CISCO SYSTEMS

WHITE PAPER

THE MOVE TO MPLS-BASED VPNS: EXPLORING SERVICE OPTIONS

EXECUTIVE SUMMARY

IT managers continue to learn more about and appreciate the values of Multiprotocol Label Switching (MPLS)-based VPN services as a viable corporate wide-area network (WAN) alternative. As IT managers consider moving to the new MPLS-based VPN services from their current legacy networks, they seek information about how to manage the migration transparently, what service options are best for them, and if the MPLS-based VPN will help achieve business goals.

This paper provides IT managers a comprehensive review of four categories of migration issues that arise when moving to MPLS-based VPNs:

- *A migration strategy*—Will you migrate incrementally, will you maintain both new and existing networks during a transition phase, or will you keep a portion of the existing network in a hybrid environment?

- *Connectivity options*—What connectivity and routing protocol options are available from service providers and how do you decide what network topology (full mesh or hub and spoke) is best for your corporate WAN?

- *Multiservice traffic*—How can a service provider meet the performance requirements for your company by supporting data, voice, and video traffic in a converged, MPLS-based VPN network environment?

- *Advanced service offerings*—What additional advanced service considerations must be made by a multinational company with global reach and multiple user communities, or companies that deal with multiple service providers?

Businesses that move to MPLS-based VPNs will realize further benefits by choosing managed VPN services from a service provider that can handle all or a portion of the enterprise's needs for installation, provisioning, and management of networking equipment; support of network transport; and network security. Service providers that operate networks with Cisco® products end to end—those that display the Cisco Powered logo—are ideally positioned to facilitate smooth migrations to MPLS-based VPN services. Managed services and guidelines to evaluate and select service providers for MPLS-based VPN services are introduced later in this paper.

IT managers can help ensure a transparent migration and tap into the benefits of MPLS VPN services in the shortest time possible by considering the issues and topics covered in this paper.

> **"Using MPLS, VPNs have become much easier to deploy and scale. This technology not only creates a more efficient network, it allows service providers to accommodate virtually any customer's requirement for remote access, intranets, extranets, and Internet access."**
>
> —Irwin Lazar, The Burton Group

INTRODUCTION

While enterprise IT managers must continually manage costs and maintain reliable WAN infrastructures to meet their business goals, success in today's business climate also depends on the ability to overcome a more complex set of challenges to their corporate WAN. Today's enterprise IT managers are faced with:

- Geographically dispersed sites and teams that must share information across the network and have secure access to networked corporate resources

- Mission-critical, distributed applications that must be deployed and managed on a networkwide basis

- Security requirements for networked resources and information that must be securely and reliably available to authorized users

- Business-to-business communication needs to users within the company as well as to partners and customers

- Increasing demands for bandwidth as more business applications are deployed over the corporate network and extended to the Internet

MPLS-based VPNs provide enterprise IT managers with a variety of benefits for meeting these challenges, including:

- Enhanced ability to deliver a wide range of connectivity options to geographically dispersed branch offices, remote users, teleworkers, and business partners, and the ability to draw on the ability of the Internet for ubiquitous access

- Quality of service (QoS) features that prioritize traffic to help ensure end-to-end application performance

- Support for the convergence of previously disparate data, voice, and video networks, which results in cost savings for the enterprise

- Security and privacy on an equivalent level with Frame Relay- and ATM-based networks

- Easier deployment of productivity-enhancing applications such as enterprise resource planning (ERP), e-learning, and streaming video

- The flexibility to easily add or remove connections—supporting several or up to thousands of sites—as companies expand, merge, or consolidate

THE MIGRATION STRATEGY

Today's enterprise WANs are typically based on leased lines, Frame Relay, or ATM technology. As businesses grow and evolve, mission-critical applications and connectivity options invariably become more complex. In addition, many existing corporate WANs are composed of multiple disparate data, voice, and video networks. Transitioning and converging these disparate networks to MPLS-based VPNs requires a migration strategy that is derived by exploring the following issues:

Would you like to introduce MPLS-based VPN services on a pilot basis before corporate wide deployment?

With existing corporate WANs already in place, IT managers can choose to introduce MPLS VPNs on a pilot basis, initially bringing up just a few sites or low-impact sites. Additional sites can be added at a pace that suits the business need. This mode of gradually transitioning to MPLS-based VPN services will minimize risk, and allow time to resolve migration issues within a project framework that has a more manageable, defined scope.

How much of the corporate WAN is invested and deployed in the Frame Relay- or ATM-based infrastructure? Should the migration to an MPLS-based VPN network be a clear cutover from the existing network?

If these investments and deployments are significant, retaining a portion of the existing network may be desirable. The retained portion can support sites that have less immediate needs for the MPLS VPN services. Those could include sites that are not projecting aggressive increases in network demand, or sites where connectivity issues are under control. While it would be technically possible to replace the existing networks and switch entirely to the new converged MPLS VPN network, it may come at too high a price and result in unrealized returns on investments from past deployments. To decide whether to maintain the existing networks, enterprise IT managers must carefully evaluate the current investments and then consider the additional options that follow.

If your company is maintaining existing networks, should it be for a finite transitional period, or for an indefinite period of time?

Several factors must be taken into consideration:

- *Circuit cost*—Service providers charge more for a Frame Relay permanent virtual circuit (PVC) or an ATM connection than for an IP VPN connection (see Table 1). Also, Frame Relay requires two PVCs per site while MPLS-based VPNs eliminate the need for PVCs and thereby lower network cost and site access charges.

- *Equipment costs*—Maintaining the old network will entail additional ongoing expenditures.

- *IT management and training*—Support resources will have to be split among the old and the new networks, and enterprise IT managers must evaluate the ability of their staff to handle a more complex, mixed environment during the transition, or evaluate the service provider's ability to fulfill the support gap. Also, the network support resources must be adequately trained and staffed accordingly as long as both networks are in place.

- *Legacy applications*—Some legacy applications may require modification as they are moved from the old to the MPLS-based VPN network. However, MPLS-based VPNs do provide generic routing encapsulation (GRE) tunneling to support non-IP applications.

- *Backup needs*—For some businesses, maintaining the existing network provides a valuable backup capability. Depending on the severity of impact to business incurred by network outages, this option should be explored for some companies.

Table 1. VPN Cost Savings for a Cisco Customer Connecting its Chicago Headquarters With Four Branch Offices (Source: Cisco, 2003)

	Frame Relay			VPN	
Location	Circuit	Function	Cost per Month (U.S. Dollars)	Internet Circuit	Cost per Month (U.S. Dollars)
Chicago	DS3	Internet	$8200	DS3	$5600
Chicago	DS3	Frame Relay	$10,500	DS1	$850
Chicago	T1	Internet for redundancy	$2100		
New York	T1	Frame Relay	$2700	T1 x 2	$1700
Seattle	T1	Frame Relay	$3000	T1 x 2	$1700
Houston	T1 x 2	Internet (traditional from acquired company)	$4000	T1 x 2	$1700
Dallas	T1 x 2	Internet (traditional from acquired company)	$4000	T1 x 2	$1700
TOTAL			$34,500		$13,200
TOTAL MONTHLY COST SAVINGS: US$25,250 PERCENTAGE SAVINGS: 61%					

For more information about the total cost of ownership (TCO) for an existing network, visit:
http://www.cisco.com/go/vpntool1

By exploring the above issues and fully understanding the costs associated with each alternative, enterprise IT managers can develop the optimal migration strategy. Ultimately, some enterprises may choose to migrate and in parallel maintain the existing networks for various reasons such as backup, legacy application support, or cost. Others will choose to make a clear cutover and switch to MPLS-based VPN completely. Enterprise IT managers should choose a plan that best fits their resources and budgets.

CONNECTIVITY OPTIONS

After developing a migration strategy, the next step involves connectivity—how will the enterprise connect to the service provider's network?

Network Topology

To improve branch-to-branch traffic efficiency, some enterprise corporate networks have evolved from hub-and-spoke topologies into *regionalized* hub-and-spoke topologies. Multiple regional hubs are established to offload headquarter and improve same-region networking between regional hub and branches for data, voice, and video. However, ultimately, as the enterprise network grows, even the regionalized hub-and-spoke topology falls short of full-mesh topology. MPLS-based VPNs offer full-mesh, any-to-any connectivity, and provide enterprises a more scalable, flexible networking option when their business spans many sites or even extends globally to multiple countries. MPLS-based networks offer the flexibility and high scalability for any-to-any connectivity, and therefore the migration to MPLS-based VPNs can help enterprise IT managers overcome many topology-related limitations.

Choice of Layer 2 Connectivity

On a site-by-site basis, a service provider's wide range of connectivity offerings—such as leased line, ATM, Frame Relay, Ethernet, 802.1q, or DSL—must be considered and matched to the networking requirements for that site. If a Layer 2 connectivity option is being considered for some sites, the factors for making the decision include:

- *Existing equipment and interfaces*—Will the service provider be able to offer a connectivity option that is compatible with existing equipment at those sites?

- *Speeds and feeds*—How much bandwidth must be provided by the service provider for those sites?

- *Ethernet availability*—Many service providers are now offering Metro Ethernet services and some sites may want to take advantage of this service option.

- *Managed or self-managed customer equipment*—Consider the installation, provisioning, management, and support responsibilities for customer equipment at each site, and factor the cost into the overall connectivity choice.

Choice of Layer 3 Connectivity

Existing enterprise corporate networks may employ a variety of Layer 3 protocols: Enhanced Interior Gateway Routing Protocol (EIGRP), Border Gateway Protocol (BGP), static routing, Open Shortest Path First (OSPF), Routing Information Protocol (RIP), or Intermediate Systems-to-Intermediate Systems (IS-IS) Protocol. Today, service providers widely support the first three options—BGP, EIGRP, and static routing. EIGRP is also currently the most prevalent in many enterprise corporate networks, and EIGRP eases migration to MPLS-based VPNs if the enterprise is planning to use a service provider that also supports EIGRP. The remaining three protocols—static routing, OSPF, and RIP—can also be successfully supported in the migration to MPLS-based VPNs. Optionally, enterprises may even select one Layer 3 protocol for some sites and another for the other sites. Any of the three most popular protocol options—EIGRP, BGP, or static routing—function equally well with an MPLS-based VPN.

MULTISERVICE TRAFFIC REQUIREMENTS

The class-of-service (CoS) capability and the support of end-to-end QoS provided by MPLS help ensures that time-sensitive traffic is given the appropriate priority over the MPLS network and that stringent latency requirements can be met. MPLS can also benefit enterprises that wish to consolidate their data, voice, and video traffic in a converged environment. As enterprise IT managers migrate to MPLS-based VPN services, they should be familiar with the characteristics and requirements for the three distinct types of traffic:

- *Voice*—Voice traffic is smooth, benign, drop-sensitive, and delay-sensitive, and is typically based on User Datagram Protocol (UDP). Bandwidth per call depends on the particular codec adopted, sampling rate, and Layer 2 media employed.

- *Video*—Video traffic is "bursty," drop-sensitive, and delay-sensitive, and requires much bandwidth. IP-based videoconferencing has some of the same sensitivities as voice traffic.

- *Data*—This category of traffic is much more varied. It can be smooth or bursty, benign or greedy, drop- and delay-insensitive, and involves Transmission Control Protocol (TCP) for send/receive acknowledgment and retransmit. Traffic patterns vary by application, and data classes must support several different priorities or application categories.

To help ensure that the specific requirements for all three types of traffic are supported by MPLS VPNs, enterprise IT managers must explore the following issues and discuss the related requirements with the service provider.

What are the traffic requirements at each site?

Will every site or only some sites require a mix of data, voice, and video support?

What kind of delay, packet loss, and jitter characteristics can your networked applications tolerate?

Data traffic is typically handled with multiple CoSs where each CoS can be defined and given the appropriate support based on the priority requirement of the application that is generating the traffic. In general, enterprises should define no more than four or five traffic classes, such as:

- *Real time and mission critical*—Transactional and interactive applications with a high business priority

- *Video interactive or transactional/interactive*—Client-server applications, messaging applications

- *Business or bulk*—Large file-transfers, e-mail, network backups, database synchronization and replication, video content distribution

- *Best effort*—Default class for all unassigned traffic; typically at least 25 percent of bandwidth is reserved for best-effort traffic

- An optional (deferential) class is "scavenger" (peer-to-peer media-sharing applications, gaming traffic, entertainment traffic)

For voice traffic, three parameters are important:

- *Loss*—Loss causes voice clipping and skips. The industry-standard codec algorithms implemented by most digital signal processors (DSPs) can typically correct for up to 30 milliseconds (ms) of lost voice with the use of concealment algorithms; therefore, the loss of two or more consecutive 20-ms voice samples will result in noticeable degradation of voice quality.

- *Delay*—Delay causes voice-quality degradation if it is above 150 ms.

- *Delay variation (jitter)*—The adaptive jitter buffers within most IP telephony devices can usually compensate for no more than 20–50 ms of jitter. As these jitter buffers are dynamically adaptive, there is no defined and absolute limit for jitter that will hold true for all circumstances. However, most testing shows that when jitter consistently exceeds 30 ms, voice quality degrades significantly.

There are two main types of video applications: interactive video (such as videoconferencing) and streaming video (such as the Cisco IP/TV® application, which may be either unicast or multicast). For interactive video traffic:

- Packet loss should be no more than 1 percent

- One-way latency should be no more than 150 ms

- Jitter should be no more than 30 ms

For streaming video traffic:

- Packet loss should be no more than 2 percent

- Latency should be no more than 4 to 5 seconds (depending on the video application's buffering capabilities)

- No significant jitter requirements exist

Working closely with a service provider, enterprise IT managers can fine-tune specific requirements for the delay, packet loss, and jitter parameters. For a complete overview of these parameters, please review two Cisco white papers about service provider QoS at:

http://www.cisco.com/warp/public/cc/so/neso/sqso/spqos_wp.pdf

http://www.cisco.com/warp/public/cc/so/neso/vpn/vpnsp/spqsd_wp.pdf

How will network performance parameters be monitored?

Service providers may offer monitoring tools to help enterprise IT managers evaluate performance of the MPLS-based VPNs they subscribe to. Two basic monitoring modes are: last-mile performance monitoring for assessing the customer edge (CE)-to-provider edge (PE) access link (CE-PE), and end-to-end performance monitoring (CE-CE). End-to-end performance monitoring provides more tangible information because it encompasses performance of the network from the CE, through the provider's network, to the destination CE. While a service provider may have deployed a highly robust core network, enterprise IT managers should not assume that the core will support infinite performance. An end-to-end monitoring tool can provide information about complete performance, in many instances. Discuss one or both of these monitoring options with the service provider, along with the service-level agreement (SLA) metrics that they provide. SLA metrics include general measurements of availability and mean time to repair (MTTR), and per-class metrics such as latency, jitter (for voice or real-time traffic only), and packet loss.

What kind of network reliability does the service provider guarantee?
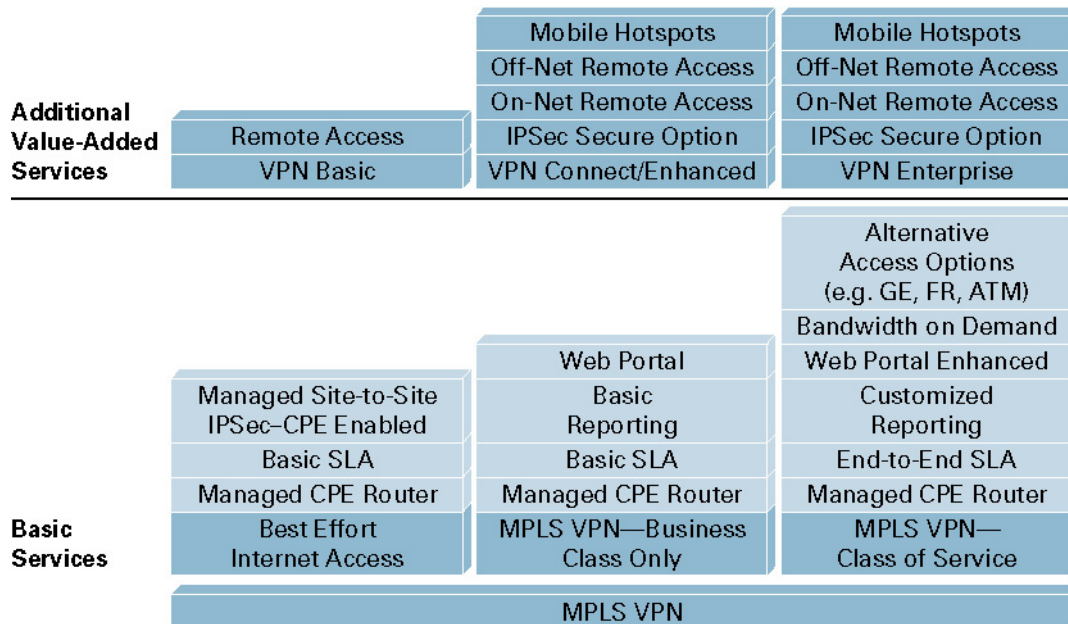
Network reliability becomes more crucial for multiservice traffic. In a data-only networking environment, the network failover mechanism can typically recover from any packet loss suffered during a network outage such as an internal link failure or node failure. In contrast, the delay- and drop-sensitive video and voice traffic are always highly affected by network downtime. Enterprise IT managers should carefully compare their multiservice QoS requirements, on a site-by-site basis, with the service provider's SLA parameters.

ADVANCED SERVICE OFFERINGS

Advanced service offerings are often required by businesses with global reach or those that have a need to separate multiple user communities within the company. Service providers are responding with a variety of new basic services and extended network capabilities based on the Internet. Advanced services are also emerging to help assure network security, to extend services globally, and to provide the closed-user-groups function.

Figure 1 summarizes the many types of basic and advanced services that can be deployed over MPLS-based VPNs.

Figure 1

MPLS-Based VPNs Serve as Foundations for Value-Added Services

Additional Value-Added Services

		Mobile Hotspots	Mobile Hotspots
		Off-Net Remote Access	Off-Net Remote Access
		On-Net Remote Access	On-Net Remote Access
	Remote Access	IPSec Secure Option	IPSec Secure Option
	VPN Basic	VPN Connect/Enhanced	VPN Enterprise

Basic Services

			Alternative Access Options (e.g. GE, FR, ATM)
			Bandwidth on Demand
		Web Portal	Web Portal Enhanced
	Managed Site-to-Site IPSec–CPE Enabled	Basic Reporting	Customized Reporting
	Basic SLA	Basic SLA	End-to-End SLA
	Managed CPE Router	Managed CPE Router	Managed CPE Router
	Best Effort Internet Access	MPLS VPN—Business Class Only	MPLS VPN— Class of Service

MPLS VPN

The Internet and Ubiquitous Access to MPLS-Based VPNs

The exponential growth and ubiquity of the Internet is contributing to the extension of VPNs outside of a service provider's network service footprint. Taking advantage of the Internet and relying on it to complement existing networks is well accepted today, and service providers offering MPLS-based services are responding by extending the service footprint into the public domain and using the Internet for ubiquitous access to their MPLS-based VPNs. Consequently, service providers today can now offer more comprehensive bundles of global end-to-end services for business customers.

IP Security Protocol

Based on open standards developed by the Internet Engineering Task Force (IETF), the IP Security (IPSec) Protocol helps ensure confidentiality, integrity, and authenticity of data communications across the public Internet or a service provider network. Service providers are integrating IPSec with MPLS-based VPN services to use existing infrastructure and the ubiquitous Internet to expand geographic coverage and enable enterprise customers to securely extend their corporate networked resources from MPLS-based VPNs to remote branch offices and mobile workers anywhere.

Note: The inherent security of MPLS has been proven to be equivalent to ATM- and Frame Relay-based VPN security. For more information about the specific network security attributes of MPLS VPNs, refer to the Cisco white paper, *Analysis of MPLS IP VPN Security: Comparison to Traditional L2VPNs Such as ATM and Frame Relay, and Deployment Guidelines* at: http://www.cisco.com/warp/public/cc/so/neso/vpn/prodlit/mpvpn_wp.pdf

A report summarizing the Miercom evaluation of MPLS VPN security is also available at: http://www.cisco.com/application/pdf/en/us/guest/netsol/ns103/c654/cdccont_0900aecd800c552e.pdf

Global Networks

New challenges arise when businesses need to extend a corporate network footprint globally. Large enterprises with global reach have a few options for handling these issues when working with service providers that provide global services. The preferred option is to work with a service provider that already has a global presence. Alternatively, enterprises may choose to work with multiple service providers to achieve the same required global network presence. When working with multiple service providers, enterprises can choose to self-manage the interconnection between the service provider networks, or require the service providers to manage the interconnection. In the case of self-managing the interconnection, the enterprise purchases and installs the appropriate network devices, provides the necessary support and management, and determines how to handle the routing policies between the networks. In the other case, the service providers involved may cooperate and work out the interoperability and interconnect service issues without active participation from the enterprise customer. It is even possible that the service providers implement mechanisms to maintain service quality consistently across the interconnecting networks. Building such VPNs typically requires the use of inter-autonomous system VPNs. No matter how it is done, the enterprise IT managers must address interconnect issues with the service providers, and be prepared to address future issues as the business and corresponding network requirements grow and as new services are introduced onto the MPLS-based VPNs.

European service providers—early pioneers and proponents of the adoption of MPLS-based VPNs—have introduced a new capability for enterprises. Based on carrier-supporting-carrier (CsC) technology developed by Cisco Systems®, many larger service providers were offering wholesale services to other service providers and are now offering the same wholesale services to enterprises.

Beyond the cost savings, the availability of CsC services provides three major benefits to enterprises:

- Fewer VPN routing and forwarding (VRF) table entries on the PE. VRF routes are offloaded to the CE, making it a more scalable solution; for example, using a traditional VPN service, one enterprise customer might require 20 VRF routes in one city (for 20 sites) and 20 VRF routes in another city (for the 20 sites/stores there). With CsC technology, the CE could handle all of these VRF routes. The PE could support the sites with fewer VRF routes.

- Multiple departments sharing the same physical premises do not need to buy multiple circuits. Separate business units can share one access link by creating a VRF at the CE. In this way, CsC technology serves a multiplexing function.

- QoS management can also be extended to the CE, being carried out on a per-customer basis and making it a more scalable solution.

As CsC technology becomes more widely adopted by service providers, enterprises will be able to buy one MPLS circuit and thereby reduce circuit costs and network complexity for multiple sites within the same areas. Ask your service providers about the availability of services based on this technology, and their plans for expanding these offerings in the future.

Closed User Groups

The different groups of users within the enterprise are often defined as "internal customers" by IT departments. Examples include enterprise departments such as human resources, finance, engineering, marketing, and sales; faculties, or research groups; as well as actual customers such as many airline operators at an airport, or external partners that share space or IT infrastructure. These internal customers, also called closed user groups (CUGs), need to remain private and separated from each other, with secure and independent VPN connectivity over the shared service provider network infrastructure.

CUG services enable the formation of user groups, with associated access restrictions. An authenticated user can be associated with one CUG, multiple CUGs, or no CUGs on each network. CUG members can communicate with other users within their own CUG. Defined restrictions can prevent unauthorized communications.

Service providers that offer CUG services provide enterprise IT managers with three key benefits—the ability to easily define groups or communities of users, the added security provided by the associated access restrictions, and simplified configuration of MPLS-based VPNs.

MANAGED SERVICES

Businesses that move to MPLS-based VPNs can take advantage of further benefits by choosing to out-task the VPN function to a service provider—the enterprise is thus purchasing "managed" VPN services from a service provider. A service provider can handle part or all of the enterprise's needs for installation, provisioning, and management of network equipment; support of network transport; and network security. Managed services provide enterprise customers immediate access to the benefits of an MPLS network, with network availability and security being managed by the service provider on a 24-hour basis. SLAs can be established to define the required network performance and establish metrics to monitor and report actual performance against the requirements. Service providers can also deliver valuable support services—such as 24-hour help desks—that would otherwise require extensive staffing resources and budgetary support if implemented in house.

Today, enterprises choose to work with service providers when they are:

- *Facing challenges*—Service providers can help enterprises overcome challenges such as constrained IT resources, difficulties managing complex infrastructures, ever-changing network security requirements, the need to respond to market demands quickly with flexible and scalable networks, keeping a competitive position, and reducing costs.

- *In transition*—Enterprises often need assistance when it becomes necessary to upgrade or relocate existing infrastructures, change the scope or scale of operations, adjust for a merger or acquisition, or introduce new services to meet customer demands or company growth.

- *Setting priorities to increase revenue*—Service providers can help enterprises remain focused on mission-critical processes rather than day-to-day support and management of networking resources, and can also help ensure secure, global communications.

For more information about selecting and working with service providers, visit:
http://www.cisco.com/warp/public/779/servpro/cpn/benefits/Cisco_Outsourcing_Guide.pdf

For more information about the business case for managed VPN services, take the managed services e-tour at:
http://www.cisco.com/go/msetour.

For more information about managed services over networks built with Cisco equipment end to end, visit:
http://www.cisco.com/go/managedvpnservices

At this site, you can view regularly updated information about topics that include:

- Frame Relay-/ATM-based VPN-to-IP-based VPN migration

- Yankee Group report on IP VPNs

- Service overview of VPNs for IT managers

- MPLS VPN security

GETTING STARTED

With a foundation of superior Cisco Systems technology, VPN services enable the most advanced and robust business communications solutions. Managed services from a provider that delivers its services over a network build end to end with Cisco equipment can help your business excel. Regardless of the size of your organization, these service providers can match your needs with the right services, based on Cisco technologies, to manage and enhance your network and your business. Managed services can help you save time and money and concentrate on what your company does best.

Service providers that display the Cisco Powered logo are uniquely positioned to assist enterprise IT managers in the migration to MPLS-based VPN services. They have earned the Cisco Powered Network designation by maintaining high levels of network quality and by basing their VPN services end to end on Cisco equipment—the same equipment that virtually all Internet traffic travels on today. More than 350 of the most successful service providers around the world have earned the Cisco Powered Network designation. Situated in 62 countries, these providers

offer a wide range of services for small and large businesses alike. From the basics, such as Internet access and Web hosting, to emerging services such as IP telephony and storage networking, they should be an enterprise's first choice.

Teaming up with a service provider enables businesses to respond to the shifting demands of the economic climate and offers many immediate benefits:

- Allows companies to stay focused on their core business functions

- Provides access to world-class capabilities that can propel growth

- Enhances network security for operations, confidential information, and applications

- Offers superior high-performance networking and bandwidth

- Increases speed and agility to meet market demands

- Supports faster implementation and optimal interoperability of new services

- Secures mission-critical applications and transactions

- Provides access to leading technology that companies might not otherwise be able to afford

For a list of recommended service providers, go to:

http://www.cisco.com/cpn

CISCO SYSTEMS

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
        800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on
the Cisco Web site at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica
Croatia • Cyprus • Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR
Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia • Mexico
The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia
Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe