strategies for MPLS networks on four dimensions: security, error recovery, Quality of Service and network integration with a special focus on grid systems. Recent developments in MPLS technology are also taken into account by analyzing possibilities of internal differentiation and inter-dimension compensation for each of the four dimensions.

2. Security strategies in MPLS VPN

A client who buys Internet services from a provider has the implicit strategy of mistrusting the received packets and providing for its own security by measures such as firewalls. By contrast, a client who buys VPN services has an implicit strategy of trusting the packets received from the provider, without additional filters. The MPLS VPN traffic is separated from Internet traffic, even if the IP provides both types of services. The level 3 MPLS VPN achieves traffic isolation by using distinct VRF (Virtual Route Forwarding) tables at the level of the PE (Provider Edge) routers. This isolation guarantees that the routes of a VPN will not be accessible to a system which does not belong to that particular VPN. Of course, it is essential that the PE routers be secured, including measures against social engineering attacks. If an intruder, either local or from the Internet, manages to gain access to such an equipment, he will also be able to access all routes from all VPNs which are using the respective systems, and thus to infiltrate in any of them.

2.1 Preventing a DoS attack

Traffic isolation still leaves open the possibility of a DoS (Denial of Service) attack on a PE router that simultaneously transports Internet and VPN traffic. In this situation the unavailability of the service also affects the VPN. Such a risk can be decreased by the strategy of homogenous risk level: each PE router would only contain VRF tables for networks with a similar security level. For example, one can differentiate between VRF tables for Internet traffic, with a security level of 0, the VRF tables for VPNs with level of security 1 and VRF tables for critical mission traffic with security level 2. Since this strategy raises service costs, it should be analyzed whether this increased cost is justified by the gain in security levels.

Fig. 1 illustrates three strategies available to the ISP for configuring the MPLS cloud, according to the proximity of Internet traffic and the VPN traffic.

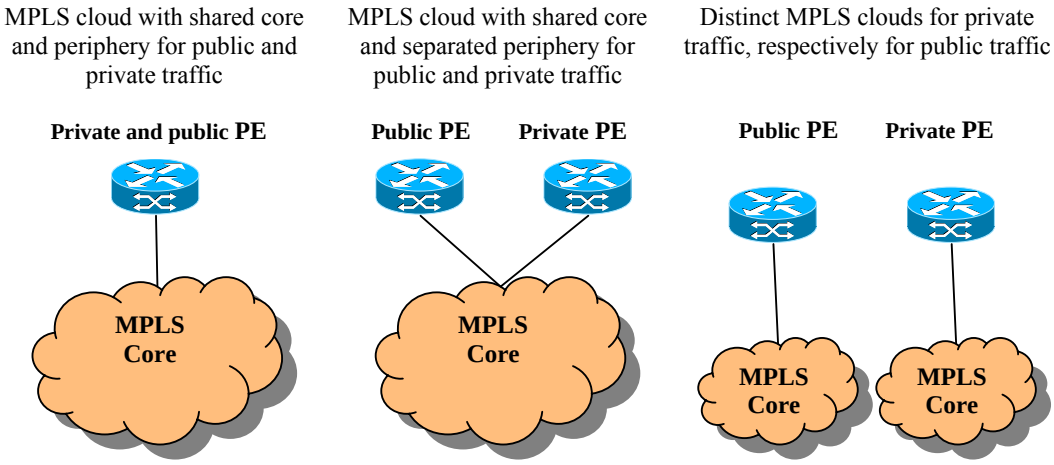

Fig. 1. Security strategies for MPLS VPN

2.2 Encryption by GET VPN

MPLS-VPN networks are based on traffic isolation and they do not include any form of encryption. Therefore, clients who require traffic encryption for various reasons – such as legal requirements of mistrust of ISP security policies – must make use of additional protocols.

One possible solution is the use of IPSec in MPLS VPN, which allows for traffic encryption and direct authentication of CE (Customer Edge) routers. IPSec may be used also in between the CE routers, in order to secure the VPN, or in between a CE and a PE router, to secure remote access to the network. The main problems raised by IPSec concern system scalability. The requirement of providing point-to-point IPSec tunnels led to a fast increase in the number of necessary connections, as the network size increased (N2 connections for N locations). It is possible that traffic be encrypted only in between CE and PE routers and not in between PE routers, but this imposes an overhead to PE routers which must decrypt and respectively encrypt traffic at the egress and ingress in the MPLS cloud.

Scalability problems have been gradually reduced from year to year, as more flexible options have emerged. The GET (Group Encrypted Transport) VPN technology, launched at the end of 2006, offers significantly increased scalability for IPSec. Unlike the tunnel-mode IPSec, GET keeps the original IP header of the packet (which is actually copied in a new header). This allows for the implementation of QoS policies and IP multicast in the entire network. Security

risks are reduced by creating a group of routers among which trust relationships are founded, by using the protocol GDOI – Group Domain of Interpretation, based on RFC 3547 [1]. It is also recommended that GET be used within a MPLS VPN.

3. Mechanisms for error recovery in MPLS

3.1 Fast-ReRoute

The MPLS option of Fast-ReRoute (FRR) aims to reduce significantly the time of error recovery by initiating a temporary back-up path by the node immediately upstream to the one that detects the error. Its implementation by vendors such as Cisco, Riverstone or Atrica has led to performances similar to SONET, in packet forwarding networks. The FRR option may or may not be activated for a given LSP, depending on the traffic engineering policy.

When a LSP is interrupted, the LSR that first detects this event will signal this information to all LSRs upstream. The LSR that had established the path will redirect traffic on the backup path. This process may take too long for real time applications such as VoIP, for example. In order to reduce latency, the neighbor of the LSR that has detected the error will redirect traffic on a temporary, pre-established backup path, until the ingress LSR redirects traffic on the secondary LSP.

3.2 Bidirectional Forwarding Detection

The BFD (Bidirectional Forwarding Detection) protocol has started to be standardized in 2006 by a dedicated IETF workgroup. Its purpose is to allow for rapid error detection in links such as virtual circuits, traffic tunnels or label switched paths. The protocol establishes a monitoring session between the two ends of the connection, communicating information on the status of the respective link. If two systems are connected by multiple links, each will be monitored separately.

4. QoS in MPLS VPN

QoS policies aim to guarantee a certain level of resources in a network for a critical application, irrespective of variations in network load levels. The main variables used in QoS policies are: bandwidth, latency, jitter (variations of latency among packets) and packet loss.

In IP networks quality of service is standardized by DiffServ, which offers the possibility of classifying packets in multiple classes. Packets are then labeled accordingly. Routers perform different actions of structuring traffic according to

QoS indications, such as leveling the rhythm of sending packets in the network, or rejecting packets in excess of a given threshold for a QoS category.

Most networks which implement DiffServ mechanisms acknowledge three types of markings:

1. Implicit marking, which signals best-effort traffic;

2. EF – Expedited Forwarding, used for guaranteed traffic such as audio or video. This marking implies reduced latency, jitter and packet loss. The packets marked as EF have absolute priority compared to other packets, within the limits imposed by the ISP. The usual practice is to allow 10% to 30% of total link capacity for EF packets and to reject the ones in excess of this quota.

3. AF – Assured Forwarding, used for guaranteeing packet delivery as long as these do not exceed the quota established by the QoS policy. Packets in excess are subjected to a certain probability of rejection. This mechanism differentiates four classes of traffic and three levels of rejection probability, leading to a total of twelve traffic categories.

These three types of markings create a packet classification with 14 classes, each one defining a particular PHB – Per-Hop Behavior of a network node in relation to a packet. An additional class, entitled CS – Class Selector, is introduced to ensure retrospective compatibility with the use of IP precedence field.

3.1 E-LSPs and L-LSPs

MPLS allows for PHB classification of packets. This information is included in the three EXP bits of the MPLS shim header. Therefore, it is possible to mark at most eight types of PHB, or even less in case that some values are reserved. Given the fact that in most cases only three or four PHB are used, this restriction may not be an impediment. Still, for situations that require a finer granularity of classification, new methods of signaling Qos have been recently put into place. MPLS allows now for two types of markings: the Exp-LSP (E-LSP) and the Label inferred LSP (L-LSP), according to the field that included the classification information (see Table 1).

In order to generate an E-LSP the ingress router to the MPLS cloud recodes the DiffServ information in the EXP bits of the MPLS shim header. At every hop of the E-LSP packets are forwarded according to the information included in the EXP bits.

An L-LSP included information about traffic class (that is, packet priority) and its probability of rejection (in case it exceeds the quota) both in the EXP bits and in the MPLS label (the first 20 bits of the MPLS shim header). The EXP bits are used to indicate the rejection probability, while the label is used to indicate class. Therefore, the type of traffic classification and the type of association between class and labels needs to be signaled when LSPs are established.

An L-LSP can support traffic either for a single PHB, or for multiple PHBs which require the same type of traffic priority, but have different probabilities of rejection. Each combination of FEC and traffic class requires though a distinct LSP. This may lead to overcharging network resources, especially for a complex traffic classification.

Table 1

Comparative analysis of E-LSP and L-LSP

E-LSP	L-LSP
EXP bits define PHB	PHB is defined by MPLS label and EXP bits
A network based exclusively on E-LSPs may accommodate a maximum of 8 PHB.	L-LSP enables as many PHB as needed. A network can include both E-LSP and L-LSP simultaneously.
Does not require signaling	PHB information needs to be signaled at the moment of LSP computation
MPLS labels are used only to indicate path	Labels indicate combinations of path and priority. More labels are required.
A LSP can transport a maximum of 8 PHB	A LSP can transport either a single PHB, or several PHBs that only differ in their probabilities of rejection in case of overrepresentation

MPLS allows the combination of L-LSPs with FRR (Fast Re-Route) error recovery mechanism. Therefore, packets labeled as Expedited Forwarding in DiffServ may be labeled and forwarded on FRR-enabled paths.

3.2 MPLS DiffServ aware Traffic Engineering

MPLS facilitates traffic engineering, since it is not limited by classic IP routing which takes place at every hop on the basis of the destination address – as discussed in detail in [3]. The router that computes a LSP can take into account multiple criteria and information. For example, each LSP may have an associated priority value (on 8 levels) for its establishment, and also for its maintenance. This priority value indicates to what extent the path can access resources which are requested by other LSPs. MPLS Traffic Engineering also takes into account the bandwidth required by a given LSP, the attributes of the links which the LSP can traverse, or the maximum number of hops. This information is processed by a modified version of the SPF (Shortest Path First) algorithm, called CSPF (Constrained SPF), which eliminates out of the set of possible paths the ones that do not correspond to given constraints. The main limit of MPLS TE in its initial version was that it computed LSPs without taking into account QoS information.

MPLS DiffServ-aware Traffic Engineering (MPLS DS-TE) is a recent mechanism which enables privileged resource reservation for classes of

guaranteed traffic. The RFC 3564 introduces the concept of Class Type – CT, defined as the set of traffic trunks traversing a given link and subject to common bandwidth constraints [4]. A traffic trunk will be defined by a same class type for all links that it traverses. IETF stipulates a maximum number of 8 class types. CSPF has been modified to take into account the bandwidth allocated to each traffic type, for each level of priority. There are 64 possible combinations of CT and priority level; still, the IETF has decided to limit the total number of allowed combinations to 8. These combinations are called TE classes. The 8 TE classes are selected among the 64 possible TE classes via configuration options. The classic MPLS TE is thus equivalent with implementing MPLS TE with 8 TE classes obtained from a single class type and 8 priority levels.

MPLS DS-TE is usually based on limiting the weight of guaranteed traffic within a link's bandwidth. It therefore becomes possible to have different policies of overbooking for normal traffic and for guaranteed traffic. Guaranteed traffic may even be under-booked, thus providing a high level of QoS throughout the LSP even though best-effort traffic is overbooked [5].

5. Network integration: MPLS and Grid systems

Network integration is mostly required when several organizations need to cooperate in closely knitted projects. We shall discuss, as an example of such a project, Grid systems.

Grid systems offer the capacity of parallel processing of massive volumes of data by interconnecting computers on conventional network interfaces. A Grid is a virtualization of the resources of participant computers, which are represented as a unique system of data storage and processing.

There are three essential features of grid systems [6]: computers' resources are under decentralized administration, public standards are used, QoS is high. Grid systems are used either as commercial services which organizations may purchase when they temporarily need fast processing of a large volume of data (utility computing), or, alternatively, are used by organizations that appeal to volunteers for public interest missions (volunteer computing). Grid systems may also be classified according to their focus on processing power (computing grids) or aggregating resources in different locations in order to create a complex data bank (data grids).

The main challenges confronting grids are especially security issues – as exemplified by the collapse of the commercial Grid of Sun Microsystens (Sun Grid Compute Utility) in March 2006, following a Distributed Denial of Service attack [7]. It is also possible that outputs provided by a given system to be negatively affected by malicious internal actors. In order to avoid such situations Grid solutions usually include mechanisms of random allocation and redundancy

in task completion, checking various outputs one against another. Grid outputs are virtualized as a unique resource by means of a software stack called Grid Middleware.

A grid is associated with a virtual organization whose aim is to maintain and to use the system. Security risks of a grid system are amplified by the diversity of participants. The more organizations are involved in the network, the higher is the complexity of harmonization policies required to secure the system and the higher the risk of an inside attack.

Grid resources which are typically accessible to utilities in the Grid Middleware fall within the 7th level – such as processor power, storage capacity or data as such. It is essential that Grid functioning be independent of the complexity of network processes at inferior levels. Some network specific resources may be virtualized such as to become available to Grid utilities – such as bandwidth or QoS requirements. Still, processes such as protocol configuration or routing and forwarding tables configurations, as well as the complex network topology are beyond reach. The rationale for integrating in the Grid some abstract network-level resources is to improve the adaptation of its functions, such as task scheduling, to network properties. It would also enable a Grid application to request directly certain services in the network – such as QoS, bandwidth, firewall configuration or MPLS-VPN services.

5.1 Grid systems and VPNs

Private virtual networks have emerged as the solution of choice to ensure security in grid systems, especially in utility computing systems. Volunteer computing grids most often use the „pull" model in which an application installed on participant computers contacts periodically the project servers and requires task allocation, reporting its results. The initiative is thus pushed towards participants because many computers are protected by firewalls which do not allow for connections from outside. Utility computing systems may achieve superior efficiency by coordinating security policies and integrating into a VPN. This is efficient because security techniques based on packet filtering introduce latency and restrict possible communication situations. A VPN is the optimal solution for Grids that encourage involvement of new organizations and a dynamic negotiation of security requirements. Such VPN may be conFig.d with MPLS either as level 2 or as level 3 VPNs.

A level 2 VPN is defined by the fact that the ISP does not receive level 3 routing information from the client; routing responsibility resides solely with the client. The ISP offers level 2 services by means of virtual circuits ("pseudowires") established between the client's locations. On the contrary, in a level 3 MPLS VPN the provider is the one which receives and transmits customer's routing

information. A level 2 MPLS VPN allows the use of MPLS infrastructure to produce heterogeneous services – such as IP traffic, superposed level 2 VPNs (IPSec based, for example), level 3 VPNs, MPLS traffic engineering or DiffServ QoS policies. A level 2 MPLS VPN is significantly more scalable than other level 2 VPNs, given that adding a new client only requires the configuration of the adjacent PE router, without requiring the configuration of the client's edge routers [2].

Level 3 MPLS VPNs are more efficient for grid systems which are managed by a core organization (such as in utility computing). The main benefit which translates directly to a grid system is scalability, by isolation information on a VPN routes from the vast majority of provider servers which participate in traffic forwarding. MPLS VPNs allow for the use of private (non-routable) IP addresses by participant organizations, and thus they facilitate connections from organizations with different addressing systems. MPLS is also useful to establish policies of QoS provision in the VPNs.

Grid systems that are heterogeneous and dynamic, such as those of research projects with mixed participation of academic and commercial organizations, benefit from the use of level 2 MPLS VPNs. These allow for the transportation of level 2 protocols over MPLS tunnels, and they do not require any provider routers to administrate VRF tables with the routes of each network. Provider's involvement is thus less complex.

5.2 Grid systems and VPLS

The development of MPLS VPN has led to the development of a new type of level 2 service: the VPLS – Virtual Private LAN Service. The main advantage of VPLS is that it allows multipoint-to-multipoint links within geographically dispersed networks, unlike the level 2 MPLS VPNs which only allow point-to-point tunnels. Each PE thus functions as an Ethernet bridge in its relation to CE equipments. This functionality requires considerable memory resources dedicated to storing MAC addresses and LSP routing information. A possible solution for this necessity is using a router as CE equipment, in order to hide MAC addresses of the respective location behind the MAC address of the router. An alternative solution is to use CAM – Content Addressable Memory in the PE equipments in order to optimize the routing process.

The comparative advantages of VPLS technology for Grid systems are discussed in [8]. Given their sensitivity to delay variations in packets, a complex topology introduces risks because of possible routing changes. It is also the case that VPLS networks decrease security risks associated with external access to system nodes. Last but not least, VPLS facilitates multicast transmissions.

6. Methods for adjustment in MPLS networks

The last years have witnessed significant optimizations of MPLS technology. It is difficult to anticipate any long term evolution, given the radical changes that periodically restructure the IT domain. In the short term we can expect a considerable development of the MPLS user community and MPLS based technologies, especially in the context of increased use of VPNs and requirements for QoS based traffic engineering.

Any network must be adjusted to its functionality and resources. We can propose, based on the above analyses a method of adjusting network features to internal and external requirements, on four dimensions: security, error recovery, QoS and network integration (see Fig. 2). We can distinguish between two strategies of adjustment for each main dimension of network design: internal differentiation, and inter-dimension compensation. Internal differentiation consists in differentiated allocation of a given volume of resources among different traffic types, by balancing needs against one another. Compensation consists of an analysis of the impact of performance in one dimension on service cost, on one hand, and performance in the other dimensions, on the other hand.

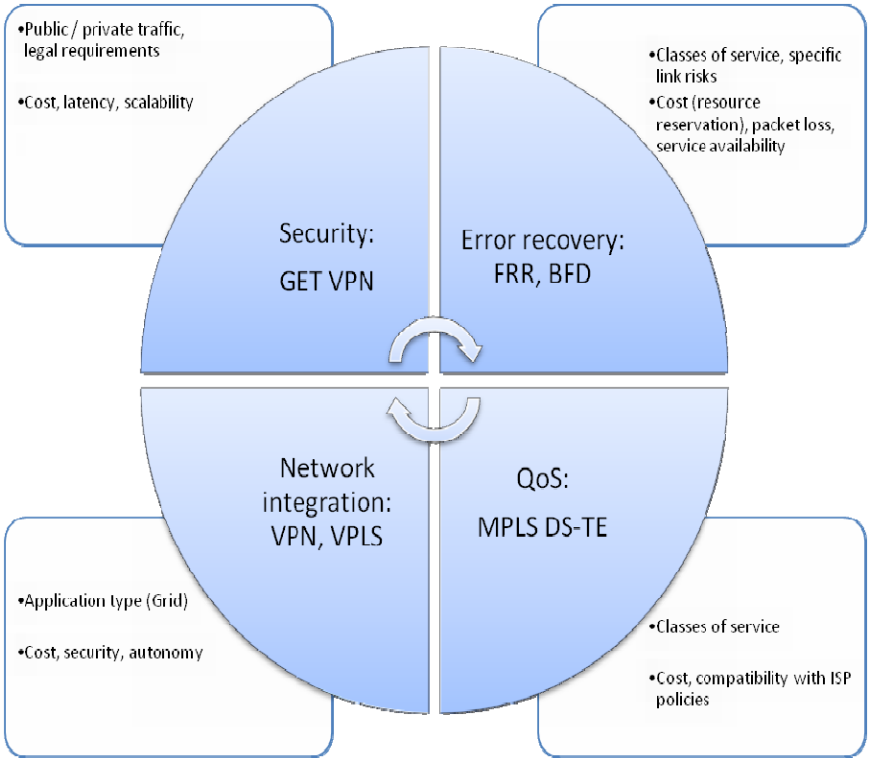

Fig. 2. A method for adjusting MPLS network policies

For example, security requirements may be differentiated according to the traffic type (public / private, with or without special legal requirements). At the same time, any improvement in security policies must take into account its consequences on service cost, latency and network scalability.

Error recovery may also take into account classes of service, but also specific risks associated with given links traversed by different types of traffic. At the same time, a global improvement in error recovery mechanisms will impact cost of service, rates of packet loss and overall service availability.

Network integration across organizations may be more or less necessary according to the specific project in which partners are involved. We have discussed, as an example, different requirements of utility and volunteer grid systems. An increase in network integration must be balanced against security requirements and autonomy of network administration.

Quality of Service relies, by definition, on a differentiation among categories of traffic, including usually two main variables: priority and probability of rejection. The more complex the QoS policy is, the more it needs to be coordinated with other ISP's QoS policies. A global upgrade of QoS levels must take into account influences on service costs and quotas allocated to different types of traffic by ISPs.

7. Conclusions

Network resources increasingly become essential parts of any project. Their efficient management requires adaptation to particular organizational contexts and project characteristics. We have proposed an analytical method that differentiated four dimensions of adjustment – security, error recovery, network integration and Quality of Service, and two alternative options on each dimension: internal differentiation and inter-dimension compensation. Network engineers must have a comprehensive view of the consequences of a specific policy, and to evaluate them in relation to organizational criteria. Our adjustment method proposes a structure for this evaluation process, which is essential in deciding the optimal policy in a given situation. The method is based on the capabilities of the MPLS technologies and its potential of evolution in the near future.

R E F E R E N C E S

[1] *M. Baugher et. al*, The Group Domain of Interpretation – RFC 3547, 2003

[2] *F. Palmieri*, "Introducing Virtual Private Overlay Network services in large scale Grid infrastructures", in Journal of Computers vol. 2 nr. 2, pp. 61-72, 2007

[3] *E. Osborne, A. Simha*, Traffic Engineering with MPLS, Cisco Press, 2002

[4] *F. Le Faucheur et. al.*, Requirements for Support of Differentiated Services-aware MPLS Traffic Engineering - RFC 3564, 2003

[5] *J. Evans, C. Filsfils*, Deploying IP and MPLS QoS for Multiservice Networks: Theory and Practice, Morgan Kaufmann, 2007
[6] *I. Foster*, What is the Grid? A Three-Point Checklist, available on December 20, 2007 at URL http://www-fp.mcs.anl.gov/~foster/Articles/WhatIsTheGrid.pdf, 2002
[7] *E. X. DeJesus*, "Grid computing and security uncertainties", in Search Security, available on December 20 2007 at URL http://searchsecurity.techtarget.com, March 30th 2006
[8] *L. Serrano, A. M. Sotos*, "Interdomain VPLS and deployment experiences", in Computational Methods in Science and Technology, vol. 11, no. 2, pp. 153-159, 2005.