Sprint Global MPLS VPN IP Whitepaper

Sprint Product Marketing and Product Development

January 2006
Revision 7.0

Cisco Powered

Sprint

1.0 MPLS VPN Marketplace

Demand for MPLS (Multiprotocol Label Switching) VPNs (standardized in RFC 2547bis) has grown steadily since MPLS technologies were introduced to the marketplace in 1999. Demand for MPLS-based solutions continues to grow in 2006, influenced substantially by enterprise customers who have recognized the significant technical and economic advantages of these solutions. Generally, enterprise customers look for an MPLS VPN solution to provide:

- Any-to-any connectivity
- Secure segmentation of network traffic
- Class of service (CoS)

In addition, MPLS VPNs are attractive to enterprise customers because they can change the networking model from an overlay model, where each customer premises router must connect to every other customer premises router, to a peer model, where each customer premises router peers only with an associated service provider edge (PE) router. This reduction in complexity allows for much greater scalability and lower equipment costs because fewer burdens are placed on the customer edge routers. Figure 1 shows the reduction in complexity as the routing is moved from each customer premises router to the service provider network.

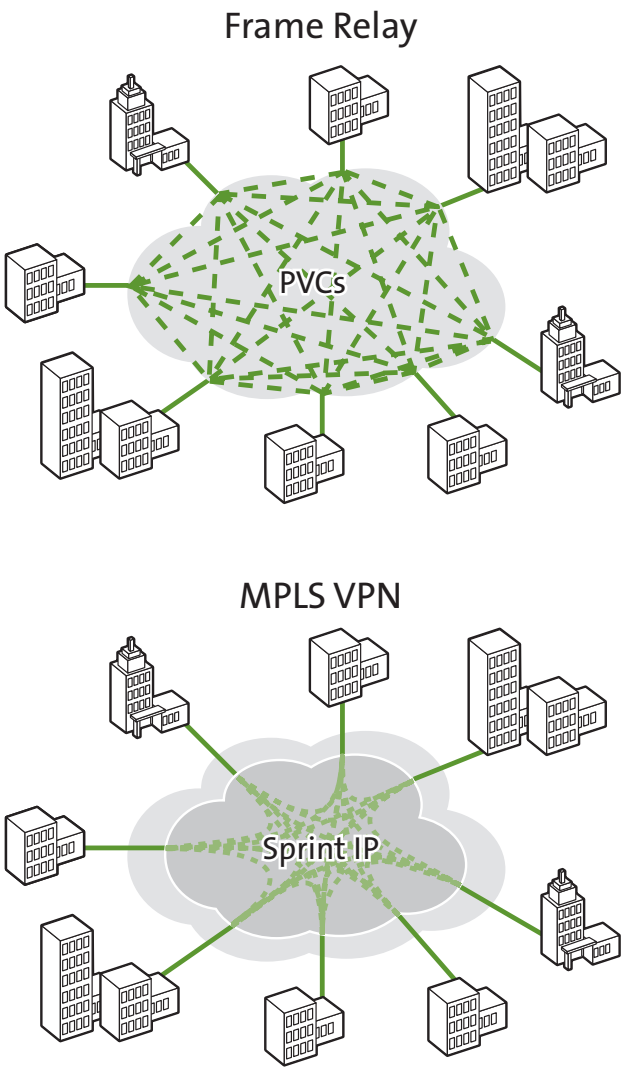

Figure 1. Reduction in Complexity as Routing Moved from Customer Premises Router to Service Provider Network

2.0 Sprint Global MPLS VPN

In 2004 Sprint introduced an advanced version of MPLS VPN based on RFC 2547bis that is delivered over Sprint's global native IP backbone infrastructure. Sprint's IP backbone carries the Cisco® Multiservice Network designation, which certifies the network's performance and capabilities to support multiple time-sensitive applications such as voice and video. This allows Sprint to use the inherent benefits of its premier global IP network to offer customers an MPLS VPN solution that provides standard MPLS VPN functionality as well as high levels of performance, flexibility, and geographical reach.

With the launch of Sprint Global MPLS VPN, Sprint is able to provide customers with a simple and flexible VPN solution with security equivalent to or better than that of Layer 2/2.5-based (Frame Relay or ATM) alternatives. In addition, Sprint is able to provide value-added services such as secure Internet access, remote access, and extranet connectivity on a single network platform.

"Sprint's MPLS VPN enables high performance, global reachability, and secure multiservice connectivity. Adhering to Cisco multiservice CPN criteria, Sprint's offering is provided over its scalable, private IP-routed backbone and affords customers full support for end-to-end quality of service for converged voice, video, and data. As a result, Sprint's customers can leverage a cost-effective, feature-rich, high-performing MPLS VPN service for their converged enterprise networks."

—Kelly Ahuja, VP, Routing Technology Group, Cisco

2.1 Security

Security is a major concern for enterprise customers. ("Sprint IP Security White Paper" is available for more details about the security features of Sprint's global IP network.) With the threat of network attacks and an increased reliance on data networking, enterprises require high levels of security to protect their sensitive data. Sprint MPLS VPN solutions operate over an IP core that uses L2TPv3 to create the PE-to-PE path. By using this architecture, the network gains built-in service integrity verification mechanisms that validate every packet that enters the PE and provides extremely strong protection against packet spoofing attacks. The multilayered security capabilities inherent in L2TPv3 add a significant protection to Sprint's multilayered security architecture and help Sprint deliver a world-class MPLS VPN solution with security equal to or surpassing that of Layer 2/2.5-based alternatives such as Frame Relay and ATM, which are limited to only a single layer of protection (virtual circuit identifier). Figure 2 shows the manner in which multilayered security capabilities are implemented.

To add security and create a private IP network, Sprint provides MPLS VPNs on MPLS-enabled Cisco 12000 Series routers gigabit switch routers (GSRs), and Cisco 7500 Series routers, completely separate from the GSRs, used for other IP services such as Dedicated IP and SprintLink Frame Relay (SLFR). The MPLS-enabled GSRs are fully meshed using L2TPv3 tunnels in compliance with RFC 2547bis. MPLS inner labels use virtual route forwarding label switching mechanisms to segregate a customer's traffic from other customer traffic and outside entities.

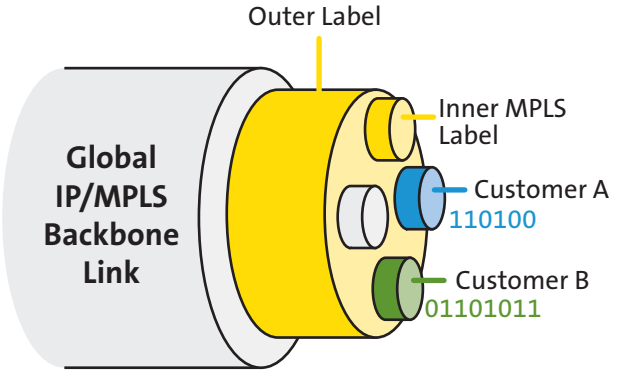

Figure 2. Multilayered Security Element Construction

2.2 Simplified Routing

Sprint MPLS VPNs simplify traffic routing by moving the complexity from the customer's premises to the carrier's cloud. Whether the customer is using static routing, Border Gateway Protocol (BGP), Enhanced Interior Gateway Routing Protocol (EIGRP), or Open Shortest Path First (OSPF), the environment is simplified at the PE. Simplified routing supports two primary benefits for customers. Because the complexity is managed by the carrier's cloud, less complex customer premises equipment (CPE) is required, potentially lowering the capital investment required; in many instances, existing CPE investment can be used. Sprint also provides the customer with service flexibility by making CPE management optional; customers can elect not to have Sprint manage their CPE while still receiving class-of-service and service-level agreement (SLA) support.

2.3 Meshed Networking

Sprint MPLS VPNs support partial and full-meshed network topologies. As more distributed applications are implemented, enterprises will require the capability of any-to-any connectivity. Sprint has eliminated the complexity of adding/moving/changing locations. All locations require only one connection into the network to have direct connectivity to all or any other sites in the enterprise.

2.4 Access Options

Sprint MPLS VPN supports multiple access options that provide enterprise customers with migration options and low-cost alternatives, including IP Security (IPSec) tunnels, traditional Frame Relay, and DSL.

- **IPSec** — IPSec half tunnels are used to connect customer locations that are beyond Sprint's footprint. These offices deploy a CPE-based IP VPN device, either Sprint or customer managed, over an Internet connection. Customers have the flexibility to connect from any ISP (dial-up or dedicated) using a client or IPSec-capable CPE.
- **Frame Relay** — Sprint's legacy PSN2 Frame Relay network will have multiple interconnections with the MPLS VPN network. These gateways will enable an easier migration from Frame Relay to MPLS VPN for existing Sprint Frame Relay customers.
- **DSL** — Sprint provides access to MPLS VPNs with its Sprint DSL service for a low-cost access alternative domestically where available.
- **Wireless** —In early 2006, Sprint will offer wireless access to the Global MPLS VPN, providing high-bandwidth primary and secondary access alternatives for both mobile users and stationary locations.

2.5 Class of Service

Definition: QoS vs. CoS

These terms are often used interchangeably. Following are the Sprint definitions:

- **Quality of service (QoS)**—The overall performance of the network supported by SLAs. Terms used in discussing QoS include availability, packet loss, latency, and jitter.
- **Class of service (CoS)**—The ability to differentiate and treat packets differently based on importance and time sensitivity.

There is a growing need for class-of-service and application prioritization as customers move to converge multiple applications over a single data network. Real-time, end-to-end CoS is required to support such time-sensitive applications as voice and video over IP.

Using Cisco Systems® innovations such as Class-Based Weighted Fair Queuing and Low-Latency Queuing, Sprint provides customers the ability to prioritize their traffic on the access links, which are the most likely places for congestion to occur because these links are frequently low bandwidth, over-utilized, and tend to experience "bursty" traffic patterns. Customers have the flexibility to determine the number and size of the queues as needed to support their applications. Figure 3 demonstrates the manner in which traffic is segregated into classes in order to prioritize traffic types.

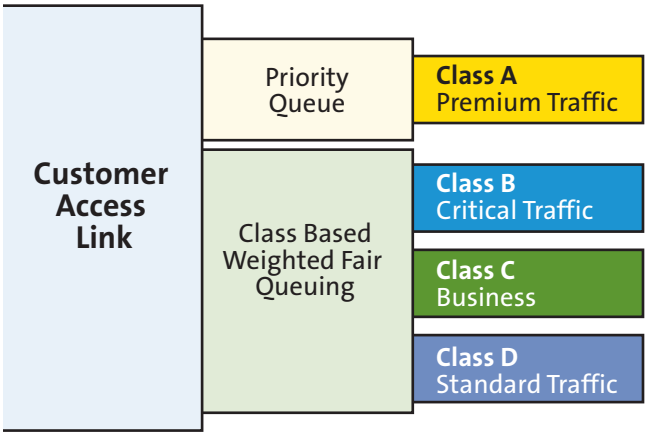

Figure 3. MPLS Enabled Class of Service Traffic Segregation Module

Sprint's OC-192 backbone, which is engineered for congestion avoidance (discussed further in Section 4.0, "Sprint MPLS VPN Network Architecture"), has the capacity to support all traffic, avoid packet delay, and not require queuing or added "insurance" to provide an acceptable level of performance. Combining the traffic prioritization at the network edge and the low utilization levels in the core, customers receive superior end-to-end quality of service for all traffic.

3.0 Sprint Value-Added Services

By using the global IP backbone, Sprint Global MPLS VPN supports a breadth of network-based value-added services. Enterprise customers have access to services that are more cost-effective and require less network management than the hardware-based alternatives.

3.1 Secure Internet Access

Sprint Global MPLS VPN supports distributed, secure Internet access. Each site in the MPLS VPN receives Internet access secured by stateful firewalls located in the Sprint network. The same policy is applied universally throughout the customer's network, providing a more efficient and cost-effective way of delivering Internet access to branch or remote offices. Network bandwidth is used efficiently in this model because each location uses its own allocated bandwidth, and Internet traffic does not traverse the wide area network or go through a hub site. This service is used primarily for browsing the Internet but does have the capability of accepting inbound traffic for services such as e-mail. This service is a strong complement to CPE-based firewall services that are recommended for a Web server environment with continuous inbound traffic demand.

3.2 Remote User Access

Sprint Global MPLS VPN provides remote access through the use of an IPSec VPN client. The client is installed on a user's laptop and builds an IPSec tunnel to a gateway in the MPLS network. This has the benefit of enabling employees to run corporate applications, such as e-mail, while away from the office. The only user requirement is an Internet connection from an ISP that does not block IPSec traffic.

Sprint's Data Link for Mobile Access service—offering secure wireless access to the wireline data network—and MPLS VPN products can be combined into one solution to allow users with wireless enabled laptops or personal digital assistants (PDAs) to access the VPN. (This access option is targeted for availability in early 2006.)

3.3 Off-net and Extranet Connectivity (via CPE-based VPN)

Sprint Global MPLS VPN provides enterprise customers with the ability to use IPSec tunnels to securely connect business partners to their VPN network or extend the reach of the network beyond Sprint's footprint. A CPE-based IP VPN device is deployed at the business partner's premises or in a customer's off-network location. The CPE VPN device can be either Sprint or customer managed and can be provisioned over any provider's Internet service. The CPE VPN device is used to establish an IPSec tunnel back to the Sprint MPLS VPN using a network gateway. Locations connected in this manner receive the same any-to-any connectivity as on-net sites.

3.4 Multicast

Multicast is a bandwidth-conserving technology that reduces traffic by simultaneously delivering a single stream of information to thousands of corporate recipients. Applications that use multicast technologies include videoconferencing; corporate communications; distance learning; and distribution of software, stock quotes, and news. Sprint offers native IP multicast at no additional charge to MPLS VPN customers.

4.0 Sprint Global MPLS VPN Network Architecture

Sprint provides MPLS VPN services on an OC-192 native IP platform composed of Cisco routers from the Cisco Carrier Routing Systems, CRS-1 a very powerful router, to the Cisco 7000 and 12000 series routers; Sprint has received the Cisco Powered Network designation, indicating that the network is built using Cisco equipment and meets the stringent guidelines specified by Cisco to receive this designation. By delivering Sprint Global MPLS VPN over a native IP network, Sprint decreases networking complexity and eliminates unnecessary overhead, leading to a more cost-effective solution for customers. Sprint's approach to traffic engineering on its IP backbone is to provision ahead of the demand curve. The Sprint philosophy is one of congestion avoidance. Therefore backbone links are maintained at traffic loads not to exceed 45 percent utilization, providing ample network capacity to effectively help ensure high-quality service to all packets on the IP backbone. Sprint's congestion avoidance philosophy helps ensure that data travels through the network routers on a first-in first-out basis without delay, jitter, or packet loss.

Sprint uses the Intermediate System–to–Intermediate System (IS-IS) dynamic routing protocol to compute metrics supporting traffic redistribution over the IP backbone links, which are provisioned in pairs using per flow load balancing between the diverse paths. In the event of a fiber cut, traffic is automatically rerouted to the other link in the pair using the fast reroute capabilities associated with IS-IS. All links in the network are live and can accept traffic if other links go down. Figure 4 illustrates the fast reroute of traffic that results from a cut in a link.

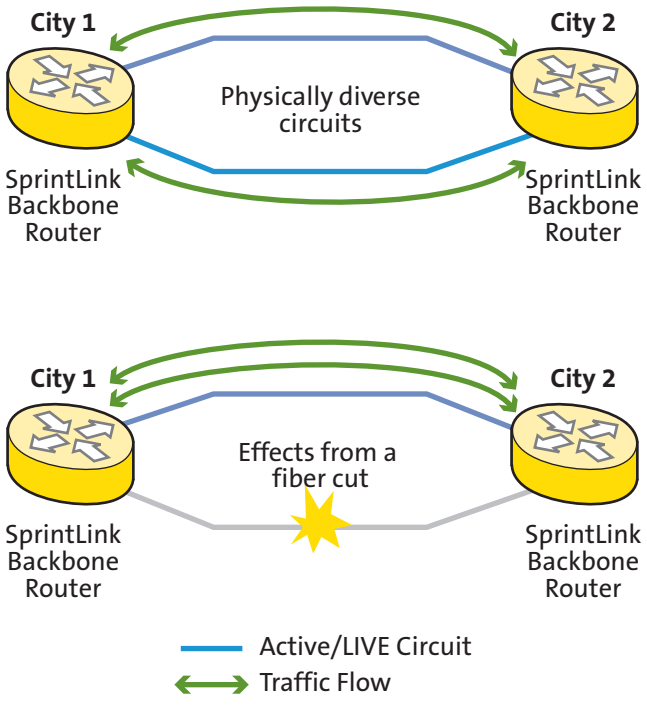

Figure 4. Traffic Fast Reroute Capability of Sprint MPLS VPN Network Architecture

Because the network is fully interconnected, Sprint is able to provide multiple redundant paths through the network, whereas other competitors with MPLS-based solutions provisioned over an existing core (ATM) are limited to defining a primary route and secondary route for traffic. Provisioning MPLS VPN over a native IP core provides customers with a greater level of reliability and redundancy for their mission critical, enterprise WAN traffic.

5.0 Sprint Global MPLS VPN Key Benefits

By operating its MPLS VPN solution over a 100 percent native IP core, Sprint can provide a more advanced solution that supports greater business benefits and capabilities.

- **Service flexibility**—Sprint Global MPLS VPN is a complete solution that supports a partial to fully meshed environment , class of service, and provides value-added services such as secure Internet access, remote user access, extranet connectivity, and multicast capabilities on a single network infrastructure.
- **Cost effectiveness**—Sprint Global MPLS VPN provides a cost-effective solution with simple billing components. Port and access are the only required components for a fully meshed MPLS VPN network. Lower cost access options such as DSL are also supported. Features such as class of service, multicast, and premium network SLAs are standard parts of the offering and are offered at no charge to the customer. Customers do not pay setup fees or monthly recurring charges for any of these additional features.
- **Security**—Sprint Global MPLS VPN is designed with security in mind and provides multiple layers of security to create a solution with security equivalent to that of a Layer 2 network.
- **Class of Service** —Sprint Global MPLS VPN supports class of service required for real-time applications such as voice and video at no additional charge to the customer.
- **Performance guarantees**—Sprint MPLS VPN is backed by industry-leading SLAs including latency, packet loss, and jitter without requiring network management or additional fees.
  - Packet loss performance metric: 0.1 percent or less globally
  - Jitter performance metric: 2 ms or less globally
  - Service credits: Sprint supports its confidence in its network by providing up to one-month port MRC credit for a missing performance metric; this is 10x greater than most other service providers.
- **Scalability**—Sprint Global MPLS VPN provides the ability to quickly add, move, or change sites to a fully meshed network without having to reconfigure CPE, because complex routing is handled in the carrier cloud.
- **Global reach**—Sprint Global MPLS VPN is available from all SprintLink nodes around the world, and global reach can be expanded through hybrid networking capabilities using CPE-based VPN IPSec tunnels, making Sprint MPLS VPN available in over 100 countries worldwide.

6.0 Conclusion

Sprint Global MPLS VPN provides a standards-compliant solution designed to meet a wide array of enterprise customers' MPLS VPN networking needs. Sprint Global MPLS VPN supports any-to-any connectivity, secure segmentation of network traffic, and excellent quality of service. In addition, Sprint Global MPLS VPN provides a full suite of value-added services to create one of the most feature-rich MPLS offerings in the industry. Sprint Global MPLS VPN is built on a 100 percent Cisco-provided native IP core that is designed for performance and congestion avoidance and is backed by industry-leading SLAs. The network security architecture is built on multiple layers to provide maximum protection to Sprint customers.

Sprint is committed to delivering best-in-class global communications solutions that provide exceptional value, functionality, and service. To deliver on this commitment, Sprint provides tailored solutions built around state-of-the-art innovations, efficient integration plans, and a full range of support and service options. For more information, please contact your Sprint representative.

Call your Sprint Representative or Authorized Sales Agent at 1-877-700-8919.

Cisco Powered

Sprint

055269