https://doi.org/10.15623/ijret.2018.0703008 Received: 17-01-2018, Accepted: 28-02-2018, Published: 20-03-2018

SECURED DATA ACCESS BETWEEN TWO VIRTUAL MACHINES

Suganthi.R[1], Naga Sushmitha Mavilla[2], Nikitha Suthahar[3], Krithika Gnanaoli[4]

[1]*Asst Professor (UG Scholar), Electronics and Communication Engineering, Panimalar Institute of Technology, Chennai, India*

[2]*Student, Electronics and Communication Engineering, Panimalar Institute of Technology, Chennai, India*

[3]*Student, Electronics and Communication Engineering, Panimalar Institute of Technology, Chennai, India*

[4]*Student, Electronics and Communication Engineering, Panimalar Institute of Technology, Chennai, India*

Abstract

The quest for cost effective, reliable and secured networks is now satisfied with the help of MPLS-VPN technology. MPLS, a contemporary solution to address a multitude of problems faced by present day networks is now being widely adopted by the service providers to implement VPNs to connect the geographically separated customer sites. This paper focuses on interconnectivity of remote customer sites using MPLS through secured and dedicated tunnels with the help of virtual machines.VPN also enables the prioritization of data and sends it through the shortest path using OSPF protocol. Using this, the network is protected and strengthened against hackers and other potential attacks which leads to accessing of data in a secured manner. In our paper we are comparing the performance analysis of OSPF and MPLS protocols using the parameters like latency and round trip time (RTT).

Keywords *— Secured, Mpls, Vpn, Remote, Virtual Machines, Prioritization, Attacks, Latency, Round Trip Time*

----------***----------

1. INTRODUCTION

This is a paper which mainly focuses on a situation where a person X has a quantitative investment firm with more than 500 employees working in different branches globally. This customer wants to have a reliable and secure connectivity among his various branches. This paper gives a solution to the problem statement presented above. At present let us provide a solution for two branches which later can be extended for all other branches in the same way. Transmitting or accessing the data from one device to another in a network is possible through different paths. Among these choosing the best path is very important. Best here refers to the shortest path. For forwarding the packets through the best path there are many routing protocols.

2. EXISTING METHOD

These protocols are broadly divided into static and dynamic. Using static protocol, the elements are connected through manual configuration. So if the link fails, admin has to configure another link until which the link will be down and it will drop the packets. Alternate paths can also be configured beforehand by the admin but it is a time consuming process.

Hence this cannot be used for larger networks. For this reason we moved on to dynamic routing protocols. These protocols work based on a metric parameter. It can choose the best path and if the best path fails it has the ability to choose the alternative path. Among the various Intra-domain dynamic routing protocols, OSPF-Open Shortest Path First which works based on Dijkstraw SPF algorithm and uses cost as a metric in choosing the best path, has many advantages like highest performance, classless routing, sensitive to fault discovery and reroutes it immediately, etc.
Despite the various advantages, it also has certain disadvantages like the routing table created by the OSPF for forwarding the packets is very large and it creates a lot of delay. In order to avoid this delay the concept of MPLS was introduced. MPLS refers to Multi Protocol Label Switching .Among the three types of routers, MPLS works on distribution and core level routers. Access level routers are avoided as MPLS requires high speed. Like OSPF, MPLS is also an Intra-domain routing protocol. An important application of MPLS is the Virtual Private Network(VPN).VPN is a service which uses MPLS technology as a backbone to transmit information securely through private networks. Thus in order to reduce the look-up delay caused by the routing table of OSPF, MPLS is preferred.

3. PROPOSED METHOD

3.1 MPLS Technology

3.1.1 Concept

MPLS is a Label switching technology which is similar to post office mechanism. MPLS introduces a new label L2.5.This label lies between the IP label L3 and Frame label L2.As said previously, MPLS works only on distribution and core level routers. While distribution routers look for L3 header, core routers look for L2.5 header. They remove L2.5 header and add a new header to forward the packets. These labels are randomly given by LDP- Label Distribution Protocol.

https://doi.org/10.15623/ijret.2018.0703008 Received: 17-01-2018, Accepted: 28-02-2018, Published: 20-03-2018

The process of adding a label is referred as PUSH operation and the router involved in the process of pushing a label is called as Ingress Router. The process of removing the label is called POP operation and the router involved in the process of popping a label is called Egress Routers. The process of removing the old label, adding the new one and forwarding is referred as SWAPPING. Core routers are always involved in swapping operation and hence they are referred as Transit Label Switched Routers.

Ingress and Egress routers are commonly referred as Label Edge Routers. The path through which the packet is forwarded is called Label Switched Path. Not all the interfaces of the router are configured with MPLS.

3.1.2 Working

LDP is enabled on the routers using commands. Interfaces where MPLS has to be configured has to be identified and enabled. OSPF is also enabled for selecting the best path. All the interfaces of the core must be MPLS configured. MPLS creates a routing table called as Forwarding Information Base (FIB). LDP gives a label number to all the entries in the FIB table. MPLS header L2.5H has 32 bits which are divided as follows:

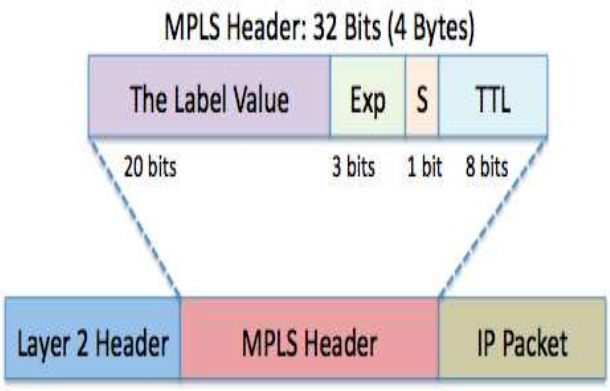


Fig 1: MPLS Header

PC: http://blog.ine.com/wp-content/uploads/2010/02/Screen-shot-2010-02-21-at-2.18.06-PM.png

2^20 number of labels can be generated by LDP in which 1-15 are reserved. Label number from 16 can be used. This information is called Label Information Base. Labels are locally significant i.e. different label number can be used by different routers for forwarding the packets to the same destination. FIB table along with the label information is called LFIB –Label Forwarding Information Base table. After this LDP messages like discovery, session, acknowledgement and notification are exchanged.LDP session is established and label information is exchanged with each other via TCP 646.

Distribution routers will receive the information and checks for IP header and a label is pushed. Using the LFIB table it will know where to transmit the information. The next router checks for L1, L2, L2.5H, removes the MPLS header and new one will be added by a process called swapping. Vice versa takes place on reaching the LER. Finally the label is removed and the packet is received.TTL in the MPLS header refers to Time To Live. It is used in loop situations. TTL values will be decremented every time the same information is received. When TTL is zero, the information is dropped.

Finally the label is dropped at LER and TTL is added. COS-Class of Service in the MPLS header is a quality of service parameter. Depending on the application scenario, MPLS adds multiple labels. In such cases, BOS-Bottom of Service in the MPLS header will see if the label is last label or not. If a link fails alternate path must be chosen which is done using OSPF protocol. After choosing the alternate path, packets are transferred by label switching using LDP.

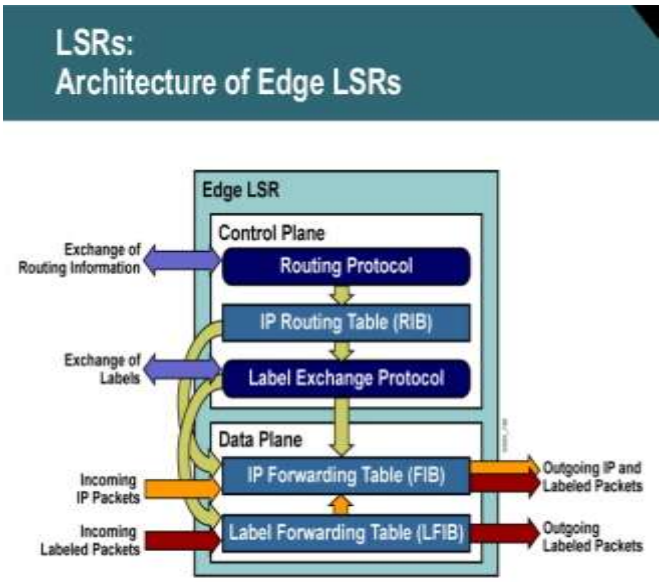


Fig 2: Planes of LER.
Pc: https://image.slidesharecdn.com/mpls-1-130416204413-phpapp02/95/mpls-1-12-638.jpg?cb=1366145097

https://doi.org/10.15623/ijret.2018.0703008 Received: 17-01-2018, Accepted: 28-02-2018, Published: 20-03-2018

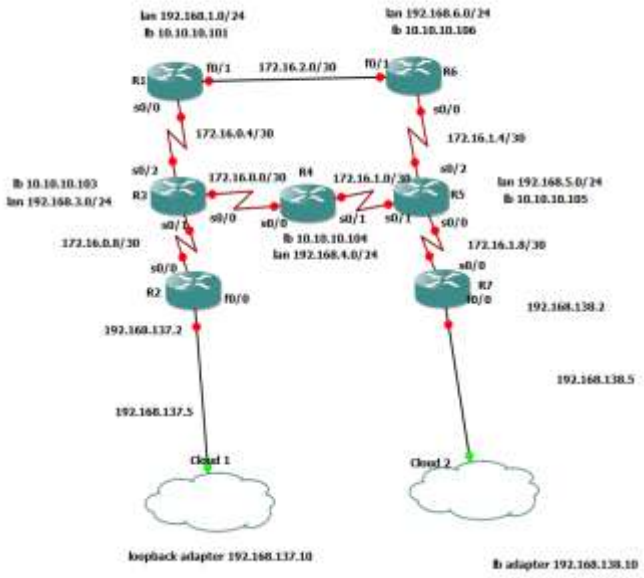


Fig 3: Circuit Diagram

The above circuit is our project diagram. It includes five core level routers and two access level routers connected in a mesh like topology. R1, R3, R4, R5 and R6 are core level routers while R2 and R7 are access level routers. The difference between these routers is the speed of transmission. R2 and R7 are in turn connected with the loopback adapters which in turn are connected with the cloud network in which the virtual machine is configured. All the routers are configured with OSPF protocol while the core routers alone are configured with both OSPF and MPLS protocol. Since the access level routers work with low speed, MPLS cannot be configured in it. Parameters like Round Trip Time (RTT) and Latency are measured. RTT is the length of the time it takes for a packet to be sent plus the length of the time it takes for an acknowledgement of the packet received. Latency is the measure of the time delay required for the information to travel across the network.

3.1.3 Applications of MPLS

There are many applications of MPLS, some of which are

1. MPLS-VPN
2. Traffic Engineering
3. AToM - Any Transport over MPLS
4. VPLS- Virtual Private LAN Service
5. QoS and many others

Among the various applications, one of the most important and popular application of MPLS is the VPN service.

3.1.4 VPN

Virtual Private Network is a service based on MPLS technology. VPNs were introduced to provide a interconnectivity of different branches of the same customer.

This interconnectivity will allow the information to be shared among the branches alone and not to everyone on the internet through tunneling method and this information is also protected from potential attackers by enabling encryption of data and providing authentication methods to the users to access their VPNs. In previous days this was done by establishing a point-to-point link. Frame relay and ATM were the first technologies adopted to implement VPNS.

- Types
  Based on the Internet Service Provider's participation in customer routing VPN is broadly classified into two types namely:
  1. Overlay model
  2. Peer-to-Peer model

3.4.1 Overlay Model

If the internet service provider provides the customer with a virtual circuitry and does not participate in the actual routing process then it is referred as overlay model. The main disadvantage of this is the full mesh of virtual circuits between the customer branches for optimal connectivity for which it requires N(N-1)/2 connections for N branches.

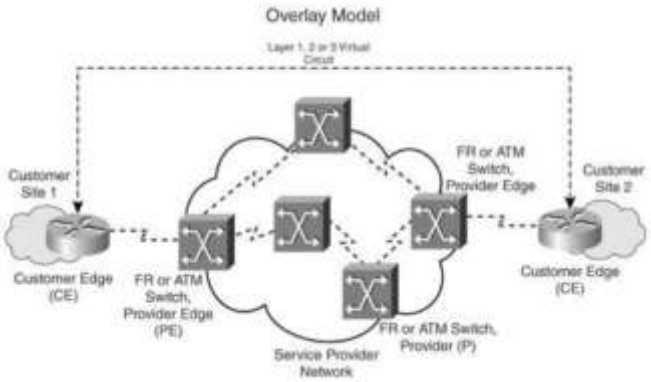


Fig 4: Overlay Model.

3.4.2 Peer to Peer Model

In peer-to-peer model service providers actively involved in customer routing. Routing information is exchanged between customer routers and service provider routers and customer data is transported across the service provider's core optimally.. This method can also be used for providing the interconnectivity between the branches.

https://doi.org/10.15623/ijret.2018.0703008 Received: 17-01-2018, Accepted: 28-02-2018, Published: 20-03-2018

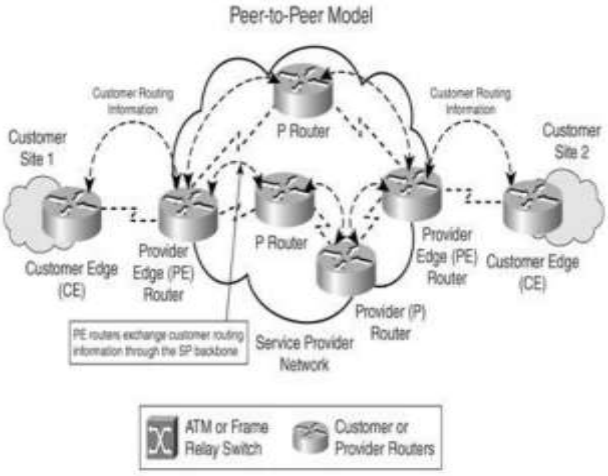


Fig 5: Peer-to-Peer Model.

- WORKING OF MPLS L3 VPNs

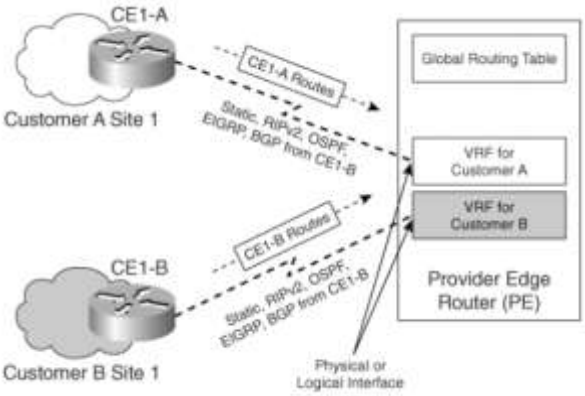


Fig 6: VRF Implementation on PE Router.

When PE is connected with both internet and VPN customers, VRF will be enabled in it. This will logically split the router based on the requirement. For VPN customers alone logical entities called logical routers are created. Each VPN customer will be assigned with a logical router. Same will be performed at the other end PE. In order to distinguish the customers with the same IP network, Router Distinguisher(RD) is used.

RD: 64 bits
Customer has to send the network information to ISPs using any of the routing protocols like static or dynamic protocols. The protocol used by the customer is used by PE at the VRF router. In the routing table, along with the IP address RD is added.

IPv4+RD -> VPN V4 address.
32+64 -> 96 bits.

RD is unique for every customer irrespective of their branches.

4. IMPLEMENTATION

Graphical Network Simulator-3 (shortened to GNS3) is a network software emulator .It allows the combination of both virtual and real time devices. It is mainly used to design complex network topologies. The circuit we have designed above is implemented using GNS3 as follow:

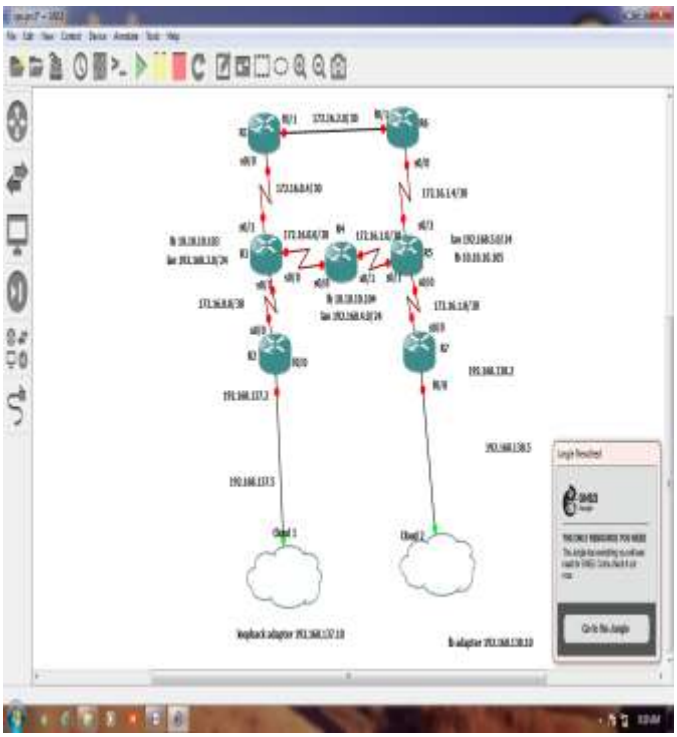


Fig 7: Implementation in GNS3

Other simulation platforms like Cisco Packet Tracer are also available but the reason for not preferring it is that it doesn't support MPLS protocol which is the backbone of our project.

Virtual machine (VM) is used rather than using a PC because of the fact that we can load as many OS as possible in a VM.

Fig 8: Representation of virtual machines in a PC.

https://doi.org/10.15623/ijret.2018.0703008 Received: 17-01-2018, Accepted: 28-02-2018, Published: 20-03-2018

Cloud 2 has the server virtual machine while Cloud 1 is has the client virtual machine. Once the configuration part is completed, FTP is enabled in both the virtual machines. Now the files present in the server can be accessed in two ways. One is by entering the ip address in the internet explorer of client virtual machine.

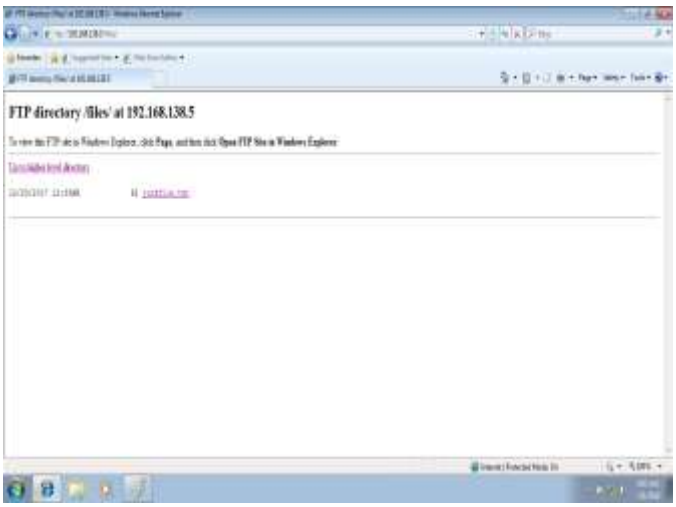


Fig 9: Method 1 of file access

Another way of accessing files is by mapping the ip address of both the client and server virtual machines. By enabling this we will be able to access the files from the network devices option of the client virtual machine.

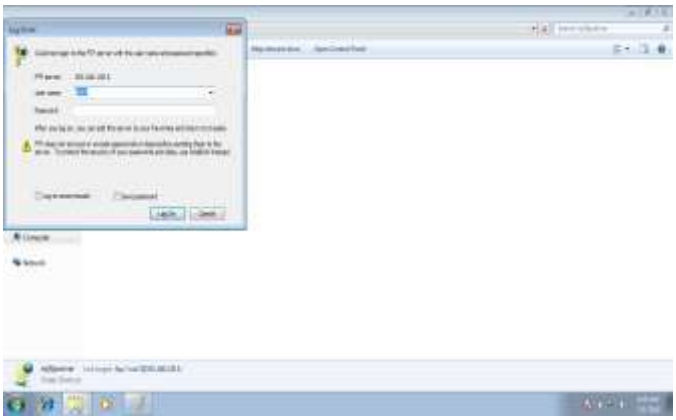


Fig 10: Authentication to access files

Fig 11: Authorized access to files

5. RESULTS

While pinging the server virtual machine from the client, 100 bytes is the default size taken by the routers to send a packet.

From the reply that is received from the server virtual machines, two parameters like round trip time(RTT) and latency is calculated.

$$LATENCY=RTT/2$$

Here we have increased the datagram size gradually and the corresponding changes in the round trip time and latency are measured. The measured values are tabulated as follows :

Parameters Measured

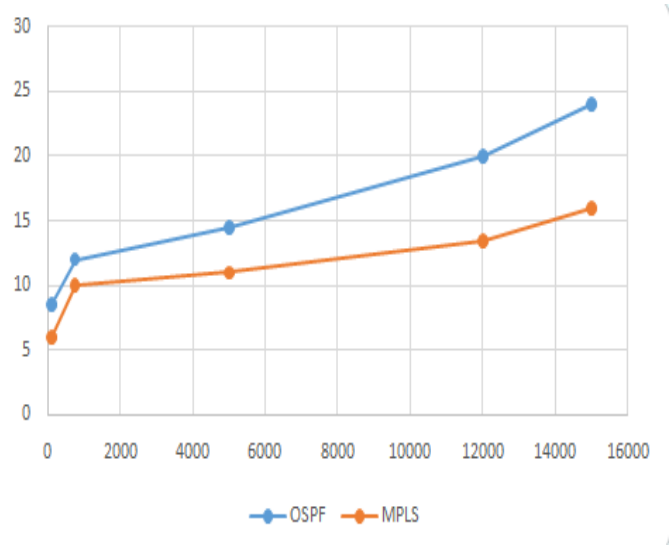
Table 1: Analysis of OSPF

DATAGRAM SIZE(BYTES)	ROUND TRIP TIME(ms)	LATENCY(ms)
100	17	8.5
750	24	12
5000	29	14.5
12000	40	20
15000	48	24

Table 2: Analysis of MPLS

DATAGRAM SIZE(BYTES)	ROUND TRIP TIME(ms)	LATENCY(ms)
100	12	6
750	20	10
5000	22	11
12000	27	13.5
15000	32	16

https://doi.org/10.15623/ijret.2018.0703008 Received: 17-01-2018, Accepted: 28-02-2018, Published: 20-03-2018



X axis: Datagram size (bytes)
Y axis: Latency(ms)

Fig 12: Comparison of latency analysis

The average latency is measured for both OSPF and MPLS protocols. It can be clearly seen that MPLS protocol reduces the latency rate when compared with the OSPF for different datagram size.

6. CONCLUSION

The benefits achieved by employing MPLS-VPN technology is

1. Interconnectivity of geographically separated customer sites and accessing of data from one branch to another using virtual machines.
2. Secured communication between branches using encryption methods.
3. Protection from potential attackers.
4. Prioritization of data.
5. Reduced latency.

Network Security is no longer a significant issue as before. We can now have a high speed, ultra secure and easy to use connectivity between the two branches.

FUTURE WORK

As far as now only a small network is considered. The same can also be employed for larger networks. Interconnectivity of different Internet Service Provider networks can also be done using interior and exterior Border Gateway Protocols. In this way communication can be made faster and more secured thereby providing a reliable network security.

REFERENCES

[1] Ankur Dumka, Hardwari Lal Mandoria, 2015 2nd International Conference on Computing for Sustainable Global Development (INDIACom) , 11-13 March 2015.

[2] Snehal Yadav, Amutha Jeyakumar, International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET).

[3] Jin-Cherng Lin, Ching-Tien Chang, et al. 17th International Conference on Advanced Information Networking and Applications, 2003, 29 March 2003.

[4] Lan jun, Lin bi ying, International Conference on Mechatronic Science Electric Engineering and Computer Research for Service Deployment Based on MPLS L3 VPN Technology, pp. 1484-1488, August 19–22 2011.

[5] Rahul Aggarwal, Juniper Networks OAM Mechanisms in MPLS Layer 2 Transport Networks IEEEcommunication magazine, pp. 124-130, october 2004.

[6] Yoo-Hwa Kang, Jong-Hyup Lee, "The Implementation of the Premium Services for MPLS IP VPNs", Advanced Communication Technology 2005 ICACT 2005. The 7th International Conference on, vol. 210.1109/ICACT.2005.246152, pp. 1107-1110

[7] R. Boutaba, W. Szeto, Y. Iraqi, Emerging Trends in Engineering and Technology 2008. ICETET '08. First International Conference on Digital Object Identifier: 10.1109/ICETET.2008.58 Publication, pp. 187-192, 2008.

[8] From Cisco recognized site available, [online] Available: www.cisco.com/en/US/docs/internetworking/technology/MPLS/VPN/handbook.

[9] Ming-hui LI, Jing-bo XIA, "Research and Simulation on VPN Networking Based on MPLS", 2008 International Conference on Wireless Communications Networking and Mobile Computing, October 12–17 2008.

[10] Ortiz Sixto, "Virtual Private Networks: Leveraging the Internet", IEEE Computer Magazine, pp. 18-20, Nov. 1997.

[11] Younglove Roger, "Virtual Private Networks-how they work", COMPUTING & CONTROL ENGINEERING JOURNAL, pp. 260-262, Dec. 2000.

[12] R. Venkateswaran, "Virtual Private Networks", IEEE POTENTIALS, pp. 11-15, Feb. 2001.

[13] Günter Manuel, Braun Torsten, khalil Ibrahim, "An Architecture for Managing QoS-enabled VPNs over the Internet", IEEE Conference on Local Computer Networks, pp. 122-131, 1999.

[14] Black Uyless, "Internet Security Protocols: Protecting IP Traffic" in , New Jersey:Prentice-Hall, Inc., 2001.

[15] Cohen Reuven, "On the Cost of Virtual Private Networks", IEEE/ACM TRANSACTIONS ON NETWORKING, vol. 8, no. 6, pp. 775-784, Dec. 2000.