# Multiprotocol Label Switching: Yesterday and Today

Adrianne Crouse

MMIS 653

Nova Southeastern University

**Abstract**

Network access methods have changed significantly since the development of multiprotocol label switching (MPLS). As an internet architecture, MPLS minimizes the need for IP header inspection by separating services from transport. The advanced networking capabilities of MPLS include fast packet service, options for traffic engineering, and both layer 2 and layer 3 virtual private networks (VPN), but the growth of technology in the data center and an increased need for flexible automated quality of service parameters reveal opportunities for improvement.

While the widespread use of MPLS among service providers is an indicator of its sophistication, some studies demonstrate higher performance in traditional IP networks or more advanced SDN networks. The functionality of MPLS, however, allows it to perform as an underlay to newer technologies, particularly where MPLS exists in stable operation.

.

.

## Multiprotocol Label Switching: Yesterday and Today

In 1999, the IETF published RFC 2547 titled BGP/MPLS VPNs. The RFC, written by two Cisco engineers, documented the use of MPLS to set up virtual routing instances to resolve problems with network segments using overlapping private IP addresses and to provide additional security. At the time, routers in non-service provider environments more likely employed static routes, routing information protocol (RIP), or open shortest path protocol (OSPF) if they were more advanced. Dial-up service was a common means of access for small businesses, but home and business internet access would soon enjoy speeds between 2Mbps and 10Mbps via digital subscriber line (DSL) and cable service providers. Internet access technologies swiftly changed over the next decade, and by 2006 when the RFC was updated, ethernet dominated the transport market and data centers, and MPLS was a buzzword. The advanced networking capabilities of MPLS include fast packet service, options for traffic engineering, and both layer 2 and layer 3 virtual private networks, but the growth of technology in the data center and an increased need for flexible automated quality of service parameters reveal opportunities for improvement.

## Literature Review or Background

Publications on Multiprotocol Label Switching (MPLS) are numerous in the Internet Engineering Task Force (IETF) Request for Comments (RFC) as well as academic studies, networking certification guides, IT related periodicals, and other writings related to internet trends. IETF RFC 2547 discusses the implantation of MPLS virtual private networks (VPNs) and the benefits of doing so (Rosen 1999). An academic study in 2000 compares MPLS networks to Asynchronous Transfer Mode (ATM) virtual circuit topologies and to traditional IP topologies which incorporate quality of service (QoS) measures for traffic prioritization and differentiation

(Armitage). A JUNOS certification guide published by Juniper in 2004 includes three chapters on MPLS functionality including the traffic engineering (TE) and VPN components examined in the RFC and Armitage study. The now defunct Frame Relay Forum which published standards on implementing frame relay virtual circuits in the 1990s published a guide for transitioning services to MPLS in 2005. The following year, Rosen updated the IETF RFC as RFC 4364, "BGP/MPLS IP Virtual Private Networks (VPNs)" (2006). Additional RFCs were published concerning MPLS including one specifically on using the MPLS header's experimental field to denote quality of service options.

Publications relating to the transition from MPLS to Software Define Networking (SDN) exist in academic works and networking how to guides. OpenFlow 1.1, a standard for moving intelligence off switches onto a controller was published in 2011 (Duffy). An IETF RFC on how SDN could benefit the service provider environment was published in 2014 (Boucadair). Chapter 1 of *SDN in the Modern Era* describes the history of internet routing via BGP, the shift from ATM to MPLS, and the development of SDN (Sonchez-Monge, 2015). An academic study later demonstrates how adding an SDN orchestrator may improve network performance over MPLS packet switched networks without a centralized controller (Bahnasse, 2020).

## Discussion

At the time of the RFC 2547 publication in 1999, Louisiana state government saw the business need for internet within K12 institutes, parish libraries and satellite offices expanding rapidly from an accountant or receptionist desk to a dozen or more computers. Ethernet (10Mbps) competed with token ring (16Mbps) for desktop access within a building. Popular wide area network (WAN) access methods such as time division multiplexing (TDM) and frame relay separated traffic into virtual circuits at the link layer in the TELCO managed devices, but

there were limitations for using these technologies in the enterprise. The chassis cards required to break out low speed TDM circuits enveloped in high speed SONET nodes were expensive, and the frame relay standard capped the access line options at a 45M DS3. The TELCOs leveraged the widespread use of frame relay using the FRF.5 standard for tunneling frame relay in Asynchronous Transfer Mode (ATM) OC3 circuits, allowing host circuits up to 155Mbps. ATM switches brought control of virtual circuits into the enterprise. As the internet exploded, the IEEE pushed Ethernet to a gigabit with 10G following close behind, birthing a most popular WAN access technology even today. The dismantling of the FRF.5 environment introduced a challenge to enterprises and service providers whose multitude of TELCO separated virtual circuits were collapsing into their own layer 3 backbone environment. While the link layer technologies changed to keep up with internet growth, firewalls and private IP space became commonplace. Re-configuring machines to avoid IP address conflicts would be disruptive and often very expensive on legacy equipment or out of support mainframes. Fortunately, RFC 2547 presented a solution, and business entities such as the State of Louisiana moved forward by rolling out MPLS VPNs.

The new infrastructure satisfied the needs of the WAN and allowed the network segments behind the firewall to occupy the same layer 3 routers and switches as the public and private WAN segments via a multitude of virtual routing and forwarding (VRF) tables. The merge allowed for simplified network management and a reduction in hardware. However, the sophisticated networking requirements of data center environment grew with the heavy load of enterprise applications, disaster recovery needs, and storage area network infrastructure. The data center, with connectivity to the cloud service providers and the redundant locations, was a network on its own, and software defined networking (SDN) vendors responded to data center

demands for centralized management with a bird's eye view and more options for network automation. The network split again into data center and user environments with separate hardware and controls.

MPLS has many capabilities, but one that is simply to deploy and clean in operation is the separation of traffic. Armitage notes that MPLS has power in its ability to tunnel packets between "non-label-switched domains" (Armitage, 2000). Where one private network is split by a carrier network segment, layer 2 VPNs allow for interior routing protocols to maintain operation as though the split did not exist. A layer 3 VPN gives the carrier visibility increased carrier network management capabilities. Either option can be relatively simply to deploy. For example, a layer 3 VRF might become operational over an existing network in just a few steps: MPLS and related label distribution protocols (LDP) are enabled, tags are applied to the entrance and exit interfaces, and routing instances are created. The result allows for a multitude of intranet and internet connections to be built across the same infrastructure (Rosen, 2006).

MPLS has a robust set of options for traffic engineering as well. Many of these rely upon label switched paths to be established for the high priority traffic. The network problems that MPLS resolves regarding converging disparate networks onto a shared infrastructure drives a need for quality of service. Carriers implementing MPLS in this manner may offer gold, silver, and bronze levels of service. Armitage compares the options presented by the MPLS 3 bit class of service field combined with the label switch paths to both the use of the IP differentiated services field and the use of multiple IP header fields combined. Armitage finds the MPLS solution to be middle ground with the multiple IP header fields implementing a variety of QoS options the most effective when deployed on high speed gigabit links on high performance switches.

Individual MPLS layer 3 VRFs provide security without the overhead of protocols such as IPSec through the separation of traffic, but this advantage has scalability issues where a VRF hosts shared services such as those related to active directory or disaster recovery. Inter-VRF traffic must be explicitly permitted in the MPLS route distinguisher definitions. With many VRFs, and multiple shared services, the simplicity of MPLS is affected; adding new segments may be complicated due to IP address conflicts, and the logical separation for security is impacted. Alternatively, VRFs may be directed to another router or a firewall, but either options adds another hop and possibly a single point of failure, and the firewall will almost certainly impact performance. Removing the policies from the network components may allow greater control; this theory follows the same logic that ATM and MPLS are founded on: simplify the transit path. In a study of voice over IP (VoIP) traffic across both MPLS and SDN over MPLS network, the SDN enabled network experienced less packet loss, greater throughput, and improved call quality. The study attributes the SDN improvement to the centralized controller (Bahnasse, 2020).

## Conclusion

Data communications networks require granularity, but complexity is not often welcome in network administration. MPLS at one time was described as “the Internet’s best long-term solution to efficient, high performance forwarding and traffic differentiation” (Armitage, 2000).

The desire for network automation and a whole network vendor agnostic view empowers programming oriented open source technologies for network orchestration and management. Though ethernet has few challengers as an access method, the delivery of ethernet services via

optical multiplexers changes continuously. Reconfigurable optical add drop multiplexers (ROADMs) are moving towards higher speeds, from 10G, 100G and 200G to 400G and 1 terabyte. As MPLS developed further as changes in access methods occurred, SDN orchestrators are expected to grow in sophistication as well, and hopefully the footprint of network access components will again be reduced.

.

## References

Andersson, L., Acreo, A.B., & Asati, R. " Multiprotocol Label Switching (MPLS) Label Stack Entry: "EXP" Field Renamed to "Traffic Class" Field", RFC 5462, February 2009. https://tools.ietf.org/html/rfc5462

Armitage, G. (2000). MPLS: the magic behind the myths. *IEEE Communications Magazine, 38* (1), 124-131, https://doi.org/10.1109/35.815462.

Bahnasse, A., Talea, M., Badri, A., Louhab, F.E., & Laafar, S. (2020). Smart hybrid SDN approach for MPLS VPN management on digital environment. *Telecommunication Systems*, *73*, 155-169, https://doi.org/10.1007/s11235-019-00603-6.

Boucadair, M. & Jacquenet, C. " Software-Defined Networking: A perspective from within a service provider environment", RFC 7149, March 2014. https://tools.ietf.org/html/rfc7149

Christophe, D. & Sen Gupta, A. (2005). *Migrating legacy services to MPLS*. MPLS Forum. http://www.webtorials.com/main/MPLScon2005/5.16_8.00AM_c_g.pdf

Duffy, J. (2011). FAQ: What is OpenFlow and why is it needed? Network World. https://www.networkworld.com/article/2202144/data-center-faq-what-is-openflow-and-why-is-it-needed.html

Moore, F. (2021). *Opening the ROADM network*. Fujitsu. https://thecinict.com/2021/03/24/opening-the-roadm-network

Rosen, E. & Rekhter, Y. "BGP/MPLS VPNs", RFC 2547, March 1999. https://tools.ietf.org/html/rfc2547

Rosen, E. & Rekhter, Y. "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, February 2006. https://tools.ietf.org/html/rfc4364

Sonchez-Monge, A. & Szarkowicz, K.G. (2015). *MPLS in the SDN era.* O'Reilly Media. https://www.oreilly.com/library/view/mpls-in-the/9781491905449/ch01.html

Soricelli, J. (2004). *JNCIS: Juniper Networks Certified Internet Specialist Study Guide*. Sybex.