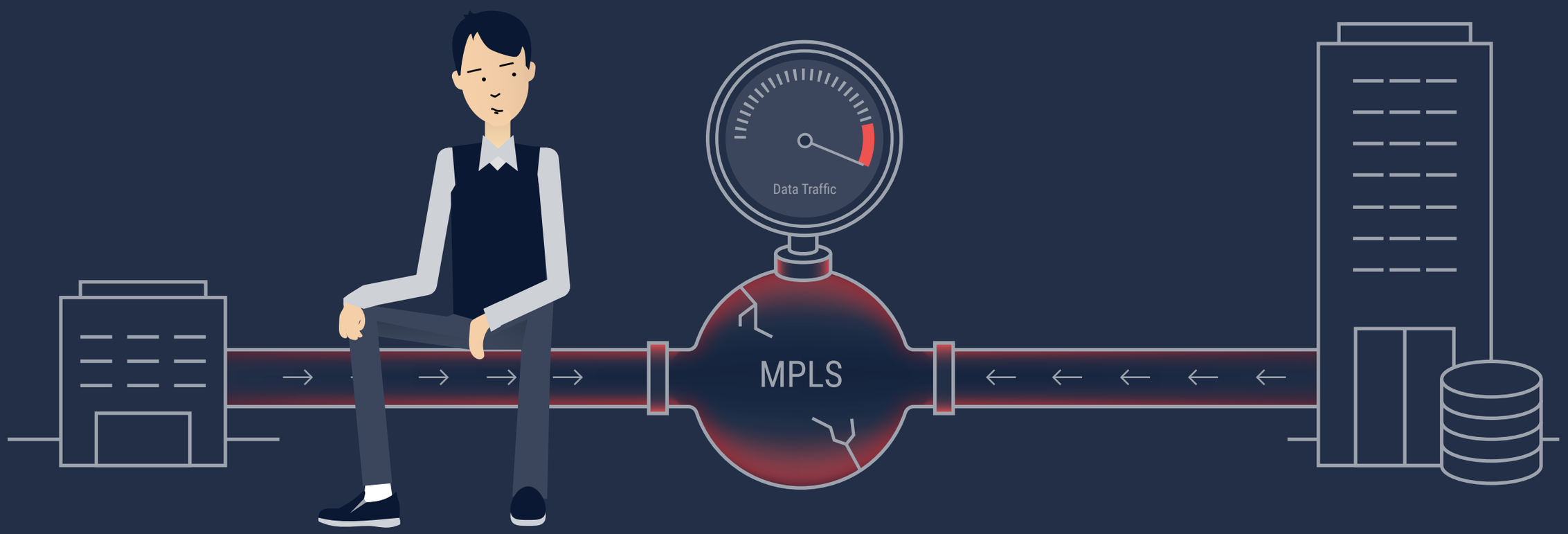
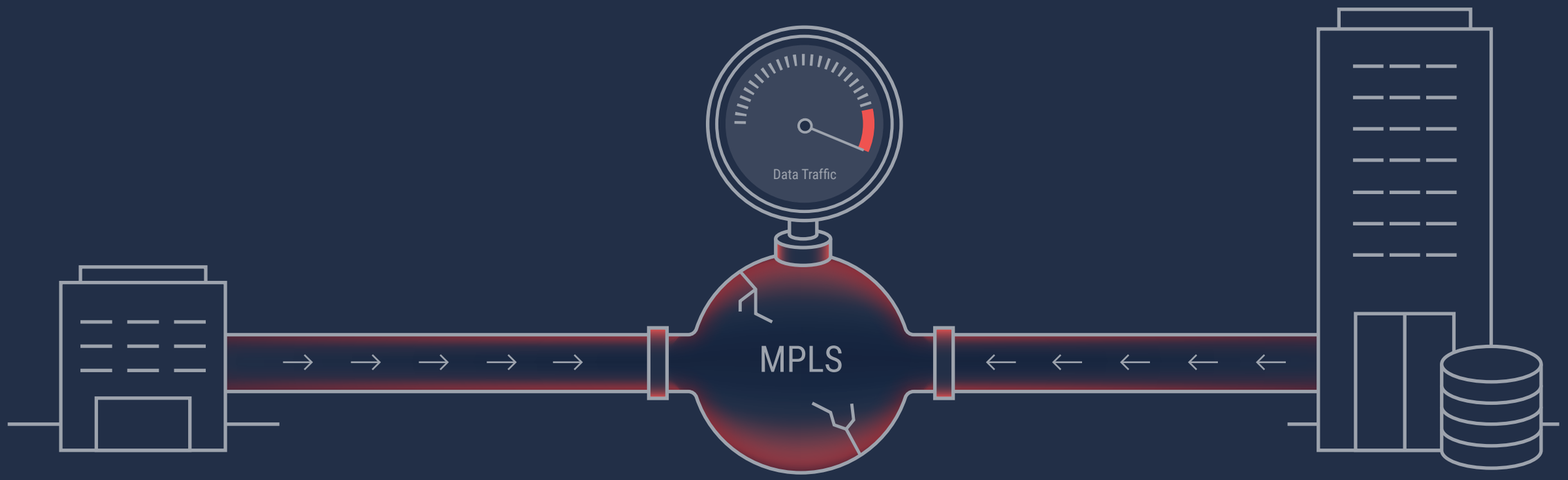
How to **Re-evaluateYour MPLS Service Provider**



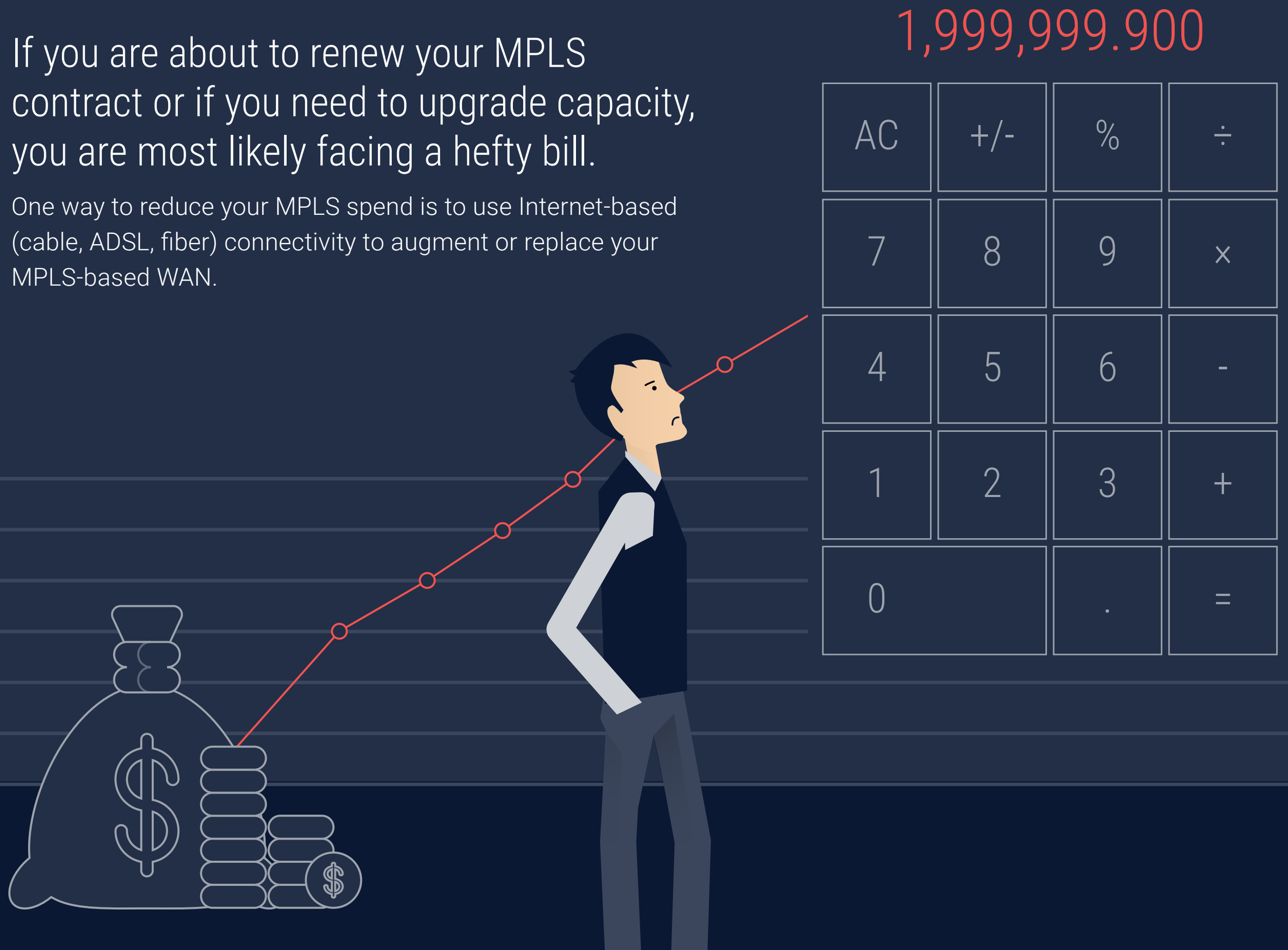
Do you run an MPLS network to some or all of your branches? If so, you are likely wasting MPLS capacity backhauling Internet traffic.

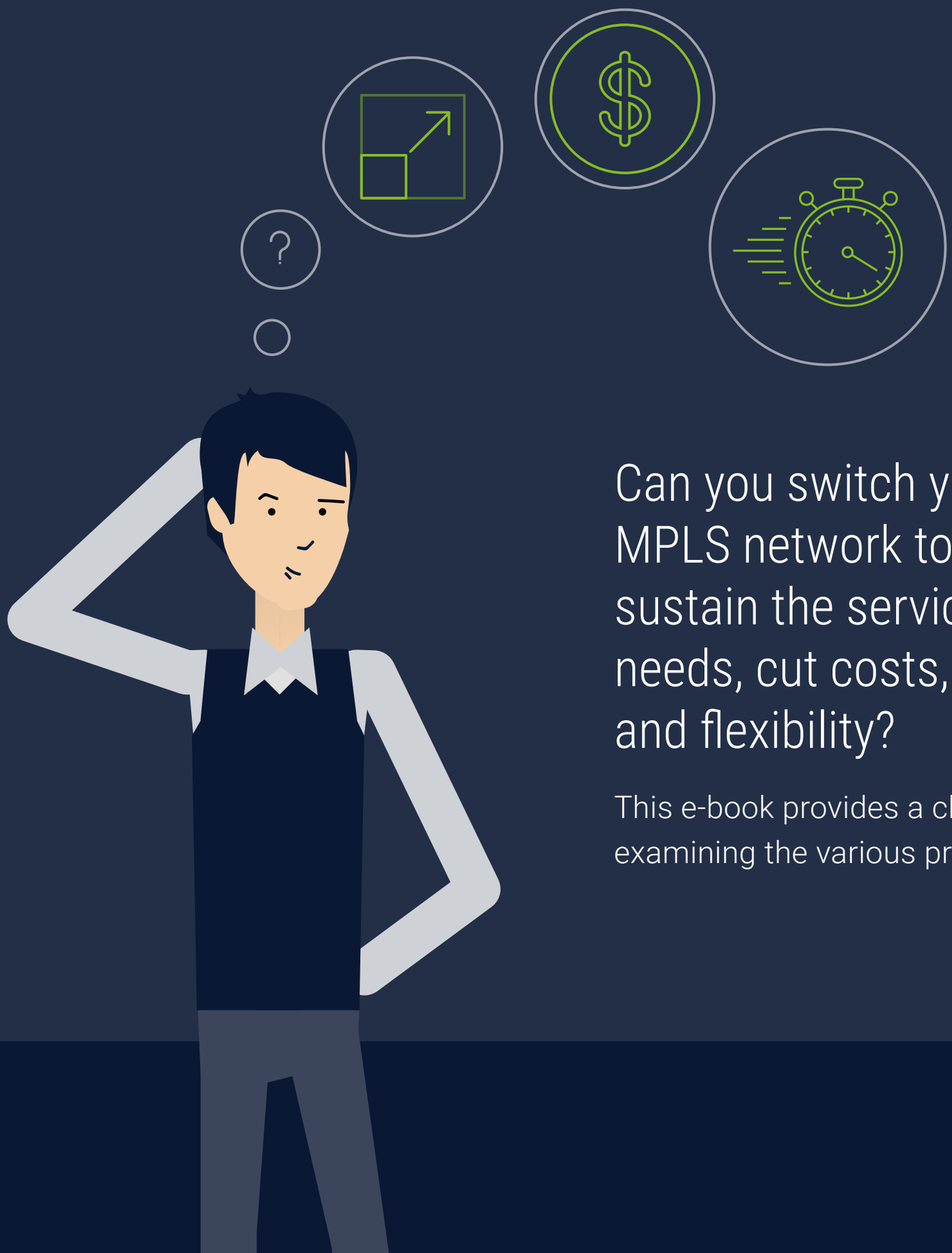
For many organizations, a lot of the traffic is Internet-bound due to increased cloud-usage. Backhauling Internet traffic over an expensive MPLS service adds latency and puts pressure on limited and expensive MPLS capacity.



If you are about to renew your MPLS contract or if you need to upgrade capacity, you are most likely facing a hefty bill.

One way to reduce your MPLS spend is to use Internet-based (cable, ADSL, fiber) connectivity to augment or replace your MPLS-based WAN.





Can you switch your dedicated and expensive MPLS network to an Internet-based network, sustain the service levels your business needs, cut costs, and improve overall agility and flexibility?

This e-book provides a checklist to help answer this question by examining the various pros and cons of different approaches.

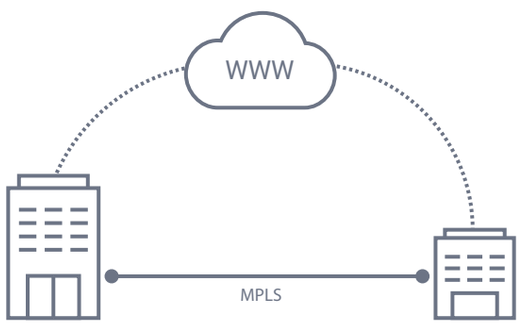
Three Approaches to Consider:

1 MPLS

Use legacy MPLS services and its guarantees if it is the only way to meet your business goals.

2 BASIC SD-WAN

Add Internet links to your existing MPLS network to avoid the cost of MPLS upgrades. You still need to rely on MPLS to support latency sensitive apps end-to-end.



3 CLOUD SD-WAN

Add Internet links and a cloud-based, SLA-backed SD-WAN alongside your existing MPLS network. You avoid the cost of MPLS upgrades and can gradually replace MPLS altogether.

Learn more

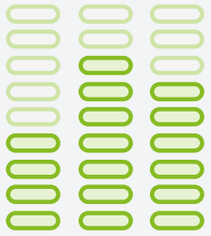
4 Key Network Design Considerations:

1 AVAILABILITY

Network availability is essential to keeping your business up and running. The majority of outages occur in the last mile where physical infrastructure is exposed at and around the customer premises. To address availability, customers look at the reliability of network connectivity they put in place and the time to fix any outages. Fully redundant connections can give Internet access MPLS-like uptime.

In addition, the time to deploy connectivity to new offices and locations is important to keep the business moving forward.

2 CAPACITY



Adequate network capacity is required to support the business. Bandwidth constraints, due to cost, require additional technologies to manage the quality of service and prioritize traffic. Even if you have ample bandwidth, the amount of capacity is dependent on the type of connectivity. Dedicated capacity, like MPLS and symmetrical Internet, is more expensive, but capacity is guaranteed (both upstream and downstream). Best-effort services, offer more bandwidth at lower cost, but capacity will decline due to congestion.

These limitations could be acceptable to the business, depending on the types of applications being used.

4 Key Network Design Considerations:

3 LATENCY

High latency as a result of suboptimal routing and packet loss can have a dramatic impact on the user's experience. Low-quality network connections and congested ISPs ISP networks increase packet loss in the last mile. Inefficient routing over the long haul (i.e the middle mile) increases latency. Latency can either be tolerated (i.e when using the public Internet) or improved (with SLA-backed and redundant connectivity).

4 SECURITY

Offloading Internet traffic at a branch directly onto the Internet enables better use of MPLS resources. While not a networking requirement per se, network security at each branch reduces the need to backhaul traffic to a secure Internet exit point at the datacenter. Many organizations architected their network for Internet-traffic backhauling to avoid the complexity of managing a network security stack at every location.

This architecture is no longer compatible with the current traffic patterns and rapid growth in Internet-bound and cloud traffic. As you rethink your WAN architecture, evaluate your network security to optimize costs, user response times and management complexity.

The Ultimate Checklist

		Considerations	MPLS	Basic SD-WAN	Cloud-based SD-WAN
Availability	**Reliability and uptime**	▪ What is the maximum uptime required by your most critical applications?	99.99%	99.99% (2 ISPs, 4G/LTE backup)	
	Time-to-Repair	▪ What level of downtime can the business withstand at a branch office (minutes/hours per year - quantify number of 9s)?	SLA-backed, 2-4 hours	Next business day (reduced downtime with multiple links and 4G/LTE backup)	
	Time-to-Deploy	▪ How critical is time-to-deploy for a new branch?	30-90 days	1-7 days for Internet, minutes to hours for 4G/LTE	
Capacity	**Dedicated**	▪ Do you need to boost WAN capacity? ▪ What is the needed upgrade for Upload/ Download? ▪ Best effort (ADSL) or Guaranteed (Fiber)?	Yes, high cost per MBPS	▪ 1-2 ADSl/Cable (best effort) ▪ 1-2 Symmetric Fiber (dedicated) ▪ Active/Active and Forward Error Correction (FEC)	
Latency	**SLA-backed, Branch-DC connectivity**	▪ Do you need global connectivity (latency is a major challenge)? ▪ What is the cost of your global MPLS network vs. an alternative SLA-backed backbone?	SLA-backed	Not guaranteed[1]	SLA-backed[2]: ▪ High quality last mile ▪ SLA-backed cloud network
Security	**Secure Internet access at the branch**	▪ Do you want to offload Internet traffic at the branch? ▪ How will you handle branch office security (beyond building VPN tunnels over the Internet to the DC)? ▪ How can you avoid deployment of network security appliances?	No	Optional (with branch firewalls)	Yes (with cloud-based network security)
Cloud & Mobile	**Integrate cloud data centers and mobile users to the WAN**	▪ Do you have AWS VPCs or Microsoft Azure instances you need to connect to your WAN? ▪ How do you securely connect mobile users to the WAN and to the Internet?	No	Limited cloud support, no mobile support	Seamless integration of cloud and mobile into the WAN

[1] SD-WANs shift traffic to the Internet, but continue to depend on MPLS connectivity for latency-sensitive applications.

[2] A cloud network provides SLA-backed backbone. For connecting locations and users over a long haul, latency will not exceed the SLA committed by the provider.

The New WAN: Rise of Globalization, Cloud and Mobility Transforms the WAN

When we think about the WAN, we tend to think about connecting physical locations to the datacenter. Nowadays, the WAN is stretching to address globalization, cloud and mobility.

GLOBALIZATION

Enterprises need to connect people and locations across intercontinental distances. Legacy MPLS solutions from your regional provider need to be stitched together with other offerings or bundled with a global vendor. Legacy SD-WANs lack the latency control to support three scenarios. Cloud-SD-WANs can provide affordable SLA-backed connectivity.

CLOUD

The migration to cloud apps and cloud infrastructure forces traffic to the Internet. The end-to-end control offered by MPLS providers doesn't really apply to these scenarios. Legacy SD-WAN appliance-based approaches stretch to support the cloud. Cloud SD-WANs naturally extend the WAN to the cloud as part of the overlay.

MOBILITY

Mobile users were always an afterthought from a network design perspective so they are not supported by MPLS and SD-WANs. But they are now a major part of how business is done and Cloud SD-WANs support them as part of the core WAN architecture.

As you look for the various solutions to improving your WAN, look beyond traditional WAN architectures to address emerging requirements.

About Cato Networks

Cato Networks provides organizations with a software-defined and cloud-based secure enterprise network. Cato delivers an integrated networking and security platform that securely connects all enterprise locations, people and data. The Cato Cloud reduces MPLS connectivity costs, eliminates branch appliances, provides direct, secure internet access everywhere, and seamlessly integrates mobile users and cloud infrastructures to the enterprise network.

Based in Tel Aviv, Israel, Cato Networks was founded in 2015 by cybersecurity luminary Shlomo Kramer, who previously cofounded Check Point Software Technologies and Imperva, and Gur Shatz, who previously cofounded Incapsula.

Network+Security is Simple Again

For more information:

www.CatoNetworks.com

@CatoNetworks