MPLS ARCHITECTURE FOR SERVICE PROVIDER

N Rajendran, K Yugandhar, Dr V P Gulati
Institute for development and research in banking technology, MasabTank,Hyderabad-500057,India

Dr S Albert Rabara
St.Joseph's College(Autonomous),Trichirappalli-620002,India

Keywords: MPLS, Label, QoS, Service Provider's Network, Traffic Engineering, VPN

Abstract: MPLS is an emerging backbone technology for service providers, which is being deployed on a large scale in recent days. Using MPLS, service providers can deliver different types of services like TE, QoS and IP VPN along with adequate security according to the specific business demands, across either switched or routed networks. This paper deals with the current problems in service providers' network, overview of the MPLS technology and MPLS architecture for service provider. By deploying the MPLS in the service provider's network, the study reveals that the throughput of the network has been improved with decreased latency for the larger file size.

1 INTRODUCTION

MPLS (Multiprotocol Label Switching) is an Internet Engineering Task Force (IETF) standard for routing traffic, where labels are attached to packets and are forwarded along the paths, which can be as secure as private circuits. The labeled packets are prioritized to provide end-to-end quality of service (QoS) and performance guarantees (Rosen, E. et al., 2001). MPLS is not just another buzzword, but represents a technology that service providers are buying and implementing in their backbone networks. As service providers start to push MPLS into their networks, network professionals will no longer have to build large WAN infrastructures (Hosein F. Badran, 2001).

MPLS utilizes the features of connectionless service and connection-oriented service on to a single bridge, thereby forming a hybrid model (Multiprotocol Label Switching (MPLS), web Proforum Tutorials). MPLS is one of several initiatives for enabling the delivery on the promise of a converged network, by combining the attributes of Layer 2 switching and Layer 3 routing into a single entity. This technology offers the benefits of both conventional IP forwarding and label switching concepts. It has the underlying strength and scalability of IP routing plus circuit switching features such as path optimization and path protection. This allows carriers to design and build networks with appropriate levels of Quality of Service (QoS) and redundancy depending on the customer's business requirements. It also enables carriers to build connectionless IP networks that behave like ATM or Frame Relay networks. By creating virtual circuit-like tunnels, service providers can reap the benefits of ATM's QoS capabilities by reserving bandwidth for mission-critical applications (Victoria Fineberg, 2003).

In this paper a complete architecture of MPLS with IP network has been discussed for service provider's network. Section 2 explains the current issues of the service provider's network. Section 3 illustrates the evolution of the MPLS and its Label switching concept along with the terminology and operations. The architecture of the MPLS for service provider's network including the format of the MPLS Header, Protocol suite, and services like Traffic Engineering (TE), Quality of Service (QoS), Virtual Private Network (VPN) and MPLS security are discussed in section 4. The experimental study

Rajendran N., Yugandhar K., P. Gulati V. and Albert Rabara S. (2004).
MPLS ARCHITECTURE FOR SERVICE PROVIDER.
In *Proceedings of the First International Conference on E-Business and Telecommunication Networks*, pages 183-190
DOI: 10.5220/0001383301830190

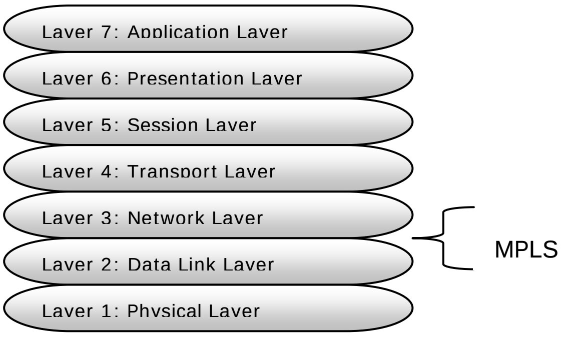

Figure 1: OSI 7 Layer ISO Model

on MPLS and the results are presented in section 5 and section 6 concludes the paper with the benefits for service providers by deploying the MPLS in their network.

2 PROBLEMS IN THE CURRENT IP NETWORKS

In recent years, there is a tremendous growth in the internet users. Due to this, there is an overhead in the IP routing and forwarding operations (Muckai K Girish et al., 2000) mainly in the backbone of the Service Provider's network.

Various issues of the conventional IP networks are presented below:

Scalability: The size of the routing table increases by the addition of routers, which leads to the scalability problem. Moreover, drawbacks of Layer 2 VPN minimize the scalability factor. The limitation of IP version 4 address space forces the enterprises to use Network Address Translation (NAT) and port Address Translation (PAT) to connect their offices which is limited to some applications and increase the latency of the applications.

Performance: The complete packet header is analyzed at every time in all routers. This degrades the performance of the network.

Load: As the number of users getting added to the network increases, there is a heavy load on the router resulting in node failure, link failure etc.

QoS: New applications such as Voice and Video drive the need for guaranteed bandwidth and increased network reliability. These applications require services, which are deterministic in nature i.e. guaranteed service across the complete path in network. Existing protocols do not support these services.

3 CONCEPTS OF MPLS

MPLS (Multiprotocol Label Switching) is a combination of two words 'Multiprotocol' and 'Label switching'. Multiprotocol means that it supports all network protocols like IPX, Apple Talk etc. It has link Layer Independence i.e., it can work over ATM, Frame Relay, SONET, Ethernet, Token Ring, and FDDI etc. Label switching is the basic operation in MPLS; the packets get forwarded based on these labels only.

In Label switching, instead of using a destination address to make routing decision, a number (a label) is assigned to the packet in order to forward it to the destination. Label switching is not a new concept, it has been there for many years, for example tag switching from CISCO systems, IP switching from Ipsilon (Nokia), Aggregate Route-based IP switching (ARIS) from IBM, Cell Switch Router (CSR) from Toshiba and IP Navigator from Cascade Communications.

Different vendors developed their own proprietary label switching technology, which provided better performance and opens wide scope for scalability but interoperability was missing between them. IETF came with a new solution, which provides interoperability between these technologies. The IETF's MPLS working group is responsible for standardizing a base technology for use of label switching (Rosen, E. et al., 2001).

MPLS brings the concept of Layer 2 switching to Layer 3. In the ISO OSI reference model, MPLS will fit between Layer 2 and Layer 3 as shown in the figure 1. MPLS is a hybrid model adopted by IETF to incorporate the best properties in both packet routing and circuit switching. As shown in figure 2 MPLS is a hybrid model through incorporating the

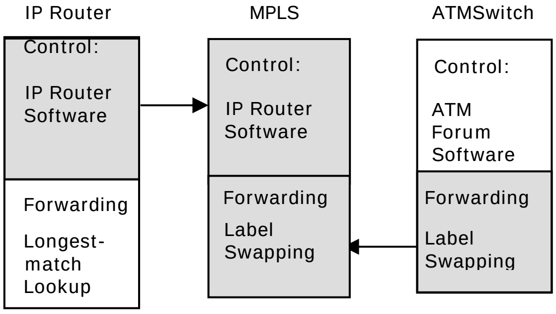

Figure 2: Hybrid model leads to MPLS

features of control plane of the IP and forwarding plane of the ATM (Multiprotocol Label Switching (MPLS), web Proforum Tutorials).

3.1 Terminology in MPLS

It's a different terminology when dealing with MPLS. Following is the list of terminology involved in MPLS, which is specified in RFC 3031(Rosen, E. et al., 2001).

Table 1 Terminology involved in MPLS

Label: A short fixed length physically contiguous identifier, which is used to identify a FEC, usually of local significance.
FEC: Forward Equivalence Class is a group of IP packets, which are forwarded in the same manner (e.g., over the Same path, with the same forwarding treatment).
LER: The entry (Ingress Router) or exit (Egress Router) pointing to an MPLS network are known as label edge routers (LER).
LSR: LSRs (Label Switching Router) are responsible for swapping the labels of a packet to ensure that packet reaches its proper destination.
LSP: Label switched path represents the complete path through a label switched network to reach the destination.
LDP: Label Distribution Protocol is an signaling protocol developed for MPLS
LFIB: Label Forwarding information Base is similar to the routing table in IP network which maintains all the routing information of its neighbors

3.2 Basic Operation of MPLS

All the traffic coming into the MPLS domain enters at the ingress router (LER) and leaves at the egress router (LER). At the Ingress router, each packet is assigned a label and the packet is forwarded through out the MPLS domain based on this label. At each router, the label gets swapped with another label called label swapping, which represents the next router. Finally, when the packet reaches the egress router, it discards the label from the packet and forwards the packet based on the network layer header.

Basic operations of MPLS are shown in figure 3 where all routers are enabled with MPLS, by forming into MPLS domain (Hosein F. Badran, 2001). The steps involved are as follows:

S1.Routing protocols exchange routing information to destination networks

S2.Label Distribution Protocol (LDP) establishes label mappings to destination network.

S3.Ingress LER receives packet and assigns a label to the packets based on FEC.

S4.LSR forwards packets using label swapping.

S5.LER at egress removes label and delivers packet based on the network layer header.

4 ARCHITECTURE OF MPLS

MPLS architecture is the combination of Layer 2 and Layer 3 switching of the conventional IP networks. The steps involved for a data packet to travel through the MPLS domain (Multiprotocol Label Switching (MPLS), web Proforum Tutorials) are:

Label creation and distribution- Label has to be created based on the FEC and it has to be distributed among the routers using protocols like LDP.

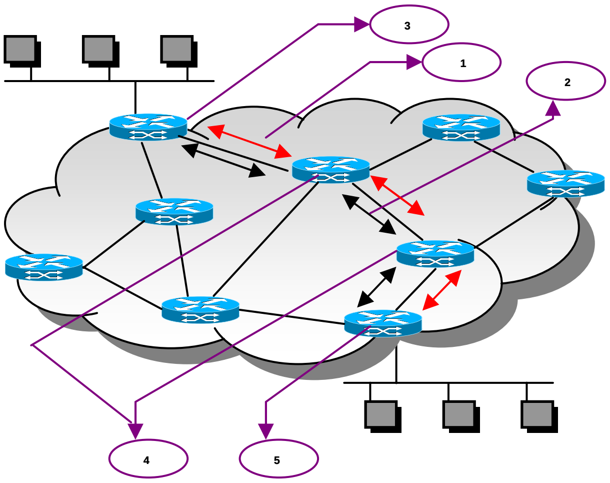

Figure 3: Basic Operations of MPLS

Table creation at each router- LFIB has to be fully populated at each router.

Label-switched path (LSP) creation- Label Switched path has to be established before the packets are forwarded.

Label insertion/table lookup- When a data packet reaches the ingress router, based on the FEC, 'label' is inserted into it and indexed into the LFIB for its next hop.

Packet forwarding- The packet gets forwarded at every router by swapping the label.

In an MPLS domain, not all of the source traffic is necessarily transported through the same path. Depending on the traffic characteristics, different LSPs could be created for packets with different CoS (Class of Service) requirements. The main feature of the MPLS is the separation of the control plane and forwarding plane (Multiprotocol Label Switching (MPLS), web Proforum Tutorials).

MPLS Control plane is responsible for establishing the label switched path by distributing the routing information among LSRs (Label Switched Router) and the procedures convert this information to LFIBs.

MPLS forwarding plane is responsible for forwarding packets based on the values contained in the attached labels. Forwarding plane forwards the packets based on the label forwarding Information Base (LFIB), which is maintained by each MPLS node.

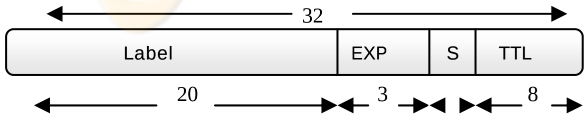

Figure 4: Format of SHIM Header

4.1 MPLS Header

For layer 2 technologies like Ethernet, Token Ring, FDDI, and P-T-P Links etc, the MPLS label is carried in *Shim Header*. The format of the shim header is shown in figure 4.

Shim Header is of 32-bit fixed length, in which Label is of 20-bits and carries the actual value of the MPLS label, experimental field is 3-bits used to represent the QoS to be provided**,** (something is wrong here) label stack is 1-bit used at the time of hierarchical routing and finally TTL field is 8-bits used at the time of loop detection and prevention (Rosen, E. et al., 2001), where TTL is an copy of IP TTL field and it performs the same functionalities of the IP TTL. *Shim header* is placed between the Layer 3 and Layer 2 headers as shown in figure 5 when referred to the ISO reference model (Multiprotocol Label Switching (MPLS), web Proforum Tutorials).

4.2 Protocol Suite

The MPLS protocol suite is classified into two categories:

- Routing protocols
- Signaling protocols

The routing protocols are responsible for the distribution of the routing information among the LSRs

Layer2 Header	SHIM Header	Layer3 Header	Layer4 Header

Figure5: Shim header is placed between Layer 2 header and Layer 3 Header

OSPF, IS-IS, BGP belongs to the routing protocols, where as LDP, RSVP, CR-LDP and RSVP-TE will belong to the signaling protocols The signaling protocols are responsible for the distribution of labels among the LSRs (Victoria Fineberg, 2003). The label binding information is distributed by the protocols LDP or RSVP. LDP is the proprietary protocol developed for MPLS by IETF. It is also possible to use the protocols OSPF, IS-IS, BGP to distribute the label information by extending them.

4.3 Traffic Engineering

Traffic engineering (TE) deals with performance of a network in supporting the network's customers and their QoS needs. MPLS is strategically significant for Traffic Engineering because it can potentially provide most of the functionality available from the overlay models like IP over ATM or IP over Frame relay, in an integrated manner, and also at a lower cost than the currently competing alternatives (RFC 2702). The connection oriented nature of MPLS allows SPs to implement TE in their networks and archive a variety of goals, including bandwidth assurance, diverse routing, load balancing, path redundancy, and other services that lead to QoS (Daniel, O. et al., 1999).

MPLS traffic Engineering can be possible by two different approaches, TE-RSVP and CR-LDP which are currently under the development by the IETF MPLS working Group. CR-LDP is a set of extensions to LDP specifically designed to facilitate constraint-based routing of LSPs. Like LDP, it uses TCP sessions between LSR peers and sends label distribution messages along the sessions. This allows it to assume reliable distribution of control messages. Generic RSVP uses a message exchange to reserve resources across a network for IP flows. The Extensions to RSVP for LSP Tunnels enhances generic RSVP so that it can be used to distribute MPLS labels (George Swallow, 1999).

4.4 Quality of Service

MPLS is frequently mentioned among major Quality of Service (QoS) technologies for packet networks. MPLS doesn't define a new QoS architecture; most of the work on MPLS has focused on supporting current IP QoS architectures (Haeryong Lee. et al., 2000). In MPLS the QoS can be archived in two ways

- Integrated Services (Intserv)
- Differentiated Services (DiffServ)

IntServ (Nicolas Rouhana et al., 2000) defines per-flow QoS and uses RSVP as the signaling mechanism used by applications to request QoS from the network. MPLS can support per-flow QoS with the extensions made to RSVP to propagate bindings between flows and labels. The way to solve the QoS problem by integrated services alone has been recognized as hardly scalable, due to its need to store per-flow state at each router, and requires substantial changes in the existing Internet architecture.

DiffServ (Le Faucheur, F et al., 2002), defines a QoS architecture based on flow aggregates that requires traffic to be conditioned and marked at the network edges (Ingress node) and internal nodes to give different QoS treatment to packets based on their markings. MPLS packets need to carry the packet marking in their headers because LSRs do not examine the IP header during forwarding. A 3-bit experimental field in the MPLS shim header as shown in figure 4 is used for this purpose. The DiffServ functionality of an LSR is almost identical to that provided by an IP router with respect to the QoS treatment given to packets (per-hop behavior in DiffServ terms) (Victoria Fineberg, 2003).

4.5 Security in MPLS using Virtual Private Network Services

A virtual private network means a private multi-site network created by using shared resources within a public network. Conventional VPNs are based on creating and maintaining a full mesh of tunnels or permanent virtual circuits among all sites belonging to a particular VPN, using IPSec, L2TP, L2F, GRE, Frame Relay or ATM. MPLS based VPNs, which are created in Layer 3, are connectionless, and therefore substantially more scalable and easier to build and manage than conventional VPNs (RFC 2547bis, 2001).

MPLS is becoming a more widespread technology for providing virtual private network (VPN) services; Components in MPLS VPN are Customer Edge (CE) and customer (C) routers, which placed at the customer end and Provider edge (PE) and Provider (P) routers, which are placed at service providers end. CE and PE routers are useful to establish a VPN connection. Service providers' MPLS VPN Architectural components are shown in the figure 6.

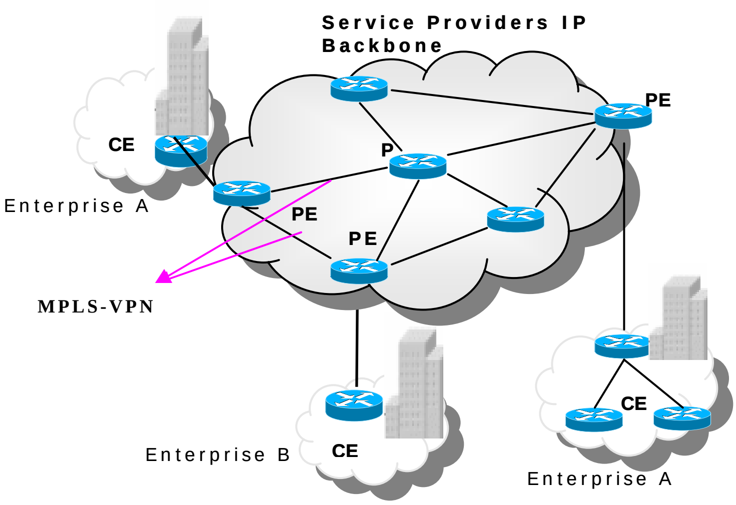

Figure 6: Service Providers MPLS VPN Architectural Components

With the deployment of MPLS VPN, both the service providers and customers are benefited in many ways.

MPLS VPNs provide a platform for rapid deployment of additional value-added IP services, including Intranets, Extranets, voice, multimedia, and network commerce. MPLS VPNs offer seamless integration with customer intranets and have increased scalability over current VPN implementations, with thousands of sites per VPN and hundreds of thousands of VPNs per service provider. MPLS VPNs provide IP Class of Service (CoS), with support for multiple classes of service within a VPN, as well as priorities amongst VPNs. MPLS VPNs offer easy management of VPN membership and easy provisioning of new VPNs for rapid deployment (Jon Harrison, 2003).

MPLS architecture security is of increasing concern to service providers and VPN customers (Cisco systems , Security of the MPLS Architecture). While MPLS based services are replacing the traditional Layer 2 VPNs such as ATM or Frame Relay, at least they should provide the same level of security as of Layer 2 VPNs. Service Providers offering MPLS services have specific demands for the security of this special VPN solution.

Hiding MPLS core structure: The internal structure of the MPLS core network i.e. provider edge (PE) and provider (P) elements should be invisible to outside networks. The only information required between the customer edge (CE) and provider edge (PE) for a routing protocol is the address of the PE router. Except the IP address of PE or interface of the CE, all the remaining information like topology, addresses of provider (P) routers are hidden from the outside world. MPLS does not reveal unnecessary information outside, not even to customer VPNs (Cisco systems , Security of the MPLS Architecture)

Resistance to Attacks: Attacks in MPLS can be possible through the routing protocols. A potential attack could be to send an extensive number of routes, or to flood the PE router with routing updates. Both of these attacks could lead to Denial of Service (DoS). To overcome this problem, ACLs should be defined such that the routing protocol allows traffic from the CE and not from anywhere else. The next measure is configuring Message Digest 5 (MD5) authentication for routing protocols. This MD5 is available for BGP [RFC2385], OSPF [RFC2154], and RIP2 [RFC2082]. Along with the routing protocols, authentication configures the LDP authentication also, and maximum number of routes accepted per virtual routing and forwarding instance (VRF) should be configured wherever possible (Cisco systems , Security of the MPLS Architecture).

Impossibility of Label spoofing: In MPLS, the packets get forwarded based on the labels rather than IP address. So the question here is whether it is possible to spoof label (insert wrong labels into the MPLS network from outside) like IP spoofing? It may be possible if one knows the MPLS core structure. As discussed earlier MPLS core is hidden from the outside world (Ravi Sinha, 2003)). Apart from this for security reasons, a PE router should never accept a packet with a label from a CE router. So if any labeled packet comes from the CE the packet is dropped at the PE.

IPSec: IPSec provides an additional security over an MPLS network (Paul Brittain, 2000)). By using the IPSec on top of the MPLS infrastructure, it provides

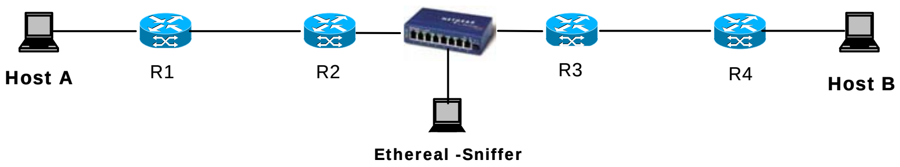

Figure 7: Set up for analyzing the traffic between routers when MPLS is enabled

encryption of parts or all traffic over the MPLS core, so that the attacker can't sniff traffic on the core. IPSec provides the *Authentication* of the end points (probably the CE routers) and the *integrity* of the traffic, which means packets can't be changed on their way through the core without the change being noticed. It also provides the *Replay* detection, so if IPSec Authentication Header (AH) is used, an attacker cannot save packet flow and reply it later.

MPLS networks on their own provide a high level of security when compared to Layer 2 VPNs. However MPLS does not support encryption, integrity, and authentication. By configuring the IPSec over MPLS, the drawbacks mentioned above can be archived (Cisco systems, Security of the MPLS Architecture).

5 EXPERIMENTAL RESULTS

A test bed has been setup using four Cisco 3745 routers as shown in figure 7. All the routers should be upgraded with Enterprise IOS of Cisco for enabling MPLS. Ethereal is the sniffer used to sniff the data between the routers. Different sizes of files like 2MB, 4MB, 6MB, 9MB, 11MB and 23MB are transferred from one end to other end and the traffic between the routers is captured and analyzed using ethereal sniffer. MPLS is enabled on links except Host-to-Router links. The IGP protocol used is OSPF. It is observed that the elapsed time to transfer a file from one end to other end is less when MPLS is enabled on the routers when compared to general IP network.

The elapsed time is varying along with the size of the file, when the file size is small the elapsed time is almost same as the size of the file increases the time also differs. As this set up is small not much difference is recorded. The difference between both the elapsed times is plotted as shown in the figure 8. Similarly the throughput of the traffic is calculated from average number of packets forwarded per second. This analysis is carried out by comparing with general IP network i.e. once without MPLS and once with MPLS. It is observed that average number of packets get switched are high by enabling MPLS compared to the IP network. The results are plotted in Figure 8a and 8b.

6 CONCLUSION

MPLS is an emerging standard rapidly gaining acceptance by both vendors and Service Providers. In this paper, it has been addressed the importance issues of MPLS such as speed scalability, service guarantee and security. The packets get processed faster when Using MPLS because of bringing the speed of layer 2 to layer 3. Since MPLS supports the concept of hierarchy, it is easy to scale the network when compared to other networks. VPN architecture of MPLS also helps the scalability. Packets can be assigned a priority label, making Frame Relay and ATM like quality of service guarantee is possible. Packets travel along tunnels in a public network, which are a foundation for Virtual

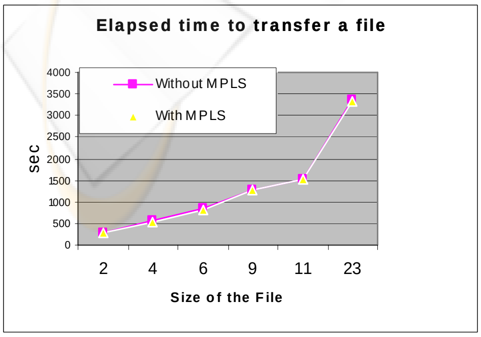

Figure 8a: Time taken to transfer a file

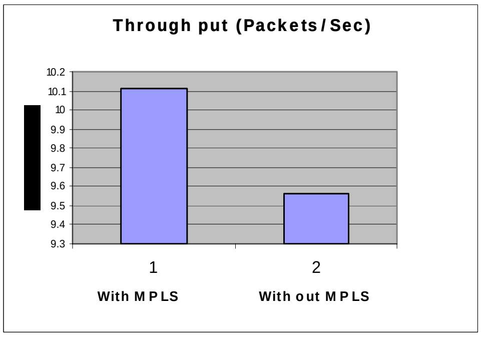

Figure 8b: Average number of packets per second

Private Networks (VPNs) provides the security along with the protocols like IPSec.

This paper addressed the problems of existing networks mainly IP networks and how service providers can overcome them by deploying the MPLS in their backbone. There is greater scope for improvements in this technology and more features could be embedded. We intend to refine the architecture and continue our developments efforts.

REFERENCES

Rosen, E., Viswanathan, A., Callon, R., (2001). *RFC 3031 Multiprotocol Label Switching Architecture*

IEC. *Multiprotocol Label Switching (MPLS)*, web Proforum Tutorials.

Dr. Hosein F. Badran., (2001). *Service Provider Networking Infrastructures with MPLS*, Proceedings of the Sixth IEEE symposium on computers and communications (ISCC'01).

RFC 2702., *Requirements for Traffic Engineering Over MPLS*

George Swallow, *(*December 1999). *MPLS Advantages for Traffic Engineering*, Cisco Systems, IEEE Communications Magazine

Muckai K Girish., Bei Zhou and Jian-Qiang Hu., (2000, May). *Formulation of the Traffic Engineering Problems in MPLS Based IP Networks*, Proceedings of the Fifth IEEE Symposium on Computers & Communications (ISCC'00)

Daniel, O., Awduche., (1999, December). *MPLS and Traffic Engineering in IP Networks*, UUNET (MCI Worldcom), IEEE Communications Magazine

IEC.,*A Comparison of Multiprotocol Label Switching (MPLS) traffic Engineering Initiatives*, web Proforum Tutorials

Xipeng Xiao., Alan Hannan., Brook Bailey., Lionel, M., Ni, *Traffic Engineering with MPLS in the Internet*, Global Center Inc, A Global Crossing Company 141 Caspian Court, Sunnyvale, CA 94089

Le Faucheur, F (Editor)., Wu,L., Davie, B., Davari, S., Vaananen, P., Krishnan, R., Cheval, P., Heinanen, j., RFC 3270, (2002, May). *Multi-Protocol Label Switching (MPLS) Support of Differentiated Services.*

Nicolas Rouhana, Eric Horlait, (2000). *Differentiated services and Integrated Services use of MPLS*, Proceedings of the fifth IEEE Symposium on Computers and Communications (ISCC'00)

Haeryong Lee., Jeongyeon Hwang., Byungryong Kang., Kyoungpyo., (2000, June). *End-to-End QoS Architecture for VPNs: MPLS VPN Deployment in a Backbone Network*, Proceedings of the 2000 International Workshops on Parallel Processing (ICPP'00 - Workshops)

Victoria Fineberg, (2003, May). *QoS Support in MPLS Networks*, MPLS/Frame Relay Alliance White Paper

Ramesh babu., Prabagaran & Joseph, Evans, B., (2001). *Experiences with class of Services (CoS) translations in IP/MPLS Networks*, Proceedings of the 26th Annual IEEE Conference on Local Computer Networks (LCN'01)

Nino Kubinidze., Mairtin o'Droma. *Multiprotocol Label Switching QoS in IP Networks* Electronic and Computer Engineering Department, University of Limerick, Ireland

Brian Williams., (2000, March). *Quality of Service Differentiated Services and Multiprotocol Label Switching*, Ericsson Australia

Ravi Sinha., (2003). *MPLS - VPN Services and Security*, SANS Institute

RFC 2547bis., (2001). *BGP/MPLS VPN Fundamentals*, White Paper, Juniper Networks, Inc

Jon Harrison., (2003, February). *VPN Technologies-A Comparison*, Data Connection Ltd

Paul Brittain., MetaSwitch., Adrian Farrel., (2000, November). *MPLS VIRTUAL PRIVATE NETWORKS-A review of the implementation options for MPLS VPNs including the ongoing standardization work in the IETF MPLS Working Group*, Data Connection Limited

Cisco systems . *Security of the MPLS Architecture* , http://www.cisco.com/en/US/tech/tk436/tk428/technologies_white_paper09186a00800a85c5.shtml