

[← Cloud Security](#)

Cloud Security

MPLS | What Is Multiprotocol Label Switching

5 min. read

What Is MPLS?

Before we dive into MPLS, let's explain how data travels through the internet. When you send an email, connect to VoIP or video conferencing, that data packet or IP packet is sent from one internet router to its destination. The internet router must decide for each IP packet/data packet how it's sent to the destination IP. Each packet requires a decision, which the router uses complex routing tables to determine. Every path the packet arrives at requires another forwarding decision until it arrives at its destination. This process can result in poor performance for users, the applications they are using and impact the network across an organization. MPLS provides an alternative for organizations to increase network performance and improve user experience.

MPLS Meaning

Multiprotocol Label Switching, or MPLS, is a networking technology that routes traffic using the shortest path based on "labels," rather than network addresses, to handle forwarding over private wide area networks. As a scalable and protocol-independent solution, MPLS assigns labels to each data packet, controlling the path the packet follows. MPLS greatly improves the speed of traffic, so users don't experience downtime when connected to the network.

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)

[Manage My Cookie Settings](#)

internet-wide addressing and routing using IP protocols. MPLS sits in between these two layers, with additional features for data transport across the network

What Is MPLS Used For

Organizations often use this technology when they have multiple remote branch offices across the country or around the world that need access to a data center or applications at the organization's headquarters or another branch location. MPLS is scalable, provides better performance and bandwidth, and improves user experience compared to traditional IP routing. But it is costly, difficult to deliver globally and lacks the flexibility to be carrier independent.

As organizations move their applications to the cloud, the traditional MPLS hub-and-spoke model has become inefficient and costly because:

- It requires backhauling traffic through the organization's headquarters and out to the cloud instead of connecting to the cloud directly, which impacts performance significantly.
- As companies add more applications, services and mobile devices to their networks the demand for bandwidth and cloud expertise increases costs and operational complexity.

How MPLS Networks Work for Cloud Adoption

MPLS networks were designed as an overlay tactic to simplify and improve performance. However, routing cloud traffic is not easy with MPLS. To make cloud traffic more efficient, many organizations are exploring how to supplement MPLS with other types of connections, such as:

- **MPLS offloading:** By using a direct-to-internet connection, an organization can offload the traffic that was bound for the web in the first place. This way, the MPLS circuit only carries the traffic intended for headquarters. The question is how to address security for branch internet connections. An organization might have to add a full stack of security products at the branch, which introduces complexity, or it might forward internet traffic through a proxy, which doesn't provide the same level of security or inspect non-web traffic.

• **MPLS replacement with direct-to-internet:** An organization might completely

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)

with affordable broadband internet links or replacing it with internet to optimize branch networking decisions based on the application, networking and bandwidth requirements.

MPLS vs. SD-WAN

SD-WAN is a solution that enables end-to-end enterprise connectivity over large geographical distances. It provides the flexibility and economics of multiple WAN links such as MPLS, wireless, broadband, virtual private networks (VPNs), and the internet to give users in remote offices access to corporate applications, cloud services and workloads, allowing them to work regardless of location. SD-WAN monitors the performance of WAN connections and manages traffic intelligently based on these measurements in an effort to maintain high speeds and optimize connectivity. SD-WANs offer organizations agility and cost savings compared to an MPLS infrastructure which is costly and not easy to make changes to. With centralized management that is often cloud-managed, it simplifies configuring and provisioning networks at scale and speed, greatly reducing operational complexity. The argument for SD-WAN vs. MPLS is never-ending, and organizations may end up choosing a hybrid of both to fit their needs.

Palo Alto Networks Prisma SD-WAN is the first next-generation SD-WAN that is application-defined, autonomous and cloud-delivered. With an application-defined approach to complete, end-to-end visibility, it provides deep SD-WAN analytics to application performance, automating application remediation and ensuring application resiliency. Prisma® SD-WAN enables branch security and networking with a cloud-delivered model while automating third-party integrations for branch services seamlessly to simplify operations. With its autonomous infrastructure, organizations can achieve quick troubleshooting and resolution using machine learning and data science capabilities.

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)

Palo Alto Networks Next-Generation SD-WAN



Consider a SASE Approach

Today, many organizations are redesigning their wide area networks, so their branch offices and mobile users can directly connect to the cloud via cloud-delivered security infrastructure or secure access service edge (SASE). This enables organizations to provide users with secure access to all applications, gain full visibility and inspection of traffic across all ports and protocols, and increase the available bandwidth regardless of the MPLS or SD-WAN strategy the organization is using.

Palo Alto Networks Prisma SASE is the industry's only complete SASE solution converging network security, SD-WAN and Autonomous Digital Experience Management into a single cloud-delivered service.

Some of the benefits of SASE include:

- **Simplified networking** as organizations can leverage the cloud for security and networking without having to backhaul traffic to headquarters.

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)

- **Consistent security** when organizations can consistently apply and enforce their security policies across all branch locations and headquarters.
- **An improved user experience** wherever an organization operates.
- **Centralized operations** to automate change management such as configuring and provisioning networking and security settings at scale.

Learn more about how [Prisma SD-WAN](#) and [Prisma SASE](#) can help your organizations transition to the cloud to support your hybrid and mobile workforce.



Share page on facebook



Share page on linkedin



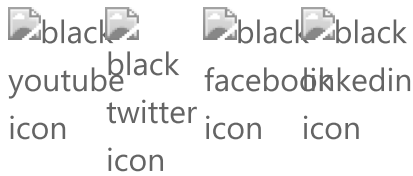
Share page by an email

Get the latest news, invites to events, and threat alerts

Your email

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)

By submitting this form, you agree to our [Terms of Use](#) and acknowledge our [Privacy Statement](#).



EN

Popular Resources

[Blog](#)[Communities](#)[Content Library](#)[Cyberpedia](#)[Event Center](#)[Investors](#)[Products A-Z](#)[Tech Docs](#)[Unit 42](#)[Sitemap](#)

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)

Terms of Use

Documents

Popular Links

About Us

Customers

Careers

Contact Us

Manage Email Preferences

Newsroom

Product Certifications

Report a Vulnerability

[Create an account or login](#)

Copyright © 2023 Palo Alto Networks. All rights reserved

This site uses cookies essential to its operation, for analytics, and for personalized content and ads. By continuing to browse this site, you acknowledge the use of cookies. [Privacy statement](#)