A Business Guide to MPLS IP VPN Migration:
Five Critical Factors
A Business Guide to MPLS IP VPN Migration: Five Critical Factors

Contents

Abstract 3
Introduction 4
The Evolving Needs of Today’s Enterprise Network 5
How MPLS Works 6
Factor 1: Understanding Your Business Goals 7
Factor 2: Defining Your Network Needs 9
Factor 3: Choosing Your Migration Path 10
Factor 4: Assessing the TCO of your Migration Solution 12
Factor 5: Selecting a MPLS IP VPN Services Provider 13
Conclusion 15
Appendix A: XO MPLS IP-VPN: Converged Voice, Data, and Video Solution with Class of Service Routing 16
Appendix B: XO MPLS IP-VPN Secure, Scalable, Redundant Solution for Multi-site Networks 17
Appendix C: XO MPLS IP-VPN Supports a Wide Range of Integrated VoIP Service Offerings 18
Abstract

This paper outlines five critical factors for successful migration to an MPLS IP VPN service. Written for business executives and IT decision makers, the paper discusses the current status of MPLS IP VPN adoption for the medium-to-large business (5 to 50 locations), especially with regard to the evolving (and expanding) role of MPLS technology. The paper also identifies key questions you should ask before migrating from a legacy infrastructure to an MPLS-enabled IP VPN, discusses the benefits of migration, describes the types of companies that would benefit from MPLS IP VPNs, and suggests what a business should look for in an MPLS provider. The good news is that the early adopters of the technology have implemented MPLS with great success, particularly as it relates to network performance.

Trends in the MPLS/IP VPN Services Market

- Traditional TDM services continue to dominate the access space, but alternative access technologies such as Ethernet and 3G wireless are gradually gaining traction

- Integration of video applications such as TelePresence is expected to drive spending on MPLS VPN services

- Layer 2 Ethernet-based VPNs (VPLS) are complementing layer 3 MPLS VPNs

- Hybrid networks are seeing growth even as VPLS gains traction

- Ability to support multicast is fast emerging as a key competitive differentiator

Introduction

With the emergence of converged IP services, all businesses are demanding greater performance from their enterprise networks than ever before, including support for media-rich applications. Medium-to-large businesses with five to 50 sites throughout the United States tell us they understand the urgent need to evolve enterprise networks and control the power of today’s information technology, but many lack the tools and budgets to do so. For these businesses, MPLS-based private IP networks, or MPLS IP VPNs, have been hailed as an ideal choice for the corporate WAN, ideal for multi-location businesses that use IP applications and want to interconnect very large numbers of sites.

Multi-Protocol Label Switching (MPLS) Internet Protocol (IP) Virtual Private Network (VPN), or MPLS IP VPN, refers to a VPN service enabled over a trusted provider’s private MPLS core backbone. It delivers the flexibility of an IP service with the essential service quality, performance and security previously available only with legacy technologies (dedicated, high bandwidth capacity lines). Other benefits include cost-effective security, any-to-any connectivity, Quality of Service (QoS), scalable bandwidth, and a platform for convergence – one that eliminates network redundancies and supports enterprise VoIP.

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. 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 applications that broadcast themselves when they come online—or VoIP.

Voice over Internet Protocol (VoIP), which uses the same communications protocol to carry voice traffic that the Internet uses to carry data traffic, is the key driver for network convergence. With MPLS IP VPN, not only are multiple networks (voice, data, and video) assimilated on one IP platform, but the converged voice and data network is also easier to maintain than two or three separate legacy networks.
The Evolving Needs of Today’s Enterprise Network

Many enterprises today have already migrated to newer technologies such as MPLS or Enterprise Ethernet from one or more of three legacy technologies--dedicated Private Line, Frame Relay, or ATM. Transport is becoming increasingly less expensive, and businesses want to take advantage of the benefits offered by convergence. Some of the criteria for today’s enterprise network, and how newer technologies are positioned against their legacy counterparts to support those requirements, are shown in Table 1.

Table 1. Today’s Enterprise Requirements and Legacy versus Newer Technologies

<table>
<thead>
<tr>
<th>Requirements</th>
<th>Legacy technologies (Private Line, Frame Relay, ATM)</th>
<th>MPLS IP VPNs</th>
</tr>
</thead>
</table>
| Performance & bandwidth       | • Some level of congestion during times of peak usage - varies from time-to-time and frame-to-frame, resulting in unpredictable and variable-length latency  
  • ‘Cell tax’—the high percentage of gross payload volume reserved for the network (typically at least 10% in ATM networks) | • MPLS supports QoS, so priority applications, and those intolerant of delay (like VoIP) have priority over all other traffic during times of peak usage. |
| Cost-efficiency               | • Separate networks required for voice and video  
  • To make a Frame Relay network fully meshed requires the addition of Permanent Virtual Circuits (PVCs), as PVCs are added, the cost goes up dramatically | • Single converged network supports all traffic  
  • Eliminates the need for PVCs—less cost and administration, and cost remains constant  
  • Because VoIP and data applications run over the same circuits, offers better use of existing bandwidth  
  • Any-to-any, fully meshed topology is flexible and scalable  
  • More bandwidth for the dollar. |
| IP support                    | • Unable to support Internet Protocol, cannot operate over one network standard (IP)                                  | • Supports IP, businesses gain major dividends from converged voice and data solution over one network standard |
| Flexibility and Scalability   | • Somewhat bandwidth limited  
  • Cannot scale bandwidth for additional capacity to meet new business needs  
  • Does not adapt easily to accommodate growing business needs  
  • Requires ordering, provisioning, managing point-to-point circuits or virtual circuits when adding locations or altering the flow of communication between locations | • Can add/alter traffic flow without ordering, provisioning, managing circuits  
  • Scales bandwidth to add capacity for meeting increased traffic requirements of media-rich applications |
How MPLS Works

Traditional IP packet routing

In most standard packet networks including traditional IP, packets are routed according to information contained in the header of each packet. As the packets make their way across the network, they are examined by each switch/router they pass through to determine how to handle it in terms of Quality of Service (QoS) and outbound routing. In many cases, each packet is encrypted before it enters the network to ensure confidentiality (Figure 1).

Each router performs all the handling functions—checking for errors, verifying address, repackaging, re-transmitting, and so on. These necessary functions result in robust network architecture, but they take time. For delay-sensitive traffic like VoIP and video conferencing, delays are unacceptable.

MPLS packet routing

MPLS makes this process faster by using another method to route and prioritize traffic. In an MPLS network, packets are given labels that identify their priority individually and relative to other packets. With this unique prioritization scheme, traffic delivered over an IP-based MPLS network demonstrates QoS levels that are identical to those previously available only on Frame Relay, ATM, and Private Line networks (Figure 2).

MPLS offers the best of both a Layer 2 and a Layer 3 network—relying on the robustness of a fully meshed network and the survivability and efficiency of a routed Layer 3 network. MPLS does a good job managing the network and the traffic that traverses it because it performs two tasks well: prioritizing traffic based on header information, and shaping traffic according to its knowledge of network topology and current load. (Shaping is the process of spreading traffic across all paths in the network to guarantee optimal traffic handling by the resources available within the network.)

Figure 1. Traditional IP Network

Packets are checked by each router along their paths to determine their priority and destination.

Figure 2. MPLS-enabled IP Network

Packets contain labels that identify their priority and destination, and quickly route to their destination without multiple checkpoints, which enhances traffic speed.
Factor 1: Understanding Your Business Goals

MPLS IP VPN is the ultimate in WAN connectivity. Are its benefits aligned with your enterprise needs?

A move to MPLS IP VPN requires a financial and operational commitment from the enterprise in order to be successful. Establishing clear business goals can help secure funding and continued support from the enterprise, and keep the project on track in terms of time and resources. Examples of some typical business goals behind a switch to MPLS IP VPN from a legacy network are given below.

Reduce costs associated with separate networks for voice, video and data: Reducing costs is often a primary goal behind network consolidation projects. MPLS IP VPN can reduce network total cost of ownership (TCO)—including costs such as acquisition, monthly recurring charges, and annual maintenance fees—by converging voice, video and data from multiple networks onto a single platform. It also decreases costs for enterprises with multiple, regionally dispersed sites that require a fully meshed network. In fact, as the degree of meshing increases, the TCO for MPLS IP VPN decreases dramatically when compared with a Frame Relay network (Figure 3). Last, the extraordinary scalability of an MPLS network enables an enterprise to deliver all the communication capacity for high-bandwidth applications (like data storage or video) without provisioning bandwidth.

Re-deploy IT resources to more critical tasks: An excellent ability to self-configure eliminates the need for circuit mapping, capacity planning, and monitoring of multiple point-to-point connections. It also simplifies billing, customer premises equipment (CPE) support, vendor management, network management, and operations functions, resulting in the ability to re-deploy some of those IT resources to other tasks within the enterprise. The remaining functions can then be handled internally or, as many companies are now doing, outsourced to a provider of managed services.

Improve network performance: IP-dependent MPLS offers QoS over IP – the best possible combination for QoS-dependent enterprise networking. An MPLS-enabled IP network provides built-in security with dedicated IP edge routers isolated from the public Internet and provides superior routing performance while adhering to stringent SLAs. MPLS delivers defensible QoS supported by SLAs that address such issues as jitter, service availability, round-trip delay, packet loss, and QoS.

Increase performance of mission-critical applications: MPLS uses Class of Service (CoS) tags on packets to ensure that VPN customers have priority throughout their network and that each application gets the quality of service it needs. The ability to control how classes of data move on the network gives MPLS-enabled IP VPNs a performance edge over traditional IP VPNs.
Improve network security: MPLS provides a private, segregated VPNs for each customer, with dedicated IP VPN provider edge routers isolated from the public Internet, plus secure Internet access options.

Provide a platform for the future: MPLS supports an array of emerging IP-enabled applications that must be supported across enterprise networks, fixed and mobile devices, and location types.

Table 2. Profiles of Typical Businesses Choosing MPLS IP VPN

MPLS IP VPN is particularly suited for certain business types, as shown below.

<table>
<thead>
<tr>
<th>Typical Profiles of Businesses Adopting MPLS IP VPN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Business characteristic</strong></td>
</tr>
<tr>
<td>Decentralized, regionally dispersed</td>
</tr>
</tbody>
</table>
| Large number of leased lines | • Easier management  
 | | • Cost savings from bandwidth consolidation |
| Multiple traffic streams | • Companies with data, voice, video conferencing, and business applications are likely to see the merits of an MPLS IP VPN.  
 | | • Inherent traffic separation  
 | | • QoS  
 | | • Traffic stream prioritization  
 | | • Security |
| Undertaking mergers or ‘organizational change’ | • Scalability  
 | | • Flexibility |
| Holding group | • Secure segregation of traffic  
 | | • Economies of scale through centralized buying and consolidation |
| Small, growing | • Scalability  
 | | • Frees up scarce resources  
 | | • Immediate cost savings  
 | | • Ability to add applications over one network solution |
Factor 2: Defining Your Network Needs

Different providers have different strengths. Assess your network needs first. Does the provider meet your bottom line requirements?

Specific network capabilities, including Quality of Service (QoS), availability, flexibility and security can vary among service providers—be sure to take these into consideration. You will need to examine your own current network operation, and determine the type of capabilities you will need. A service provider should be able to help. Some use a ‘discovery questionnaire’ to identify the functions performed at each of your locations, survey your current telecom environment, and ask about your growth plan and future network requirements. Following are some examples of network needs:

- **Quality of Service (QoS) backed by SLAs**: SLAs for QoS parameters typically include measures of uptime, mean time between failures, degree of survivability, repair response time, latency (delay), jitter, and packet delivery.

- **End-to-end service quality**: As bandwidth-hungry voice and video conference traffic spills over to another traffic class, circuits can be overloaded and network performance deteriorates. Class of service (a tag applied to each packet indicating level of priority must be monitored at the application level so that network managers have visibility into application-specific traffic performance. Service providers may offer tools to help.

- **Availability**: A subjective measure of network performance typically negotiated by the buyer and seller of network services. Most commonly defined as a percentage of uptime in a given period of time, like the ‘five nines of reliability’ (99.999% availability).

- **Flexibility**: A measure of network flexibility related to survivability and customer service. One measure is the degree to which a network can self-configure during facility failure to avoid disruption of service. A fully meshed architecture lends itself to this because in the event of failure of the primary route, traffic can be instantly and automatically rerouted to ensure service continuity. Another measure is how much the network can adapt to the disparate traffic types.

- **Security**: Privacy, confidentiality, and non-repudiation are critical today. In VPN environments, private traffic is routed across public infrastructures with absolute confidence, and the need to guarantee this level of information security continues to be critical.
Factor 3: Choosing Your Migration Path

When migrating from legacy technologies, there are options. What plan will work best for you?

Staying with what you have: The legacy Layer 2 VPN

Initially, virtual network services were delivered over Layer 2 networks (Frame Relay and ATM), using full-duplex virtual circuits established through a traditional call setup signaling process. These Layer 2 VPN networks are typically organized around a physically centralized, hub-and-spoke architecture (Figure 3). While this architecture has its limitations, it also has advantages. Because these networks are based on dedicated resources, they are secure and predictable. And while they aren’t based on IP, which is a Layer 3 IP protocol, a very high percentage of the traffic transported over them (more than 75%) are IP packets. Therefore, these hub-and-spoke designs can form the basis for a very effective transition strategy to MPLS-enabled IP VPNs, since they are already transporting IP packets and offer a high degree of performance.

However, Layer 2 VPNs, while effective, are connection-oriented and therefore costly and inflexible. Also, because communication must transit a hub, it takes longer to transmit, creating delays and bottlenecks. Also, hub failure can affect multiple sites. By extension, the only way a Layer 2 network can have the many-to-many flexibility of a Layer 3 (IP) network is if it is fully meshed; that is, the network architecture is such that every node in the network has a connection to every other node in the network.

The fully-meshed Layer 2 VPN

In a situation where a meshed network is already in place (Figure 4), MPLS can be implemented directly over it, taking advantage of the survivable Layer 2 architecture as a foundation for the robust Layer 3 capabilities enabled by MPLS. In this case, communication bypasses the hub, avoiding bottlenecks. Expensive Layer 2 switches become far more capable Layer 3 routers. VPNs are implemented through these routers.

While this scenario may be a feasible migration path for some large enterprises with special needs and security concerns, enabling a fully-meshed Layer 2 VPN architecture is infeasible for most medium-to-large enterprises.

The Layer 3 MPLS IP VPN

Choosing an MPLS IP VPN service allows a business to minimize personnel and capital in managing the enterprise WAN, and leverage the expertise of a service provider (Figure 5). The most commonly outsourced functions include some aspects of design, installation, and ongoing management (such as VPN installation and testing, router management and monitoring, security management, VPN design, and VPN product selection).
VPN Migration Paths

Figure 3. Layer 2 Hub-and-Spoke VPN Architecture

Critical, costly resources are focused in the center of the network (yellow circle). All edge devices have access to them on a shared basis. Costs are controlled by limiting the number of point-to-point connections between edge devices. However, communication (blue dotted lines) must transit through the hub, creating delays and bottlenecks.

Figure 4. Fully Meshed Layer 2 VPN Architecture

The hub (yellow circle) and surrounding “spoke” devices are connected in a fully meshed topology. Communication between sites (blue dotted line) now bypasses the hub, avoiding bottlenecks. However, establishing multiple point-to-point connections significantly increases operating and maintenance costs.

Figure 5. Layer 3 MPLS IP VPN Architecture

A service provider can offer a fully managed MPLS IP VPN with end-to-end network management and monitoring. Only one link per site to the service provider’s network is needed to provision applications enterprise-wide.
Factor 4: Assessing the TCO of your Migration Solution

Your network costs now—and in the future

To establish a foundation for making sound financial decisions regarding migration, it is important to assess the total cost of ownership (TCO) of the solution. Consider capital expenditures, operating expenses, and opportunity costs over a period of time—beyond the initial deployment.

- **Capital Costs**: The ability to consolidate disparate network operations within an organization naturally leads to cost reductions through the more efficient use of existing equipment, property, and facilities. Companies that decide to migrate to an MPLS IP VPN find that accessing a service provider’s lower cost structure results in a greater economy of scale, and this is one of the most compelling reasons for outsourcing. A service provider can also charge less than a business would otherwise spend for operations, maintenance, service, equipment, and technology upgrades.

- **Operating Costs**: Companies that migrate to an MPLS IP VPN not only reduce their capital costs, they make recurring costs more predictable by shifting from a variable cost to a fixed-cost model. Businesses will know their monthly costs in advance, as compared to businesses that need to find the budget for unexpected expenses related to network hardware, software and service upgrades, and maintenance. The good news is that for multi-location businesses that require T1 or higher services, an MPLS IP VPN is actually a cost-cutting measure that frees IT resources to concentrate on the core objectives of the business.

- **Opportunity Costs**: Though sometimes difficult to quantify, opportunity costs may include lost enterprise revenue and lower productivity, often the result of network downtime or the inability to deploy new services and locations. Service providers have the resources to offer 24-hour monitoring, management, and support—capabilities not readily available in-house to any but the largest enterprises. Service providers also can offer rapid deployment of applications and services because of their deployment experience. Even for companies with large in-house staffs, service providers can fill critical resource gaps, which typically require special training and expertise.

As more PVCs are added to a Frame Relay network to make it fully meshed, the cost goes up dramatically. For MPLS IP VPN, the cost remains constant.

Factor 5: Selecting a MPLS IP VPN Services Provider

What can a service provider do for you?

MPLS eliminates the need for circuit mapping, capacity planning, and monitoring of multiple point-to-point connections. It also simplifies billing, customer premises equipment (CPE) support, vendor management, network management, and operations functions, so some of those IT resources can be re-deployed to other tasks within the firm. The remaining functions can then be handled internally or outsourced to a provider of managed services.

By outsourcing all or some of the migration a business can more fully realize the benefits of its MPLS-based network. Outsourcing enables a business to minimize personnel and capital in managing the enterprise WAN, while leveraging the expertise of the service provider. The most commonly outsourced functions include some aspects of design, installation, and ongoing management (such as VPN design, product selection, installation, and testing; router management and monitoring; and security management).

When selecting a provider, verify that its network supports the business strategy that drove you to migrate to MPLS in the first place. While very few providers will excel in every category, consider those that will support your highest priorities now and in the foreseeable future.
**Table 3. Service Provider Selection Criteria Checklist**

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Questions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Options</td>
<td>Does the provider offer an array of access speeds and technology options (remote access, T1/DS3, Ethernet, fiber, and higher speed optical interfaces) to support site connectivity, legacy networks, and scalability needs?</td>
</tr>
<tr>
<td>Voice/Data Convergence</td>
<td>Does the provider offer a range of VoIP options that will enable an end-to-end VoIP solution that connects all of your company sites?</td>
</tr>
<tr>
<td>Performance Measurement</td>
<td>How does the company measure network performance? Are those measures available to the enterprise? If so, how? What are the key performance thresholds that the provider uses as service delivery triggers?</td>
</tr>
<tr>
<td>Service and Support</td>
<td>Is the service provider capable of managing end-to-end QoS and network security, even when the circuit traverses other providers' networks?</td>
</tr>
<tr>
<td>Service Level Agreement</td>
<td>Are there Class of Service SLAs that prioritize application traffic differently? Does the SLA address remuneration for service outages? What are the terms for response to a network problem or failure?</td>
</tr>
<tr>
<td>Universal Connectivity</td>
<td>Does the service provider have agreements with other providers to ensure universal connectivity, even in areas where the provider lacks a presence?</td>
</tr>
<tr>
<td>Security</td>
<td>How robust is the service provider’s network security? MPLS is a highly secure infrastructure, but even the best networks have vulnerabilities. Is Internet access provided across the same core infrastructure as access to the VPN, or is it done over a separate infrastructure? For multi-site networks, find a service provider with a private, MPLS-enabled IP backbone, thereby segregating your data from other customers and the public Internet.</td>
</tr>
<tr>
<td>Redundancy</td>
<td>Does the service provider offer some level of Business Continuity support? Look for redundant service offerings that may include both wireless and non-wireless links, collocation, back-up power, customized design, and 24/7 technical support.</td>
</tr>
<tr>
<td>Managing VPNs</td>
<td>Does the service provider configure, deploy, and manage CPE at each of your network sites? Some MPLS service providers will simplify network management this way. Are Web-based reporting and monitoring tools available?</td>
</tr>
</tbody>
</table>
Conclusion

What Every Enterprise Should Know

MPLS is enjoying success as a viable solution for multi-site enterprise connectivity. The majority in the industry that are implementing VoIP, expanding their reliance on VoIP, or improving their QoS ratings are also implementing MPLS as part of their strategy to do so. Because IP has also ascended to a level of prominence in large, QoS-dependent enterprise networks, and because it is beginning to demonstrate its ability to support the promise of convergence, MPLS emerges as an ideal access and transport solution. It offers the same level of service as legacy Layer 2 technologies, but at a much lower cost and with much greater flexibility.

Is Your Enterprise Ready to Migrate to MPLS?

The time to consider converting to an MPLS solution has arrived. Before doing so, however, be sure that the decision to convert is based on: (1) your business goals, (2) an understanding of your network needs, (3) a strategic migration path, (4) the TCO of your migration solution and (5) a service provider with a network, features and capabilities that supports your business strategy. The end result will be a secure, flexible, cost-effective network with near-infinite scalability that will meet your enterprise needs for a very long time.

What’s Next?

Solution providers, such as XO Communications, offer a suite of MPLS migration tools, people, and processes to assume management of your networking environment should your enterprise not have the resources to design and operate an MPLS-based network. For more information on XO MPLS IP-VPN service and how XO can help you migrate to MPLS, please visit: http://www.xo.com/services/network/mpls-ipvpn/Pages/overview.aspx.
APPENDIX A: XO MPLS IP-VPN: Converged Voice, Data, and Video Solution with Class of Service Routing

XO MPLS provides performance and flexibility with Class of Service routing and traffic prioritization, ensuring that critical applications get the quality of service they need.
XO-managed MPLS supports financial services company with robust disaster recovery, redundancy, scalable access speeds (from DS-1 to Gigabit Ethernet), and XO-managed solutions without requiring major capital outlay for a new network.
APPENDIX C: XO MPLS IP-VPN Supports a Wide Range of Integrated VoIP Service Offerings

Fig. C: From legacy key systems to IP PBX systems, XO can design a flexible, fully managed solution to meet your network migration needs.

EXAMPLES PRESENTED FOR DEMONSTRATION PURPOSES
About XO Communications

XO Communications is a leading nationwide provider of advanced broadband communications services and solutions for businesses, enterprises, government, carriers and service providers. Its 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 broadband wireless capabilities, XO Communications 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, visit www.xo.com.

For more information on XO MPLS IP-VPN, please visit: http://www.xo.com/services/network/mpls-ipvpn/Pages/overview.aspx.

For XO updates, follow us on: Twitter | Facebook | Linkedin | SlideShare | YouTube | Flickr