HUGHES®
An EchoStar Company

MPLS VS. SD-WAN

Is it Really an Either/Or Choice?

INTRODUCTION

For 25 years, MPLS reigned as the preferred networking service. With the advent of SD-WAN, enterprises and agencies should compare relative advantages and disadvantages as they evolve their networks to meet changing needs.

Multiprotocol Label Switching (MPLS) has been widely deployed across commercial and government networks over the past 25 years. However, the time has come for many organizations to consider evolving their networks from MPLS to Software-Defined Wide Area Networks (SD-WAN) for cost-savings, agility, and scalability, especially when considering Cloud deployments and increasing demand for heightened network security.

Here, we compare MPLS vs SD-WAN and explore their relative advantages and disadvantages.

The Battle of Bandwidth

As a routing technique, MPLS applies a circuit-switched discipline to deliver packets and avoid packet loss over a distributed network. That means it is reliable and efficient at keeping traffic flowing. In addition, since the buyer leases the entire circuit, it is not shared with anyone else, making it inherently more secure. Most organizations with an MPLS network connect their locations and branch offices to a central data center, using a hub-and-spoke WAN model to connect the different points. Data travels to the data center to be processed and redistributed to the branch.

That approach worked well for decades. But that was before the Cloud, bandwidth hungry apps, broadband, Software as a Service (SaaS) and our culture's wholesale reliance on the Internet—all of which have diminished some of the distinct advantages of MPLS.

Insufficient Bandwidth

Because MPLS was designed for networks that depended on data centers, it simply is not well-suited for situations where branch or field office employees want or need direct access to the Cloud. Organizations with MPLS networks that have adopted Cloud applications must "backhaul" all traffic from their branches through their data center (or HQ) and on to the Cloud. Backhauling causes slower Internet access due to the delay or latency associated with routing traffic over longer distances to the data center and then on to the Cloud service, leading to poor user experiences. When critical Cloud applications are involved, productivity also suffers.

The problem has been magnified in the last few years by the steady rise in video traffic. In 2018, Cisco predicted that video would account for 82% of all internet traffic by 2022.[1] That was before the pandemic and the 70% spike in Internet use in 2020; and before Zoom had over 300 million meeting participants per day on its videoconferencing platform.[2]

Typical MPLS networks depend on T1 lines that are limited to only 1.5 Mbps service; the challenge here is that the standard T1 line is too small for bandwidth hungry apps and the growing number of users and devices. Since there's no end in sight to these usage trends, organizations will likely find themselves playing a costly game of catch up as they strive to meet rising bandwidth demands by adding new T1 lines, which may prove insufficient and not resolve performance issues.

Inescapable Costs

In addition to MPLS networks being inefficient when it comes to operating in a Cloud environment, they are also expensive compared with IP-based broadband deployments. Today, it's easier and much less expensive to add IP-based broadband than new private MPLS connections. Because MPLS is purchased as an entire leased line from a carrier, it is far more expensive than sending traffic over the public Internet — especially in more remote areas where costs are dictated by circuit distance. Even with new services like 3, 5, and 10 Mbps Ethernet, the costs are still much higher than IP-based broadband.

If a network needs to be expanded geographically, there is also the added expense of infrastructure and the common delays associated with deployment. As organizations expand into new areas, they may find it difficult to identify an MPLS service provider capable of coverage. For all these reasons, it is not unusual for broadband to deliver cost savings of 60% to 70% when compared to T1 and other MPLS transport options.

1 https://www.fiercevideo.com/video/video-will-account-for-82-all-internet-traffic-by-2022-cisco-says

2 https://www.livewebinar.com/blog/webinar-marketing/50-video-conferencing-statistics-for-the-year-2020

SD-WAN as a Leading Alternative

With the advent of SD-WAN, there's another option to meet the changing needs of distributed networks. SD-WAN is a virtualized WAN architecture that connects and extends networks over large geographical distances. SD-WAN can simplify branch or field office networking and assure optimal performance and security protocol application, creating a network with more capacity and security than MPLS. In their 2020 WAN Market Survey Report, Gartner stated that SD-WAN is now "becoming the de facto option for new WAN edge sourcing initiatives."

So, what are the differences between the two? As noted, traditional MPLS networks rely on static physical links to connect remote or branch users to applications hosted in data centers via a hub-and-spoke design. Data flow is typically determined by a network engineer or administrator who writes rules and policies, often manually, for each router on the network—a process that can be time-consuming and prone to errors.

SD-WAN, on the other hand, uses software to control and manage network traffic from a central location with dynamic execution at every site. SD-WAN routes application traffic over the best path in real time. In the case of Cloud services like SaaS, SD-WAN can connect to Internet- and Cloud-bound traffic directly from a branch, doing away with backhauling and delivering improved user experiences.

SD-WAN can also manage multiple types of connections, including MPLS, broadband, LTE and others, as well as support applications hosted in data centers, public and private Clouds, and SaaS services like Salesforce.com, Workday, Office 365, and Dropbox.

The flexibility and scalability of SD-WAN enable an organization to either shift completely away from MPLS or to apply a hybrid approach, seeking the right mix of MPLS connections (for high-priority data center applications, for example), broadband (for high-bandwidth and Internet-based applications), and even 4G LTE (and eventually 5G) wireless connections to meet each location's needs. SD-WAN's greatest strength might be its ability to leverage multiple broadband transports to connect field office locations securely, reliably, and cost-effectively to ensure users across the network have a consistent and high-performance experience. The result? Organizations with SD-WAN win the battle of bandwidth.

MPLS Amid a Changing Enterprise Environment

Beyond bandwidth, another issue in the MPLS vs. SD-WAN discussion centers on the assumption that encryption or additional security measures aren't necessary with MPLS. Yet, today's enterprise environment differs dramatically from that of 25 years ago, when MPLS debuted. In the late 1990s, remote workers, Cloud-based applications, and SaaS didn't exist (or at least not in their current form!) Operations and technologies have moved far beyond what MPLS was designed to support, and workarounds to its limitations often inject performance inefficiencies and other security challenges. Not only have technologies evolved, security practices and protocols have, too.

Because MPLS depends on predetermined routes that need to be designed and provisioned by knowledgeable network engineers, making changes to the network calls for significant expertise and effort. As a result, any small update to the MPLS network and its security requires coordination between telecom operators and IT teams. If that doesn't happen, security vulnerabilities can be exposed, and overall risk levels rise.

Unfortunately, applying Cloud security to MPLS doesn't solve the issue. One of the advantages of MPLS is its efficient point-to-point architecture. By forcing an MPLS network to route to a Cloud security provider, traffic flows outside the network, adding extra destinations (hops) and latency into the path; all negating point-to-point efficiencies.

Similarly, Zero Trust Network Access (ZTNA) or two-factor authentication must be validated elsewhere, like at a data center or Cloud Access Security Broker (CASB), again nullifying the advantages of an MPLS network. Here again, this routing of traffic outside the point-to-point MPLS network requires extra steps (or hops) and increases network complexity and latency—in many cases, to a greater degree than in an IP-based network optimized for this type of multi-hop approach. Consequently, MPLS networks underperform compared to IP-based networks when connecting remote users and Cloud services. They also run counter to efforts by Hughes and other industry leaders to simplify networks and make them more flexible and agile.

A Hybrid Approach to the MPLS-to-SD-WAN Transition

Given the challenges of securely connecting remote users and Cloud services via MPLS and its higher costs, does it make strategic sense for an enterprise to transition away from its MPLS network? Eventually, yes. For the short term, however, many organizations will choose a hybrid approach with a combination of MPLS and broadband.

As mentioned earlier, SD-WAN is transport agnostic and can be deployed to manage multiple types of connections, including MPLS, broadband, LTE and others. Further, SD-WAN is

designed to allow centralized management, allowing network policies to be easily applied across all WAN devices, creating network agility and simplifying operations. Even with applications hosted in data centers, public and private Clouds, or SaaS services like Salesforce.com and Office 365, SD-WAN routes application traffic over the best path in real time to improve user experiences.

Succeeding with a hybrid strategy hinges on understanding how and where to leverage the MPLS network's advantages versus the Cloud-enabled SD-WAN solution's benefits. For example, an organization may choose MPLS to connect multiple data centers or to support applications and traffic volume served exclusively from one data center, while using

SD-WAN to serve branch location traffic going to the Internet or Cloud services more efficiently. This is ideal for sectors, such as healthcare and banking, which will likely always have justification for private circuits. Of course, organizations that don't require the advantages of MPLS can move confidently to a lower cost, more agile, and more capable

SD-WAN network.

Eventually, MPLS usage will shrink as SD-WAN capabilities fill the gaps. In fact, we already see this across many Hughes customers. But there's no pressing need to choose SD-WAN over MPLS or to view it as an either/or proposition. MPLS will be with us for many more years. The key action is to assess your network needs, determine whether a hybrid approach fits, and develop a strategy for which sites and technologies should be supported by MPLS and which are better suited to SD-WAN. Then, as technology evolves and MPLS becomes less critical, your enterprise will be firmly positioned on the path to digital transformation.

For a different look at how SD-WAN works, watch this video from our colleagues at Hughes Europe.

For additional information, please call 1-888-440-7126 or visit www.hughes.com.

HUGHES
An EchoStar Company

11717 Exploration Lane
Germantown, MD 20876 USA

www.hughes.com