aryaka

WHITEPAPER

How to mitigate MPLS migration risk

Tips to network modernization

© 2025 Aryaka Networks, Inc. All Rights Reserved

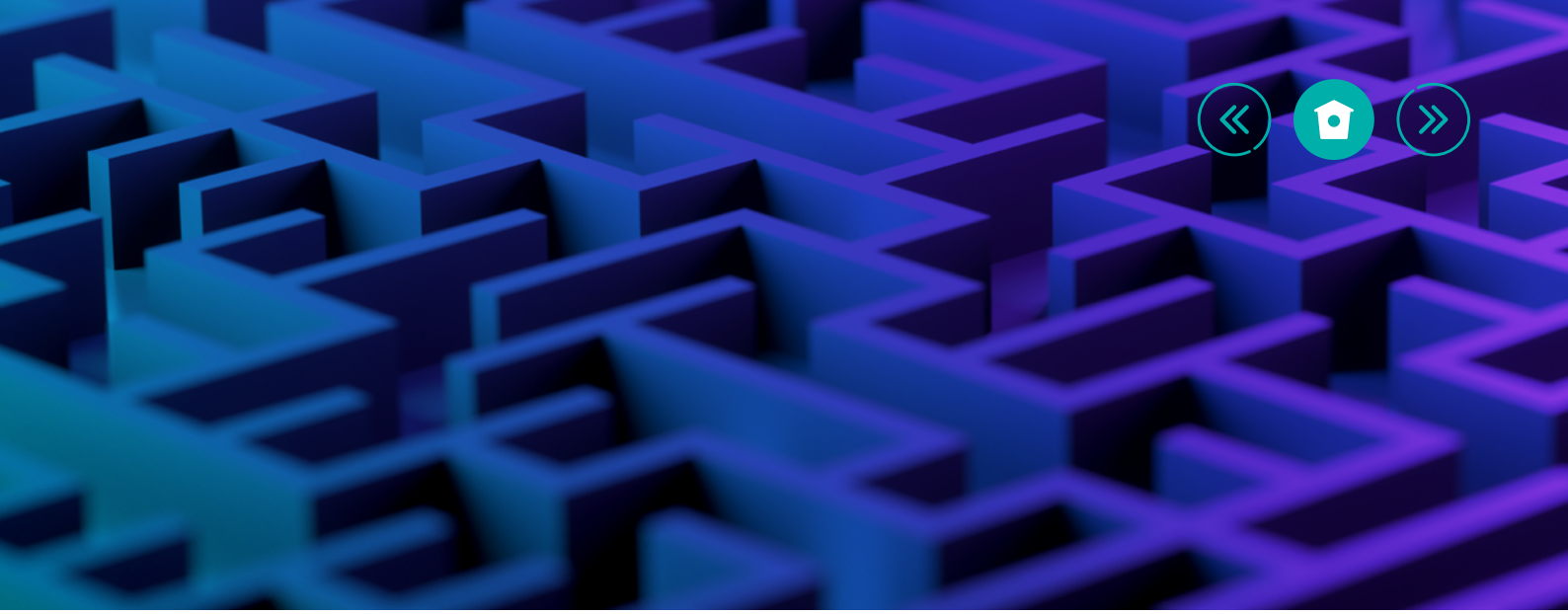


Table of Contents

MPLS is dying, right? 02

The perception of risk? Or the fear of change 03

Steps for Mitigating MPLS Migration Risk 03

Choosing the Right Tools 03

Elements of a Modern Network Architecture 04

Three P's of MPLS Migration 04

Migration Plans 05

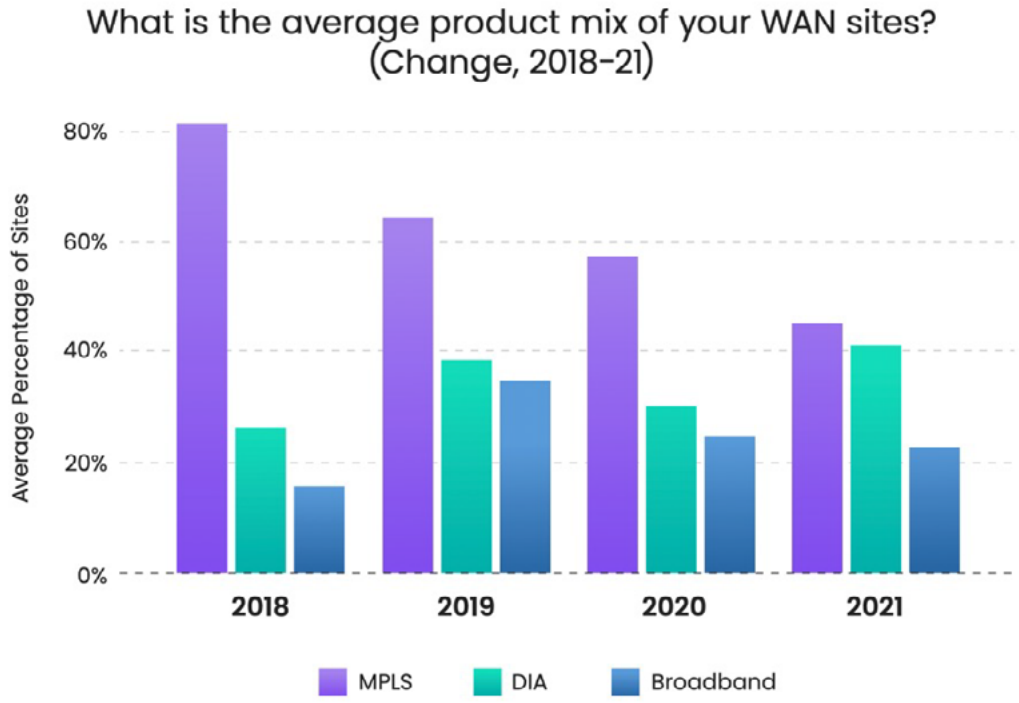
Team Selection 06

About Aryaka 07

MPLS is dying, right?

MPLS has reliably served enterprises for more than two decades. In a cloud-first world though, it comes with limitations that are increasingly difficult to justify and as a result, usage rates are in sharp decline over the last 5 years.

In 2018, 82% of enterprises were still leveraging MPLS but by 2021, only 46% still reported relying on the outdated technology.



With more flexible alternatives such as managed SD-WAN / SASE / Network-as-a-Service (NaaS) and the continued migration of workloads to the cloud, the question is not why MPLS usage is declining but rather, why are 46% of enterprises still using it?

The perception of risk? Or the fear of change

Many enterprises are holding 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.

Steps for Mitigating MPLS Migration Risk

Step 1. Choose the Right Tools for the Job.

Perhaps the biggest mis-perception among network teams retaining MPLS is the idea that it provides the highest level of security and application performance available. While that may have been true in the past, in a world where applications and workloads live in the cloud, MPLS is likely causing the organization more harm than good.

The first step before migrating is gaining a more granular view on the performance needs and security requirements across the organization. Questions to consider:

- Which applications require the highest level of performance?
- Are there offices or users that require an enhanced level of performance?
- Are there offices or geographies that traditionally have challenges accessing certain environments?

- Are there certain critical times of the day/month/year that require more strict performance requirements?
- Where does company sensitive data live?
- What security policies need to be implemented that have not?

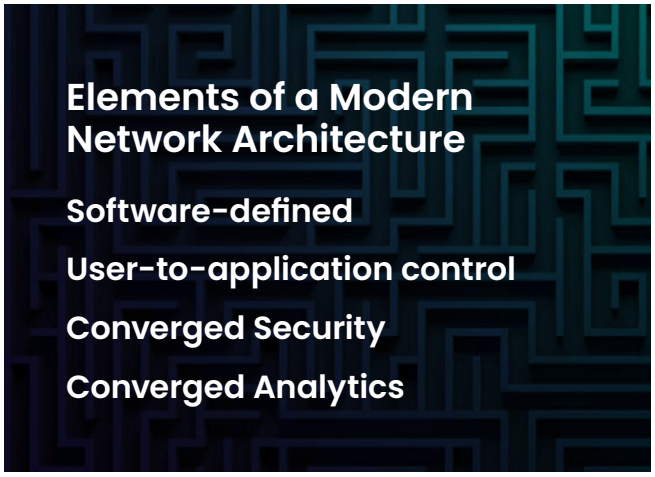
From this deeper understanding of the application performance and security needs, teams can then start to evaluate tools and platforms. While this may vary from enterprise to enterprise, some general rules of thumb include the following.

Software-defined.

Without a doubt, the single most important aspect when migrating from MPLS is to deploy a software-defined network. Managed SD-WAN / SASE / NaaS solutions provide IT teams with an incredible amount of flexibility and visibility to optimize routing of critical and latency-sensitive applications. Additionally, scaling or de-scoping transport is infinitely simpler with a SDN than MPLS.

Line-of-sight to the network.

Where many enterprises stumble during their transition to a next-generation solution is not having clear visibility into the network that sits between them and their applications in cloud environments. The downstream peering arrangements between your provider has an incredible impact on the performance of the network as a whole. Organizations should leverage platforms or providers that give a holistic view of network performance across first, middle, and last miles of connectivity.



Security Embedded.

Modern network architectures are built with security as part of the platform, not a bolt-on that sits outside of it. 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.

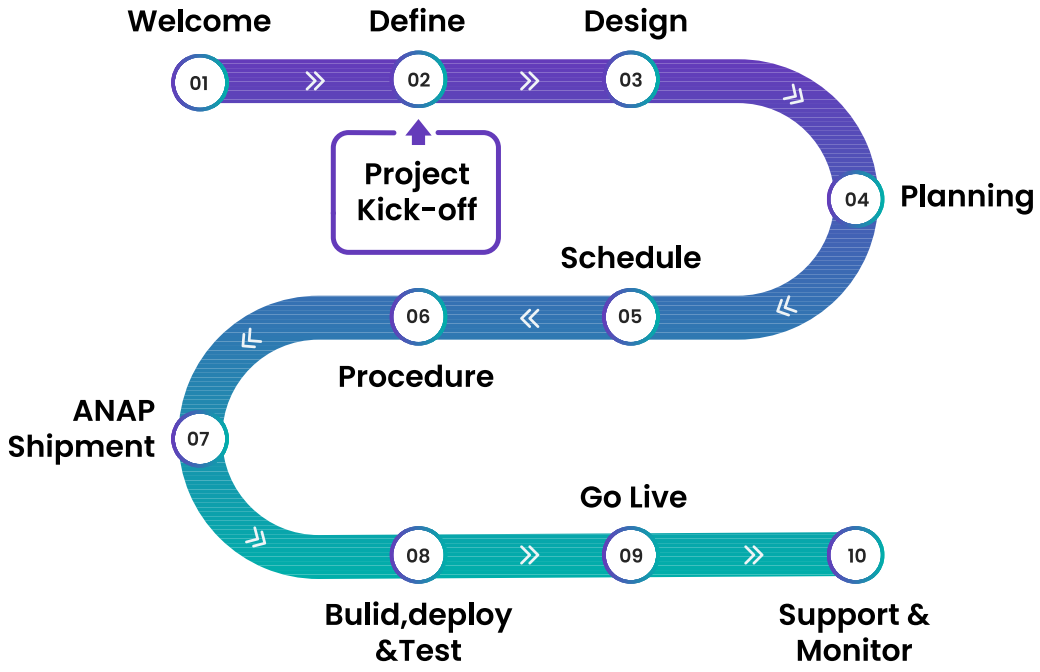
Similar to the convergence of security in the network, enterprise teams require a granular level of visibility across networks. Gone are the days of the black box for your network traffic. Modern IT teams rely on cloud-like reporting and visibility that is available at their fingertips, 24x7.

Step 2. Define a migration plan

While creating migration plans is never fun, when it comes to migrations, they are necessary. Here are some elements to consider when developing your migration plan.

Create a project plan.

Aligning on an agreed upon timeline and phasing of events will help to coordinate efforts. Consider things like holidays, major launches, seasonal fluxes, and even company blackout periods.



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.

Create the right plans.

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.** Defines who, how, and when stakeholders in the organization will be notified of key events.
- **Change management.** Review updates and procedures to the change management plan as a result of new partners, tools, or policies.

- **Network staging and link provisioning.** Define a section of the plan to outline any hardware staging needs and circuits that need provisioning or deprovisioning.
- **Documentation.** A migration is one of the best times to assess the level of documentation across the enterprise. Inventory, update, and create documentation as needed.
- **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 and when working with the right team who has conducted migrations in the past.

Migration Workflows and Plans

- Stakeholder communications
- Change management
- Network staging
- Link provisioning
- Documentation
- Reporting
- Incident response plan

Step 3. Get the right team behind you

You will want to enlist the help of team members or outside teams who have done the migration before. Expertise is derived from experience, helping to quickly identify potential issues early, before they have a chance to grow into actual problems.

As an example, the team at Aryaka has helped 100s of enterprises from every vertical and every 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. Assigning a dedicated project team is critical for success. The nuances and details of the migration warrant a team of experts to plan and execute the migration. The team becomes an extension of your team and includes:

Dedicated Project Team

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

- Agree on Strict Service Level Agreements. The team should create and adhere to agreed-upon SLAs. 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. Always the forgotten stepchild, documentation is more important than ever in this increasing world of change. 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 Demo →

© 2025 Aryaka Networks, Inc. All Rights Reserved