The WAN of the Future: MPLS or the Internet?

Joanie M. Wexler

March, 2016

The WAN of the Future: MPLS or the Internet?

Multiprotocol Label Switching (MPLS) virtual private networks (VPNs) have long been the darling of the enterprise WAN. Secure, reliable, and high-performing, they offer business-grade traffic control features particularly well-suited to carrying real-time and business-critical data. Combine these characteristics with the single-operator nature of MPLS VPNs and end-to-end network service-level guarantees, and you can see why MPLS has remained top dog in the enterprise WAN for the past 15 years.

But we all know that the only constant in technology is change. And, indeed, there are finally rumblings afoot when it comes to MPLS in the enterprise WAN, too.

Cost, Technology Challenge MPLS

Some enterprises are seriously investigating the use of public broadband Internet links to augment or replace MPLS VPNs in some or all of their distributed sites. There are several reasons why:

- Budget-strapped enterprises want to save a few bucks in sites they don't think merit MPLS's comparatively hefty price tag.
- By using IPsec encryption, you can make Internet circuits, including wireless WAN access connections, as secure as MPLS VPNs.
- CPE vendors are making public Internet connectivity and routing "smarter," mimicking some of MPLS's traffic control features to deliver better performance to buyers.
- Software-defined WANs (SD-WANs) are coming into their own to automate the configuration and actions of edge routers. That makes it easier to deploy and use the intelligent CPE services mentioned above, including IPsec-based VPNs.
- The uptake of cloud computing means enterprises need fewer dedicated pipes from branches into their data centers. Data center connectivity has long been a primary application for MPLS VPNs.

There's no question that MPLS VPN still offers premium value and will continue to deliver benefits over and above broadband Internet links (see Table 1, page 2). Still, Internet circuits are gaining some features that are competitive with MPLS while generally costing what Nemertes Research estimates to be about an order of magnitude less. And that's hard for network decision makers to ignore.

Table 1. MPLS and Internet VPNs: Comparison Summary

Characteristic	MPLS VPN Service from Carrier	Internet VPN Built on IPsec CPE from OTT Vendors
Cost	High $300 to $600 per Mbps per annum (Nemertes) *Example: $30,000 to $60,000 per year for a 100-Mbps link*	Low $29 to $60 per Mbps per annum (Nemertes) *Example: $2,900 to $6,000 per year for a 100-Mbps link*
Bandwidth	Very high (up to 10 Gbps)	Medium (10s to 100s of megabits per second)
Security level	High	High
Service-level agreements (SLAs)	Yes, end to end	No
Procurement	MPLS VPN operator	Router vendor plus ISP(s)
Provisioning time	Long (weeks or months)	Short (possibly minutes)
Intelligent routing	Yes	Yes
Multicast	Supported	Not typically supported
SD-WAN configuration automation capabilities	Coming	Yes
Prime use cases	• Data center connections • Critical and latency-sensitive apps, such as voice over IP • Multicast traffic (such as video and brokerage communications apps)	• Public cloud connections • Machine-to-machine (IoT) communications • Credit card data transfer • Failover/backup to primary link • VPN offload • Remote access for single user
Each WAN type has its merits and its shortcomings. Enterprises are starting to do a better job of matching the right technology to the right location based on their particular network and budget requirements.		

Buyer Trends

Whether there will be a wholesale shift off of MPLS onto Internet (wired or wireless) links is unknown. But many large enterprises using MPLS today are likely to move at least some traffic onto broadband links if they haven't already. While network security and performance will remain top of mind for most enterprises indefinitely, many perceive that the Internet has become more stable and reliable and figure that it is up to the job of carrying corporate WAN traffic in certain circumstances.

For example, the number of companies using Internet connections in place of one or more traditional WAN links grew from 30 percent in 2012 to about 55 percent in 2014, according to Nemertes, and "the trend continues," says Johna Till Johnson, the firm's founder and CEO.

One big reason is cost, of course. In fact, even putting transport service costs aside, Gartner estimates that the emergence of SD-WANs and running a mix of MPLS and Internet links in a hybrid fashion can save up to 40 percent in capital expenses, maintenance and operational costs (see Table 2).

Table 2. Comparative Costs*

Example: Three-Year Costs for 250-Branch WAN		
Item	Traditional	SD-WAN
Router Capex	$1,000,000	$250,000
Router Maintenance/Support	$180,000	$150,000
Staffing Opex	$105,000	$52,500
Total	$1,285,000	$452,500

*Not including network transport services
Source: Gartner (July 2015); table 1

Consider companies running MPLS with T1 services and planning to deploy apps needing greater bandwidth. When they discover that increasing to 5 or 10 Mbps MPLS will double their monthly service costs, their budget might force them to turn to broadband for the needed capacity.

Different Solutions for Different Sites

Not all work sites are created equal. It's true that many branch offices are starting to need network capabilities on a par with regional and headquarters locations. That's because they are experiencing growing traffic loads brought about by explosions in mobility, cloud connectivity, guest access requirements, and multimedia applications. Still, some locations have more modest needs. Consider the retail site that might transmit low-speed credit card transaction and inventory data only, for example. At least some network managers reckon that a secure broadband Internet link could handle the job just fine.

And what about the Internet of Things (IoT), which is also adding volumes of traffic to the overall WAN load? If a given site is transmitting only IoT traffic from one machine to another without stringent latency requirements, that site, too, might get by much less expensively using a broadband connection.

These are among the reasons that MPLS VPNs are running into new competitors positioning the Internet with IPsec encryption as a low-cost MPLS alternative. Broadband links are fast enough for the needs of many secondary enterprise sites and are available nearly everywhere, making price-to-performance gains very attractive. To date, most businesses that are deploying "Internet as WAN" are doing so in their smaller sites or as a secondary, backup path to a primary MPLS VPN connection.

Secure Direct Internet Connections in Branches

It's also becoming common to provide branch sites with direct Internet access (DIA). It is far more efficient to build DIA connections than to backhaul all branch traffic to the data center, apply security policies and protections there, and then forward it back out over the corporate Internet connection. The backhauling setup wastes bandwidth and impedes performance.

A few years ago, DIA was known primarily as "split tunneling" and was considered a reckless thing to do. At that time, companies worried that malware on the public Internet could leak from the Internet onto the MPLS VPN through the branch router and infect corporate traffic. At the very least, without backhauling, users' Internet access connections would be insecure unless separate security was procured and applied to the separate, branch-based Internet traffic flows. And that meant more cost and complexity.

However, today's emerging SD-WAN approach to hybrid networking – running both an MPLS connection and a direct Internet connection out of a single router in a branch – builds in special routing security zones into the endpoint CPE. The capability segments traffic and makes it unable to intermingle between the private and public networks. Often, SD-WANs also layer advanced threat protection into the CPE. Some integrate with your own security policy servers to automatically extend data center security mechanisms. So "split tunneling" no longer has the nasty connotations it once did.

Lexicon for Tomorrow's WAN

DIA - Direct Internet access. Connecting a branch location directly to the public Internet, rather than backhauling traffic from the site through a data center hub to apply security policies before sending it on to its destination.

Hybrid WAN. A network that uses two or more wide-area service types to link geographically dispersed locations. Today, the term most often describes a mix of MPLS VPN and broadband Internet links in a given enterprise network.

NFV - Network functions virtualization. Converting traditional network equipment appliance functions – such as routing, firewalling, WAN optimization, load balancing, and others – into software instances, or "virtual appliances." Virtual appliances are analogous to "virtual machines" in the application server area of IT and allow very quick deployment of network infrastructure functions. Multiple NFVs can run on a single piece of host equipment.

OTT - "Over the top." A phrase used to describe new WAN competitors who do not offer WAN network services per se, but do offer endpoint equipment with built-in security and smart network features to use in conjunction with Internet transport services. OTT suppliers are traditional router vendors and new WAN equipment entrants who provide security and other intelligent software in their CPE. Some, but not all, also offer software-defined, programmatic capabilities to configure and change the network (see below).

SDN - Software-defined networking. A modern, automated way of configuring networks by using programmatic interfaces to activate, change, or decommission physical or virtual network appliances. This is a much simpler and speedier way to operate networks than the traditional approach of buying, installing, testing, managing, and updating each piece of networking equipment separately.

SD-WAN - Software-defined wide-area network. Building on the principles of the SDN (above), a simplified, automated approach to supporting branch office connectivity, usually in the form of a hybrid WAN.

Who's offering what?

MPLS alternatives are appearing primarily from equipment makers bundling security and traffic control features into routing gear at customer endpoints. They are, in effect, taking on MPLS VPN network service providers such as AT&T and Verizon by revving up the boxes that sit at network sites with intelligent network services akin to those found in MPLS services. Some, like Cisco, are also virtualizing many of the functions so that they are fast and easy to deploy.

Many of these companies are referred to as "over the top," or "OTT," vendors. That's because they do not sell network services per se; instead, they sell an adjunct to the services in their CPE that makes Internet routing smarter and more secure.

Some of these devices are basic routers with IPsec capabilities. Others have multiple functions bundled in, such as firewall, WAN acceleration, wireless LAN control, advanced threat detection, load-balancing and mobile device analytics. Some also offer policy-based routing, a feature that continually monitors the available WAN links and routes traffic over the best-performing one at the moment. And some are full-blown SD-WAN vendors, allowing customers to use a captive portal to configure, change, and deploy features across remote sites in software, making it less time-consuming and far easier to turn up new sites and network functions.

It won't be long until x86-based servers can host multiple network functions – starting with routing and firewalling – as 'virtual appliances' in a single platform.

Network appliance makers such as Cisco, Meraki (a Cisco company), Fortinet, Velocloud, and Viptela are among those offering various combinations of these features. Perhaps the best-known SD-WAN is Cisco's Intelligent WAN (IWAN), a collection of network services that run on Cisco routers to make Internet, LTE, and other low-cost WAN connections more MPLS-like. An IWAN App has been created for use with the company's SDN controller to automate setting up all the various and sundry IWAN features. The app reportedly reduces about 1000 CLI commands to 10 clicks.

There is a growing list of SD-WAN vendors; others include Citrix, Riverbed, Silver Peak, and Talari. Most of these deployments today are on respective vendors' router platforms; however, X86-based servers, too, are beginning to house network infrastructure functions as virtual software instances. Cisco is offering the x86-based host platform option, for example, and so is AT&T, which is both a Cisco partner and competitor. AT&T has announced a Network on Demand initiative that includes a Universal CPE (uCPE) option for eventually running multiple virtualized network functions on a single x86 box.

The trend toward network functions virtualization (NFV) – whether you get it from a box vendor or a network service provider – is analogous to what's happened in the computing area. Enterprises have been using virtualization to create, move, and decommission application servers as "virtual machines," or VMs, quickly across a farm of compute infrastructure as needed. Similarly, it won't be long until x86-based servers can host multiple network functions – starting with routing and firewalling – as "virtual appliances" in a single platform.

Both Cisco and AT&T, for example, allow virtual appliances from third parties to run on their servers. That's appealing, because you can get the best-of-breed function you choose rather than being locked into a single vendor's network appliance technology.

What are the carriers doing?

The IPsec box-plus-broadband combo being offered in various enhanced forms by CPE vendors is growing more attractive, but you can bet that the traditional network service providers aren't sitting still. There are efforts afoot by them to take on their new competitors with greater integration among their many service options. For example, today, delivering the multifunction nature of emerging CPE might require two or more separate service contracts from an MPLS VPN service provider. Better integration and interoperability among those services would help ease that barrier.

The MPLS carriers have also alluded to plans to supply businesses with lower-end Internet services that are more price competitive with broadband offerings today, perhaps by using depreciated consumer-grade networks. And AT&T's uCPE rollout indicates it has no intention of ignoring the multifunction trend of CPE-makers: As mentioned, it has partnered with Cisco to put Cisco software-based routing instances in its uCPE and has also announced similar partnerships with Brocade, Fortinet, and Juniper Networks for other virtual network functions.

Who's to say MPLS prices won't begin to drop as real WAN competition looms?

And, finally, who's to say MPLS prices won't begin to drop as real WAN competition looms?

Summary

Internet-based IPsec VPNs, particularly when coupled with multifunction CPE and SD-WAN capabilities, are providing competition to MPLS offerings. Broadband options are growing particularly attractive in smaller sites and for failover, machine-to-machine, telecommuter, direct Internet and cloud connectivity applications.

Some companies just want to offload their MPLS VPNs of non-critical and non-real-time traffic, leaving existing premium links available for the SLA-covered traffic. That has resulted in the birth of the hybrid WAN, where a site might have one MPLS connection for premium traffic and one Internet connection for best-effort traffic.

The good news is that the emergence of Internet-based intelligent WANs will force MPLS providers to act, either with pricing or a broader portfolio of offerings that better match the diverse needs of various sites. Better integration of the carriers' MPLS, remote access, Internet, and cloud offerings will likely be a side effect, too, allowing customers to orchestrate a portfolio of carrier services from a common portal.

It's doubtful anyone would claim that Internet IPsec VPNs are on a par with the features, speed, and reliability of MPLS VPNs – at least not yet. However, in certain sites and for some applications, it just might not matter.

About the author: Joanie M. Wexler is an independent editor who has been writing about the business implications of computer networking technology for more than 25 years. Reach her at joanie@jwexler.com.