International Journal of Engineering Research and Development
e-ISSN: 2278-067X, p-ISSN: 2278-800X, www.ijerd.com
Volume 10, Issue 9 (September 2014), PP.38-43

A Short Study on MPLS with Internet Traffic Engineering

Mr. Manjunath B Talawar[1], Dr. D V Ashoka[2]
[1]*Department of Computer Science & Engineering, JSSATE, Bangalore-60, VTU, India*
[2]*Department of computer Science and Engineering. JSSATE, Bangalore-60, VTU. India*

Abstract:- In last couple of years, area of internet traffic measurement has advanced enormously in the number of users connected, in the increase in user access speeds and in the appearance of network-hungry applications[21]. These changes greatly affected the work of Internet Service Providers and network administrators, which have to deal with increasing network users and capacity demands and abrupt traffic changes caused by new applications. The traffic engineering [1] is a method of optimizing the performance of a telecommunication network by dynamically analysing, predicting and regulating the link utilization over the network. The main objective of traffic engineering is to avoid congestion in the network and to make good use of available resources by controlling and optimising the routing, handles the unexpected traffic dynamics for achieving better quality of service. The connection-oriented approach uses signalling and is being used by techniques like Multi Protocol Label Switching (MPLS)[2]. Connection-oriented techniques offer a convenient way to monitor, allocate, reroute, and protect resources for a given traffic on an explicit and flexible basis. This survey explains the short overview about MPLS network traffic engineering and future challenges of MPLS in future internet traffic control.

Keywords:- Traffic Engineering (TE), Multi-Protocol Label Switching (MPLS), Label Switched Routers (LSRs), Quality of Service (QoS), Interior Gateway Protocols (IGP)

I. INTRODUCTION

The unprecedented growth (e.g Fig-1) of the Internet has lead to a growing challenge among the ISPs to provide a good quality of service, achieve operational efficiencies and differentiate their service offerings. ISPs are rapidly deploying more network infrastructure and resources to handle the emerging applications and growing number of users. The traffic engineering is an important tool for network managers.

The traffic engineering has been used to imply a range of objectives, including load-balancing, constraint-based routing, multi-path routing, fast rerouting, protection switching etc. traffic engineering is concerned with the performance optimization of networks. It addresses the problem of efficiently allocating resource in the network so that user constraints are met and operator benefit is maximized. It can be performed automatically or through manual intervention.

The network traffic engineering is the practice of reserving bandwidth for specific workloads and mapping traffic onto particular paths and links in order to optimize network resource allocation and enforce policies. Sometimes, traffic engineering is required to accommodate network maintenance, work around a component failure, or specify path constraints and routing policies.

Fig.1: Internet Traffic

The traffic engineering is the process of controlling how traffic flows through one's network so as to optimize resource utilization and network performance [22]. Traffic engineering is needed in the Internet mainly because current IGPs always use the shortest paths to forward traffic. Using shortest paths conserves network resources, but it may also cause the following problems.

1. The shortest paths from different sources overlap at some links, causing congestion on those links.
2. The traffic from a source to a destination exceeds the capacity of the shortest path, while a longer path between these two routers is under-utilized.

There is a debate of whether network capacity will one day become so cheap and abundant that these two problems will be eliminated. This debate is beyond the scope of this paper. Here we simply note that currently all ISPs have the above problems. By performing traffic engineering in their networks, ISPs can greatly optimize resource utilization and network performance. Revenue can be increased without large investment in upgrading network infrastructure. Therefore, Traffic Engineering is definitely useful for ISPs now. The traffic engineering is difficult to do with IGP in large networks for the following reasons:

1. Among the Equal-Cost Multi-Paths (ECMPs) from a source, every path will have an equal share of load. This equal ratio cannot be changed. Therefore, one of the paths may end up carrying significantly more traffic than other paths because it also carries traffic from other sources.
2. Load sharing cannot be done among multiple paths of different cost.
3. Modifying IGP metric to trigger some traffic shift tends to have side effects, and undesirable traffic shifts may also be triggered.

II. MPLS

The Multi-Protocol Label Switching (MPLS) was originally presented as a way of improving the forwarding speed of routers but is now emerging as a crucial standard technology that offers new capabilities for large scale IP networks, MPLS is an advanced forwarding scheme. It extends routing with respect to packet forwarding and path controlling. Unlike legacy routing, MPLS (e.g. Fig.2) uses labels to forward traffic across the MPLS domains. When packets enter the MPLS domain, labels are imposed on the packets, and the label (not the IP header) determines the next hop, labels are removed at the egress of the MPLS domain. The traffic engineering, the ability of network operators to dictate the path that traffic takes through their network, and Virtual Private Network support are examples of two key applications where MPLS is superior to any currently available IP technology.

The essence of MPLS is the generation of a short fixed-length label that acts as a shorthand representation of an IP packet's header. This is much the same way as a ZIP code is shorthand for the house, street and city in a postal address, and the use of that label to make forwarding decisions about the packet. IP packets have a field in their 'header' that contains the address to which the packet is to be routed. Traditional routed networks process this information at every router in a packet's path through the network (hop by hop routing).

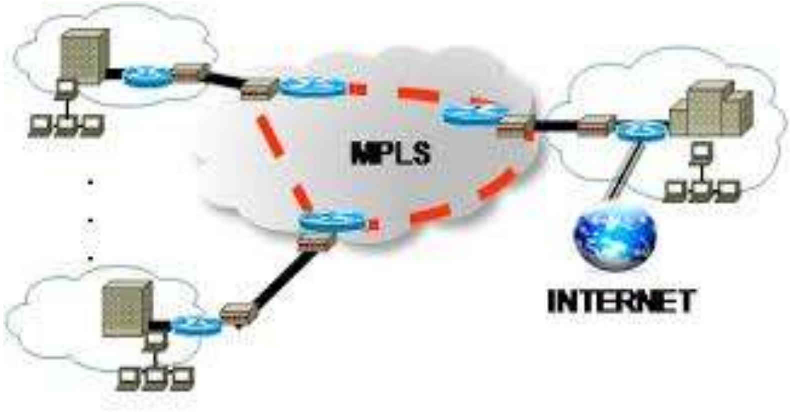

Fig.2: MPLS Network

In MPLS, the IP packets are encapsulated with these labels by the first MPLS device they encounter as they enter the network. The MPLS edge router analyses the contents of the IP header and selects an appropriate label with which to encapsulate the packet. Part of the great power of MPLS comes from the fact that, in contrast to conventional IP routing, this analysis can be based on more than just the destination address carried in the IP header. At all the subsequent nodes within the network the MPLS label, and not the IP header, is used to make the forwarding decision for the packet. Finally, as MPLS labeled packets leave the network, another edge router removes the labels. There are two broad categories of LSR. At the edge of the network, we require high performance packet classifiers that can apply (and remove) the requisite labels: we call these MPLS edge routers. Core LSRs need to be capable of processing the labeled packets at extremely high bandwidths.

When a labeled packet arrives at a Label Switching Router (LSR), the incoming label will determine the path of this packet within the MPLS network. MPLS label forwarding will then swap this label to the appropriate outgoing label and send packets to the next hop. These labels are assigned to packets based on grouping or forwarding equivalence classes (FECs). Packets belonging to the same FEC receive the same treatment. This MPLS lookup and forwarding system allows explicit control routing, based on destination and source address, allowing easier introduction of new IP services.

Label switching has traditionally been used as a forwarding scheme. ATM uses the same techniques to forward packets via virtual path identifier/virtual channel identifier (VPI/VCI) regardless of the payload (IP, other).

III. MPLS TRAFFIC ENGINEERING

Although MPLS label switching provides the underlying technologies in forwarding packets through MPLS networks, it does not provide all the components for Traffic Engineering support such as traffic engineering policy. Traffic Engineering (TE) refers to the process of selecting the paths chosen by data traffic in order to facilitate efficient and reliable network operations while simultaneously optimizing network resource utilization and traffic performance.

The goal of TE is to compute path from one given node to another such that the path does not violate any constraints (bandwidth/administrative requirements) and is optimal with respect to some scalar metric. Once the path is computed, TE is responsible for establishing and maintaining forwarding state along such a path.

IV. MOTIVATION FOR MPLS

The explosive growth of the Internet presents a serious challenge to service providers and equipment suppliers in terms of the tremendous escalation in traffic. There is also an increased demand to create differentiated IP services and bring these to market quickly is also increasing. Other challenges include the cost of mapping IP over layer 2 networks, as well as difficulties in identifying better network utilization and fault handling. Service providers already address these issues in several ways: increase bandwidth and/or the number of powerful routers, exploit QoS to better shape and police traffic, utilize available bandwidth more effectively. MPLS technology is key to scalable virtual private networks (VPNs) and end-to-end quality of service (QoS)[18], enabling efficient utilization of existing networks to meet future growth and rapid fault correction of link and node failure.

V. TRAFFIC ENGINEERING COMPONENTS

A router capable of supporting MPLS is known as Label Switching Router (LSR)[18]. The LSR, found just before the last LSR in the MPLS clouds, is known as the penultimate hop. The end-to-end MPLS path is known as Label Switched Path (LSP). LSP is originated at the head-end router and terminates at the tail-end router. The existing Interior Gateway Protocols (IGP) is not adequate for traffic engineering. Routing decisions are mostly based on shortest path algorithms that generally use additive metric and do not take into account bandwidth availability or traffic characteristics.

The easiest way to provide such features would be to use an overlay model, which enables virtual topologies on top of the physical networks. The virtual topology is constructed from virtual links that appear as physical links to the routing protocol. Further, the overlay model should be able to provide: (1) constraint based routing, (2) traffic shaping and traffic policing functionality, (3) survivability of the virtual links.These capabilities allow easy movement of traffic from an oversubscribed link to an underused one.

MPLS is the overlay model used by Traffic Engineering. It provides:

1. Explicit label switched paths which are not constrained by the legacy destination based traffic forwarding (as featured in all the existing IGPs).
2. LSPs that can be efficiently maintained.
3. Traffic trunks that can be instantiated and mapped into LSPs.
4. A set of attributes that can be associated with traffic trunks.
5. A set of attributes that can be associated with resources that constrain the placement of LSPs and traffic trunks across them.
6. MPLS allows for both traffic aggregation and disaggregation whereas destination based IP forwarding allows only aggregation. “Constraint based routing” and trunk protection can be integrated easily to MPLS.

These components should be available to support TE:

Table.1 TE Components

Sl.No	Components
1	**Information distribution sends information about network topology and constraints pertaining to links (i.e., bandwidth).**
2	**Path selection algorithm—computes and selects best paths that obey the constraints.**
3	**Route setup Resource Reservation Protocol TE (RSVP-TE) extension for signaling LSPs setup.**
4	**Link Admission Control: decides which tunnel may have resources.**
5	**TE control: establishes and maintains trunks.**
6	**Forwarding data across the path.**

VI. GENERIC ISSUES OF DESIGNING AN MPLS SYSTEM FOR TRAFFIC ENGINEERING

To build an MPLS system for Traffic Engineering, the following design parameters [22] must be determined:

Table.2 Design Parameters

Sl.No	Design Parameters
1	Geographical scope of the MPLS
2	Routers in participate
3	Hierarchy of MPLS system
4	LSPs of the bandwidth requirement
5	Adaptability and Resilience attributes of the LSPs
6	Affinity of the LSPs and the links
7	Number of parallel LSPs between each endpoint pair
8	Priority of the LSPs
9	Path attribute of the LSPs

The process of deciding the scope of an MPLS system is driven by administrative policy. The second step is to decide the participating routers in the MPLS system, i.e., the ingress LSRs, the transit LSRs and the egress LSRs. This should also be guided by the administrative policy. Network administrators may want to forbid some routers from participating in the MPLS system for some reason, for example, because those routers cannot be trusted or because those routers do not have enough processing power and/or memory capacity. Another factor for consideration is the tradeoff between the number of LSPs and efficiency of the links. More ingress and egress LSRs mean more LSPs and thus higher LSP-routing complexity. But because the average size (bandwidth requirement) of the LSPs is smaller, Constraint-based Routing has more flexibility in routing the LSPs. Higher link efficiency may be achieved. After the LSRs are decided, network administrators need to decide the hierarchy of the MPLS system.

One alternative is to fully mesh all LSRs, resulting in a single layer of LSPs. For large ISPs, there can be hundreds of LSRs[22]. A full mesh will result in a huge MPLS system. Another alternative is to divide one's network into multiple regions. LSRs in each region are meshed. This forms the first layer of LSPs. Some selected LSRs from each region, for example the core routers, are also fully meshed to form the second layer of the LSPs. This hierarchical design can significantly reduce the number of LSPs in the network, and hence the associated processing and managing overhead. Unless an end-to-end traffic matrix is available beforehand, the bandwidth requirement of the LSPs is usually unknown and has to be guessed for the first time LSPs are deployed. Later, the measured rate of the LSPs can be used as the bandwidth requirement of the LSPs.

LSP paths can be manually specified or dynamically computed. Unless offline Constraint-based Routing is used to compute the paths, manually specifying paths for LSPs is difficult. Therefore, LSPs are usually dynamically computed by an online Constraint-based Routing algorithm in the routers. Important LSPs, such as those carrying large amount of traffic, can be given a higher priority than other LSPs. In this way, these LSPs are more likely to take the optimal paths. This will result in higher routing stability and better resource utilization from a global perspective. Multiple parallel LSPs can be configured between an ingress-egress pair. These LSPs can be placed on different physical paths, so that the traffic load from the source to the destination can be distributed more evenly. By using multiple parallel LSPs, the size of each LSP is also smaller.

These LSPs can be routed more flexibly. These are the primary motivations for parallel LSPs. It is recommended that parallel LSPs be used to keep the size of each LSP below 25 Mbps. Affinity, or color, can be assigned to LSPs and links to achieve some desired LSP placement. For example, if network administrators want to prevent a regional LSP from traversing routers or links outside the region, color can be used to achieve the goal. All regional links can be colored green, and all inter-region links can be colored red. Regional LSPs are constrained to take only green links. In this way, regional LSPs can never traverse any inter-region link. The process of assigning color to LSPs and links is again guided by administrative policy. Depending on the stability of the network, when better paths become available, network administrators may or may not want to switch LSPs to the more optimal paths. The switching of LSPs to better paths is called LSP reoptimization. Reoptimization is not always desirable because it may introduce routing instability.

In the case that reoptimization is allowed, it should not occur too frequently. Performing reoptimization once per hour may be a good choice. As to the resilience attribute, LSPs are generally allowed to be rerouted when failure occurs along their paths. In the cases of failure, it may even be desirable to reroute LSPs regardless of their bandwidth and other constraints.

VII. QUALITY OF SERVICE (QoS) IN A NETWORK WITH MPLS

With Differentiated Services (Diffserv), packets are classified at the edge of the network. The Differentiated Services-fields (DS-fields) [22] of the packets are set accordingly. In the middle of the network, packets are buffered and scheduled in accordance to their DS-fields by Weighted Random Early Detection (WRED) and Weighted Round Robin (WRR). Important traffic such as network control traffic and traffic from premium customers will be forwarded preferably. With MPLS, QoS is provided in a slightly different way. Packets still have their DS-fields set at the edge of the network.

In addition, the experimental fields in the MPLS headers are set at the ingress LSRs. In the middle of an LSP, packets are buffered and scheduled in accordance to the experimental fields. Whether MPLS is involved or not in providing QoS is transparent to end-users. Sometimes it is desirable to use different LSPs for different classes of traffic. The effect is that the physical network is divided into multiple virtual networks, one per class.

VIII. CONCLUSION

The Internet traffic volumes continue to grow at a great rate, now pushed on by video and TV distribution in the networks. Increasing traffic volumes and the introduction of delay and loss sensitive services makes it crucial for operators to understand and manage the traffic situation in the network. More traffic also necessitate upgrades of network equipment and new investments for operators, and keep up-to-date the question of over-dimensioning network capacity versus using traffic engineering mechanisms for better handling the traffic. This paper discusses the advantages and application of MPLS in internet traffic engineering and the concepts and challenges in the internet are reviewed.

REFERENCES

[1]. D. Awduche et al, ``Overview and Principles of Internet Traffic Engineering" IETF Internet Draft draft-ietf-tewg principles-02.txt, Work-in-progress, Jan 2002.
[2]. D. Awduche, ``MPLS and traffic engineering in IP networks," IEEE Communications Magazine, Vol. 37, No. 12, pp. 42-47, 1999.
[3]. Dahai Xu, Member, IEEE, Mung Chiang, Senior Member, “Link-State Routing With Hop-by-Hop Forwarding Can Achieve Optimal Traffic Engineering”, IEEE, and Jennifer Rexford, Senior Member, IEEE, Fellow, ACM, 2011.
[4]. B. Fortz and M. Thorup, “Increasing Internet capacity using local search,” Computational Optimization and Applications, vol. 29, no. 1, pp. 13–48, 2004.
[5]. A. Sridharan, R. Guerin, and C. Diot, “Achieving near- optimal traffic engineering solutions for current OSPF/IS- IS networks,” IEEE/ACM Transactions on Networking, vol. 13, no. 2, pp. 234–247, 2005.
[6]. Bernard Fortz, Jennifer Rexford, Mikkel Thorup, “Traffic EngineeringWith Traditional IP Routing Protocols”.
[7]. D. Andersen et al, ``Resilient Overlay Networks," ACM SOSP, October 2001
[8]. ATM Forum, Private Network-Network Interface Specification Version 1.0 (PNNI 1.0), International Standard, af pnni-0055.000, March 1996
[9]. Cisco, Configuring OSPF, 1997. [12] Douglas Comer, ``Internetworking with TCP/IP Vol.1: Principles, Protocols, and Architecture," 4th Edition, Vol. 1. Prentice Hall, 2000.
[10]. T.H. Cormen, et. al., ``Introduction to Algorithms", The MIT Press, McGraw-Hill Book Company
[11]. Zheng Wang, Jon Crowcroft, ``Analysis of Shortest-Path Routing algorithms in a Dynamic Network
[12]. Environment," Computer Communication Review, Vol. 22, no. 2, pp.63-71, 1992.
[13]. E. Davies et al, ``Future Domain Routing Requirements," IRTF Routing Research Draftdraft-davies-fdr-reqs-01.txt, Work-in-progress, July 2001.

[14]. A. Elwalid, et al, ``MATE: MPLS Adaptive Traffic Engineering," INFOCOM'01, April, 2001 End-to-End Mailing List Thread, ``Traffic engineering considered harmful," June 2001.
[15]. B. Fortz, M. Thorup, ``Internet Traffic Engineering by Optimizing OSPF Weights, in Proceedings of the FOCOM 2000, pp. 519-528, 2000.
[16]. B. Fortz, M. Thorup, ``Increasing Internet Capacity Using Local Search," Preprint, 2000.
[17]. C. Huitema, ``IPv6: The New Internet Protocol," Prentice Hall, Second Edition, 1998.
[18]. Cisco, www.cisco.com
[19]. Google,www.google.com
[20]. Debashis Basak, Hema Tahilramani Kaur, Shivkumar Kalyanaraman ”Traffic Engineering Techniques and Algorithms for the Internet”
[21]. Arthur Callado, Carlos Kamienski, Member, IEEE, Stênio Fernandes, Member, IEEE, Djamel Sadok,Senior Member, IEEE,Géza Szabó, Balázs Péter Gerő. “A Survey on Internet Traffic Identification and Classification”
[22]. Xipeng Xiao, Alan Hannan, Brook Bailey global Center Inc, Lionel M. Ni “Traffic Engineering with MPLS in the Internet”
[23]. Bernard Fortz, Jennifer Rexford, MikkelThorup “Traffic Engineering With Traditional IP Routing Protocols”
[24]. “Internet Traffic Management” Henrik Abrahamsson, November 2008, School of Innovation, Design and Engineering M¨alardalen University V¨aster˚as, Sweden
[25]. Daniel O Awduche, “MPLS and Traffic Engineering in IP Networks”.
[26]. Nick Feamster , Jay Borkenhagen, Jennifer Rexford “Guidelines for Interdomain Traffic Engineering”
[27]. R.S. Dayama, S.P. Pingat “Optimal Traffic Engineering in Link State Routing Protocols” International Journal of Computer Applications (0975 – 8887) Volume 68– No.18, April 2013.
[28]. Hao Wang⋆ Haiyong Xie⋆ Lili Qiu† “COPE: Traffic Engineering in Dynamic Networks”
[29]. Eric Keller, Michael Schapira ,Jennifer Rexford “Rehoming Edge Links for Better Traffic Engineering”.
[30]. https://www.ietf.org/rfc/rfc2702.txt
[31]. Richard Mortier,“Internet traffic engineering”, UCAM-CL-TR-532 ISSN 1476-2986.