Problems in Configuration of VPNs over MPLS Network

Veneta Aleksieva[1]

Abstract – **Recent years many internet service providers offer not only access to the Internet services, QoS, traffic engineering, but also Intranet VPNs, Extranet VPNs, VPNs with network management. Some problems exist during the creation, monitoring and usage of VPNs over MPLS. In this paper are presented these problems and are suggested some decisions, which are able to overcome them.**

Keywords – **MPLS, VPN, LSP, backbone networks**

I. Introduction

Recent years there is a very active research in the field of multiprotocol label switching (MPLS), and more and more networks are supporting MPLS [1]. One of the most notable applications of MPLS is traffic engineering (TE) [2], since label switching paths (LSPs) can be considered as virtual traffic trunks that carry flow aggregates generated by packet classification.

VPN solutions support remote access and private data communications over public networks as a cheaper alternative to leased lines. VPN clients communicate with VPN servers utilizing a number of specialized protocols as PPTP, L2TP etc. Building of VPNs in an enterprise network in the WAN transport uses Frame Relay, ATM or any other layer-2 transport technology, including MPLS [3]. There are two different methods to construct VPNs across IP backbone, i.e., CPE (Custom Premises Equipment) based and network based. Most of the current VPN implementations are based on CPE equipment.

IP/MPLS VPNs are compelling for many reasons. It defines IP VPNs's meaning that the VPN service accepts IP datagrams from customer sites and delivers them also as IP datagrams to other customer's sites. The connection between a customer's site and the core network, also referred to as an attachment circuit, may be a Layer 2 service such as ATM, SDH, Ethernet, but the VPN service handles only IP datagrams transmitted over this link[4,6]. One example is presented in Figure 1. (In this example: CE means customer edge, PE means provider edge, such as Ingress Label Switching router(LSR) or Egress LSR, which belong to the provider, P means providers' LSR.) For enterprises, they enable right-sourcing of WAN services and yield generous operational cost savings. For service providers, they offer a higher level of service to customers and lower costs for service deployment. When used with MPLS, the VPN feature allows several sites to interconnect transparently through a service provider's network. One service provider network can support several different IP VPNs. Each of these appears to its users as a private network, separate from all other networks. Within a VPN, each site can send IP packets to any other site in the same VPN.

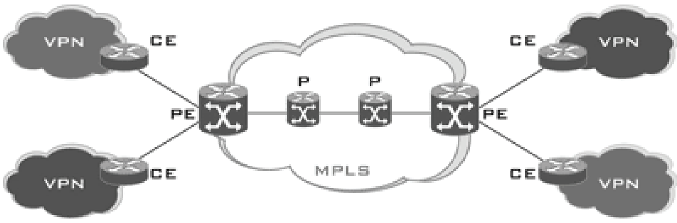

Fig. 1. Example of MPLS VPNs

In this paper are presented problems which related to MPLS VPNs and some suggestions for its overcoming. In particular, it is presented architecture of MPLS VPNs with QoS routing capability as well as some methods for operating QoS routing in MPLS VPNs.

II. Advantages and Disadvantages of MPLS VPNs

When uses leased lines, each company will be responsible for the security of the information and network in a Point to Point connection. Here, in MPLS VPNs, security has the following characteristics:

- **Confidentiality, integrity, availability**— Security can usually be defined using these three properties. In the MPLS context, every VPN customer will have slightly different requirements for these parameters, but generally, customers will expect their data to be confidential, such that they are not accessible outside their VPN. They will expect the data not to change in transit, and they will expect the MPLS VPN service overall to be available to them.
- **Defense in depth**—It is good practice to add several layers of defense around everything that needs to be protected. This design principle is also important in MPLS networks.
- **Secure failure**—When the primary method fails, the backup method also needs to be secured appropriately. This is usually done through out-of-band access, mostly over the telephone network. It is important that this backup mode be as secure as the principal access mode.

MPLS VPNs are advantageous because they allow computers and devices to communicate with each other across large distances without using cables or wireless devices. MPLS VPNs cost less to maintain than other types of networks and can be created at any time by any computer in the world. Likewise, MPLS VPNs only have to look at the top label in a label stack in order to forward a data packet to another device. This allows MPLS VPNs to be much faster and more efficient than other types of networks.

[1] Veneta P. Aleksieva is with the Department of Computer Science and Engineering, Technical University of Varna, str."Studentska "1, 9010 Varna, Bulgaria, e-mail: ven7066@abv.bg

Although MPLS VPNs can be advantageous, they also have several disadvantages. The most notable disadvantage of an MPLS VPN is that it does not provide any security for the data packets that are sent out. This is because MPLS VPNs depend on each device within the network to forward the data packet to the next device. Therefore, once a data packet has been sent out, any device in the network could potentially intercept the data packet and view its contents. However, encryption protocols are available that they could be used in conjunction with an MPLS VPN.

Moreover, the benefits of the MPLS VPN Service for the customer are:

- Simple network implementation
- Easy to configure and manage
- QoS, CoS and better Traffic Engineering
- Easy network expansion at customer premises
- Easy introduction of new services as Multicasting, VoIP or hosting over the same link
- Security is the responsibility of MPLS Network
- Network is very reliable due to built in redundancy
- Flexible reconfiguration -instantaneous addition and deletion possible
- Less cost per link than leased lines
- Offer different level of service and protect specific part of traffic
- Traffic engineering gives maximal effectiveness of bandwidth usage
- Existing equipment gives possibility to use human resources with less qualification and less salary
- Faster then Layer 2 VPNs
- Cheaper than leased lines
- A single point of contact with access to a large number of licensed and certified carriers and local access providers
- A single point of contact for network performance and capacity management
- A network with enhanced flexibility and scalability which enables the customer to let its network grow with the growth of its business.

MPLS-VPNs are divided into:

- access channel,
- pick throughput ,
- quantity of sent packets,
- CoS,
- size of routing table,
- members of VPN,
- protocol between customer router and ingress label switching router (LSR).

In each of them each PE router maintains a number of separate forwarding tables. One of the forwarding tables is the "default forwarding table". The others are "VPN Routing and Forwarding tables", or "VRFs". Management of MPLS is based on database LIB (Label Information Base). Ingress LSR puts label to the packet when packet input in MPLS network, but Egress LSR deletes label from IP packet when packet leaves the MPLS cloud. Method for rerouting and making decisions with IP packets with/without labels is presented in Figure 2.

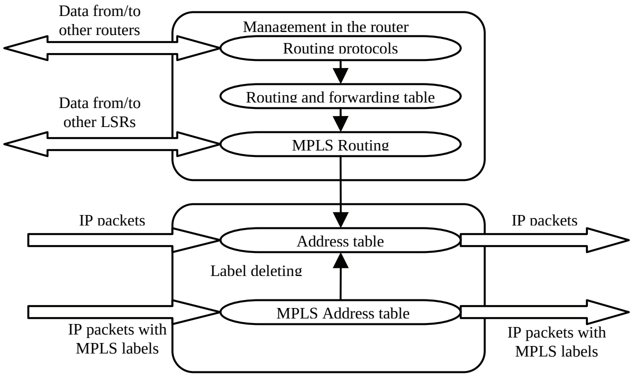

Fig. 2. Example of PE router’s functions in MPLS VPNs

To be possible to monitor how work MPLS network, to predict some problems and manage them, there exist two main methods for managing LSRs:

- **with global routing table** (in Fig.3)- Loopback address of P and PE routers are inside in this table, but address of management workstation is inside in the VRF table. The connection between backbone MPLS network and this management workstation is with global static route in VRF table to the address of MPLS network and with global static route in global routing table to the address of management workstation.

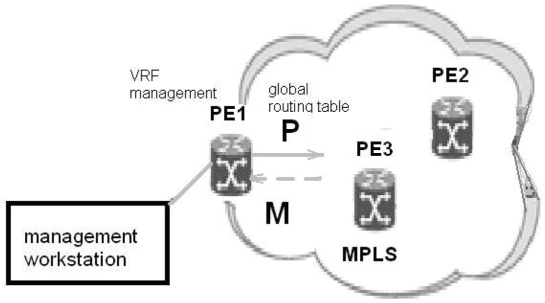

Fig. 3. Management of MPLS core with global routing table

- **with routing/forwarding table** (in Fig. 4) - This method is more simple. Here management network is directly connected to the interface, which is defined from global routing table, without association to VRF table.

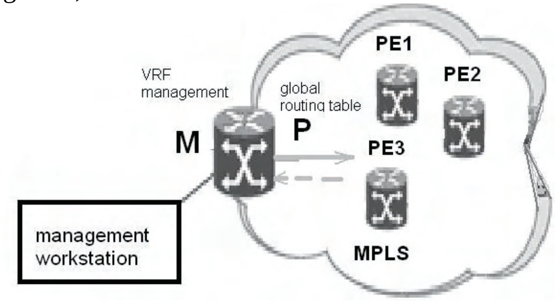

Fig. 4. Management of MPLS core with VRF table

III. ARCHITECTURE OF HUB AND SPOKE MODEL VPN

VPN decisions must differentiate different type of traffic quickly, to be possible ISP to group different customers and services. It is easy to make this with MPLS, because MPLS divides the traffic, protects it without encryption and tunneling, offers scalable VPN service. All sites send traffic to the hub, which must know all sites for this VPN. If ISP must work with 100 sites, each of them with hub and spoke and 100 VPNs, logical topology will be created carefully and each device must carefully configure.

But if two VPNs have no sites in common, then they may have overlapping address spaces. Thus, a given address might be used in VPN V1 as the address of system S1, but in VPN V2 as the address of a completely different system S2. This is a common situation when each VPN uses a RFC 1918 [7] private address space. But MPLS overcomes this problem, because sends data based on labels, not based on IP addresses.

It is present the architecture as it is shown in Figure 5.

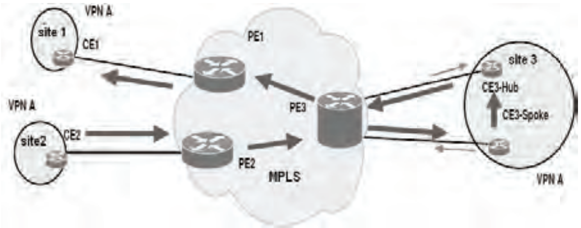

Fig. 5. Hub and spoke MPLS VPN

This structure has some advantages:

- ISP's work, when MPLS is used, is directly proportional to count of customer sites, which is included in VPN, while in Frame Relay it is directly proportional to the power 2 of count of customer sites.
- It supports optimal routing for customer traffic on ISP backbone, because here absent transit CEs.
- Customer doesn't manage own backbone, he only connect CE routers to the ISP.

On the other hand, this model has some disadvantages:

- Overload of P-routers with routing information –large resource of memory, CPU power, and bandwidth.
- In this architecture are existing customers with addresses schemes, which is difficult to co-ordinate with ISP's backbone topology and route aggregation absent.
- Because of the private addresses in customer's networks, unique addresses do not exist. In this case P-routers don't guarantee packet's delivery.
- In this architecture CE router hasn't the possibility to define where will send next packet. This gives chance to eavesdropping.

IV. Architecture of mesh model VPN

A MPLS VPN is built up by connecting MPLS sites through tunnels across IP backbone. Each MPLS site has a Bandwidth Broker (BB), which is to exchange route and signaling information and to manage and maintain VPN networks. Customer routers don't exchange each other information about routes. Data is sent from input customer router to ingress ISP router, then follows some LSRs to the egress LSR, then sent to the customer router in second site.

It is presented the architecture as it is shown in Figure 6.

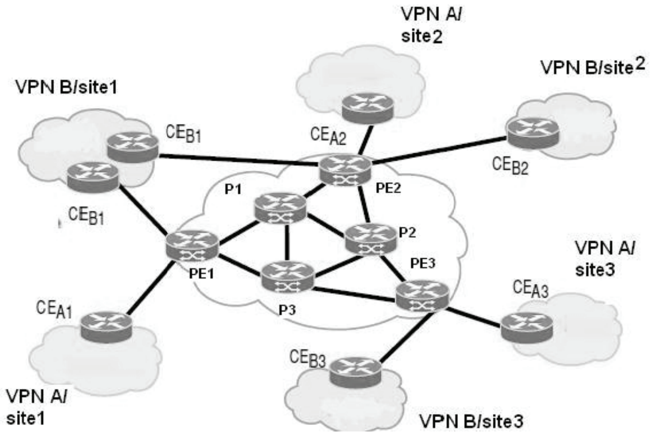

Fig. 6. Mesh MPLS VPN

This architecture has some disadvantages:

- To achieve optimal routing in customer's network, which uses ISP's network, it must be put a router in each end branch, which is connected to all other customers' routers in each branch. This means that this topology is full mesh.
- If used topology is different from full mesh topology, sometimes one customer's router sends packets to the central customer's router, which is placed in different customer's branch, using ISP network and this central customer's router makes decision about forwarding and send back packets to the destination router in the same source brunch. This means that this customer uses ISP's network pointless.
- If used topology is full mesh topology, the customer pays for virtual channels and ISP gives them resources.
- This topology is not well scalable, because here focus is on the links, not on the type of traffic.
- ISP must have tools to recognize different types of applications and based on this information to create security and QoS for customer's data.

On the other hand, this architecture gives some benefits:

- It is support large number VPN, without increasing of data quantity for routes, which is keeping in P-routers.
- It is not possible to send by chance traffic among VPNs, because each of them has own routing information.
- Routing table on PE is used only for directly connected to this router networks, and not for packets, which come from different PE. The route is calculate in the node, where is connected to the ISP backbone.
- If different sites use the same routes, they will consolidate in one routing table in PE, instead two different tables.

V. Configuration of MPLS for VPNs

Above are presented two different architectures for MPLS VPNs, but they use the same devices and this devices are configured in the same way, only the logical links among devices are different. When it must be configured MPLS for VPN, must be followed the next basic steps:

- Specify the interfaces used for communication between PE routers and between PE routers and provider routers:

```
LSR# edit protocols mpls interface interface-name
```

- For RSVP only, configure an MPLS LSP to the destination point on the PE router. The path name is defined on the source router only and it is unique between two routers.

```
LSR# edit label-switched-path path-name
```

- Specify the IP address of the LSP destination point, which is an address on the remote PE router.

```
LSR# set to ip-address
```

- Commit the configuration if you have finished configuring the device.

```
LSR# commit
```

- Configure OSPF with traffic engineering support on the PE routers.

```
LSR# edit protocols ospf traffic-engineering shortcuts
```

- Enable RSVP on interfaces that participate in the LSP. For PE routers, enable interfaces on the source and destination points. For P routers, enable interfaces that connect the LSP between the PE routers.

```
LSR# edit protocols rsvp interface interface-name
LSR# commit
```

- Configuring Routing Options for MPLS VPNs
- Configure the AS number.

```
LSR# set routing-options autonomous-system as-number
LSR# commit
```

- To configure a VPN routing instance on each PE router:

```
LSR# edit routing-instances routing-instance-name
LSR# set description “text”
```

- Specify the instance type, either l2vpn for Layer 2 VPNs or vrf for Layer 3 VPNs.

```
LSR# set instance-type instance-type
```

- Specify the interface of the remote PE router.

```
LSR# set interface interface-name
```

- Specify the route distinguisher using one of the following commands:

```
LSR# set route-distinguisheras-number:numberuser@host#
set route-distinguisher ip-address:number
```

- Specify the policy for the Layer 2 VRF table.

```
LSR# set vrf-import import-policy-name vrf-export export-
policy-name
```

- Specify the policy for the Layer 3 VRF table.

```
LSR# set vrf-target target:community-id
LSR# commit
```

VI. CONCLUSION

MPLS VPNs are used due to its distinguished benefits - fast forwarding, tunneling, etc. QoS routing is naturally used in MPLS VPNs for providing feasible routes with considerations on QoS constraints. QoS routing is beneficial for developing QoS guaranteed MPLS VPNs across IP networks. While other forms of VPN have desirable characteristics, only MPLS provides the network intelligence businesses demand with the reassurance of future capabilities. With its ability to reduce in-house IT resources, coupled with its inherent resilience, MPLS provides the most cost- effective and beneficial VPN solution. For very large organizations, MPLS VPNs offer additional virtualization options, along with advanced capabilities for rapid network failover (within 50 msec) and traffic management for optimizing the link usage. MPLS segmentation yields several benefits, including security through separation, isolation of unpredictable applications and traffic congestion, and prioritization of performance-sensitive applications.

In this paper, it is investigated both benefits and problems when introducing MPLS VPNs. Particularly, it is present architecture of MPLS VPNs with QoS routing capability and discuss some issues on running QoS routing in MPLS VPNs.

ACKNOWLEDGEMENT

The work presented in this paper was supported within the project BG 051PO001- 3.3.04/13 of the HR Development OP of the European Social Fund 2007-2013

REFERENCES

[1] Aleksieva V. P., Comparison Studies on Path Recovery Schemes in MPLS Network, ICEST’10, Macedonia, Bitola 2010, vol.2, p.497-500

[2] Awduche D. O., Malcolm J., Agogbua J., O`Dell M., McManus J. Requirements for traffic engineering over MPLS. IETF RFC 2702. – September 1999. – Available at: www.ietf.org/rfc/rfc2702.

[3] Behringer, M. H.; M. J. Morrow , MPLS VPN Security, Cisco Press, 2005, ISBN 1-58705-183-4,p.312

[4] Eric C. Rosen, Yakov Rekhter, BGP/MPLS IP VPNs, draft-ietf-l3vpn-rfc2547bis-03.txt, 2004

[5] B. Gleeson, et al: A Framework for IP Based Virtual Private Networks. IETF RFC2764, 2000

[6] E. Rosen, Y. Rekhter, BGP/MPLS IP Virtual Private Networks (VPNs), IETF RFC4364, 2006

[7] Y. Rekhter, B. Moskowitz, D. Karrenberg, G. J. de Groot, E. Lear, Address Allocation for Private Internets, IETF RFC1918, 2006