White paper

Making the case for MPLS in the modern enterprise.

verizon

Data communications have been the cornerstone of enterprise networks for decades. As the economy gradually grew more global – and the computer revolution took hold – companies needed to rapidly exchange data between locations around the world, faster than ever before. Throughout the decades, network operators like Verizon have developed new, more advanced technologies designed to meet the network needs of enterprises as they continue to evolve.

From the 1960s all the way to the '90s, fixed private lines were the primary vehicle for exchanging information between sites. But one of the primary drawbacks was – and still is – that the further the distance, the more it costs. Because the connections were fixed, service disruptions – caused by acts of nature or something else – would negatively impact the flow of data.

The introduction of Layer 2 in networks in the '90s was hailed as a data revolution, because it made connections between locations virtual rather than physical. That meant an enterprise could have a single physical port into a provider's network point of presence and exchange data with many different sites on their network by using Permanent Virtual Connections, or PVCs. Layer 2 networks also provided the same level of security as a private line, but at a significantly lower cost, because service providers could aggregate customer traffic over a shared network infrastructure.

But shifting from private line to Layer 2 wasn't an easy upgrade, mainly because there was a significant upfront investment when shifting from private lines to Layer 2 networks. Making the Layer 2 change required an entirely new infrastructure to be built, including new customer premises equipment (CPE) at all locations. Because the long-term savings resulting from the elimination of expensive distance-sensitive private lines, enterprise customers were willing to make the one-time expenditure.

Also, the migration to Layer 2 wasn't without its shortfalls. Frame Relay, the most commonly used type of Layer 2 network, treated all forms of data as equal and didn't prioritize traffic. Voice was treated the same as data, and it often required a single, dedicated PVC assigned to it. This added to the cost and complication of managing the network. So while Layer 2 networks reduced expenses as a replacement for private lines,

they weren't considered future-proof. They also certainly couldn't meet the growing demands for the new types of data that were gradually being introduced to the enterprise environment.

The year 2000 not only marked the beginning of a new century, but also the concept of network-based virtual private networks (VPNs) that use MultiProtocol Label Switching (MPLS) as a new Layer 3 form of data communications. This offered the same level of security as Layer 2 but with additional flexibility to support any-to-any connections.

MPLS was originally proposed to allow high-performance traffic forwarding and engineering in IP networks – specifically the public internet. It's a scalable, protocol-independent transport in which data packets are assigned labels. Packet-forwarding decisions are made solely on the contents of this label, without any need to examine the packet itself.

This means you can create end-to-end circuits across any type of transport medium, using any protocol. The primary benefit is to eliminate dependence on a particular Open Systems Interconnection (OSI) model data-link layer technology, such as Asynchronous Transfer Mode (ATM), Frame Relay, Synchronous Optical Networking or Ethernet. It can also eliminate the need for multiple Layer 2 networks to satisfy different types of traffic.

MPLS-based VPNs are positioned as evolutionary migrations from Layer 2 networks, since they allowed enterprises to reuse their existing CPE – a major advantage over a private-line-to-Layer-2 conversion. Because MPLS uses Layer 3 in its core, it eliminates the need for virtual connections between locations. Instead, traffic is delivered between two customer locations based on IP address. Once an MPLS port

is activated on the customer's VPN, it can communicate with any other site on the VPN, no matter where it's located on the carrier's network. This was seen as a clear advantage over Layer 2 networks. Another advantage of MPLS VPNs is that they offer the same level of security offered by both private line and Layer 2 networks, since sites can only communicate with other locations on their VPN.

The introduction of differentiated services or DiffServ in 2003 proved to be a game changer for MPLS VPNs by specifying simple and scalable mechanisms for classifying and managing network traffic, and providing quality of service (QoS). DiffServ can, for example, be used to provide priority, low-latency service to critical network traffic such as voice or streaming media. It can also provide simple best-effort service to non-critical services such as web traffic or file transfers.

An unprecedented growth of MPLS VPNs started almost immediately following the introduction of DiffServ, since it allowed enterprises to place all their locations on a single platform, giving them the ability prioritize their traffic and make use of common applications used over the public internet—such as video conferencing and email—on a secure network. As a result, MPLS VPNs have become the gold standard for data communications ever since.

Beginning in 2014, two new terms began to make their way into the network management lexicon: software-defined networking (SDN) and software-defined wide area network (SD WAN). The firms offering these services weren't network operators but rather hardware- and software-based companies selling that combination so enterprises could manage their data networks using the public internet instead of MPLS VPNs.

A big part of their argument for migrating to the public internet was that, thanks to investments from both the public and private sectors, internet access was offered almost anywhere globally, with much higher speeds for both consumers and businesses of all sizes. This prompted a number of enterprises to ask:

- Does my company still need an MPLS VPN?
- Can't I protect my data in transit by encrypting it and using established protocols like IPsec or even an SD WAN?
- Isn't MPLS VPN much more expensive than a consumer-class broadband connection?

Yes, all the statements above are true. But it doesn't take into account that the public internet is focused strictly on the transport of data packets with no QoS, no uptime guarantees and no ability to increase capacity on an as-needed basis. Plus, it's vulnerable to distributed denial-of-service (DDoS) attacks. In effect, an enterprise is sending their packets over a best-effort network and hoping their traffic arrives intact at its destination. The design of the internet has worked brilliantly since its inception for the delivery of email and file transfers, but it's not ideal for dealing with dynamic and mission-critical data applications.

SD WANs rely on point-to-point connections between devices at the customer's locations and the service provider. Essentially SDWAN is a management tool, and the vendors do not own or manage the connections, they just manage the traffic based on the networks they are able to access.

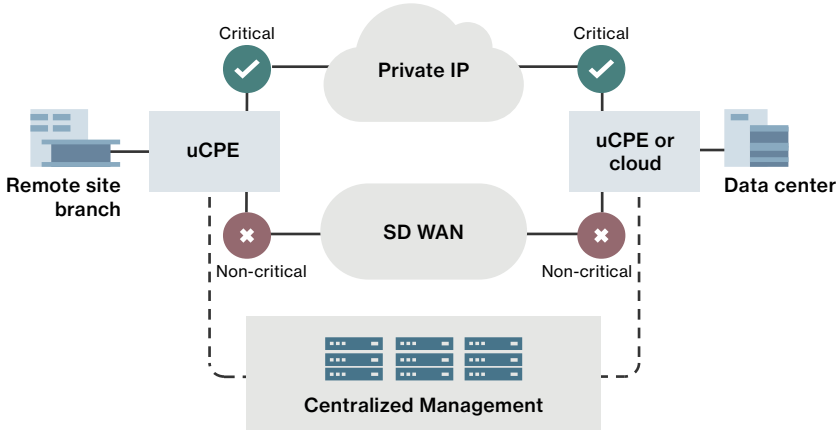
By the year 2020, up to 75% of the internet will be used to support video applications, thanks to "over-the-top" services.

In contrast, an MPLS VPN is a business-grade service which doesn't use the public internet and is therefore not subject to the same risks that go with it. MPLS networks are engineered with QoS, resiliency, capacity flexibility and business continuity built in. MPLS provides layers of enhanced services specifically targeted toward business-grade traffic and high availability. And unlike the internet, MPLS networks are ideal platforms for real-time applications, such as IP telephony and multicasting.

There are a number of considerations an enterprise should review when determining whether the internet or an MPLS VPN is the best option for their business traffic:

Limitations on capacity

An internet connection at an enterprise may not have enough capacity to support converged applications and video traffic. Recent white papers have concluded that by the year 2020, up to 75% of the internet will be used to



support video applications, thanks largely to the increase of "over-the-top" (OTT) services that enable consumers to use the internet for entertainment in place of typical broadcast networks. Even if an enterprise is restricting access to video applications on their IPsec or SD WAN network, this will be done on a provider edge (PE) device being used by consumers who regularly access video. That could impact the performance of their business traffic. An enterprise may have to purchase and manage connections on many different internet service providers (ISPs) to get the capacity it needs during peak traffic periods, adding cost and complexity. MPLS network performance and capacity are not subject to the quality of an ISP's peering arrangements.

Private IP—Verizon's MPLS-based VPN offering—is built on an architecture that uses a closed infrastructure with no internet reachability. This means the network is not susceptible to the impact of consumer-based internet traffic, such as OTT video applications. Plus, network capacity is proactively monitored and can be increased rapidly to stay ahead of customer demand.

Static versus dynamic

Both SD WAN and IPsec internet connections are connection-oriented—similar to the older Layer 2 networks such as Frame Relay and ATM—and rely on tunnels to create connections. This may be ideal for situations where one location communicates exclusively with another. But in today's enterprise environment, locations are dispersed geographically and often mobile. If you want to fully mesh topologies, you have to create multiple tunnels at every location within your network, increasing management complexity. A hub-and-spoke network is easier to manage, but is not ideal for real-time or latency-sensitive applications.

An MPLS VPN provides any-to-any connectivity. This enables enterprise landline sites and mobile users to exchange voice, data and video traffic directly with one another rather than requiring traffic to cross a central hub, slowing performance, to get to the preferred destination. Classes of Service (CoS) and any-to-any connectivity enable business applications to perform at a high level and are a must for real-time applications, like voice and video.

> "Claiming SDWAN is an MPLS killer is hyperbole, but the reality is that SDWAN does offer a number of attractive benefits to enterprise customers, such as more effective use of multiple WAN links, more efficient management workflows defining access and quality policies, improved application and network performance visibility and improved security enforcement."
> —Current Analysis Research

DDoS vulnerability

Even if an enterprise opts to encrypt its traffic, the internet doesn't protect you from service outages caused by DDoS attacks. Your own IP addresses won't be able to be spoofed if encrypted. However, if others are, you're susceptible to the resulting downtime.

Since private address space is used with an MPLS VPN, enterprises are not susceptible to having their addresses hijacked, used as spoofed source addresses, or other threats that exist on the internet. MPLS doesn't reveal additional unnecessary information even to customer VPNs. Since the interface to the VPNs is Border Gateway Protocol (BGP), there is no need to reveal any information about the core. The only information that is required in the case of a routing protocol between a PE and a customer edge (CE) is the address of the PE router. If this is not desired, static routing can be configured between the PE and CE. With this measure, the MPLS core can be kept completely hidden and be addressed using public or even private address.

Single-owned infrastructure

The internet is essentially a conglomeration of many service providers who control only their own networks; once they pass traffic across network borders, any policies and priorities that have been specified for how to handle traffic vanish. An ISP cannot control a service degradation whose underlying cause is in a physical segment of the internet controlled by a different provider.

Because MPLS VPNs are owned and operated by a single network service provider, that provider has the ability to engineer and manage the network so that your traffic behaves in accordance with your specified policies and priorities.

An enterprise can opt to encrypt data crossing a broadband access link using IPsec, but securing the business data in transit is where the benefit of this type of VPN ends. A business-grade VPN, such as an MPLS VPN, reduces additional types of risk while offering network service enhancements designed to make user experiences consistent and reliable. Along with supporting additional security, MPLS was designed to be a networking platform for business, so it layers many other business-class network service enhancements on top of secure transport, including:

- Inherent infrastructure redundancy for business continuity that allows traffic to be rerouted around failures in milliseconds rather than seconds or minutes
- CoS capabilities to prioritize and manage traffic so that the most important or delay-sensitive traffic is delivered first

There is a role for SD WANs in the enterprise space. But SDN and SD WAN should not be seen as alternatives to MPLS; they're enhancements. Both technologies can be carried over an MPLS network as an alternative to the public internet. This might be especially beneficial for accessing non-critical business applications on a cloud service provider while maintaining the level of security offered by MPLS.

Another approach would be to incorporate a hybrid environment using both an MPLS VPN and the public internet. As with the all-MPLS solution described above, all non-mission critical applications could be supported using an SD WAN while business-sensitive data would remain on the MPLS VPN. This hybrid approach provides the level of security enterprises require while offering a cost-effective method for accessing cloud-based applications.

The introduction of SDN and SD WAN has provided another item in the Chief Technology Officer's tool belt that makes it easier to manage their daily business. It's part of the ever-evolving world of data communications, which began with private lines in the mid-20th century, MPLS VPNs in the 21st and continues on today.

Learn more.

To learn more about our MPLS network, speak with your account representative.

i White paper: *Cisco VNI Forecast and Methodology, 2015-2020* http://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html

ii A Competitive Assessment of SD WAN Offerings (If SD-WAN isn't on your competitive radar, you're missing out on an opportunity.) Mike Fratto, Current Analysis, September 2016.