SERVICE OVERVIEW

MANAGED IP VPN SERVICES FOR ENTERPRISE ORGANIZATIONS

EXECUTIVE SUMMARY

Many e-business initiatives such as workforce optimization, customer care, e-commerce, and corporate communication often depend on unprecedented levels of network access and agility. Pursuing these initiatives requires complex networking, dedicated IT resources for 24-hour monitoring and management, and cost-effective integrated voice and data services. In the face of these demands, many large businesses are reassessing their corporate networking infrastructures and seriously considering out-tasking alternatives, such as carrier-managed public networking solutions. Service providers offering managed IP VPN services can help your business meet today's challenges.

High-speed network connectivity, greater reliability, security, and management make IP-based VPNs viable for supporting a range of enhanced services, such as IP telephony, videoconferencing, e-commerce, and content hosting. Service providers offering managed IP VPN services also enable large businesses to extend corporate resources to mobile workers, small branch locations, and partners.

Effective VPN solutions are available whether you proceed with in-house deployment or partner with a service provider. This document provides a basic overview of managed IP VPN services, VPN business requirements, VPN service types that are available for enterprise organizations, several VPN case studies, and tools to assess your network and your service provider.

Finding the right VPN solution for your organization begins with assessing and prioritizing your unique requirements, as well as becoming informed about your alternatives and some of the key decision points. This service overview provides a starting place. More in-depth information about IP VPN services and technology is available at:

http://www.cisco.com/go/managedservices

including an e-tour discussing the features and benefits of managed services. You may also speak directly with a Cisco Systems® representative or a service provider that is a member of the Cisco® Powered Network Program by visiting:

http://www.cisco.com/cpn

MARKET OVERVIEW

IP-based VPNs are enabling enterprise organizations to contain costs, improve security, and gain greater access and availability while enhancing their business processes and best practices. IP VPNs can deliver reliable, ubiquitous, businesswide connectivity over a shared network infrastructure, using the same access policies as private networks. Large businesses are turning to IP VPNs to cut costs, reduce dialup infrastructure, and boost network security. They also are taking advantage of faster network performance and VPN-enabled applications such as voice over IP (VoIP).

IP VPNs can also enable cost-effective, secure remote access to a corporate network. Many large enterprise organizations have substantial numbers of mobile workers and telecommuters. It is now a necessity to provide employees, business partners, and customers with immediate access to relevant business data and applications while ensuring privacy and security. Remote-access VPNs securely connect telecommuters and mobile users to corporate intranets and extranets over dialup, ISDN, broadband, and wireless technologies.

While IP VPNs have clear value for enterprise organizations, the base infrastructure can be costly to build out and manage. For this reason, service providers offer options to supply not only the VPN network infrastructure and ongoing management, but also a full range of other VPN-enabled services. By partnering with a service provider, you can realize the benefits of a VPN network and stay focused on your core competencies. Gartner Dataquest forecasts *(IP VPN Hitting the Big Time [2003])* that by 2006 nearly all large U.S. enterprises will use enhanced IP services (including IP VPNs) in some parts of their network, and at least 20 percent of these enterprises will have replaced their Frame Relay networks with these services.

Forrester Research reports that costs can be reduced by as much as 60 percent when businesses utilize the global shared carrier infrastructures of VPNs *(Choosing the Right VPN, Forrester Research [2003]).* Service providers offering managed IP VPN services bring dedicated expertise and a carrier-class, scalable network infrastructure along with 24-hour monitoring and management to the VPN service portfolio, helping ensure peace of mind and reliability for their regional and global business customers.

VPN SERVICES DESCRIPTION

Virtual private networks are constructed over a shared or public infrastructure that uses a range of technologies to help ensure reliability, traffic separation, and data privacy. A VPN can be built on the Internet or on a service provider's infrastructure. VPNs can offer businesses the same security, quality of service, reliability, and manageability of private networks.

A service provider can help you assess your business communications requirements and determine the appropriate managed IP VPN solutions for your organization. Table 1 outlines basic managed IP VPN service types for site-to-site and remote access networking needs, and categorizes them by intranet and extranet networks and access speeds.

Table 1. Basic VPN Service Types

Service Type	Intranet	Extranet	Access Speed
Managed site-to-site IP VPN	• Interconnects enterprise sites over a service provider shared infrastructure • Connects main and branch office locations using always-on connections to a third-party network or the Internet	• Connects enterprise network resources with third-party vendors, franchise, and business partners • Provides business partners with limited access to specific portions of the company network for collaboration and coordination	56k, fractional T1, T1, fractional T3, T3; OC-3, OC-12; EMEA: E1, E3, STM-1, STM-4
Managed remote-access IP VPN	• Connects telecommuters, mobile workers, and day extenders to their corporate network resources over a service provider shared infrastructure	• Interconnects enterprise network resources with mobile workers from third-party vendors, franchise, and business partners	56k dial, broadband high-speed xDSL, ISDN, cable, wireless

IP VPNs have two distinct architectures:

- Network-based IP VPNs: The VPN intelligence is in the service provider network and is generally completely transparent to users. By using a network-based architecture, service providers can reduce the scaling complexity and cost of delivering VPN services to customers.
- Customer premises equipment (CPE)-based IP VPN: The VPN intelligence is in the network access equipment at the customer's sites. A single class or multiple classes of service may be implemented across the WAN, depending on the capability of the service provider's network infrastructure.

An IP VPN provides a foundation for additional value-added services including managed security and extranet services, Webcasting, voice, and more. A service provider works with you to determine the basic and enhanced services that best fit your current needs and growth requirements.

BUSINESS REQUIREMENTS

You may choose to out-task part or all of your corporate networking requirements to service providers, which offer management and maintenance of connectivity, access routers, network security, enhanced value-added services, and support. Cost control is frequently a primary objective when organizations make this decision. Table 2 outlines the various features and benefits of managed IP VPNs.

Table 2. Managed IP VPN Features and Benefits

IP VPN Features	Enterprise Customer Benefits
Fully managed network service	• Enterprises can focus on core competencies rather than network operations • Eliminates cost and problems associated with designing, deploying, and maintaining private WANs • Reduces networking training requirements and operational costs • Service provider manages network and provides 24-hour help desk for comprehensive support
Control	• Customer need not relinquish in-house control over core business processes • Organizations can arrange with service providers to maintain their own control of workflow • Businesses with in-house IT expertise can determine where control is desirable and where service provider support can free time and resources
Scalability	• IP VPN service scales easily to as many sites and users as needed in response to business growth or changes • Enterprises can expand capacity without incurring capital expenditure • Fast provisioning to connect new sites, users, and applications
Affordability	• Can reduce capital equipment expenditures • Predictable installation and monthly recurring cost • Less expensive (and quicker to install) than legacy Frame Relay/ATM service • Can reduce expenditures on network implementation, maintenance, monitoring, and connectivity charges • Using ubiquitous Internet or third-party IP transport to connect remote workers and offices can eliminate expensive dedicated WANs and dialup access infrastructures • Local dial numbers further reduce access charges
Availability	• Helps ensure high availability • Helps prevent network downtime • Service providers can guarantee network reliability up to 99.999 percent as stipulated in the service-level agreement (SLA) • VPNs offer access to a mobile workforce while simplifying remote access management

IP VPN Features	Enterprise Customer Benefits
Consolidation	• Data, voice, and video consolidation • Providers can configure an IP VPN that integrates with existing infrastructure • Enables advanced multimedia applications • Costs are lower than with services from multiple networks or providers • Reduces capital equipment expenditure
Access	• Supports a wide variety of available access options, bandwidth speeds, and technologies (such as analog dial, ISDN, cable, wireless, and DSL) • Ubiquitous access to intranet, extranet, and Internet resources • Allows remote users to securely access corporate networked services
Security	• Essential security protection including firewalls, public key infrastructure (PKI), and intrusion detection, as well as access control lists, packet filtering, spoof proofing, digital certificates, advanced encryption, and authentication protocols to protect data from unauthorized access • 24-hour monitoring and rapid response provides 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	• Detailed reporting and billing provide records of VPN usage and monitoring
Supply chain automation	• Improve ability to conduct business with branch offices, customers, suppliers, and partners • Manage total costs
Single point of contact	• Eliminates burden and complexity of managing multiple vendors

BUSINESS SUCCESS STORIES

GWR Group plc, the United Kingdom's most listened-to commercial radio group, migrated from a Frame Relay network to a Multiprotocol Label Switching (MPLS) VPN that included multicast capability along with the support of its corporate voice telephony, data, and real-time broadcast audio flows. This VPN delivers the quality of service (QoS) required by GWR Group to prioritize radio broadcast streams with the network efficiency of multicast, where the source sends content out across the network only once with receiving stations opting in and out of the stream as appropriate. http://www.cisco.com/en/US/solutions/collateral/ns340/ns414/ns465/net_customer_profile0900aecd801a9e88.pdf

Jones Lang LaSalle, a global provider of real estate and investment management services, replaced its existing Frame Relay network with a managed MPLS VPN service. The new service enables Jones Lang LaSalle to transform the way its global infrastructure and IT assets are exploited and managed on an international basis.
http://www.cisco.com/application/pdf/en/us/guest/netsol/ns465/c647/cdccont_0900aecd801aa039.pdf

The **Van Wijnen Group**, a Netherlands-based real estate development and construction company, migrated to IP VPN in conjunction with a businesswide adoption of new enterprise resource planning (ERP) construction software. The software required a more flexible any-to-any network than the firm's existing leased lines could support. After rejecting a Frame Relay solution because of excessive latency, Van Wijnen selected an MPLS-based service that meets the low latency tolerance required for its applications. The company rolled out its new managed IP VPN network across 20 sites, including its headquarters and branch offices, and is confident about the success of the IP VPN solution.
http://www.cisco.com/en/US/netsol/ns465/networking_solutions_customer_profile0900aecd801aa3f5.html

DECISION POINTS

The type and quantity of managed IP VPN services your business out-tasks depend on your business objectives and challenges, current infrastructure configuration, bandwidth and performance requirements, and the desire to deploy additional network services supported by IP VPN.

The material presented in Table 3 and Figure 1 can provide a starting place for you to decide if you should adopt a managed VPN service. Table 4 provides a checklist to assess whether your service provider has the ability to meet your business and technical requirements for a managed IP VPN service.

Table 3. Assessing Your Network Requirements

		Check Your Requirements
Network objectives	• Reduce costs • Implement security measures • Replace dialup infrastructure • Consolidate disparate networks (data, voice, video) • Provide remote access to employees and business partners • Plan for disaster recovery • Deploy new IP-based applications • Attain primary WAN service • Replace existing Frame Relay/ATM service with IP VPN • Improve scalability	
Network services	• Security • Networking—intranet • Networking—extranet • Networking—remote access • QoS • Application • Authentication • Reporting management • Provisioning management • Administrative management	
Bandwidth (consider both headquarters and remote/branch offices)	• Fractional T1 • T1 • OC-3/STM-1 • OC-12/STM-4 • OC-48/STM-16 • More than OC-48	

Figure 1

Decision Tree for Evaluating Networking Requirements and Managed IP VPN Services

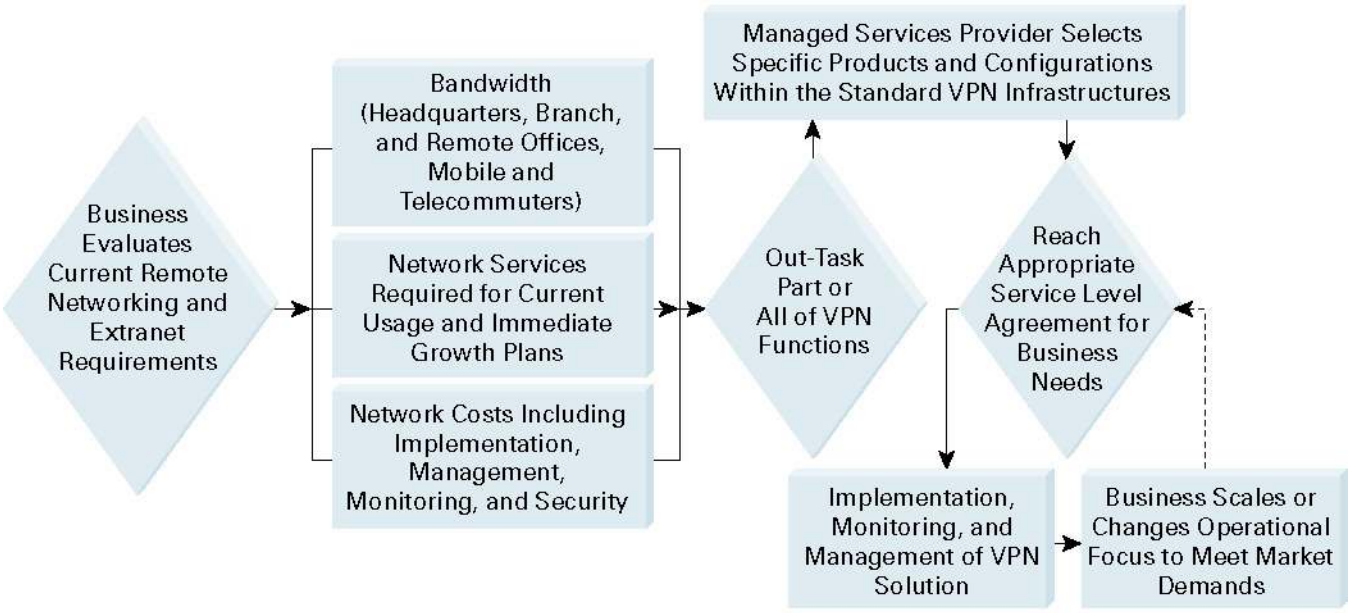

Table 4. Assessing Your Service Provider

		Check Your Requirements
QoS	• Ability to handle voice, video, data, and multiple applications • Low latency and packet loss • Classes of services • Performance metrics • 24-hour support • Accurate billing and reporting	
Service uptime	• Network redundancy • Fast reroute and convergence in the event of failure • Network recovery transparent to users and applications • Traffic engineering	
Security	• Data encryption • Intrusion detection • Firewall protection • 24-hour security monitoring	
Management	• Performance management • Fault management • On-time, flexible add, move, change	
Multicast	• Support over IP VPN • Support for branch and remote workers • Large number of simultaneous streaming users • IP multicast	

OUT-TASKING STRATEGIES

Typically, enterprise-level IP VPN services must support strong security and complex network designs, as shown in Table 5. At the same time, IP VPNs should ensure continuing cost savings and scalability. Large enterprises commonly take a selective approach to out-tasking, retaining control of their network and only outsourcing network elements that they cannot cost-effectively manage by themselves.

Table 5. Business Strategies

Networking Strategy	Managed VPN Services Options
Extend existing network infrastructure to enable secure remote access to corporate applications	• Managed customer-edge equipment • Managed extranet services • Real-time monitoring • Network-based VPN for scalability
Help ensure ongoing cost savings and scalability in the event of growth or downsizing	• Configuration of change management • Performance management and optimization

FINANCIAL ANALYSIS

Out-tasking managed VPN services can bring distinct cost benefits compared to current networking, management, monitoring, and connectivity expenditures. Savings can be realized from the service provider's economies of scale, deployment, support, and expertise. Cost advantages to businesses include:

- Lower implementation and infrastructure costs
- Lower connectivity charges for network access worldwide
- Lower costs for increased 24-hour VPN network monitoring and support
- Lower security costs, with enhanced, state-of-the-art security coverage
- "Pay as you go" scalability

If your managed service provider is a member of the Cisco Powered Network Program, ask that it help you calculate VPN return on investment (ROI) with the Cisco Total Cost of Ownership (TCO) tool.

CISCO POWERED NETWORK DESIGNATION

Since 1997 Cisco has awarded the Cisco Powered Network designation to service providers that deliver their services over a network built end to end with Cisco products and technologies and that meet Cisco standards for network support.

Companies that select a service provider with a Cisco Powered Network designation know that their services are delivered over the same high quality Cisco equipment that powers their own networks.

For companies seeking a provider of multiservice IP VPN services for real-time traffic such as voice and video, the Cisco Powered Network designation provides even more assurance. Providers qualifying for this certified service have passed a QoS assessment that measures delay, latency, and jitter. These are critical factors for delivering high-quality real-time voice and video services.

To identify services with a Cisco Powered Network designation, look for the following logo on the service provider's advertisements and other promotional materials.

CISCO POWERED LOGO

Nearly 400 of the most successful service providers worldwide are members of the Cisco Powered Network Program. They offer a wide range of network-based services—over networks built with Cisco products and solutions—for small and large businesses alike.

FOR MORE INFORMATION

To learn more about managed VPN services, view the Cisco managed services e-tour, or locate a designated Cisco Powered Network service provider, visit: http://www.cisco.com/go/managedservices

You can read additional Cisco service overviews about other managed services that take advantage of Cisco products and solutions including:

- Security services
- Business voice services
- Metro Ethernet access services

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

DM/LW7716 01/05

Printed in the USA