Ebook

Simplify your migration from MPLS to SASE

Tips to reduce risk when modernizing your network

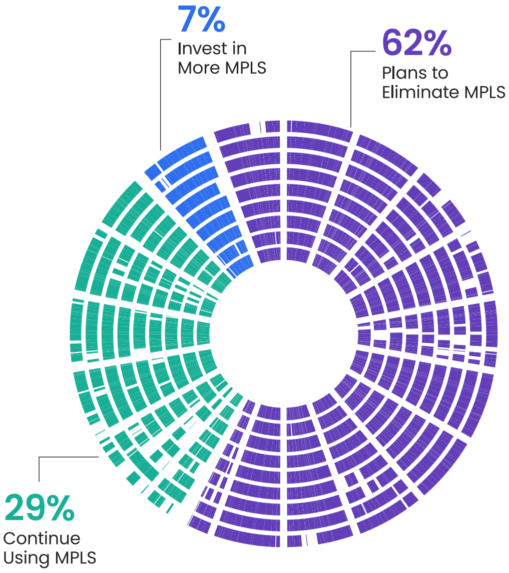
aryaka

Time to Retire Your MPLS?

MPLS has reliably served enterprises for more than two decades, but in a cloud-first world it comes with limitations that are increasingly difficult to justify. As a result, MPLS continues to shrink in proportion to the overall WAN market.

According to a 2023 Enterprise WAN survey of CIOs, CISOs and IT leaders, 62% plan to eliminate MPLS vs. just 7% who plan to invest more.

Given the clear trend, why are enterprises taking so long to move away from MPLS?



Perception of risk? Or fear of change?

Enterprises hold onto antiquated MPLS networks because of perceived risks and the apprehension that comes with network migration. Common concerns include:

Network performance and security

Some organizations believe MPLS is the only way to attain guaranteed performance and reliable security.

Internal resources

Change requires time and expertise that are often in short supply.

Migration complexity

Nobody wants unexpected surprises or outages, and large-scale network migrations are often viewed as risky.

Whether they are real or perceived, all of these risks can be mitigated and avoided with the right approach.

Tips for Mitigating MPLS Migration Risk

1. Platform: choose the right tools for the job

While MPLS was a secure option in the past, it may be causing organizations more security issues than benefits in today's world of cloud workloads and applications.

Some important questions to consider when preparing to migrate from MPLS:

- Which applications require the highest level of performance?
- Which offices or users may require an enhanced level of performance?
- Which offices or geographies experience challenges accessing certain environments?
- Do critical times of the day/month/year require more strict performance requirements?
- Where does company sensitive data live?
- What security policies need to be implemented that have not?

After answering these questions, teams can evaluate new network tools and platforms that will best achieve their application performance and security needs, such as:

Software-defined.

Managed SASE solutions and secure SD-WAN provide IT teams with much more flexibility and visibility to optimize routing of critical and latency-sensitive applications. Additionally, scaling or descoping transport is much simpler with a secure SDN than MPLS.

Line-of-sight to the network.

The downstream peering arrangements with your provider have a substantial impact on network performance. Organizations should leverage platforms or providers that give a holistic view of network performance across first, middle, and last miles of connectivity.

Security Embedded.

Network events and security events are now not only related, but often indistinguishable from each other. Reducing complexity and providing easy correlation between events is critical for teams required to respond to an evolving threat landscape.

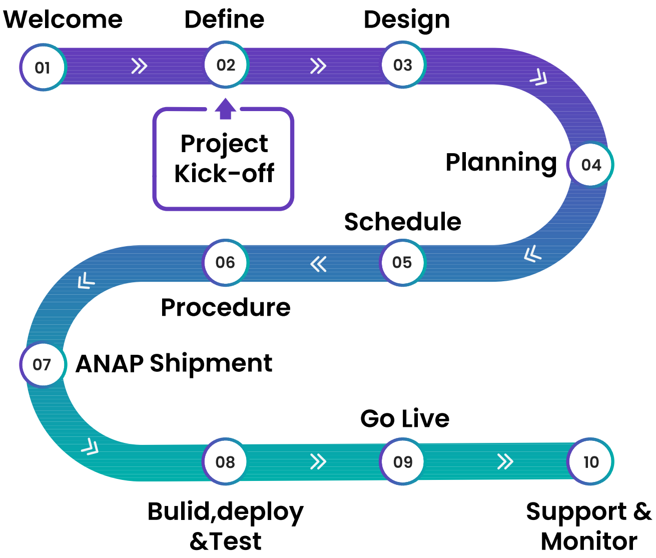
Converged Analytics.

Gone are the days of the black box for your network traffic. Modern IT teams rely on cloud-like reporting and visibility that is available at their fingertips, 24x7.

2. Plan: define a 'tried and trusted' migration plan

While creating migration plans is never fun, these strategies can spare you from unnecessary headaches and risk:

Create a project plan.



Phase the deployment

It's important to note that network migrations can, and often should, be performed in stages. As the saying goes, you do not need to eat the whole elephant at once.

Plan for everyone that may be impacted

IT teams focused on the technical aspects of the migration sometimes lose sight of the other ancillary plans and impacted teams. Some workflows and plans that may need to be created, revised, or reviewed include:

- **Stakeholder communications:** Define who, how, and when stakeholders will be notified of key events.
- **Change management:** Update for new partners, tools, or policies.
- **Network staging and link provisioning:** Outline any hardware staging needs and circuits that need provisioning or deprovisioning.
- **Documentation:** A migration is one of the best times to inventory, update, and create new documentation across the enterprise.
- **Incident response plan:** As new partners and vendors integrate, update incident response plans to account for how the team will respond to new events that arise.

These plans become significantly easier when migrating off of MPLS to a well-established platform with the help of an experienced partner.

95% of C-level leaders expect managed services and network-as-a-service to play a bigger role in 2023.*

*Source: The Report on Enterprise Network Transformation, 2023 Survey

3. People: build a winning team of experts

To ensure success, leverage a team that has done it before to help you identify potential issues early, before they turn into actual problems.

As an example, the team at Aryaka has helped 500+ enterprises from every vertical and geography migrate from MPLS to managed SD-WAN / SASE / NaaS. Some lessons that we have learned over the years include:

- Assign a Dedicated Project Team. Acting as an extension of your staff, ensure seamless execution with a:

- **A dedicated project manager**
- **A network architect**
- **CCIE or equivalent**
- **24/7 NOC**

- Agree on Strict Service Level Agreements. SLAs should extend to the performance of first, middle and last mile of service. Additionally, establish SLAs for service-related items such as tickets, maintenance, and incident response.
- Document the Process. The knowledge stored in the network team's collective heads needs to find its way onto a shared document repository where it can be reviewed and updated as needed.

Aryaka can help.

Aryaka has helped countless enterprises migrate from legacy MPLS networks to modern, software-defined architectures. Helping in every facet from project planning to documentation, our goal is to not only make migration easy, but fast. Contact us today!

About Aryaka

Aryaka is the leader in delivering Unified SASE as a Service, a fully integrated solution combining networking, security, and observability. Built for the demands of Generative AI as well as today's multi-cloud hybrid world, Aryaka enables enterprises to transform their secure networking to deliver uncompromised performance, agility, simplicity, and security. Aryaka's flexible delivery options empower businesses to choose their preferred approach for implementation and management. Hundreds of global enterprises, including several in the Fortune 100, depend on Aryaka for their secure networking solutions. For more on Aryaka, please visit www.aryaka.com.

Schedule a Free Network Consultation with an Aryaka Expert

See How It Works Live →

Experience Aryaka's Unified SASE as a Service

View Interactive Tour →