

White Paper

MPLS IP VPNs: Are You Ready to Migrate?

Five Critical Factors for the
Medium-to-Large Business

Written by Steven Shepard,
President, Shepard
Communications Group, LLC

Commissioned by
XO Communications

Table of Contents

ABSTRACT1
INTRODUCTION1
Limitations of Legacy Networks1
How MPLS Enhances IP Networks2
Five Critical Factors for Migration4
FACTOR 1: YOUR BUSINESS GOALS4
Reduce Costs4
Lower Risk5
Increase Productivity5
FACTOR 2: YOUR NETWORK CAPABILITIES5
Requirements for Migration5
The Next-Generation Network6
FACTOR 3: YOUR MIGRATION PATH8
Why Migrate to MPLS?8
Perceived Barriers to Migration9
Migration Profiles9
FACTOR 4: YOUR OPERATING BUDGET10
Capital Costs10
Operating Costs10
Opportunity Costs11
FACTOR 5: YOUR MPLS SERVICE PROVIDER11
Service Provider Selection Criteria & Checklist11
CONCLUSION12
What Every Enterprise Should Know12
Is Your Enterprise Ready to Migrate to MPLS?12
Where to Begin12
APPENDIX13-15

MPLS IP VPNs: Are You Ready to Migrate?

Five Critical Factors for Medium-to-Large Businesses

by Steven Shepard, President
Shepard Communications Group, LLC

Abstract

This paper outlines five critical factors for successful migration to MultiProtocol Label Switching (MPLS) Internet Protocol (IP) Virtual Private Networks (VPNs). 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. The time has come for mass migration to the technology

Introduction

With the emergence of converged IP services, medium-to-large businesses are demanding greater performance from their enterprise networks than ever before. To meet the evolving needs of these five to 50-site companies and their media-rich applications, enterprise networks are challenged to evolve in lockstep with those demands. CIOs and IT Managers throughout the U.S. tell us they understand the *urgent need to evolve their enterprise networks* and control the power of today's information technology, but many lack the tools and budgets to do so.

The good news is that there is a solution for today's enterprise networks: *MultiProtocol Label Switching* (MPLS) technology. MPLS has now reached a level of maturity in the market that positions it favorably against legacy technologies. Based fundamentally on Internet Protocol (IP), MPLS technology delivers the extraordinary flexibility of an IP service with the essential service quality previously available only with legacy technologies.

For businesses with multiple locations, MPLS-enabled IP VPN is an ideal solution for enterprise connectivity. It offers cost-effective security, any-to-any connectivity, quality of service, scalable bandwidth, and a platform for convergence – one that eliminates network redundancies and supports enterprise Voice over Internet Protocol (VoIP).

In fact, VoIP is the key driver for network convergence. VoIP uses the same communications protocol to carry voice traffic that the Internet uses to carry data traffic. 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.

Limitations of Legacy Networks

Most enterprise networks today rely on one or more of three legacy technologies: *dedicated Private Line, Frame Relay, or Asynchronous Transfer Mode (ATM)*. Increasingly, though, the limitations of these technologies are beginning to appear, particularly as the demand for a more *dynamic and flexible* architecture emerges. For example:

“For businesses with multiple locations, MPLS-enabled IP VPN is an ideal solution for enterprise connectivity. It offers cost-effective security, any-to-any connectivity, quality of service, scalable bandwidth, and a platform for convergence.”

“Today’s savvy business owners and CIOs are turning to service providers for help when migrating their legacy networks to MPLS IP VPNs, seizing the full potential of MPLS technology.”

- **Limited Bandwidth** – In spite of their service history, Private Line, Frame Relay, and ATM are somewhat bandwidth limited. With Frame Relay, for instance, some level of congestion is ensured during times of peak usage. The level of congestion varies from time-to-time and frame-to-frame, resulting in latency (delay), which is unpredictable and variable in length.
- **Cell Tax** – Frame Relay and ATM suffer from what is known throughout the industry as “cell tax,” which is the high percentage of the gross payload volume that is reserved for the network. Because the tax can be high (typically a minimum of roughly 10% in ATM networks), throughput suffers. Private Line, while not burdened by cell tax, is still costly and inflexible.
- **Inability to Support Internet Protocol** – The use of Private Line, Frame Relay, and ATM precludes businesses from gaining the major dividends from a converged voice and data solution operating over one network standard, Internet Protocol.
- **Insufficient Flexibility and Scalability** – Private Line, Frame Relay, and ATM can’t adapt as easily to accommodate growing business needs (e.g., when adding locations or altering the flow of communication between locations) without the hassle of ordering, provisioning, and managing point-to-point circuits or virtual circuits. Neither can they scale bandwidth when you need additional capacity to meet increased traffic requirements of media-rich applications.
- **Not Cost Effective** – While legacy technologies like Private Line, Frame Relay, and ATM do precisely what they were designed to do, they are not as functionally efficient or as cost effective as more modern technologies like MPLS and enterprise Ethernet. And Frame Relay’s inherent inefficiency for supporting voice and video traffic has required enterprises to incur the costs of separate voice and video networks. *As transport becomes less and less expensive, businesses will seek the most cost-effective solution available.*

The bottom line? Private Line, Frame Relay, and ATM are expensive, inefficient, and largely incapable of adapting to the rigorous demands of the media-rich payloads that are appearing on enterprise networks today. Consequently, today’s savvy business owners and CIOs are turning to service providers for help when migrating their legacy networks to MPLS IP VPNs, seizing the full potential of MPLS technology.

How MPLS Enhances IP Networks

Because IP seems to be the “anointed protocol” for dominance of future networks, it is important to understand how it works, particularly with MPLS. In traditional IP networks (in fact, in most standard packet networks), 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 the packet should be handled 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. See **Figure 1**.

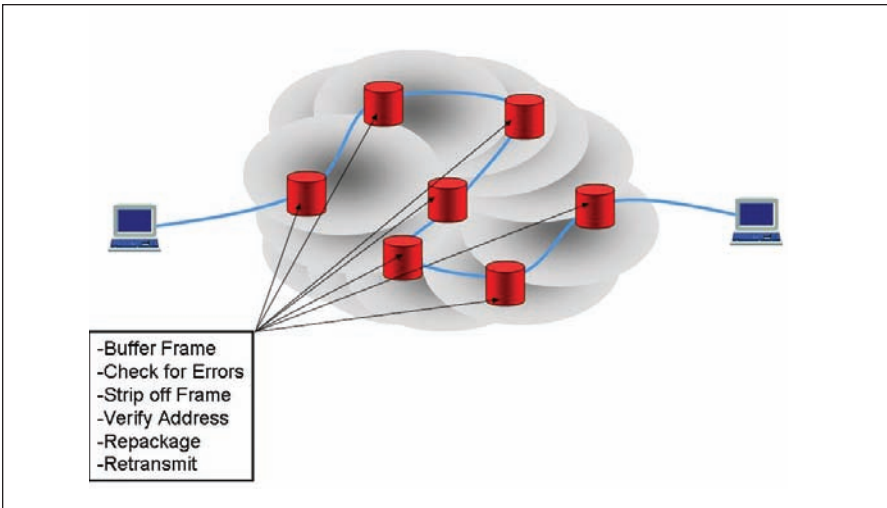


Figure 1: Traditional IP Network

Each router performs all the functions shown in the box at left. This results in robust network architecture, but because of the need to buffer and examine each packet as it arrives, it is not as efficient as it could be.

All of these functions (e.g., checking for errors, verifying address, repackaging, re-transmitting), while necessary, take time to perform and introduce delay into the equation – an unacceptable fact for delay-sensitive applications like voice and video, both of which are becoming major elements in enterprise IP networks. MPLS eliminates this problem, as **Figure 2** illustrates.

As packets are created for transport in an MPLS network, they are given a “label” that identifies not only the priority of the payload they contain, but also the relative priority of each packet as well. By relying on 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.

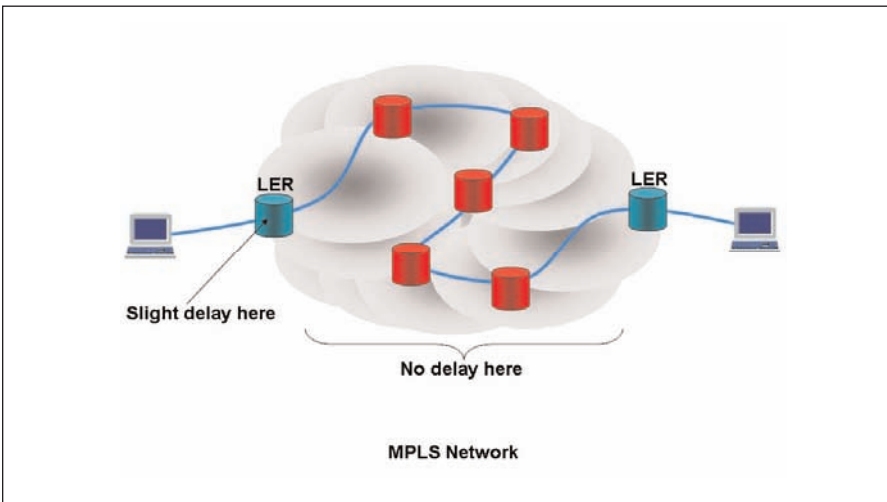


Figure 2: MPLS-enabled IP Network

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.

In essence, MPLS works because it performs two tasks very well: It *prioritizes* traffic based on header information, and it *shapes* the traffic according to its knowledge of network topology and current load (Shaping is simply the process of spreading traffic across all paths in the network to guarantee optimal traffic handling by the resources available within the network). MPLS *doesn't perform network magic; it simply manages the network and the traffic that traverses it very well.*

“MPLS works because it performs two tasks very well: It prioritizes traffic based on header information, and it shapes the traffic according to its knowledge of network topology and current load.”

Five Critical Factors for Migration

This paper outlines five critical factors to consider when determining if you are ready to migrate your enterprise network to an MPLS IP VPN. These factors include:

- Your Business Goals
- Your Network Capabilities
- Your Migration Path
- Your Operating Budget
- Your MPLS Service Provider

Factor 1: Your Business Goals

Before making the leap to MPLS, the main question to ask yourself is this: *What are the fundamental reasons why you are considering a migration to MPLS in the first place?* There should be tangible business advantages that result from the MPLS migration. For example:

Reduce Costs

Consolidating disparate systems, circuits, and equipment into a single platform helps reduce operating expenditures by eliminating redundancies and costs required to maintain multiple systems. Moreover, the extraordinary scalability of an MPLS network enables an enterprise to deliver all the communication capacity needed for high-bandwidth applications (e.g., data storage or video), without having to provision more bandwidth than required at any moment.

In addition, converging multiple networks helps reduce Total Cost of Ownership (TCO) – the primary goal and driver of many network consolidation projects. When analyzing Total Cost of Ownership (TCO) for MPLS IP VPN (e.g., acquisition costs, monthly recurring costs, annual maintenance costs), the cost is significantly less than Frame Relay networks¹ as the degree of meshing increases, as shown in **Figure 3**.

“The extraordinary scalability of an MPLS network enables an enterprise to deliver all the communication capacity needed for high-bandwidth applications (e.g., data storage or video), without having to provision more bandwidth than required at any moment.”

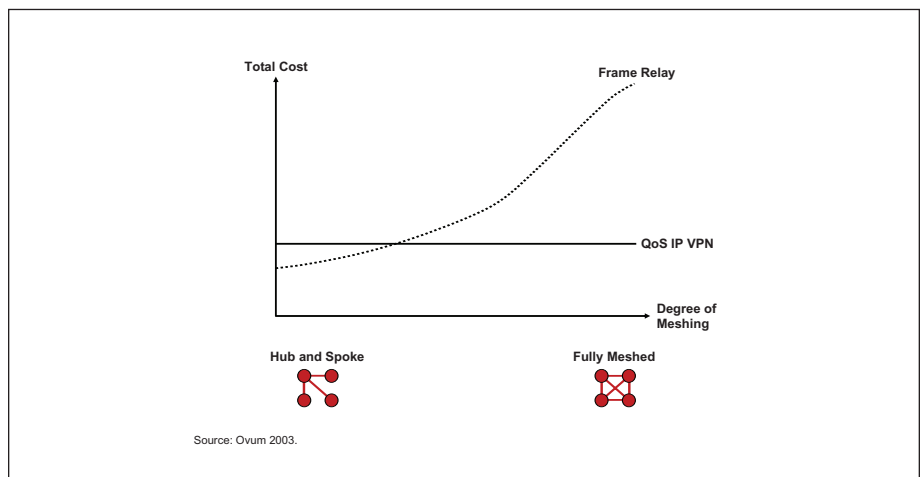


Figure 3: Total Cost for Frame Relay vs. MPLS IP VPN

As more Permanent Virtual Circuits (PVCs) are added to a Frame Relay network to make it fully meshed, the cost goes up dramatically; whereas, with an MPLS IP VPN, the cost remains constant.

¹ Ovum 2003, “Frame Relay versus QoS IP VPN Costs,” reprinted in “From Frame Relay to VPN: Why to Migrate, Why to Out-task to a Service Provider” white paper by Cisco Systems, 2005, p. 6.

Lower Risk

When IP first found its way into the enterprise, it was lauded for its “technological courage” in the sense that it brought a degree of network flexibility that previously had never been experienced in network environments. However, it also brought a connectionless legacy of best-effort service, which hampered its desire to be taken seriously by enterprise networks and IT organizations. That, however, has radically changed.

Today, 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 Service Level Agreements (SLAs). For all these reasons, MPLS has become a widely acceptable technology, as evidenced by the increasing adoption rate of MPLS in the United States.²

Increase Productivity

Regardless of whether you are a medium-size business with three-to-five sites or a major enterprise with hundreds of locations, *IT resource constraints will always be a looming reality*. By migrating to a converged, MPLS-enabled IP platform that simultaneously supports voice, data, and video applications, the effectiveness of those same resources can be optimized.

Additionally, MPLS has an extraordinary ability to self-configure, which 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 firm. The remaining functions can then be handled internally or, as many companies are now doing, outsourced to a provider of managed services.

Factor 2: Your Network Capabilities

Ask your service provider to assist you in examining your current network operation to determine the type of capabilities you will need. Some providers use a “discovery questionnaire” to identify the functions performed at each of your locations and to survey your current telecom environment as well as your growth plan and future network requirements. The central question to ask yourself is this: *Will your existing network be able to support your future requirements?*

Requirements for Migration

Successful network migration to MPLS depends on four requirements: *quality of service, availability, flexibility, and security*.

- **Quality of service** is dependent upon the other three requirements, but in many ways is the most important because it is the measure (or set of measures) upon which Service Level Agreements (SLAs) are based. Furthermore, because SLAs typically include non-performance clauses that carry financial penalties for the service provider, QoS is a critical measure. Defining factors include measures of uptime, mean time between failures, degree of survivability, repair response time, latency (delay), jitter, packet delivery, and others.
- **Availability** is a subjective measure of network performance but is important nonetheless. Typically negotiated by the buyer and seller of network services alike, it is most commonly defined as a percentage of

“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 Service Level Agreements.”

² Forrester Research, “Business Technographics® March 2006 North American and European Enterprise Network and Telecommunications Survey,” p. 4.

uptime, most commonly as the famous “five nines of reliability” – meaning 99.999% availability in a given period of time.

- **Flexibility** is directly related to both survivability and customer service. One measure of network flexibility is the degree to which the network can self-configure during a 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 via alternate routes, thus ensuring service continuity. Similarly, the degree to which the network can be adapted to accommodate the disparate requirements of alternative traffic types is important as well and is a measure of network flexibility.
- **Security** takes on several forms. On the one hand, the need to guarantee privacy, confidentiality, and non-repudiation (the ability to unquestionably and confidently verify the source of a transaction or message) are critical in enterprise networks 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.

“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.”

The Next-Generation Network

The primary demand that has emerged in the enterprise for MPLS-enabled networks is for the establishment of Virtual Private Networks (VPNs), which offer the performance and security of a dedicated network with the cost effectiveness of one that is shared. 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, as shown in **Figure 4**, and while this architecture has its limitations, it also has advantages. Because these networks are based on dedicated resources, they are both 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.

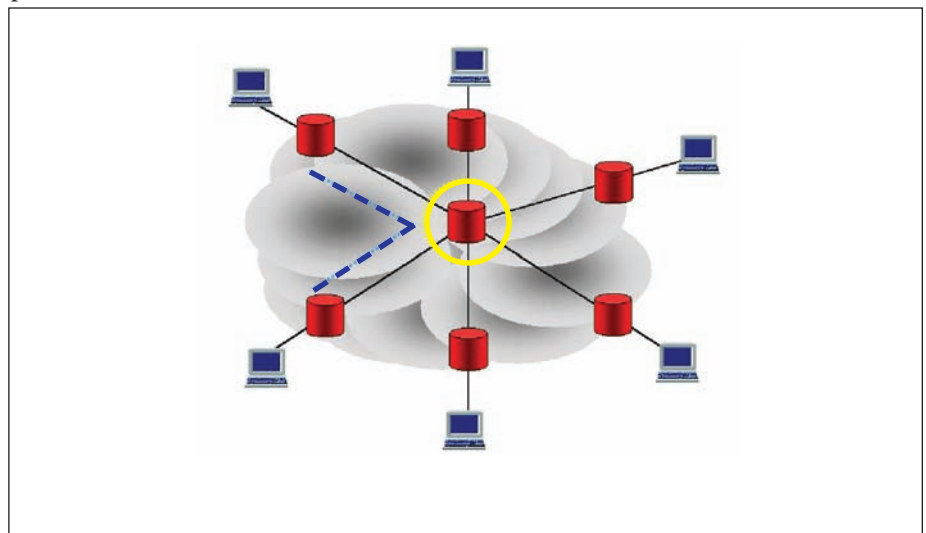


Figure 4: Layer 2 Hub-and-Spoke VPN Architecture

Critical, costly resources are focused in the center of the network (yellow circle), and 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.

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. Even worse, 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.

Now let's turn our attention to MPLS and VPNs. In a situation where a mesh network is already in place (such as the one shown in **Figure 5**), MPLS can be implemented directly over it, taking advantage of the survivable Layer 2 architecture as a foundation for the robust Layer 3 capabilities that MPLS enables. In this case, communication bypasses the hub (avoiding bottlenecks). The expensive Layer 2 switches become far more capable Layer 3 routers, and VPNs are implemented through them.

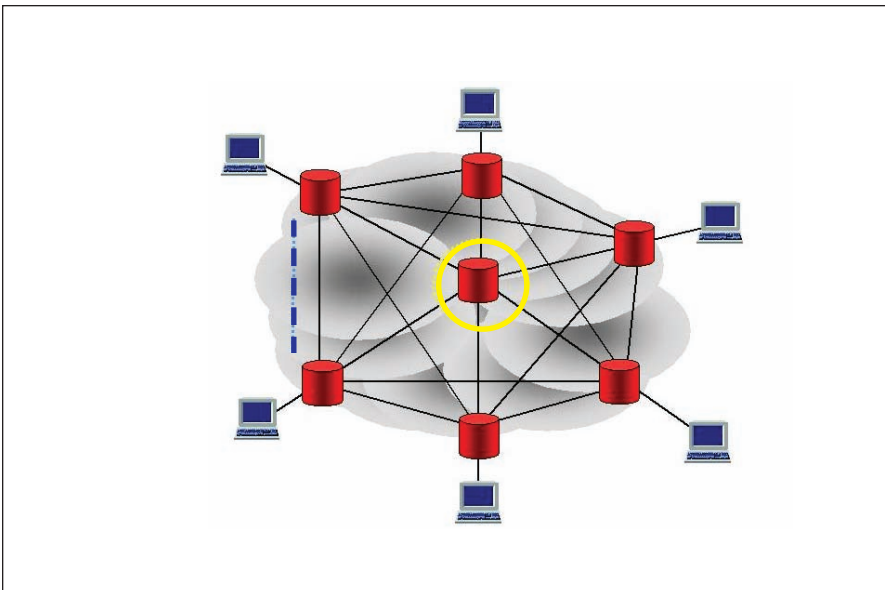


Figure 5: Fully Meshed Layer 2 VPN Architecture

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.

While the **Figure 5** scenario may be feasible as a migration path for many large enterprises to address special needs and security concerns, it is no longer practical for the majority of medium-to-large enterprises that have scarce resources and other IT priorities. Outsourcing your MPLS IP VPN networking needs to a service provider, as depicted in **Figure 6**, enables your company to minimize personnel and capital in managing your company's wide area network needs, while leveraging the expertise of your service provider. The most commonly outsourced functions include some aspects of design, installation, and ongoing management (e.g., VPN installation and testing, router management and monitoring, security management, VPN design, and VPN product selection).³

“Outsourcing your MPLS IP VPN networking needs to a service provider enables your company to minimize personnel and capital in managing your company's wide area network needs, while leveraging the expertise of your service provider.”

³ Infonetics, “User Plans for VPN Products and Services: North American Vertical Markets 2005,” reprinted in “IP VPN Market Overview” presentation by Cisco Systems, 2003, p. 15.

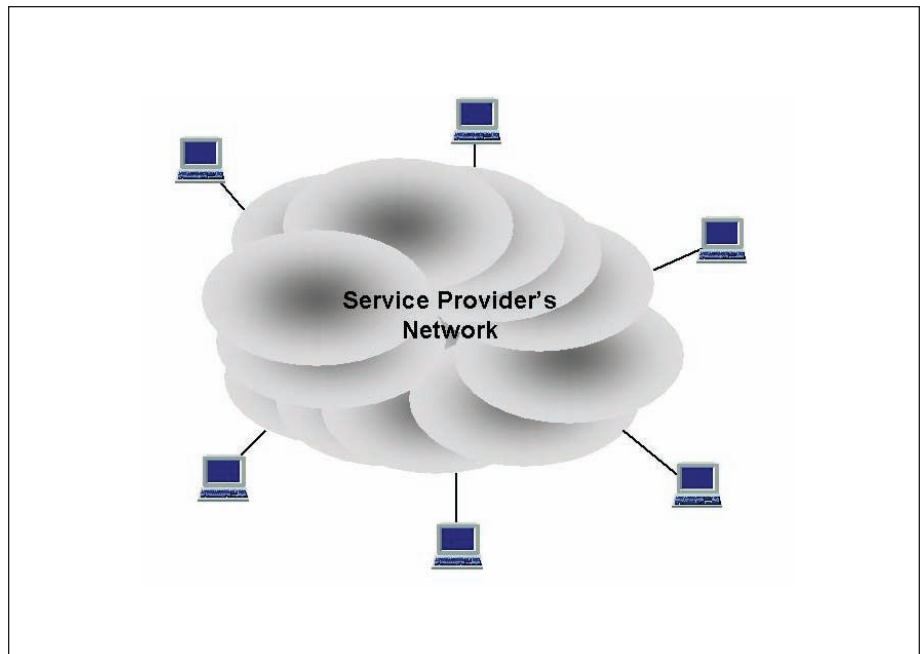


Figure 6: Layer 3 MPLS IP VPN Architecture

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 all that is needed to provision applications enterprise-wide.

Factor 3: Your Migration Path

If you need to convince executive management that MPLS migration is a good business decision, then be prepared to refute any perceived barriers to migration, and have a well-researched answer to this question: *What types of companies are well suited for MPLS IP VPNs, and how have they benefited from migration?*

Why Migrate to MPLS?

Medium- to large-size companies considering the move to an IP-based MPLS network will benefit from its design and capabilities, which are quite different from Layer 2 solutions. Some additional benefits include:

- **Quality of Service** – MPLS delivers defensible QoS supported by SLAs that address such issues as jitter, service availability, round-trip delay, packet loss, and QoS.
- **Priority Class of Service** – 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.
- **Single Infrastructure** – MPLS delivers on the promise of convergence: the ability to deliver a broad array of services over a single network infrastructure, simplifying life for the customer and the service provider alike.
- **Cost-effective Migration** – MPLS offers a cost-effective solution for the migration of complex networks. Networks that rely on MPLS in combination with in-place network assets (such as Ethernet) to interconnect regional or far-flung sub-networks are generally about 20% less expensive than many other options.⁴

“Networks that rely on MPLS in combination with in-place network assets (such as Ethernet) to interconnect regional or far-flung sub-networks are generally about 20% less expensive than many other options.”

⁴ Nagendra Bommadevara, James M. Kaplan, and Samir Patil, “Choosing the Right Corporate Network Strategy,” McKinsey & Company white paper, 2007, p. 2.

- **Built-in Security** – MPLS provides a private, segregated VPN for each customer, with dedicated IP VPN provider edge routers isolated from the public Internet, plus secure Internet access options. For companies that have already implemented IP VPNs, security was the overwhelming reason for adopting IP VPN (71.4%).⁵
- **Platform for the Future** – MPLS will support a vast array of emerging IP enabled applications that will be supported across enterprise networks, fixed and mobile devices, and location types.

Perceived Barriers to Migration

Despite the obvious advantages of MPLS for medium-to-large enterprise networks, potential adopters have admitted some reservations or “perceived barriers” to migration.⁶ For example:

- **Security** – For multi-site networks, security remains a top priority. To help ensure security, look for a service provider with a private, MPLS-enabled IP backbone, thereby segregating your data from other customers and the public Internet.
- **End-to-end Guaranteed Service Quality** – As bandwidth-hungry voice and videoconference traffic spills over to another traffic class, circuits can be overloaded and network performance deteriorate.⁷ Class of service (a tag applied to each packet indicating level of priority) needs to be monitored at the application level so that network managers have visibility into application-specific traffic performance. Over time, these tools will become more widely available by service providers managing the network.
- **Cost** – Because VoIP and data applications run over the same circuits, you get better use of existing bandwidth. What’s more, the any-to-any, fully meshed topology of MPLS is flexible and scalable, providing a broad range of Ethernet and bandwidth options when you need additional capacity to meet increased traffic requirements of media-rich applications. In short, MPLS-enabled IP VPNs offer more bandwidth for the dollar.
- **Managing VPNs** – To simplify network management, some MPLS service providers will configure, deploy, and manage CPE at each of your network sites. Some will even provide Web-based reporting and monitoring tools.

Migration Profiles

Is your company the type that would benefit from an MPLS IP VPN? The table below describes typical profiles of companies that would benefit from migrating to a fully managed MPLS-enabled IP VPN.⁸

“Because VoIP and data applications run over the same circuits, you get better use of existing bandwidth. What’s more, the any-to-any, fully meshed topology of MPLS is flexible and scalable, providing a broad range of Ethernet and bandwidth options when you need additional capacity to meet increased traffic requirements of media-rich applications.”

⁵ IDC, “IP VPN End-User Survey, 2005,” August 2005. N=400 companies with at least five employees. Reprinted in “IP VPN Market Overview” presentation by Cisco Systems, p. 19.

⁶ Infonetics, “User Plans for VPN Products and Services: North American Vertical Markets 2005,” reprinted in “IP VPN Market Overview” presentation by Cisco Systems, 2003, p. 21.

⁷ Peter Hall, “Meeting the Demands of Business-Critical Applications with Next-Generation Networks,” Ovum white paper, November 2006, p. 5.

⁸ Cisco Systems, “The Cisco Powered Network Service Provider IP VPN Sales Toolkit: Selling the Foundation for Value-added Services,” 2005, p. 18.

“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.”

Types of Companies	Specific Needs
Decentralized, regionally dispersed companies	MPLS IP VPNs are particularly well suited to serving companies that need any-to-any communications across numerous and regionally dispersed sites.
Companies with a large number of leased lines	Companies with a large number of leased lines have a difficult management task; these companies will be interested in the cost savings offered by bandwidth consolidation onto an MPLS IP VPN.
Companies with multiple traffic streams	Companies with data, voice, videoconferencing, and business applications are likely to see the merits of an MPLS IP VPN. Inherent traffic separation and QoS features in MPLS will provide traffic stream prioritization and counter concerns about security.
Companies undertaking mergers or organizational change	These companies will find the scalability and flexibility of a managed MPLS IP VPN attractive.
A holding group	The holding group will find an MPLS IP VPN of great benefit in securely segregating traffic from its companies while taking advantage of the economies of scale through centralized buying and consolidation.
Smaller companies that are growing	These companies typically take advantage of the Internet for email and file transfer, and may have Private Line or Frame Relay connections with a limited number of remote company sites. With limited IT staffing, MPLS IP VPN will free up scarce resources while offering immediate cost savings and the ability to add additional applications over one network solution.

Table 1: Company Characteristics Indicating the Need for MPLS IP VPN

These characteristics have proven to be good indicators that a company is well-suited for MPLS IP VPNs. Is your company described on this table?

Factor 4: Your Operating Budget

To control your bottom line and get a healthier return on investment for your MPLS-enabled IP network, it is important to assess the total cost of ownership (TCO), which includes capital expenditures (CAPEX), operating expenses (OPEX), and opportunity costs, all of which are key drivers in lowering TCO.⁹ A key question to ask yourself is: *How will a migration to an MPLS IP VPN affect my IT workload, capital expenditure, and ongoing operational expenses in the future?*

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-

⁹ Cisco Systems, “Total Cost of Ownership: A Key Metric for Cost-effective Networking” white paper, 2003, p. 1.

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 difficult to quantify, opportunity costs may include lost enterprise revenue and lower productivity, which are 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.

Factor 5: Your MPLS Service Provider

When selecting an MPLS service provider, be sure to verify that the company's network supports the business strategy that drove you to migrate to MPLS in the first place. While very few service providers will excel in every single checklist category, consider the ones that will support your highest priorities now and in the foreseeable future. Specifically, you should ask for answers to the following questions:

“When selecting an MPLS service provider, be sure to verify that the company’s network supports the business strategy that drove you to migrate to MPLS in the first place.”

Service Provider Selection Criteria & Checklist

- **Access Options** – 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?
- **Voice/Data Convergence** – 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?
- **Performance Measurement** – 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?
- **Service and Support** – Is the service provider capable of managing end-to-end QoS and network security, even when the circuit traverses other providers' networks?
- **Service Level Agreement** – 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?
- **Universal Connectivity** – Does the service provider have agreements with other providers to ensure universal connectivity, even in areas where the provider lacks a presence?
- **Security** – How robust is the service provider's network security? MPLS is a highly secure infrastructure, but even the best networks have vulnerabilities. One question to ask is whether Internet access is provided across the same core infrastructure as access to the VPN, or whether it is done over a separate infrastructure.
- **Redundancy** – 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.

“MPLS offers the same level of service as legacy Layer 2 technologies, but at a much lower cost and with much greater flexibility. The time to consider converting to an MPLS solution has arrived.”

Conclusion

What Every Enterprise Should Know

MPLS has reached “critical mass” in the marketplace and 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 capabilities, (3) a strategic migration path, (4) your operating budget, and (5) solid proof that your service provider’s network has the features and capabilities to support 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.

Where to Begin

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. Getting advice from our network analysts is a good place to begin.

APPENDIX A

XO MPLS IP-VPN

Converged Voice, Data, and Video Solution with Class of Service Routing

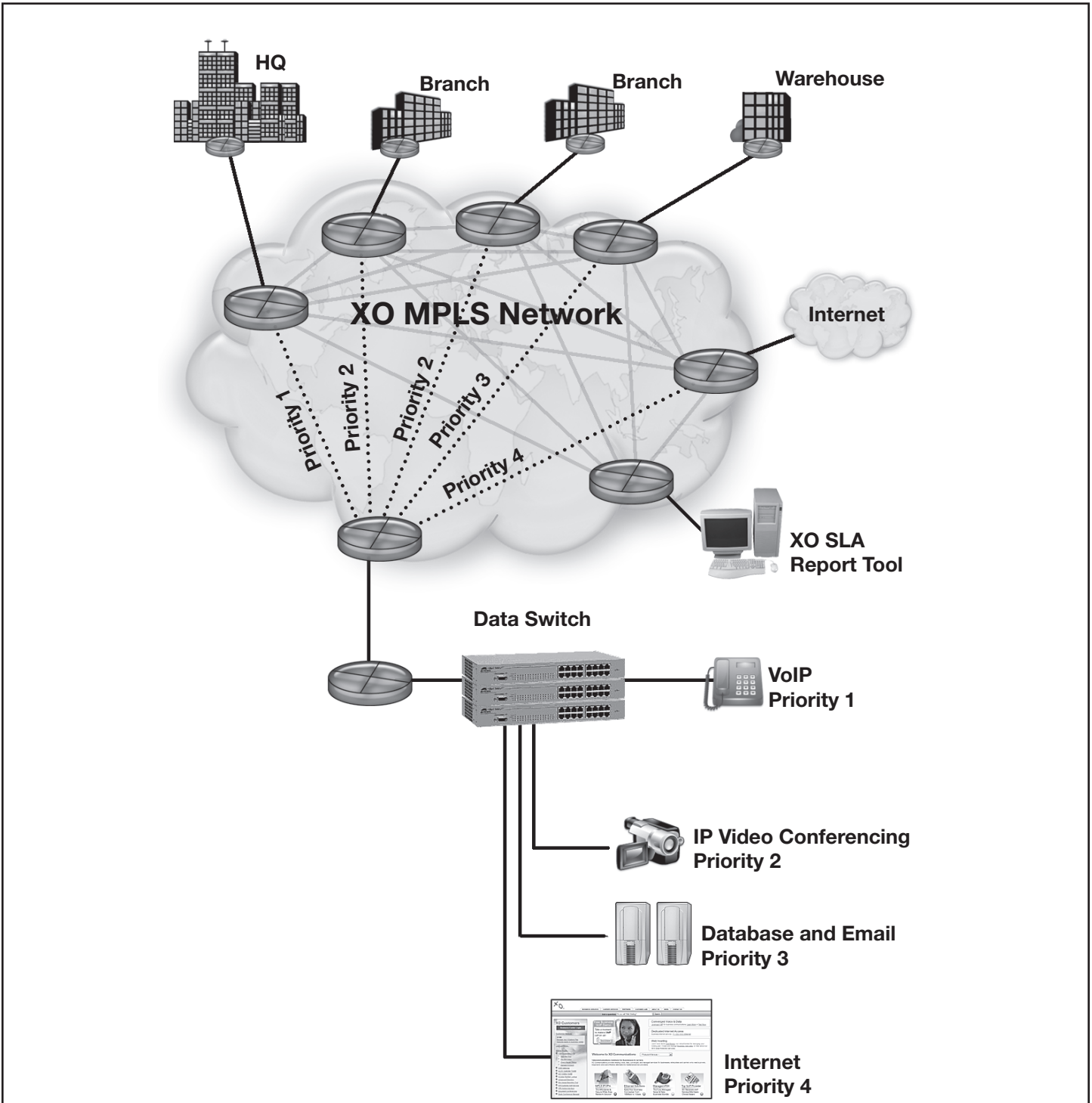


Fig. A: XO MPLS provides performance and flexibility with Class of Service routing and traffic prioritization, ensuring that critical applications get the quality of service they need.

APPENDIX B

XO MPLS IP-VPN

Secure, Scalable, Redundant Solution for Multi-site Networks

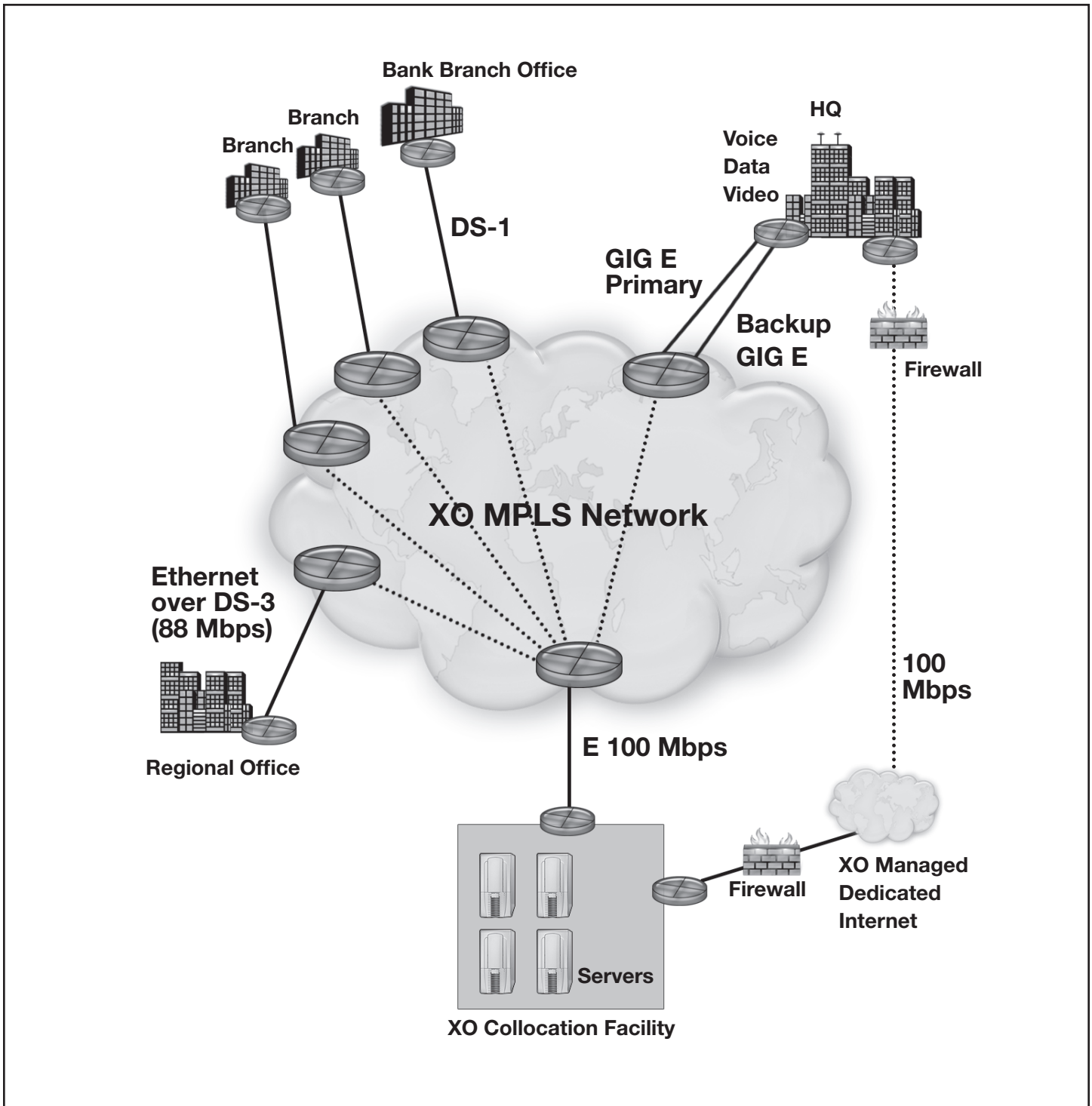


Fig. B: XO-managed MPLS supports financial services company with robust disaster recovery, redundancy, scalable access speeds (from DS-1 to Gigabit Ethernet), and XO-managed solutions without requiring major capital outlay for a new network.

APPENDIX C

XO MPLS IP-VPN

Supports a Wide Range of Integrated VoIP Service Offerings

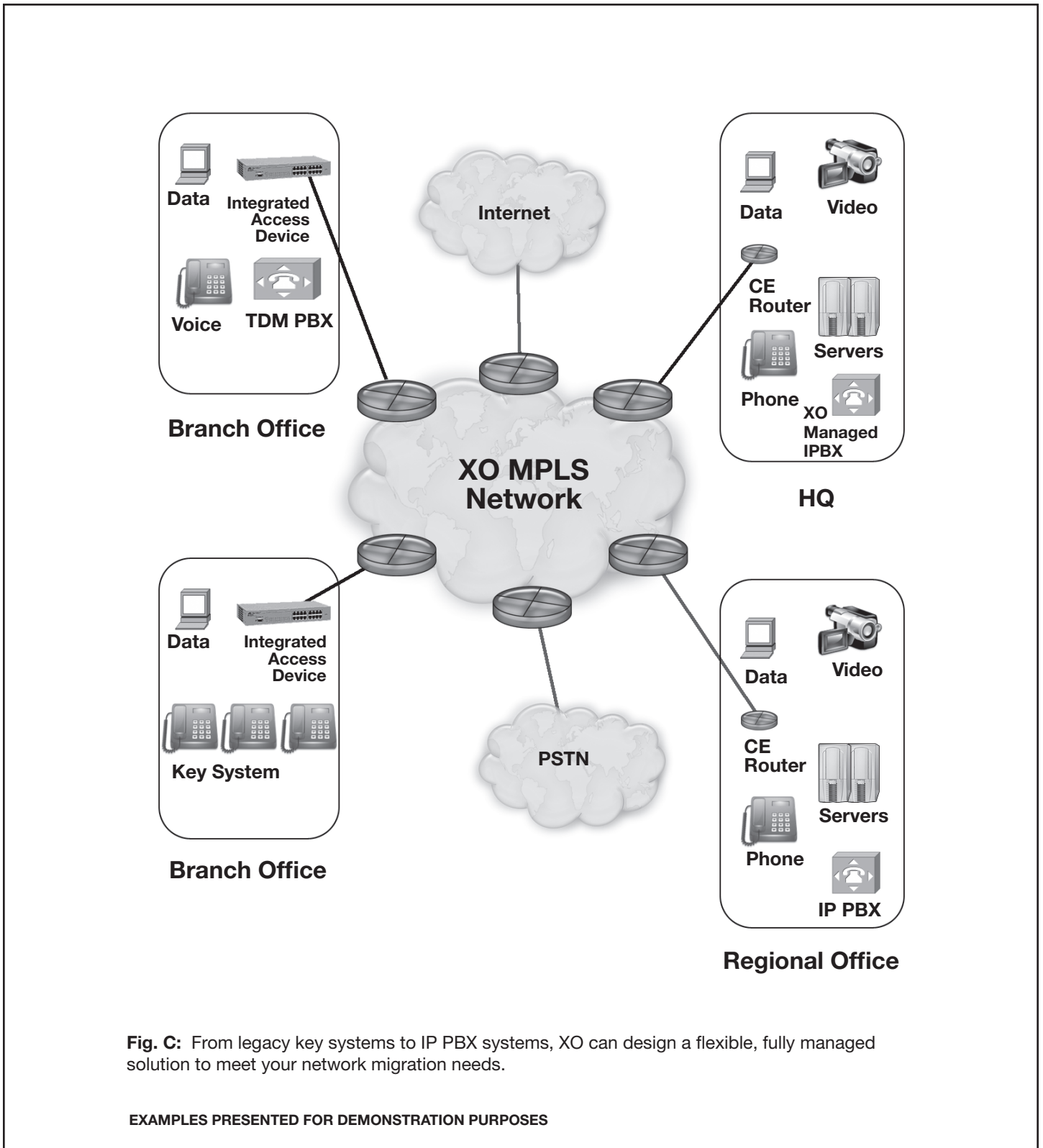


Fig. C: From legacy key systems to IP PBX systems, XO can design a flexible, fully managed solution to meet your network migration needs.

EXAMPLES PRESENTED FOR DEMONSTRATION PURPOSES

About XO Communications

XO Communications is a leading provider of telecommunications services exclusively to businesses. XO® services include local and long distance voice, dedicated Internet access, private networking, data transport, and Web hosting services, as well as bundled voice and Internet solutions. With more than a billion dollars in annualized revenue, XO is a proven provider of IP bundled services, including the award-winning Voice over Internet Protocol (VoIP) services bundle, XOptions® Flex. XO operates an 18,000-route mile nationwide network that connects 75 metropolitan markets, and operates close to 900,000 miles of metro fiber.

XO also offers an MPLS IP-VPN service that is ideal for medium-to-large businesses looking for operational advantages and savings associated with an IP-based wide area networking (WAN) solution. The XO MPLS IP-VPN solution delivers more bandwidth for the dollar, faster application deployment, lower network operating costs, and more access options than traditional WAN services. To find out how XO can meet your specific networking requirements, visit www.xo.com or call 1.866.266.9696.

About Shepard Communications Group, LLC

Shepard Communications Group (SCG) provides industry analysis, training, and consulting services to component and device manufacturers, service providers, regulatory agencies, professional services firms, universities, advertising agencies, venture capital firms, vertical industry sectors, and global economists. All services are offered in both English and Spanish and are always customized for the market in which they are delivered.

Steven Shepard is the president of SCG, located in Williston, Vermont. He is a professional author and educator with over 25 years of varied experience in the telecommunications industry. Shepard specializes in international issues in telecommunications with an emphasis on strategic technical sales, network convergence, and the impact of emerging technologies. For more information, visit www.shepardcomm.com or call 1.802.878.0486.