

# Virtual **Private** Networks: Your **Guide** to the **New World** Opportunity



It's a New World in networking. The advent of the 21st century invites new ways of thinking about global networks. We are on the brink of a huge transformation as service providers seek to meet customer demand for global network services by building carrier-scale, intelligent networks.

Along with the tremendous new capabilities that the New World network offers business customers, Cisco Systems sees a New World of how service providers do business. A world that displaces the "old-world" approach of providing only raw connectivity and competitively priced bit-pipes. In the old world, networks emphasized lower-level transport such as leased lines and Frame Relay. In the New World, service providers team with business customers to run a portion, or all, of their networks. Business customers want support for intranet and extranet applications to integrate data, voice, and video traffic securely over dedicated Virtual Private Networks (VPNs). They also require Access VPN options, including dial, digital subscriber line (DSL), cable, and wireless, to allow remote users to securely access a corporate intranet through the shared infrastructure.

New World providers increasingly offer customers complete service solutions tailored to their particular businesses. VPNs are an excellent example of New World services that benefit both service providers and business customers. By addressing unique customer needs, service providers can capture and hold new business. These value-added services represent service providers' best profit opportunities for the future.

With its experience in building the Internet, the world's largest Frame Relay networks, and thousands of enterprise networks, Cisco is uniquely positioned to help service providers build intelligent networks that create new revenue opportunities through the development of value-added services that businesses want today. Cisco is the only vendor that provides the equipment and software for consumers, business customers, and service providers to enable end-to-end intelligent networks. With its leading VPN solutions, Cisco joins service providers and subscribers to create a seamless network and a successful partnership.

—Larry Lang  
Vice President, Service Provider Marketing  
Cisco Systems, Inc.

**“Developing the New World network gives Telenor Telecom a unique opportunity to bring our customers into the modern world of communications,”—Per Bjork, Chief Technology Officer, Nextra**

### **Services for the New Millennium**

VPNs are the cornerstone of New World services. When properly implemented, they can streamline network operations while reducing capital expenses. This fundamental shift in strategy opens opportunities for continued growth, increased profitability, and the utmost efficiency for both service providers and subscribers. In the old world, service providers emphasized lower-level transport, such as leased lines and Frame Relay. In the New World, service providers team with business customers to meet their networking requirements through VPNs.

Companies that formerly handled their own communications requirements are partnering with service providers that can help develop, grow, and manage their networks on a global scale. For most of them, the starting point is to connect widely dispersed workgroups in an efficient, cost-effective manner. From there, service providers use the core technology as a foundation for offering incremental services such as packet telephony, videoconferencing, e-commerce, and content hosting.

The payoff is substantial: Service providers become trusted experts on their customers’ inter- and intrabusiness communications needs, enjoying increased revenue while differentiating themselves in a highly competitive—and lucrative—marketplace. VPNs help service providers build customer loyalty while delivering network services that are fundamental to their customers’ business operations.

### **Leading the Charge toward New World Services**

Many service providers are working with Cisco to build and manage VPNs, laying a foundation for the types of business applications that companies need to thrive in the Internet economy. Cisco offers a complete range of carrier-class, fully manageable VPN solutions, of which service providers can take advantage to offer services tailored to subscriber needs. The comprehensive Cisco VPN offering enables service providers to deploy three distinct services across a common infrastructure:

- Access VPNs, which securely connect telecommuters and mobile users to the corporate intranet and extranet over dial, ISDN, wireless, and cable technologies
- Intranet VPNs, which link corporate headquarters to remote offices over a shared, prioritized network
- Extranet VPNs, which extend these services outside the organization to link customers and business partners

Industry-leading Cisco routers, WAN switches, access servers, IP Security (IPsec) VPN concentrators, and firewalls—combined with the pervasive Cisco IOS® Software and carrier-class management solution—provide the foundation for delivering truly scalable, business-critical network services over a secure IP backbone.

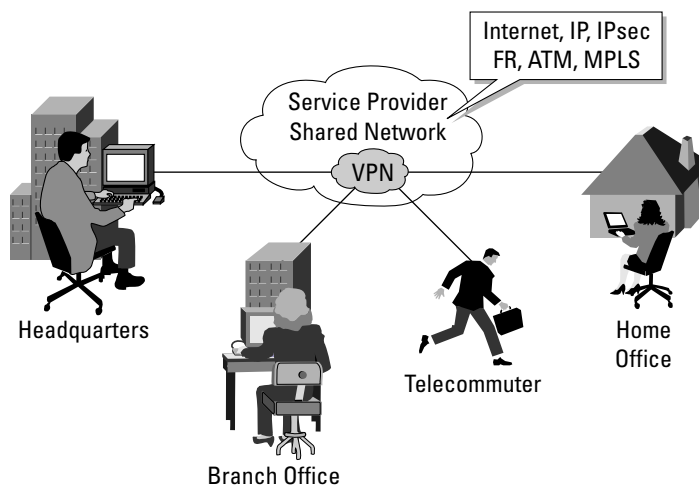
### **Opening New Doors for Service Providers**

IT managers are turning to VPNs not just for remote access but to replace expensive and difficult-to-manage legacy networks. They are using VPNs to tie together broad-reaching networks and link employees anywhere in the world to critical corporate applications. They’re also relying on VPNs and the ubiquity of the Internet to reach out to customers and suppliers.

This fundamental shift in strategy opens opportunities for continued growth, increased profitability, and the utmost efficiency for service providers and their subscribers. As telecommuters, mobile users, and satellite offices all vie for dependable access to company intranets, businesses of all sizes are beginning to recognize the advantages of an outsourced communications solution.



**Figure 1** VPNs can be built on the Internet or on a service provider's IP, Frame Relay, or ATM infrastructure.



### What are VPNs?

VPNs deliver enterprise-scale connectivity deployed on a shared infrastructure with the same policies enjoyed in a private network. A VPN can be built on the Internet or on a service provider's IP, Frame Relay, or ATM infrastructure (Figure 1). Businesses that run their intranets over a service provider's VPN service enjoy the same security, quality of service (QoS), reliability, and manageability as they do in their own private networks.

VPNs can also extend the ubiquitous nature of intranets over wide-area links to remote offices, mobile users, and telecommuters. Further, they can support extranets linking business partners, customers, and suppliers to provide better customer satisfaction and reduced manufacturing costs. Alternatively, VPNs can connect communities of interest, providing a secure forum for common topics of discussion.

**“Thirty percent of all VPNs are outsourced today, but that number will swell to 90 percent by 2003, with spending for VPN services expected to grow even more dramatically.”—Cahners In-Stat Group**

### New Business Opportunities

New IP-based services such as videoconferencing, e-commerce, packet telephony, distance learning, and information-rich applications offer businesses the promise of improved productivity at reduced costs. As these networked applications become more prevalent, businesses increasingly look to their service providers for intelligent services based on a rich set of controls that extend beyond transport to optimize the delivery of applications end to end. Business customers want their critical corporate applications to traverse a network in a secure, prioritized environment, and they want the opportunity to reduce total costs, improve connectivity, and gain access to networking expertise.

For service providers, VPNs are the key to staying competitive in the years ahead. Service providers have an unprecedented opportunity to reap the benefits of increased revenue and expanded services.

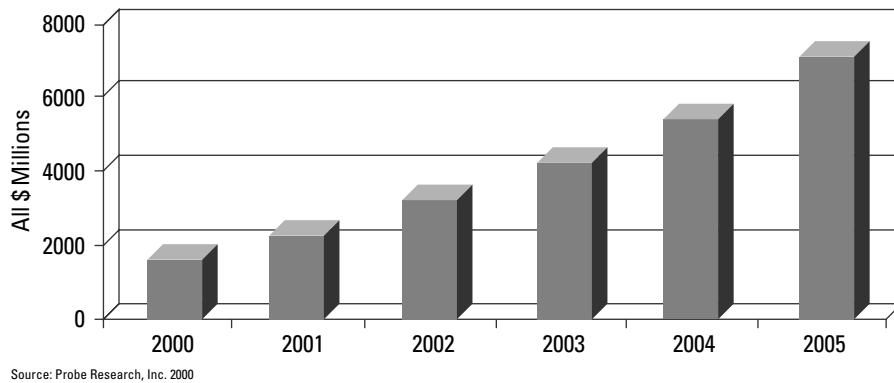
Industry analysts recognize the tremendous revenue opportunity that VPNs afford service providers. Cahners In-Stat Group estimates that 13 percent of U.S. businesses already outsource part of their network operations to a service provider and another 20 percent plan to do so over the coming year. Probe Research estimates that United States and European IP VPN services market revenue will reach US\$7.1 billion and US\$850 million respectively by 2005 (Table 1 and 2).

The Yankee Group predicts that by 2003, 70 percent of all companies will use VPNs for up to 90 percent of their data communications needs in place of private-line or alternative services. This trend will be driven by:

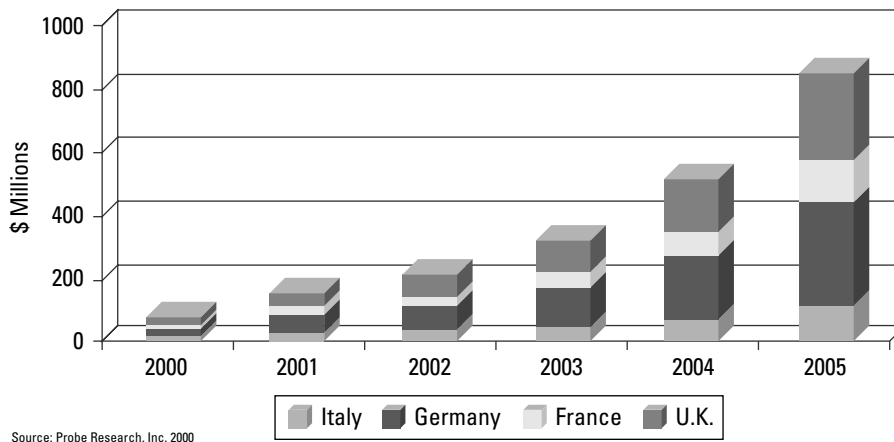
- Pressure on businesses to accommodate their increasing data communications needs and reduce total cost of ownership
- Changing business requirements to connect customers, suppliers, and partners to internal networks
- Internet accessibility from any point on the globe

**"Teaming with Cisco was a logical decision and will help enhance our leadership position in the managed VPN and Internet security services marketplace,"—John Summers. Director, Product Strategy, Genuity**

**Table 1** U.S. IP VPN Service Market Forecasts for Service Providers



**Table 2** European IP VPN Service Market for Service Providerst



**"Global IP VPN is optimized for the full scope of e-business communication, including supplier, partner, and customer applications—exactly what today's businesses require,"—Tom Wyrick, Vice President of Market Development, Global One.**



### **Case in Point: Global IP VPN Drives e-Business for Renault Spain**

When Renault Spain needed a large amount of horsepower to connect hundreds of automotive dealers and Renault business sites to a common service network, it selected Global One to deliver an innovative communication solution. The business driver was supply chain optimization: reducing the time between order and delivery of cars and spare parts. Other key requirements included improved information sharing, decreased sales reporting times, and flexible Internet access for thousands of personnel.

Global One ([www.globalone.net](http://www.globalone.net)) is a world leader in providing international communications to enable e-business, with more than 5,000 employees, sales and support offices in more than 70 countries and revenues exceeding US\$1 billion per year. In August 1999, Global One launched the world's first MPLS-based commercial VPN service. Global IP VPN is highly flexible and scalable, supporting intranet, extranet, and public Internet services for IP, data, and voice requirements. The service is available today in about 40 countries with local access to MPLS-based provider edge routers, in almost 80 countries using IP over Frame Relay, and virtually worldwide with integrated, secure IPsec tunneling over the public Internet. Secure dial access is available in 60 countries. Global IP VPN uses a Cisco Powered Network infrastructure consisting of Cisco 12000 and 7500 series routers at the provider core and Cisco 7500 series routers at the provider edge, connected to the Global One terabit optical backbone. Global IP VPN is a fully managed, end-to-end service, and includes customer premises routers such as Cisco 1700, 2600, 3600, and 7200 series models.

For Renault, the Global IP VPN solution has exceeded their requirements. Hundreds of sites are operational today, enjoying a New World of communications among Renault staff, partners, suppliers, and dealers over the secure, private domain Global IP VPN service. The time from order to delivery has decreased, from 40 to 60 days to a planned 14 days. Network administration has been simplified because of automatic any-to-any connectivity, and the quality of service (QoS) is excellent, with three unique, prioritized service classes. Today, the bottom line for Renault Spain is optimized e-business communications—secure access to the Internet and cost-effective dealership intranet/extranet services. And tomorrow, according to Antonio Guidian, Network Manager for Renault Spain, “We are making it a priority next year to give these same sites voice over IP.”

### **Benefits of VPNs for Service Providers**

As Renault Spain has demonstrated, VPNs offer service providers new managed services that extend far beyond the old-world service model of raw connectivity and transport, laying a foundation for incremental services such as e-commerce, hosting, and multimedia applications. By furnishing comprehensive VPN services to their business subscribers, providers can enjoy increased revenue and greater customer reach. They can also differentiate themselves in an increasingly competitive marketplace. As subscribers team with service providers for their business-critical network requirements, their loyalty increases, thereby reducing customer churn and providing a more stable, profitable customer base.

### **Attracting Business Customers**

VPNs put service providers in a partnership role with their customers to meet their inter- and intrabusiness communication needs. A VPN supplied by a service provider offloads the challenges of scaling a corporate network and allows a company to focus on its core competencies. The result is simplified WAN operations and a renewed focus on primary business goals.

Another advantage of buying a VPN service from a provider is reduced total cost of ownership. Rather than fund the equipment, bandwidth, staffing, and operations costs in house, business customers can seek the resources of a service provider, which lowers overall costs.

VPNs also can result in improved connectivity. Businesses are quickly connected worldwide for their remote-access, intranet, and extranet communications through the global span of a service provider's IP, Frame Relay, or ATM infrastructure, often in conjunction with the Internet.

Businesses that run their intranets over a VPN service enjoy the same security, quality of service, reliability, and manageability as they do in their own private networks.

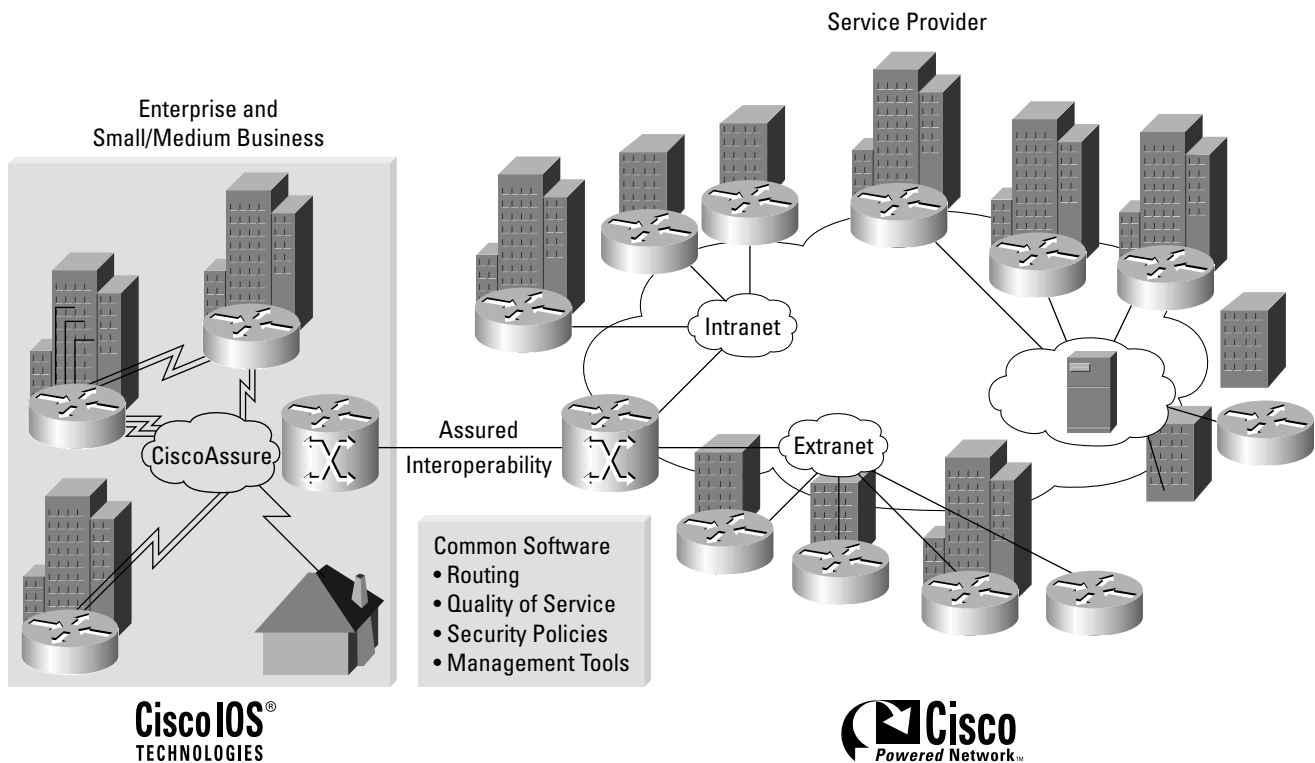
### VPNs Powered by Cisco

Virtually all Internet traffic travels on internetworking equipment from Cisco Systems, and many Fortune 1000 companies have made Cisco their networking vendor of choice. These factors make Cisco uniquely positioned as the guide to the New World of VPNs.

Cisco IOS Software and the carrier-class management provide the thread that binds VPNs to support the policies that subscribers need to thrive in today's Internet economy (Figure 2). Industry-leading platforms from Cisco, including routers, WAN switches, VPN concentrators, access servers, and firewalls—combined with robust Cisco IOS Software and the carrier-class management solution—are the foundation for deploying the broadest set of VPN architectures.

“Leveraging of a service provider’s infrastructure will give us the global presence we need and all the security and benefits of a private dial-up solution. It’s a Win-Win for both of us.”—Saul Adler, VP Network Engineering, Bankers Trust

Figure 2 End-to-End Policy Networking



The Cisco VPN suite of solutions enables three distinct VPN services: Access, Intranet, and Extranet VPNs (Figure 3). Each service meets different business requirements for connectivity to mobile users, remote offices, partners, and customers. In each case, Cisco IOS Software ties these services together, enabling end-to-end networking with consistent policies over a shared infrastructure.



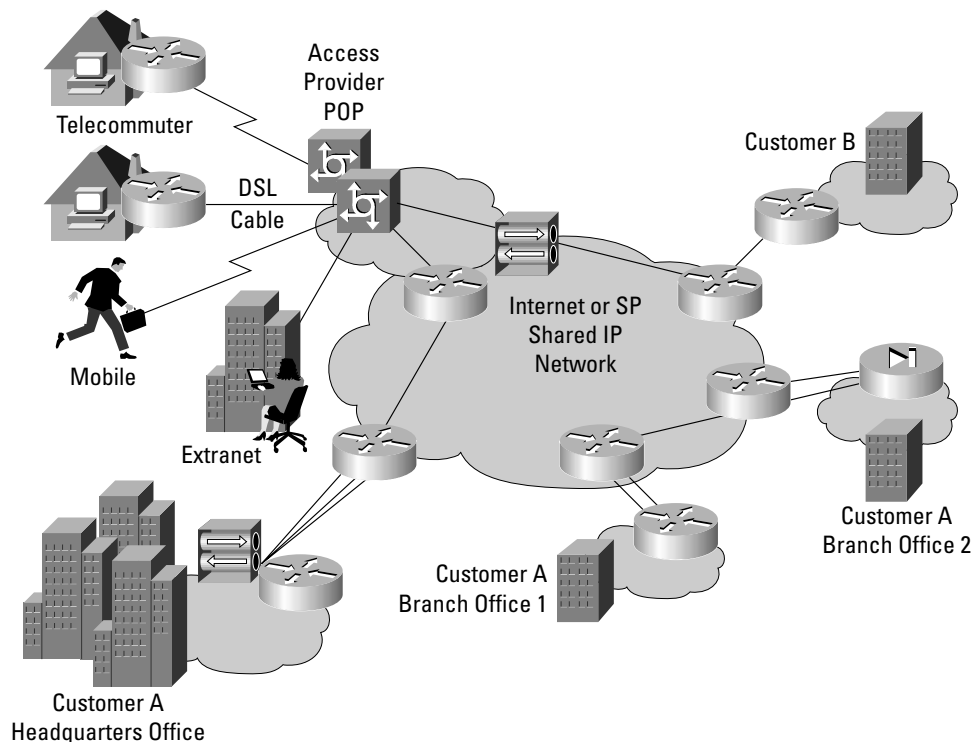
**Figure 3** VPN Services and Technology

Service	Architecture	Technologies
Access VPN	Client-Initiated NAS-Initiated	CPE and Network-Based IPsec, L2TP, PPTP Dial, ISDN, DSL, Cable
Intranet VPN	IP Tunnel Virtual Circuit MPLS	CPE and Network-Based IPsec, GRE FR, ATM IP or IP + ATM
Extranet VPN	IP Tunnel Virtual Circuit MPLS	CPE and Network-Based IPsec, GRE FR, ATM IP or IP + ATM

**Access VPNs**

Access VPNs streamline computing activities for today’s increasingly mobile workforce, enabling users to connect to their corporate intranets or extranets whenever, wherever, or however they need to (Figure 4). The services are most popular with mobile users and telecommuters requiring remote-access connectivity through dial, ISDN, DSL, wireless, and cable technologies.

**Figure 4** Access VPNs



Access VPNs encompass two architecture options: client-initiated and network access server (NAS)-initiated connections. With client-initiated Access VPNs, IPsec client software is used to establish an encrypted tunnel between the Internet or a service provider's shared network and the corporate network. Service providers manage the client software that initiates the tunnel. Client-initiated Access VPN services are well-suited to mobile and remote users who require frequent access to their corporate networks. Typically, with client-initiated Access VPNs, the customer decides when and where to establish a VPN across a public network and manages the software directly. Because the user has discretion, this type of VPN is also called a "voluntary" VPN.

NAS-based VPNs, by contrast, aggregate dial or other Point-to-Point Protocol (PPP)-based connections and initiate a Layer 2 Tunneling Protocol (L2TP) VPN tunnel between the NAS in the service provider network and a home gateway within the customer network.

In an Access VPN environment, security requires a user to be identified as a member of an approved customer company and establish a VPN session, often called a tunnel, to the customer network, typically through a VPN concentrator. The VPN concentrator handles per-user authentication, security policy enforcement, and accounting. Authentication is based on a combination of user name and passwords, often using one-time password products or digital certificates for businesses employing the emerging public key infrastructure technologies. When the remote user is authenticated and has an IP connection, the VPN tunnel is set up per the policies stored in the VPN concentrator, either at the customer network edge, referred to as customer premises equipment (CPE) based, or as an additional service in the service-provider network (network based).

**"A new trend in network-based IPsec VPNs is emerging. With service providers offering VPN services based on the Cisco VPN 5000 series, enterprise customers can now turn more confidently toward outsourcing their WAN requirements."—Ron Westfall, Senior Analyst, Current Analysis**

### **VPN Access Equipment**

VPN IPsec concentrators are multipurpose devices designed specifically to terminate VPN connections. Cisco offers three families of these devices: the Cisco VPN 3000 and VPN 5000 concentrators, the Cisco 10000 Series with the IPsec VPN Service Module, and the Cisco IOS Software-based VPN routers such as the Cisco 7200 specifically designed as a Cisco IOS IPsec concentrator.

The Cisco VPN 3000 Concentrator Series is a family of remote-access VPN platforms with Windows client software. The high availability and easy manageability of these concentrators make them ideally suited for service providers delivering Access VPN offerings along with fully managed CPE.

The Cisco VPN 5000 Concentrator series provides very-high-volume IPsec tunnel aggregation to facilitate network-based architectures deployed at the provider edge. The Cisco VPN 5000 provides the Customer Virtual Context capability to support overlapping address ranges among multiple service provider customers on the same platform. The Cisco VPN 5000 Series supports Windows, Macintosh, Linux, and Solaris clients, broadening the potential customer base for Access VPN services.

The alternative architecture for Access VPNs defines tunnels initiated from the NAS. In this scenario, remote users dial into a service provider's point of presence (POP) via a local or toll-free number. The service provider, in turn, initiates a secure tunnel to the corporate network. With an NAS-initiated architecture, service providers authenticate the user to gain initial access to the corporate network; however, businesses retain control of their own security policies, authenticating users, authorizing access privileges, and tracking user activity on their networks.



## **Intranet and Extranet VPN Architectures**

Intranet and Extranet VPN services link remote offices, suppliers, partners, customers, and communities of interest over a shared infrastructure with the same policies as a private network (Figure 5). Cisco provides a range of MPLS-based and IP-based choices for deploying large-scale Intranet and Extranet VPN services, including:

- IP VPN tunnels, which can be based on IPsec, generic routing encapsulation (GRE), or mobile IP for wireless communication
- Virtual circuits (VCs) based on ATM or Frame Relay
- Multiprotocol Label Switching (MPLS)-based IP VPN services that enable secure business-quality VPN solutions that scale to support thousands of VPN customers over IP or IP+ATM technologies

In all these cases, Intranet and Extranet VPN services create secure/private tunnels/paths across an IP network. They take advantage of industry standards to establish secure connections in a service provider's trusted IP network or the public Internet. As with Access VPNs, Intranet and Extranet VPNs can be maintained end-to-end terminating between customer sites across the network (CPE-based) or they can be network-based, where the VPN functionality takes place at the service provider network and is completely transparent to the end customer.

IPsec is a suite of IETF standards designed to offer network layer protection by cryptographic security mechanisms that can flexibly support combinations of authentication, integrity, access control, and confidentiality. When IPsec is used to protect all traffic, Cisco IOS routers and Cisco VPN concentrators ensure the security of information traversing an IP-based service provider's network.

An alternative approach to Intranet and Extranet VPNs is to establish VCs across an ATM or Frame Relay backbone. With this architecture, privacy is accomplished with permanent virtual circuits (PVCs) instead of tunnels. VC architectures enable prioritization through QoS for ATM and committed information rate (CIR) for Frame Relay.

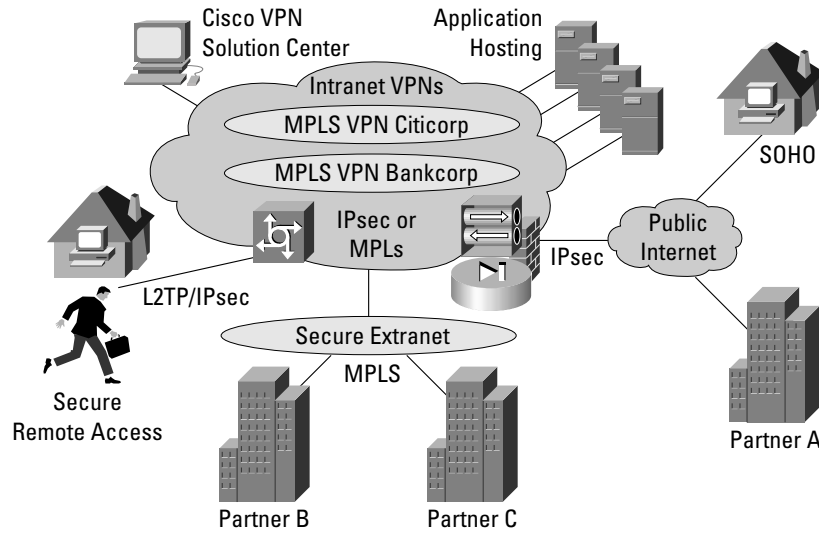
MPLS is a suite of IETF standards originally based on Cisco's Tag Switching and can be implemented across either frame-based or cell-based network cores. MPLS forwards packets using labels: VPN-based addresses are analogous to a postal zip code. MPLS-enabled edge routers have multiple routing and forwarding tables called VPN Routing/Forwarding (VRF) and routing information of a VPN remains inside a VRF. Labels are assigned based on VPN information received by routing protocols, thus isolating traffic to that VPN. In contrast with IPsec tunnel and virtual-circuit architectures, MPLS-based VPNs in a fully MPLS-enabled network environment provide connectionless routing within each VPN community. Consequently, service providers can easily scale their services to support thousands of VPNs on the same infrastructure, with full QoS and traffic engineering benefits across IP and ATM environments.

Cisco offers service providers the broadest portfolio of VPN technologies and management tools. Access VPN solutions work in conjunction with Intranet and Extranet VPN architectures such as MPLS, GRE, and Frame Relay and ATM VC architectures. These solutions enable providers to offer a fully integrated, manageable, and comprehensive service portfolio that is highly scalable and easy to manage.

As MPLS becomes a key architecture for delivering VPN services, Cisco is enabling a full range of MPLS-based solutions for the core and edge of service-provider networks. These include the Cisco GSR 12000, the Cisco 7500 and 7200 series, and the BPX<sup>®</sup> and MGX<sup>™</sup> solutions for the IP+ATM platforms. Other platforms that support MPLS include the Cisco 3600 Series, Cisco 6400 Universal Access Concentrator, and Cisco 10000 Series.

In addition, the Cisco 10000 Series provides a comprehensive set of IP services, at network edge, for nonstop subscriber access without compromising the performance, scale, or carrier-class reliability demanded by today's service providers. With the IPsec VPN Service Module, the Cisco 10000 Series can deliver a full-suite of IP VPNs including MPLS VPNs and IPsec VPNs for site-to-site connectivity or terminating access VPN services.

**Figure 5** Intranet and Extranet VPNs

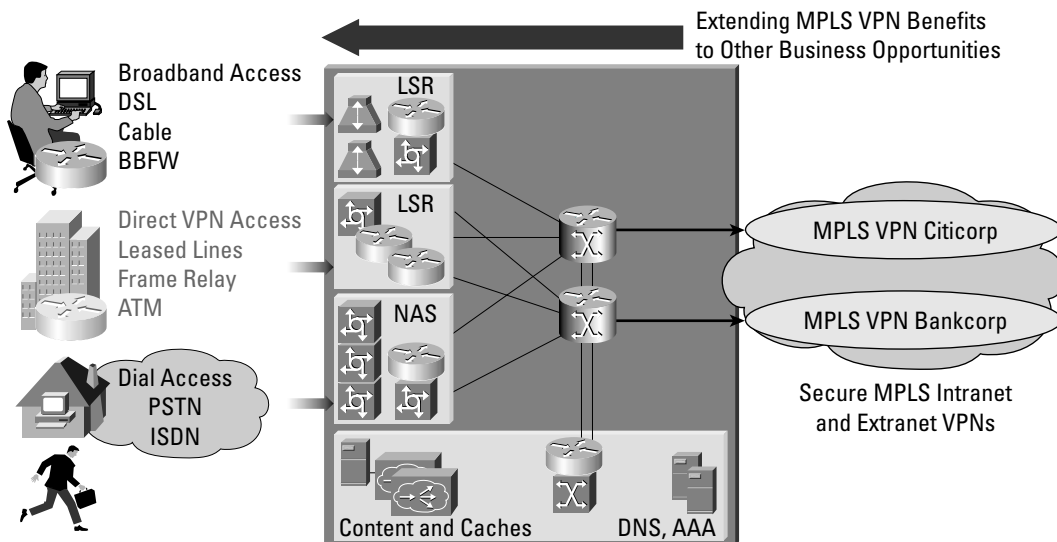


**Integrated Access VPN with Intranet and Extranet VPN Services**

The true promise of VPN services lies in a service provider’s ability to deliver a range of bundled VPN solutions that can integrate Access VPN services with Intranet and Extranet VPN services. Cisco now offers an industry-first fully integrated remote access to MPLS VPN solutions, across a wide range of flexible Access options (Figure 6). This enables service providers to link their customers remote office and mobile workers with mission-critical corporate applications. Service providers enjoy increased revenues, service differentiation, and greater customer reach.

**“Cisco shares our vision that the IP network is the foundation for delivering business solutions that will provide our customers with a strategic competitive advantage. By deploying market-leading Cisco technology, we are able to develop and offer the best in secure and reliable e-business services to our customers,”—Mayer G. Becker, Vice President Marketing, Telenisus**

**Figure 6** Integrated Access VPN with Intranet and Extranet VPN Services





### **IPsec-Based VPN Architecture**

IPsec is a framework of open standards for ensuring secure private communications over the Internet. Based on standards developed by the Internet Engineering Task Force (IETF), it ensures confidentiality, integrity, and authenticity of data communications across a public network. IPsec is implemented by defining security relationships between peers, such as between branch offices and headquarters sites, or between mobile or remote users and the corporate network.

IPsec is the architecture of choice for many service providers to deliver encrypted VPN services to customers or when traffic must traverse outside of a service provider's network (off-net). It is a highly secure infrastructure for the transport of sensitive information over the public Internet. It also provides data security through a flexible suite of encryption and tunneling mechanisms that protect packet payload as it traverses the network.

Another strength of IPsec is its flexibility: it can be deployed across any existing IP network. This gives service providers more choices in network structure and enables rapid time to market. An IPsec-based VPN does not require application modifications, so there is no need to deploy and coordinate security on a per-application, per server basis. Further, customers can secure their network infrastructures without costly changes to every computer.

### **MPLS-Based VPN Architectures**

In Intranet and Extranet VPNs based on Cisco MPLS, packets are forwarded using an MPLS label switched paths. The label switched paths are established based on routing information distributed via the IGP. Service providers enable the edge routers with virtual routing and forwarding capability and configure a unique route distinguisher (RD). RDs, which are unknown to end users, are uniquely assigned when the VPN is provisioned. The RD is attached to the IP address to create a globally unique VPN addresses and this information is then distributed using BGP extended communities. The routers then filter the VPN addresses they need and install the routes in the VRF. To participate in a VPN, a user or site must be attached to its associated VRF. The packets received from the user or site are then attached with a VPN label, assigned by BGP, attached with the IGP label (to reach the destination edge router), and then forwarded to the LSP.

MPLS packets are forwarded using labels attached in front of the IP header. Because of the unique RD, by virtue of assignment, VPN addresses are masked by attaching the RD. This creates globally unique addresses that can then be distributed using BGP extended communities. Therefore, the same IP address space can be shared among different customers, simplifying IP address management. Service providers can deliver fully managed MPLS-based VPNs with the same level of security that users are accustomed to in Frame Relay/ATM services, without the complex provisioning associated with manually establishing PVCs and performing per-VPN CPE router design. The security of MPLS VPN has been validated by Mier. For a full report, please see <http://www.mier.com/reports/cisco/MPLS-VPNs.pdf>. VPNs put service providers in a partnership role, helping customers optimize application delivery with end-to-end security and QoS.

### **Dual Architecture VPNs—IPsec to MPLS Internetworking**

Until recently, all service providers had to choose between IPsec and MPLS architecture to deploy, and with that choice came a necessary limitation to a service provider's customer base. Today, a well-executed, comprehensive VPN service portfolio based on both IPsec and MPLS allows a service provider to capture the full opportunity of New World VPNs. IPsec can be used to greatly extend a service provider's MPLS-based VPN network and to use the public Internet as off-net transport. In addition, an intranet or extranet deployment can use MPLS to lay a service foundation with traffic engineering and QoS that extends the VPNs today to other value-added services in the future. IPsec over MPLS allows a service provider to extend encryption to their MPLS-based service.

## Secure Building Blocks for VPNs

VPN building blocks are provided through industry-leading Cisco IOS Software and hardware features, including:

- Security
- QoS
- Manageability
- Reliability

### Security

Subscribers want assurance that their VPNs are, in fact, private and that applications and communications are isolated and secure. Cisco offers many robust security measures to secure confidential information such as encrypted data, restricted access to authorized users, user tracking after establishing a network connection, and real-time intrusion auditing. If a network provides limited or inconsistent higher-layer security, a provider cannot guarantee the integrity of a VPN service.

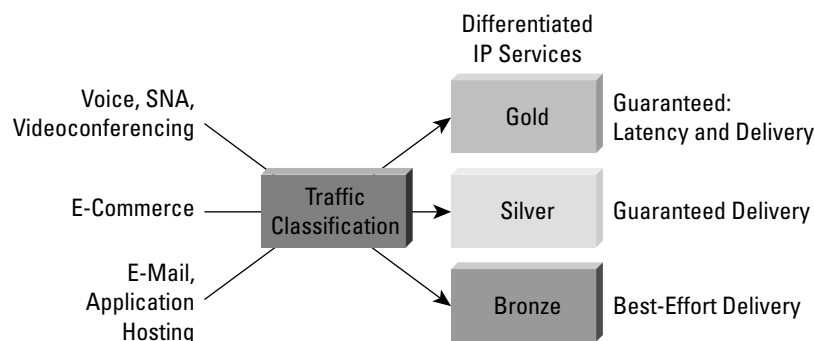
Though approaches may differ, all VPNs offer privacy over a shared network infrastructure. A tunnel creates a logical, point-to-point connection in a connectionless IP network. An encrypted tunnel provides privacy by scrambling data so that only designated senders and receivers understand it. IPsec, a new industry standard, offers a scalable Layer 3 solution for network encryption. It uses proven encryption technologies, including Encapsulating Security Protocol (ESP) and the Data Encryption Standard (DES), to protect packet payload as it traverses the network.

**“Global One chose Cisco MPLS technology to power our Global IP VPN because Cisco has the best hardware and software, as well as the sales, marketing, and operational support to turn a new technology into a successful, worldwide commercial service,”—Tom Wyrick, Vice President of Market Development, Global One**

### Quality of Service

Cisco offers a range of solutions that provide greater granularity to individual applications for priority and bandwidth management. Using these solutions, providers can easily deliver incremental services. QoS affords an enormous opportunity to service providers to provision varying service levels (such as first class, business class, and economy class) and subsequently create differentiated pricing models. QoS is a key ingredient of a VPN because it determines the ability of the network to assign resources to mission-critical or delay-sensitive applications (Figure 7). QoS mechanisms ensure that mission-critical applications receive priority over other traffic. QoS is an essential ingredient in Intranet and Extranet VPN services that support New World services such as packet telephony, e-commerce, and content hosting. Service providers can now realize a substantial cost benefit when the VPN network is built once and can support multiple New World applications.

**Figure 7** Differentiated Quality of Services





QoS addresses two fundamental requirements for applications that run on a VPN: predictable performance and policy implementation. Policies are used to assign resources to applications, project groups, or servers in a prioritized way. The increasing volume of network traffic, along with project-based requirements, results in the need for service providers to offer bandwidth control and align network policies with business policies dynamically and flexibly. Cisco offers the industry's most comprehensive set of QoS capabilities that enable providers to prioritize service classes, allocate bandwidth, avoid congestion, and link Layer 2 and Layer 3 QoS mechanisms. One of the best examples is Committed Access Rate, which classifies packets by application and protocol, and specifies bandwidth allocation. Low-latency queuing and class-based weighted fair queuing techniques implement efficient bandwidth usage by always delivering mission-critical application traffic and deferring noncritical application traffic when necessary. Weighted random early detection provides congestion avoidance to slow down transmission rates of faster flows by discarding lower-priority traffic before congestion occurs and ensures predictable service for mission-critical applications that require specific delivery guarantees. Network-based application recognition (NBAR) provides classification up to the application layer. NBAR enables application-aware QoS by classifying traffic based on application type, by URL, and even among dynamically assigned TCP ports.

Cisco also provides a robust set of Layer 3 traffic-engineering tools that let service providers map traffic through specific routes based on available bandwidth or preferred paths. This lets them simply engineer backbone networks to deliver the total subscribed capacity to all Intranet and Extranet VPN customers more efficiently.

**“Being able to offer solid, comprehensive service-level agreements across an IP network is key to the VPN market really taking off. Cisco is far ahead with the QoS features that make this possible.”—Darin Quest, Group Product Development Manager, Qwest**

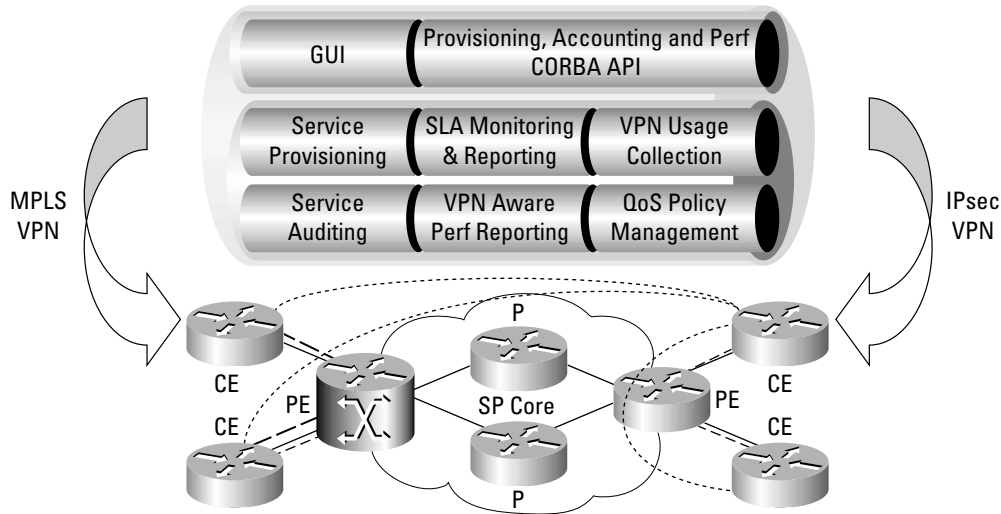
### **Manageability**

As service providers build VPNs that include WAN switches, routers, firewalls, VPN concentrators, and Cisco IOS Software, they need to seamlessly manage these devices across the network infrastructure and provide service-level agreements (SLAs) to their customers. They also need to enable business customers to personalize their access to network services and applications. In addition to offering the broadest portfolio of VPN technologies, Cisco also provides the most comprehensive, industry leading, carrier-class VPN service management for service providers to effectively deploy outsourced VPN services that many businesses want today.

The Cisco VPN Solutions Center (VPNSC) release 2.0 (Figure 8) provides for service and network management of both IPsec-based and MPLS-based IP VPNs. In addition, VPNSC offers a suite of service management solutions to enable service providers to rapidly plan, provision, operate, and bill for VPN services.

Cisco VPNSC is designed with robust redundancy and database journaling capability to ensure carrier-class availability, which is crucial for demanding mission-critical production networks. The scalable multithreaded design enables service providers to easily and rapidly add, upgrade, or reconfigure VPN in response to customer's changing needs. The Cisco VPNSC system can also be operated on a distributed concurrent environment to support VPN provisioning and management of very large carrier-class networks.

**Figure 8** VPN Solutions Center Architecture



With the Cisco VPN Solutions Center, service providers can use a graphical user interface (GUI) administration console or programs developed using VPNSC's Operational Support System (OSS) interfaces to automatically perform the following management functions in easy steps:

Automate the set of processes required to:

- Create a new VPN site
  - Set up a new VPN between given sites
  - Autogenerate network configurations based on service requests
  - Generate customer default configuration files for remote installation
- Create IP VPN policy definitions
- Provide for point-and-click VPNs
  - User or device authentication methods
  - Encryption to be used
  - What traffic is to be protected
  - Class-of-service (CoS) profiles
- Audit the service requests, VPN sites, or customer VPNs, and generate audit reports
- Provide VPN-specific SLA and performance reports
- Provide per VPN-traffic matrix for accounting and usage-based billing purposes
- Provide templates to support Cisco IOS Ipv4 and firewall provisioning

Finally, for service operations, the Cisco VPN Solution Center offers tools that monitor performance and faults on existing services to improve quality, and that monitor service accounting and planning.

### **Reliability**

Service providers that build their VPN offerings using Cisco equipment and Cisco IOS Software can rest assured that they have the best solution to meet the performance requirements contracted in their SLAs. The broad Cisco product line is designed for carrier-class reliability, reducing the risk of downtime due to unexpected component failures. Moreover, Cisco IOS Software offers many features that provide backup paths if a link or device fails. For example, Cisco MPLS supports rerouting IP traffic to backup label virtual circuits (LVCs) to ensure fast restoration times for Layer 3 traffic if a node or link fails. In addition, the VPN Solution Center offers high availability standby and redundancy using journaling and replay of critical data and by using operating system clustering software, multiple disk arrays, fiber channel, and redundant workstations.

## Case in Point: Comprehensive Support Services

To build customer satisfaction and loyalty, service providers must deliver highly reliable network services. Subscribers must have confidence that VPNs can support their mission-critical applications. To help service providers win this confidence and trust, Cisco offers a wide range of support services.

Through the standard Cisco service offering called the Service Provider Base Plan, service providers may access the Cisco Technical Assistance Center (TAC), online support tools, software updates and fixes, and hardware maintenance support.

Cisco also offers specialized programs to ensure highly proactive and cost-effective risk management. Expert assistance is available for network design, performance engineering, software deployment, and routine audits.

In addition to operational support services, Cisco offers marketing support through JumpStart and Cisco Powered Network programs. The JumpStart program gives service providers access to marketing consultants to create and market new services. Further, the Cisco Powered Network program offers providers an ingredient brand mark that matches the provider's service offering to the rich set of Cisco technologies installed in their business customers' networks. And through joint marketing activities, the Cisco Powered Network program steers Cisco business customers to an ecosystem of providers labeled as Cisco Powered Network members.

By taking advantage of expert Cisco support services, service providers can be confident that their Cisco VPN offering will maintain satisfied customers.

## In Step with Tomorrow

Cisco looks forward to teaming with service providers to deploy carrier-class VPNs that enable our mutual customers to lead their industries. With leading Cisco technology and management solutions as the foundation, service providers can be confident that their VPN offerings will provide the most advanced and robust business communications solutions available to propel them and their customers confidently into the New World in networking.

The future belongs to service providers that can furnish customers with turnkey solutions for inter- and intrabusiness communication needs.

Cisco.com offers a wealth of information about Cisco VPN solutions for service providers. Visit [www.cisco.com/go/vpn](http://www.cisco.com/go/vpn) for a detailed discussion of VPNs powered by Cisco.



### Corporate Headquarters

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

### European Headquarters

Cisco Systems Europe  
11, Rue Camille Desmoulins  
92782 Issy-les-Moulineaux  
Cedex 9  
France  
[www-europe.cisco.com](http://www-europe.cisco.com)  
Tel: 33 1 58 04 60 00  
Fax: 33 1 58 04 61 00

### Americas Headquarters

Cisco Systems, Inc.  
170 West Tasman Drive  
San Jose, CA 95134-1706  
USA  
[www.cisco.com](http://www.cisco.com)  
Tel: 408 526-7660  
Fax: 408 527-0883

### Asia Pacific Headquarters

Cisco Systems Australia, Pty., Ltd  
Level 17, 99 Walker Street  
North Sydney  
NSW 2059 Australia  
[www.cisco.com](http://www.cisco.com)  
Tel: +61 2 8448 7100  
Fax: +61 2 9957 4350

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](http://www.cisco.com/go/offices)**

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • 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