Multiprotocol Label Switching: An In Depth View

LoyCurtis Smith

East Carolina University

Abstract

Multiprotocol Label Switching (MPLS) is a revolutionary packet forwarding WAN technology that operates between Layer 2 and Layer 3 of the OSI model, which has been classified as Layer 2.5. It is placed between the two layers because it integrates the fast paced switching, that takes place in the data link layer ,with IP routing, that takes place in the network layer, to do what is called label based switching. It is a multifaceted technology that shifts the paradigm of how packets are passed throughout the network. Multiprotocol label switching is a core network switching technique that offers numerous benefits such as increased performance, increased traffic control with traffic engineering, Quality of Service (QoS), secure transportation of traffic with MPLS Virtual Private Networks (VPNs), disaster recovery, as well as many other things, to Internet Service Providers (ISPs), telecommunication carriers, as well as large enterprises. It has the capabilities to do so much that often times it is hard for one to grasp the concept of what MPLS truly is because the information may be so overwhelming. To have a better understanding of multiprotocol label switching, one should know what exactly MPLS is, what lead to its conception, what type of MPLS services and applications are available for use throughout the Internet, the benefits of using MPLS, and the challenges associated with the use of this phenomenal technology. Once one has learned all of the above, then they should have a better understanding of what multiprotocol label switching is and what it has the ability to offer an organization

Introduction

Multiprotocol label switching (MPLS) is a revolutionary packet forwarding Wide Area Network (WAN) technology that exists between Layers 2 and 3 of the Open Systems Interconnection (OSI) model, which has been classified as Layer 2.5. It is located in the intermediate layer 2.5 because it incorporates characteristics of both OSI layers. According to webopedia.com, MPLS is an Internet Engineering Task Force (IETF) initiative that integrates Layer 2 information about network links (e.g. bandwidth, latency, utilization) into Layer 3 (IP) within a particular autonomous system, or Internet Service Provider (ISP), in order to simplify and improve packet exchange (Beal). In a nutshell MPLS integrates the fast paced switching, that takes place in the data link layer (Layer 2), with IP routing, which takes place in the network layer (Layer 3), to do what is called label based switching. It is a core technology that is utilized by a lot of Internet Service Providers (ISPs), telecommunication companies, and large enterprises due to its many benefits. According to Tang, Akymac, Chu, and Nagarajan in their paper MPLS Network Requirements and Design for Carriers: Wireline and Wireless Case Studies, it has become the choice of packet transport technology to meet multiple service requirements in the next generation network (NGN). More and more service providers, both wireline and wireless, are starting to deploy MPLS as a common packet backbone to achieve convergence of existing Time Division Multiplexing (TDM) and packet (X.25, ATM/FR, best-effort IP) networks and services (Tang, Akymac, Chu, and Nagarajan, 2006). Due to the increasing popularity of this technology it is imperative that networking professionals develop a better understanding of MPLS in preparation of potential implementation in their organization. In order to assist networking professionals with developing that better understanding, this paper will cover the following topics: what lead to the inception of MPLS, what exactly is MPLS, how does it work, what are the types of services and applications that MPLS offer to be used throughout the Internet, the benefits of using MPLS, and the challenges associated with the use of this phenomenal technology.

What caused the creation of MPLS?

When MPLS was introduced in the late 1990's its initial intent was to solve the shortcomings that the service providers were experiencing with traditional routing, ATM, and Frame-Relay. According to Sinha in his whitepaper titled MPLS – VPN Services and Security, as the demand of newer network applications such as video teleconferencing (VTC), Layer 3 VPN, and VoIP increased, so did the demand for low latency networks. The solution that met these demands would also have to address the following:

- Limitations of traditional routing due to its connectionless nature, problems with its forwarding component, and its difficulty of predicting network performance in an ever increasing large meshed networks.
- Limitations of connectionless traditional routing overlying connection oriented ATMs and Frame-Relays. Although the combination increased the performance of an ISP's networks, there were issues in regards to scalability due to the requirement of an ATM Virtual Circuit (VC) for every router to form an adjacency with each other.
- Requirements for more management capabilities, network predictability, to be a connection oriented technology, and awareness of the end-to-end state of the network
- Separation of the routing problem from the forwarding problem, through the use of label swapping forwarding techniques (Sinha, 2003).

What is Multiprotocol Label Switching?

Multiprotocol label switching is a multifaceted protocol that includes a myriad of services and applications that are utilized by multiple organizations to include Internet Service Providers, telecommunication companies, and large enterprises. It is a protocol independent packet switching WAN technology that uses labels to forward packets throughout a given network. According to Mahidi and Khaitan in their article titled Faster Conversion and Security Issues in MPLS Networks, MPLS is an evolving technology that facilitates several problems in the Internet, such as routing performance, speed, and traffic engineering. MPLS provides mechanisms in IP backbones for explicit routing using Label Switched Paths (LSPs), which encapsulates the IP packet in an MPLS packet. An MPLS network combines a label-swapping algorithm, similar to the one used in Asynchronous Transfer Mode (ATM), with network layer routing (Mahidi & Khaitan, 2014). Brian Daugherty and Chris Metz in the article titled Multiprotocol Label Switching and IP, Part I: MPLS VPNs over IP Tunnels describe it as being a lightweight tunneling technology used by many service provider networks (Daugherty & Metz, 2005). As can be seen across the web, there are numerous definitions that describe this technology. Majority of those separate definitions can be pieced together to provide an overall conclusion of what MPLS is exactly, since the technology in itself is still growing. Essentially MPLS is the service provider’s solution to the growth of the network. Prior to its inception in the late 1990s, service providers were relying on WAN technologies such as Frame-Relay, Asynchronous Transfer Mode (ATM), and traditional routing, however the growth of the Internet was becoming more than those technologies could handle.

How does MPLS work?

Two of the most important things networking professionals will need to familiarize themselves with to completely grasp this technology, outside of its definition, would be what components make up MPLS and how exactly multiprotocol label switching takes place. This section will only cover the basic components involved and the basic details of how the IP/MPLS version of the protocol operates. It will not cover how its different applications and services operate, since they will be mentioned later in this paper.

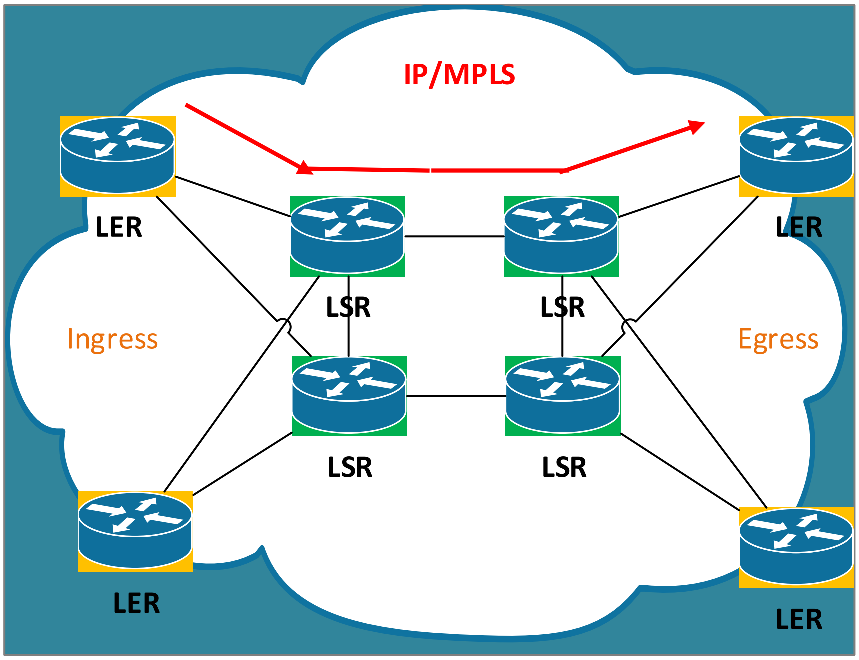

Figure 1: Topographical View of Multiprotocol Label Switching

MPLS Components
Forwarding Equivalence Class (FEC)
Label
Label Distribution Protocol (LDP)
Label Switched Path (LSP)
Label Switch Router (LSR)
Ingress Label Edge Router (iLER)
Egress Label Edge Router (eLER)

Table 1: MPLS components

Figure 1 displays the topological view of how IP/MPLS operates. Table 1 displays the components involved in its operation. As can be seen in the table, MPLS has the following components: Forward Equivalence Class (FEC), Label, Label Distribution Protocol (LDP), Label Switched Path (LSP), Label Switching Routers (LSRs), ingress Label Edge Router (LER), and egress LERs. The descriptions of the listed components are as follows:

- **Forward Equivalence Class (FEC):** is a group of IP packets which are forwarded in the same manner (Rosen et al., 2001).
- **Label:** is a short, fixed length, locally significant identifier that is used to identify a stream. It is based on the stream or Forwarding Equivalence Class that a packet is assigned to (Le Faucheur, 1998).
- **Label Distribution Protocol (LDP):** is a set of procedures used by an LSR to inform another LSR of the label/FEC bindings it has made (Rosen et al., 2001). It can be used by LSRs to determine the label switched path.
- **Label Switched Path (LSP):** is the path through one or more LSRs at one level of the hierarchy. It is followed by packets in a particular FEC (Rosen et al., 2001). The red path in figure 1 represents an LSP.
- **Label Switch Router (LSR):** is the name given to a router that supports MPLS (Le Faucheur, 1998). In MPLS networks it can be seen that although all the routers involved meet that qualification, only the intermediate routers of the MPLS network are classified as such. The purpose of these routers are to map the incoming labels to the outgoing labels and the outgoing interface (Nagarajan & Ekici, 2008). They are essentially the backbone of the network. According to Andersson and Bryant in the article titled The IETF Multiprotocol Label Switching Standard: The MPLS Transport Profile Case, LSRs take forwarding decisions based on a label that was added between the data link layer and network layer headers, and also participates in the control plane information exchange to setup Label Switched Paths (Andersson & Bryant, 2008).

- **Ingress Label Edge Router (I-LER):** an LSR that is located at the beginning of the MPLS domain that assigns a label to an IP Packet for each FEC and sends that label with the packet (Andersson & Bryant, 2008).
- **Egress Label Edge Router (E-LER):** an LSR located at the end of an MPLS domain that strips the label, reads the IP packet header, and forwards the packet to its final destination (Sinha, 2003).

Now that the components have been discussed a brief overview of the label switching technique, can now be discussed. In MPLS instead of every router performing an analysis of a packet's network layer header like that of traditional routing, it is only performed once. According to Daugherty and Metz multiprotocol label switching takes place as follows:

- A contiguous set of routers in a network running MPLS software creates a tunnel, or a label switched path (LSP), by distributing a set of fixed length 32-bit labels along a path from the network's ingress (entry point) to its egress (exit point).
- The ingress router appends packets that enter the LSP with a label.
- As the labeled packet traverses through the MPLS network its appended label is swapped out with another label at each hop in its respective LSP.
- At the end of the LSP, the egress router disposes of the label and sends the packet on its way (Daugherty & Metz, 2005).

MPLS Applications and Services

There are a myriad of applications and services that one can choose from when deploying MPLS as the backbone in either a large enterprise, telecommunications carrier, or Internet Service Provider network. Each application and service has its own set of procedures, benefits, and requirements for a successful deployment. Each application has also assisted in the increasing popularity of the protocol which has led to the widespread deployment of MPLS across the Internet. Multiprotocol label switching has several capabilities and can be deployed in the numerous ways. In the paper Network Convergence over MPLS, authors Vasquez, Alvarez-Campana, and Garcia list the following multiprotocol label switching applications: IP Virtual Private Networks (VPNs), Traffic Engineering (MPLS-TE), support of Differentiated Services (DiffServ), DiffServ-aware Traffic Engineering (DS-TE), and fast rerouting (Vasquez, Alvarez-Campana, and Garcia, 2004). Santanu Dasgupta, in a Cisco presentation titled Introduction to MPLS, on the other hand broke MPLS applications up into the following service types: End to End Services and MPLS Network Services (Dasgupta, 2010). Table 2 displays the applications that are considered MPLS End to end data connectivity services and Table 3 displays the applications that are considered to be MPLS Network Services.

End to End Data Connectivity Services
Layer 3 VPNs
Layer 2 VPNs

Table 2: MPLS End to end Data Connectivity Services

MPLS Network Services
MPLS Quality of Service (QoS)
MPLS Traffic Engineering (TE)
MPLS Operations Administration and Maintenance (OAM) / Management Information Base (MIB)

Table 3: MPLS Network Services

MPLS End to end services

As seen in table 2 the end to end data connectivity services offered by MPLS are both Virtual Private Networks. The main difference between the two VPN services is the OSI layer in which they operate. One operates on Layer 2, while the other operates on Layer 3. This section will cover the two VPN services in detail.

MPLS VPN Services

MPLS has the ability to support Virtual Private Networks. It can do so at both the data link layer (Layer 2) and at the network layer (Layer 3). The MPLS VPN is the most popular MPLS enabled application in operation today. This type of service is typically offered to large corporate customers that require IP connectivity to any number of other remote sites (Daugherty & Metz, 2005). Multiprotocol label switching technology provides service providers the ability to separate traffic belonging to different VPNs. In the paper titled Virtual Private network Implementation over Multiprotocol Label Switching Azher, Aurengzeb, and Masood state that MPLS VPNs achieve customer segregation through the use of virtual routing and forwarding (VRF). With VRF the provider edge (PE) router is subdivided into virtual routers serving different VPNs or customer sites (Azher, Aurengzeb, and Masood, 2005). One of the benefits of virtual private networks built using MPLS is that it does not require site to site peering or any type of pre-defined relationships as does IPsec. In its deployment of VPN the process is as follows: Packets are labeled for specific VPNs with the network and only those ports that are part of the specified VPN receive traffic. One of the drawbacks however is that MPLS is a network-based solution and does not go out to the computing endpoints. MPLS stops at the edge of the Internet Service Provider's network (Sinha, 2003). The next half will cover the MPLS VPN service in regards to which layer of the OSI model it operates on.

Layer 2 VPN

MPLS Layer 2 VPNs can be configured in the following manner: Point to Point Layer 2 VPNS and Point to MultiPoint Layer 2 VPNs. Figure 2 displays an in depth view of the Layer 2 VPN options offered in MPLS VPN services.

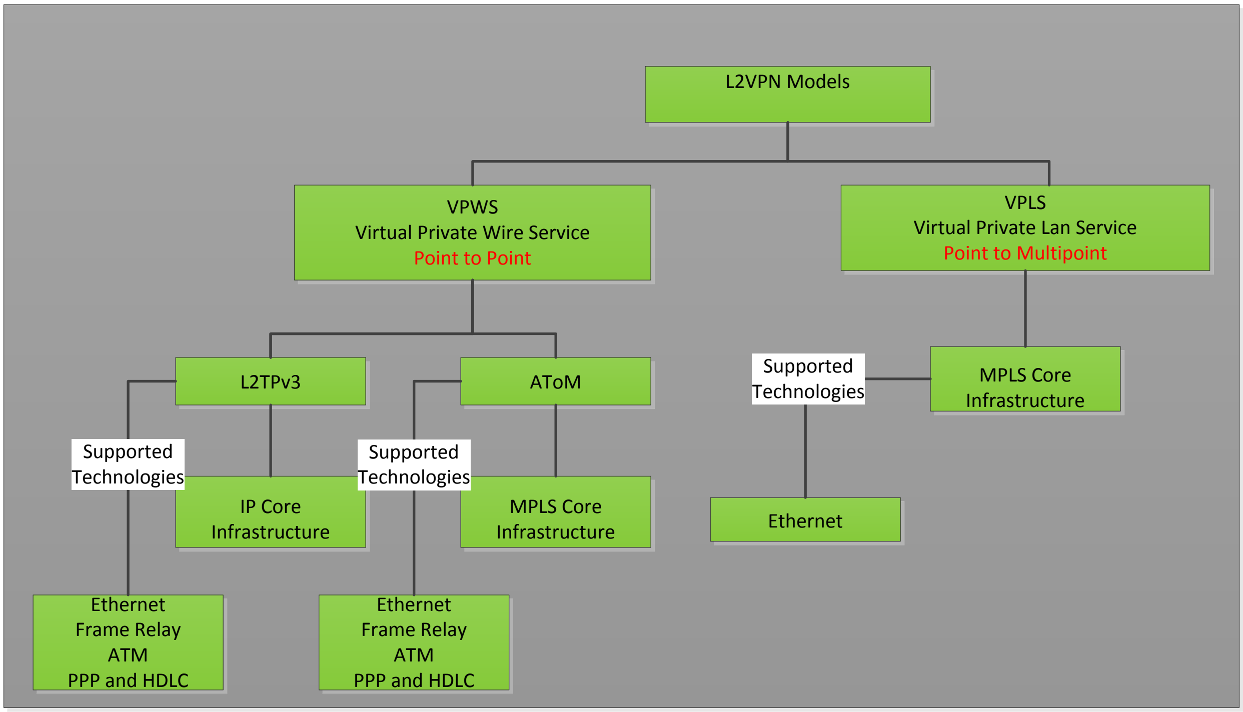

Figure 2: MPLS L2VPN Service Models

In the figure it can be seen that L2VPN can be broken down into two different service models: Virtual Private Wire Service (VPWS) and Virtual Private LAN Service (VPLS). The two service models are defined as follows:

- **VPWS**: provides a network of point to point layer 2 connections that interconnect a set of customer edge (CE) nodes belonging to the same VPN. It is appropriate if a provider wants to emulate a traditional point to point Frame Relay or ATM permanent virtual circuit across the packet switch network (Metz, 2004).

- **VPLS**: is a telecom carrier provided service that makes it possible for customers to create a logical local area network (LAN) structure between separate sites. All services in a VPLS appear to be on the same LAN, regardless of the location (Rouse, 2007). Allows for point to multipoint layer 2 connectivity.

In the service VPWS service model it has the two services Layer 2 Transport Protocol Version 3 (L2TPv3) and Any Transport over MPLS (AToM). The two are defined as follows:

- **Layer 2 Transport Protocol version 3 (L2TPv3):** encapsulates MPLS in a Layer 2 Transport Protocol version 3 header.
- **Any Transport over MPLS (AToM):** is a Cisco Layer 2 tunneling solution. It addresses the issue that service providers had when they initially deployed MPLS. In the past, when deploying MPLS service providers still had to utilize a legacy technology to pass the Layer 2 traffic from its customer. It allows service providers to carry their customers' Layer 2 traffic over the MPLS backbone (Hung, Cuong, & Mai, 2010)

MPLS L3VPN

MPLS L3VPNs are IP based VPNs that are configured for the customer by the service provider on their provider edge (PE) equipment. According to Ivan Pepelnjak, in L3VPNs the customer edge routers exchange routes with the provider edge routers. The service provider's equipment forms the core of the WAN backbone (Pepelnjak, 2010). The MPLS L3VPN can use Border Gateway Protocol (BGP), any Interior Gateway Protocol (IGP), or static routing to form virtual route forwarding domains on PEs. MPLS VPNs enable full mesh, hub and spoke, and hybrid connectivity among connected customer edge sites (Dasgupta, 2010). It is considered the most scalable service provider offered VPN solution.

MPLS Network Services

As seen in table 3 the network services offered by MPLS are Quality of Service (QoS), Traffic Engineering (TE), and MPLS Operations Administration and Maintenance (OAM) / Management Information Base (MIB).

MPLS QoS

Quality of Service (QoS) is the sorting and classifying of packet requests into different traffic classes followed by the allocation of the proper resources to direct traffic based on various criteria to include the application type, user application ID, source or destination IP address, and other variables (Hung, Cuong, & Mai, 2010). MPLS QoS is used for MPLS packet-specific marking and classification through the use of the Differentiated Service (DiffServ) architecture. QoS in IP networks use the IP Precedence/ DiffServ Code Point (DSCP) value located in the IP header to determine the class of a packet. However, in an MPLS label MPLS Experimental (EXP) bits are used for packet classification and prioritization. The DSCP values are mapped into EXP bits at the ingress PE router of the MPLS network (Dasgupta, 2010). There are three tunneling model for when DSCP values are mapped to EXP bits in an MPLS network: uniform model, pipe model, and short pipe model. In the Juniper technical document titled Tunneling Model for Differentiated Services Overview, the tunneling models are described as follows:

- **Uniform Model**: this model of tunneling renders MPLS transparent to the differentiated services operation. From the DiffServ perspective, MPLS is not used. If traffic conditioning is applied along the LSP, the EXP bits of the inner header must be changed at the egress when the inner header becomes the outer header.

- **Pipe model**: in this model any traffic conditioning applied in the LSP has no effect on the EXP bits coding in the inner header. The EXP bits go unchanged during ingress and egress. The EXP value is set based on the ingress classification. At the egress PE, the EXP value is not copied back into the DSCP value.
- **Short Pipe model**: this model is the same as the pipe model, however at the egress PE the original IP DSCP value from the CE is used for QoS processing (Tunneling Model, 2013).

MPLS Traffic Engineering

Traffic Engineering is defined as the ability to dynamically plan resource commitments on the basis of known demands, define routed dynamically and optimize network utilization. It seeks to control traffic flows and the network resources so that predefined objectives can be met (Sinha, 2003). MPLS Traffic Engineering is considered a key application in the evolution of MPLS and has also assisted with its popularity among service providers. According to the Cisco whitepaper MPLS Traffic Engineering, MPLS traffic engineering does the following:

- Enhances standard IGPs, such as IS-IS or OSPF, to automatically map packets onto the appropriate traffic flows.
- Transport traffic flows across a network using MPLS forwarding.
- Determines the routes for traffic flows across a network based on the resources the traffic flow requires and the resources in the network.

- Employs “constraint-based routing,” in which the path for a traffic flow is the shortest path that meets the resource requirements (constraints) of the traffic flow. In MPLS traffic engineering, the traffic flow has bandwidth requirements, media requirements, a priority versus other flows, and so on.
- Recovers to link or node failures that change the topology of the backbone by adapting to a new set of constraints (MPLS Traffic, 1999).

MPLS OAM/MIB

According to Request for Comment (RFC) 6291: Guidelines for the Use of the OAM Acronym in the IETF defines Operation, Administration, and Maintenance (OAM) as being a group of network management functions that provide network fault indications, performance information, and data and diagnosis functions (Andersson, van Helvoort, Bonica, Romascanu, & Mansfield, 2010). MPLS OAM has the following functions to assist ISPs with network management:

- **Detection of broken label switch path:** provides the ability to avoid hop by hop troubleshooting and synchronization of detection time bounds by the tools implementing it.
- **Diagnosis of a broken label switch path:** allows the ability to detect, diagnose, and isolate a failed component (link or node); it is implemented through a path trace function.
- **Path characterization:** reveals details on LSR forwarding operations, such as ECMP, algorithms used, data/control plane OAM capabilities of the LSR, stack operations performed by the LSR, and time to live (TTL) propagation at penultimate hop LSRs.

- **Service level agreement measurement**: provides the ability to measure service level agreement parameters such as availability, performance, latency, packet loss, jitter, and etc.
- **Frequency of OAM execution**: to configure how frequently the OAM functions must be executed to guarantee consistency with SLA related function, a special function with minimum impact on the network resources is needed. It must be tuned in harmony with other technologies.
- **Alarm suppression, aggregation, and layer coordination:** allows the discarding of superfluous traffic by correlating and aggregating the notifications. Requires fault notification to the LSP egress. Can also select which LSPs to monitor.
- **Support for OAM Internetworking for fault notification:** the ability to translate an MPLS defect or error into native technology's error condition. Function is required for the use of multiple technologies over MPLS. Requires MPLS to detect the anomaly in a bound time interval.
- **Error detection and recovery**: guarantees that some well identified mechanisms can automatically fix and recover from an error, prior to customers' detection of the error. Function must accept various types of automation procedures.
- **Standard management interfaces:** operators must have a common programmatic interface to access operations and management functions and their status.
- **Detection of denial of service attacks:** the ability to detect denial of service (DoS) attacks against the data or control planes.
- **Per-LSP accounting and scalability metrics**: supports the different types of traffic accounting in order to ensure that service providers can measure traffic accounting in

order to ensure that service providers can measure traffic from an LSP to the egress of the network (some MPLS MIBs will be used). Can be used to design a network, check SLA violations, or to measure per operator partial services in a multi-provider service network.

- **Security (LSP mis-merging security implications):** function is provided by a series of tools that must be self-protected (Dini, Hasan, Morrow, Parr & Rolin, 2004).

According to Hoster and Pandian, a Management Information Base (MIB) is a set of network objects that can be managed using Simple Network Management Protocol (SNMP) remotely (Hoster& Pandian, 2005). In order to take advantage of what the MPLS OAM functions have to offer, MPLS MIB is used. It allows service providers to achieve proactive monitoring of the MPLS network. MPLS MIBs can be used to provide LDP, VPN, and TE management information (Dasgupta, 2010).

MPLS Benefits

The use of MPLS in one of its numerous flavors offers a myriad of benefits to Internet service providers, telecommunications carriers, large enterprises, and customers. To the service provider/ telecommunications carrier MPLS allows them to:

- Reduce costs.
- Consolidate the network for multiple Layer 2 and Layer 3 services.
- Support increasingly stringent SLAs.
- Handle the increasing scale and complexity of IP-based services.

From the enterprise and end user perspective MPLS networks provide them with:

- Network segmentation.
- WAN connectivity.

- Easier configuration of site to site WAN connectivity (Dasgupta, 2010).

MPLS also allows for the use of QoS to prioritize traffic, traffic engineering to optimize network utilization to achieve optimal performance, and the support of IPv6. According to HighSpeed Office, MPLS also has the following benefits:

- **Improves Uptime**: MPLS improves uptime by sending data over an alternative path in less than 50 seconds, if one exits. It also reduces the amount of manual intervention done by the ISP to create a WAN.
- **Creates Scalable IP VPNs** – it's easy to add an additional VPN, which removes the need to configure a complex mesh of tunnels, as would be the case in traditional approaches.
- **Hide Network Complexity**: an MPLS connection between two sites can be configured to act like a long Ethernet cable, with the hops involved hidden from view. This is possible with VPLS.
- **Reduce Network Congestion**: with the use of traffic engineering both latency and congestion can be reduced (MPLS Benefits, 2015).

MPLS Challenges/Disadvantages

Nothing can be without flaw. Although MPLS seems like the perfect protocol it has a few setbacks. To initially setup MPLS it is costly in regards to initially setting up MPLS backbones due to the need for capable devices. According to Steenbergen, MPLS has the following potential disadvantages:

- MPLS hides suboptimal topologies from BGP, where multiple exits may exist for the same route.

- Building the full mesh of LSP tunnels is left up to the operator/ operator supplied scripts or purchased software solution. Vendors like Cisco offer basic auto-mesh capabilities.
- Large LSPs cannot fit down small circuits. Multiple parallel LSPs would be necessary (Steenbergen, 2010).

Conclusion

MPLS is a phenomenal technology that is constantly growing. There are a myriad of advantages and only very few disadvantages that pretty much have solutions or may have solutions in the works. It allows for service providers to offer VPN services at both Layer 2 and 3, prioritizing of traffic with QoS, network optimization with traffic engineering, the deployment of any transport over MPLS, a reduction in costs, and network management functions to maintain the MPLS network to provide maximum uptime to the customer. Multiprotocol label switching is a lot to truly digest because it offers a lot to an organization and its customers. It solves the issues that service providers were experiencing with traditional routing and layer 2 transport mechanisms before its inception.

References

[1] Andersson, L., & Bryant, S. (2008). The IETF multiprotocol label switching standard: The MPLS transport profile case. *Internet Computing, IEEE*, *12*(4), 69-73.

[2] Andersson, L., Van Helvoort, H., Bonica, R., Romascanu, D., & Mansfield, S. (2010). Guidelines for the use of the OAM acronym in the IETF. *work-in-progress, draft-ietfopsawg-mpls-tp-oam-def*.

[3] Azher, I., Aurengzeb, M., & Masood, K. (2005, August). Virtual Private Network Implementation over Multiprotocol Label Switching. In *Engineering Sciences and Technology, 2005. SCONEST 2005. Student Conference on* (pp. 1-5). IEEE.

[4] Beal, V. (n.d.). MPLS - Multiprotocol Label Switching. Retrieved April 25, 2016, from http://www.webopedia.com/TERM/M/MPLS.html

[5] Dini, P., Hasan, M. Z., Morrow, M., Parr, G., & Rolin, P. (2004, October). IP/MPLS OAM: challenges and directions. In *IP Operations and Management, 2004. Proceedings IEEE Workshop on* (pp. 1-8). IEEE.

[6] Dasgupta, S. (2010). Introduction to MPLS. Retrieved April 25, 2016, from http://www.sanog.org/resources/sanog17/sanog17-mpls-intro-santanu.pdf.

[7] Daugherty, B., & Metz, C. (2005). Multiprotocol label switching and IP, part I: MPLS VPNs over IP tunnels. *IEEE Internet Computing*, *9*(3), 68-72. doi: http://dx.doi.org/10.1109/MIC.2005.61

[8] Fang, L., Bita, N., Roux, J. L. L., & Miles, J. (2005). Interprovider IP-MPLS services: requirements, implementations, and challenges. *Communications Magazine, IEEE*, *43*(6), 119-128.

[9] Hoster, J., & Pandian, K. (2005, April). What is management information base (MIB)? - Definition from WhatIs.com. Retrieved April 25, 2016, from http://whatis.techtarget.com/definition/management-information-base-MIB

[10] Hung, T. C., Cuong, L. Q., & Mai, T. T. T. (2010, February). A study on any transport over MPLS (AToM). In *Advanced Communication Technology (ICACT), 2010 The 12th International Conference on* (Vol. 1, pp. 64-70). IEEE.

[11] Le Faucheur, F. (1998, June). IETF multiprotocol label switching (MPLS) architecture. In *ATM, 1998. ICATM-98., 1998 1st IEEE International Conference on* (pp. 6-15). IEEE.

[12] Mahidi, N., & Khaitan, S. (2014). Faster conversion and security issues in MPLS networks. *The International Journal of Science and Techneledge*, *2*(12), 255-260. Retrieved from

[13] Metz, C. (2004). The latest in VPNs: part II. *Internet Computing, IEEE*, *8*(3), 60-65.

[14] MPLS Benefits Explained - Why Multi-Protocol Label Switching Rocks! (2015). Retrieved April 25, 2016, from http://www.hso.co.uk/leased-lines/mpls/mpls-benefits-explained/

[15] MPLS Traffic Engineering. (1999, December 20). Retrieved April 25, 2016, from http://www.cisco.com/c/en/us/td/docs/ios/12_0s/feature/guide/TE_1208S.html

[16] Nagarajan, R., & Ekici, E. (2008). An efficient and flexible MPLS signaling framework for mobile networks. *Wireless Networks*, *14*(6), 859-875.

[17] Pepelnjak, I. (2010, October). Classes of MPLS services: Find the best MPLS/VPN service for your WAN. Retrieved April 27, 2016, from

http://searchenterprisewan.techtarget.com/tutorial/Classes-of-MPLS-services-Find-the-best-MPLS-VPN-service-for-your-WAN

[18] Rosen, E., Viswanathan, A., & Callon, R. (2001). Multiprotocol label switching architecture," RFC 3031.

[19] Rouse, M. (2007, April). What is virtual private LAN service (VPLS)? - Definition from WhatIs.com. Retrieved April 27, 2016, from http://searchnetworking.techtarget.com/definition/virtual-private-LAN-service

[20] Sinha, R. (2003, May 29). Https://www.sans.org/reading-room/whitepapers/vpns/mpls-vpn-services-security-1124. Retrieved April 25, 2016, from https://www.sans.org/reading-room/whitepapers/vpns/mpls-vpn-services-security-1124

[21] Steenbergen, R. A. (2010, June 13). MPLS for Dummies. Retrieved April 25, 2016, from https://www.nanog.org/meetings/nanog49/presentations/Sunday/mpls-nanog49.pdf

[22] Tang, B., Akyamac, A. A., Chu, C. H. K., & Nagarajan, R. (2006, November). MPLS network requirements and design for carriers: Wireline and wireless case studies. In *Telecommunications Network Strategy and Planning Symposium, 2006. NETWORKS 2006. 12th International* (pp. 1-6). IEEE.

[23] Tunneling Model for Differentiated Services Overview. (2013, July 10). Retrieved April 25, 2016, from https://www.juniper.net/techpubs/en_US/junose10.3/information-products/topic-collections/swconfig-bgp-mpls/tunnel-model-diff-serv-overview.html

[24] Vázquez, E., Álvarez-Campana, M., & García, A. B. (2004). Network convergence over MPLS. In *High Speed Networks and Multimedia Communications* (pp. 290-300). Springer Berlin Heidelberg.