Customer Profile

Infonet—Global IP VPN Service is More Secure, Scalable, and Versatile using MPLS and BGP Features in Cisco IOS Software

"Using MPLS, VPNs have become much easier to deploy and scale," says Joe Fusco, Director of Private IP Services at Infonet. "You configure the virtual circuits centrally across the IP network, so it's also a lot easier and cost effective to manage."

EXECUTIVE SUMMARY

BACKGROUND

Infonet Services Corporation is a leading provider of value-added global communications services to over 2,600 multinational clients, providing innovative network-based solutions to support the business needs of our clients.

Using a unique consultative approach to gain insight into the needs of our clients, Infonet offers solutions that optimize the relationship between enterprise applications and network infrastructures. Our global project management capabilities are the foundation for the services that constitute our solution offerings (broadband, Internet, intranet, multimedia, remote and local access, provisioning, application and consulting services), positioning Infonet as the ideal single-source partner for multinationals.

CHALLENGE

In an effort to reduce network costs while optimizing and expanding its IP VPN services, Infonet researched effective solutions. As part of selecting what would be the company's third generation of backbone routers, Infonet's network engineers became aware of Cisco's newest architecture and software features for IP VPNs, and embarked upon developing enhanced and streamlined IP VPN solutions.

Infonet, an international service provider with 140 points of presence (POPs) globally and a multinational Global 1000 clientele, has had an Internet Protocol (IP)-based network since 1991. Through the 1990s the company's clientele enjoyed the benefits of extending their corporate networks regionally and internationally to major and minor offices, through various network protocols and provider backbones as virtual private networks (VPNs). In the middle of 1999, the company took a major step forward, retooling its Cisco Powered Network with Cisco 12000 Series Internet routers for its optical IP networking core backbone, Cisco 7500 Series and 7200 Series Internet routers for the edge, and Cisco 2500, 2600, and 3600 Series routers for installation in customer premises. This hardware was only part of the build out, which was also based on implementation of Cisco System's IP VPN solutions, including the wide area network (WAN) backbone technology Multiprotocol Label Switching (MPLS) and IP Security (IPSec) features in Cisco IOS® Software. Driving the project was the promise of faster and simpler VPN deployment, and greater security, management, scalability, flexibility, and quality-of-service (QoS) features to serve a range of new applications.

Switching versus Routing at the Network Core

In addition to building IP VPNs, Infonet also provides ATM and Frame Relay VPNs. With ATM or Frame Relay networks, traffic flows over virtual circuits built and maintained between each VPN site. These circuits are like private, dedicated lines that must be created, maintained, and paid for fully whether they are heavily or hardly in use. In "hub-and-spoke" architectures, each router has to extract information for forwarding from the header of each packet. The header information becomes an index for a routing table lookup for the packet's next hop.

"Using MPLS, VPNs have become much easier to deploy and scale," says Joe Fusco, Director of Private IP Services at Infonet. "You configure the virtual circuits centrally across the IP network, so it's also a lot easier and cost effective to manage."

The Cisco MPLS infrastructure uses information in IP addresses to build any-to-any linkages in a Layer 3 "connectionless" network instead of hub and spoke connections of virtual circuits.

Routing is also simplified. "Before MPLS, we were operating an IP VPN network using the access control filtering feature on Cisco routers," says Fusco. "It was cumbersome and if you made any changes to the network you had to update the routing tables and virtual circuits between sites."

Now, the routers at the Infonet network core handle the label swapping, assigning a short, fixed-length label to each packet. The switch routers at the network's edge analyze the forwarding information for the packets based on the labels and send them to the router closest to the ultimate destination, where the label is removed and the packet is delivered to its ultimate destination. Cisco Provider Edge routers do the header analysis to determine the appropriate service class (via the label) to apply to a packet. The labels used in MPLS networks tell the routers and switches both where to send the packets and how to send it. Service attributes such as service class, priority, and privacy are contained in the forwarding table and indexed by the label.

While this process may appear transparent to Infonet customers, the single table lookup allows for much greater performance at the network core.

"While access control lists were effective before, it was possible for a configuration manager to type in a wrong IP address and lose connectivity," says Fusco. "With MPLS, you create a separate routing plane for each customer. Different customers can have the same private address and still use them, since the MPLS header encapsulates the IP address once at the edge within the VPN."

EXECUTIVE SUMMARY

CISCO SOLUTION

In 2000, Infonet became one of the first providers to begin deploying Multiprotocol Label switching (MPLS) through a Cisco IOS Software upgrade. MPLS, Border Gateway Control (BGP), and other features in the Cisco IOS Software simplify routing, allow labels to carry directional as well as class-of-service and security information, and thereby allow for diversified, secure network applications on IP VPNs.

RESULTS

MPLS has proven its worth at Infonet by greatly streamlining and enhancing the company's IP VPN offerings. From point-to-point, hub-and-spoke VPN networks to "connectionless" Layer 3 private virtual circuits, MPLS-based IP VPNs are simpler and more cost effective to deploy and maintain for Infonet. The traffic engineering component of MPLS has made managing class of service much easier and paved the way for new network services, much greater scalability, privacy and security for corporate VPNs, and service-level agreements that can be precisely monitored. In December 2001, Infonet was awarded a five-year multiservice contract by Nestle S.A. of Switzerland valued at U.S.$125 million over five years. Infonet will build a global network for Nestle linking 1,500 sites across 90 countries.

Interprovider MPLS

In June of 2001, Infonet announced "Interprovider-capable MPLS," with global class of service available for data services across multiple IP VPN backbones. Infonet's Interprovider MPLS services give multinational customers the ability to run VPNs that reach beyond national networks through agreements forged with interconnect partners willing to integrate MPLS-enabled IP VPN services.

"The initial version of MPLS was designed to run on a single, autonomous system," explains Fusco.

"We discovered that by dividing our network into three separate, autonomous systems—in Europe, Asia, and the Americas—we reduced the number of routes that need to be supported in each system. We worked with Cisco on making these VPNs recognize different autonomous or logical networks."

Building VPNs that span multiple providers yet appear seamless to the customer is possible today through tunneling, but this is far more expensive than using MPLS. Additionally, tunneling doesn't deliver the full mesh connectivity across the VPN and between providers that is available with MPLS.

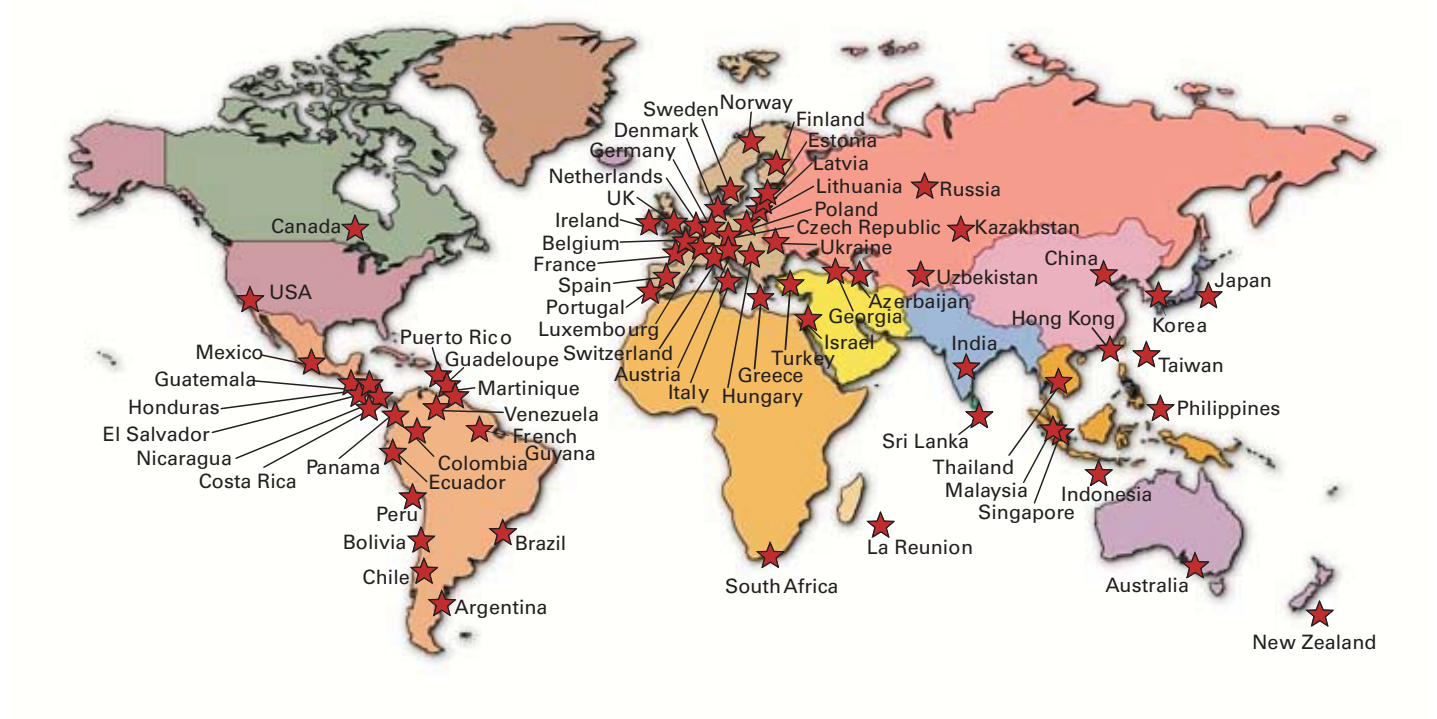
Private Addressing Advantages

With MPLS, Infonet customers who want to use the private addresses from their LANs for the VPN can use them securely. Each customer site is connected to the IP VPN cloud through private tail circuits but users gain full mesh connectivity to all sites connected to their VPN because edge label switch routers instead of core routers make forwarding decisions.

DiffServ Enables Class of Service Offerings, Traffic Engineering

After the initial deployment of MPLS at Infonet, Fusco and his colleagues are now readying a rollout of class-of-service (CoS) offerings through Differentiated Services (DiffServ)-aware traffic engineering. The ability to offer priority handling for voice over IP through the local area network (LAN) or existing PBXs will be a prominent feature.

Infonet IP VPN Global Reach



"There are applications that people have been leery of running over their IP network because they haven't been able to choose a class of service. Now they can. Through MPLS, we can map quality of service settings in the edge routers to control jitter in voice or video and distribute traffic on shortest and other paths based on bandwidth availability."

These MPLS-enabled QoS features will let Infonet quickly create multiple routing instances connecting to a customer site for videoconferencing on demand. Virtual tunnels can be built to manage priority traffic. Less delay-sensitive applications such as File Transfer Protocol (FTP) can be specified to move these packets to a queue behind voice and video services. By labeling each packet, each hop in the network can implement the appropriate QoS without the overhead of an end-to-end private virtual circuit or a separate signaling protocol. Infonet will be able to manage these services with traffic engineering and thereby link them to service-level agreements.

"The initial version of MPLS was designed to run on a single, autonomous system," explains Joe Fusco, Director of Private IP Services at Infonet. "We discovered that by dividing our network into three separate, autonomous systems—in Europe, Asia, and the Americas—we reduced the number of routes that need to be supported in each system. We worked with Cisco on making these VPNs recognize different autonomous or logical networks."

With the growth in managed corporate network services and the current competition and cost pressures among service providers, Infonet's MPLS-enabled IP VPN services via Cisco IOS Software are viewed as a launching pad for compelling service offerings. Each Infonet VPN can be a private, connectionless, secure service on the IP network. Classes of service can be selectively enabled, based on MPLS labels. Customers can use private IP addresses without translation and privacy and security can be achieved without tunnels or encryption.

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 Europe
11, Rue Camille Desmoulins
92782 Issy-les-Moulineaux
Cedex 9
France
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
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: 65 317 7777
Fax: 65 317 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

Printed in the USA