Cyber Hub (/cyber-hub/) / Secure The Network (/cyber-hub/network-security/)

/ What is MPLS?

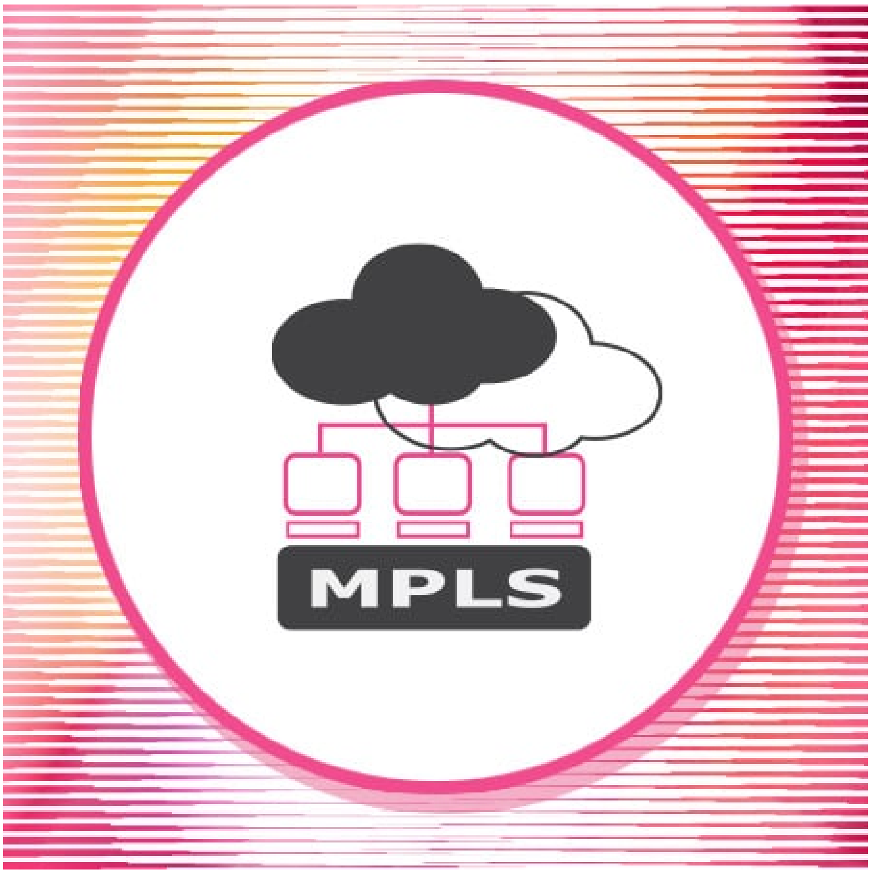
# What is Multiprotocol Label Switching (MPLS)?

Multi-protocol label switching (MPLS) is a routing technique used in carrier backbones and in enterprise networks to connect branch offices and enterprises that need quality of service (QoS) for real-time applications. Instead of using complex lookups in a routing table like that used in IP networks, MPLS directs traffic using path labels rather than long network addresses, thus the name label switching.

MPLS is multi-protocol, i.e. it was designed as an overlay and is able to encapsulate other network protocols. This packet switching technique groups transmitted data as it enters the MPLS network into packets with a header and a payload. Along the path, a label in the header is used by MPLS routers to direct the packet to its destination, where the payload is then extracted and used by application software.

**Request a Demo (https://pages.checkpoint.com/harmony-connect-internet-access-demo.html)**

**SD-WAN Buyer’s Guide (https://pages.checkpoint.com/sdwan-buyers-guide.html)**



## How Does MPLS Work?

When traffic enters the MPLS network, an ingress MPLS router will add an MPLS header to it. This assigns a forwarding equivalence class (FEC), indicated by appending a short bit sequence (the label) to the packet.

The MPLS header or label stack contains 4 fields:

1. A 20-bit label that determines where the packet is to be forwarded.
2. A 3-bit field originally named Experimental that today is used for QoS priority and ECN (Explicit Congestion Notification).
3. A 1-bit bottom of the stack field that, when set, indicates the packet has reached the end of the MPLS network.
4. An 8-bit time-to-live (TTL) field.

By encapsulating data, MPLS separates forwarding mechanisms that can be used to create forwarding tables for any underlying protocol. The FEC defines routing criteria that are used to create a predetermined path to route traffic through the MPLS network, which is called a label-switched path (LSP). These paths are unidirectional, and return traffic is sent over its own LSP.

The primary goal of MPLS is to improve the performance and reliability of network traffic. However, it does have some security benefits as well. While MPLS links are not encrypted, they are partitioned from the rest of the Internet, providing security similar to a virtual private network (VPN (/cyber-hub/network-security/what-is-vpn/)).

## MPLS Disadvantages

MPLS provides certain performance benefits, but it has its downsides as well. Some of the limitations of MPLS include:

- **Centralization**: MPLS circuits are typically laid out in a hub-and-spoke model that routes traffic through the headquarters network. As remote work and cloud computing become more common, these routing inefficiencies can create network latency.
- **Cost**: MPLS circuits provide better network performance and reliability than broadband Internet. However, MPLS bandwidth costs significantly more per bandwidth than broadband Internet.
- **Geographic Footprint**: MPLS circuits are dedicated circuits partitioned from the public Internet as part of an ISP’s network. This limits where MPLS can be deployed based upon where an ISP has MPLS circuits available.
- **Provisioning Delays**: The process of provisioning dedicated MPLS circuits on an ISP’s network is a slow one. This limits an organization’s agility and ability to react to sudden surges in traffic.

## MPLS Alternatives - SD WAN

MPLS is designed to implement a high-performance, reliable WAN. However, these benefits come at a significant cost and force organizations to accept the limitations of MPLS.

As these MPLS drawbacks begin to hinder the achievement of business goals, Software-defined WAN (/cyber-hub/network-security/what-is-sd-wan/) (SD-WAN) is an MPLS alternative (/cyber-hub/network-security/what-is-sd-wan/mpls-alternatives/) that allows organizations to more cheaply and easily create a flexible, high-performance, and reliable corporate WAN.

Rather than relying on dedicated links, SD-WAN works by optimizing the use of available transport media. SD-WAN appliances aggregate various transport media (broadband, MPLS, mobile networks, etc.) and select routes based upon application-specific policies. This enables expensive, high-performance bandwidth (like MPLS links) to be reserved for application traffic that requires these features, while less important traffic (like web browsing) is routed over less expensive links.

By decreasing an organization's dependence on MPLS circuits, SD-WAN not only decreases costs but also improves network flexibility. SD-WAN can use transport media that lack the same geographic restrictions as MPLS and can be deployed more quickly and cheaply. This allows traffic to be routed anywhere, not just where MPLS links are available.

## SD-WAN Solution with Check Point

MPLS provides high-performance, reliable connectivity at the cost of a high price tag and decreased flexibility. As enterprise networks evolve, SD-WAN provides an alternative that better fits enterprise business needs.

When selecting an SD-WAN solution, it is important to choose one that meets both networking and security requirements. By default, SD-WAN lacks encryption and integrated security just like MPLS. However, some SD-WAN solutions offer built-in software-defined protection to secure the traffic flowing over the corporate WAN.

Check Point's SD-WAN Security solutions (/solutions/sd-wan-security/) integrate with all major SD-WAN solutions. To learn more about deploying a Secure SD-WAN solution, check out this buyer's guide. Then, request a demo (/solutions/sd-wan-security/technology-partners/) to see how Check Point solutions integrate with your preferred SD-WAN solution.

Check Point also offers secure remote connectivity for remote users and branch offices via Secure Access Service Edge (/cyber-hub/network-security/what-is-secure-access-service-edge-sase/) (SASE). Learn more with a free demo (https://pages.checkpoint.com/harmony-connect-internet-access-demo.html) of Check Point Harmony Connect.

## Get Started

SD-WAN Security (/solutions/sd-wan-security/)

SASE (Secure Access Service Edge) (/harmony/connect-sase/)

Branch Office Firewalls (/quantum/next-generation-firewall/branch-office-security/)

## Related Topics

What is SD-WAN? (/cyber-hub/network-security/what-is-sd-wan/)

What is SASE (Secure Access Service Edge)? (/cyber-hub/network-security/what-is-secure-access-service-edge-sase/)

Top 3 Benefits of SASE (/cyber-hub/network-security/what-is-secure-access-service-edge-sase/top-3-benefits-of-sase/)

MPLS Alternatives (/cyber-hub/network-security/what-is-sd-wan/mpls-alternatives/)

Benefits of SD-WAN (/cyber-hub/network-security/what-is-sd-wan/benefits-of-sd-wan/)

## Recommended Resources

2023 Miercom NGFW Firewall Security Benchmark

(https://resources.checkpoint.com/network-security/2023-miercom-

Cyber Security Report 2023

Combat Against Sophisticated Cyber Attacks with Check Point's Next...

network-security-firewall-competitive-report?utm_term=cyber-hub&utm_content=td)

(https://pages.checkpoint.com/cyber-security-report-2023.html?utm_term=cyber-hub&utm_content=td)

(https://pages.checkpoint.com/nex generation-firewall-buyers-guide.html?utm_term=cyber-hub&utm_content=td)