



SERVICE OVERVIEW

STRATEGIC RELIANCE ON OUT-TASKING CAN STREAMLINE IT OPERATIONS, BOOST FLEXIBILITY, AND REDUCE COSTS

In today's business environment, ubiquitous connectivity and maximized use of corporate networked resources can be decisive factors that enable a business to reduce costs, increase productivity, and maintain a competitive edge. Pressured by limited resources and budget, IT managers increasingly rely on more cost-effective, flexible, and scalable IP-based VPNs to streamline their corporate networks and facilitate stronger external relationships with customers, suppliers, and partners. Adding to this challenge is a need to integrate data, voice, and video traffic over economical, scalable, and dependable networks. IP-based VPNs have emerged as a viable solution for meeting these challenges, and increasing numbers of IT managers are now looking to service providers for value-added, cost-effective, VPN-based services.

EVOLVING NEW STRATEGIES TO MEET TODAY'S TECHNICAL AND BUSINESS DEMANDS

Challenge

Faced with the need to converge disparate networks, maximize return on investment, and work with constrained resources, IT managers have discovered that selectively out-tasking network implementation and some aspects of the ongoing management of their evolving network to a qualified service provider is a viable alternative that brings distinct cost savings and operational advantages. Out-tasking also can lower implementation as well as ongoing support cost and free valuable resources to focus on strategic IT initiatives.

Solution

Out-tasking can:

- Reduce day-to-day network management hassles.
- Free time for high-value IT initiatives.
- Reduce overhead and unpredictable costs associated with implementing and managing a network in house.
- Provide a cost-effective foundation to add other network-based, value-added managed services (such as IP telephony and managed security).
- Facilitate moves, adds, and changes with ease and lower cost.

ENTERPRISE IT MISSION-CRITICAL CONCERNS

The present economy has significantly influenced the global business environment—businesses must constantly reduce costs, improve productivity, increase revenue, and maintain competitive differentiation.

Directly affected by this focus, IT organizations face the challenge of having to do more with limited available resources, and must now extract the most value from past infrastructure investment. They must also support a more diverse workforce along with a need to consolidate disparate networks as they deploy more network-based, value-added business applications. Many IT managers also must support a constantly changing corporate network as a result of business expansion, consolidation, mergers, and acquisitions.

Business climate changes also impact IT infrastructure. Today's workforce is increasingly more mobile and geographically dispersed, boosting demand for greater flexible, ubiquitous, and secure access to corporate networked resources. Communication channels designed for data are increasingly forced to accommodate additional bandwidth-intensive voice, video, and multicast information, placing greater demands on bandwidth use. Security measures to safeguard the network are becoming more vital as well as problematic as the breadth and scope of corporate networks broaden.

As the scope of corporate networks continues to broaden, enterprise IT organizations face technical challenges as well. They include:

- Existing hub-and-spoke or partially meshed network topologies cannot effectively support the any-to-any communication that many businesses now require.
- Existing network management and planning tools have limited scope and capability.
- Inflexible, lengthy installation and provisioning processes hamper rapid network growth and response to changes in today's dynamic market environment.
- Organizations must maintain high availability as more mission-critical corporate networked resources are extended over a wide area.
- Organizations must extend multicast over a WAN without compromising service quality.

Selectively out-tasking network implementation and some aspects of the ongoing network management can help IT managers overcome these challenges, but does require attention to key areas of concern, including the following:

- **Quality of service (QoS)**—Today's networks must support consolidated data, voice, and video traffic, each of which places different requirements on the network. IT managers are constantly exploring options to ensure that their networks can handle the different types of traffic intelligently, boosting overall bandwidth and minimizing disruptions for users.
- **High availability**—Availability is increasingly important as enterprises deploy and rely upon networked mission-critical applications. Downtime that disrupts business operations is not an option. Systems that provide greater network reliability are required, while at the same time network failure and recovery must be transparent to users and applications.
- **Security**—Maintaining rigorous access controls in a shared infrastructure environment is essential. The service provider must safeguard all communications so that customer data remains private and protected in a shared environment.
- **Network management**—IT managers constantly need to be aware of their corporate network for anomalies, such as link failure, customer-premises-equipment (CPE) failure, or loss of connectivity. Network management also consists of capacity planning; provisioning; usage and billing; managing add, change, and delete operations; and monitoring performance metrics.
- **Multicast**—Network requirements to support multicast-dependent applications such as broadcast, music on hold, and video streaming place unique demands on a network. IT managers must anticipate and plan for how multicast applications can be supported over a WAN, how multicast can be extended to remote branches and teleworkers, and the number of multicast streams that can be supported simultaneously.
- **Support**—Supporting a corporate network and its users is a significant task for any IT organization, made more complex by the proliferation of mobile workers, teleworkers, and in-office personnel using a mixture of technologies, applications, operating systems, and communications channels. Inadequate user support invariably leads to unacceptable productivity and degrades network performance, directly affecting the strategic requirement to boost overall organizational competitiveness and operational excellence.

IP VPN TECHNICAL OVERVIEW

IP-based VPNs enable construction of private networks over a service provider-shared IP infrastructure or the Internet—providing significantly greater flexibility, reach, and scalability. Enterprise IT managers adopt IP-based VPNs to obtain the following capabilities:

- Deliver cost-effective and scalable wide-area connectivity over a shared network infrastructure.

- Build a foundation to deploy additional value-added, enhanced business applications.
- Enable convergence of existing disparate corporate data, voice, and video networks.
- Provide the ability to extend corporate networked resources to geographically dispersed branch offices, teleworkers, mobile workers, and business partners.
- Offer ubiquitous access.
- Support a broad spectrum of corporate network topologies, such as full mesh, national hub and spokes, or regional hubs and spokes.
- Improve scalability, flexibility, and manageability.
- Reduce configuration and provisioning time.
- Reduce installation time and complexity.
- Reduce network costs.

Two basic types of IP VPN services follow:

- Site-to-site VPNs
- Remote access VPNs

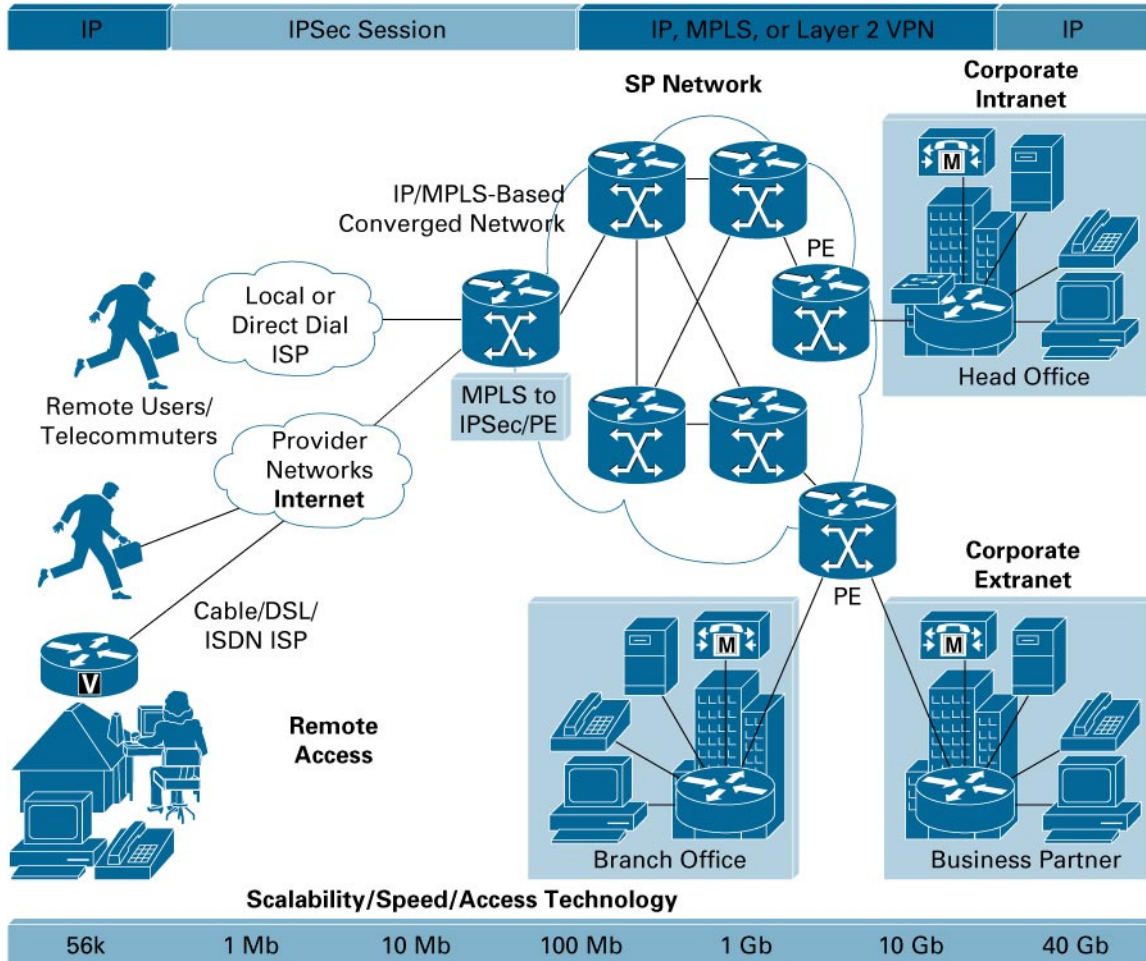
Both are applicable in the types of network operating environments that predominate in today's business enterprises, which are shown in Figure 1. The network operations can be either:

- On-net, where all enterprise sites, mobile workforce, or business partners are within a service provider's service area
- Off-net, where some enterprise sites, mobile workforce, or business partners are outside of a service provider's service area

IP VPNs also can be categorized by architecture as follows:

- Network-based IP VPNs—In a network-based VPN, the intelligence lies in a service provider's shared infrastructure, which offers integrated security, scalability, and end-to-end QoS. By adopting a network-based IP VPN, IT managers can take advantage of the service provider's investment in technology and scalability to extend networked corporate resources more cost effectively over a shared infrastructure to their branch offices, mobile workforce, and business partners.
- CPE-based IP VPNs—In a CPE-based IP VPN, the VPN intelligence resides in the equipment deployed at the customer access equipment, such as in a VPN-enabled router. The advantage of CPE-based IP VPNs is that they are independent of the underlying IP infrastructure, and therefore can be deployed across any existing IP network or the Internet.

Figure 1
Multiservice VPN Architectures



IP VPNs can be based on the following environments:

- Native IP
- Multiprotocol Label Switching (MPLS)
- IP Security (IPSec)
- A combination of these technologies

MPLS TECHNOLOGY

MPLS fuses the performance of switching with the intelligence of routing, providing significant benefits to networks with a pure IP architecture as well as those with IP and ATM or a mixture of other Layer 2 technologies. MPLS is often called a Layer 2.5 protocol because MPLS labels can encapsulate packets at Layer 3 (such as IP packets) and also frames at Layer 2 (such as ATM cells). MPLS-labeled packets can be carried across a variety of Layer 2 interfaces—ATM, Frame Relay, Point-to-Point Protocol (PPP), packet over SONET (POS), or Ethernet. Because MPLS allows service providers to maximize the efficiency of their shared infrastructures and rapidly respond

to any link or node failure, MPLS technology is critical to scalable VPNs and end-to-end QoS. MPLS traffic engineering and fast reroute can significantly improve the offered service-level agreement (SLA) for VPN customers by providing the ability to reroute traffic rapidly in failure conditions.

MPLS-BASED LAYER 3 VPNS

MPLS extends the capabilities of IP to enable very large-scale implementations of VPNs. MPLS-based Layer 3 VPNs use a peer-to-peer VPN model based on Border Gateway Protocol (BGP) as defined in the specification RFC 2547*bis* by the IETF L3VPN working group.

MPLS-based Layer 3 VPNs can support the present intranet and extranet communication needs of an enterprise, as well as future value-added applications. They also can create an intranet that links a corporate headquarters to remote offices over a shared, prioritized network and provide a cost-effective alternative to traditional leased-line, ATM, and Frame Relay technologies. MPLS-based VPNs can link the network resources of an enterprise with third-party vendors and business partners. MPLS-based VPNs provide the flexibility and any-to-any connectivity that links members of the VPN to each other—a requirement for extranets because of their dynamic nature.

With an MPLS-based VPN, IT organizations benefit from a variety of unique service features, such as:

- Scalable, any-to-any connectivity
- Advanced QoS features that ensure network priority for mission-critical traffic with guaranteed service levels
- Transparent integration of data, voice, and video traffic
- Simpler configuration, provisioning, and management
- IP Multicast, a technique for using bandwidth efficiently when sending routine or common information to multiple sites
- Support for a customer's private IP addressing scheme, including Network Address Translation (NAT) and Dynamic Host Configuration Protocol (DHCP) services
- Automatic failover features to assure high network availability
- Additional managed Internet access with security and privacy features such as integrated firewall and intrusion detection

The inherent security of MPLS-based VPNs has been proven to be equivalent to ATM- or Frame Relay-based VPN security. For more information about the specific security attributes of MPLS VPNs, refer to the Cisco Systems® 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.

IPSEC TECHNOLOGY

Based on open standards developed by the IETF IP Security Protocol working group, IPsec ensures confidentiality, integrity, and authenticity of data communications across an IP-based network. IPsec provides:

- Data confidentiality—Encrypts packets before transmission
- Data integrity—Authenticates packets to ensure that the data has not been altered during transmission
- Data origin authentication—Authenticates the source of received packets, in conjunction with data integrity service
- Antireplay—Detects aged or duplicate packets, rejecting them to avoid replay attacks

The IPsec standard also defines several new packet formats, such as encapsulating security payload (ESP), for confidentiality. ESP supports any type of symmetric encryption, including the standard 56-bit Data Encryption Standard (DES), the more secure Triple DES (3DES) standard, and the emerging Advanced Encryption Standard (AES). IPsec parameters are communicated and negotiated between network devices in accordance with the Internet Key Exchange (IKE) protocol.

IPSec functions at the network layer and is most applicable in network environments where there is a higher degree of exposure to breaches of data privacy and where IPSec mechanisms such as tunneling and encryption can best be applied. The IPSec protocol provides protection for IP packets by allowing network designers to specify the traffic that needs protection, define how that traffic is to be protected, and control who can receive the traffic.

IPSEC-BASED VPN

IP VPN services based on IPSec are typically deployed in a point-to-point, hub-and-spoke, or partially meshed topology over a service provider network or the Internet with an encrypted or authenticated tunnel. IPSec-based intranet or extranet VPNs require a CPE security appliance, such as an IPSec-enabled router or an IPSec-enabled firewall to support IPSec tunnels and encryption at each site.

IPSec VPNs replace or augment traditional VPNs based on traditional WAN infrastructures such as leased lines, Frame Relay, or ATM. IPSec VPNs surpass the requirements of traditional WAN alternatives by supporting multiple protocols, offering increased reliability, and also with greatly improved network security measures. The advantage of IPSec is that it meets network requirements more cost effectively and with great flexibility using today's most pervasive transport technologies:

- The public Internet
- Service provider IP backbones
- MPLS-based networks

With an IPSec-based VPN, enterprise organizations can take advantage of the primary strengths of this technology to achieve several key benefits:

- Security—IPSec VPNs help ensure data privacy with a flexible suite of encryption and tunneling mechanisms that protect packets as they travel over the network. Users are authenticated with digital certificates or preshared keys. Packets that do not conform to the security policy are dropped.
- Ease of deployment—IPSec VPNs support rapid deployment and additions because they can be provisioned across the Internet or any service provider IP-based network.
- Geographic breadth—IPSec VPN can be extended to provide ubiquitous global Internet access in addition to operating across the service provider-shared infrastructure, thereby greatly increasing the customer geographic reach for remote offices and mobile workers of an enterprise worldwide.

LAYER 2 VPN

IT managers also can cost-effectively deploy a corporate wide area network with the emerging Layer 2 VPN that is offered by service providers on an IP- or MPLS-based infrastructure. Layer 2 VPNs include:

- Layer 2 transport—Layer 2 service that provides Layer 2 point-to-point connectivity (such as Frame Relay data link connection identifier [DLCI], ATM virtual path identifier/virtual connection identifier [VPI/VCI], and point-to-point Ethernet) across an IP- or MPLS-enabled IP network
- Virtual private LAN service (VPLS)—Layer 2 service that emulates LAN across an IP- or MPLS-enabled IP network, allowing standard Ethernet devices to communicate as if they were connected to a common LAN segment

Cisco® Any Transport over MPLS (AToM), a Cisco implementation of MPLS-based Layer 2 VPN and Layer 2 Tunneling Protocol Version 3 (L2TPv3), helps enable a service provider to offer Layer 2 VPN service. AToM is a Cisco product-based solution for transporting Layer 2 packets over an MPLS backbone. It helps enable enterprise customers to connect among their sites with existing data link layer (Layer 2) networks through a packet-based network infrastructure. AToM provides a common framework to encapsulate and transport supported

Layer 2 traffic types over an MPLS network core. Many service providers support a single, converged MPLS network infrastructure to offer connectivity for supported Layer 2 traffic and for IP traffic in Layer 3 VPNs.

VPLS is a class of VPN that supports the connection of multiple sites in a single bridged domain over a managed IP or MPLS service provider’s shared infrastructure. VPLS presents customers an Ethernet interface, simplifying the LAN-to-WAN boundary and helping enable rapid and flexible service provisioning, because the service bandwidth is not tied to the physical interface. All services in a VPLS appear to be on the same LAN, regardless of location. VPLS uses service provider edge routers that can learn bridging and replicate on a VPN basis. These routers are connected by a full mesh of tunnels within a service provider network, enabling any-to-any connectivity.

L2TPv3 is a solution for transporting Layer 2 packets over a service provider native IP network. L2TPv3 is a viable alternative for supporting traditional services over IP infrastructures and for supporting several new connectivity options, including Layer 2 VPNs and Layer 2 virtual leased lines.

INTEGRATING IPSEC WITH MPLS VPNS

MPLS- and IPsec-based VPNs are complementary rather than competitive. When used in combination, MPLS and IPsec give IT manager’s greater flexibility and capability to extend corporate networked resources securely and ubiquitously. For example, business customers can use the IPsec-based VPN for off-net traffic that needs strong authentication and confidentiality and link these VPNs directly to corresponding MPLS VPNs within a service provider’s core network to take advantage of their extended connectivity, traffic engineering, and QoS.

The Cisco Network-Based IPsec VPN solution helps service providers enable business customers to map authenticated IPsec sessions directly into corresponding MPLS VPNs. IT managers can, therefore, securely extend their corporate networked resources far beyond the boundaries of a service provider’s service area by using the Internet or a service provider’s partner networks. Business customers gain the ability to securely connect their remote offices, telecommuters, and mobile users from anywhere to the corporate network. See Table 1.

Table 1. VPN Summary

Service Types	Intranet	Extranet	Access Speed	Technologies
Site-to-site VPN	Interconnects enterprise sites over a service provider-shared infrastructure or the Internet	Interconnects enterprise network resources with third-party vendors and franchise and business partners	Fractional T1, T1, fractional T3, T3, OC-3, OC-12 EMEA: E1, E3, STM-1, and STM-4	Network-based MPLS Layer 3 VPN Network-based Layer 2 VPN CPE-based IPsec VPN IPsec-over-MPLS VPN
Remote access VPN	Interconnects telecommuters, mobile workers, and day extenders to their corporate network resources over a service provider-shared infrastructure or the Internet	Interconnects enterprise network resources with mobile workers from third-party vendors and franchise and business partners	56K dial, broadband high-speed xDSL, ISDN, cable, wireless	IPsec software or hardware client PPPoX, L2TP, Point-to-Point Tunneling Protocol (PPTP) clients IPsec end to end IPsec integration to MPLS VPN IPsec integration to Layer 2 VPN

OUT-TASKING VPN SERVICE MANAGEMENT

IT managers who decide to adopt IP VPN can design, build, provision, support, and manage the VPN using in-house resources or selectively or totally out-task to a managed service provider. The decision affects IT workload, capital expenditure, and ongoing operational expenses and can potentially affect service availability, network security, and QoS.

According to Gartner Dataquest, most Fortune 1000 companies are presently out-tasking or planning to out-task the management and support of their corporate network. For midsize businesses in the United States and Canada, 41 percent and 23 percent, respectively, are planning to out-task; and for small businesses in the United States and Canada, 12 percent and 13.5 percent will out-task (source: Gartner Dataquest, *Managed Services Uncovered: North America*, July 2002).

Incentives for IT managers to out-task VPN service management include the following:

- Free resources to focus on strategic IT initiatives—By working with a service provider for managed IP VPN services, IT managers can delegate the routine tasks they do not see a compelling reason to control, such as daily monitoring, support, provisioning, transport, and router maintenance (refer to the sidebar). At the same time, they free staff resources to focus on the core business as well as strategic IT initiatives such as network design and planning.
- Reduce costs—Gartner Dataquest reports that large enterprises in the United States that out-task network management to service providers cut their network costs by as much as 25 percent, whereas small U.S. businesses can experience up to 15-percent cost reductions. In fact, access to the service provider's lower cost structure—the result of a greater economy of scale—is one of the most compelling tactical reasons for out-tasking, according to The Outsourcing Institute of Jericho, New York (<http://www.outsourcing.com/>).
- The service provider can deliver services more economically than in-house IT departments would otherwise spend for operations, maintenance, service, equipment, and technology upgrades.
- Manage costs—Companies that out-task network management not only reduce their costs, they also make recurring costs more predictable by shifting from a variable to a fixed-cost model. Businesses that out-task know their monthly costs in advance, as compared to businesses that need to find the budget for unexpected expenses related to network upgrades, outages, equipment malfunction, and technical training. Out-tasking also enables “pay-as-you-grow” scalability, eliminating the need to overpurchase at the outset of service deployment to accommodate anticipated growth.
- Gain expertise and support not available in house—IT managers often can obtain networking skills not always available internally within the enterprise. The value of this benefit increases as companies deploy more networked applications and add more users and as network management becomes more complex. Service providers have the resources to offer 24-hour round-the-clock monitoring, management, and support—capabilities not readily available in house to all but the largest enterprises. Service providers also can offer rapid deployment because of their experience. Even for companies with large in-house staffs, service providers can fill critical resource gaps such as network security, which typically requires special training, expertise, and full-time resources.

In a 2003 report, the Yankee Group summarized the technical benefits experienced by several companies that used a managed IP VPN service provider (refer to sidebar on following page).

It is good practice to be selective when out-tasking. A methodology that the Cisco IT department employs to analyze networking tasks and determine which ones are suitable for out-tasking is shown in Figure 2. Cisco IT prioritizes networking activities by how closely linked they are to the company's competitive stance, as follows:

- Core—An activity that contributes to the competitive advantage of the company
- Context—An activity that does not contribute to the competitive advantage of the company

Following are IP VPN service management components that businesses can consider out-tasking:


- Managed customer-edge equipment
- Managed network security
- Telecommuter services
- Internet-access integration
- Secure off-net access
- Site-to-site encryption services
- Managed extranet services
- Real-time physical and logical monitoring (event logs, trunk usage, call detail, resource usage, etc.)
- Maintenance of router configuration and upgrades
- Performance management and optimization (jitter, round-trip delay, packet loss, circuit availability, network availability, WAN link, and router usage)
- Fault identification, network management, and resolution with managed backup connectivity for critical sites
- Configuration or change management
- Auditing or asset management
- Maintenance and help desk support services

Next, activities are prioritized by how closely the activity is linked with the company's mission.

- **Mission-critical**—An activity that, if performed poorly, would immediately put the company at risk
- **Non-mission-critical**—An activity that, if performed poorly, would not immediately put the company at risk

Networking activities that are not closely associated with the company's competitive stance and mission are ideal candidates for out-tasking to a third party such as a service provider, especially if performing these activities consumes resources that could otherwise be deployed to focus on strategic IT initiatives.

Figure 2
Four-Quadrant Out-Tasking Analysis Tool

	<p>Core Any Activity That Contributes to Competitive Advantage for the Company</p> <p>Engage</p>	<p>Context Any Activity That Does Not Contribute to Competitive Advantage for the Company</p> <p>Disengage</p>
	<p>Mission-Critical Any Activity That, if Performed Poorly, Would Pose an Immediate Risk to the Company</p> <p>Control</p> <ul style="list-style-type: none"> • Integrated Voice, Video, and Data • Web Services Cisco.com • Enterprise Solutions Management 	<ul style="list-style-type: none"> • ERP/Cisco Resource Manager • Larger Server Support • Hardware Support
	<p>Non-Mission-Critical Any Activity That, if Performed Poorly, Would Not Pose an Immediate Risk to the Company</p> <p>Entrust</p> <ul style="list-style-type: none"> • New Technologies • New Service Models 	<ul style="list-style-type: none"> • Proven Technology: IP VPN, IP CDN, IP Telephony • PC Desktop • Router, Static Content Management

The most effective approach to out-tasking is to:

- Be selective about out-tasking
- Know the business process, architecture and retain that intelligence
- Maintain control of the out-tasked areas

MANAGED IP VPN FEATURES AND BENEFITS TO IT MANAGERS

The benefits realized by IT managers who selectively out-task network implementation and some aspects of the ongoing management of their network to a qualified service provider are summarized in Table 2.

Table 2. Managed IP VPN Features and Benefits to IT Managers

IP VPN Features	Business Customer Benefits
Fully managed network service	<ul style="list-style-type: none"> • IT managers can focus on core competencies and strategic IT initiatives, not mundane daily network operations. • The cost and hassle of designing, deploying, and maintaining a private WAN is eliminated. • Intensive networking training requirements and operational costs are reduced. • Service providers can manage the network and provide a 24-hour help desk for comprehensive support.
Control	<ul style="list-style-type: none"> • Out-tasking VPN does not mean relinquishing in-house control over core, mission-critical business processes. • IT managers continue to maintain control of workflow internally. • IT managers with in-house networking expertise can determine where control is desirable and where out-tasking support can free time and resources to devote to widespread infrastructure management and strategic IT initiatives.
Scalability	<ul style="list-style-type: none"> • Managed IP VPN offers greater scalability and cost reduction when adding new sites and users in response to business growth or changes. • Managed IP VPN services enable enterprises to expand capacity without incurring capital expenditure. • Fast provisioning enables connection of new sites, additional users, and new applications.
Affordability	<ul style="list-style-type: none"> • Capital equipment expenditures can be eliminated. • Installation and monthly recurring costs are predictable. • Managed IP VPNs are less expensive and quicker to install when compared to traditional Frame Relay or ATM. • Managed IP VPNs enable IT managers to reduce network implementation, maintenance, and monitoring expenditures, as well as connectivity charges. • Managed IP VPN services are affordable also for small and medium-sized businesses where they can gain cost reductions by out-tasking management of dialup access, equipment, and maintenance.
Availability	<ul style="list-style-type: none"> • High network availability is possible. • Corporate network downtime is minimized. • Service providers can guarantee network reliability of up to 99.999 percent, depending on the subscribed level specified in the SLA. • Managed IP VPNs offer access to mobile and telecommuting workforce, while simplifying remote access management.
Consolidation	<ul style="list-style-type: none"> • Data, voice, and video can be consolidated. • Integration with existing infrastructure is transparent, while offering support on data, voice, and video traffic in a converged network environment. • Managed IP VPNs enable advanced multimedia applications. • Customers enjoy lower costs compared to services from multiple networks or providers.
Access	<ul style="list-style-type: none"> • Managed IP VPNs support a broad range of available access options, bandwidth speeds, and technologies (such as analog dial, ISDN, xDSL, cable, and wireless). • Access for intranet, extranet, and mobile workers is ubiquitous. • Managed IP VPNs enable remote users to securely access corporate network services.

IP VPN Features	Business Customer Benefits
Security	<ul style="list-style-type: none"> • Optional security protection includes firewalls, public key infrastructure (PKI), and intrusion detection, as well as access control lists, packet filtering, spoof proofing, digital certificates, advanced encryption, and authentication to protect data from unauthorized access. • Security monitoring and rapid response from a qualified service provider 24 hours per day helps to provide additional security to corporate network resources, applications, and communications. • Defined access control based on private security policy determines which users can access designated portions of the network.
Reporting and billing	<ul style="list-style-type: none"> • Detailed reporting and billing provide records of VPN usage and associated cost.
Supply chain automation	<ul style="list-style-type: none"> • Managed IP VPNs improve the service provider's ability to do business with branch offices, customers, suppliers, and business partners. • Total costs are manageable.
Single point of contact	<ul style="list-style-type: none"> • Managed IP VPNs eliminate the burden and complexity of dealing with and managing multiple vendors.

OUT-TASKING VPN SERVICES—DECISION TREE

Determining the type and scope of managed VPN services a business can out-task requires a rigorous assessment of the organization's current and future status and networking requirements. The analysis should encompass the business's objectives and networking challenges, current network infrastructure configuration, bandwidth and performance requirements, future plan to deploy additional services, timeline, and security.

ASSESSING EXISTING NETWORKS

Assessing network requirements in support of business objectives is an important first step toward finding a service provider that can complement internal IT resources and reduce overall network support costs.

When an enterprise corporate network is very large and highly distributed, IT managers may not always have a comprehensive understanding of the technologies and systems that are actually in place throughout an organization. This can occur for several reasons, such as company mergers, ongoing changes, a tradition of local decision-making for technology, or the time and cost of sending staff into the field to track network assets that have already been in place for years.

Table 3 can be used as a guide to review an organization's existing network status and support requirements, and determine which service areas could be out-tasked.

Table 3. Assessing Network Requirements

		Network Requirements	Check Your Network Requirements √
1.	Network objectives	<ul style="list-style-type: none"> • Reduce costs. • Implement security measures. • Replace traditional dialup infrastructure. • Consolidate disparate networks (data, voice, and video). • Extend corporate network resources to remote workers or business partners. • Plan for disaster recovery. • Deploy new IP-based applications. • Attain wide-area networking capability. • Replace existing Frame Relay or ATM. • Improve scalability. 	
2.	Network services	<ul style="list-style-type: none"> • Security • Networking – Intranet • Networking – Extranet • Networking – Remote access • Quality (QoS) • Managed value-added services, for example, voice, security, unified messaging, hosting, content distribution, etc. • Authentication • Reporting management • Provisioning management • Administrative management 	
3.	Bandwidth (consider both headquarters and remote and branch offices)	<ul style="list-style-type: none"> • Fractional T1 • T1 • OC-3/STM-1 • OC-12/STM-4 • OC-48/STM-16 • More than OC-48 	

SELECTING A SERVICE PROVIDER

Choosing the right service provider is vital. The network assessment given in Table 4 provides a starting point for discussions with managed service providers.

Table 4. Assessing a Service Provider

Service Provider Ability			Check Your Requirements
1.	QoS	<ul style="list-style-type: none"> • Ability to handle data, voice, and video traffic and associated networked mission-critical applications • Low latency and packet loss • Classes of services • Performance metrics • 24-hour support • Accurate billing and reporting 	√
2.	Service uptime	<ul style="list-style-type: none"> • Network redundancy • Fast reroute and convergence in event of failure • Network recovery transparent to users and applications • Traffic engineering that can efficiently and reliably route traffic 	
3.	Security options	<ul style="list-style-type: none"> • Data encryption • Intrusion detection • Firewall protection • 24-hour security monitoring 	
4.	Management	<ul style="list-style-type: none"> • Performance management • Fault management • On-time provisioning, flexibility to add, remove, or change users or sites 	
5.	Multicast	<ul style="list-style-type: none"> • Support over VPN • Support for branch and remote workers • Number of simultaneous streams supported • IP Multicast 	

Cisco also can help businesses choose a managed service provider. Cisco recommends providers that deliver their services over networks built end to end with Cisco equipment, technologies, and solutions and that meet Cisco support standards. Businesses can find these providers by looking for the Cisco Powered logo in the provider’s promotional materials, or by visiting the Cisco Powered Network search tool at <http://www.cisco.com/cpn>.

Nearly 400 service providers in 60 countries have qualified for this designation. They offer a wide range of advanced managed services for small to large businesses. Whether you are considering outsourcing your security, virtual private networking, or other networking needs, these are providers that you can trust with your company’s critical business functions.

IT MANAGERS NETWORKING STRATEGIES

Creating an effective partnership between internal and external resources requires balancing networking strategies and service options. Table 5 summarizes best practices in achieving this balance.

Table 5. Networking Strategies

	Networking Strategy	Managed VPN Service Options
Enterprise business	<ul style="list-style-type: none"> • Extend the corporate WAN. • Enable secure remote access to corporate applications. 	<ul style="list-style-type: none"> • Managed customer-edge equipment • Managed extranet services • Real-time monitoring • Network-based VPN for scalability
	<ul style="list-style-type: none"> • Ensure ongoing cost savings and scalability, and accommodate growth, merger, or consolidation. 	<ul style="list-style-type: none"> • Configuration of change management • Performance management and optimization
Small to midsize business	<ul style="list-style-type: none"> • Deliver increased bandwidth for remote users and the ability to add new users and sites quickly. 	<ul style="list-style-type: none"> • Telecommuter services • Internet-access integration
	<ul style="list-style-type: none"> • Improve security, quality, and ease of management. 	<ul style="list-style-type: none"> • Managed network security • Maintenance of router configuration and upgrades • Managed network- or CPE-based VPN services

FOR MORE INFORMATION

Refer to the managed VPN services eTour at <http://www.cisco.com/go/managedservices>.

Look for Cisco overviews on additional managed services that are based on Cisco products and solutions:

- Cisco Security Services
- Cisco Business Voice Services
- Cisco Metro Ethernet Access Services

“The Move to MPLS-Based VPNs: Exploring Service Options”:

http://www.cisco.com/application/pdf/en/us/guest/netsol/ns193/c654/cdccont_0900aec800f6d9a.pdf.

iQ Magazine, managed services article:

http://business.cisco.com/prod/tree.taf%3Fasset_id=88779&MagID=88873&public_view=true&kbns=1.html.

“From Frame Relay to IP VPN Migration”:

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

Outsourcing guide (Cisco Powered Network):

http://www.cisco.com/warp/public/779/servpro/cpn/benefits/Cisco_Outsourcing_Guide.pdf.

**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 Website 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

Copyright © 2004 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0406R) He/LW6620 06/04