International Journal of Sciences: Basic and Applied Research (IJSBAR)

ISSN 2307-4531

http://gssrr.org/index.php?journal=JournalOfBasicAndApplied

Internet Protocol/MultiProtocol Label Switching (IP/MPLS) Networks

Engr. Sajjad Hussain[1]*, Engr. Muhammad Tariq Javed [2]

[1]Department of Electrical Engineering

[2]Department of Electrical Engineering

APCOMS affiliated with University of Engineering and Technology TAXILA, Pakistan

[1]Email:engineer.sajjadhussain@gmail.com

Abstract

This paper discusses different aspects of Multi-Protocol Label Switching (MPLS) networks. In this paper, we first discussed MPLS in detail, the technology was developed to advance the IP networks reliability, efficiency and controllability to meet the requirements of next generation networks and its flexibility allow the service providers to transport converged services over a single packet infrastructure. Further we discussed the IOS mechanisms to design an MPLS system for Traffic Engineering (TE), and IPv6 support in MPLS standards to solve the issue of IPv4 to IPv6 transition process. This document details a MPLS Virtual Private Network (VPN), a service that offers managed secure connectivity between corporate sites. Our discussion also includes different issues regarding Quality of Service (QoS) in a network with MPLS.

Keywords: Internet Protocol, MultiProtocol Label Switching, (IP/MPLS) Networks.

I. OVERVIEW OF IP/MPLS NETWORKS

MPLS is an elegant solution for the problems that are present in today networks, e.g. speed, scalability, traffic engineering and quality of service (QoS) management. MPLS is also a versatile solution to meet the requirements related to service requirements and bandwidth management for the next generation IP based core networks [1].

MPLS is an emerging technology which enhanced the capabilities of large scale IP networks and the routers forwarding speed is also increased. Over the last few years the internet is used everywhere and is required a variety of new applications that can fulfill the business and enterprise network requirements. This variety of applications requires the guaranteed speed and bandwidth. The exponential growth in users and volume of traffic is a great challenge to the existing internet infrastructure. Despite these initial challenges and to meet the service and bandwidth requirements through the next generation networks MPLS will have to play an important role in packet forwarding, switching and routing.

---

* Corresponding author.

E-mail address: engineer.sajjadhussain@gmail.com.

A. How MPLS Works

MPLS works on packets and each packet has labels which have properties related to IP forwarding. The protocols results with IP switched paths are called LSP. The Label Switch Router (LSR) can follow specific topological routes and other constraints such as resource availability and explicit routes by using IP routing protocols and then set up the paths across the network. The traffic is mapped onto LSP and then the MPLS follows these predefined paths and forwards the data by label swapping. In label swapping the MPLS monitors the incoming label and input port and swap it with outgoing label and output port and this is independent of the encapsulated IP header fields. Another important MPLS aspect is that the LSPs can work on many link layers types such as frame relay, Ethernet and ATM.

All LSRs are not equal they vary in their capabilities like paths, services management, congestion and network failure. LSR specify these capabilities and shows the implementation of MPLS. Some LSRs are designed and programmed for the traditional best-effort services related to internet level services, some LSRs are specifically designed to handle business class IP, video, or voice services. For the purpose of fully utilizing of the capabilities of an MPLS-enabled IP network, first of all LSRs should be reliable and predictable in performance behavior and must support the TE and TE functions in fully advanced range.

B. MPLS vs. Traditional IP forwarding

In traditional IP forwarding, Layer 3 routing information is distributed by using routing protocols. The packets are forwarded based on the destination address only and routing lookups based on only destination address are performed on every hop. Also every router may need full routing information.

MPLS is a label based forwarding mechanism and routing of packets is done according to their labels. Like traditional IP forwarding mechanism Packets labels may rely on IP destination, but it is possible that labels may have correspondence to other parameters such as Quality of Service (QoS) or source address. MPLS design also support the transportation of other protocols. In MPLS the routers that are on edge must perform routing lookup, the routers that are internal to the network, switch packets and swap labels based on simple label lookups.

C. System architecture:

MPLS is a technology that combines layer 2 and layer 3 capabilities of switching and routing respectively. At the beginning it was used to improve forwarding speed. It was originated from IPv4 and MPLS key technologies can be extended to multiple network protocols, such as internet packet exchange (IPX), IPv6 and appletalk. There are two main components of MPLS:

a. Control Plane

Control plane Exchanges routing information of layer 3 and labels. Control plane contains complex mechanisms or protocols to exchange routing information that are OSPF, EIGRP and BGP, and to exchange labels like Tag Distribution Protocol (TDP), Label Distribution Protocol (LDP), BGP and Resource Reservation Protocol (RSVP). The control plane maintains contents of Label-Switching table.

b. Data Plane:

Data plane has a simple forwarding engine [3].

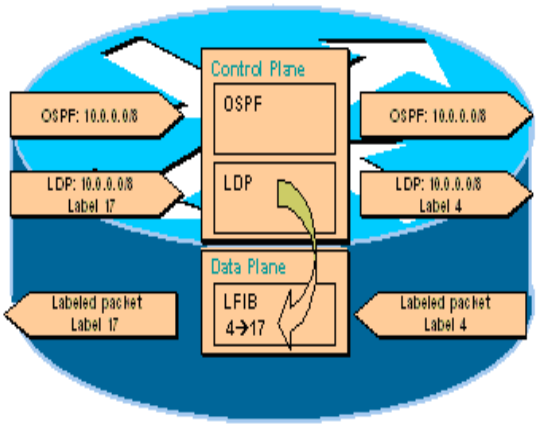

Figure 1: MPLS Architecture

D. Basic Concepts:

Some basic concepts of MPLS Technology are as follows:

a. Forwarding Equivalent Class

The MPLS forwarding technology is based on classification. It classifies the packets into a category that fall in the same forwarding mode; this category is called Forwarding Equivalent Class (FEC). In MPLS the packets are treated the same that are related to same FEC. The Packets are grouped together that have identical source and destination address, protocol type, VPN source port, destination port, or any combinations of these.

b. Labels

A label is a fixed-length short identifier and it is used to identify a specific FEC. It is of local significance. There may be a case of more than one label that is called label stack. The label contains no topology information. A label contains four bytes. The format of MPLS label is shown in Figure 2.

Figure 2: MPLS Label Format

There is the following information that is contained by MPLS 32 bit label field:

- 20 bit label (a number)
- the experimental field of 3 bit which is used to carry the value of IP precedence
- the bottom of stack indicator of 1 bit which is denoted here as S and it indicates whether this is the last label before the IP header
- 8 bit TTL

c. Label Switch router (LSR):

In MPLS network the basic element is LSR. The LSR is made up of a forwarding plane and a control plane. Exchanging routing information and labels is part of control field and forwarding of packets (LSR and Edge LSR) or cells (ATM LSR and ATM edge LSR) is the part of forwarding plane.

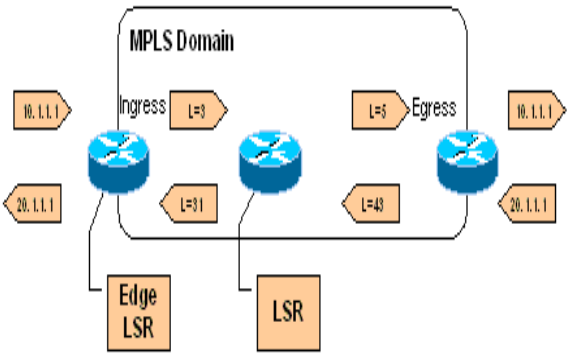

Figure 3: Working of LSR in MPLS

The routing table and a label mapping table for LSRs is created by routing protocols such as OSPF, ISIS. The ingress LSR or edge router receives a packet, examines its FEC and then adds a label to the packet. The transit LSR forwards the packet according to its label and the label forwarding table. The Egress LSR takes off the label and forward the packet [3].

II. The Role of IP/MPLS Technology

in Next Generation Networks

Now businesses everywhere are using the Internet and to fulfill their business requirements they have a need of value-added services from their service providers. The new businesses focus for Internet service providers has new requirements that include reliability, performance and the ability to deliver differentiated levels of services. This time in the internet the users, traffic, ISP networks and new applications are increasing continually and due to this there is a huge demand on the Internet infrastructure and the service providers whose networks constitute the Internet. we can now have update our networks by simply adding more bandwidth to handle the load, but it is uncertain for the network performance, now the time is remove these uncertainties and to focus on increasing efficiency in network performance. The purpose of MPLS technology is to improve the reliability, and efficiency and thereby profitability of IP networks. [4]

A. MPLS Path towards Convergence

The switching and routing technology have strength to converge the networks. When routers and switches are combined in a network then they can build a converged network. There are some weaknesses in routers such as traffic management and it can be recovered by switches. Similarly router can recover switch weaknesses e.g. switches are weak in situation of large number of paths that can overcome by dynamic route selection ability of routers.

B. IP Networks Today

The internet service demand is increasing day by day and it is the real challenge is that how we scale the network usage and to improve the performance with less expenses. The managing of network changes at both routing and switching layer also requires incremental cost and effort.

In a fully meshed router network there are many virtual circuits between routers and it seems that each router is adjacent to all other routers. So when the number of users increase and the number of routers will also increase. This increase in the number of adjacencies there is created stress of scaling and stability of routing protocol.

The bandwidth requirement can also met in a number of ways which includes high capacity ATM switches and high capacity and high performance routers. IP routers are able to integrate a large mesh into a number of smaller meshes. MPLS provides the solution for the next generation of networks by consolidating the switching and routing together between IP and Layer 2 [4].

III. Network Convergence over MPLS

MPLS is a very flexible technology in which over a single packet infrastructure it is easy to transport voice, IPv6 and layer 2 services ATM, Frame Relay and Ethernet etc. This is the solution to the network convergence problem that is an old problem of networks. MPLS has capabilities like traffic engineering, fast restoration and quality of service support. These capabilities provide each service with strict service-level agreements (SLAs) cost-efficiency [5].

A. Voice Transport over MPLS

Voice packets can be transported in MPLS and they do not include the overhead associated to the typical RTP/UDP/IP encapsulation. When in case of end points e.g. between two same gateways the voice communications are transported, before labeling and transmission the voice packets are concatenated. This helps to reduce the encapsulation overhead.

There are different algorithms that are used to compress the RTP/UDP/IP headers in IP. There are different protocol layers e.g. Composite IP (CIP) and Lightweight IP Encapsulation (LIPE). In these protocol layers the concatenation may be implemented. The CIP and LIPE concatenate voice packets above IP while Point-to-Point Protocol Multiplexing (PPPmux) concatenates voice packets at layer 2.

There are two main solutions that are proposed in voice over MPLS for concatenation. The first one supports transport of multiplexed voice channels, silence removal and silence insertion descriptors, various voice compression algorithms transfer of channel associated signaling and dialed digits. The voice packets that are concatenated are preceded by a 4-octet header. This header includes a channel identifier, a payload type, a counter, and a payload length field. If there is the case that the payload length is not a multiple of 4 octets, then to make it a word (32 bits) aligned, up to 3 pad octets are included. Up to 248 calls can be multiplexed within a single LSP identified by the outer MPLS label there can be up to 248 calls multiplexed.

The second solution addresses similar functions, but instead of defining a new voice encapsulation like , it reuses components of the ATM Adaptation Layer type 2 (AAL2), defined for transport of several variable bit rate voice and data streams multiplexed over an ATM connection.

IV. IP-MPLS TRAFFIC ENGINEERING

Using Traffic Engineering (TE) methodologies traffic flows can be controlled in such a way that network performance and resource utilization can be optimized. TE is helpful to ISPs to route network traffic in an organized manner that they can provide the best service to their customers in terms of delay and throughput.

MPLS is an advanced forwarding scheme, using MPLS routing mechanism extends with respect to path controlling and packet forwarding. A header is included in each MPLS packet which contains 20-bit label in non-ATM networks, 3-bit *Experimental* field, 1-bit label stack indicator and 8-bit TTL field. While considering ATM Networks, MPLS header consists of a label encoded in VCI/VPI field. *Label Switching Router* (LSR) examines the label and perhaps the experimental field while forwarding packets in the network [10].

MPLS traffic engineering accounts for the amount of traffic flow while determining explicit routes across the network backbone and for link bandwidth. MPLS provides a dynamic adaptation mechanism which has a complete solution to TE a backbone. Fault occurrence is minimized in the backbone with the help of this mechanism, even though several primary paths are precalculated offline. RFC 2702 discusses the requirements for TE in MPLS networks.

A tunnel is automatically establishes and maintains by MPLS TE across the backbone using Resource Reservation Protocol (RSVP), for given tunnel a path can be determined at any instant of time by using the network resources and tunnel resource requirements such as bandwidth. If the traffic flow is so large that it can't be carried out by a single tunnel then multiple tunnels between a given ingress and egress can be configured to load shared the traffic among them.

A. IOS mechanisms for MPLS TE

IOS mechanisms for MPLS Traffic Engineering as discussed in [11] are as follows:

- Label Switched Path (LSP) tunnels, which are signaled through RSVP, with TE extensions. LSP tunnels are represented as IOS tunnel interfaces, have a configured destination, and are unidirectional.
- A link-state IGP (such as Intermediate System to Intermediate System (IS-IS)) with extensions for the global flooding of resource information, and extensions for the automatic routing of traffic onto LSP tunnels as appropriate.
- An MPLS TE path calculation module that determines paths to use for LSP tunnels.
- An MPLS traffic engineering link management module that does link admission and bookkeeping of the resource information to be flooded.
- Label switching forwarding, which provides routers with a Layer 2-like ability to direct traffic across multiple hops as directed by the resource-based routing algorithm.

MPLS TE supports preemption between TE LSPs of different priorities. Each TE LSP has a setup and a holding priority, which can range from zero (best priority) through seven (worst priority). Recent advancements in MPLS technology open new possibilities to illustrate the limitations of IP systems regarding TE. Though MPLS is a simple technology which based on classical label swapping paradigm. It introduced the sophisticated control capabilities that advance the TE function in IP Networks.

V. TRANSITIONING TO IPV6 USING IP-MPLS NETWORKS

IPv6 is in the market for quite some time but NAT extended the life of IPv4, the deployment of IPv6 is delayed due to lack of motivation and that most vendors did not support IPv6. However in the recent years large number of different types applications (e.g. Point to Point) are developed and NAT is no longer sufficient. Internet users are

increased enormously due to DSL and now a day's not only PCs can connect to the internet but 3G mobile devices also use internet. So the use of IPv6 is now boosted, vendors now support IPv6, and ISPs deploy IPv6 services.

MPLS system can be used to forward IPv6 traffic in the IPv4 network, the complete scenario is illustrated in Figure 4 [12]. The steps are:

- From Router-B to Router-A, a tunnel is built by advertising the following IPv4 address: "12.128.76.23".
- Router-A assign a green label (four-octet MPLS label with label value) to the IP "12.128.76.23".
- Then IPv6 packet is forwarded.
- The green label is added instead of encapsulating the IPv6 packet in IPv4 format, and Router-A determines that packet must be forwarded to Router-B.
- Router-C replaces the green label with the purple label.
- Router-D replaces the purple label with the blue label.
- Router-B strips and send IPv6 packet to its destination.

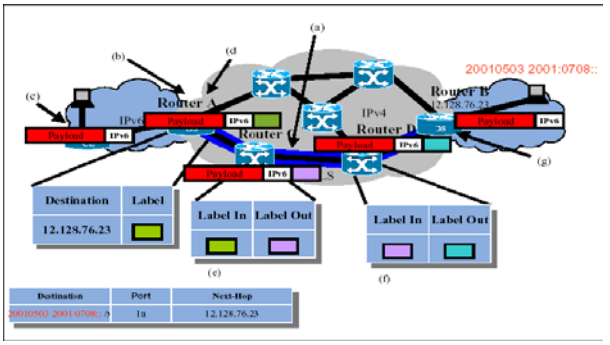

Figure 4: IPv6 traffic forwarding in IPv4 network using MPLS

A. Transition Mechanisms

The most debated topic among the Internet Engineering Task Force (IETF) is the transition from IPv4 to IPv6, and if not forever how long it is possible that both versions will coexist. Types of transition mechanisms include [12]:

a. Dual-Stack

In this mechanism both IPv4 and IPv6 protocol stacks exist in the same terminal or network equipment.

b. Tunneling

The mechanism is mainly used to tunnel traffic between two IPv6 hosts through IPv4 network, or vice-versa.

c. Translation

Using translation mechanism an IPv4 host becomes capable to talk to an IPv6 host.

B. Configured Tunnel

Configured tunnels may be used for those sites that regularly exchange traffic to connect IPv6 hosts over current IPv4 network, IPv4 headers are used to encapsulate the IPv6 packets. The destination of encapsulating router is the endpoint of configured tunnel, tunneling is illustrated in Figure 5.

IPv6 hosts can communicate over the existing IPv4 network via MPLS Circuit Cross-connect mechanism, point-to-point configured tunnel can be used for information sharing. MPLS header is used to encapsulate the IPv6 packets. Ingress router need to be configured with the tunnel address.

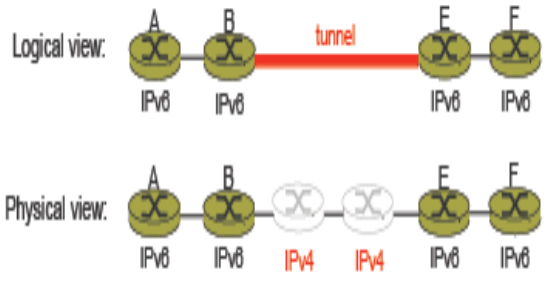

Figure 5: Tunneling

MPLS platform is also reliable and economical solution to transport the IPv6 traffic on existing IPv4 network, service providers can get benefit from this method by just enabling IPv6 on the Provider Edge (PE) router, no other alternation needed in their existing IPv4/MPLS network (scenario is illustrated in Figure 6), this will help the service providers to offer IPv6 services to their customers without any complexity and extra operational cost, it will also help them to optimize their existing network by minimizing the number of IPv6 enabled devices required in their network [13].

Figure 6: IPv6 over MPLS

The MPLS is widely noticed as a technology for the next generation Internet that provides speed and functionality in packet forwarding. However, as a result of the rapid deployment of the MPLS technology, a rack of IPv6 support in MPLS standards is rapidly emerging as a practical issue in the IPv4 to IPv6 transition process.

VI. Comprehensive MPLS VPN

Solutions

A. Overview of VPN Networks

The VPN market is growing on regular bases at a record pace worldwide. IDC reports that provider-provisioned VPNs now dominate the VPN services market with VPNs deployed by over half of the multisite companies that

have 50 or more employees. The worldwide VPN services market reached to handsome amount of $24.4 billion in year 2007 and is expected to climb to almost $36 billion in year 2012. In the U.S. alone, it is estimated that the VPN market will have a 10.4 % increase over the next five years [15].

A VPN is a network in which customers from different sites are get connected on a shared network, the access and security policies are same for VPN as a private network. VPN has a great impact on business world as a result the growth rate of VPN infrastructure is very fast, its also provide the alternate solutions to expensive leased-lines or circuit-switched networks [17].

To solve the scalability issue in VPN networks, a new VPN based standard protocol known as border gateway protocol / Multiprotocol label switching (BGP/MPLS) is introduced which provide network layer VPN solutions using BGP to carry routing information on MPLS infrastructure. Using this Layer 3 MPLS-VPN solution the traditional Layer-2 security approach is maintained and scalability is increased due to Layer-3 routing technology. The key benefit of the new approach is the use of Border Gateway Protocol and a set of extensions, known as BGP-VPN, which help to maintain distinct routing and forwarding information for each VPN client. BGP use label distribution protocol (LDP) to carry that information over MPLS infrastructure [19].

B. MPLS VPN Overview

MPLS VPN offers managed and secure connectivity among the corporate sites. MPLS VPN is the world wide de facto standard technology which replaces the old traditional technologies such as data link layer Switch Network and WAN.

MPLS VPN Service Providers allows the network traffic to be differentiated according to class of service (CoS) parameters via the Internet backbone. The CoS mostly comes in Video Conferencing, Multimedia, Platinum, Gold and Silver editions. The key advantage of CoS system is to prioritized the user traffic according to the class, hence business critical traffic is not affected by other traffic and at the same time cost efficiency is maintained by offering lower and economical CoS to the customer where appropriate, each CoS has it own set of SLA's which are based on packet loss, jitter, latency and availability of the network [14].

MPLS VPN service can be defined as [16]:

- Provider Edge (PE) - Customer Edge (CE) protocol and the protocol-specific configuration.
- Allocations of IP Addresses
- Customer Edge router should be configured in case of managed CE.
- Customer Edge routing protocols should be redistributed
- Provider Edge routing protocols should be redistributed
- Option of joining the Management VPN
- Provider Edge router must be configured for Virtual Routing and Forwarding Instance (VRF) (VRF should be configured for maximum number of routes, and VRF routing table should me maintained for import and export maps).

C. MPLS VPN Model

MPLS-VPN model is also known as "true peer VPN" model, traffic separation is performed at Layer-3 in this model, and a separate IP/VPN table is maintained for forwarding purposes. A unique VRF is assigned to each customer's VPN to separate the traffic from different customers. This feature of MPLS-VPN is comparable to the security of a Frame-Relay and ATM networks, because the users from different VPNs can't see the traffic of each other.

Forwarding in the service provider backbone is performed on the bases of labels. MPLS set these label switched paths (LSPs), which starts and ends at the Provider Edge router while normal routing is performed on the Customer Edge router. Packet handling is performed by PE router on its incoming interface with the help of forwarding table

because each incoming interface of a PE router is associated with a particular VPN. Hence a packet can be entered in a VPN through an associated interface.

In this model no tunneling or encryption is needed for traffic separation because it is directly built into the network itself. The route distribution is controlled by Provider Edge routers with the use of Extended BGP community attributes. Provider Edge routers assign a label to each VPN customer route and distribute these labels with other Provider Edge routers, which assures that packets are directed to the correct egress Customer Edge router.

During packet forwarding process two labels are used. Top label is used to direct the traffic to the correct Provider Edge router and the second label is the indication that how the Provider Edge router should handle that particular packet. After the completion of above process MPLS forward the packet over its backbone using dynamic IP paths or TE paths.

For the sack of simplicity standard IP forwarding mechanism is used among the Provider Edge and Customer Edge routers. Provider Edge router maintains a VRF forwarding table which contains only set of routes available to that Customer Edge router. Customer Edge router is a routing peer of directly connected Provider Edge router but not a routing peer of Customer Edge routers exists at other sites. Routing information does not exchanged directly between the routers of different sites. The benefit of this approach is that it allows the simplification of route configuration at individual site while considering large VPNs [17].

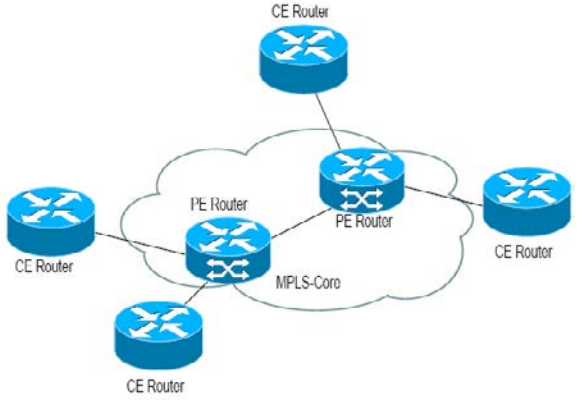

Figure 7: MPLS-VPN

D. Requirements of a Secure Network

MPLS/VPN based solutions and traditional layer 2 based VPN solutions can be compared on following key security requirements [17].

- Addressing and routing should be separated from each other.
- Internal structure of MPLS/VPN core network should be kept secret from outside. Just like Frame-Relay and ATM network backbone is hidden.
- The network should be capable to resist against both Denial-of-Service (DoS) and intrusion attacks.

VI. QUALITY OF SERVICE (QOS) FOR MPLS NETWORKS

The increase in the convergence of network services leads directly to the need for Quality of Service (QoS) approach. QoS is defined as, "the ability of a network to recognize different service requirements of different application traffic flowing through it and to comply with Service Level Agreements (SLAs) negotiated for each of the application services, while attempting to maximize the network resource utilization". QoS has an important role in a multi-service network, in order to meet SLAs of different services.

If QoS is not implemented, datagrams are serviced in a network on a first-in, first-out (FIFO) basis, also known as *best-effort service*. Priority is not assigned to the datagrams in such scenario, based on the type of application that they support. As a result, differential treatment for different types of application traffic can't possible. Therefore, SLAs for any service other than best-effort service cannot be met. QoS maximizes network resource utilization and optimizes revenue generation by providing priority access to network bandwidth for high-priority traffic, and by allowing low-priority traffic to gain the bandwidth committed to high-priority traffic in the absence of high-priority traffic.

A. MPLS QoS Architecture

MPLS does not define new QoS architecture; it uses Differentiated Services (DiffServ) architecture defined for IP QoS. DiffServ architecture is defined in RFC2475, MPLS support for DiffServ defined in RFC3270. As MPLS is a selected choice for next generation multiservice networks. So, MPLS QoS architecture must fit mutiservice strategy and must be flexible and scalable [22].

At present time QoS has a key role in implementation of IP and MPLS networks. But QoS is one of the complex features of networking. With the advancement in technology today networks support multiple applications and multiple network services over a standalone converged network. Therefore QoS plays an important part when network design and different operations are implemented.

Initial design of IP infrastructure supports the connectionless services for packet routing in which each packet flows via independent path over the network to reach the destination. The design did not include TE mechanism, resource reservation protocol and no support was implemented to meet the requirements of differentiated services. To improve the efficiency of QoS, MPLS with label was introduced that supports connection-oriented switching. The design of MPLS supports scaling, provides TE and rerouting mechanisms within the IP domain.

B. Working towards QoS

Several issues arise within transport services while transferring the user and control-plane data over the networks. In most cases services are provided through wired or wireless networks. One of the major issues at transport layer is how to ensure the reliability and predictability of QoS for time critical applications over the IP network infrastructure which is basically designed for connectionless data transport. This problem is somewhat solved by running IP-over-ATM, and using the built-in ATM Quality of Service mechanisms. But this approach has some limitations on carriers which do not implement ATM.

To deliver the QoS over IP infrastructure an early stage intelligence service layers schemes known as MPLS is developed. Using MPLS service providers can define specific packet delivery paths to transport the traffic via IP networks, and there is no need of intermediate routers for packet-forwarding. Traditional routing mechanism route the traffic via shortest and less congested path through the network, but using MPLS system the network response time and traffic load can be balanced more efficiently [23].

In MPLS explicit paths are set to solve the QoS problem through the network. In other words we can say that MPLS integrate the best effort delivery IP technology to connection-oriented technology like ATM. Labels are allocated to IP packets and then packets are placed in IP frames. Then those frames are forwarded over the packet or cell-based networks and switching is done on the bases of labels instead of IP address lookup.

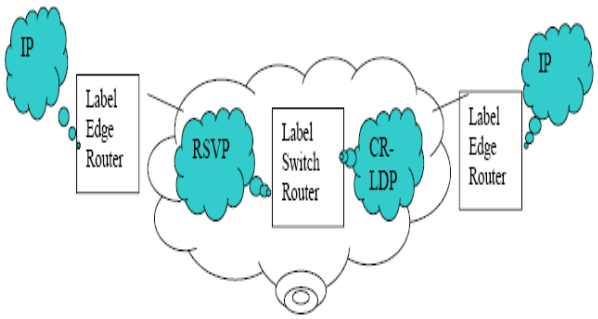

Figure 8: Working towards QoS

The label is assigned to each packet on entry into MPLS network. Routing on each node is done on the bases of label value and incoming interface and sent out of the node by assigning a new label value on the outgoing interface. The paths are known as LSP. LSP is a well defined path through an IP network; it provides a means for ensuring a specified quality of service where QoS is provided by the underlying infrastructure. Due to its multiprotocol nature MPLS support IP networks over any Layer-2 infrastructure such as ATM, packet over SONET, frame relay, Gigabit Ethernet etc [23].

VIII. CONCLUSION

In this paper, we first discussed the general architecture of a Multi Protocol Label Switching infrastructure. The IP/MPLS technology has essential role in next generation networks to meet the performance and the ability to deliver differentiated levels of services in a converged services environment. Our Research experience shows that deployment of MPLS system is feasible in a large ISP network for traffic engineering purposes. Another very useful advantage of MPLS system is its transition process from IPv4 to IPv6. The MPLS VPN solution ensures the cost efficiency and smooth flow of business-critical traffic simultaneously. The paper also discusses that how Quality of Service (QoS) goals can be achieved because increase in the convergence of network services leads directly to performance issues. The next step for the ongoing research project is to identify specific areas that will be addressed in the near term research efforts.

REFERENCES

[1] TRILLIUM: Multiprotocol Label Switching (MPLS).

[2] Enovate: Multiprotocol Label Switching (MPLS).

[3] HUAWEI Technologies Proprietary: Quidway MA5200G MPLS Configuration Guide, June 2007.

[4] Alcatel: The Role of MPLS Technology In Next Generation Networks, October 2000.

[5] Technical University of Madrid: Network Convergence over MPLS.

[6] MPLS Forum Technical Committee: Voice over MPLS - Bearer / Transport Implementation Agreement. MPLSF 1.0, July 2001.

[7] UIT-T: Service requirements and architecture for voice services over MPLS. Rec. Y.1261, December 2002.

[8] MPLS/Frame Relay Alliance Technical Committee: I.366.2 Voice Trunking Format over MPLS. MPLS/FR 5.0.0, August 2003.

[9] Brunnbauer, W., Cichon, G.: AAL2 over IP for radio access networks. IEEE Globecom 2001, San Antonio, November 2001.

[10] Xipeng Xiao, Alan Hannan, Brook Bailey. GlobalCenter Inc, A Global Crossing Company, 141 Caspian Court Sunnyvale, CA 94089. Lionel M. Ni. Department of Computer Science, 3115 Engineering Building, Michigan State University East Lansing, MI 48824-1226. "Traffic Engineering with MPLS in the Internet".

[11] MPLS Traffic Engineering, Cisco IOS Release 12.0(5) S

[12] Technical Paper. "IPv6 Transition Test Challenges", Agilent Technologies.

[13] Internet Protocol version 6, Juniper Networks. www.juniper.net

[14] MPLS Virtual Private Networks. www.is.co.za

[15] COMPREHENSIVE MPLS VPN SOLUTIONS: Meeting the Needs of Emerging Services with Innovative Technology. 3510324-003-EN.pdf, Jan 2010.

[16] IP Solution Center-MPLS VPN: Deploying MPLS VPN Service. White Paper, Cisco Systems, Inc.

[17] Cisco MPLS based VPNs: Equivalent to the

security of Frame Relay and ATM, White Paper. March 30, 2001.

[18] Alexandre Ribeiro. A small MPLS VPN tutorial. alexandregomesribeiro@gmail.com

[19] MPLS–VPN: IP Infusion Inc. application note.

[20] Kelly DeGeest. SANS Institute InfoSec, Reading Room. "What is a MPLS VPN anyway?".

[21] Srihari Raghavan, Blacksburg Virginia. "An MPLS-based Quality of Service Architecture for Heterogeneous Networks". November 12, 2001

[22] Santiago Álvarez. "QoS in MPLS Networks", RST-1607. CCIE 3621.saalvare@cisco.com

[23] Carter Horney for Nuntius Systems, Inc. 13700 Alton Pkwy., Suite 154-266 Irvine, CA. "Quality of Service and Multi-Protocol Label Switching", White Paper.www.nuntius.com

AUTHORS PROFILE

Engr. Sajjad Hussain did his bachelor's in Electrical Engineering from Air University Islamabad, Pakistan in 2008, and masters in Telecommunication engineering from UET, Taxila Pakistan. He is working as junior lecturer at department of Electrical Engineering at APCOMS Rawalpindi, Pakistan. His areas of interest are computer networks and wireless communications.

Engr. Muhammad Tariq Javed did his BS Computer Engineering from COMSATS Institute of Information Technology WAH CANTT, Pakistan in 2009. He is currently student of MS Computer Engineering at UET TAXILA, Pakistan. He is working as junior lecturer at department of Electrical Engineering at APCOMS Rawalpindi, Pakistan. His areas of interest are data communication, computer networks and network management.