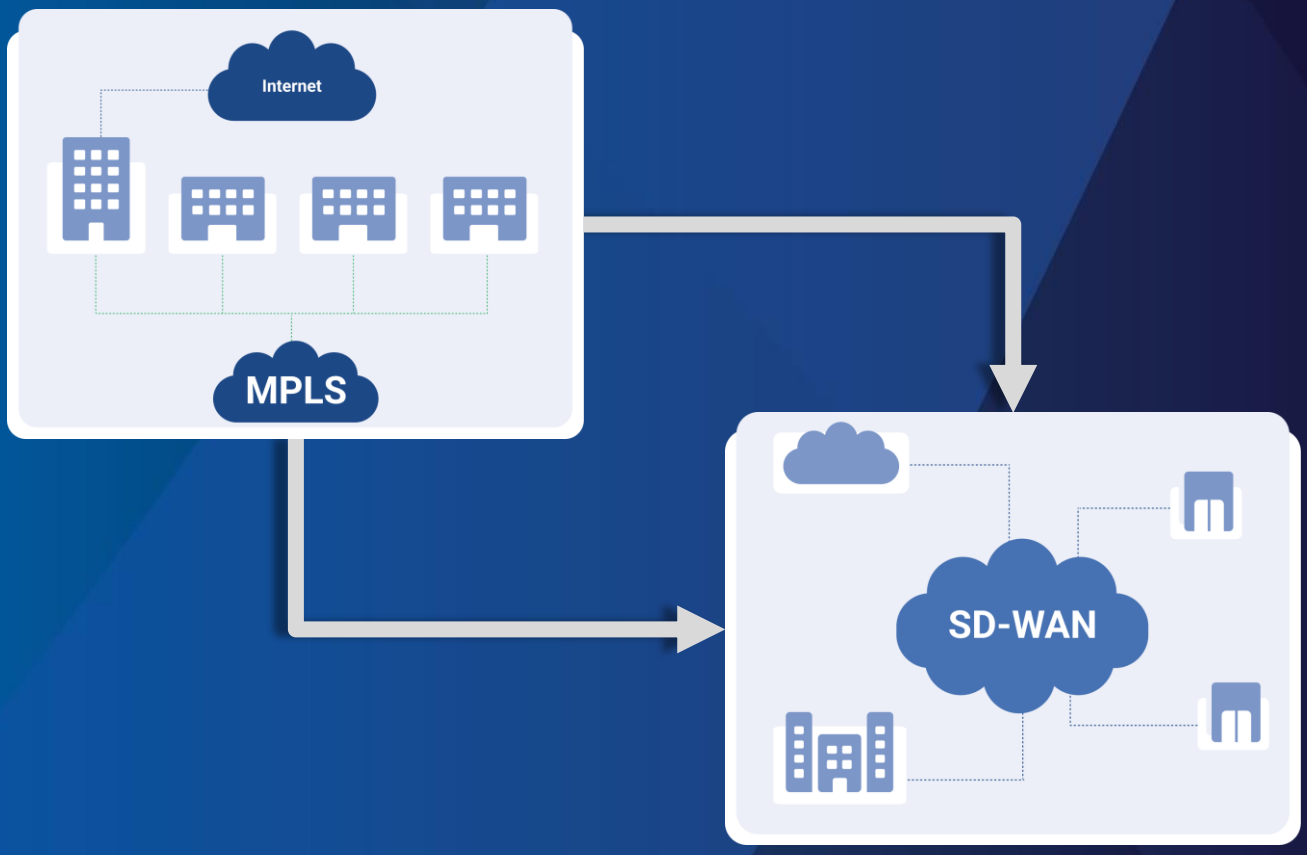
lightyear

Networker's Guide to

Transitioning from MPLS to SD-WAN



LEARN MORE AT LIGHTYEAR.AI

Introduction

The data shows that enterprises are transitioning from MPLS to SD-WAN, but why? And more importantly... how?

If you've been tasked with transitioning your enterprise from MPLS to SD-WAN, you've come to the right place.

Multiprotocol Label Switching (MPLS) changed the networking game back in the 1990s, allowing enterprises to build layer 1 networks in a hub and spoke manner while its layer 3 routing technology created a "fully meshed"/any-to-any, virtual topology.

But as data utilization and enterprise networks continue to grow, the limitations of MPLS are pushing enterprises to explore new technologies. Enter SD-WAN, the latest evolution in networking that decouples the underlay and overlay networks, enabling a much more efficient and scalable means of networking.

What's Inside?

- Review of MPLS & SD-WAN
- Why are enterprises moving to SD-WAN?
- What to know when transitioning to SD-WAN
- Action Plan for transitioning from MPLS to SD-WAN
- Hybrid MPLS & SD-WAN Networks

Like all new technologies, there are still tons of questions surrounding the capabilities of SD-WAN, a confusion made worse by the wide variety of solution types (and a wide variety of SD-WAN providers) available out there today - all of which makes the decision to move your network from MPLS to SD-WAN a daunting one.

This guide is here for those who are evaluating the switch from MPLS to SD-WAN and will provide step-by-step guidance and diagrams showing how to do it (and do it right).

Quick review of MPLS & SDWAN

Quick Review of MPLS and SD-WAN

What is MPLS?

Multi-protocol label switching (MPLS) is a proven networking technology that has powered enterprise networks for over two decades. Unlike other network protocols that route traffic based on a source destination address, MPLS routes traffic based on predetermined labels. Via private networks, enterprises can use MPLS to connect remote branch offices that require access to data or applications that reside in their data center or company headquarters.

Unlike VPNs (complicated to manage) and point-to-point links (inflexible), which put the onus on IT staff to implement and manage, MPLS is a carrier-managed solution, which means the telecom carrier is responsible for guaranteeing interconnectivity, delivering high Quality of Service (QoS) and maintaining the associated service level agreements (SLAs).

What is SD-WAN?

SD-WAN is a software-based architecture that acts as a virtual overlay to an underlying hardware-based network and provides a centralized control function to efficiently steer traffic across a WAN based on an enterprise's business needs.

By enabling traffic prioritization, SD-WANs can support many of the same quality of experience and security benefits of MPLS or P2P for important applications, but with data transmission occurring, for the most part, over the public internet rather than on preset or dedicated routes. A key difference when comparing SD-WAN vs MPLS is that SD-WAN acknowledges the public internet as arguably the most important node on the enterprise WAN. SD-WAN's reliance on the internet is why many people think it is a cheaper WAN option than dedicated circuits (more on that later).

An important distinction to make is that other WAN options rely on having their own physical form of transport while SD-WAN does not. SD-WAN provides a decoupling from the physical underlay network, allowing it to be completely vendor agnostic, while software manages the overlay network essentially as an intelligent VPN (see this post on SD-WAN vs VPN). However, in many cases, SD-WAN's overall quality is only going to be as strong as that of the underlying network on which it rides.

Because it technically uses the public internet in many cases, SD-WAN may raise security concerns for some customer profiles. However, modern SD-WANs can be encrypted to such a level so that this should no longer be the gating item keeping you from transitioning from MPLS to SD-WAN.

Why are enterprises transitioning from MPLS to SD-WAN?

Why are enterprises transitioning from MPLS to SD-WAN?

A summary of factors driving enterprises to transition from MPLS to SD-WAN:

- **Flexibility & Ease of Set-up**
- **Cloud-Readiness**
- **Cost (Sometimes)**
- **Ease of administration**
- **Reporting/Network insights**
- **Network resiliency**

Flexibility & Ease of Set-up

The flexibility and ease of set-up of SD-WAN makes it a very attractive network option compared to the old, and inflexible, ways of MPLS.

From a routing perspective, adding a new network node on an MPLS network is not a cumbersome process, thanks to dynamic routing protocols such as BGP routing. However, anytime you want to add an additional network node to your traditional MPLS WAN, you are required to utilize the same provider that you use at your existing locations. This can be extremely costly and time consuming, depending on if your provider already has fiber ready at the new node or not.

If you want to expand your MPLS network beyond the reach of the backbone of your MPLS provider, you'll either need to pay for them to build to your new location, or you'll have to procure Tier 2 circuits (your provider reselling the on-net provider's connectivity).

With SD-WAN, however, it is extremely easy to spin up a new network node. Given the fact that you can utilize the underlay network from any provider, your network expansion isn't restricted to the footprint of one provider. Typically, all you need is an additional appliance from your SD-WAN provider to get a new node going (and the underlay, of course).

Cloud-Readiness

With the rapid adoption of cloud-based applications in the form of SaaS and IaaS, an organization's WAN architecture experiences an explosion of traffic accessing applications distributed across the globe - and traditional wide area networks (WANs) based on conventional routers were never designed for the cloud.

Traditional WANs require backhauling all traffic, including traffic destined for the cloud,

Why are enterprises transitioning from MPLS to SD-WAN?

Cloud Readiness (Cont'd)

from branch offices to a hub or headquarters/data center where advanced security inspection services can be applied. The delay (or latency) caused by backhaul impairs application performance, resulting in a poor user experience and lost productivity. Simply put, this WAN architecture is not ready for the unprecedented explosion of WAN traffic that cloud adoption brings. This adds a layer of management complexity and application-performance unpredictability.

Unlike the traditional router-centric WAN architecture - which distributes the control function across all devices in the network and simply routes traffic based on TCP/IP addresses and Access Control Lists (ACLs) - the software-defined WAN model is designed to fully support applications hosted in on-premises data centers, public or private clouds, and SaaS services such as Salesforce.com, Workday, Dropbox, Microsoft 365, and more, while delivering the highest levels of application performance.

By utilizing SD-WAN, your IT team can guarantee better performance for cloud based applications (often with real time optimization) and optimized cloud workflows. This is true, even more so, if you utilize an SD-WAN provider who offers middle mile network management and is directly peered with the clouds and applications that you want to utilize.

Cost (Sometimes)

SD-WAN is often a cost-effective solution compared to MPLS, for a few reasons.

First, SD-WAN includes the public internet as part of its network which is inherently less expensive than a network composed solely of dedicated private lines.

Additionally, due to the provider limitations of MPLS mentioned in the flexibility section, your cost can scale rapidly with MPLS as you expand your network (due to build requirements and Type 2 circuit utilization).

The flexibility to use different carriers and connectivity types (dedicated and best effort) empowers users to optimize their costs, enabling them to route low priority traffic over less expensive network routes.

However, there is a common misconception that SD-WAN is ***always*** cheaper than MPLS, but this isn't the case.

Why are enterprises transitioning from MPLS to SD-WAN?

Ease of administration

Because MPLS is implemented, managed and maintained by the telecom provider, users have minimal network management involvement. That said, routing protocol changes or general maintenance requires the user to interact with an Internet Service Provider (ISP), which can be slow and frustrating at times.

In contrast to MPLS, a self managed SD-WAN requires considerable user involvement, but with the added benefit of control and transparency. Most vendors provide a single, centralized, cloud-delivered management dashboard for configuration and management of your WAN, cloud, and security. Additionally, they provide template-based, zero-touch provisioning for all locations: branch, campus, and cloud.

For users who do not want the responsibility of managing their SD-WAN, there are available managed SD-WAN solutions - which of course offer the easiest administration (compared to MPLS and self-managed SD-WAN), but this comes with incremental cost.

Reporting/Network insights

SD-WAN comes with robust reporting capabilities that can be configured (by you or your managed SD-WAN provider) to analyze the performance of your network. This is a big benefit compared to MPLS where you don't have any visibility into your network performance.

For example, with SD-WAN reporting capabilities you can:

- View bandwidth utilization by each path/link in the network
- Access detailed reporting of application and WAN performance for business analytics and bandwidth forecasting.
- Assess top applications or links with the highest frequency of path degradation
- Generate a Link Performance report to verify if the guaranteed bandwidth your ISP committed to is being honored (i.e., SLA enforcement)
- Monitor the quality of experience (QoE) of your SD-WAN

Network resiliency

Network reliability and resiliency are of paramount importance due to the high cost of network downtime. Because SD-WAN is a centralized, software-driven solution that requires minimal hardware coding or infrastructure changes, SD-WAN makes it easy to build relatively low-cost network redundancy via multiple carriers.

Additionally, with SD-WAN there are multiple routes for your data traffic to traverse the network. You are no longer reliant on a single private line, which can quickly turn into a network bottleneck and single point of failure. Most SD-WAN applications make it easy to dynamically route traffic based on your network needs, ensuring resilient and stable network performance.

What to know when transitioning from MPLS to SD-WAN

What to know when transitioning from MPLS to SD-WAN

A summary of what you need to know when transitioning your network to SD-WAN:

- **Network Requirements**
  - Throughput/bandwidth
  - QoS vs QoE
  - Appliance
- **Provider Type**
  - Define “managed”
  - Middle Mile networks
  - Priority application peering
  - Underlay network management
  - Edge security

Network requirements

Throughput requirements

Before kicking off an SD-WAN procurement project, you should have a good idea of your network bandwidth requirements. To estimate your bandwidth requirements, you need to know all the applications and services you want to put on your SD-WAN overlay and the bandwidth requirements of each. These requirements will vary depending on where you are accessing your applications from: public cloud, private cloud, or locally. You also need to consider what your users are doing on those applications, what the application use cases are, when they are being used, and how often.

Note that SD-WAN appliance bandwidth needs often take into consideration your primary and your secondary circuit. I.e., if you have 100 Mbps DIA primary circuit and a 500 Mbps best effort secondary circuit, the SD-WAN provider will likely charge you for 600 Mbps of throughout.

Bandwidth needs estimation is both an art and a science. The general rule we follow is based on determining if your network utilizes primarily “low bandwidth activities” (such as internet browsing or emailing) or “high bandwidth activities” (such as large file downloads/uploads and video calling).

Here’s an example:

- **For low-bandwidth businesses** with, say, 20 employees, simply multiply the number of user devices (let’s assume three devices per employee) by 3Mbps to give you an estimate of required bandwidth. In other words, 20x3 = 60 devices. Multiply that by 3Mbs gives you 180Mbps, and you would round that up to 200Mbps.

- **For high-bandwidth businesses**, multiply the number of user devices by 10Mbps. For example, 30 users x 3 devices per user = 90 devices. Multiply that by 10Mbps = 900Mbps, rounded up to 1000Mbps or 1Gbps.

What to know when transitioning from MPLS to SD-WAN

Understand QoS from QoE

Before signing up for SD-WAN, you need to understand the difference between QoS and QoE and why it matters.

MPLS & Quality of Service:

To ensure the optimum service availability and transmission quality, the telecom provider deploys a set of technologies that manage network resources to minimize packet loss, latency and jitter. This is referred to as Quality of Service (QoS). Carriers typically provide MPLS service level agreements (SLAs) of at least 99.9% to guarantee they deliver on these QoS commitments of speed, bandwidth, reliability and performance.

SD-WAN & Quality of Experience:

Quality of Experience (QoE) refers to the rules set by the SD-WAN network administrator to prioritize and selectively route ingress and egress traffic during times of network congestion. QoE is NOT a guarantee of network performance and is not contractually backed.

In summary, the QoS + SLA guarantees that come with MPLS are more iron-clad than the QoE you receive with SD-WAN. That said, there are a few things you can do to create an SD-WAN that is just as resilient:

First and foremost, you can build your SD-WAN with a mix of dedicated and best effort circuits to help avoid public internet network congestion.

You can work with an SD-WAN provider who offers their own “middle mile network” which gives them full control over routing and traffic prioritization between all nodes on a WAN.

Going one step further - you can choose an SD-WAN provider who will manage your underlay network as well which reduces the headache of network management and (should) reduce network downtime.

SD-WAN Appliance Considerations

Before diving in with an SD-WAN provider, you’ll need to make an assessment of their appliance capabilities. Every SD-WAN appliance or “edge device” has its own unique set of capabilities.

The key things to consider are:

- How many WAN interfaces does the device have?
- What is the throughput/bandwidth capacity?
- Does it have redundant power supplies?
- Can you stack the devices for high availability?

You’ll need to determine your appliance needs at each location and then make sure that the provider can meet those needs. Ideally, they have a solution that can handle your current and future network needs as you grow.

What to know when transitioning from MPLS to SD-WAN

Choose an SD-WAN provider type

Define "Managed"

As mentioned previously, you can procure SD-WAN on a managed or unmanaged basis. With managed SD-WAN, it's important to understand that the definition of "managed" will vary by provider.

While some managed SD-WAN providers will manage your underlay network, others will not. This means that if there is an issue with your underlying circuit, the SD-WAN provider who manages your underlay network is responsible for communicating with the network provider to troubleshoot and resolve the issue. If your SD-WAN provider does not manage the underlay network, then it's up to your IT team to troubleshoot and resolve any underlay network issues.

Additionally, the demarcation point between what the managed SD-WAN provider is responsible for and what your IT team is responsible for can vary between providers. Some managed SD-WAN providers will manage your VPNs while other providers will not (but for the most part, "managed SD-WAN" includes VPN management).

Lastly, some managed SD-WAN providers will help you manage circuit Move/Add/Change/Disconnect (MACD) requests, while some providers will not include MACD requests in their definition of "managed SD-WAN".

Middle Mile Networks

When choosing a managed SD-WAN provider it's important to know whether or not they provide a middle mile network and how well-peered it is, if so.

The middle mile refers to the network connection between the last mile and the public Internet. The middle mile network is when the managed SD-WAN provider owns and manages their own points of presence (POPs), direct cloud connectivity, and peering relationships into the public internet. Peering is when one internet network connects directly to another, enabling a faster throughput and exchange of information without having to pay a third party to carry traffic across the Internet.

If your SD-WAN provider has a middle mile network, you will send all of your traffic to their network and they will move it for you. For example, instead of you connecting to the Microsoft Azure cloud over the public Internet, you send traffic to your provider and they connect to Azure on your behalf.

Priority Application Peering

When procuring managed SD-WAN, you should have a list of your most business-critical applications/clouds and choose a provider that is well peered to those applications/clouds via their middle mile network or otherwise.

What to know when transitioning from MPLS to SD-WAN

Priority Application Peering (Cont'd)

This is especially important if you utilize voice applications that are in the cloud given how sensitive voice traffic is to network issues such as packet loss, jitter, and latency.

PeeringDB is an open-source database that lets you check how well-peered SD-WAN providers are. However, you should not rely solely on PeeringDB; do your own research on these peering relationships with the actual provider.

Underlay network management

As previously described in the "Define Managed" section, some SD-WAN providers will manage your underlay circuits for you and others will not.

This means that if there is an issue with your underlying circuit, the SD-WAN provider who manages your underlay network is responsible for communicating with the network provider to troubleshoot and resolve the issue. If your SD-WAN provider does not manage the underlay network, then it's up to your IT team to troubleshoot and resolve any underlay network issues.

Edge Security or not?

While MPLS comes out-of-the-box as a more secure WAN solution, SD-WAN has the potential to make security easily configurable and highly customizable (depending on your vendor). Different SD-WAN vendors offer different types of security options, so you should make your needs clear up front.

Secure access service edge (SASE) combines network security functions (such as SWG, CASB, FWaaS and ZTNA) with SD-WAN capabilities to support the dynamic secure access needs of organizations.

Ok, now onto the good stuff.

Action Plan for transitioning from MPLS to SD-WAN

Action Plan for transitioning from MPLS to SD-WAN

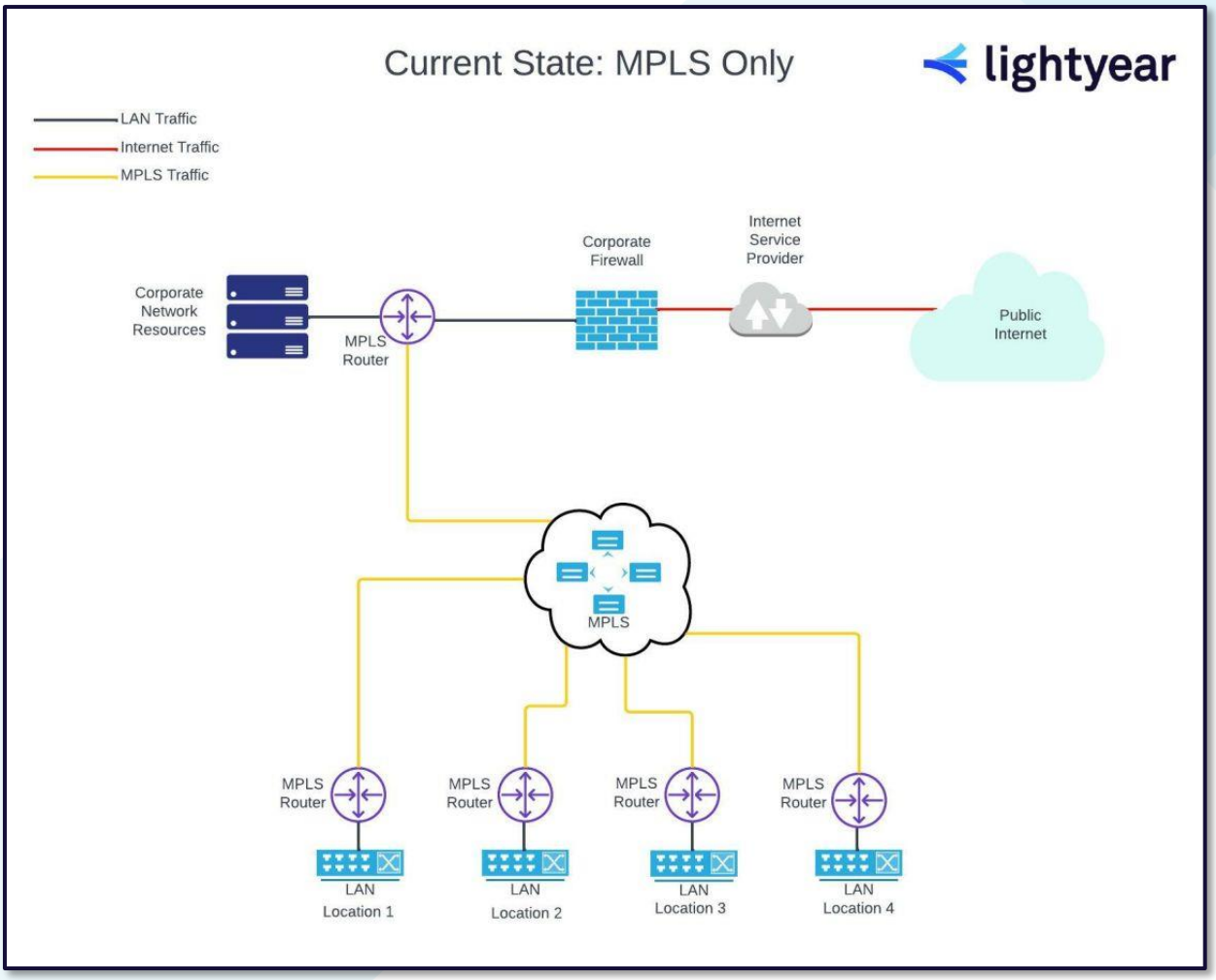
This section includes a few custom network diagrams to walk you through the transition. To start, below is the "Current State" of the hypothetical network we will walk through.

Step 1: Documentation & Planning

Documentation and planning are critical to any successful network migration. This holds especially true when converting from MPLS to SD-WAN.

Here are the critical items to document:

- Overall network topology
- Subnets at each location
- Default gateways
- DHCP scope / reservations
- Business critical applications
- Internet source and IPs
- Cloud hosted applications (and the location of those clouds/applications)
- Corporate hosted applications



Action Plan for transitioning from MPLS to SD-WAN

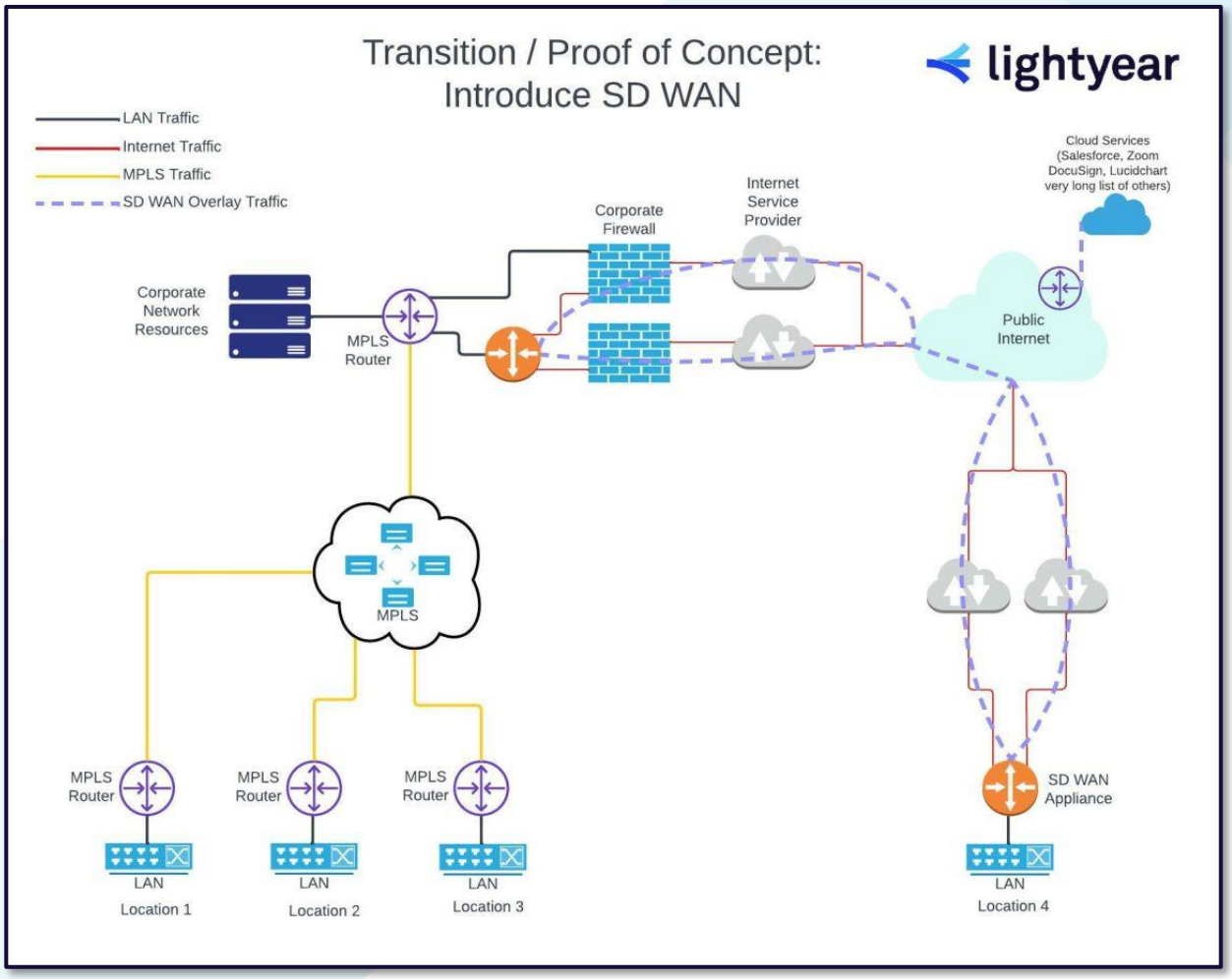
Step 2: Proof of Concept (PoC)

Now that you have your ducks in a row, you need to do the math to figure out if SD-WAN is actually a good idea for your enterprise.

A standard next step, before moving the entire network over to a new topology all at once, is to conduct a Proof of Concept (PoC) exercise and move just one of your remote locations over to SD-WAN.

If you have experience doing this sort of thing and read this section and think, “That’s not how I would do it.” You’re probably right - SD-WAN is an extremely flexible WAN topology and there are quite a few ways to successfully stage and deploy.

Here’s our suggestion:



Action Plan for transitioning from MPLS to SD-WAN

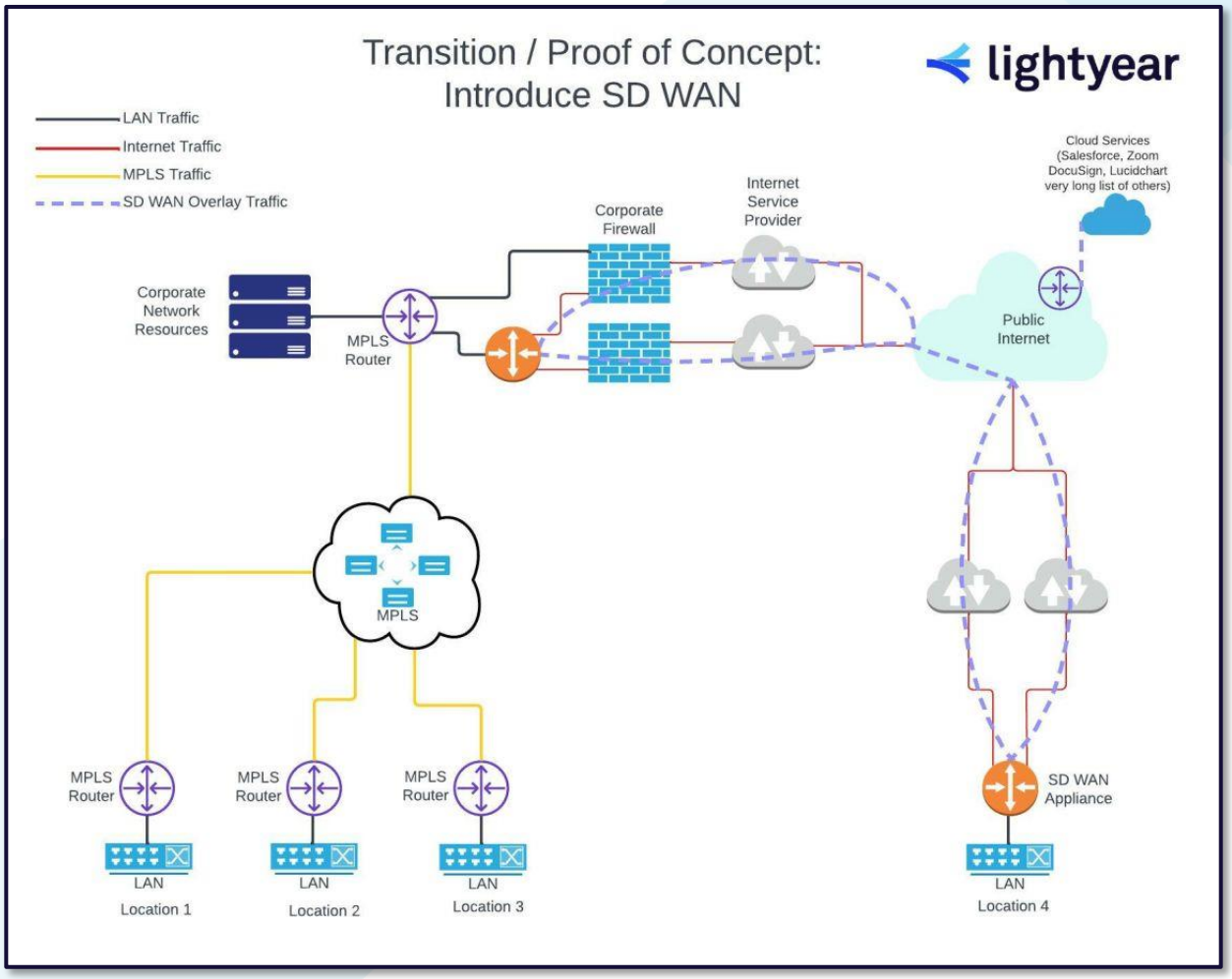
Step 2: Proof of Concept (PoC)

Now that you have your ducks in a row, you need to do the math to figure out if SD-WAN is actually a good idea for your enterprise.

A standard next step, before moving the entire network over to a new topology all at once, is to conduct a Proof of Concept (PoC) exercise and move just one of your remote locations over to SD-WAN.

If you have experience doing this sort of thing and read this section and think, “That’s not how I would do it.” You’re probably right - SD-WAN is an extremely flexible WAN topology and there are quite a few ways to successfully stage and deploy.

Here’s our suggestion:

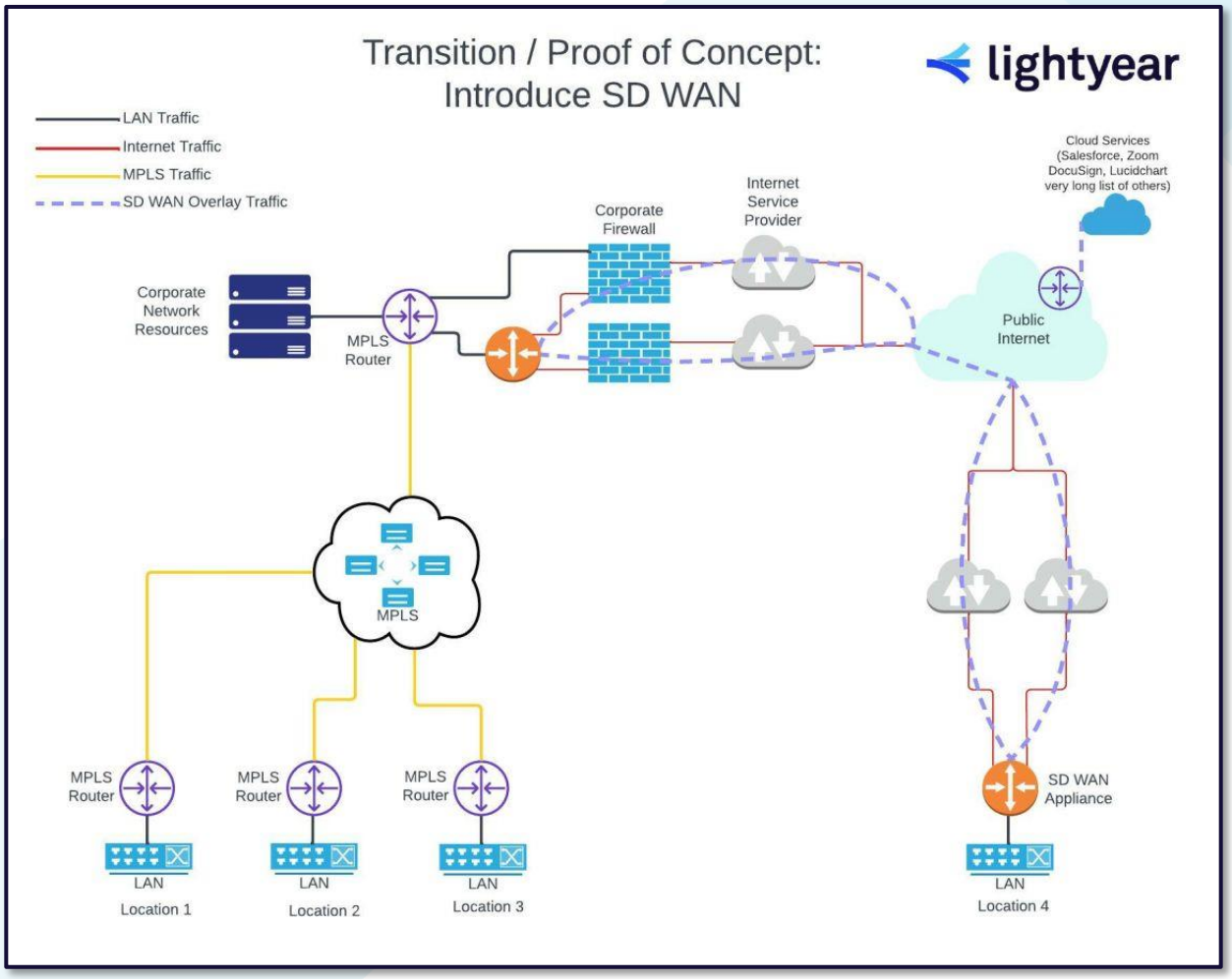


Action Plan for transitioning from MPLS to SD-WAN

Step 2: Proof of Concept (Cont'd)

A few key elements to prepare for the PoC step:

- Select appropriate SD-WAN equipment for your business needs.
- Determine if you have the appropriate experience on staff to deploy the equipment and network elements in-house or select an appropriate partner to assist with the SD-WAN deployment.
- Install internet services at the selected site(s). Internet services should be ordered and delivered by two or more Internet Service Providers.
- Find the appropriate place to bridge the existing Corporate Resources and MPLS network with the SD-WAN Proof of Concept network.
- During a maintenance window, migrate the POC site over to SD-WAN.

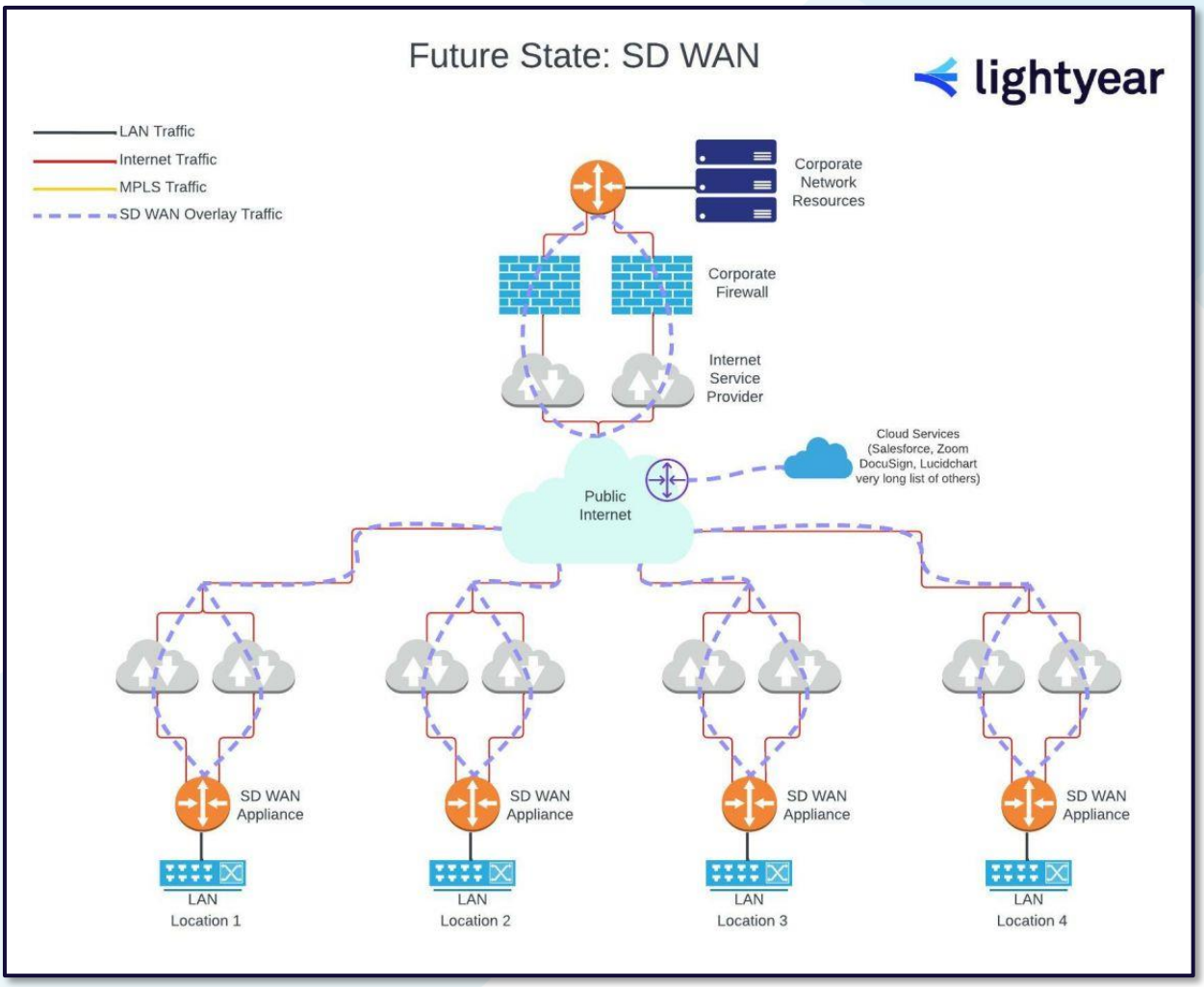


Action Plan for transitioning from MPLS to SD-WAN

Step 3: Implement Full SD-WAN Transition

After thoroughly testing the SD-WAN network to ensure that routing, applications, and end user experience are working and acceptable, you can move through the network one site at a time or schedule a time to move all sites during a major cutover event.

Here's what that future state could look like for your network:



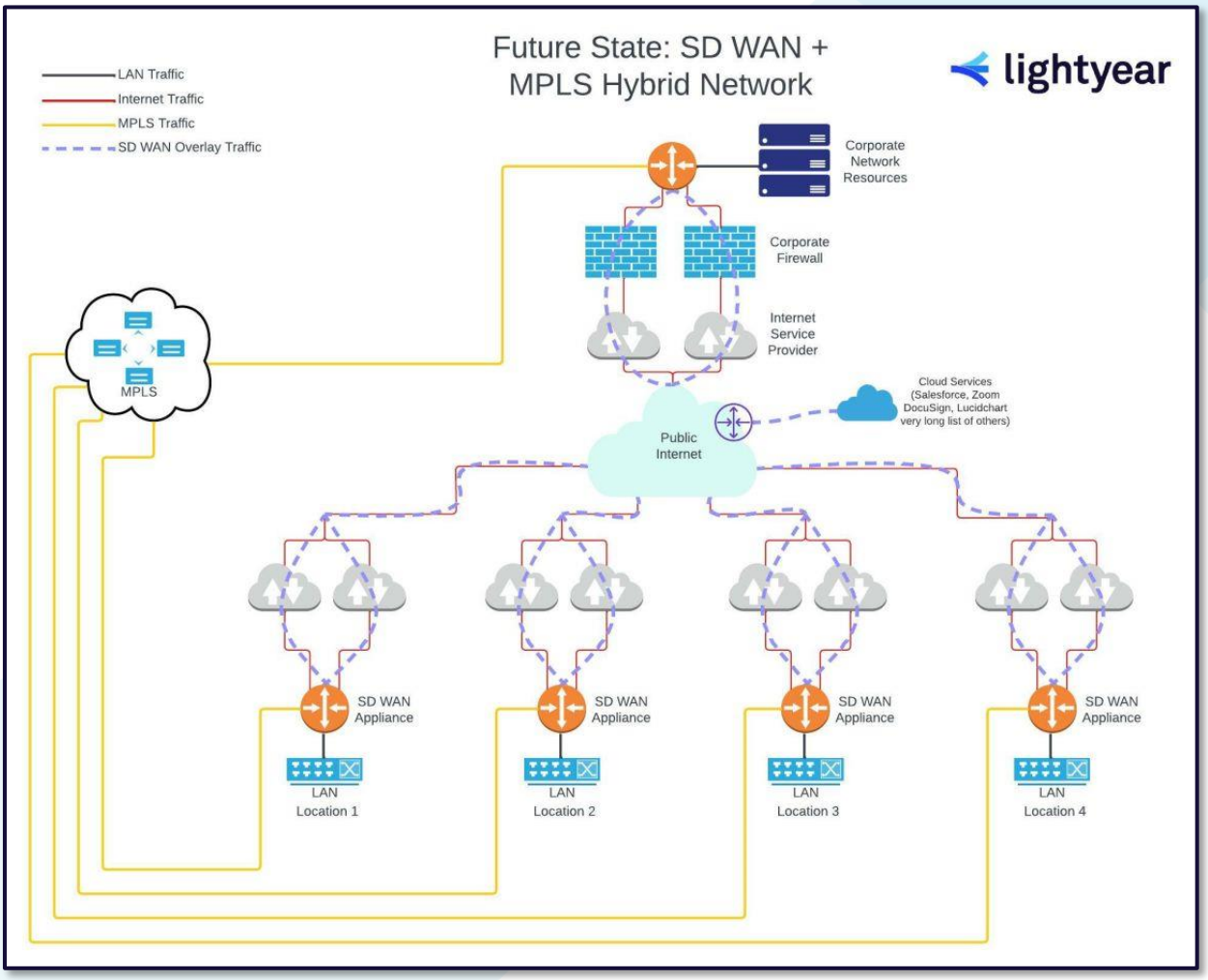
Alternative: Hybrid MPLS & SD-WAN Network

Hybrid WAN

One thing to keep in mind, there are SD-WAN equipment manufacturers and topologies that are designed to accommodate BOTH internet and MPLS connections.

If your business has a requirement to keep MPLS as a network element, there is an option for a hybrid network.

The diagram below showcases what your hybrid network could look like:



Thanks for reading!

We hope this guide is helpful for evaluating if SD-WAN is right for your enterprise, as well as how to make the transition from MPLS to SD-WAN.

Would you like to learn more about how Lightyear's software can help you evaluate, procure, and implement the optimal SD-WAN for your enterprise?

Talk to us

lightyear