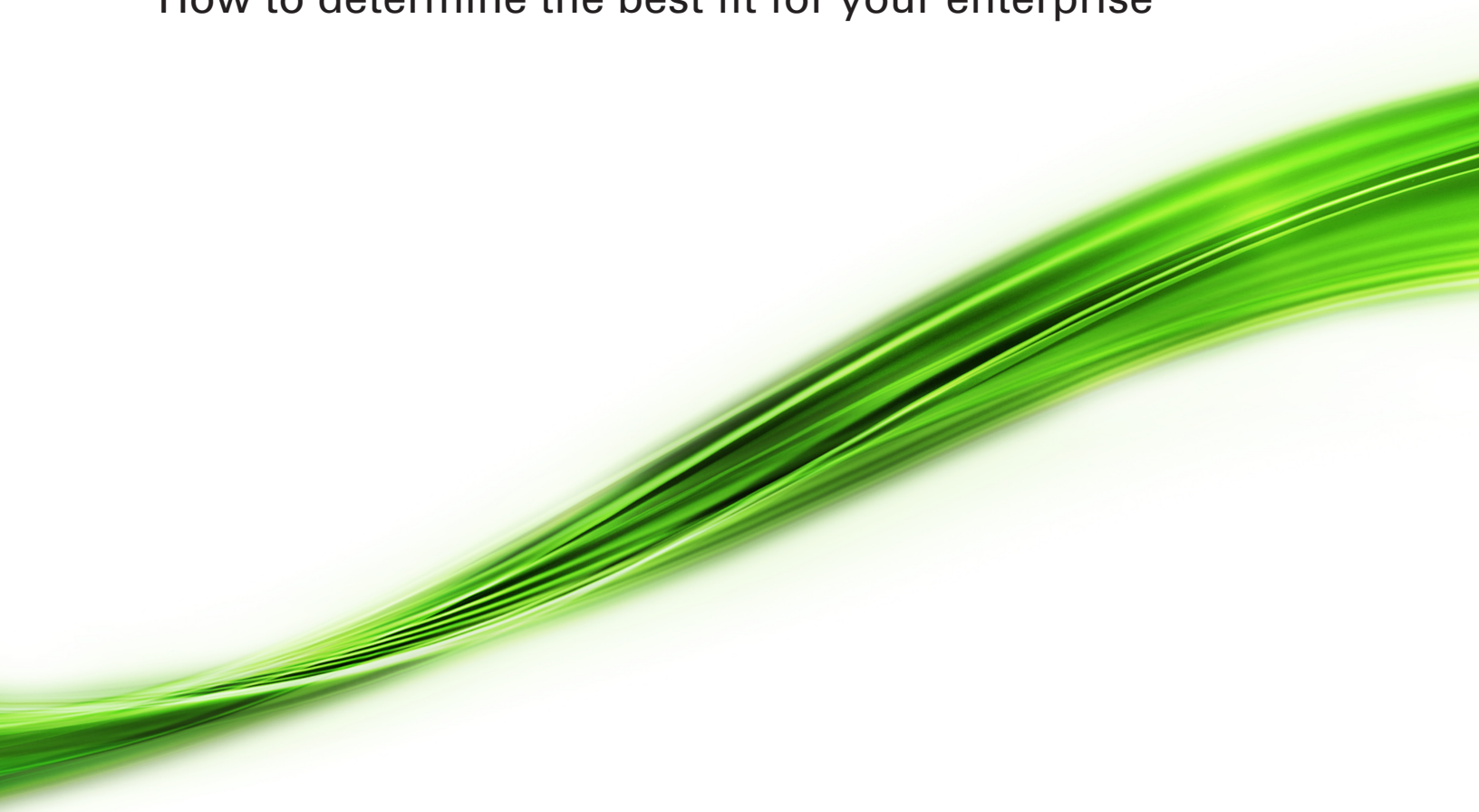
Evolving Your Network with Metro Ethernet and MPLS VPNs

How to determine the best fit for your enterprise



A CenturyLink White Paper

CenturyLink™ Business

Stronger Connected™

Evolving your Network with Metro Ethernet and MPLS VPNs

How to determine the best fit for your enterprise

Change is a constant in enterprise networking and the axiom definitely holds true when considering wide-area connectivity options. Experienced IT managers have lived through the evolution of time-division multiplexing, x.25 packet switching, Frame Relay, and ATM. Today IT managers have newer and improved options to choose from, including Multi-Protocol Label Switching (MPLS) Virtual Private Networks (VPNs) and Ethernet, which has re-emerged as a very affordable networking solution in Wide Area Networks (WANs). For most enterprises, choosing from MPLS VPNs and Ethernet is not an either-or decision but a question of where and when to implement each solution. Just like tools purpose-built for different tasks, MPLS VPNs and Ethernet offer enterprises significant value but only when properly matched to the corresponding business requirements.

Just like tools purpose-built for different tasks, MPLS VPNs and Ethernet offer enterprises significant value but only when properly matched to the corresponding business requirements.

MPLS VPNs are best known for their flexibility to handle many different protocols and operate across a wide range of commonly available connection speeds that are typically used in branch office connectivity, point-of-sale applications, and the like. Ethernet has also become a popular solution for higher speed WANs. It leverages the simplicity of Layer 2 switching (ubiquitous on high-speed LANs) and is therefore best used where IP is the sole protocol and only if multi-Mbps or Gbps connection speeds are possible.

Choosing one of these WAN connectivity options is easy once managers tally up the number of connections, throughput needed, protocols, amount of technical resources available, class of service, and other criteria. This paper summarizes the use cases and benefits of each WAN option and how to select the networking solution that best matches the needs of the enterprise.

MPLS VPNs in Wide Area Networking

MPLS is a data packet switching technology that is widely used by service providers today to connect the data networks of organizations with multiple, dispersed locations while still allowing them to operate disparate protocols such as Frame Relay, ATM, and Ethernet. By encapsulating these varying protocols in "labels," an MPLS network can make packet-forwarding decisions without understanding the contents of the packet. Within the OSI Model, MPLS VPNs operate above Layer 2 but just below Layer 3 (see Figure 1 on next page). Because they operate independent of Layer 2 information, MPLS VPNs are known to be protocol agnostic, interconnecting networks independent of the underlying protocol. The technology's unique attributes enable the creation of virtual circuits that can scale nationally and even globally to connect a large number of remote networks – completely independent of which Layer 2 protocols may be running. While organizations still maintain their unique LAN infrastructures and varying WAN access approaches in these configurations, MPLS unifies them.

Network (OSI Layer 3)	**IP**
OSI Layer "2.5"	**MPLS**
Data (OSI Layer 2)	**Frame Relay, ATM, Ethernet, PPP**
Physical (OSI Layer 1)	**Fiber, DSL, etc.**

Figure 1: *As seen in the table above, MPLS VPN is unique in that it sits between OSI model Layers 2 and 3, is protocol agnostic, and works across multiple Layer 2 technologies.*

By using MPLS VPNs, IT managers gain a single and centralized approach to WAN connectivity that eliminates the inefficiencies of maintaining separate duplicative networks. Moreover, they can prioritize one type of traffic over another. For example, voice or video can be ensured low latency and packet loss. That's because MPLS VPNs can assign a Quality of Service (QoS) based on the labels applied to different packets, an important attribute when multiple networks are combined.

By using MPLS VPNs, IT managers gain a single and centralized approach to WAN connectivity that eliminates the inefficiencies of maintaining separate duplicative networks.

MPLS VPNs' flexibility also means that enterprises can access a service provider's MPLS network using many different access technologies including fractional T1, T1, DSL, Frame Relay, and Ethernet. Managed service providers typically connect customer networks to MPLS VPNs using link speeds ranging from 56 Kbps (DS0) to 45 Mbps (DS3).

Ethernet in Wide Area Networking

Ethernet's popularity is gaining rapidly as it offers a wide range of high-speed connections (hundreds of Mbps to Gbps) at lower cost when compared to Sonet services of similar speeds. Ethernet is a cost-effective option in part due to its reliance on a single standard and because it works across homogeneous hardware that is readily available from multiple vendors. This makes it inexpensive when compared to alternatives such as Frame Relay or ATM. Beyond the benefit of low capital costs, Ethernet is widely understood and less complex than other networking options. As a result, enterprises can connect to this WAN service easily and without sophisticated knowledge or IT management skills. For example, in most instances, Layer 2 switching and previously established Virtual LANs are used to connect, thereby avoiding the cost and complexity of managing routing infrastructure.

Beyond the benefit of low capital costs, Ethernet is widely understood and less complex than other networking options.

However, there are limitations to this LAN-based technology. Ethernet is a viable WAN access option provided the enterprise only needs to connect a limited number of endpoints, and that they all use IP over Ethernet. In comparison to MPLS VPNs, Ethernet does not typically offer quality or class of service options necessary for traffic engineering when many different networks are combined. This can make it challenging to ensure data isn't competing for bandwidth needed by critical voice applications in a converged network, for example. Moreover, because Ethernet operates at such high speeds (5 Mbps to 10 Gbps), its availability is limited, preventing its use to interconnect distant regional users lacking access to higher speed links.

There are three types of wide-area Ethernet services available today:

Ethernet Private Line – Here Ethernet is used to form point-to-point connections for each circuit throughout the transport network. The most common example is the connection of remote facilities to centralized resources at a headquarters facility. Another use case is the connection of a PBX to a Session Interface Protocol (SIP) gateway to enable Voice over IP (VoIP) service.

Ethernet Virtual Private Line – When there are multiple locations to be connected, this variant of Ethernet enables point-to-multipoint connections that would be found in the hub-and-spoke topology typical of headquarters to branch office connections. Using virtual circuits, Ethernet Virtual Private Line eliminates the need for ports in Customer Premises Equipment (CPE).

Metro Ethernet – In this instance, Ethernet is used in a metropolitan setting to connect LANs by creating a Metropolitan Area Network (MAN)—sometimes referred to as an Ethernet LAN or ELAN. Alternatively it can create a high-speed connection to the Internet to support an extremely large number of users.

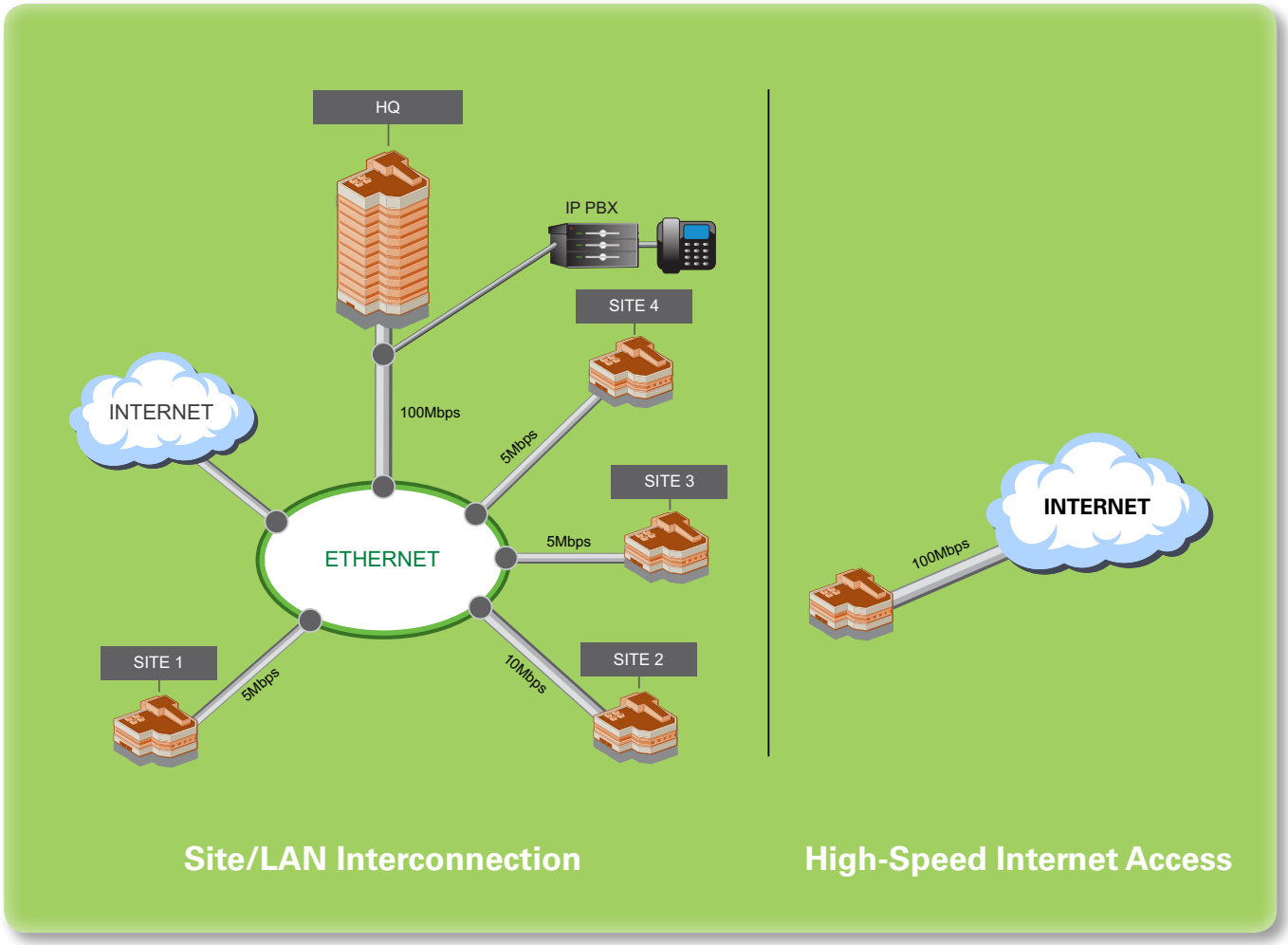


Figure 2: *As seen in the diagram above, Ethernet can be used to interconnect multiple LANs in a metropolitan setting or it can provide a single high-speed connection to the Internet for a large number of users accessing bandwidth-intensive applications such as video*

Where to Use MPLS VPNs

MPLS VPNs are, by design, highly flexible and can therefore be used in a range of scenarios. But that doesn't mean they should be used everywhere. Its four main benefits are:

- Integration of disparate protocols
- Operation across a wide range of connection types and speeds
- Prioritization of latency-sensitive traffic such as voice or video using class-of-service tagging
- Inherent security through internal and independent label addressing schemes that provide additional security, for example, to prevent Denial of Service attacks or spoofing that is possible via IP

These attributes and flexibility make MPLS VPNs a good choice for highly distributed and heterogeneous networks where:

- It is difficult or impossible to mandate the use of a single protocol or infrastructure
- A wide variety of delay-sensitive applications compete for bandwidth (VoIP)
- WAN connection methods and speeds are sub-Mbps, such as in remote access cases
- IT management resource or competency vary widely
- Businesses are highly distributed or expanding rapidly

The following examples illustrate how MPLS VPNs are used in some sample industries.

Finance/banking – Well known for mergers and acquisitions, financial and banking networks are most often a multi-protocol patchwork of networks. Access speeds run the gamut from higher speeds at headquarters to lower speeds at branch networks and even lower speeds at ATM terminals. Such a distributed architecture makes it impossible to maintain technical support resources at each endpoint. MPLS VPNs can carry all protocols, work across all speed links and are fully managed, significantly reducing the amount of internal IT management overhead required.

Insurance – Regional and national insurers typically employ a large headquarters for data warehousing and claims processing and a highly regionalized employee base to service customers. Collaboration and communication between central administration and remote field offices is key. While MPLS VPNs' ability to enable an integrated network lowers operating costs for insurers, uniform access to information accelerates decision-making and improves customer satisfaction.

Real Estate – All real estate brokerages operate regional offices that need access to a common database of present listings and past sales. Field agents are constantly transmitting images of properties, scanned contracts, and the like. Mergers and acquisitions are frequent in this industry, often producing a patchwork of different data networks. MPLS VPNs can interconnect all offices and network all applications, including voice.

Utilities – Utility companies are in constant contact with remote systems through a system called Supervisory Control and Data Acquisition or SCADA. Everything from tank volumes, system voltages, currents, and alarms are fed to centralized offices for monitoring and troubleshooting. This remote telemetry is accomplished through a mix of legacy protocols and Frame Relay that can be easily aggregated using MPLS VPNs.

Manufacturing - The voice and data networks of manufacturing companies are highly meshed, interconnecting a web of developers, suppliers, partners, and dealers. In fact, connections are as dynamic as the nature of their business. MPLS VPNs interconnect bandwidth-intensive CAD applications and CAM applications as well as lower-speed connections to dealers for inventory tracking and replenishment.

These distributed businesses share similar characteristics and requirements:

- Use of varying protocols (Ethernet, Frame Relay, and ATM)
- Support for lower speed endpoints, such as ATM machines, point-of-sale machines, and remote employees
- IT management constraints, which make it difficult to scale across geographies and varying network types
- Voice and data usage that demands Quality-of-Service features
- Robust security and availability of networks
- User expectations for high reliability and performance of applications, independent of location

MPLS VPNs are the right choice for these environments due to their inherent flexibility as well as their ability to support value-added services such as remote access via SSL, IPSec VPNs, and Internet access using managed firewalls.

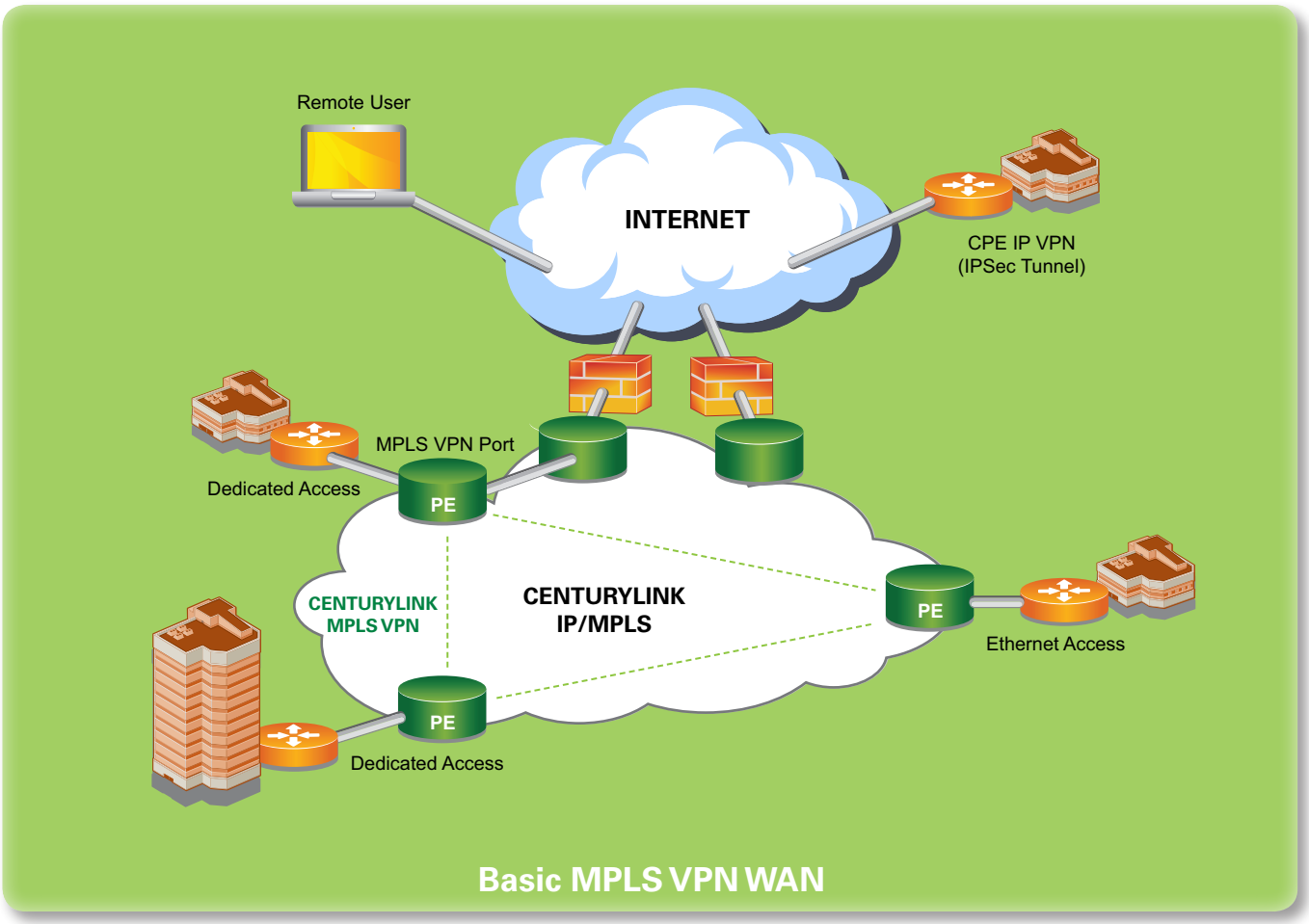


Figure 3: *As illustrated above, MPLS VPNs can support a wide range of protocols and access types including remote access, VPN connections, and dedicated access for a range of connection types and speeds.*

Where to Use Ethernet

By design, Ethernet is built to rely on a single protocol and access method – IP over Ethernet. This allows it to operate at extremely high speeds but also limits its availability as most regional locations don't have access to high-speed connections. In addition, as most Metro Ethernet services use Layer 2 switching (versus routing, as is the case with MPLS), they can only support 50 or fewer endpoints.

The following are ideal high-bandwidth applications for Ethernet.

Data center consolidation – Distributed data centers prevent enterprises from realizing economies of scale. While there are efficiencies in consolidating data center operations into a single location, this introduces the possibility of a single point of failure. Though redundancy and uptime can be enhanced through database or SAN replication and backup to an alternate location, the required connections are latency and packet-loss sensitive. Ethernet provides a high-speed connection that can support these requirements.

Campus LAN extension – Whether in a university setting or on a corporate campus, high-speed LAN interconnectivity is a requirement as content and applications become more and more bandwidth intensive. Distance-learning applications, video conferencing, and desktop sharing are examples of applications that demand extremely high throughput but in a relatively limited geographic area. Metro Ethernet can provide the required connections at a competitive price point.

Software-as-a-Service (SaaS) and Cloud Computing services – A growing number of software companies are moving away from selling software licenses and instead are selling their technology in a pay-per-use model. Because it's a challenge to predict uptake and use of these SaaS offerings, traditional WAN connections can quickly become overtaxed. Ethernet offers high-speed connections that can scale very rapidly to meet demand so that companies are never victims of their own success.

Contact center connectivity – Call centers grapple with the dual challenge of handling a high volume of voice connections while being dependent on fast data retrieval to deliver satisfactory customer service. Here Ethernet can furnish the Gbps connection speeds needed to handle voice and data. While voice traffic can be handed to a SIP gateway, IP connectivity ensures customer data is available to contact center employees instantly.

Video or other rich content delivery – YouTube may be the preeminent example of video delivery on the Internet but its success has paved the way for similar uses of video in the enterprise. Many companies use video on demand for employee skills training, HR compliance training, and customer support. Though the benefits are clear, throughput requirements are exponentially higher than that of traditional data access. Ethernet Private Line connections enable enterprises to easily scale to meet demand as needed.

A Guide to Selecting the Right WAN Technology

By answering a few qualifying questions, enterprises can determine whether they need an MPLS VPN service, Metro Ethernet, or both. Some of the key questions for consideration:

Number of locations. Where MPLS VPN supports routing and is scalable to thousands of locations, making it ideal for remote access, Metro Ethernet's Layer 2 switching limits it to implementations with fewer than 50 locations.

Protocols supported. As the M in MPLS VPN indicates, it can integrate multiple protocols through encapsulation. Ethernet is primarily designed for use with IP only.

Type of Application. In a converged network scenario, delay-sensitive applications like voice and video need prioritization over ordinary data. MPLS VPNs' ability to assign a Class of Service helps it avoid packet loss and latency that leads to declined Quality of Experience.

Connection speeds. The majority of enterprises rely on T1 or lower access speeds for the periphery of their networks (branch offices). Because MPLS VPN services are available at Mbps and sub-Mbps connection speeds, they are the best choice for highly distributed networks. In contrast, Metro Ethernet is only available at very high speeds and typically in limited (metro) areas.

Security. While both MPLS VPNs and Metro Ethernet can be made fully secure, MPLS routing capabilities provide an additional benefit in that they automatically adjust to network breaches, all done completely transparently to users.

Management overhead. MPLS VPN services are turnkey; enterprises pay the service provider to own the headaches of routing and maintenance of the CPE. While Metro Ethernet is a simpler technology, in most models, the service provider expects self-management and with that, knowledge of IP switching fundamentals.

Cost. The flexibility and the outsourced network management that comes with an MPLS VPN means that it is usually priced at a premium, as much of the network management work is transferred to the service provider. That said, while Metro Ethernet is typically sold at a much lower price point, the customer must usually manage the infrastructure.

Qualifying Question	MPLS VPNS	Ethernet
How many locations?	Supports large number of endpoints, national reach	Supports less than 50 endpoints in metro area
What protocols are in use?	Multiprotocol	IP over Ethernet
What applications must be supported?	Supports delay-sensitive applications like voice and video	Best for applications not impacted by packet loss and latency
What connection speeds supported?	56Kbps to 1 Gbps	3 Mbps up to 10 Gbps
Are future optional services needed?	Supports services such as Remote Access, VPNs, and secure Internet connections	Supports high-speed Layer 2 data access and transfer
What security features are required?	Inherent ability to reroute around network breaches	Security features can be added based upon client needs
Management model	Management of Layer 3 routing is typically outsourced to service provider	Client manages intersite routing and transport
Budget Impact	Includes service management	Low cost, client IT provides support

Summary

Enterprises researching WAN connectivity options will invariably encounter MPLS VPNs and Ethernet. As a leading provider of managed services, CenturyLink offers solutions in both areas. In fact, many CenturyLink customers use MPLS VPN solutions for internetworking a large number of sites using remote access VPNs or secure Internet access. CenturyLink's popular Ethernet-based solutions include Private Line solutions, Virtual Private Line solutions used in a metropolitan area network, and Metro Ethernet services used to connect multiple LANs in a single metro area. Both MPLS VPN and Ethernet carrier services offer enterprises a range of technology and business benefits, but perform best when deployed in environments that closely match their capabilities. Where MPLS VPN provides a flexible platform to unify communications across an enterprise's distributed locations, Metro Ethernet is best at supporting high-throughput applications within a more limited footprint. By evaluating their needs across the appropriate range of criteria outlined in this paper, enterprises can match the networking capabilities to their business needs.

Where MPLS VPN provides a flexible platform to unify communications across an enterprise's distributed locations, Metro Ethernet is best at supporting high-throughput applications within a more limited footprint. By evaluating their needs across the appropriate range of criteria outlined in this paper, enterprises can match the networking capabilities to their business needs.

Both MPLS VPN and Ethernet carrier services offer enterprises a range of technology and business benefits, but perform best when deployed in environments that closely match their capabilities.

For more information about how to evolve your network, contact your CenturyLink representative or call 1-866-345-0814.

Or visit centurylink.com/stronger.

centurylink.com/business