



# *Sprint IPv6 Services*

*White Paper*  
*July 2007*

## ***Sprint IPv6 Services***

<b>Abstract</b>	<b>3</b>
<b>IPv6 Defined</b>	<b>3</b>
<b>IPv6 and the Federal Government</b>	<b>4</b>
<b>Sprint IPv6 history</b>	<b>5</b>
<b>Sprint IPv6 services</b>	<b>6</b>
Dedicated IP Services	6
BGP/MPLS VPNs (VPNv6)	7
Technology DescriptionFeatures	7
Functionality	8
Service Availability	8
Managed Network Services	9
IPv6 Consulting	9
<b>About Sprint Nextel</b>	<b>10</b>

## **Abstract**

Sprint Nextel (Sprint) has led efforts to standardize, test, and deploy Internet Protocol version 6 (IPv6) since 1997. As an early adopter of IPv6 in an experimental capacity, Sprint builds upon knowledge gained through operating an IPv6 test-bed and encourages standardization and evolution of the IPv6 protocol. Sprint networks and services migrate to IPv6 not only to support wireless, wireline, and converged IP architecture objectives, but to also provide IPv6 services to customers and enable federal agencies to comply with IPv6 mandates.

Dedicated IP services continue to be available from Sprint to assist with IPv6 testing and evaluation. Dual-stack IPv4/IPv6 MPLS VPN services offer network-based IP VPN support for customers interested in deploying an IPv6-capable backbone. Value-added services such as managed network services of IPv6 customer premise equipment and IPv6 consulting enable customers to reduce operational expenses and mitigate risks associated with IPv6 planning and transition efforts.

Federal agency customers may leverage Sprint contract vehicles such as Network Enterprise, which Sprint refreshes with the latest IPv6 services. The Sprint Peerless IP network provides a platform that is physically and logically isolated from the public internet, mitigating threats associated with evolving IPv6 security standards. Sprint's currently executing project plan for dual-stack IPv4/IPv6 MPLS VPN services delivers key infrastructure necessary to comply with federally mandated schedules.

## **IPv6 Defined**

IPv6 is the evolving, designated successor to Internet Protocol version 4 (IPv4). Representing the Internet layer of the Transmission Control Protocol/Internet Protocol (TCP/IP) suite, or equivalent to the network layer in the Open Systems Interconnection (OSI) reference model, IPv4 is the dominant packet transport protocol in packet-switched internetworks.

Originally recommended by the Internet Engineering Task Force (IETF) IP next generation (IPng) working group in 1994, the core IPv6 protocols became a draft standards in the late 1990s and continue to evolve. Several key factors drive the need for IPv6 development in the industry in general; additionally, Sprint strategic direction also recognizes key IPv6 drivers and result in the corporation's continuing commitment to the evolving standards. A few of these drivers are summarized below:

- > **Address space scalability:** While the needs of new technologies driven by applications development necessitate IPv6 development in part, arguably the largest IPv6 driver is address space scalability to support the growing number of applications and users. The lifespan of the original IPv4 32-bit address space was prolonged by migrating to a classless addressing hierarchy and the introduction of technologies such as Network Address Translation (NAT). Even with these changes however, by the 1990s it was clear that the exponential growth of IP hosts would soon result in an exhaustion of IP addresses. This growth was witnessed by Sprint not only as a Tier 1 Internet Service Provider (ISP) providing packet transport for IP hosts, but also as a provider of the IP hosts themselves such as IP-enabled wireless data devices, Voice over Internet Protocol (VoIP) end-points, and managed network services equipment. IPv6 increases the original 32-bit addresses space by a factor of four to 128 bits, thus providing  $3.4 \times 10^{38}$  (340 trillion trillion trillion) unique addresses and more address scalability than humanity can envision requiring for the foreseeable future.
- > **Improved Security:** The IPSec architecture defined by RFC 2401 supports both IPv4 and IPv6, but is a mandatory component of IPv6. Larger IPv6 address space also eliminates one of the issues associated with IPSec, that being the implications of Network Address Translation (NAT). For example, the IPSec Authentication Header (AH) extension provides source integrity and

authentication. AH protects the IP packet payload and header fields that would not be altered in transit. NAT, however, by definition changes the IP addressing information resulting in a failure to authenticate the packet. By eliminating the main reason for NAT, namely IPv4 address exhaustion, IPv6 removes one of the more problematic aspects of IPSec deployment. With IPv6, an end-to-end IPSec model becomes more realizable. An additional benefit of the larger IPv6 address space is that vulnerability reconnaissance, accomplished via port mapping or ping sweeps, is not a relatively quick exercise as in was with IPv4.

- > **Mobility:** Mobile devices, both in terms of subscriber growth and the ability for devices to easily move their network attachment point in a network, also drive IPv6 development. Increased address space for the mobile nodes, without requiring NAT for RFC 1918 addresses, is again a primary need. Additionally, Mobile IPv6 (MIPv6) builds upon its corresponding IPv4 predecessor by integrating better with IPv6, removing the need for a “foreign agent” to provide a Care of Address due to IPv6’s greater address space, and integrated route optimization that allows routing between the mobile node and the Correspondent Node—thus avoiding transit through the mobile node’s home agent.

In addition to IPv6 protocol development to address the above drivers, IPv6 includes several features and benefits beyond IPv4. The following are a few:

- > **Simplified IP Header:** IPv6 improves packet processing efficiencies by removing some fields from the IPv4 header, or making them optional.
- > **Improved handling of extensions and options:** Options are moved out of the base header and are generally handled by the destination node, resulting in lower overhead and increased efficiency.

- > **Streamlined fragmentation support:**

Fragmentation information is moved out of the base header, and fragmentation is handled on an end-to-end basis through the use of MTU discovery. Routers in between IPv6 endpoints do not fragment packets.

- > **Improved Quality of Service support through flow identification:**

IPv6 adds a flow label, which aims to provide Integrated Service (IntServ) per-flow handling of packets requiring specific QoS support. As with some aspects of IPv6, this feature is an example of one that is still evolving.

### **IPv6 and the Federal Government**

IPv6 migration is a critical issue facing Federal Agencies. The Office of Management and Budget (OMB), the Executive Branch Office responsible for assisting the President with oversight of the federal budget’s preparation, submission to the Congress, and administration within the Executive Branch Agencies, directed federal agencies to migrate their backbones to IPv6 by 30 June 2008. OMB provided this and other IPv6 guidance to Federal Agency CIOs in memorandum M-05-22 released on 2 August 2005, which is located at:

<http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf>

In the context of the memorandum, IPv6 backbone migration is defined as the Agency backbone using IPv6 either natively or in a the destination node, resulting in lower overhead and increased efficiency.

- > Assign Agency planning leadership, complete inventories, and begin impact analysis
- > Provide an update progress report and complete a transition plan as part of an enterprise architecture submission to OMB
- > Complete inventory and impact analysis efforts

The Federal CIO Council's Architecture and Infrastructure Committee released additional transition guidance in 2006, located at: [http://www.cio.gov/documents/IPv6\\_Transition\\_Guidance.doc](http://www.cio.gov/documents/IPv6_Transition_Guidance.doc). Expanding upon M-05-22, the Transition Guidance document provides multiple chapters on IPv6 architecture planning and transition strategy. For example, a federal agency must be able to demonstrate that they are able route traffic via the IPv6-enabled backbone to and from agency networks and the internet, and do so without compromising network security or legacy IPv4 capabilities.

### **Sprint IPv6 History**

Sprint has an established history of IPv6 leadership dating back to when the core set of IPv6 protocols became draft IETF standards in the late 1990s. Since 1997, Sprint has been actively involved in the standardization, testing, and deployment of IPv6. When the IETF Next-Generation Transition (ngtrans) working group founded and began administering the 6bone IPv6 test network, Sprint was an early adopter and quickly became one of the largest and best connected IPv6 networks in the world.

To support 6bone deployment and foster interest in IPv6 testing, Sprint established an IPv6 test bed network with dedicated IPv6 routers, obtained initial 6bone address space (3ffe:2900::/24), and began offering interested IPv4 SprintLink customers the ability to connect to the 6bone network—at no additional cost. The Sprint IPv6 test bed network was overlaid on the SprintLink IPv4 network by using Generic Routing Encapsulation (GRE)

tunneling. Additionally, Sprint coauthored Request for Comments (RFC) 2772 documentation (<http://www.ietf.org/rfc/rfc2772.txt>), which provided guidelines for 6bone operators to ensure efficient, stable deployment of 6bone routing systems and promote a scalable IPv6 backbone.

The Sprint IPv6 test bed network was one of the largest and best connected networks in the world and grew considerably while in operation. Sprint had 15 customers on the network in 1998; by the end of 2000, that number had grown to 110 customers. Through 2002, Sprint obtained additional address space from ARIN (2001:440::/35 -> /32), added additional IPv6-capable Points of Presence (POPs), and was turning up IPv6 customers at the rate of 2-3 per week. The Sprint IPv6 test bed customer count eventually reached over 400 with the footprint shown in Figure 1. Having served its purpose to promote the standardization and evolution of IPv6 networks, the IETF phased-out the 6bone on 6 June 2006.

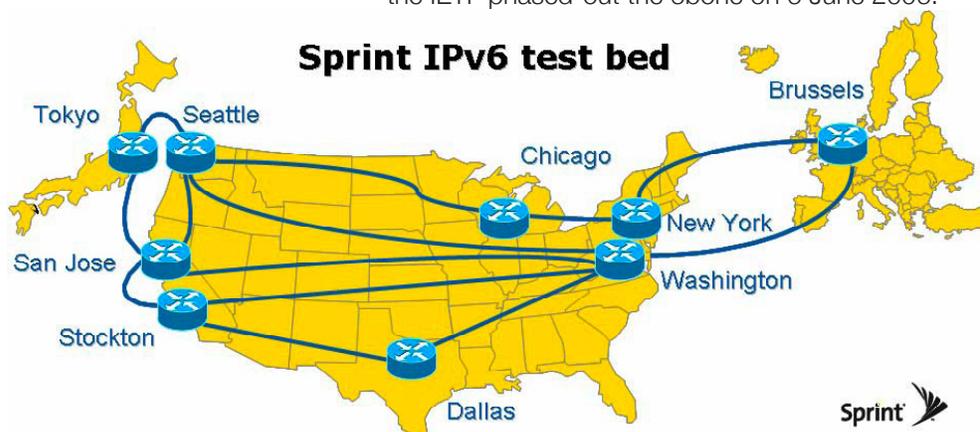


Figure 1: The first Sprint IPv6 test bed network was a part of 6bone, and was one of the largest and best connected IPv6 networks in the world.

In addition to 6bone and IETF ngtrans experience, Sprint has been actively involved with the IETF IPng working group since 1997, provided engineering support to the Moonv6 project, worked with vendors to develop and trial wireless and wireline IPv6-enabled equipment, and developed plans for its own

adoption of IPv6 internally. The experience and knowledge gained through these activities forms the foundation for current Sprint IPv6 plans, which are discussed in the following section.

### **Sprint IPv6 Services**

Sprint offers a variety of IPv6 services and will continue to expand them in parallel with IPv6 evolution. These services include Dedicated IP, MPLS VPN, Managed Network Services, and Consulting services. The primary IPv6 vehicle for Sprint federal customers is the Network Enterprise contract. Sprint adds IPv6 services to the federal Network Enterprise contract as they become available, and offers Network services including Managed Network Services and Customer Specific Design and Engineering Services (CSDS) for IPv6 planning and transition support.

### **Dedicated IP Services**

The Sprint IPv6 Evaluation Network IPv6 network, Autonomous System (AS) 6175, is shown in Figure 2. Sprint IPv6 Evaluation Network is the primary means for Sprint customers to use IPv6 over the public internet, or more specifically the SprintLink IP network. Similar to the earlier Sprint 6bone network, the current Sprintv6 network is an overlay on the SprintLink IPv4 network using dedicated routers. These routers use GRE tunnels to transport traffic across SprintLink. Each node has multiple connections to other nodes, similar to a design strategy of SprintLink, and there is an interior Border Gateway Protocol (iBGP) full-mesh between the IPv6 routers-providing the network with reliability and the ability to route around failures.

The Sprint IPv6 Evaluation Network allows current IPv4 SprintLink customers to use IPv6—at no additional charge. IPv4 connections to Sprintv6 are

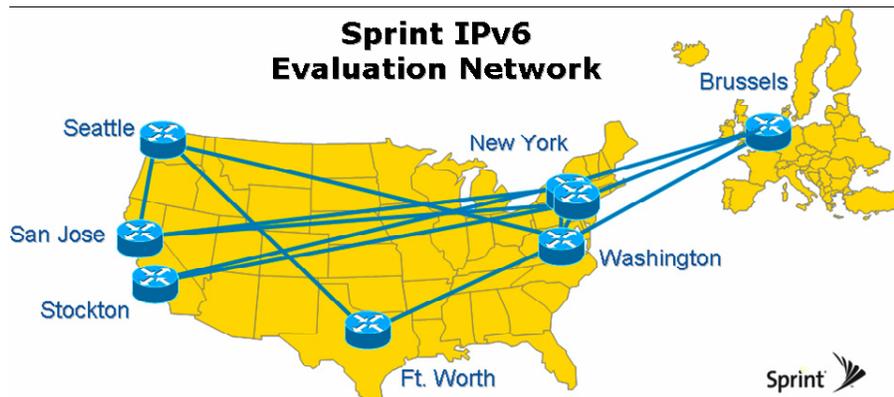


Figure 2: The Sprintv6 network is available to SprintLink IPv4 customers for transporting IPv6 traffic over the public internet

supported by terminating tunnels on the routers in AS 6175 via GRE or IPv6IP encapsulated tunnels.

Sprint IPv6 Evaluation Network is one of the best-connected IPv6 networks in the world. Sprint maintains numerous peering relationships with other IPv6 networks. These BGP4+ peering sessions are established at native IPv6 exchanges, such as The Stokab in Stockholm, Sweden and AMS-IX in Amsterdam, Netherlands, or via IPv6-over-IPv4 tunneling to other IPv6 networks. Currently, Sprint maintains connections to over 600 Autonomous Systems.

In addition to Sprint IPv6 Evaluation Network connectivity for SprintLink IPv4 customers, Sprint provides non-portable IPv6 address space from our allocation in 2600::/29 (e.g. a /48 globally scoped address block). Customers also use their own globally or locally scoped addresses assigned to them by their Regional Internet Registry (RIR). Sprint provides Domain Name System (DNS) services, both forward and reverse, to customers. Customers using DNS services provide the hostname of their IPv6 DNS server to Sprint, and that reverse zone is delegated to them. Sprint IPv6 DNS is completely separate from Sprint IPv4 DNS, and some services may not have IPv4 addresses associated providing reachability only via IPv6.

The Sprint IPv6 Evaluation Network exists and is able to support customers today. Over time, IPv6 support migrates to the larger SprintLink IPv4 network as more internet hosts become IPv6 enabled. Initially, most customers will use IPv6-enabled Virtual Private Networks (VPNs) for IPv6 enterprise networks, such as an IPv6 extension for BGP/MPLS VPNs (VPNv6). This naturally follows from the large demand for IPv4 MPLS VPN services, and is therefore part of the reason for Sprint focus on VPNv6. Sprint VPNv6 services are described next.

### BGP/MPLS VPNs (VPNv6)

#### Technology Description

Sprint provides MPLS VPN services as the primary solution for an enterprise backbone capable of transporting IPv6 traffic. MPLS VPNs provide customers with a proven, network-based, IP VPN service with capabilities such as inherent any-to-any routing topologies, Class of Service, and secure isolation of customer traffic. Adoption of IPv4 MPLS VPN services is high, and therefore a MPLS VPN model for VPNv6 is advantageous in order to support customers as they migrate to IPv6. Sprint also recognizes that given the state of IPv6 ecosystem evolution, most customers will not be in a position to immediately adopt a native IPv6 model. As such, a dual-stack IPv4/IPv6 model provides the greatest benefit for customers with an initial mix of both IPv4 and IPv6 traffic and lowers associated transition risk by providing support for both protocols over an appropriate length of time.

Sprint provides VPNv6 services as dedicated IPv6 overlay networks on core Sprint IP transport. Cisco 12000

Series Gigabit Switch Routers (GSRs) provide a dedicated dual-stack IPv4/IPv6 network overlay and comprise the Provider Edge (PE) of the VPNv6. By enabling IPv4/IPv6 dual-stack support on the edge, Sprint leverages the operational efficiencies of core IP networks such as Peerless IP and SprintLink without adding additional complexities to the Provider (P) router core. An illustration of the dual-stack overlay on the Sprint Peerless IP network is shown in figure 3. This is a similar approach to providing Sprint MPLS VPN service in general, and subsequently provides IPv6 capabilities in a more cost-effective and timely manner. The Provider routers support core IP transport independent of either the VPNv6 or VPNv4 traffic on the network.

Existing IPv4 MPLS VPN concepts such as the use of Route Distinguishers (RDs) and Route Targets (RTs) are extended to VPNv6 and allow for address space overlap and the ability to import/export specific VPNv6 routes, respectively. Multiprotocol interior BGP (MP-iBGP) distributes VPNv6 routing information between PE routers. Multiprotocol Virtual Route Forwarding (VRF) provides support for both IPv4 and IPv6 VPNs, following from the dual IPv4 and IPv6 protocol stacks on the PE routers. Each

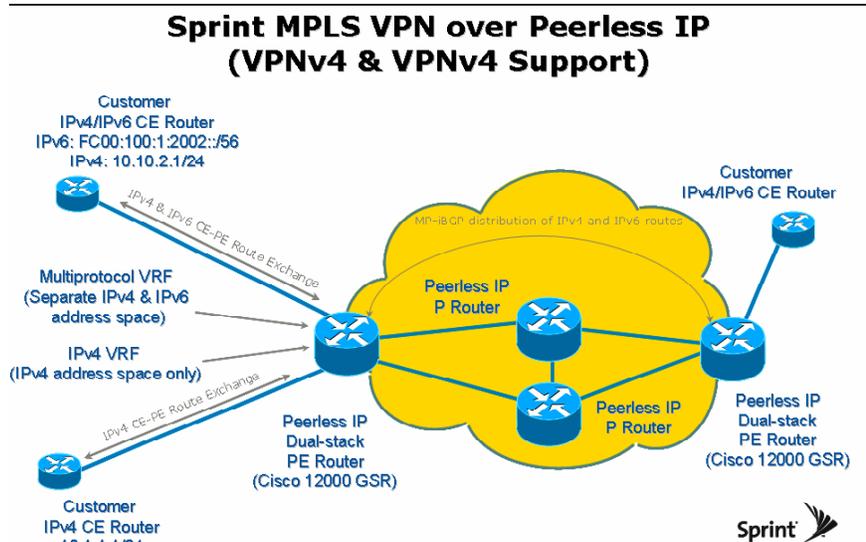


Figure 3: Customers will be able to utilize the dual-stack IPv4/IPv6 implementation over the Peerless IP network to support both VPNv4 and VPNv6 traffic, thus enabling MPLS VPN sites to transition to IPv6.

VPN (VPNv4 and VPNv6) has two Route Information Bases (RIBs), one each for IPv4 and IPv6 address families, to provide traffic separation and allow customers to operate IPv4 and IPv6 MPLS VPNs simultaneously.

### Features and Functionality

Sprint initially offers many Peerless IP VPNv6 features similar to those provided by the original Peerless IP VPNv4 offering, and enables additional VPNv6 functionality to provide greater feature parity as the Sprint VPNv6 service evolves. Following is a partial description of the Peerless IP VPNv6 service offering:

- > **Port Speeds:** Sprint initially provides comparable access methods and port speeds to its MPLS VPN over Peerless IP service, including Fractional DS-1, DS-1, Multi Megabit (nxDS-1), Fractional DS-3 and DS-3 standard, with OC-n and ethernet options by special arrangement. Encapsulation methods include HDLC, PPP, frame relay (multi-VRF), and Multilink PPP (nxDS-1).
- > **Topologies:** VPNv6 provides a full-mesh topology by default, with familiar topologies such as hub-and-spoke also available to address design requirements.
- > **Routing Protocols:** CE-PE routing protocol support is expanded to include IPv6-applicable protocols, to include static, BGP4+, EIGRP and OSPF (IPv4 initially, OSPFv3 for IPv6 as a future enhancement).
- > **Multicast:** Sprint supports multicast for the IPv6 MPLS VPN (mVPNv6) via PIM Sparse Mode or PIM Dense Mode on the customer interface with Source Specific Multicast (SSM) used in the Peerless IP multicast domain between PE routers (IPv4 initially, IPv6 multicast is a future enhancement).
- > **QoS support:** Sprint supports CoS technologies to mitigate the impacts of congestion. As with IPv4-based services, Sprint provides CoS support

on the provider edge to mitigate congestion at the greatest source—the relatively smaller local loop versus the high-performance Sprint IP core. As an provide edge service, packet queuing occurs on the egress interface to the customer. As shown in figure 4, The IPv6 packet header provides the traffic class field that captures classification data so the packet may be acted upon by a specific queuing strategy. Familiar IPv4 packet classification values such as IPP and DSCP are mapped to the traffic class field, with queuing accomplished by Modified Deficient Round Robin (MDRR).

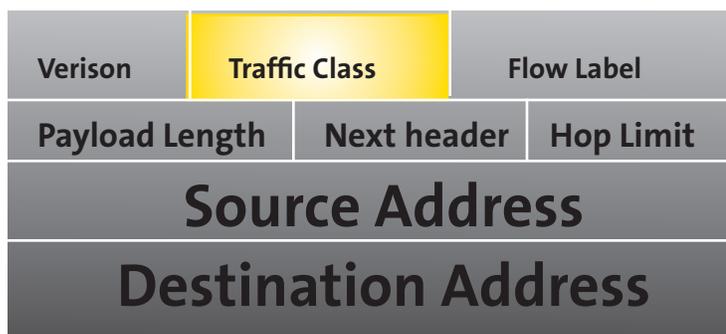


Figure 4: The IPv6 header traffic class field uses familiar DSCP values to support IPv6 QoS strategies

### Service Availability

Sprint offers VPNv6 services over the Peerless IP network with a dual-stack IPv4/IPv6 implementation during 4Q 2007, and welcomes beta customer use of the service during late 2007/early 2008. Corresponding VPNv6 service follows on the Global MPLS platform, which is supported by the SprintLink rather than Peerless IP platform.

As with any network deployment, Sprint has a detailed test and verification process for ensuring operational readiness of the dual-stack IPv4/IPv6 overlay network. All network components, such as the dual-stack PE routers and their VPNv6-capable software, are tested in Sprint labs prior to deployment. Lab testing validates VPNv6 software functionality and network operation. Following

successful completion of lab testing, VPNv6 services move into a field integration testing phase where it is fully integrated with the Sprint network including the Peerless IP network. Sprint further validates the functionality of the VPNv6 features, assesses network impacts, and confirms the comprehensiveness of the overall service.

In order to ensure service availability for key customers and support federal agency compliance with the OMB mandate, Sprint established the milestones shown in figure 5. Sprint developed the test plan for the VPNv6 router software and tests feature-functionality required for the service. Thorough software testing occurs over a two month period while an initial 5 sites in the network receive the Cisco GSR routers that will be used for network functional integration testing. Initial service availability commences upon successful completion of network functional integration testing, and Sprint welcomes beta customer participation at an appropriate stage during testing. Initial service availability commences in late 2007/early 2008, prior to the federal OMB mandate, to allow migration time for Agency customers.

Throughout 2008 Sprint deploys additional GSR routers, targeted to include 1-2 per Peerless IP node to provide an increased footprint and node diversity options. Sprint plans full implementation of the dual-stack IPv4/IPv6 overlay on the Peerless IP network by 3Q 2008.

### Managed Network Services

Sprint offers Managed Network Services for IPv6 capable Customer Premise Equipment (CPE). As a CPE-based solution, Managed IPv6 tunnels IPv6 traffic over GRE tunnels established on

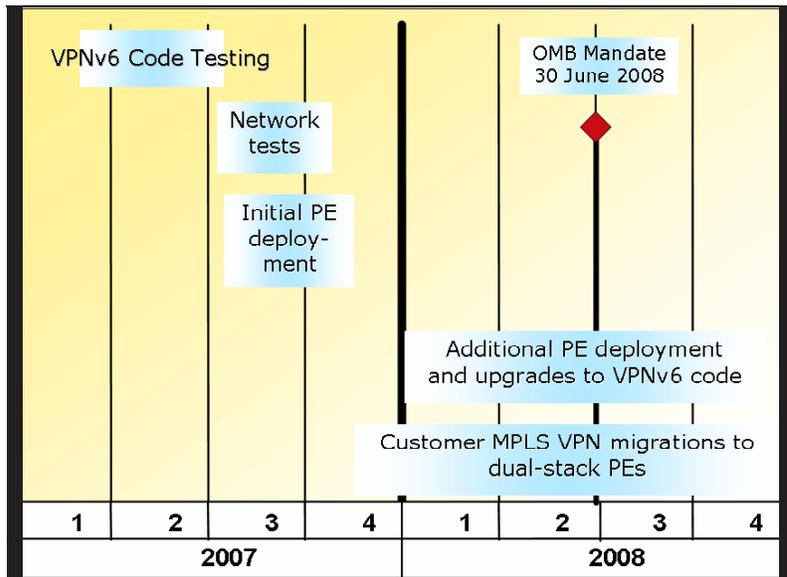


Figure 5: Sprint's currently executing project plan for dual-stack IPv4/IPv6 MPLS VPN service on the Peerless IP network provides customers with a network-based VPN for their enterprise networks, and in particular allows federal agencies to comply with mandated dates for IPv6 adoption. Sprint continues with a similar implementation schedule for dual-stack IPv4/IPv6 services on the Global MPLS platform.

Sprint-managed routers. Managed IPv6 uses RFC 4364 MPLS VPN services over the Sprint Peerless IP network, providing access to the platform already used by many federal agencies today to maximize opportunities for premise-based interoperability between IPv4 and IPv6 networks.

The Sprint Managed IPv6 solution provides an interim premise-based step for customers wishing to support IPv6 traffic while leveraging the experience of Sprint network management professionals. For federal customers, Managed Network Services are provided via the Sprint Network Enterprise contract. Future enhancements to Managed IPv6 include management of CPE connected to Sprint dual-stack IPv4/IPv6 networks.

### IPv6 Consulting

Sprint offers additional support to customers planning IPv6 migrations, for example federal

agencies that need to address interim milestones set forth by their agency transition plans or other federal guidance. These consulting services include inventory data gathering, inventory data analysis, transition risk analysis, and transition cost/impact analysis. For federal IPv6 planning, Sprint helps agencies successfully meet the milestones set out by OMB to mitigate risk and reduce transition challenges with a formalized methodology. IPv6 Consulting services for transition planning and support are available to federal customers via the Customer Specific Design and Engineering Services (CSDS) section of the Network Enterprise contract.

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

### **About Sprint Nextel**

Sprint Nextel offers a comprehensive range of wireless and wireline communications services bringing the freedom of mobility to consumers, businesses and government users. Sprint Nextel is widely recognized for developing, engineering and deploying innovative technologies, including two robust wireless networks serving 53.6 million customers at the end of the first quarter 2007; industry-leading mobile data services; instant national and international walkie-talkie capabilities; and a global Tier 1 Internet backbone. For more information, visit [www.sprint.com](http://www.sprint.com).

With 18 years of experience as a General Services Administration (GSA) telecommunications provider, a proven history of innovation, secure solutions, and a dedication to service, Sprint offers federal agencies a seamless and interoperable communications environment. Sprint gives agencies the power to meet today's communications challenges, such as upgrading enterprise architectures, orchestrating the convergence of disparate technologies and networks, mobilizing the workforce, and ensuring business continuity and responsiveness during emergencies.