SD-WAN vs. MPLS

turnium

COMPARISON OF FEATURES AT-A-GLANCE

The profit margins of traditional leased lines have eroded over the past 20+ years leaving Service Providers (SP) to look for new valueadded revenue streams. The introduction of multi-protocol labeling switching (MPLS) in the early 2000s helped to relieve that strain on SP finances.

However, Hosted and Cloud applications and services need more dynamic and flexible networking technologies. For Small-Medium Business customers needing reliable, managed connectivity, SPs can deliver faster, increase customer satisfaction, and increase revenues and profit margins by deploying SD-WAN. For Enterprise customers, SD-WAN can be integrated with existing MPLS deployments, to help customers manage costs, while adding off-net sites into a single hybrid network with secure, encrypted SD-WAN that provides Quality of Service for voice and other applications.

Features	SD-WAN	MPLS
Affordable	Yes	No
AES data encryption	Yes	No
Flexible contracts	Yes	No
Rapid deployment	Yes	No
Carrier redundancy	Yes	No
BYO connectivity	Yes	No
Hybrid networks	Yes	No
Quality of service (QoS)	Yes	Yes

EASE OF DEPLOYMENT AND MANAGEMENT

SD-WAN

SD-WAN simplifies the configuration, deployment and management of networks and provides easy visibility into performance metrics like link health.

Changes in network topography (e.g. MACD) no longer need long provisioning and architecture lead times to implement. Because of this, there is no limit to how rapidly the organization's network can adapt in scale and/or size.

In the event that an organization has already invested heavily in MPLS, SD-WAN can integrate into existing MPLS networks in a hybrid deployment architecture.

With an SD-WAN network in place, organizations control the timing of deployments whether they be new sites or moves, adds, changes or deletions (MACDs).

MPLS

Common MPLS deployments are black box to the end-customer or the wholesale partner. The core network and core/CPE devices are controlled by the incumbent service provider with little visibility into performance or network health granted to wholesale partners or end-customers.

In addition, as MPLS is provided by the larger telecoms, the architecture requires long design, quote, order and implementation cycles. Configuration is also a complex undertaking that can lead to costly errors that take time to identify and fix.

Organizations are ultimately using someone else's network and are reliant on trouble tickets, escalations and MACD requests to manage the network's implementation and configuration according to the negotiated terms and conditions of the Service Provider contract.

FINANCIAL OUTCOMES

SD-WAN

A study of Turnium SD-WAN partner deployments shows that break-even is less than 1 year with a 143% return on investment in that first year with a 4-year ROI of 2,645%.

These higher profit margins offset any margin erosion experienced by SPs. Flexible contracting is a feature that is attractive to organizations that are in the midst of a digital transformation.

MPLS

MPLS, by nature, is a mature product with pricing and margins that have eroded over time. SPs that continue to rely on MPLS as a source of revenue must look for value-added products and services to upsell in order to maintain profitability levels and attain financial goals.

In addition, long-term fixed contracts are a detractor to organizations considering developing their WAN strategy using MPLS.

RELIABLE AND SECURE BY DESIGN

SD-WAN

Data flows can be encrypted end-to-end using AES 128- or 256-bit encryption. This is enabled through configuration in the software and implemented on the SD-WAN equipment itself.

In addition, when bonding multiple links in a SD-WAN, data flows can be obfuscated by using transmitting and receiving packets over all links at the same time. This mitigates man-in-the-middle attacks that attempt to capture data while in transit. Multiple bonded links work with all links active simultaneously and deliver up to 95% of the available bandwidth with no route reconvergence.

MPLS

Encryption is not enabled in MPLS as it requires a separate endpoint device to handle the encryption portion.

Instead MPLS relies on a secure network core and labeling for data privacy. Should the organization require redundancy, MPLS requires reconvergence of routes so that the failover link becomes active in the event of primary link outage, meaning that at any given time the organization is effectively only using 50% of its available bandwidth.