White Paper

Transition to IPv6 for Managed Service Providers: Meet Customer Requirements for IP Addressing

What You Will Learn

With the exhaustion of IPv4 addresses, businesses and government agencies around the world are now considering a gradual transition to IPv6. This transition will span several years, and the pace and motivation for each business and organization to access IPv6 services and content will vary tremendously based on country mandates, business imperatives, security, applications, and geographic and cost constraints, among other factors. During the transition to IPv6, service providers have the opportunity to offer new managed service solutions that provide address translation for IPv4 and IPv6 and unique architectures to support the coexistence of both addressing formats. This document outlines the challenges inherent in the transition to IPv6 for both service providers and different categories of customers, describes network technologies and architectures to ease the transition, and examines different service topologies based on wireline broadband, mobile, VPN, and data center services. It also outlines potential consulting services that may be offered by service providers and a roadmap of consulting deliverables to prepare for, deploy, and scale IPv6 networks.

Customers Confront the Transition to IPv6

As all service providers now know, the Internet Assigned Numbers Authority (IANA) has distributed the last block of IPv4 addresses to Regional Internet Registries (RIRs). Depletion of IPv4 addresses will occur throughout the world at different times for different regions between 2011 and 2012. The exhaustion of IPv4 addresses has been hastened by billions of new IP devices (such as smartphones, cameras, home appliances, and networked sensors) providing data, voice, video, and multiple converged services. In the last decade, large numbers of new users in areas of the world with high population densities have also played a part in speeding depletion of IPv4 addresses.

IPv6 is supported by most software applications, hardware devices, and network, storage, and computer operating systems. But full IPv6 operability must be supported end to end, both within domains and across the Internet. Until this end-to-end support is a reality, enterprises and service providers must implement transitional strategies that support IPv4 alongside IPv6.

To date, businesses and service providers have generally been slow to adopt IPv6. A July 2010 survey by Cisco® of mainstream enterprise customers found that 60 percent have plans to deploy IPv6 addressing infrastructure within 24 months. Some of these customers say they are responding to the growing use of IPv6 on the Internet by new applications and devices. Others have been forced to move to IPv6 by government mandates. Still others simply want to be prepared for the future and do not want to be limited by existing equipment.

Different managed services customers will feel the full effect of the scarcity of IPv4 addresses and require IPv6 services at different times - some much sooner than others. While many enterprises have enough public and private IP address space to meet their intranet demands in the coming years and use Network Address Translation (NAT), stateful Address Family Translation (AFT), and other techniques to stretch existing IPv4 address pools, other companies will need to consider IPv6 dual-stack service solutions more rapidly.

Four different customer profiles have emerged based on different levels of motivation and therefore different planning horizons for their transition to IPv6.

- **The Mandated Customer** category includes government and public sector organizations or companies working with them that are mandated to move to IPv6 rapidly, based on initiatives from the U.S. National Institute of Standards and Technologies (NIST), the Next Generation Internet (NGI) project in China and Japan, and similar efforts in the European Union and elsewhere.
- **The Motivated Customer** is indirectly affected by the exhaustion of IPv4 addresses and may include content providers, global enterprises with consumer or business interaction on the public Internet, companies engaged in mergers and acquisitions, and companies with many user-provided devices on their networks. These customers see the need to move to IPv6 in the near term.
- **The Early Adopter Customer** is looking to IPv6 as a competitive advantage, using it to solve business problems and provide new services such as cloud applications, remote desktop support, peer-to-peer applications, and hosting.
- **The Mainstream Customer** includes companies that do not feel compelled to move swiftly to IPv6 and are content to wait for its evolution on the Internet. This category of customer includes large enterprises, as well as medium-sized and small organizations. It encompasses those organizations in the Cisco survey that do not expect to move forward with IPv6 within the next two years.

Helping Customers Make the Transition to IPv6

Today, an all-IPv6 network is not possible, except in the mobile environment, where some limited test networks are underway. Instead, a prudent strategy for service providers is to transition to IPv6 by preserving IPv4 addressing while also deploying a dual-stack IPv4 and IPv6 infrastructure prior to running IPv6 only at a later date.

In the transition to IPv6, different categories of business customers may now require the following.

- **IPv4 and IPv6 Internet presence:** Businesses rely on three main services as part of their Internet presence: email, web servers, and Domain Name System (DNS). If any employees, customers, partners, or suppliers need to access these services from an IPv6 device, IPv6 must be enabled on these services along with IPv4. Certain operational support systems and network operations procedures must also become IPv6-aware. For example, application proxies (including those for web and email applications) used between the IPv6 Internet and the IPv4 enterprise servers will allow Internet users to continue accessing content with IPv4 devices. Allowing external Internet users with IPv6-only devices to access these servers through the proxies requires the use of AFT. Application proxies can be delivered by service providers as a managed service that allows business customers to quickly achieve an IPv6 Internet presence without having to migrate their servers to IPv6. Service providers can build and deliver these services using Cisco Application Control Engine (ACE) blades or appliances.
- **IPv4 and IPv6 Internet access:** Providing IPv6 Internet access alongside IPv4 access allows business users to access both types of content through the Internet. The service provider must deploy solutions for handling the exhaustion of IPv4 addresses to allow IPv4 devices to continue to access Internet IPv4 content. An IPv6 to IPv4 translation service is also needed for IPv6-only devices to access IPv4 Internet content. Native access for intranet users to IPv6 Internet content can be provided by making the intranet hosts and all network devices dual stack, providing tunneled access, or deploying a hybrid of both solutions.

- **Dual-stack VPN services:** Customers using VPN services will need both IPv4 and IPv6 services, which can be deployed in a variety of ways based on different requirements. The primary incentive for dual-stack VPN service is to allow business customers to continue using IPv4 devices to access IPv4 intranet applications while being able to access IPv6 Internet content and IPv6 public or private cloud services from any site.

Consulting Services for IPv6 Transition

The move to IPv6 is complex, and service providers are in an ideal position to provide consulting services to help businesses with the transition. Some service providers have already created these services, while others may wish to contract with Cisco for training to develop consulting offerings or work with Cisco Services jointly to deliver services to business customers. Consulting services for the IPv6 transition are discussed later in this document.

Another important decision business customers must make is where to obtain their IPv6 addresses. As with IPv4, the decision can affect the cost of renumbering intranet hosts, along with certain other considerations, as described in Table 1.

Table 1. IPv6 Address Options

IPv6 Address Option	Description
Provider assigned	These addresses come from the service provider's block of addresses, and are a valid choice for a business intranet without multihomed Internet access. If the service provider's network is down, the enterprise will lose access to the Internet until the service provider network is operational.
Provider independent	There is additional logistical overhead for these addresses, which come directly from the RIR. The addresses may be transferred by the business to a different service provider, if desired, without the need for renumbering. The business can also be multihomed, offering resilient Internet access.
Privately assigned	Unique local addresses (ULAs) that are randomly chosen address blocks are free of charge but are not intended to be routed on the Internet. A business customer using these addresses must therefore access the Internet through application proxies or through new and evolving techniques using NAT between the ULAs and public IPv6 addresses.

IP Address Management Services

In the transition to IPv6, businesses must define a new address plan for IPv6 and a policy for how these IPv6 addresses will be managed and assigned to devices. Service providers can assist customers in this process, providing guidelines and suggesting the best options.

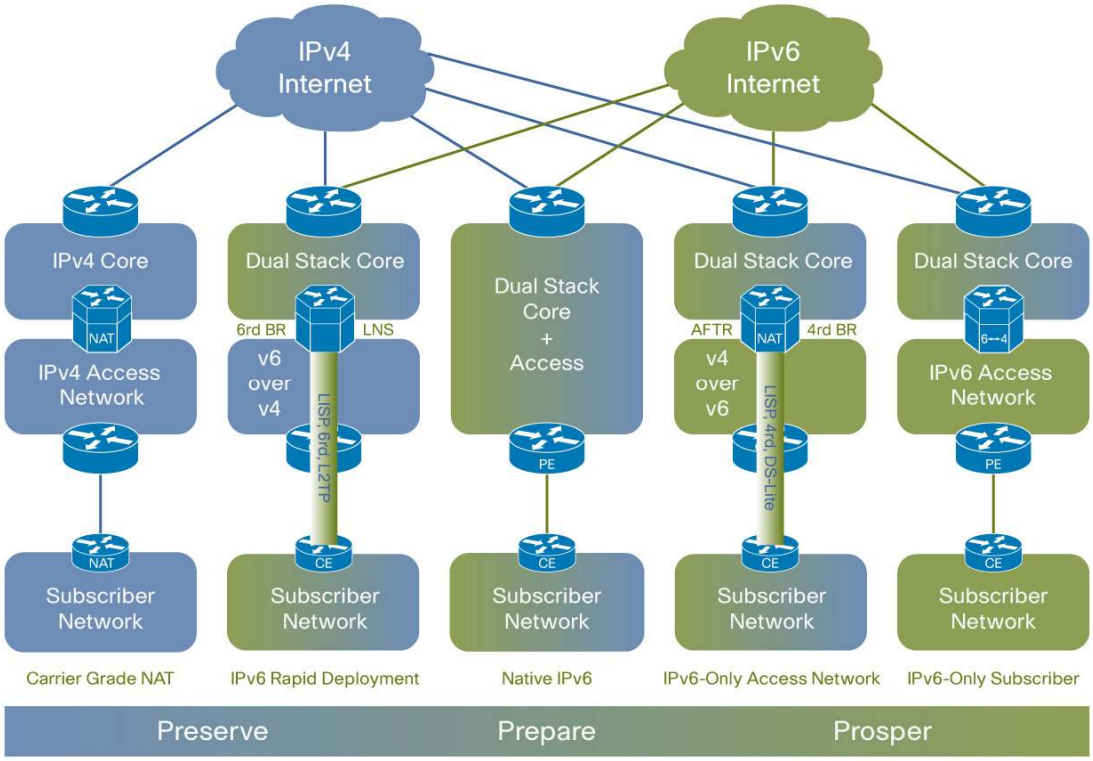
IPv6 addresses can be assigned to devices using either stateless address autoconfiguration (SLAAC) or Dynamic Host Configuration Protocol (DHCP) servers. SLAAC allows devices to connect to the network without interaction with a DHCP server. Although this may be acceptable for residential home networks, most businesses will prefer a more structured approach based on centralized IP address management and the use of DHCP servers that will enable identity and security through stateful configuration. IP address management can be delivered as a managed service by the service provider using the Cisco Network Registrar product, the industry's most scalable and proven DHCP server, supporting over 50 million devices in a single deployment and tens of thousands of requests per second.

Connectivity and VPN Services for the IPv6 Transition

As previously mentioned, the transition from IPv4 to IPv6 will occur gradually. During this process, service providers will rely on Network Address Translation 44 (NAT44) to extend IPv4 addresses, combined with dual-stack architectures to support both IPv4 and IPv6. As the IPv6 web becomes more available and less traffic passes through NAT, IP traffic will be handled much more efficiently.

In Figure 1, the gradual transition from IPv4 (in blue) to IPv6 (in green) is shown, with current topologies relying on NAT on the extreme left and a depiction of an IPv6-only network on the extreme right.

Figure 1. Transitional IPv4 and IPv6 Addressing Services



Between the beginning and end scenarios shown are intermediate solutions.

IPv6 rapid deployment (6rd) allows a service provider to rapidly deploy IPv6 services to existing IPv4 sites to which it provides customer premise equipment (CPE). This approach uses stateless IPv6 in IPv4 encapsulation to transit IPv4-only network infrastructure. The encapsulation (also referred to as softwires) must be supported by the CPE, while a solution such as the Cisco Carrier-Grade IPv6 (CGv6) Gateway supports tunnel termination to route packets to Internet hosts on IPv6. The provider access network continues to be on IPv4, while customers see IPv6 and IPv4 service simultaneously. One of the leading deployments of this technology has been Free Mobile in France.

Another technique is Cisco Locator/ID Separation Protocol (LISP), a revolutionary new tunnel technology developed by Cisco and the Internet Engineering Task Force (IETF) that implements a new paradigm for IP addressing. Using LISP, the device identity - known as an endpoint identifier (EID) - and its location - known as its routing locator (RLOC) - are separated into two different namespaces. Creating separate IP addresses for EID and RLOC functions improves the scalability of the routing system through greater aggregation of RLOCs and improves multihoming efficiency and ingress traffic engineering.

Using Dual-Stack Lite (DS-Lite), the subscriber router is provisioned only and natively with IPv6. Any IPv4 traffic on the local customer LAN is tunneled by the CPE over the IPv6 infrastructure to the Carrier Grade NAT (CGN) device. The IPv4 address space the subscriber gets would normally be RFC1918 or similar non-globally-routable addressing. The CGN terminates the tunnel and translates the IPv4 local addressing into globally routable IPv4. If the subscriber network has the capability to use IPv6, the IPv6 traffic is routed natively through the ISP's infrastructure. A single IPv4 NAT operation is applied in the service provider network to the subscriber traffic.

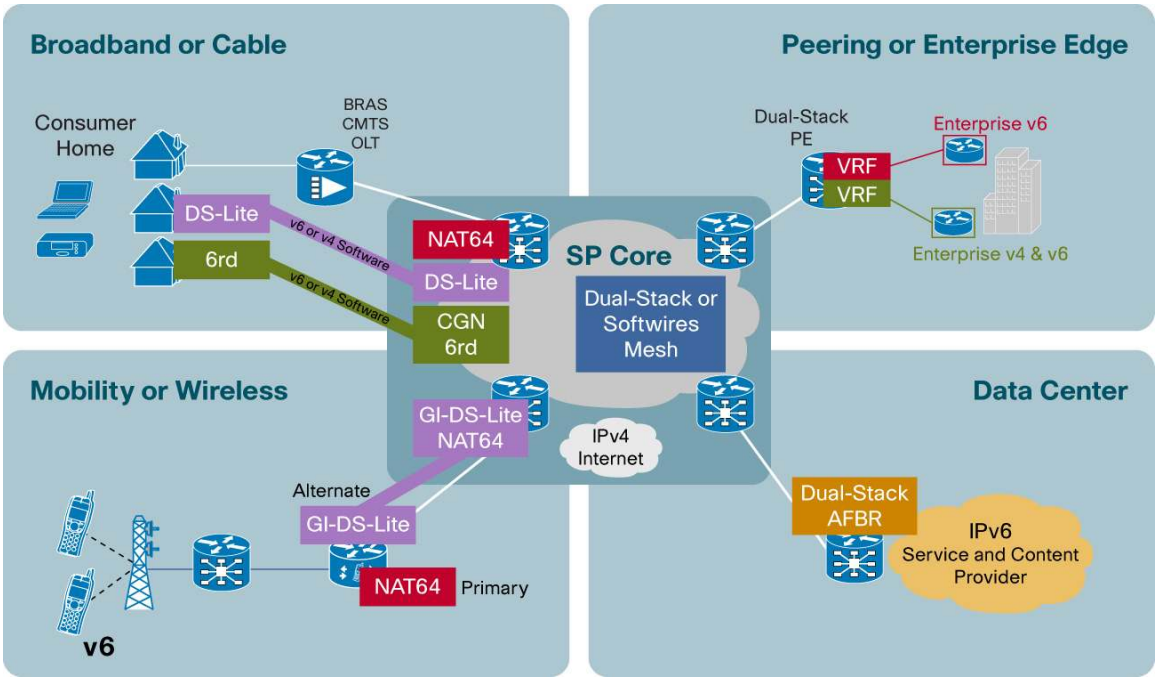
With native IPv6, part of the service provider network (for example, the access and aggregation layers) only supports IPv6 routing. The CPE is provisioned only and natively with IPv6. Any IPv4 traffic on a local LAN is tunneled by the CPE over the IPv6 infrastructure to a solution such as the Cisco CGv6 Gateway. The encapsulation (or softwires) must be supported by the CPE. The IPv4 address space of the subscriber is a private one. The Cisco CGv6 Gateway terminates the tunnel and translates the IPv4 local addressing into globally routable IPv4 (NAT44). If the subscriber network has the capability of using IPv6, the IPv6 traffic is routed natively through the service provider infrastructure. A single IPv4 NAT operation is applied in the service provider network to the subscriber traffic.

An IPv6-only access network supports IPv6 for Internet access while preserving IPv4 addressing within the intranet, with various tunneling and NAT technologies supporting IPv6-to-IPv4 address translation and alleviating the need to dual-stack both core and access layers.

IPv6 Service Transition Architectures

Different solutions for providing IPv4 and IPv6 addressing services by different types of service providers are shown in Figure 2.

Figure 2. IPv4 and IPv6 Service Topologies by Service Provider Type



- **Broadband and cable access services:** Service providers deploying new broadband, cable, or mobile services will choose to increasingly base their new access infrastructures on IPv6 but must allow customers to access IPv4 content. Enterprise branches, small- and medium-sized business offices, and home offices that need to connect to a corporate IPv4-based VPN can be provided with an IPv4 over IPv6 tunneling solution such as 6rd, Cisco LISP, or Gateway-initiated DS-Lite (GI-DS-Lite) and NAT64 for address translation.
- **Mobile and wireless services:** Mobile users with devices such as smartphones and tablet computers will receive an IPv6 address when connecting to some wireless services. They will also require connectivity to the public IPv4 Internet and their corporate IPv4-based intranet. Again, this will require a dual-stack tunneling solution and NAT64 or its equivalent.
- **Enterprise dual-stack VPN services:** Users within enterprise organizations (including those in the public sector) that access their intranet VPN through a service provider's managed Multiprotocol Label Switching (MPLS) VPN or IP Security (IPSec) VPN service, will need dual-stack IPv4 and IPv6 services at the provider edge to provide access to both intranet and Internet IPv4 and IPV6 content as well as dual-stack extranet services to business partners and Internet access.
- **Data center services:** For most businesses, IPv6 Internet presence will be the first phase of a transition to IPv6. Service providers delivering hosting services for web, email, and DNS can provide a dual-stack Address Family Border Router (AFBR) for IPv4 and IPv6 services and content.

These examples are just some of the solution topologies service providers may deploy in the transition to IPv6. Solutions for each customer will depend on a variety of factors and existing infrastructure and services. Some businesses are enabling their campus networks for IPv6 first and then planning to move to IPv6 for Internet communications afterwards. Others are considering doing the opposite.

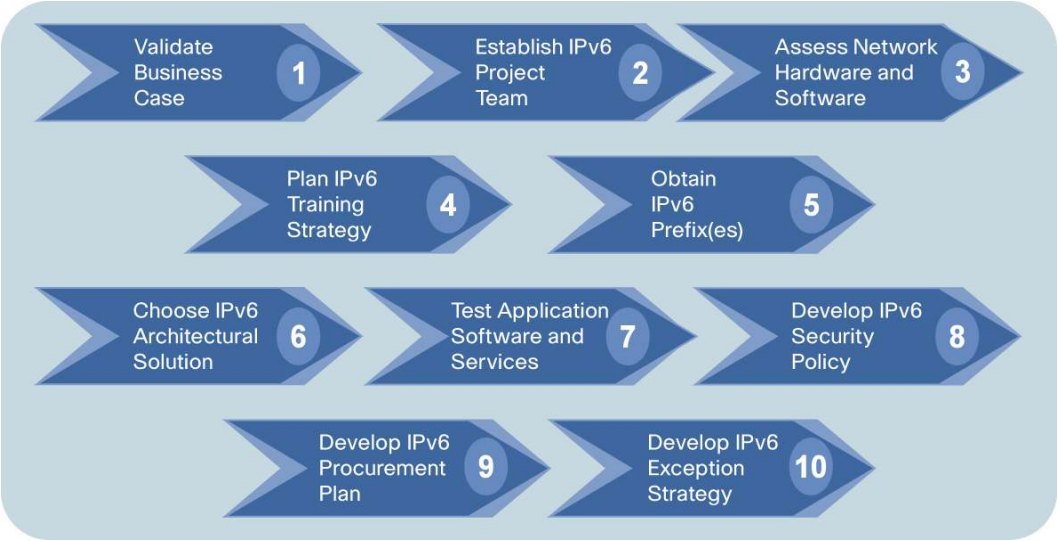
Integrating IPv6 into Managed Services

Beyond addressing the short-term needs of business customers by providing IPv6 Internet presence, dual-stack Internet access, and VPN connectivity, service providers should consider creating a roadmap for the evolution of their managed services portfolio to encompass IPv6 over the next 2 years. Customers will expect the same service-level agreements (SLAs) for IPv6 as they do for IPv4, and Cisco already has in place many of the solutions that are required to bring IPv6 functionality to managed router services, managed LAN and WLAN services, managed application performance management, managed security, and managed unified communication services.

Helping Customers Plan for their Transition to IPv6

The IPv6 transition is an opportunity for service providers to sell both consulting services and managed services to a range of business types and sizes. A lifecycle management discussion can begin with the strategic deliverables suggested in Figure 3. The customer may rely on the service provider as a trusted partner to help with or be responsible for some or all of the following.

Figure 3. IPv6 Transition Strategy for Service Provider Customers

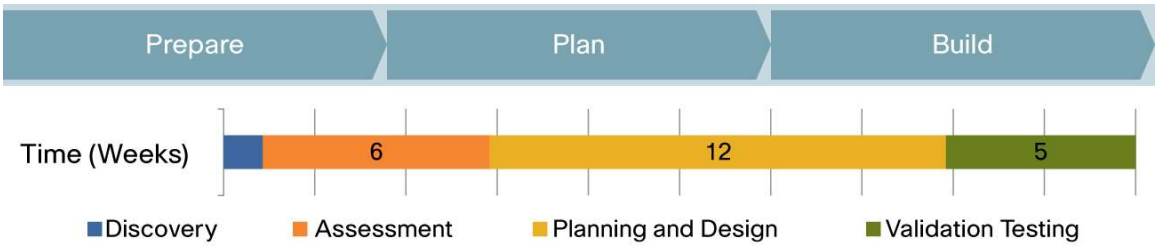


1. **Validate a firm business case:** Service providers can assist their customers in identifying applications, opportunities, threats, and other issues that necessitate access to IPv6 services and content. The return-on-investment in IPv6 services should then be calculated.
2. **Establish an IPv6 project team:** A customer project team should be created that may include help from the service provider and partners, including Cisco. The team should establish goals, a critical path, and timelines.
3. **Assess network hardware and software:** Network hardware and software should be checked to verify that they are IPv6-compliant and that hardware has sufficient memory for running dual-stack services and handling NAT. The Cisco IPv6 Network Assessor Tool can be used to accomplish this. If any infrastructure is not compliant, an upgrade plan should be created.
4. **Plan IPv6 training strategy:** Operations staff must understand how to manage IPv6. Design architects must understand IPv6 capabilities. Security architects must understand IPv6 risks and mitigation. The managed service provider can supply these services as part of an overall services agreement.
5. **Obtain IPv6 prefix(es):** IPv6 addresses can either be provider assigned or provider independent, based on the customer's requirements.
6. **Choose IPv6 architectural solution:** As previously discussed, native IPv6, dual-stack, IPv4-to-IPv6 tunnels, IPv6 on Provider Edge Router (6PE), and IPv6 on VPN to Provider Edge Router (6VPE) are all different architectural options. An addressing plan should be developed that clearly defines how addresses will be distributed to customers.
7. **Test application software and services:** Either the service provider can handle this in-house or the provider can help enterprise customers establish a lab for testing applications and services for IPv4 and IPv6 functionality and interoperability. Network management systems (NMS) and billing systems should also be fully tested for dual IPv4 and IPv6 interoperability.
8. **Develop IPv6 security policy:** IPv6 has the same security threats as IPv4. A security policy must be articulated that protects against threats that may arise during the transition from IPv4 to IPv6 and beyond.
9. **Develop IPv6 procurement plan:** All future hardware, software, and applications should be IPv6 compliant and IPv6 requirements should be incorporated into a procurement plan.

10. **Develop IPv6 exception strategy:** Network, server, and storage components that will remain on IPv4 must be identified. Factors that influence an exception policy may encompass technical, business, or cost constraints.

A 6-month, scoped consulting engagement, such as the one shown in Figure 4, may include the following deliverables.

Figure 4. IPv6 Consulting Services and Timeline



- **Discovery phase:** Evaluate the potential effects of IPv6 on the IT infrastructure, discuss IPv6 capabilities, align business strategy and IT strategy to encompass IPv6, and identify business-critical applications and network infrastructure.
- **Assessment phase:** Align business and IT strategy consistent with the Discovery phase, gather technical and business requirements for implementation of IPv6 on infrastructure and applications, analyze the network for IPv6 readiness, and implement recommended changes and upgrades.
- **Planning and design phase:** Assess the current network architecture and map business objectives and technical requirements for one critical application or network area to a proposed high-level network architecture design. Analyze and document a business profile and requirements and network success metrics relative to Cisco best practices for the critical application or network area, create an adoption schedule, and translate a high-level design into a low-level design. Provide consultative support and knowledge transfer sessions while the customer is implementing the architecture.
- **Validation testing phase:** Develop and apply a plan for implementing IPv6 in a Cisco or service provider laboratory on a pilot network and then on a production network, develop test plans for each stage of the network implementation, and provide consultative support and knowledge transfer sessions to the customer during validation of the design and implementation of the architecture.

The Cisco Advantage

Cisco is leading the transition to IPv6 with a multitiered approach, expertise, and solutions to help service providers and their customers move to IPv6. The Cisco strategy includes efforts to preserve IPv4 addressing infrastructure and associated services and content, to prepare for the gradual transition to IPv6 with hybrid IPv4 and IPv6 strategies, and to help service providers prosper during the migration to a predominantly IPv6 network. With IPv6, new revenue-yielding managed service and consulting opportunities are possible. The technologies of translation, tunneling, and encapsulation are complex, and Cisco has been working to provide solutions and guidance to help service providers promote and support an orderly and gradual transition toward IPv6 for customers.

The transition to IPv6 will take time and involve diverse techniques and end-to-end interoperability. Cisco solutions for dual IP addressing stacks, tunneling, and NAT are supported across most of the company's network portfolio. As an early pioneer in IPv6 technology since its inception, Cisco has been a leading force in developing IPv6 standards through various standards bodies, including the IETF, and has been shipping a wide variety of end-to-end IPv6 products and solutions.

Cisco's strategy is to empower our service provider partners to deliver IPv6 transition offerings by creating flexible services using the provider's value propositions and market strategies. Cisco offers industry-leading technology and expertise and has become the internetworking supplier of choice because of its global, 24-hour support and clear vision of network, service, and application convergence over IP/MPLS technologies. Cisco helps managed service providers build new managed service offerings with tested, documented, and validated solution architectures, technical training, and certification assistance.

Cisco Services can assist service providers through the managed services development lifecycle. This lifecycle offering includes Advisory Services (to help build the business case for a new service), Advanced Services (to provide specialized expertise for the design, building, and testing of a service), and Collaborative Services (to help operate the service or services on an ongoing basis, as needed).

Additionally, the Cisco Managed Services Channel Program (MSCP) supports Cisco partners that sell and deliver managed services to their customers. The program provides escalating discounts, rebates, and rewards for partners based on Cisco solutions and corresponding SLAs delivered to the end user. Cisco supports MSCP partners as they market and sell their services with marketing campaign resources and sales training resources.

For More Information

Cisco IPv6 Site
http://www.cisco.com/go/ipv6

Cisco Carrier-Grade IPv6 Solution
http://www.cisco.com/en/US/netsol/ns1017/networking_solutions_solution_category.html

Cisco IPv6 Strategies - Podcast
http://www.cisco.com/cdc_content_elements/podcast/3_26_09_94754_RobSloanPodcast_Chip.mp3

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA C11-670230-00 06/11