White Paper

From Frame Relay to IP VPN: Why to Migrate, Why to Out-Task

Executive Summary

Migrating a corporate network from a conventional Layer 2 Frame Relay to a Layer 3 IP-based virtual private network (VPN) offers strategic and tactical advantages to companies of any size, from large multinational enterprises to small and midsized businesses. IP VPNs can be based on native IP, Multiprotocol Label Switching (MPLS), IP Security (IPSec), or a combination of these technologies. This white paper does not distinguish between the technologies except when only one of the implementations provides a particular business benefit.

The primary advantages of IP VPNs in general include:

- Reduced network costs
- Enhanced ability to provide network connectivity to geographically dispersed branch offices, remote users, teleworkers, and business partners
- Convergence of previously disparate data, voice, and video networks, which reduces costs and enables the introduction of new productivity-enhancing IP-based applications
- Easier deployment of IP-based applications such as Enterprise Resource Planning (ERP), e-learning, and streaming video
- Improved scalability

Businesses that transition to IP VPNs can realize further benefits by selectively or totally out-tasking the management of network transport, equipment, and network security to a service provider that offers managed IP VPN services. Out-tasking frees the company to focus on its core business and improves the availability and security of the network by ensuring that skilled resources are available 24 hours a day from the service provider. Network performance is assured when companies select a service provider that can offer service-level agreements (SLAs). Out-tasking also can give companies access to valuable network support services that are too costly or impractical to provide with in-house resources, such as problem resolution via 24-hour help desks.

This white paper explains considerations for companies that are evaluating migration from Frame Relay to IP-based VPNs. It compares the two technologies, discusses the business and technical advantages of migration, and explains the benefits of out-tasking to a service provider. The paper concludes with criteria for selecting a service provider that will deliver outstanding availability, quality of service (QoS), network security, manageability, and multicast support.

Comparing Frame Relay and IP VPN Capabilities

Table 1 compares how well Frame Relay and IP VPN networks meet business requirements for enterprises and small and midsized companies.

Table 1 Frame Relay and IP VPN Comparison

Criteria	Frame Relay	IP VPN
Low Cost	• Service providers charge more for a Frame Relay permanent virtual circuit (PVC) than for an IP VPN • Usually requires two PVCs per site	• Eliminates the need for a PVC • Reduces network cost and site access charges • Enables consolidation of data, voice, and video traffic
Scalability	• Scalability is challenging for very large, fully meshed Frame Relay deployments	• Is highly scalable, especially in a network-based IP VPN because no site-to-site peering is required • Greatly simplifies WAN operations
Rapid Service Deployment	• Typically from 1 to 7 weeks for a new PVC	• No PVC configuration is required; fast time to deployment
Flexibility	• Typically deployed for site-to-site connectivity between corporate and branch offices only • Does not allow controlled access to extranet partners	• Extends the network to remote branch offices, extranet, and mobile workers with one simple connectivity approach • Enables secure extranet with partners, suppliers, and resellers
Support for IP-based Applications	• Designed for Layer 2 transport • Has no knowledge of upper layer traffic and offers little added value to upper layers	• Provides the foundation to deploy enhanced IP-based services that are not viable over Frame Relay, such as unified communication, multicast video, extranet, remote access, and network security services
Geographic Coverage	• Limited to service provider service area	• Improves geographic coverage and offers the framework for global connectivity
Remote Access	• Does not typically offer remote access	• Extends network security to mobile workers and telecommuters
Network Security	• Relies on traffic separation for data transport security	• Provides security equivalent to or better than Frame Relay, depending on customer’s choice of MPLS or IPSec VPN technologies; use of strong encryption standards in IPSec, such as Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES), makes the VPN more secure than Frame Relay

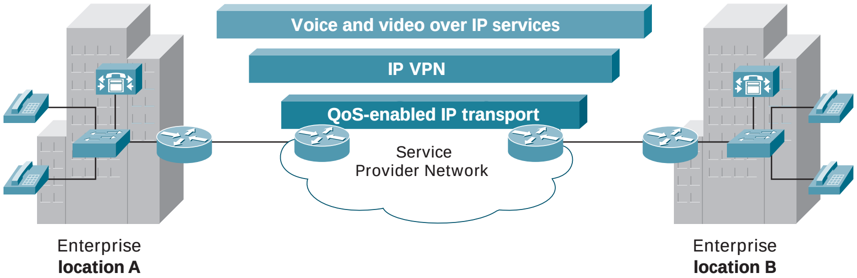
Why Migrate from Frame Relay to IP VPN?

Migrating a corporate network from Frame Relay to IP VPN has become an attractive business strategy because of evolving changes in business application requirements and advances in VPN flexibility, ease of management, and cost efficiency.

Support for Today's Applications and Future IP-Based Applications

An IP-based VPN infrastructure enables rapid, enterprise-wide deployment of IP-based applications such as ERP, e-learning, hosting, telephony, e-mail suites, centralized application services, and video services. While it is possible to offer some of these applications with Frame Relay, deployment is far simpler on IP VPNs, and IP VPNs offer greater geographic reach. In addition, IP VPNs provide the foundation to offer other value-added IP-based managed services that are not viable over Frame Relay, such as unified communication, multicast video, and extranets. The Cisco® IP VPN architecture (Figure 1) helps ensure compatibility with network security solutions and IP-based applications.

Figure 1
Cisco VPN Architecture



In addition to supporting emerging new applications, an IP VPN provides a migration path for a company's existing applications that are not IP-based. An example is a company that wants to begin using IP telephony but needs to continue using a traditional inventory system that would be difficult to migrate to IP. The company can continue to use its non-IP applications by using generic routing encapsulation (GRE) tunneling over the IP VPN. The resulting converged backbone would support both IP-based applications and non-IP applications.

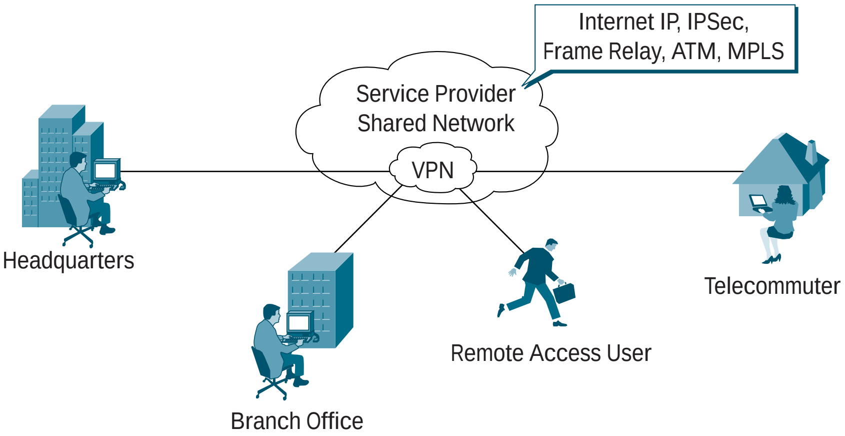
Support for Geographically Dispersed Branch Offices and Mobile Workers

Frame Relay networks typically are limited to the geographical service area of the service provider, preventing companies from easily providing network access to their branch offices outside of the service area. In fact, multinational companies with Frame Relay networks must resort to establishing and maintaining relationships with one or more service providers in every country in which they operate. By migrating to IP VPN, companies often can consolidate their contracts with fewer service providers, which reduces costs and simplifies support, monitoring, and payment. The reason is that many service providers are beginning to offer greater coverage for their IP VPNs than for their Frame Relay networks. And even if the company has remote branch offices and mobile workers outside of the service provider's VPN coverage area, these users can access corporate resources via the Internet, using a local Internet service provider (ISP).

Ability to Extend Network Access to Teleworkers

Providing network access to remote users over Frame Relay typically requires provisioning a separate PVC at each site—a time-consuming and expensive process. What's more, the company incurs recurring charges from the PVC. Remote-access VPNs provide a diverse and more cost-effective means of connecting mobile users, teleworkers, and others to the company's intranet over the service provider network or public Internet (Figure 2). Users can securely connect to the network wherever there is Internet access, via dialup, DSL, cable, or wireless technology.

Figure 2
VPN Archecture Options



Ability to Extend Extranet Applications to Business Partners

With an IP VPN, companies can securely extend network access to partners over the public Internet, without provisioning a PVC. In fact, if a company's suppliers and partners are served by the same service provider, it can provision an extranet VPN between the suppliers and the corporate resources, distinct from the intranet used to connect headquarters and branch offices. This adds another layer of network security by preserving the integrity of the corporate network.

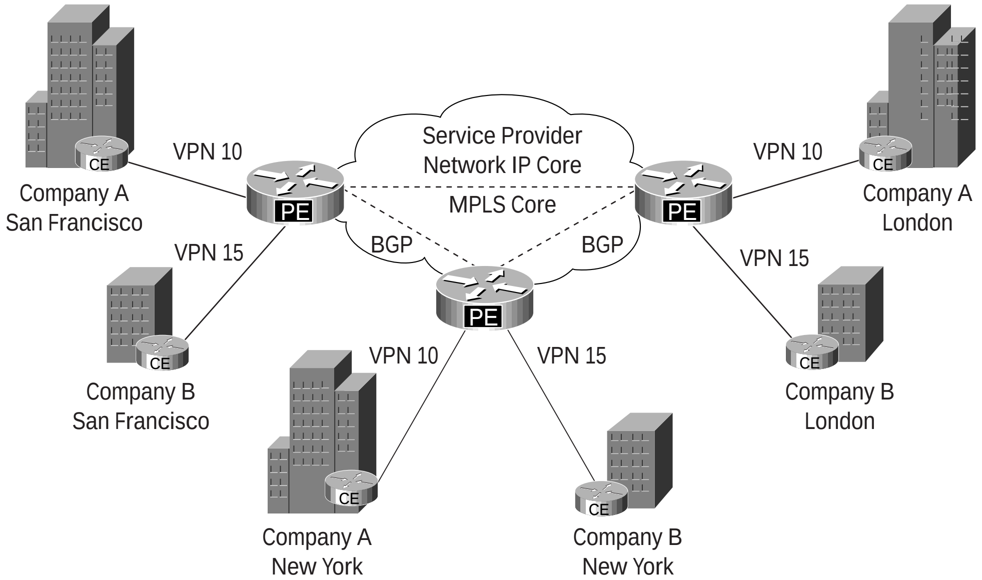
Simplified Scalability

In a typical Frame Relay fully meshed topology, all branch offices and headquarters must establish a point-to-point peer link with every other office. Adding a new site typically requires updating the router configuration at all other peer sites: headquarters, other branches, and partner offices on the network. This increases costs and complicates scalability as the company grows and adds new sites. In addition, point-to-point peering adds complexity in terms of managing and monitoring latency and delays and using bandwidth efficiently.

Companies with high-scalability requirements can take advantage of MPLS-based VPNs. These VPNs scale far more easily than Frame Relay networks because they use a local-peering model and Layer 3 connectionless architecture. With a local-peering model, a customer site need only "peer" with the provider-edge (PE) router to which it is attached, as opposed to all other customer premises equipment (CPE) or customer-edge (CE) routers on the VPN (Figure 3). The connectionless architecture, in turn, allows the creation of VPNs in Layer 3, eliminating the need for point-to-point tunnels or virtual circuits that inhibit scalability.

Figure 3

VPN—Multiple Customers and Services over a Single Network Infrastructure

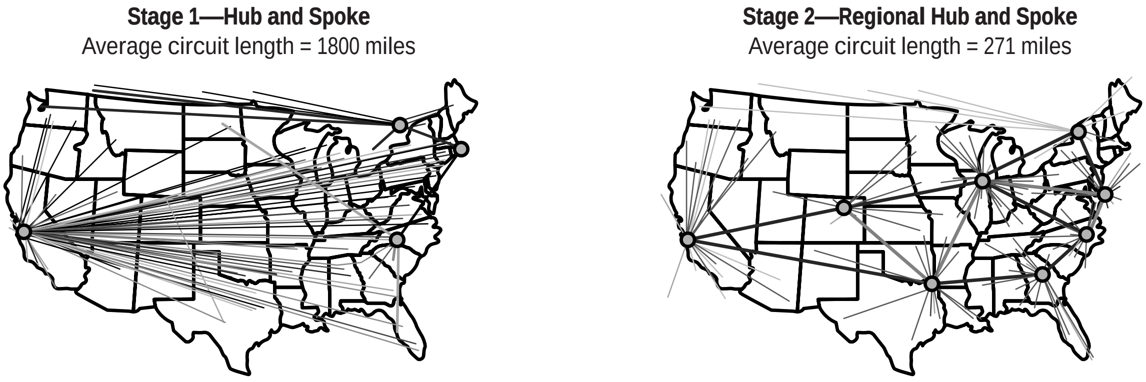


Simplified Transition to Regional Hub-and-Spoke Network

IP VPNs also facilitate the transition from a national hub-and-spoke network to a regionalized hub-and-spoke network (Figure 4). A regionalized network topology eliminates the need for localized, regional-based communications to be routed through the headquarters, and thereby reduces network traffic between the region and increases performance.

Figure 4

Enterprise WAN Evolution


Stage 1—Hub and Spoke
Average circuit length = 1800 miles
Stage 2—Regional Hub and Spoke
Average circuit length = 271 miles

- Topologies not suited for any-to-any voice/video/collaboration type of traffic
- Lack of control over delay; wasted bandwidth on site-to-site traffic

Reduced Costs

In many cases, enterprise customers dramatically reduce monthly connection costs by migrating from Frame Relay networks to IP VPNs. For example, Cisco customer Lante Corporation, of Chicago, Illinois, was spending US$34,500 per month in Frame Relay charges for connecting its headquarters and four branch offices. After migrating to an IP VPN, Lante Corporation reduced its monthly network charges to US$13,250—a savings of 61 percent—as detailed in Table 2.

Table 2 Cost Savings with IP VPN Migration

	Frame Relay			VPN	
Location	**Circuit**	**Function**	**Cost per Month (U.S. Dollars)**	**Internet Circuit**	**Cost per Month (U.S. Dollars)**
Chicago	DS3	Internet	$8,200	DS3	$5,600
Chicago	DS3	Frame Relay	$10,500	DS1	$850
Chicago	T1	Internet for redundancy	$2,100		
New York	T1	Frame Relay	$2,700	T1 x 2	$1,700
Seattle	T1	Frame Relay	$3,000	T1 x 2	$1,700
Houston	T1 x 2	Internet (traditional from acquired company)	$4,000	T1 x 2	$1,700
Dallas	T1 x 2	Internet (traditional from acquired company)	$4,000	T1 x 2	$1,700
TOTAL			$34,500		$13,250
		TOTAL MONTHLY COST SAVINGS: US$25,250 PERCENTAGE SAVINGS: 61%			

The potential cost savings to be gained from migrating to IP VPN are on the rise as the costs of low-speed Frame Relay connections increase in some regions. Network World Fusion reported in April 2003 that some companies are paying up to twice as much today for low-speed Frame Relay than they did 18 to 24 months ago. Therefore, they stand to save even more now than in the past by migrating to an IP VPN service.

Why Out-Task VPN Service Management?

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

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

America, July 2002.) In its 2003 report, the Yankee Group summarized business benefits experienced by several companies that migrated from Frame Relay to IP VPN, including companies that out-tasked to a managed IP VPN service provider (see sidebar).

Following are the primary incentives for enterprises to out-task VPN service management.

Free Up Resources to Focus on the Core Business

By working with a service provider for managed IP VPN services, companies can delegate the routine tasks they do not see a compelling reason to control, such as daily monitoring, support, provisioning, transport, and router maintenance (see sidebar). At the same time, they free up staff resources to focus on the core business as well as strategic initiatives such as network design and planning.

Out-Tasking Options

Following are IP VPN service management components that businesses might consider out-tasking.

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

Reduce Costs

Gartner Dataquest reports that large enterprises in the United States that out-task network management to service providers cut their network costs by up to 25 percent, while small U.S. businesses can experience up to 15 percent cost reductions. In fact, access to the service provider’s lower cost structure, the result of a greater economy of scale, is one of the most compelling tactical reasons for out-tasking, according to The Outsourcing Institute of Jericho, New York. The service provider can charge less than its customers would otherwise spend for operations, maintenance, service, equipment, and technology upgrades.

Companies that out-task network management not only reduce their costs, they make recurring costs more predictable by shifting from a variable to a fixed cost model. Businesses that out-task know their monthly costs in advance, as compared to businesses that need to find the budget for unexpected expenses related to network upgrades or outages. Out-tasking also enables “pay-as-you-grow” scalability, eliminating the need to overpurchase at the outset of service deployment to accommodate anticipated growth.

Gain Expertise and Support Not Available In-House

Service providers often can provide networking skills not available internally within the enterprise. The value of this benefit increases as companies add more applications and users, and as network management becomes more complex. Service providers have the resources to offer 24-hour monitoring, management, and support—capabilities not readily available in-house to any but the largest enterprises. Service providers also can offer rapid deployment because of their deployment experience. Even for companies with large in-house staffs, service providers can fill critical resource gaps such as network security, which typically requires special training and expertise.

In a 2003 report, the Yankee Group summarized the business benefits experienced by several companies that migrated from Frame Relay to IP VPN, including companies that out-tasked to a managed IP VPN service provider (see sidebar).

Frame Relay to IP VPN Migration Case Studies

The following summaries appeared in a Yankee Group report published in May 2003, titled “*Navigating the IP VPN Market: A Decision-Making Guide for European Businesses*”

British American Tobacco Group plc, based in London, England, migrated from Frame Relay to an IP VPN as part of a larger strategy to reduce costs not related to manufacturing. Now the company is using the IP VPN for several trials of IP-enabled applications intended to increase productivity and profitability, including Web conferencing, Wi-Fi, and DSL for remote access and home users, as well as IP telephony, which probably will be used for in-country voice.

HJ Heinz, the international food manufacturer, migrated to IP VPN and out-tasked to a service provider that would manage all 37 European sites. The company achieved both of its goals: to gain a better view of total network costs and to reduce mobile phone usage. To date, HJ Heinz has installed more than 7000 IP phones and soft phones at remote sites. IP telephony has allowed HJ Heinz to conduct moves, adds, and changes 86 percent faster than with a PBX, and has freed IT staff to focus on other projects. Mobile phone usage is down because employees traveling between sites use the soft phones. The availability of voice mail has increased productivity by up to 25 percent for some employees. The savings achieved through the IP telephony implementation helped pay for an E1 connection to sites with existing E1s, effectively doubling bandwidth at a savings of more than 60 percent compared to a Frame Relay network.

Outokumpu, with headquarters in Espoo, Finland, is an international metals and technologies business with more than 20,000 employees across 200 sites. The company decided to migrate some locations from Frame Relay to IP VPN, primarily to support IP-based applications such as a global SAP system and a pilot VoIP initiative.

Criteria for Assessing Service Provider Capabilities

Service providers that offer IP VPNs typically provide varying levels of high availability, network security, QoS, manageability, and multicast support, depending on their network infrastructures. By evaluating prospective service providers according to the following criteria, companies can determine which service provider can best meet their IP VPN requirements.

High Availability

Frame Relay networks are inherently very stable. Companies planning to migrate to IP VPN need assurance that their prospective service provider will meet or exceed current availability levels. Service providers typically demonstrate their ability to deliver high network availability by offering service-level agreements (SLAs). When an SLA is in place, the service provider incurs a penalty or must provide a credit if the service level falls below an acceptable level stipulated in the SLA agreement.

To acquire the confidence to offer an SLA, service providers bolster their networks with one or more of the following techniques:

- Network redundancy
- Fast routing convergence to route traffic around trouble spots
- Traffic engineering to improve traffic distribution and network usage

Service providers can more easily afford these techniques because they can amortize the costs over multiple customers.

Network Security

Service providers with robust security infrastructures and support processes can ensure that their customers' migration from Frame Relay (Layer 2 technology) to IP VPN (Layer 3 technology) is achieved without compromise to network security. Service providers that offer IP VPN services will provide all or a subset of the following network security features and services:

- Traffic separation
- Control route distribution
- Data encryption
- Policy-based access control
- Real-time intrusion detection and auditing
- Monitoring of denial-of-service (DoS) attacks

Quality of Service

Quality of service (QoS) refers to the capability to provide predictable performance and better service to specific classes of network traffic. Primary goals of QoS include dynamic bandwidth allocation for mission-critical applications and prioritization of delay-sensitive traffic such as voice and video. QoS mechanisms include queuing, network congestion avoidance, traffic shaping, and packet classification.

By deploying specific QoS mechanisms to manage delay, delay variation (jitter), bandwidth, and packet loss on a network, service providers can achieve the level of end-to-end QoS that their enterprise customers require. Companies concerned with QoS should ask whether the prospective service provider has the following QoS capabilities:

- Preserving QoS service type (voice, video, or data) and prioritization of delay-sensitive traffic across the entire VPN infrastructure
- Maintaining multiple classes of services across the VPN
- Offering SLAs around latency and packet loss
- Offering the option to add more classes and locations as needed

Manageability

Service providers that offer IP VPNs must provide network management services that can meet or exceed those available in-house. Depending on their business needs, companies should look for service providers that can offer some or all of the following network management capabilities:

- Ability to preserve route type and route metric elements so that the migration to IP VPN does not require costly upgrades within the enterprise's internal network
- Ability to support current and future number of unicast IP routes and non-contiguous networks across VPN sites
- Performance management
- Fault identification and resolution
- Billing
- Reporting
- Service add, remove, and change management

Multicast Support

To support current and future multicast services, such as e-learning and corporate broadcasts, companies should look for a service provider that supports:

- Multicast extension to remote branch locations and teleworker
- Required number of simultaneous multicast streams

Cisco Powered Network Member Service Providers

When both the service provider and its customer use Cisco IOS® Software, the customer acquires the highest levels of availability, network security, QoS, manageability, and multicast support. The reason is that Cisco Systems® has developed a set of leading-edge technologies for provider-edge and customer-edge devices. Therefore, when a customer with Cisco equipment out-tasks a fully managed IP VPN service to a service provider with an end-to-end Cisco network, the customer gains additional benefits from the exclusive Cisco innovations described in Table 3.

Table 3 Cisco IOS Software Features and Benefits

Exclusive Cisco IOS Software Feature	Description	Benefit for Enterprise Customers
Nonstop Forwarding (NSF)	At the customer edge, a small NSF-aware router is able to interact with the NSF process on the provider edge. In the event of a failure on the provider-edge side, the provider-edge router can route around the failure—providing full backup—across redundant route processors, with little or no impact to traffic.	• Improves uptime. • Enables service provider to confidently offer SLAs to its custome**rs.**
AutoQoS	AutoQoS automates the configuration of QoS mechanisms and offers added intelligence at the juncture of the provider edge and customer edge. Service providers can drop-ship a router to an enterprise site, configure QoS for greater flexibility at the provider-edge side, and effectively deliver QoS throughout the enterprise. AutoQoS dramatically decreases deployment time and cost of offering QoS.	• Speeds implementation of QoS services.
Network-based Application Recognition (NBAR)	NBAR provides full classification capabilities up to Layer 7, the application layer. It can be configured on the customer-edge routers for full application-level classification. Specific enterprise applications are designated with a Differentiated Services (DiffServ) classification or IP precedence level. At the provider-edge side, NBAR can react to the assigned classification level and decide which Class-Based Weighted Fair Queuing (CBWFQ) it assigns to the application, whether to drop the application, and whether to guarantee a particular bandwidth to the application.	• Enables classification of traffic and bandwidth allocation based on required class of service (CoS).
Multi-VPN Routing and Forwarding (VRF)	Exclusive to Cisco equipment, this feature provides virtual separation of traffic at the customer side, using multiple separate routing tables. Multi-VRF enables provider-edge capabilities to be extended down to the customer-edge router for better separation of traffic. It does not require separate distinct provider edge to customer-edge lines or require the service provider to deploy multiple customer-edge routers for multiple customers sharing a single site—for example, in a high-rise building.	• Lowers capital costs for companies located in high-rise buildings because multiple companies can share a single router and provider-edge to customer-edge lines.
Broad Support for Routing Protocols	Cisco IOS Software supports major routing protocols: Routing Information Protocol (RIP), Enhanced Interior Gateway Routing Protocol (EIGRP), Open Shortest Path First (OSPF) Protocol, Border Gateway Protocol (BGP), and Intermediate System-to-Intermediate System (IS-IS) Protocol.	• Allows access to robust, secure routing-protocol options with least disruption.
Service Assurance Agent (SAA)	SAA uses preconfigured router probes embedded in Cisco IOS Software for detailed service level measurements. Metrics can be used to monitor jitter, Hypertext Transfer Protocol (HTTP), Transport Control Protocol (TCP), User Datagram Protocol (UDP), Dynamic Host Configuration Protocol (DHCP), and individual application parameters measured from the customer-edge to the provider-edge router or end-to-end from one customer-edge router to another remote customer-edge router.	• Enables the service provider to create comprehensive SLA reports. SAA measurement data can be massaged, stored in databases, and reported by the provider to the enterprise customer for evaluating SLA delivery status.

Companies can identify service providers that deliver the enterprise capabilities described above by their membership in the Cisco Powered Network program. The Cisco Powered Network designation indicates that a service provider builds its service on Cisco equipment end-to-end and follows best practices in design, operations, and maintenance. Companies that choose a service provider offering Cisco Powered Network designated services gain the assurance of end-to-end quality; simplified, cost-efficient network management; higher network availability; and services that are more reliable, scalable, secure, and easy to deploy and expand as business needs change.

Conclusion

By migrating from Frame Relay to IP VPN, companies gain both tactical and strategic advantages. In the near term, companies benefit from cost-effective, secure network connectivity to branch offices and secure access to remote workers, teleworkers, and partners around the world. In the long term, they position themselves to benefit from emerging value-added, IP-based applications without difficulty and to scale with little effort or cost to add more users and applications. These applications ultimately improve productivity, increase competitiveness, and reduce costs.

Out-tasking VPN service management introduces additional benefits to enterprises and small and midsized businesses alike. By out-tasking some or all of IP VPN service management to a service provider, companies free up their in-house resources to focus on the core business. They shift from a variable to predictable cost structure for recurring network management costs, and eliminate the need to overpurchase to accommodate anticipated growth. Network availability, QoS, and network security often exceed what would be possible with in-house VPN management because service providers offer SLAs, provide highly-skilled staffs available 24 hours a day, 365 days a year, and have invested in a secure infrastructure that can be used for multiple customers.

Service providers that are members of the Cisco Powered Network program have the capability to offer the best possible availability, QoS, network security, multicast support, and management—essential ingredients for a reliable, trouble-free, scalable network.

To search for service providers offering Cisco Powered Network designated managed IP VPN, visit: http://www.cisco.com/cpn.

White Papers and Presentations

Numerous white papers including those listed below are available to help in the out-tasking decision process. To find these and other resource materials, visit http://www.cisco.com/cpn.

- Cisco Powered Network Outsourcing Guide
- Finding the Network Service Provider Who Won’t Let You Down
- Outsourcing Managed Network Services
- Getting the Most from Your Service Provider: The Technical Advantages of Using a Cisco Powered Network Designated Service
- Choose a Service Provider with the Cisco Powered Network Designation

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

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

ETMG 203098—LH 09/03