

# Implementing Managed IP Virtual Private Network Services

## Executive Summary

Increasingly challenged to offer much more than just basic connectivity and Internet access, service providers must address key business concerns of today's enterprises to attract and keep customers. Managed Internet Protocol (IP) virtual private network (VPN) services meet these challenges. Service providers can use managed IP VPN services as a foundation for a portfolio of value-added services. This first step beyond basic connectivity and access services creates an opportunity for simultaneously satisfying existing customers and generating additional new revenue streams.

Managed IP VPN services must meet an extensive list of networking requirements set forth by the enterprise technical decision makers. To succeed in this arena, service providers must:

- Convince enterprise IT managers that the provider network meets the requirements for high availability, security, quality of service (QoS), multicast, and management
- Provide managed IP VPN services that enable enterprises to smoothly migrate and potentially out-task their context-based applications in the future
- Deliver a continually expanding portfolio of value-added managed IP VPN services that set the service provider apart from the competition

This paper provides a concise summary of the key networking issues that service providers need to address to deliver profitable managed IP VPN services. The market opportunity is briefly explained, followed by a discussion of the key networking requirements for today's enterprises. The service provider's implementation challenges also are detailed, followed by an overview of the Cisco® technology features that greatly enhance the implementation and delivery of managed IP VPN services to enterprise customers. The appendix provides four abbreviated customer profiles as examples of the challenges faced and solutions deployed by some specific service providers in successfully offering managed IP VPN services.

## Managed IP VPN Services: Opportunities for the Service Provider

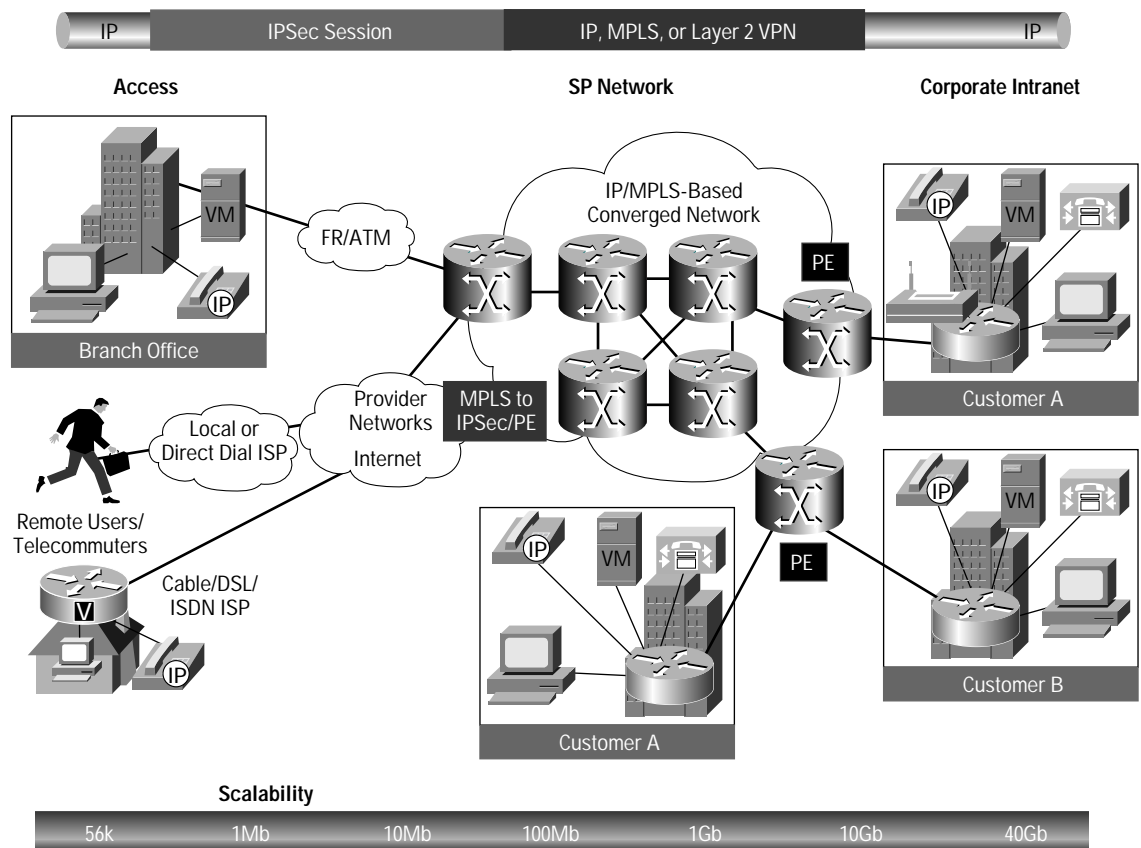
Networks have gone through a number of different technology-based eras over the last decade and a half: leased lines, X.25, Frame Relay, and Asynchronous Transfer Mode (ATM). Separate overlays were built for each new technology. Similarly, access or connectivity services emerged based on the underlying technology: X.25 for dial-up and low speed lines, Frame Relay for sub-E1 speeds, and ATM for speeds above that.



Today, enterprises and service providers alike recognize the need to progressively converge disparate networks. The compelling reasons for convergence include lowering costs, simplifying support, improving overall scalability, and streamlining day-to-day operations and provisioning. Managed IP VPN services facilitate convergence to consolidate disparate networks, and serve as a foundation for delivering numerous emerging IP-based value-added services over the entire 56 K to 40 Gb range (see Figure 1). In addition to traditional Layer 2 VPNs, such as frame-relay and ATM, new Layer 3 IP-based VPN technologies are emerging. These IP-based VPNs can better support value-added Layer 2 and Layer 3 services. Layer 3 VPNs typically fall into two categories—those that use IP Security (IPSec) functionality to tunnel over IP infrastructures, and those that leverage Multiprotocol Label Switching (MPLS) capabilities.

Managed IP VPN services offer enterprises the benefit of greatly improved network performance, and meet the requirements of many emerging IP-based applications such as voice over IP (VoIP) and videoconferencing. With simple Layer 2 VPNs, the network managers must engineer and manage capacity for the supported applications. It can quickly become very time-consuming and cost-prohibitive to manage these full-mesh Layer 2 networks. Service providers must determine a strategy for implementing and offering managed Layer 3 IP VPN services, or risk missing out on the growth opportunities in the market. At the same time, service providers must still be able to offer managed IP VPN services to those enterprises that are currently using Layer 2 VPN functions for their legacy applications.

Figure 1  
Architecture for Multiservice VPNs





## Enterprise Requirements for Managed IP VPN Services

To plan its managed IP VPN services offerings, a service provider must first consider if the proposed offerings match the requirements of the enterprises. Buying criteria do not differ for technology and services—buying decisions are based to a large extent on a solution's ability to solve business problems or overcome challenges. Today, the most pressing enterprise business concerns fall into three areas:

- **Protection:** Enterprises want to identify and address uncertainties and mitigate risks whenever possible. Global uncertainty and a declining economy raise questions about how to be prepared to sustain operations in a challenging environment encompassing restricted travel, a displaced workforce, loss of resources, new laws and regulations, and other complications.
- **Profits:** In today's economic climate, profits have dropped in many sectors and there is a need to optimize investments and reduce operational costs while continuing to sustain operations and satisfy customers. Reducing total cost of ownership (TCO) and using networking technologies to lower costs are current priorities in this area.
- **Productivity:** The need to increase worker productivity is driving the adoption of on-line collaboration, customer relationship management (CRM), and workflow automation applications that can both increase efficiency and strengthen a business' competitive position. Better access to resources—being able to access resources on demand, regardless of location—also improves productivity by minimizing wasted time and allowing remote workers to do something that was previously impossible.

Based on concerns about protection, profits, and productivity, enterprises are evaluating current wide-area networks (WANs) and looking for ways to:

- Consolidate voice, video, and data networks as a means to enable collaboration while lowering costs
- Move to distributed, regionalized data centers for increased productivity, application availability, and lowered costs
- Achieve any-to-any connectivity for increased productivity among business offices and employees, and simplify overall infrastructure support
- Offer secure teleworker solutions that allow workers to access corporate resources from any location

Accomplishing these types of improvements requires a dependable network foundation supported by five persuasive, key attributes:

- High availability
- Security
- QoS
- Multicast
- Comprehensive management solutions

These five network attributes repeatedly surface in the questions being raised in today's enterprises (see inset). Today's enterprises will embrace managed IP VPN services when they find answers to all of their questions and they are convinced that all of the key network attributes—high availability, security, QoS, multicast, and ease of management—are more cost-effectively realized by involving service providers. Enterprise requirements must also be clearly understood by service providers as they relate to network topologies (moving to full mesh topologies), convergence of multiple types of traffic onto one network, teleworker access, and overall cost reduction. The following sections cover each of these topics.



### Typical Questions Being Asked In Today's Enterprises

- **How can I maintain existing high-availability when my network is extended over a WAN?**  
Today, my network already handles combined voice and data throughout my campus and in my data center. Who can I partner with to extend that over the WAN? How can a service provider help me?
- **How can I extend multicast capabilities over a WAN?**  
We currently rely on videoconferencing and some vertical financial applications—all of which require multicast. Can a service provider help me extend these capabilities over the WAN without compromising the service quality of these and other multicast-dependent applications?
- **Can a service provider carry our QoS scheme transparently across the WAN?**  
We are converging voice, video, and data on our corporate network. QoS is a must for us—we have to be able to differentiate voice from data if we are to achieve adequate performance for voice.
- **How can a service provider guarantee that my traffic is secure?**  
In a shared infrastructure environment, how secure is my traffic? Will my traffic be compromised when it is co-mingling with traffic from other companies?
- **Can a service provider make sure that the transition to managed IP VPN services will be smooth?**  
Will there be any required changes to my existing network addressing scheme or routing protocols? What will be the impact on my users? What aspects of my network can I still retain control of and be able to monitor?

### Enterprises Moving to Full-Mesh Managed IP VPN Services

Today's enterprise networks are typically partially meshed or *hub-and-spoke* topologies. This design suits an organization with a central headquarters, where information predominantly flows to and from the headquarters and many branch offices or data centers. But hub-and-spoke topologies result in wasted bandwidth for interbranch offices traffic since everything must be sent to headquarters and then back out to a remote site.

Many enterprises consider a regionalized hub-and-spoke topology as an evolutionary improvement compared to a national hub-and-spoke network, and are moving from centralized to regionalized topologies as a result. The regional hub and associated local branches are connected to offload headquarters and improve regionalized interbranch traffic performance in terms of latency, jitter, and throughput. However, as a business grows or as companies merge and consolidate, this regionalized static topology also falls short in the long term when compared with the benefits of any-to-any connectivity offered by managed IP VPN services.

In contrast to enterprises, most service providers have already achieved any-to-any connectivity, or full-mesh network topologies. Enterprises that choose managed IP VPN services gain all of the advantages of a service provider's any-to-any connectivity. These include:

- **High availability:** A full mesh of alternate paths mitigates downtimes and the high-availability mechanisms built into a service provider's network enable the provider to deliver service level agreements (SLAs). SLAs define the specific terms or metrics regarding availability of resources, and give enterprises a contractual guarantee for network up time. SLAs can also define multiple levels of service, with low-cost alternatives for less critical traffic.
- **Security:** Network-wide monitoring and built-in security features can deliver an increased level of protection for enterprise customers.
- **QoS:** Service providers can offer scalable voice and video deployments and advanced Layer 3 QoS capabilities. Proactive monitoring, performance management, project management, customer service resources, installation and support services, and detailed network reports are other benefits that can be provided to enterprise customers and that can be applied to achieve the required QoS for VoIP, videoconferencing, video on demand (VoD), and other quality-sensitive applications and services.



- Multicast: A service provider's full-mesh network delivers multicast capabilities more efficiently, and can more selectively deliver those services to subscribers.
- Management: Service providers can extend network management efforts to include remote branches and teleworkers, and can carry out provisioning with minimal enterprise management overhead.

### **Enterprise Requirements for Consolidating Voice, Video, and Data Traffic**

Many of today's enterprise networks already support consolidated voice, video, and data traffic. Enterprises have invested time and resources to understand and characterize the handling requirements for the three distinct types of traffic, and have created the network environment to meet those requirements at the edge and throughout the campus core. For an enterprise to consider managed services for a portion of, or all of their networking needs, the enterprise must be confident in the service provider's ability to meet these requirements to handle the three distinct traffic types at the provider edge, and maintain the levels throughout the service provider core. The network attributes most critical for meeting these requirements include high availability, QoS, and management. Some enterprises may also have varied security requirements related to one of more of these traffic types.

#### **Voice traffic**

Voice traffic is smooth, benign, drop sensitive, delay sensitive, and involves User Datagram Protocol (UDP) priority. Bandwidth per call depends on the particular codec adopted, sampling rate, and Layer 2 media employed by the customer. Enterprise requirements for VoIP include:

- Latency 150 ms
- Jitter 30 ms
- Loss 1percent

#### **Video traffic**

Radically different from voice traffic, video traffic is bursty, bandwidth greedy, drop sensitive, and delay sensitive. IP-based videoconferencing does, however, have the additional latency, jitter, and loss requirements similar to VoIP.

#### **Data traffic**

The third category, data traffic, is much more varied than the voice or video traffic. It can be smooth or bursty, benign or greedy, drop and delay insensitive, and involves Transmission Control Protocol (TCP) retransmits. Traffic patterns for data vary among applications and even among different versions of the same application. Data classes must support several application categories: mission-critical, interactive, bulk data, best-effort (default), and optionally scavenger applications that take advantage of otherwise unused bandwidth.

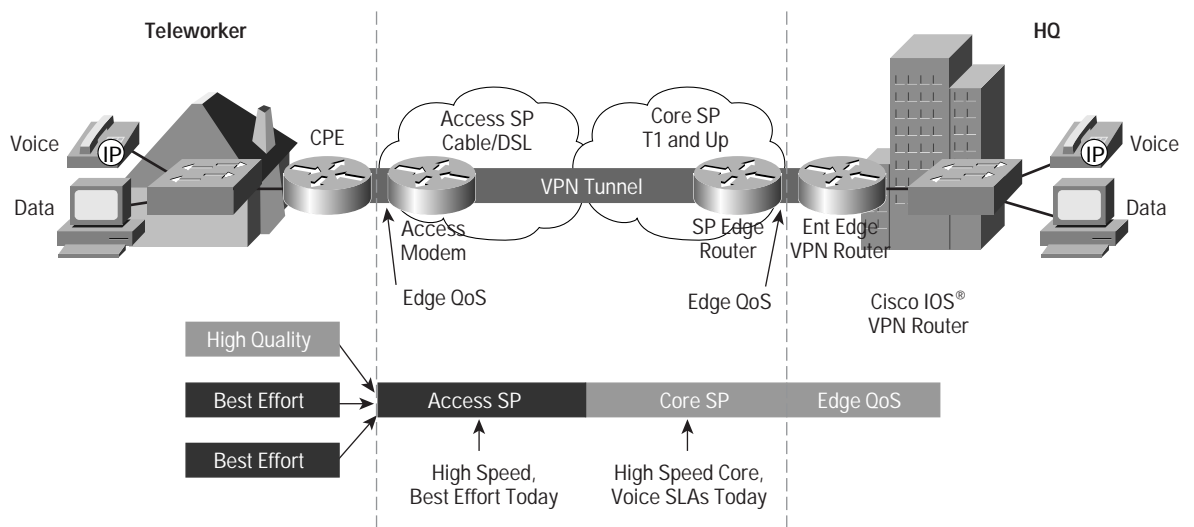
### **Enterprise Requirements for Teleworkers**

Most of the previously discussed enterprise WAN requirements concern a fixed location such as a corporate office, branch office, or data center. The enterprise also encompasses another segment of users: teleworkers, or those employees that work outside of the office. Teleworkers need to access their office resources from many places—work must travel with them instead of them traveling to work. Teleworkers' workplaces obviously include homes. Ideally, teleworkers want their in-home environment to experience the same voice and data capabilities that they have in the office. Wherever the teleworkers are, that's where they want to do business using the same tools. With enough bandwidth, teleworkers can have access to corporate resources and can also use applications like IP/TV and streaming VoD.



Service providers must offer managed IP VPN services that meet these teleworker requirements to take advantage of this huge and growing customer segment and increase revenue-generating services. QoS is particularly important for teleworker support, and management solutions must be able to reach these remote workers. While the per-month charges for home-based teleworker services appear to be lower than charges associated with branch office services, the revenue potential is significant due to the huge size of the rapidly growing teleworker market. A company with hundreds of branches typically employs thousands of workers, all of whom represent potential service users. Every enterprise today recognizes teleworker support as an essential part of the WAN requirement. Figure 2 illustrates how a service provider can deliver enhanced services to serve the rapidly growing teleworker market.

Figure 2  
Service Provider Delivery of Enterprise-Class Teleworker Services



### Ensuring Significant Returns on Investment for the Enterprise

Cost considerations continue to rank very high for any enterprise buying decision. Enterprise customers evaluating migration from existing network services, such as Frame Relay to managed IP VPN services, must see compelling cost advantages in cases of moving to similar speeds (T1 to T1, for example), and also in cases where customer wish to upgrade speed (512K to T1). Service providers must be prepared to detail the cost savings that will result from managed IP VPN services, and should also promote managed IP VPN services as a foundation for other managed services that can further reduce costs. The network attributes that will be the most critical for reducing costs and ensuring significant returns on investments for enterprise customers will be QoS, and to some degree high availability, since reducing network downtime can translate into savings for an enterprise. Similarly, a service provider's network management solutions can reduce support costs for an enterprise compared to the expenses associated with an in-house support team.



## Deployment Challenges for the Service Provider

The previous sections detailed the current set of business challenges faced by today's enterprises, and mapped those business concerns into several categories of requirements that must be met by a service provider. Table 1 summarizes those enterprise requirement categories and the network attributes that can meet those requirements.

Table 1 Enterprise Requirements and The Network Attributes That Address Those Requirements

Enterprise Requirement	High Availability	QoS	Multicast	Security	Network Management
Full-mesh networks (any-to-any connectivity)	X	X	X	X	X
Consolidating voice, video, and data traffic	X	X	X	X	X
Teleworker solutions		X		X	X
Ensuring significant ROI on network investments	X	X		X	X

Enterprise IT managers are constantly looking for solutions that directly address their business challenges and meet their specific requirements. Service providers must be able to demonstrate that their network offers the attributes that can meet those requirements. The five key network attributes—high availability, security, QoS, multicast, and simplified management—are the service provider's selling features for winning managed IP VPN services business from these enterprises. This section details each of these key network attributes, providing information about the deployment challenges associated with each, and the capabilities and features that the service provider network must support in each of these areas.

### High Availability

Business IT managers are demanding SLAs to ensure that service providers deliver the adequate level of services required for their needs. While service providers today have already built redundancy into their networks, the challenge is to accurately define the correct levels of service for a particular customer base. Enterprises are looking for service providers that can deliver—and verify satisfactory delivery of—the best levels of service for the price. The service provider that can successfully achieve high availability throughout the network can gain additional revenue and is able to offer enterprises many benefits and premium services such as guaranteed performance levels required for voice traffic, consistent end-to-end service, highly resilient traffic, and decreased fail-over times that minimize disruptions to end users.

### Security

The primary obstacle in this area involves overcoming a common misconception. Many enterprise customers perceive Layer 3 services as less secure than Layer 2 services. With Frame Relay networks, traffic passes over a common Frame Relay infrastructure protected by data encapsulation. An MPLS VPN is a "true peer VPN." Traffic separation happens at Layer 3 through the use of separate IP VPN forwarding tables. MPLS VPNs enforce traffic separation between customers by assigning a unique virtual route forwarding (VRF) value to each customer's VPN—users in a specific VPN cannot see traffic outside their VPN. Service providers offering managed IP VPN



services on a native IP network without MPLS can enhance security by leveraging IPSec, a flexible suite of encryption and tunneling mechanisms that ensures the confidentiality, integrity, and authenticity of data communications across a shared network infrastructure. These schemes exceed the security level in a Frame Relay or ATM network. Service providers will have to work closely with business customers to address and overcome this perception.

Some customers require additional security features. For example, the health care industry in the U.S. must comply with Health Insurance Portability and Accountability Act (HIPAA) regulations to protect patient privacy while accommodating the needs of health insurers, pharmacies, doctors, and other health care providers. In these cases, service providers can implement IPSec capabilities to enable encryption when health-care-related information is sent across a shared network infrastructure.

Protection from network attacks represents yet another customer requirement that must be addressed by the service provider. Wide-spread concern about malicious denial-of-service attacks, such as the D-DOS situation, require that service providers demonstrate what internal measures are in place that are capable of guarding against these attacks in a managed IP VPN environment. In most cases, service providers are substantially more equipped than most enterprises when fighting network attacks. Around-the-clock network security monitoring operations can quickly assure an enterprise of the security benefits associated with managed services.

## QoS

Network QoS refers to the overall integrity of the network and relates to the quality of the services being delivered over the network. A class of service (CoS) more specifically defines a particular level required for a traffic type (voice, video, or data) or the quality of the service:

- Gold: Guaranteed latency and delivery, applicable for voice
- Silver: Guaranteed delivery for e-commerce
- Bronze: Best-effort delivery, for e-mail, Web browsing

While service providers today typically offer these three classes of service, enterprises can require five or more:

- Level 4: Real time (voice, interactive video)
- Level 3: Business interactive (call signaling, SNA, Oracle, PeopleSoft, SAP, Telnet, etc.)
- Level 2: Real time (streaming video, network management)
- Level 1: Business LAN-to-LAN (Internet Web, IBM Lotus Workplace, Novell Groupwise, etc.)
- Level 0: Best-effort data (Simple Mail Transfer Protocol [SMTP], FTP, Internet Web, etc.)

To meet the CoS needs for all customers, service providers must be able to map their existing three CoS classes into multiple levels of service, or offer the flexibility of additional classes and locations. An SLA is put into effect as a contractual commitment of the service provider, and to define the specific CoS metrics. SLAs may contain a credit or refund stipulation for unmet CoS metrics. For each CoS, providers must be able to meet the latency and packet-loss criteria specified in the SLA, and implement pricing and reporting schemes that correspond with the offered classes of service.



## **Multicast**

Several popular applications—videocasts, network meetings, virtual whiteboard capabilities—depend on multicast. An enterprise with multicast requirements will need a service provider to demonstrate how multicast applications will be supported over the WAN, how multicast can be extended to remote branches and teleworkers, and the number of multicast streams that can be supported simultaneously.

## **Management**

Service providers offering managed IP VPN services must have management functions that meet or exceed the capabilities available within today's enterprises. These management functions must include:

- Preserving route type and route metric elements
- Ability to support the current and future numbers of unicast IP routes and discontinuous networks across VPN sites seamlessly
- Ability to facilitate performance management, fault identification and resolution, billing, reporting, and service addition/removal/change functions

## **How Service Providers Can Sell the Benefits of Managed IP VPN Services to Enterprises**

Cisco IOS<sup>®</sup> Software and a broad range of scalable Cisco platforms enable service providers worldwide to deliver Layer 2 and Layer 3 managed IP VPN services. Cisco IP VPN solutions offer end-to-end QoS capabilities and provide comprehensive management solutions and features for streamlining the provisioning process. They also empower service providers to offer their enterprise customers improved network performance, fewer design challenges, and lower support costs, as described below. These benefits of managed IP VPN services can be presented as benefits to potential customers during the selling process.

### **Improved Network Performance**

Managed IP VPN service providers can attract and retain customers by providing enterprises with improved overall network performance. The delivery of increased performance can be achieved by taking advantage of Cisco capabilities and technologies for:

- QoS
- Any-to-any network topology
- Higher availability (the inherent redundancy already built into the service provider's core network)
- Lower latency (packets can be routed on more direct physical paths over the service provider's WAN)
- Higher bandwidth (shared access to high-bandwidth links for rates lower than enterprise point-to-point connections)
- Multicast enabling features (packet replication performed more optimally)



### **Fewer Network Design Challenges**

Service providers can promote many network design benefits associated with managed IP VPN services. Service providers can eliminate the need for enterprises to engineer and manage capacity for point-to-point communications. Similarly, service providers can eliminate the necessity for customers to perform tasks associated with determining the optimum paths and routes for hub-to-spoke interconnections. Managed IP VPN services also save an enterprise the time and effort required to determine the capacity requirements when upgrading or adding new sites and users.

### **Lower Support Costs**

Service providers can relieve enterprise customers of inter-site connectivity issues and challenges. Enterprises will ultimately be able to enjoy reduced support costs since capacity upgrades for new applications can be more cost-effectively handled by the service provider. Managed IP VPN services also provide enterprises a migration path to converge data, voice, and video onto one network.

### The Cisco Difference: Service Enablers

The Cisco IOS Software technology provides many features that directly address the requirements and challenges to service providers associated with offering managed IP VPN services, and Cisco is committed to respond to dynamic industry requirements by continually enhancing Cisco IOS Software capabilities. When Cisco IOS Software is deployed at the customer equipment (CE) and at the provider equipment (PE) edges, service providers are uniquely positioned to offer greatly enhanced managed IP VPN services to enterprise customers. Cisco IOS Software technology provides many Cisco innovations that form a strong link between an enterprise network and a service provider's network, specifically at the CE-to-PE boundary. Prior to looking at the Cisco IOS Software features that strengthen the CE-to-PE link, first consider the challenges for the service provider at the CE-to-PE boundary. The service provider must be able to:

- Improve the handling of link and routing failures
- Deliver QoS at a basic and granular level of traffic
- Deliver cost effective services to multi-dwelling units (high-rise buildings) with many separate customers at one site
- Provide a smooth implementation of managed services with the least disruption to existing network design
- Effectively capture SLA measurements

With Cisco IOS Software bridging the CE-to-PE connection, all of these requirements are met. Six key Cisco IOS Software features embedded in Cisco software, establish a strong link between what enterprises need and what the service provider can deliver. These technologies include:

- Cisco Non-Stop Forwarding (NSF)
- Cisco AutoQoS
- Network-Based Application Recognition (NBAR)
- Multi-Virtual Route Forwarding (Multi-VRF)
- Robust routing protocol support
- Cisco Service Assurance Agent (SAA)



## **Cisco NSF**

To make the network highly available, Cisco NSF enables routers to continuously forward IP packets in the event of a route processor takeover, or switchover to another route processor.

Cisco NSF maintains and updates Layer 3 routing and forwarding information in the backup route processor. This ensures that the forwarding of IP packets and routing protocol information are continuous during the switchover and route convergence process. Cisco NSF eliminates router downtime and increases network availability during scheduled maintenance of a route processor and also during a route processor failure.

While Cisco NSF is critical to the core of the service provider network and helps to minimize disruption of service, Cisco NSF also comes into play at the CE-to-PE boundary. It provides each enterprise VPN customer an experience similar to using a dedicated leased line. Typically, at the provider edge, a Cisco-based PE router is fully NSF capable and enabled. At the customer edge, a smaller Cisco NSF-aware router is able to interact with the NSF process on the PE. In the event of a failure on the PE side, the PE router can route around the failure—providing full backup—across redundant route processors, with little or no impact to traffic.

## **Cisco AutoQoS**

An exclusive Cisco IOS Software feature, Cisco AutoQoS automates the configuration of QoS mechanisms and offers added intelligence at the PE-CE juncture. Service providers can drop-ship a pre-configured CE router to an enterprise site, configure QoS for greater flexibility at the PE side, and effectively deliver QoS throughout the enterprise. Cisco AutoQoS dramatically decreases deployment time for the service provider, which results in a lower cost of operation, and enables quicker startup times for the enterprise.

## **NBAR**

NBAR provides full classification capabilities up to Layer 7 (the application layer). It can be configured on the CE routers for full application-level classification. Specific enterprise applications—VoIP, enterprise resource planning (ERP), and supply chain applications like SAP—are designated with a Differentiated Services (DiffServ) classification or IP precedence level. At the PE side, NBAR can react to the assigned classification level and decide which class-based weighted fair queuing it assigns to the application, whether or not to drop the application, or guarantee bandwidth to a particular application.

## **Mutli-VRF**

This Cisco IOS Software exclusive feature provides virtual separation of traffic at the customer side, using multiple separate routing tables. PE capabilities can be extended down to the CE for better separation of traffic, without having to run separate distinct PE-to-CE lines and without requiring the service provider to deploy multiple CEs for multiple customers sharing a single site (for example, multiple customers in a high-rise building).

## **Robust Routing Protocol Support**

Cisco IOS Software offers the industry's broadest support of the most comprehensive and robust routing protocols. These include standards-based Routing Information Protocol (RIP), Open Shortest Path First (OSPF) Protocol, Border Gateway Protocol (BGP), Intermediate System-to-Intermediate System (IS-IS) Protocol, and the Enhanced Interior Gateway Routing Protocol (EIGRP), which is exclusive to Cisco. Based on the Diffusing Update Algorithm (DUAL), EIGRP brings the best features of a link-state protocol to IGRP while preserving the simplicity, improved



route summarization, multiprotocol support, and lower processing requirements of a distance vector protocol. EIGRP enjoys widespread deployment within Cisco-based enterprise networks, especially those originally deployed using IGRP.

Cisco supports fully encrypted, secure Message Digest Algorithm 5 (MD5) route exchange between all routing protocols supported, to ensure the identity of the CE and PE and the integrity of routing information. The wide range of CE-to-PE routing options supported by Cisco enables service providers to offer smooth migrations of existing enterprise architectures to managed IP VPN services by easily matching what each enterprise customer is currently using.

### Cisco SAA

Another feature exclusive to Cisco, Cisco SAA, uses preconfigured router probes embedded in Cisco IOS Software for detailed service-level measurements. Metrics can be used to monitor latency, jitter, packet loss, HTTP, TCP, UDP, Dynamic Host Configuration Protocol (DHCP), and individual application parameters measured from the CE to the PE or end-to-end from one CE to another remote CE. Cisco SAA measurement data can be massaged, stored in databases, and reported by the service provider to the enterprise customer for evaluating SLA delivery status.

### Summary

The Cisco technologies benefit both service providers and their enterprise customers (see Table 2). By serving to strengthen the PE-to-CE edge, Cisco IOS technologies contribute to the success of the service provider in the managed services arena.

Table 2 Examples of Cisco IOS Software Technology Enablers

Cisco IOS Software Technology Enablers	Enabled Network Attributes	Benefits to Enterprises	Benefits to Service Providers
<b>Cisco Non-Stop Forwarding (NSF)</b>	High Availability	Greater uptime and lower network outages	Fewer penalty payments due to downtime
<b>Cisco AutoQoS</b>	QoS	Eases access to QoS services	Reduced operating expenses (OpEx) and quick deployment turnaround
<b>Network-Based Application Recognition (NBAR)</b>	QoS	Enables segregation of traffic for better network utilization	New revenue streams due to "granular QoS"
<b>Multi-VRF (VRF Lite)</b>	Management	Eases access to reduced-cost services	Reduced capital expenditures (CapEx); eliminates parallel copper/fiber pairs
<b>Broadest robust routing protocol support</b>	Management	Access to robust, secure routing protocol options with least disruptions	Eases entry point into new subscriber markets and enables new revenue streams
<b>Cisco Service Assurance Agent (SAA)</b>	Management	Access to comprehensive SLA reports	Access to comprehensive SLA reports



Adding up the benefits of these features, Cisco IOS Software at the PE-to-CE edge gives service providers a strong advantage for growing managed IP VPN services revenues:

- Enhanced service delivery opportunities and reduced deployment overhead
- Robust and flexible service offerings for reducing an enterprise's total cost of ownership (TCO)
- Improved management, administration, and SLA delivery

For More Information

For more information about Cisco VPN solutions and services, go to:

<http://www.cisco.com/go/vpnsolutions>

<http://www.cisco.com/go/vpnservices>

APPENDIX: Managed IP VPN Services Case Studies

#### Bell Canada

Canada's leading Internet service provider, Bell Canada, offers connectivity to residential and business customers through wired and wireless voice and data communications, high-speed and wireless Internet access, IP broadband services, and e-business solutions. The company's managed IP VPN enterprise service delivers secure, scalable access to information at any time from anywhere, over a carrier-class IP network.

The Bell Canada VPN Enterprise service lets customers consolidate voice, data, and video on one network, and provides customers access to a Web portal for self-provisioning bandwidth and quality of service on demand, viewing reports, placing orders, and paying for services. One customer, St. Joseph's Healthcare in Hamilton, Ontario, performed the world's first hospital-to-hospital telerobotics assisted operation over Bell Canada's state-of-the-art national IP backbone. A three-armed robot directly translates a surgeon's natural hand, wrist, and finger movements, allowing the surgeon to operate on a patient hundreds of miles away. For the complete story on this application, please visit: [http://newsroom.cisco.com/dlls/prod\\_030403.html](http://newsroom.cisco.com/dlls/prod_030403.html)

The results of the Bell Canada deployment include:

- Business customers can conduct e-commerce and share content with their customers and partners on a secure, flexible, high-speed private network over the provider's IP backbone
- Customers incur lower support costs by letting Bell Canada host, manage, and administer VPN services
- Customers have the flexibility to choose managed services for some or all of their network services
- Access is delivered internationally for truly global networking.

**"The IP VPN Enterprise service takes the flexibility of the Internet, adds to it a class of service capability, and offers businesses a way to improve their organization from the inside out, rather than from the outside in."**

*Jeremy Wubs, IP VPN Enterprise Product Manager, Bell Canada*



## Cable & Wireless

A major global telecommunications business, Cable & Wireless offers a full range of services in 33 countries. The company focuses on IP and data services and solutions for business customers, and has developed advanced IP networks and value-added services in the U.S., Europe, and the Asia-Pacific region. Cable & Wireless operates an IP network powered by Cisco Systems®. Cable & Wireless teamed up with Cisco® to expand its advanced IP networks and value-added services in response to growing demand for managed IP VPN services, and converged telephony and data applications, especially in the U.K.

The company has successfully expanded its IP network with additional Cisco routers and switches, all running Cisco IOS Software. The company has packaged managed IP VPN services that carry e-mail, Internet and intranet traffic, and other traffic including voice, audio, and video. Different contract management options can scale to accommodate thousands of users. QoS services enable converged data, voice, telephony, and video traffic between offices, partners, and suppliers with an optional firewall-protected connection to the Internet and extranets.

The results of the Cable & Wireless deployment include:

- Expanding the number of countries served
- A highly secure and cost-effective solution portfolio for business customers
- Flexible deployment and management features
- Common infrastructure for telephony, Web, videoconferencing, and other IP applications

**“What our customers really want are full service level agreements for each class of service for the efficient transport of applications. Cable & Wireless delivers that capability. With Cisco as a key technology partner, we’re now perfectly positioned for the global market with a leading product and service offering.”**

*Tony de Vizio, Product Manager for IP-VPN QoS service, Cable & Wireless*

## Equant

Equant, a premier European provider of global IP and data services, offers network integration and managed services to multinational businesses. More than 50 years of experience in data communications are behind the company’s extensive portfolio, services including IP Telephony (IP dial and dial access service), Voice for IP VPN, and IP VPN (an MPLS-based IP VPN data service). Its managed IP VPN services have been delivered over a Cisco network since their introduction in 1997. Recently, Equant announced its global IP Telephony service using Cisco IP telephony technology over a Cisco Multiservice VPN architecture to deliver IP telephony and converged voice, video, and data across LANs and WANs. Equant chose to work with Cisco because of the long history of collaboration between Equant and Cisco, the proven Cisco products and their ability to address large sites, and the ability of the Cisco Multiservice VPN architecture to provide seamless integration into the existing Equant network.

The newest Equant managed service provides customers with:

- Value-added IP telephony features and applications, and converged voice, video, and data
- Abbreviated private dialing plans on a global basis
- Least-cost routing
- Call overflow on access or termination if the network is busy
- Ability to pay only for bandwidth used to carry voice calls (no usage-sensitive charges)

**“Over the years, Equant has worked collaboratively with Cisco to deliver integrated voice and data services. Through our collaboration, Cisco and Equant have developed a strong partnership. Cisco’s product support and account teams have always gone the extra mile and Cisco has always been able to provide the leadership and robust technology required to ensure Equant’s success in offering value-add managed services to our customers.”**

*Michael Burrell, Senior Product Manager, Equant*



## Infonet

Infonet Services Corporation, a leading provider of value-added global communications, offers innovative network-based solutions to more than 2,600 multinational clients. The company's global project management capabilities are the foundation for services that span broadband, Internet, intranet, multimedia, remote and local access, provisioning, and application and consulting services. Infonet employs a Cisco VPN architecture to offer enhanced and streamlined managed IP VPN services. Cisco IOS Software features simplify routing, allow labels to carry directional as well as class-of-service and security information, and allow for diversified, secure network applications on IP VPNs.

The Cisco IP VPNs deployed by Infonet, ranging from point-to-point, hub-and-spoke to "connectionless" Layer 3 private virtual circuits, offer many improvements to their enterprise customers:

- Simpler and more cost-effective deployments
- Simplified management using Cisco traffic engineering
- Smoother path to new services
- Much greater scalability, privacy, and security for corporate VPNs
- SLAs that can be accurately measured

**"... VPNs have become much easier to deploy and scale. You can configure the virtual circuits centrally across the IP network, so it's also a lot easier and cost effective to manage."**

*Joe Fusco, Director of Private IP Services, InfoNet*



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.  
Capital Tower  
168 Robinson Road  
#22-01 to #29-01  
Singapore 068912  
www.cisco.com  
Tel: +65 6317 7777  
Fax: +65 6317 7799

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

All contents are Copyright © 1992–2003 Cisco Systems, Inc. All rights reserved. Cisco, Cisco Systems, Cisco IOS, Cisco Powered Network, and the Cisco Systems logo are registered trademarks or trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other trademarks mentioned in this document or Web site 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.  
(0304R) ETMG 203098—LH 08/03