International Journal of Future Generation Communication and Networking
Vol.6, No.5 (2013), pp.81-96
http://dx.doi.org/10.14257/ijfgcn.2013.6.5.09

IP Backbone Security: MPLS VPN Technology

Abid Shahzad[1] and Mureed Hussain[2]

Faculty of Computing, Shaheed Zulfikar Ali Bhutto Institute of Science and Technology (SZABIST), H-8/4, Islamabad 44000, Pakistan.
a4abishah@gmail.com[1], mhussain@szabist-isb.edu.pk[2]

Abstract

The Multiprotocol Label Switching (MPLS) technology is currently the most deployed technology by service providers over backbone networks. The highly useful MPLS application nowadays is the MPLS Virtual Private Network (VPN). Due to the enterprises and organizations demand of allowing the remote sites and users to connect to enterprise network, MPLS VPNs have become more attractive. The service providers are using MPLS VPN technology to provide the end users a secure channel across the public internet, with flexibility and scalability. MPLS VPNs have the functionality to operate over both MPLS networks as well as existing IP networks. Variety of research has been conducted in this area and many researchers have proposed different models and solutions to implement MPLS VPN technology more effectively and efficiently. This paper presents the detail analysis of the existing and future techniques and models which are used to implement, optimize, secure MPLS VPN technology.

Keywords: *MPLS, VPN, TE, QoS, LSP, BGP, PE, CE*

1. Introduction

Multiprotocol Label Switching (MPLS) was introduced by IETF [1]. It is a tunneling technology, which gives the platform to create and implement MPLS based Virtual Private Networks (VPNs). It is developed to enhance the packet forwarding over the high performance backbone networks. MPLS forwards the IP packets to the distinct routers instead of the end devices on the basis of small labels [2]. The MPLS application helps to create a tunnel or Label Switched Path (LSP). The small labels are sent over the path. The ingress (entry point of MPLS network) router over the MPLS network path appends this small label to the arriving packet. Over LSP, the hops swap the labels with the new ones to forward the packet. This process keeps on going until the packet arrives at the egress (exit point of MPLS network) router. The egress router strips-off the label and sends the packet towards its destination [3]. The basic advantage of MPLS technology which we just noticed is that IP header analysis which on the other hand is necessary in traditional IP packet forwarding mechanism does not need here. The IP header is analyzed and a small label is appended to the packet at the entry point of the MPLS network. The ingress router may also analyze some extra information about the entering packet to assign it the best route which results in achieving the Quality of Service (QoS). When we talk about the traffic engineering as compared to traditional IP networks, it becomes so easier after choosing the explicit routes in MPLS network. So, this makes the MPLS technology more efficient.

The demand of securely sharing confidential data over public networks is growing day by day as the organizations are expanding their networks. The data sharing between offices, sub offices, and end users is an important requirement of large organizations and ensuring data

ISSN: 2233-7857 IJFGCN

confidentiality and integrity is a major concern. Keeping these requirements in view, the technology which is in use is VPN. The VPNs provides the platform to share data securely across the public network. The main users of VPNs are the service provider administrators, local enterprise network administrators and the end users [4].

The MPLS based VPNs offers verity of good services as compared to the traditional VPNs. They offer scalability, better flexibility, eases management. They are low cost, and support different QoS models MPLS VPNs use Border Gateway Protocol [5] to distribute routes and MPLS technology to forward packets across the network. BGP/MPLS is point-to-point VPN, which uses the services of both BGP and MPLS [5]. The introduction of MPLS technology into VPN network is made to achieve different services like, easy integration, simplification of virtual network, enhance network security, minimizes the complexity, cost reduction and the most important is QoS. The QoS is the major point of concern when services are required from service providers. Therefore, the MPLS VPN technology helps the service provider to achieve QoS over high performance backbone networks.

The MPLS VPNs have many benefits but two of them are very important. The one is scalability and the other is traffic engineering.

1.1. Scalability

If a MPLS VPN is deployed in a well planned way then it is capable to manage tens of thousands of VPNs over the same MPLS network. MPLS VPNs are highly scalable because they do not need site to site connection and mesh across the network.

1.2. Traffic Engineering

Service provider's system administrators can create and implement policies on the basis of traffic engineering over the core network. These policies help to ensure the proper utilization of network resources and optimal traffic distribution.

This paper presents critical analysis of different techniques and models which are used to design, implement, deployment and evaluate MPLS based VPN technology. In addition, the paper also focuses on the limitations of the existing proposed models, evaluation techniques and their procedures. However, the significant of this study is to describe importance of MPLS VPNs in high performance IP backbone networks.

The structure of the paper is as follow: The Section II contains the information that how MPLS VPN works. Section III contains the benefits and section IV highlights the background study of MPLS VPN technology. The purpose is to provide an overview of existing techniques, models and solutions provided to implement and deploy MPLS VPNs effectively. Critical analysis is provided in Section V based on the evaluation of the literature review presented in this paper.

2. Operations of MPLS VPNs

In MPLS VPNs, the customers share routing information by connecting to their service provider edge (PE) router. The routing information is on per site basis. Over the core backbone network the service provider uses MP-BGP protocol to share the routing information and associated labels with others PE routers but within the same VPN. The information like, the source routes, VPN labels, and starting advertising PE router's IP address are stored in the recipient PE router's separate virtual routing and forwarding routing tables the(VRFs). When the packet destined to some customer networks arrives at the ingress router of MPLS VPN, the ingress router looks into the VRF table to identify the destination network. During this process the two labels are in use, the VPN label that represents the

destination network and the tunnel label, which contains the information about LSP leading towards the egress router. The egress router at the end removes the label from the packet and forwards it to the destination network.

The below figure shows that the customer IP packet encapsulated in a VPN, sent across an MPLS label-switched path (LSP). This packet includes tunnel labels processed at each MPLS router along the LSP [3].

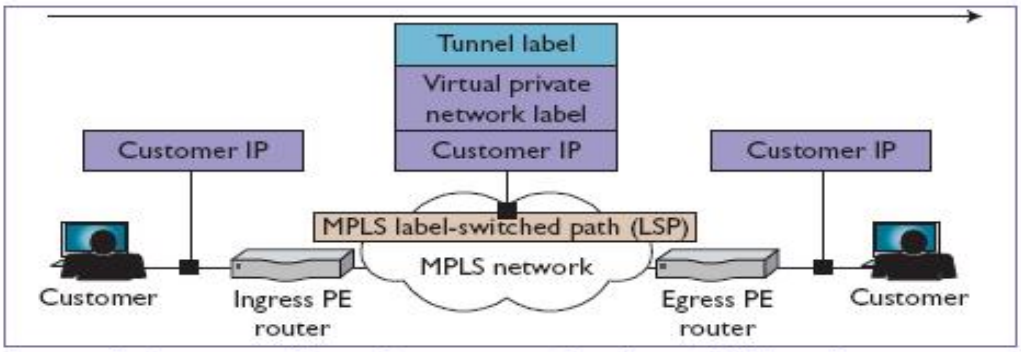

Figure 1. Operation of MPLS VPN [3]

3. MPLS Benefits

3.1. Scalability

As compared to IP based network, the MPLS network is very scalable and it scales thousands of IP based ATM networks. It provides point to point connection to the local users as well as the users connecting from outside the local network. MPLS network is capable of managing of tens of thousands of VPN networks.

3.2. Easy Management

It provides MPLS administrators a great ease when they manage MPLS network. Its creation and management is very easy and involves no complexity. The other important thing which is very attractive is that MPLS does not require traffic matrix updating, no permanent virtual circuit mesh resizing, and no need to update the topology table.

3.3. Foundation to get Premium Services

Due to advancement in the information technology the amount of data sharing over the backbone network is increasing day by day. The MPLS technology provides the platform to create MPLS VPNs which ensures the users to get premium services from the service providers. When the service providers implement MPLS VPNs over their core backbone network, then there is surety that users will get premium services even at the peak time.

3.4. Standard Based

The Internet Engineering Task Force (IETF) has introduced MPLS as a standard. It is available to all network vendors like, CISCO, JUNIPER to make sure that there should be interoperability in large networks where different vendor's products are in use [6].

Table 1. MPLS VPN Supports [7]

L2 VPN	L3 VPN
Ethernet Level Connectivity	IP Level Connectivity
Customer Managed	Service Provider Managed
No sharing of internal routers	Sharing of internal routers
Needs Virtual Forwarding Tabels	Needs Virtual Routing & Forwarding Tables

4. Literature Review of Existing Proposed Models and Techniques

4.1. MPLS Technology on IP Backbone Network

Gurpreet Kaur *et al.*, [1] presented MPLS Tunneling architecture on the IP backbone network. MPLS technology provides the platform to deploy MPLS based VPN. MPLS framework is used by service providers to provide data scalability, security, fast routing and forwarding to the customers. MPLS VPN helps the users to share per site routing details by connecting to local service provider router PE (Provider Edge). Using Multiprotocol Border Gateway protocol (MP-BGP), the service provider PE router routes information and the added label to packet to the next customer site router, but within the same VPN. The author also discussed the Traffic Engineering concept based over MPLS technology and different encryption techniques to secure MPLS network. One of the most common threats to MPLS technology is brute force attack to break the encrypted data. Algorithms like, Advance Encryption Standard (AES), DES and triple DES are used to protect the MPLS networks. This paper lacks the explanation and validation of the proposed MPLS VPN architecture. The encryption techniques simulation results are not shown in the paper.

4.2. A Novel Approach to Improve the Performance of MPLS-VPN

Geng Yanhui *et al.*, [2] claimed that their proposed approach by using label stack instead of simple labels proved to be more appropriate than the existing techniques. It helps to reduce the routing table size and also increase the performance of MPLS VPNs. Due to excellent characteristics of VPNs; the corporate organizations are using VPN to allow remote sited and corporate clients to connect to the organization over high performance IP backbone network where MPLS VPN technology is used. MPLS VPN works on the labels by forwarding the packet to distinct routers instead on the basis of analyzing the whole part of the IP packet header. To achieve better performance and QoS the ingress router may add some additional information regarding the best path selection along with the label of course. MPLS technology has also made traffic engineering much easier. MPLS VPNs performs so efficiently over high speed backbone networks. To make the MPLS VPN performance more optimized the authors proposed label stack instead of single label to each packet. The label stack helps to reduce the size of the label which results in excellent performance of MPLS VPN. Due to stack label technique the size of the routing table is reduced. So, when routers exchanges their routing table's required low bandwidth and processing power will also be fast. The simulation results also verified that this approach resulted in fast packet forwarding and minimizes the delay factor. The paper lacks a model and this stack label is not implemented in real MPLS model in the paper.

4.3. Multiprotocol Label Switching and IP: MPLS VPNs over IP Tunnels

Brian Daugherty *et al.*, [3] present the functionality of MPLS VPNs over IP tunnels. MPLS VPNs works over MPLS network, but also support IP networks. The paper mainly describes that how different services made for MPLS network can also support native IP networks. There are two key issues which need to be focus while evaluating MPLS VPNs. One is security because when an IP packet reaches at the egress (exit point) router, then the router needs to know that this packet came from the legitimate source. So, there is need of fast path to provide that information to the egress router. The other issue is processing overhead, when a packet arrives at the egress router along with the MPLS payload, the egress router needs to know about the MPLS service context in the router. This information is needed to direct that how to forward packet. A comparison is shown in the paper for MPLS-over-IP tunneling solutions. The one solution which is MPLS-over-GRE (Generic Routing Encapsulation) supported by different vendors like, CISCO and Juniper is vulnerable to blind insertion attacks. The service providers need to address this type of issues and ensures that proper precautions have been made. For example, use of filters to avoid such attacks. During the comparison, the MPLS-over-L2TPv3 solution is considered perfect which address all the concerns of all other solutions. The main limitation of this paper is that comparison presented in this paper is not supported by any simulation so that results cannot be verified and tested.

Security for MPLS based VPNs it is very simple for Egress PE routers to trust the routers who send the packet because each incoming packet uses MPLS encapsulation and PE tunnel labels. So, it is very difficult for the attackers to insert the spoofed packet in the core network of the service provider because there is very less chance that they extend their MPLS network beyond the boundaries of their core network.

On the other hand, without the characteristics of the protocol the MPLS VPN based on IP tunnels makes the customer network vulnerable to attack. The simple type of attack is the blind insertion attacks. The attacker dodges and breaks the service provider security perimeters which he is implemented at the PE routers. The attacker sends the spoofed packets towards the PE router which is the entry point for a customer VPN. If the attacker is launching iteratively spoofed packets with 20 or 30 labels, there is huge possibility that after sometime the spoofed packet is matched with the original label entry which is stored in the PE router. The source IP will be fake in the spoofed packet and the customer entry router will forward it to the network which will result in compromising the data confidentiality and data integrity. Let’s assume that an attacker launches spoofed packets at the rate of 1Mbps and there are around 100 labels stored in every PE router in its VRF table then there is possibility that the attacker will hack the GRE-based MPLS VPN in around 1.04 seconds. However, the L2TPv3 based VPN would take minimum of 585,000 years to be cracked even after the VPN labels were considered valid. L2TPv3 has the optional cookie information in the header which makes him unbreakable and provides maximum security against the packet spoofing attacks.

Table 2. MPLS-over-IP Comparison [3]

	MPLS*-over-IP	MPLS-over-GRE*	MPLS-over-IPSec	MPLS-over-L2TPv3*
Supports MPLS VPN	Yes	Yes	Yes	Yes
Deployed in large networks	No	Yes	No	Yes
Low administrative impact	Yes	Yes	No	Yes
Low performance impact in PEs	No	No	No	Yes
Effective antispoofing protection	No	No	Yes	Yes
Supports PE capabilities exchange	No	No (possible)	No (possible)	Yes

*MPLS: Mulitprotocol Label Switching; GRE: Generic Routing Encapsulation; L2TPv3: Layer-2 Transport Protocol, version 3

4.4. Design and Implementation of Two level VPN Service Provisioning Systems over MPLS Networks

Li – Der Chou *et al.*, [4] presented a design and implementation of two levels VPN service processing system which is based on MPLS VPN technology. As we are aware of the benefits of simple VPN, the corporate are using VPN to connect with different separated sites and remote users. The VPN technology reduces the communication medium cost, as they are easy to implement and simple to manage. Using LSP we can achieve MPLS IP VPN service over IP backbone high performance networks. There are three different types of users involved in MPLS VPN networks, the service provider network administrator, who is responsible to manage service provider backbone networks, the local enterprise administrator who is responsible to manage enterprise local network and the third one is the end user. The local administrator manages the communication between service provider network and the local enterprise network. The service provider administrator takes care of providing global network services to enterprise local devices of different enterprises. The author's proposed design is based on two levels. The provider edge router (PER) is responsible for providing MPLS VPN service to local enterprise managers, while corporate edge router (CAR) is responsible for local enterprise devices and its job is to provide LPE based VPN services to the end users. The PER manages the CAR and inform them timely in case of any fault and attack. As PER is at central location and has all the information about the VPN traffic from and into local enterprise network. On the basis of this information, the PER signals against any attack or intrusion. The author has provided the results which show that implementation of this two level VPN services results in flexibility, security and ease of management. The proposed virtual network is divided in three different classes and three different users are involved, which make this model a little complex.

4.5. The Implementation of the Premium Services for MPLS IP VPNs

Keeping the QoS issues of current MPLS IP VPNs in the mind, the authors Uou-Hwa Kang *et al.*, [5] proposed the workflow architecture to get premium services in MPLS VPNs. There are three VPN technologies which are very common for their usage; the ATM/FR based VPN, MPLS based VPN and old IP tunneling based VPNs. When we analyzed, we found that MPLS based VPNs offer VPN services with low cost, easy management, and very flexible to enhance and support a variety of QoS. Despite all the improved characteristics of MPLS VPNs over traditional VPN technologies the paper proposed a new design of MPLS VPN to support premium services. The model mainly focuses on best efforts and traffic engineered LSPs. As we already know that MPLS based VPN uses labels to forward packets to distinct routers, but in the model we add experimental bits in the shim header of the packet.

To manage different services belonging to a particular VPN, the Diffserv is used to differentiate. So, the idea is to implement premium services which can be achieved in a way that each VPN should be allocated best efforts or traffic engineered LSP. This will help to reduce the effort of packet manipulation or additional Diffserv function. The commands available in this model can be executed by the user in order to make premium services to a MPLS IP VPN. The weak point of this paper is that proposed design is very complex. It needs to have some additional services to achieve the premium services. The user also needs to execute different commands which seem to be a worry for the users.

4.6. Quantitative Analysis of Multiprotocol Label Switching (MPLS) in VPNs

The paper presented by Muzammil Ahmed Khan [6] gives a detailed analysis of MPLS technology for creating VPNs. When we compare conventional routing with label switching, we find a lot of different characteristics. When we talk about performance then we can see that conventional routing performs complete IP header analysis of the packet at each hop. While on the other hand, the label switching performs it only one time at the egress router. The conventional routing requires several multicast routing and packet forwarding algorithms, whereas label switching only requires forwarding algorithm. The routing decisions are made on the basis of destination address in conventional routing but in label switching the decisions are made on the basis of destination address, type of the data in the packet and QoS. The paper supported arguments and assumptions by generating simulation results by checking throughput analysis with respect to time. So, the MPLS VPN compatibility with other architectures makes MPLS VPNs more flexible and interoperability with existing IP backbone networks. So, the MPLS VPN compatibility with other architectures makes MPLS VPNs more flexible and interoperability with existing IP backbone networks. The limitation of this paper is that the author did not propose a model to support his results in real environment.

4.7. Multiprotocol Label Switching and IP: Multicast VPNs

Chris Metz [7] proposed a new solution which elaborates multicast VPN. We are aware that existing MPLS VPN solutions can only provide unicast routing over the service provider network. However, this solution helps the customers to achieve IP multicast services over the MPLS VPNs. The proposed solution is very helpful for the service provider. On this basis of this solution the service provider can offer both MPLS VPNs which supports both unicast and multicast routing applications. Using MPLS VPN services the customers allow their large enterprise CE routers to connect to the nearest available provider Edge router. To provide routing information of one customer to another customer is the responsibility of service provider. The service provider uses the core backbone network to share IP packets between two customer sites. The existing MPLS works on unicast routing and it only forwards packets from one machine of a VPN to another machine of another VPN. Due to increase demand of customers to communicate and share the same information with multiple hosts simultaneously, the need of multicast VPN increased. To complete the need of existing customers and to gain the attraction of new customers the service providers would have to provide IP multicast VPN services. This paper lacks a model or simulation results to support the arguments made by the author.

4.8. A Monitoring Network on Highways Based MPLS VPN and Study of its QoS Mechanism

Yin Guofu [8] proposed a network model based on the MPLS VPN for highway monitoring networks. The idea is to use the MPLS VPN technology to improve the network security, to minimize the complexity and to enhance reliability as compared to the existing networks which are there to monitor traffic. In China, due to rapid increase in road transportation, the existing highway monitoring networks have become so complicated resulting in congestion. The security of the existing systems also a major concern, because the current system works as web based connection oriented network system. There is currently no mechanism in use to encrypt the data to avoid data theft. Mostly the applications are web based. So, the MPLS VPN network structure is proposed to avoid these problems. Due to the new network the congestion, transmission delays and image transmission jerking problems have been eliminated. The author also proposed Diffserv model [8] which is used in combination of MPLS VPN based highway monitoring networks, which results in cost effective, efficient, delay free and improved throughput capacity and enhanced network security. The simulation results showed in the paper also acknowledged that MPLS VPN technology helped building a good monitoring network with improved efficiency and security. This model is successfully implemented in Shaanxi province in China and resulted in positive output. The limitation of this model is that it is not used by other remote sites and users. On the other hand the VPN technology provides the best platform to allow remote sites and users to connect to a corporate enterprise or location.

4.9. A Detailed Implement and Analysis of MPLS VPN Based on IPSec

Rong Ren *et al.*, [9] presented an idea of enhanced MPLS VPN. Their solution is more secure and efficient as compared to the original and existing MPLS VPN. Due to the rapidly increasing changes and developments in internet technology demands more security and efficiency. The existing MPLS VPNs are unable to provide best security and efficient transmission of data when we compare it to our proposed new MPLS VPN model. In the enhanced model, the authors used MPLS technology for efficient transmission, IPSec protocol to encrypt the data and Certification Authority (CA) for authorizing the entities involved in the communication. The model uses four different techniques which are VPN Tunneling, Encryption and Decryption, Key Management achieved by CA, and Authentication. This model helps to remove all the concerns and issues related to the security of existing MPLS VPN technology architecture. It gives more flexibility to the end users to choose either security or efficiency depending on the type of data communication users are having. The paper presented a well detailed enhanced version of MPLS VPN based on IPSec and CA model. The results are also verified by performing the simulation. The weakness of the paper is that after adding some techniques, the model became so complex and its management seems very difficult.

4.10. A Distributed Bandwidth-Guaranteed Routing Algorithm for P2MP VPLS Virtual Connections

Najah Abu Ali *et al.*, [10] proposed a distributed routing algorithm while keeping the limitations of switched networks. The Ethernet switched networks does not provide the functionality to create internet scale distributed networks. This algorithm functions over Point to Multipoint (P2MP) VPLS (Virtual Private Label Switched) connections. The VPLS technology requires MPLS technology to be implemented. One of the limitations of simple MPLS is that it only supports point to point (P2P) Label Switched Path (LSP) and is not

capable for P2MP LSPs. This algorithm not only provides MPLS and Traffic Engineering (TE) functionality over P2MP but also provides quality of Service (QoS) to best use of network resources and safety against the network failures. The proposed algorithm is very simple, less complex and easy to implement. It does not need to have prior information about the network. It chooses the paths which are less used and leaves the critical links which are used for quite number of times. The results of the proposed algorithm are verified by the simulations. The results are compared with the other two critical link algorithms like, WSP and Plotkin [10] and the results shows that this algorithm outclasses the functionality of the other two because this algorithm resulted in low blocking probability. The idea behind the success of this algorithm is that it balances the load over point to multipoint (P2MP) links by ignoring the critical links which are used very often. The problem with this technique is that the path chooses by the algorithm other then critical path increases the number of hops.

4.11. Efficient QoS Implementation for MPLS VPN

An efficient Quality of Service (QoS) scheme for MPLS VPN is proposed by Muhammad EL Hachimi *et al.*, [11]. The idea of this scheme is to provide MPLS VPN services to the customers to fulfill their demand of extreme services. This scheme will help the customers to get at least some of the services even when there is too much traffic load on MPLS VPN path. In the current age of technology the customers demand QoS when they acquire voice, video and data services from the service provider. The service provider needs to assure QoS within the MPLS VPN services and this can be achieved in MPLS VPN when service provider's PE to CE policies are consistent with customer's CE to PE policies. Therefore, the service provider can analyze the traffic flow whether it is in or out of the customer's contracted bandwidth. The proposed scheme helps the customers to acquire the residual bandwidth if available over the VPN to enhance and increase their contracted bandwidth. The residual bandwidth can be used if other VPNs are currently not using their contacted bandwidth. So, the customer will get good bandwidth which helps to get QoS, but customer will be charged for the extra bandwidth which they are using other than their contracted bandwidth. However, all the VPNs are ensured that their contracted bandwidth will be available all the time for their own use whenever it is needed. The problem seems with the proposed scheme is that the customers will be charged for the extra residual bandwidth they use. There should be mechanisms that they should not be charged for the useless bandwidth available over the network.

Qos in MPLS VPN a usual Scheme: To identify the advantages of this proposed solution over the existing MPLS VPN scheme, a detailed analysis has been performed to highlight the advantages. As far as the volume of traffic over the edge networks, the policies made by administrator are used to control the traffic which results in possible congestion [11].

4.12. End to End QoS Architecture for VPNs: MPLS VPN Deployment in a Backbone Network

Haeryone Lee *et al.*, [12] proposed an architectural model to deploy MPLS VPN efficiently in existing IP backbone networks. The model guides and provides directions to efficiently implement VPN service in MPLS network. The benefits of VPN should be there that it could be accommodated with existing IP backbone networks. MPLS supports the packet based network to provide QoS to the end users. So, MPLS VPN when deployed over high performance backbone networks results in range of QoS capabilities. The issues in IP based VPNs are like, scalability issues, QoS issue and mainly the security issue which is always a major concern for the end users. The proposed architecture helps in solving the

virtual circuit multiplication and QoS issues. Therefore, MPLS VPN technology is very crucial and key factor to the large IP backbone networks in the near future. The MPLS technology helps the deployment of IP networks, facilitates with traffic engineering characteristics, ensures QoS capabilities and also aids IP based VPNs. There are no simulations performed to validate the results of MPLS VPN and comparing these results with IP VPN.

When we talk about the issues in the current IP based VPNs, and then we found out some concerned areas. Although we know that the IP VPNs have benefits as compare to simple IP based network. The VPN over the private network is always beneficial for all the parties, like organizations, service providers and the end users. Despite these benefits which VPN technology give us over IP based network, there is still a big problem which IP VPNs are having is to achieve QoS. So, overall there are three different types of problems which appear in IP VPNs, the first one is the security, the second one is large number of virtual circuits and the last one is the inability of IP VPNs to ensure the QoS.

Scalability problem: A simple VPN has the ability to manage and support hundred of thousand of VPN connections and the private network which is internet support millions of relationships. A simple formula is used to count the number of VPNs in network is N(N-1)/2, if the network N number of points of service. If a network has 5 service points, then there is support for 10 virtual circuits. If we increase the number of service points like 200, then we will need around 20,000 virtual circuits.

QoS problem: The second problem which we face in IP VPN is the QoS. There is not mechanism used by IP based applications to specify QoS, a large number of activities, like, RSVP has the direction at adding QoS, the users and carries does not feel comfortable by selecting Qos individually, which results in high amount of bills if the user selected high level of QoS. A better approach is that an entire VPN has been assigned a certain QoS level, which normally happens in IP and ATM Relay networks. Therefore, even dynamic routing protocols like, OSPF are used for routing and to create routing tables are not able to share QoS information and the information about the usage of trunk and node's resources.

Security problem: Security is the major concern for all the users and organizations which uses public network to share and exchange their confidential data. In ATM and Frame Relay networks a dedicated medium is used for communication but in VPNs there is not such dedicated link. So, the security is a concern here when we talk about VPN. In recent years the IETF has introduced IPSec protocol, which is widely in use for IP based VPNs. It is a tunneling protocol and is compatible with IPv4 networks because originally it was designed for IPv6 networks. IPSec provides the traffic security over IP networks. The IPSec framework which is based on the mechanisms which is used to manage, terminate and establish secure channels or tunnels for the authentication and encrypting each and every packet [12].

4.13. VPN Scalability over High Performance Backbones Evaluating MPLS VPN against Traditional Approaches

This paper shows a comparison between MPLS VPN and the traditional VPN approaches like, IPSec based VPNs. The author Francesco Palmieri [13] has analyzed the positive point of both the approaches in this paper. The old VPNs had limitations and weaknesses like performance and scalability issues as compared to MPLS VPNs. The results shown here have found that MPLS VPNs are more scalable, which can be extended in less time. The MPLS has less impact on the CPU and memory during the configuration and enabling VPNs. On the other hand, when we configure IP VPNs, the CPU load increases to 30% approximately, this seems too high. The simulation results of latency and packet Loss showed that MPLS output is almost like baseline (normal), but in IPSec VPN latency (Average RTT) is so high. During

the packet loss analysis, it was 0% loss in MPLS VPN and 3% in IPSec based VPN. The author also measured end to end throughput measured via TTCP, the MPLS VPN provided high throughput as compared to IPSec VPN. Therefore, as compared to IPSec VPN, the MPLS VPN reduces the cost and complexity, provides cost effective connection, reduces the complexity and ease to add new sites in MPLS VPN. The negative point is that the author did not propose any model to support and verify his test results.

4.14. Pure MPLS Technology

Liwen He *et al.*, [14] presented an idea to implement and deploy a MPLS network to achieve different security services like availability, security and reliability. The main idea is to implement MPLS network without the use of IP packets which is used for routing and traffic forwarding. The author presented a well detailed comparison between IP networks and MPLS based networks. The MPLS technology offers great flexibility, scalability and traffic engineering capabilities. The comparison clearly shows that the MPLS technology has many benefits over IP based networks. MPLS technology is very focusing technology and is currently most usable in service provider backbone networks. In this paper the author also highlighted some problems currently exists in MPLS technology. The author did not presented simulation results of both IP and MPLS network, which should have been very helpful to highlight the difference.

4.15. Securing MPLS Networks with Multi-path Routing

Sahel Alouneh *et al.*, [15] claimed that the existing MPLS network technology is not secure enough to ensure data confidentiality. The author proposed a technique which uses multipath routing to improve the security of MPLS network. This technique ensures that when a packet arrives at entry point router, it is to be divided into share packets. These shared packets then assigned disjoint paths over the MPLS network. When these shared packets arrives at the exit point of the MPLS network, the exit point router then reconstruct the shared packets to get the sent IP packet. In this case the attacker needs to capture multiple paths to find out the original packet which seems impossible. The author only focused on the confidentiality of the data which is sent across the MPLS network. There should be some methods to also ensure the data integrity and availability.

Table 3. Summary of MPLS VPNs Models/Solutions/Practices/Techniques

Research Topic	Author(s)	Problem Discussed	Solution Purposed	Strengths	Weakness
MPLS Technology on IP Backbone Network	Gurpreet Kaur et al.	The Traffic Engineering concept based over MPLS technology and different encryption techniques to secure MPLS network from brute force attack to break the encrypted data.	Algorithms like, AES, DES and tripe DES are used to protect the MPLS networks.	The encryption algorithms which are used to secure the MPLS are the best algorithms used for encryption. E.g, AES and Triple DES are currently very much in use.	The encryption techniques simulation results are not shown in the paper.
A Novel Approach	Geng Yanh	The size of the labels used in MPLS	Label stack instead of	The label stack helps to reduce	The paper lacks a model and

to Improve the Performance of MPLS-VPN	ui et al.	VPN, which results in increasing the routing table size.	simple labels, resulted in reducing the size of routing table.	the size of the label which results in excellent performance of MPLS VPN. The less bandwidth is also required in this scenario.	this stack label did not implemented in real MPLS model in the paper.
Multiprotocol Label Switching and IP: MPLS VPNs over IP Tunnels	Brian Daugherty et al.	Security and Processing Overheads over core backbone networks.	The MPLS-over-L2TPv3 solution is found perfect which address all the concerns like, security, flexibility, performance of all other solutions.	A detailed comparison is shown in the paper for MPLS-over-IP tunneling solutions.	The comparison presented in this paper is not supported by any simulation so that results can be verified and tested.
Design and Implementation of Two level VPN Service Provisioning Systems over MPLS Networks	Li – Der Chou et al.	The flexibility and scalability issues in the IP based networks.	Implementation of two level VPN service Processing System.	The VPN based solution reduces the communication medium cost, they are easy to implement and very simple to manage.	The proposed virtual network is divided in their different classes and three different users are involved, which make this model a much complex.
The Implementation of the Premium Services for MPLS IP VPNs	Uou-Hwa Kang et al.	Packet manipulation and traffic engineering difficulties in existing VPN technologies	Proposed a workflow architecture to get premium services in MPLS VPNs.	MPLS based VPN offers VPN services with low cost, easy management, and very flexible to enhance and support a variety of QoS.	Proposed design is very complex. It needs to have some additional services to achieve the premium services.
Quantitative Analysis of Multiprotocol Label Switching (MPLS) in VPNs	Muzammil Ahmed Khan	Performance issues in conventional routing like, it performs complete IP header analysis at each hop and requires several multicast routing and packet	The detailed analysis of MPLS technology for creating VPNs which elaborates and highlights the MPLS VPN	MPLS VPNs provides centralized server, scalability, security, ease to implement, flexible addressing and straight forward	The limitation of this paper is that the author did not propose a model to support his results in real environment.

		forwarding algorithms.	features which leads us with no choice other than MPLS VPNs.	and easy migration.	
Multiprotocol Label Switching and IP: Multicast VPNs	Chris Metz	MPLS VPN solutions can only provide unicast routing over the service provider network	The proposed solution helps the customers to achieve IP multicast services over the MPLS VPNs	Proposed a well elaborated model	This paper lacks a model or simulation results to support the arguments made by the author.
A Monitoring Network on Highways Based MPLS VPN and Study of its QoS Mechanism	Yin Guofu	Network security, complexity and reliability issues in existing IP based traffic monitoring networks	Diff-Serv model which is used in combination of MPLS VPN based highway monitoring networks, results in cost effective, efficient, delay free and improved throughput capacity and enhanced network security.	MPLS VPN technology helped building a good monitoring network with improved efficiency and security. The solution is successfully implemented in Shaanxi province in China and resulted in positive output.	The limitation of this model is that it is not used by other remote sites and users.
A Detailed Implement and Analysis of MPLS VPN Based on IPSec	Rong Ren et al.	Security and efficiency issue in the existing MPLS VPN	An enhanced model which uses MPLS technology for efficient transmission, IPSec protocol to encrypt the data and CA for authorization.	Four different techniques which are, VPN Tunneling, Encryption and Decryption, Key Management achieved by CA, and Authentication which resulted in more security.	After adding some techniques, the model became so much complex and its management became very difficult.
A Distributed Bandwidth - Guaranteed Routing Algorithm	Najah Abu Ali et al.	MPLS is that it only supports point to point (P2P) Label Switched Path (LSP) and does not capable for P2MP	Proposed an algorithm which functions over Point to Multipoint	This algorithm not only provides MPLS and Traffic Engineering (TE) functionality over P2MP but also provides quality	The problem seems that may be the path chooses by the algorithm other then critical path increases

for P2MP VPLS Virtual Connections		LSPs.	(P2MP) VPLS.	of Service (QoS)	the number of hops.
Efficient QoS implementation for MPLS VPN	Mohammed El Hachimi et al.	Customers demands QoS even during peak hours when they acquire voice, video and data services from the service provider.	An efficient Quality of Service (QoS) scheme for MPLS VPN.	The proposed scheme helps the customers to acquire the residual bandwidth if available over the VPN to enhance and increase their contracted bandwidth.	The problem seems with the proposed scheme is that the customers will be charged for the extra residual bandwidth they use. There should be mechanisms that they should not be charged for the useless bandwidth available over the network.
End to End QoS Architecture for VPNs: MPLS VPN Deployment in a Backbone Network	Haeryone Lee et al.	Scalability issues, QoS issues and mainly the security issues in IP VPN.	Architectural model to deploy MPLS VPN efficiently in existing IP backbone networks which address scalability and security issues. It ensures the QoS.	MPLS VPN supports the packet based network to provide QoS to the end users.	There are no simulations performed to validate the results of MPLS VPN and comparing these results with IP VPN.
VPN Scalability over High Performance Backbones Evaluating MPLS VPN against Traditional Approaches	Francesco Palmieri	Traditional VPNs have limitations and weaknesses like performance and scalability issues	Performed different performance test between traditional and MPLS VPNs, which highlighted the benefits of MPLS VPNs over traditional VPNs.	The MPLS creates very less impact on the CPU and Memory during the configuration and enabling VPNs.	The author did not proposed any model to support and verify his test bed results.
Pure	Liwe	Security,	Presented an	The author	The author did

MPLS Tech	n et al.	availability and reliability issues in IP based networks	idea to implement and deploy a MPLS network to achieve different security services.	presented a well detailed comparison between IP networks and MPLS based networks.	not presented simulation results of both IP and MPLS network, which should have been very helpful to highlight the difference.
Securing MPLS networks with Multi-path routing	Sahel Alouneh et al.	Security issue in existing MPLS, especially the data confidentiality issue.	The author proposed a technique which uses multipath routing to improve the security of MPLS network.	The proposed technique is explained in detail with simulation results and comparisons.	The author only focused on the confidentiality of the data which is sent across the MPLS network. There should be some methods to also ensure the data integrity, and availability.

5. Conclusion

In this paper, we have made an attempt to present a complete understanding of MPLS based VPN technology. We have discussed the existing proposed models, implementation and deployment techniques of the MPLS VPNs over the core IP backbone networks in the context of MPLS tunneling technology. We have highlighted some of the papers pointing towards the flexibility, scalability, and easy traffic engineering benefits of MPLS VPNs compared to traditional VPNs and IP based networks. The main idea behind this research is to review the various models and techniques used to implement MPLS VPNs effectively and efficiently.

This research is particularly useful for service providers and local enterprises administrators in context of their area job responsibilities to effectively specify, model and implement MPLS VPNs over high performance IP Backbone networks.

On the basis of the literature review conducted in this paper, we conclude that most of the techniques discussed are effective for service providers to implement MPLS VPNs instead of traditional VPNs over core backbone networks.

References

[1] G. Kaur and D. Kumar, “MPLS Technology on IP Backbone Network”, International Journal of Computer Applications, vol. 5, **(2010)**, pp. 13-16.
[2] G. Yanhui, S. Qiong, C. Yuzhong and Y. Nenghai, “A Noval Approach to Improve the Performance of MPLS-VPN”, 8th Korea-Russia International Symposium on Science and Technology, KORUS, **(2004)**, pp. 35-39.
[3] B. Daugherty and C. Metz, “Multiprotocol Label Switching and IP: MPLS VPNs over IP Tunnels”, IEEE Internet Computing, **(2005)**, pp. 68-72.

[4] L.-D. Chou and M. Yuan Hong, "Design and Implementation of Two level VPN Service Provisioning Systems over MPLS Networks", Proceedings of the 7th IEEE International Symposium on Computer Networks (ISCN'06), **(2006)**, pp. 42-48.
[5] Y.-H. Kang and J.-H. Lee, "The Implementation of the Premium Services for MPLS IP VPNs", Proceedings of the 7th International Conference on Advanced Communication Technology ICACT, **(2005)**, pp. 1107-1110.
[6] M. Ahmad Khan, "Quantitative Analysis of Mutiprotocol Label Switching (MPLS) in VPNs", Proceedings of the IEEE Students Conference, ISCON'02, **(2002)**, pp. 56-65.
[7] C. Metz, "Multiprotocol Label Switching and IP: Multicast VPNs", IEEE Internet Computing, **(2006)**, pp. 76-81.
[8] Y. Guofu, "A Monitoring Netwok on Highways Based MPLS VPN and Study of its QoS Mechanism", Proceedings of the International Conference on Networking and Digital Society, China, **(2010)**, pp. 278-281.
[9] R. Ren, D.-G. Feng and K. Ma, "A Detailed Implement and Analysis of MPLS VPN Based on IPSec", Proceedings of the 3rd International Conference on Machine Learning and Cybernetics, Shanghai, **(2004)**, pp. 2779-2783.
[10] N. Abu Ali, H. Mouftah and S. Gazor, "A Distributed Bandwidth-Guaranteed Routing Algorithm for Point to Multipoint VPLS Virtual Connections", Proceedings of the IEEE international Conference, **(2005)**, pp. 1561-1565.
[11] M. EL Hachimi, M.-A. Breton and M. Bennani, "Efficient QoS implementation for MPLS VPN", 22nd International Conference on Advanced Information and Networking and Applications, **(2008)**, pp. 259-263.
[12] H. Lee, J. Hwang, B. Kang and K. Jun, "End to End QoS Architecture for VPNs: MPLS VPN Deployment in a Backbone Network", Proceedings of the International workshop on Parallel Processing, **(2000)**, pp. 479-483.
[13] F. Palmieri, "VPN Scalability over High Performance Backbones Evaluating MPLS VPN against Traditional Approaches", Proceedings of the 8th International Symposium on Computers and Communication (ISCC'03), **(2003)**, pp. 975-981.
[14] L. He and P. Botham, "Pure MPLS Technology", Third International Conference on Availability, Reliability and Security, **(2008)**, pp. 253-259.
[15] S. Alouneh, A. En-Nouaary and A. Agarwal, "Securing MPLS Network with Multi-path Routing", Fourth International Conference on Information Technology, **(2007)**, pp. 809-814.

Authors

Abid Shahzad is a MS CS student at Shaheed Zulfikar Ali Butto Institue of Science and Technology, Islamabad, Pakistan. He has more than 10 years of professional and two years of part time teaching experience. Presently he is working at Askari Bank Limited, Islamabad as Systems Engineer in Data Center. His area of interest includes Networks and Information Security. So, far he has one conference publication in 2009.

Mureed Hussain has first graduated B Sc(Hons) in Applied Physics from the university of Sheffield, England. Soon after his first degree, he developed interest for the computer communication technologies. He obtained his M Sc degree in Computer Networks and Distributed Systems from the University of Aix-Marseille-II- Luminy. Later, he obtained his PhD from the University of Paris5-Rene Descartes- in Information Security. Although main research area of Dr. Hussain is Information security, however, with time he has developed interest in sensor networks and light weight security protocols used for low frequency devices. He is an Associate professor at Shaheed Zulfikar Ali Butto Institue of Science and Technology, Islamabad, Pakistan since 2006 and his teaching subjects involve mathematics, computer networks, cyber security and telecommunication systems.

