MPLS vs. SD-WAN: Which Is Best For Your Network?

Comparing MPLS and SD-WAN to determine the winners and losers of each network technology

Is it a fair argument to compare SD-WAN (software-defined networking) to MPLS (Multiprotocol Label Switching)?

We'll let you be the ultimate judge of that. But for the sake of those still searching for clear answers, we at EnableIP wanted to share our take.

First, let's make sure we're focused on what we believe is most important in this comparison:

Both MPLS and SD-WAN solutions have come to exist in order to carry applications across the Wide Area Network (WAN) in the most timely and efficient manner. These applications are used by employees at a business to perform a series of job functions:

- Sending email to customers and vendors
- Carrying phone or video calls
- Inputting data into a cloud-based ERP or CRM
- Backing up critical data in real-time (or near-real-time)
- POS systems used to run credit cards and track inventory

It's that simple really.

The real discussion is about which technology — MPLS or SD-WAN — will allow your employees to experience the best performance without taxing IT resources. In the article below, we hope to help you determine which technology achieves the highest marks for each major category.

Cloud Controllers

What if you could control your entire data network across a single cloud-based controller, and implement those policies to all the devices?

What a novel concept…

MPLS networks can, in fact, do this — but it's limited to Class of Service (CoS) settings and routing, and it's at the carrier level that these options have to be requested.

SD-WAN, on the other hand, has the ability to control application policies, firewall policies, best-path/link bonding policies. Every aspect of the WAN is able to be controlled with SD-WAN from a simplified graphical user interface (GUI) as opposed to complicated configuration settings.

The MPLS providers have SD-WAN type functionality at their fingertips, but this is rarely ever given to the end-user customer.

Winner: SD-WAN (by a wide margin)

Static vs. Dynamic

MPLS is configured by the provider to carry traffic using a certain set of policies (CoS or QoS) and network tags related to the application performance that the customer is most interested in supporting. This can only be changed by the carrier when a customer submits an order request. For the sake of argument, let's say the change takes 1 week to implement. Even though you may not need to change the network tags very often, the point here is that it can't be changed easily.

With SD-WAN, on the other hand, applications that are most important can be identified using a single policy and, seemingly by magic (aka pre-set configurations provided through a GUI setting), the traffic that's most important to your business will be provided the best route while throttling the lower priority traffic and thus sending out the degraded circuit. This happens "auto-magically" through the use of dynamic settings that have rules applied to them based on certain network congestion situations.

Winner: SD-WAN

Network Up-Time

With MPLS, the router has the ability to fail from SD-WAN to another network solution — and it's relatively immediate. But calls will occasionally be dropped and other web-based sessions will likely be lost. MPLS doesn't allow for real-time link bonding or best-path allocation.

Using SD-WAN, a customer has the ability to bring in multiple connection types (including MPLS) into a customer site and fail those connections over to one another in the event of an outage in a matter of milliseconds. With the use of dynamic DNS, your employees' use of applications isn't impacted as all calls and sessions will stay active.

In addition, multiple connections also allow for real-time link bonding, which is where the SD-WAN device identifies the best-path based on the application and sends the traffic down the appropriate link. SD-WAN's ability to identify network connection is not only on par with MPLS, it's slightly ahead in our view because there's more bandwidth available since it can be purchased at a lower price point. So arguably, there's less congestion and a better user experience.

Yep, you guessed it:

Winner: SD-WAN

Integrated Security

MPLS is a closed user group network, which means it's private with no public facing IP addresses. Some have mistaken the private nature of MPLS to mean that it's inherently secure. However, MPLS allows for shared network elements, and it doesn't offer any encryption of packets with no firewall capabilities inherent to any of its features.

While SD-WAN primarily focuses on public facing internet connections, it can actually be made to be highly secure because of integrated security features such as intrusion detection, packet encryption, web-filtering,

application firewalling and deep packet inspection, to name a few features. In most cases, the SD-WAN solutions available include a fully featured next generation firewall completely integrated into the solution.

Winner: SD-WAN

Remote Site Performance

MPLS does improve packet-specific performance at remote sites by packet tagging and predetermined destination forwarding of packets. These features allow for packets to be prioritized based on the application that is sending the packets. In the event of network congestion, this will allow the more latency sensitive packets to be prioritized and sent to their destination first.

As previously mentioned, SD-WAN treats packets a little differently by identifying the path that has the least amount of congestion to be used for priority applications. SD-WAN's goal is to remove congestion as an issue through link bonding of multiple connections in order to pass application traffic to the best path available. In addition, should there be an outage of one of the links, the traffic instantaneously will be rerouted across the secondary or tertiary connection without the user even noticing.

So, while MPLS does have inherent improvements for remote sites, it doesn't have the ability to use multiple connections. As a result, MPLS doesn't actually limit network congestion — it just solves for it when it occurs.

Once again:

Winner: SD-WAN

Provider Independence

Image no longer being beholden to a single provider. Sounds dreamy, right?

MPLS requires a single carrier provider because of the nature of it being a closed user group and a private network.

SD-WAN solutions, on the other hand, can involve MPLS networks, but it can also be 100% public internet connections as well. In the case where it's all public, any internet connection can be used at any location. This allows for the flexibility of finding the *best* last mile provider, which not only helps lower costs but also assists with network troubleshooting since it's a loop and port provided by the same provider.

In our view, MPLS holds the customer hostage to a single provider and is too dependent on multiple last mile providers (loop providers) to provide connectivity back to the MPLS providers ports. This is expensive and often more difficult for your carrier to troubleshoot.

Winner: SD-WAN (bigtime)

Which is Best: MPLS or SD-Wan?

Make no mistake, there's still a place for MPLS networks when there's very sensitive information and extreme latency sensitive applications, just like there's still a place for Point-to-Point private lines. However, the majority of businesses are finding that SD-WAN allows for more scalability, simplicity, visibility and control — all while still being able to play well with an MPLS network thrown in for those applications that require a private connection (with the inherent benefits of security that SD-WAN offers).

When it comes to MPLS vs. SD-WAN, a head-to-head comparison isn't really possible because of all the inherent features that are now rolled into SD-WAN (i.e. VPN device, NG firewall, cloud controller, link bonding, instantaneous failover, etc.)

In addition, SD-WAN technology *can* and *does* support 99.5% of the applications across the web. With nearly 30 major providers of SD-WAN solutions, it's a matter of identifying what is most important to your organization and finding a solution provider that can provide solutions that meet your most important needs.

About Enable IP

EnableIP is a telecom solutions provider founded by Wired Networks' founder Jeremy Kerth and head engineer Steve Roos after they realized there was a deep market need for helping mid-size businesses establish better uptime rates for their Wide Area Networks (WANs). Armed with the best-in-class carriers and partners, Jeremy and Steve set out with a bold plan: **Guarantee better uptime rates than the industry standard of only 99.5%.**

Their bold plan became a reality. EnableIP's solutions guarantee clients 99.99% (even 99.999%) network uptime. But we don't stop there. Many telecom providers promise high availability network solutions but fail to deliver because they're in the business of providing services, not solutions.

That's the EnableIP difference: We deliver highly available networks by providing a complete system (called "Cloud Assurance") that ensures 99.99% or above uptime.

We deliver this bold promise by:

- ✔ Owning the entire customer experience. From pricing, contracting, ordering and provisioning to installing, servicing and billing—we do it all! This means no stressful negotiations, confusing setups, or finger pointing if something goes wrong. We actually *deliver* on our promise.

- ✔ We manage the entire system, and monitor and manage issues as they occur so you can focus on your business—not your network.

The Enable IP solution is like no other. Contact us to get started and experience the difference of a system that truly delivers on its 99.99% network uptime promise.

More Resources

How To Migrate From MPLS To SD-WAN Internet

View White Paper

Essential Networking Hardware for Mid-Market Businesses

View White Paper

What WAN Is & Which Kind Your Business Needs

View White Paper