



WAN and VPN Solutions:

Choosing the Best Type for Your Organization

xo.com

WAN and VPN Solutions: Choosing the Best Type for Your Organization

Introduction	1
Types of WAN Solutions	1
Distinguishing WAN Characteristics	2
MPLS IP-VPN Services	4
Ethernet Virtual Private LAN Service (VPLS)	5
Private Lines	6
Ethernet Virtual Private Line Service (EVPL)	7
Summary	8
About XO Communications	8

Introduction

In enterprises today, Wide Area Networks (WANs) are no longer operating behind the scenes. WANs are central to the daily operations and core business of organizations large and small. However, enterprises must choose from a variety of ways to implement WANs. This eBook examines the various types of Wide Area Networks (WANs), and why IT departments gravitate towards specific WAN solutions. In addition, the paper provides constructive guidelines for organizations seeking Local Area to Wide Area Network extension.

Types of WAN Solutions

Unquestionably, the two most developed designs for Wide Area Network solutions are MPLS-based IP-VPNs and Ethernet-based Virtual Private LAN Services (VPLS). Both of these solutions are network-based Virtual Private Networking (VPN) services.

Both IP-VPNs and VPLS services offer the benefits of converging VoIP, video, data and Internet over a single, interconnected, company-wide network—advantages that ATM and Frame Relay technologies could not achieve. Also, IP-VPNs and VPLS help eliminate multiple leased lines and customer equipment, which makes them far less costly than the older technologies.

Unquestionably, the two most developed designs for Wide Area Network solutions are MPLS-based IP-VPNs and Ethernet-based Virtual Private LAN Services (VPLS).

Distinguishing WAN Characteristics

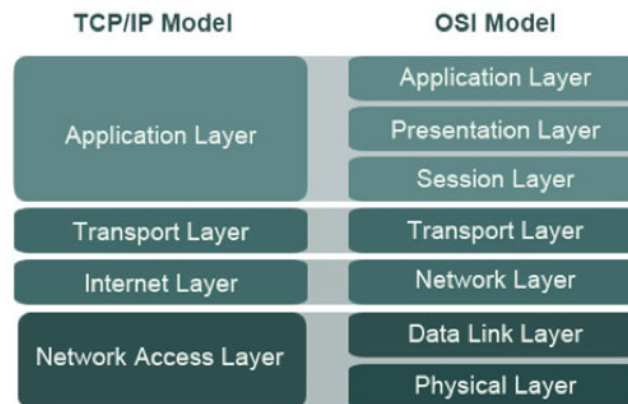
When considering WAN solutions, enterprises should understand some key characteristics about how service providers describe their offerings.

Network-Based vs. Premise-Based VPNs

In contrast to Customer Premise Equipment-based VPNs that create a private network using signaling from equipment at the customer facilities, service providers offer network-based VPNs that are delivered at the edge of the service provider's network, which is most frequently an MPLS-based nationwide network. With a network-based VPN, the service provider can create the virtual network and the customer doesn't have to buy expensive onsite equipment to set up the network.

MPLS vs. Ethernet Technologies

Both Layer 3 (IP VPN) and Layer 2 (VPLS) VPNs rely on MPLS as the underlying protocol. Both of these services have similar features and functionality, such as Class of Service. The difference between MPLS IP VPN and VPLS is that with MPLS IP VPN, traffic is routed based upon IP addresses, and with VPLS, the customers' sites are discovered by the network based on the MAC addresses associated with their routers and/or switches. In other words, the technologies are not mutually exclusive; they complement each other. And there are solid reasons why many enterprises have elements of both technologies within their total Wide Area Network.



Layer 2 vs. Layer 3 VPN

Generally, Layer 3 networks are built to run on top of Layer 2 networks. A Layer 3 network typically connects through routers that work with IP addresses at the Layer 3 (network) layer of the OSI model; whereas Layer 2 networks connect through hubs, bridges, switches or routers that work with MAC addresses at Layer 2 (data) layer of the OSI model.

With traffic on a Layer 3 network, the service provider has to view the IP addressing to route the information. This means that organizations must be willing to outsource their routing tables. Organizations in specific industries like healthcare or finance that are under rigorous scrutiny to completely protect privacy of data may not want service providers to have any access to routing. Companies in these industries largely prefer Layer 2 networks, including legacy Private Line, Frame Relay and ATM because they need to control all or parts of the network.

Conversely, there are companies who prefer Layer 3 solutions because they want the service provider not only to have access to their routing tables, but also to manage their entire WAN. These enterprises may be more interested in conserving IT resources and staff than total security for all networking.

Until recently, Layer 2 Ethernet networks would broadcast all traffic over the entire network, causing congestion. With the introduction of Layer 2 VPLS networks, however, companies gained the same capability to prioritize traffic and assign Class of Service settings that previously only existed with Layer 3 IP-VPN services. Similarly, both Layer 2 and Layer 3 networks

can have fully meshed architectures—a configuration previously only available through a Layer 3 VPN.

These distinctions are shown in the following table:

Layer 2 VPN	Layer 3 VPN
Data link layer (or Link layer in the TCP/IP Model)	Network layer (including the Internet layer of the TCP/IP Model)
Ethernet, Frame Relay, ATM	MPLS IP
Hubs, bridges, switches, routers	Routers
Multiprotocol	IP Protocol only
Service provider passes through all traffic without touching addressing tables	Service provider must have access to view routing tables to forward traffic

Ultimately, the choice of Layer 2 vs. Layer 3 VPN may come down to how much control network administrators need to maintain over the entire WAN or part of the WAN network, and whether or not the organization already has a Layer 3 network in place that will enable Layer 2 network virtualization. Enterprises considering advanced, private, integrated networking solutions usually evaluate both MPLS-based IP-VPN and Ethernet VPLS designs.

MPLS IP-VPN Services

For many multi-location businesses that use IP applications and want to interconnect very large numbers of sites, MPLS IP-VPN is the ideal choice for a corporate WAN. An MPLS IP-VPN network may also be referred to as MPLS-based VPN, Layer 3 multipoint VPNs or IP-VPNs. The solution is essentially a multi-site WAN that supports IP protocols. IP-VPNs offer scalability and reach across the enterprise, and characteristically include the performance and security aspects previously only found by buying dedicated, high-bandwidth capacity lines.

With an IP-VPN, businesses can use their existing IP network components and gain economies of scale. An MPLS IP-VPN service works well for the larger enterprise

network—for example, with hundreds of branch offices requiring broad geographic coverage. Since many enterprises find it difficult to manage routing across hundreds of sites, an MPLS-based IP-VPN service is popular because organizations can outsource network management to a service provider. MPLS IP-VPN is preferable for companies with hundreds of branches because IT departments who manage these complex networks must be knowledgeable enough to handle the limitations and details of sophisticated routing tables.

MPLS IP-VPN also can be a better choice for organizations using VoIP or applications that broadcast themselves when they come online.

Key Decision Factors for Current and Prospective Managed Network Services

- Cost
- Operational performance
- Simplified service management

Source: IDC, 2009 U.S. WAN Manager Survey

Ethernet Virtual Private LAN Service (VPLS)

With Ethernet Virtual Private LAN Service (VPLS), sometimes referred to as E-LAN or Layer 2 multipoint VPN, the service provider uses an MPLS-based network to virtually connect multiple sites using a meshed design. Ethernet VPLS uses Pseudo-Wire technology to virtually connect remote LANs into a single, bridged WAN. Since familiar and ubiquitous Ethernet interfaces connect the network, VPLS greatly simplifies LAN to WAN connectivity. With all sites appearing to be on the same Ethernet interface, every part of the user experience has the same ease and familiarity as using the local office network.

Ethernet VPLS, then, is a good choice for organizations that already have an MPLS-based network and want Ethernet at specific sites to complement an overall WAN design. Ethernet VPLS is also popular with companies that want to run their own, or another provider's, MPLS IP-VPN or Private Line network. For these reasons, Ethernet VPLS networks typically involve fewer sites and larger bandwidth needs than MPLS IP-VPN networks. VPLS works best for enterprises that need to connect high value data centers, call centers, or media centers—or need to deliver special high-bandwidth applications such as video transfer, storage area networks, and VoIP among data centers and other mission-critical areas.

With Ethernet VPLS, it is easier than with MPLS IP-VPN for IT departments to control access and networking among separate domains, special applications or departments—regardless of where

the users are located. In addition, for parts of a network that require special security, Ethernet VPLS provides complete privacy and full control of routing.

Ethernet VPLS often is an easier and less costly solution for companies to implement than an MPLS-based network because it usually doesn't need as many connections and equipment, accepts multiple protocols and doesn't require special IT expertise and training unless the company needs to connect hundreds of locations.

Since Ethernet VPLS is a newer offering than MPLS IP-VPN, many industry experts tout it as the latest WAN technology. Certainly, upcoming Metro Ethernet Forum (MEF) adoption of official E-NNI interoperability standards and Operating, Administration and Maintenance (OAM) standards could make Ethernet VPLS the preferred WAN solution for specific circumstances within the overall WAN design. Total public Ethernet revenues are projected to grow to over \$9.7 billion in 2015, at a compounded growth rate of 25 percent.¹

For all of these reasons, Ethernet VPLS is a good choice for enterprises that require a high-speed, simplified network for a smaller number of sites, when it is necessary to control routing and management. Many enterprises are in the process of replacing their older ATM and Frame Relay circuits with Ethernet VPLS services because of WAN routing control and for cost reasons.²

With Ethernet Virtual Private LAN Service (VPLS), sometimes referred to as E-LAN or Layer 2 multipoint VPN, the service provider uses an MPLS-based network to virtually connect multiple sites using a meshed design. Ethernet VPLS uses Pseudo-Wire technology to virtually connect remote LANs into a single, bridged Wide Area Network.

¹ Insight Corporation, Carriers and Ethernet Services: 2010-2015

² WAN News, 11/25/2009, SearchEnterpriseWAN.com

Private Lines

With dedicated Private Line as well as Ethernet Private Line services, enterprises benefit from high-speed, full-duplex, point-to-point connections. Bandwidth capacity is solely dedicated to the customer's use 24/7, which is the reason why enterprises select Private Lines to send extremely time-sensitive or mission-critical communications with top speeds and reliability. Enterprises often use Private Line services to securely transport data; Internet; live streaming video, television or movies; or to support bulk transfer of data among storage access networks or data centers. Distance learning, medical imaging, financial transactions and engineering are all examples of industry applications ideal for Private Line transport.

Among the advantages of Private Line services are security, resiliency, high-speed connectivity and low latency (delay). With Private Lines, companies can rapidly send large volumes of data across a single connection without the need of a local "loop"—and at significantly lower costs per megabyte than older technologies. Private Line circuits are good when you need to connect two sites, but can get costly if you need to connect multiple locations. Pricing for Private Lines also can be geographically sensitive, creating a drawback for businesses with locations in some areas.

With dedicated Private Line as well as Ethernet Private Line services, enterprises benefit from high-speed, full-duplex, point-to-point connections.

Ethernet Virtual Private Line Service (EVPL)

An EVPL service is similar to a Private Line service, in that the network transports traffic in real-time over a dedicated connection. However, the connection is virtual, using Pseudo-Wire technology, to transmit Layer 2 protocols usually over an MPLS-based IP network.

This type of connection works by creating the connection using virtual tunnels across the packet network. One of the advantages of the EVPL is that it may be less expensive than a point-to-point Private Line.

With an EVPL service, multi-location businesses can simplify data traffic to and from smaller locations and a central location or data center using a single interconnection. This Layer 2 point-to-multipoint configuration provides one physical connection to equipment that, in turn, fans out to

Virtual Ethernet Local Area Network (VLAN) or multiplexed sites. Instead of having to buy “last-mile” access from many local phone companies to connect locations to a network, the enterprise buys one or two large Hub connections at very high-speeds and these connections extend to virtual connections with other sites. In this way, an EVPL uses an MPLS-based network to virtually connect smaller branch locations.

EVPL lowers networking costs for enterprises by simplifying the network with fewer, higher-capacity interconnections between the primary data centers and the network, or among HQ and branches. Another one of the key advantages of an EVPL service is that it allows organizations to maintain separation of traffic as it converges over a single connection.

This type of connection works by creating the connection using virtual tunnels across the packet network. One of the advantages of the EVPL is that it may be less expensive than a point-to-point Private Line.

Summary

Currently, most enterprise WAN are comprised of hybrid solutions that combine some aspects of more than one network-based VPN service and point-to-point Private Line services. Organizations often consult with service providers to custom build the WAN that best meets the myriad of special requirements that confront IT WAN managers. These requirements may be based on multiple and sometimes conflicting objectives for the WAN and may include user access needs, location access needs, reliability, scalability, ease of management and cost savings. What's

more, network-based VPN solutions with Quality of Service guarantees are preferable.

Network administrators should carefully consider the cost-saving benefits of consolidating services with a single provider, thereby eliminating duplicative lines and equipment and making it easier to move, add or delete sites. The WAN solution should support existing and planned equipment and infrastructure technologies, and in this way, support multiprotocol and access agnostic connectivity.

About XO Communications

XO Communications is a leading nationwide provider of advanced communications services and solutions for businesses, enterprises, government, carriers and service providers.

XO customers include more than half of the Fortune 500, in addition to leading cable companies, carriers, content providers and mobile network operators. Utilizing its unique combination of high-capacity nationwide and metro networks and fixed wireless capabilities, XO offers customers a broad range of managed voice, data and IP services with proven performance, scalability and value in more than 85 metropolitan markets across the United States.

For more information, call your XO sales representative, visit www.xo.com or call: 800.474.1703

For XO updates, follow us on:

[Twitter](#) | [Facebook](#) | [LinkedIn](#) | [Slideshare](#) | [YouTube](#) | [Flickr](#)