How Cisco IT Is Implementing IPv6: Progress Update

Cisco IT now provides permanent IPv6 Internet presence and is well on the way toward ubiquitous IPv6 network access.

EXECUTIVE SUMMARY

CHALLENGE

- Develop IPv6 Internet presence
- Progress toward ubiquitous IPv6 access on internal network
- Keep costs down

SOLUTION

- For Internet presence, initially used reverse-proxy approach to save time; long-term plan is dual-stack approach
- For Internet access, enabled dual-stack support from the inside out, starting with core network
- Coordinated equipment upgrades and software updates with Cisco IT's Fleet Upgrade Program

RESULTS

- Enabled IPv6 on cisco.com, webex.com, and home.cisco.com
- Provided IPv6 access in approximately one-third of global offices and in 90 labs
- IPv6-enabled 75 percent of core network

LESSONS LEARNED

- Carefully plan address space
- Complete design early so IT team can certify hardware and software
- Consider using reverse proxy as temporary measure until native IPv6 support can be implemented

NEXT STEPS

- Enable IPv6 throughout cisco.com, including product ordering, support, and more
- Provide dual-stack support for IaaS platform (CITEIS) and extranet
- Enable IPv6 on approximately 10,000 desktops at 90 sites

Background

At Cisco, the network connects people to people, people to devices such as sensors, and devices to devices. The confluence of people, process, data, and things, known as the Internet of Everything (IoE), is helping to increase asset utilization, improve productivity, create efficiencies in the supply chain, enhance the customer experience, and foster innovation.

IoE requires a vast number of IP addresses. This posed a challenge at Cisco because the Internet Assigned Numbers Authority (IANN) handed out its last IPv4 address block to the five regional Internet registries on January 31, 2011. As of March 2013, two of the registries had exhausted their address space, and the others are not far behind.

The solution is IPv6, which supports an unlimited number of global addresses. While IPv4 addresses contain 32 bits, or up to approximately 4.3 billion addresses, IPv6 addresses contain 128 bits, or up to of 2^{128} IP addresses. That number equates to billions and billions of addresses for every square meter on the planet, supporting the Internet of Everything.

An ancillary benefit of unlimited global addressing is eliminating the need for hardware and software to perform Network Address Translation (NAT) from IPv4 to IPv6. With IPv6, no translation is necessary because every device can have its own address. Although Cisco IT will continue to use NAT and firewalls for network edge security, not having to use it for communications protocols simplifies configuration.

Challenge

Cisco IT has been planning and executing the integration of IPv6 into the IT infrastructure since 2002, balancing the effort with other IT priorities such as cloud computing, data center virtualization, and continuing adoption of Cisco TelePresence® and other collaboration technologies. The initiative became more urgent as the IPv4 address space approached depletion. "Compliance requirements from governments where we do business, lack

of new IPv4 addresses, especially in emerging markets, and proliferation of mobile devices drove the business case for our internal IPv6 adoption," says John Manville, senior vice president of Global Infrastructure Services for Cisco IT.

The transition to IPv6 affects the entire enterprise network, which connects 450 Cisco offices in 90 countries. More than 180,000 people connect to the Cisco corporate network, including 68,000 employees, 20,000 channel partners, more than 100 application service providers, and approximately 200 development partners.

Planning requirements included:

- Not disrupting existing business processes
- Developing processes to support operational efficiency
- Coexisting with IPv4 for many years to come

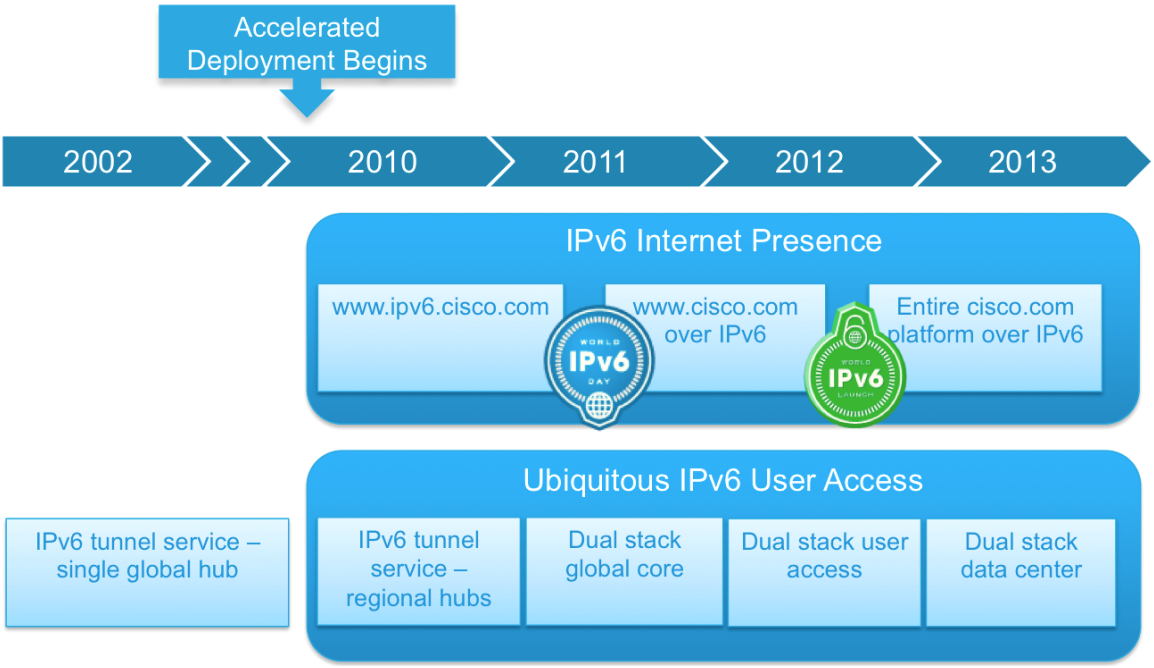
Implementation requirements, in turn, included:

- Maintaining the same service-level agreements (SLAs) and security posture for the dual-stack environment (IPv4 and IPv6) at the same level as for IPv4 alone
- Keeping costs down by scheduling equipment and software upgrades to coincide with the global Fleet Upgrade Program schedule
- Making sure that Internet service providers and software vendors (for monitoring, content distribution, and more) could work with IPv6 traffic, through close partnership with the Vendor Management Office
- Expediting IPv6 support for Cisco business units and labs that would need to test IPv6 before Cisco IT could offer native IPv6 transport across the core and distribution networks

Solution: 2002–2010

Cisco IT's journey to IPv6 can be viewed in two stages: a gradual effort from 2002–2010, and then an accelerated effort beginning in 2010, as IPv4 address exhaustion became imminent (Figure 1).

Figure 1. Timeline for Journey to IPv6 at Cisco



In 2002, development and testing of IPv6 features in Cisco® routers and switches were well under way. The corporate network needed to support IPv6 for lab-to-lab testing and to allow developers and test engineers to connect from their desktops to the labs.

The first steps on the journey to IPv6 were to:

- Acquire IPv6 address space
- Define a global IPv6 address plan
- Provide IPv6 connectivity to connect IPv6-enabled labs

Acquiring IPv6 Address Space and Defining Global IPv6 Address Plan

Cisco IT received a /32 Provider Aggregatable (PA) address block from ARIN in early 2001 (Figures 2 and 3). ARIN gave Cisco the same type of address space that Internet service providers use because Provider Independent (PI) space was not yet available. “Each type of address space has its pros and cons and routing challenges,” says Jon Woolwine, Cisco IT distinguished engineer and lead architect for the IPv6 program. “Cisco IT chose to continue with the Provider Aggregatable address space to align with current industry trends toward strict filtering and top-level aggregation policies.”

Cisco IT carefully planned how to allocate the address space to different geographies, following the same principles that the company had used for IPv4 addresses. The team considered each region’s anticipated growth when developing the plan.

Figure 2. Cisco IPv6 Breakout Plan: 50 Percent Spares Held at Each Level of Address Hierarchy

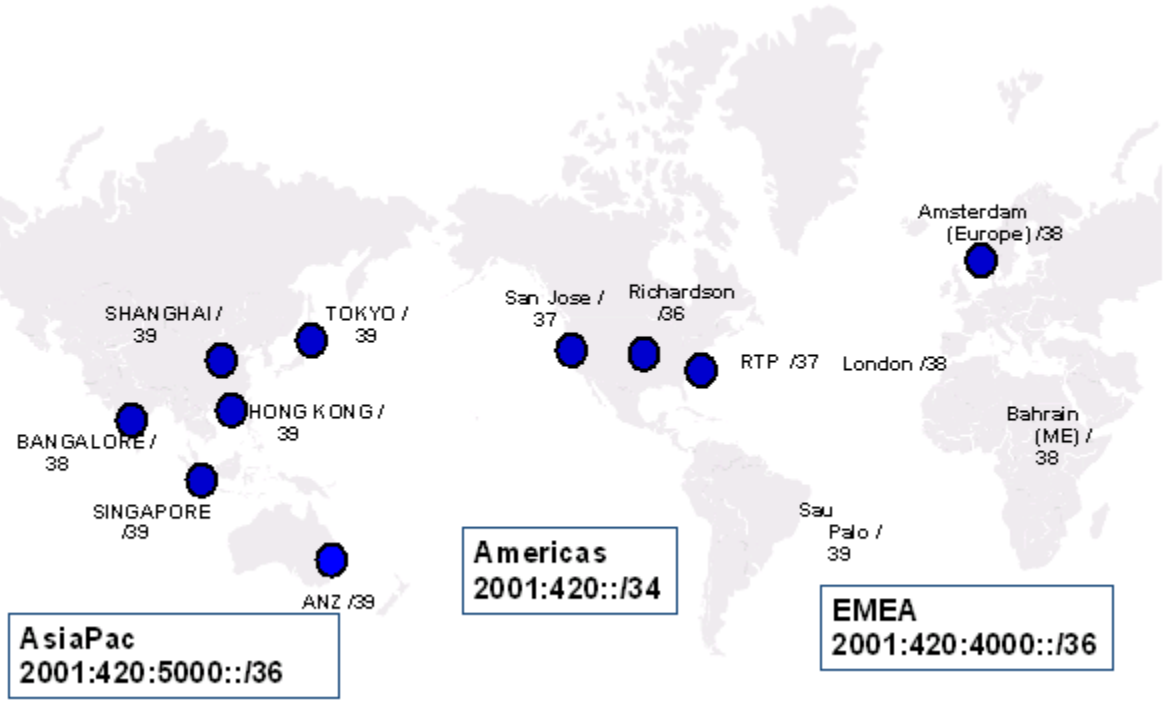
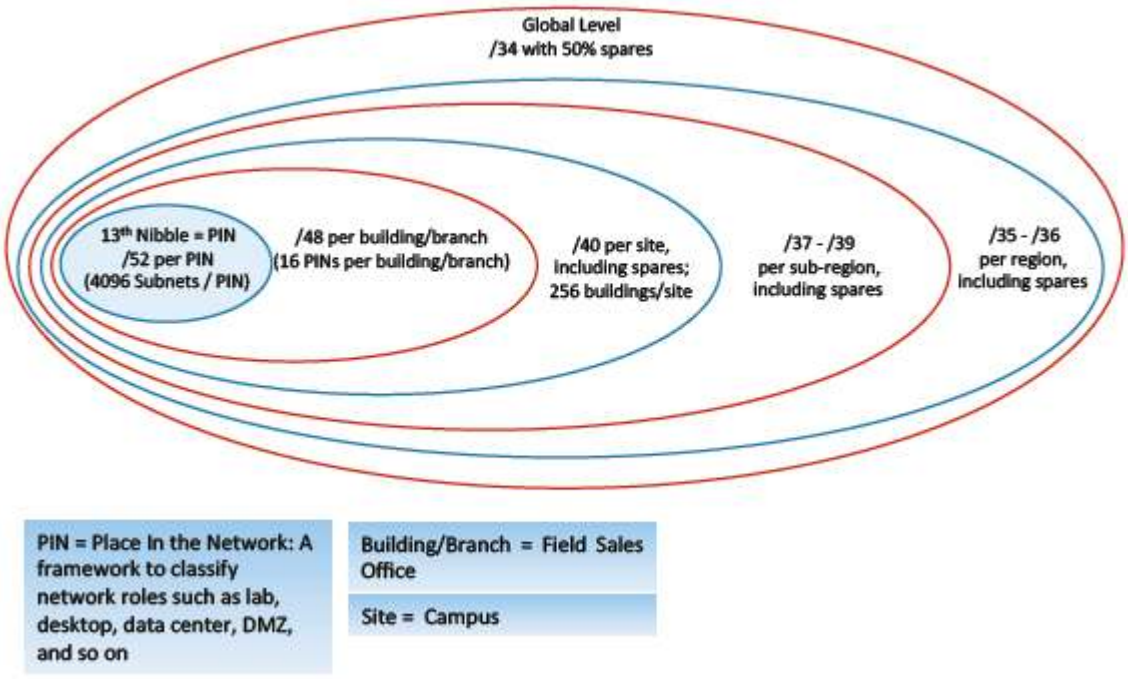


Figure 3. IPv6 Address Planning: Breaking Down /32 Prefix



To simplify operations and automate address allocation for environments, including the internal private cloud and labs, Cisco IT followed these guidelines when developing the IPv6 addressing scheme:

- Allocating IP addressing across clean-bit boundaries to facilitate troubleshooting of infrastructure-related issues
- Using specific bit places to represent network functions, another way to simplify troubleshooting
- Keeping subnet sizes the same size to avoid the intricate sizing planning that the IPv4 addressing scheme required

To manage the IPv6 address space, Cisco IT modified a dedicated web-based application to support IPv6 and added support for IPv6 in the company's domain name system (DNS) services. "Early on, we enabled our DNS infrastructure to advertise AAAA records so that domain names can be resolved to IPv6 addresses," says Woolwine. In the early stages of the transition, Cisco IT also used Cisco Prime™ Network Registrar to enable DHCPv6, which provides dynamic IPv6 address assignment.

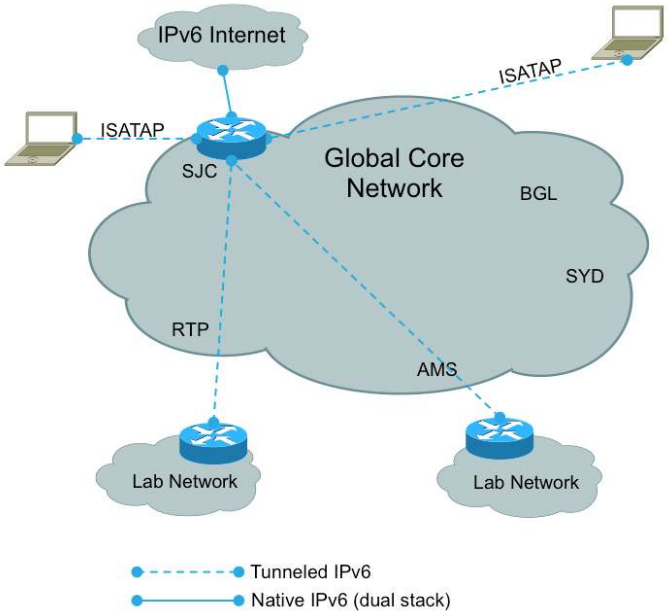
Knowing that Regional Internet Registries will eventually exhaust their IPv4 address pools, Cisco IT recently developed a plan to conserve existing public IPv4 addresses to use for Internet-facing applications and services. "In some areas of our network, we've begun swapping out publicly routable IPv4 address space for RFC1918 space," Woolwine says. "The goal is to repurpose this public routable IPv4 address space in our data centers." Cisco IT swaps address space during network hardware refreshes.

Developing Lightweight Solution for IPv6 Connectivity to Labs

After developing the IPv6 address plan, Cisco IT turned its attention to developing a lightweight solution to provide IPv6 connectivity for labs, engineering teams, and Cisco headquarters in San Jose, California. To implement the

solution quickly, the team decided to use 6in4 tunnels as a transition technology. “At this stage, the labs were islands of IPv6 that connected over the IPv4-only corporate network,” says Bob Scarbrough, member of the technical staff with the Cisco IT Customer Strategy and Success team. All tunnels terminated on a single router in San Jose, California (Figure 4). Engineering teams that needed IPv6 connectivity from desktop PCs to labs used Intra-Site Automatic Tunnel Addressing Protocol (ISATAP), and these tunnels terminated on the same router as the 6in4 tunnels.

Figure 4. Early Stages of IPv6 Connectivity, with Tunneling



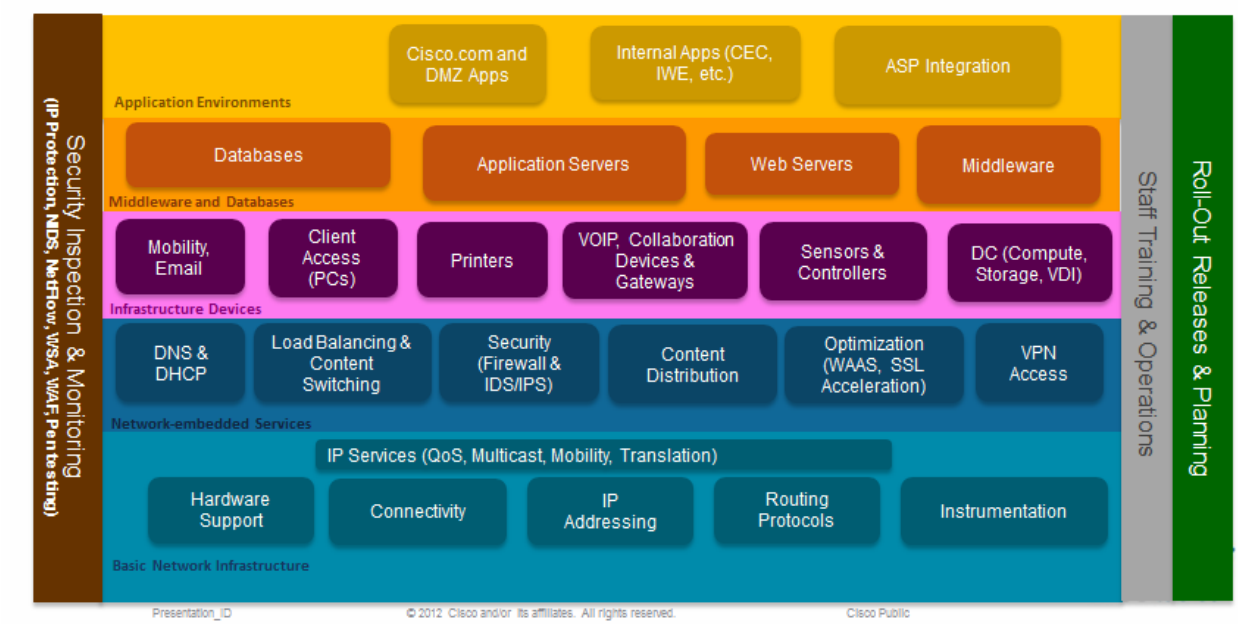
Solution: 2010–Present

In 2010, IPv4 address exhaustion was imminent and IPv6 adoption quickened. Anticipating customers’ needs, Cisco product development teams began accelerating product support for IPv6, providing the same functions available with IPv4.

Forming Project Team and Agreeing on Design Goals

The first step was to form a cross-functional team to agree on goals for IPv6 integration and migration. “To develop the program structure, we envisioned the final result and worked backwards to identify changes to the network and infrastructure,” says Shannon Sharma, Cisco IT program manager for IPv6. “This requires extensive teamwork across multiple organizations.” Figure 5 shows the teams involved in the IPv6 program, which correspond to the elements in the Cisco IT stack.

Figure 5. Framework for IPv6 Adoption at Cisco: Cisco IT Stack



"The cross-functional team that began with the networking and data center services teams has spread to also include application, security, and web teams," says Brian Christensen, senior director and executive sponsor for the IPv6 Infrastructure deployment.

> "The cross-functional team that began with the networking and data center services teams has spread to also include application, security, and web teams."
> **Brian Christensen, Senior Director and Executive Sponsor for the IPv6 Infrastructure Deployment.**

The team developed two strategies, executed in parallel, to integrate IPv6 into the global Cisco network. One track was to develop an IPv6 Internet presence, making public content, services, and applications available to customers, partners, and employees connecting with IPv6 devices. The other track was to provide ubiquitous IPv6 connectivity to all access networks. Both efforts are in progress today. Design objectives included:

- Not jeopardizing existing IPv4 services and applications, such as cisco.com and the internal corporate network, during the transition. This was the guiding principle.
- Preserving the cisco.com brand and control over the cisco.com experience.
- Not compromising the corporate security posture.

- Re-using existing infrastructure, capabilities, content, and application environments whenever possible
- Compiling lessons learned to share with customers

Readiness Assessment

As the first step, Cisco IT engaged Cisco Services to provide IPv6 readiness support through the Cisco Network Optimization Service. “We had to make sure that hardware and software were ready for a large-scale IPv6 deployment,” says Woolwine. As part of the Network Optimization Service, Cisco Services uses Cisco Network Collector to retrieve hardware and software configurations from every device in the network. Using this information, Cisco Services created an easy-to-read IPv6 readiness report that made it easy to see which hardware and software needed upgrades or replacements.

Referring to the reports, the team first determined if the hardware platform supported basic IPv6 functions. If it did not, Cisco IT replaced the hardware through the normal Fleet Management Program, Cisco IT’s infrastructure lifecycle management program. Upgrading through the Fleet Management Program spread out the capital expense associated with IPv6 adoption. “We wanted to absorb costs in the established upgrade process rather than incur the all-at-once costs of ripping and replacing,” says Woolwine.

If the hardware was IPv6-capable, Cisco IT determined whether the Cisco IOS® Software version supported IPv6. Where necessary, the team upgraded the software. “We also worked with our vendors to find out when third-party software would be IPv6-compliant,” says Joseph Chieng, a Cisco IT project manager focusing on the IPv6 efforts with the Cisco Global Government Solutions Group.

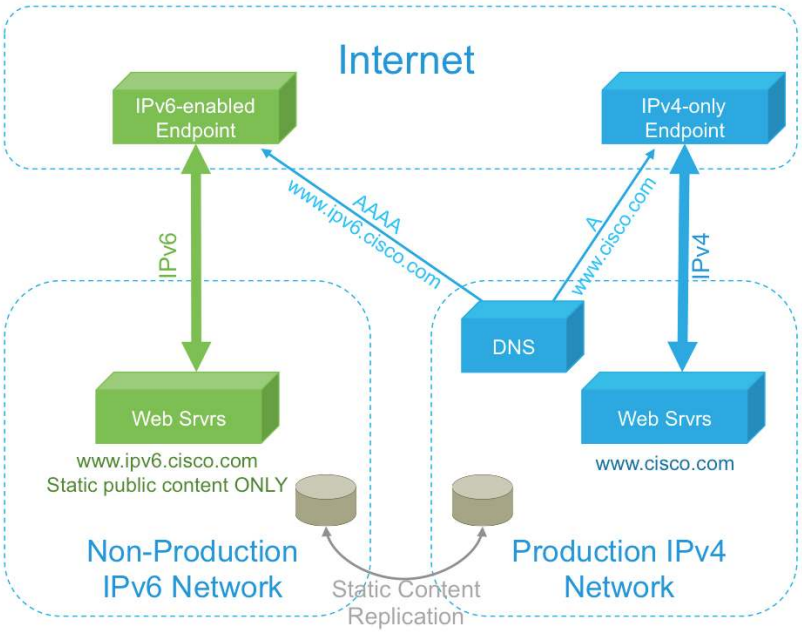
Developing IPv6 Web Presence

The following paragraphs describe the steps that Cisco IT took to develop an IPv6 web presence.

Step 1. Enabled Native IPv6 Access to Public Website

The team began with a low-risk project, enabling native IPv6 access to the public website in an isolated test, or “sandbox” environment with a non-production domain name, www.ipv6.cisco.com. The goal was to give the web team hands-on experience with IPv6 without placing public-facing content and services at risk. To accomplish this, the team first built a non-production IPv6 network with dual-stack web servers. Then they replicated static public content from the production web servers to the non-production dual-stack web servers, which exposed the content to users connecting from IPv6-enabled hosts (Figure 6). To provide IPv6 Internet connectivity, Cisco IT implemented tunnels to service providers.

Figure 6. First Phase: IPv6 Internet Presence on Non-Production Web Servers

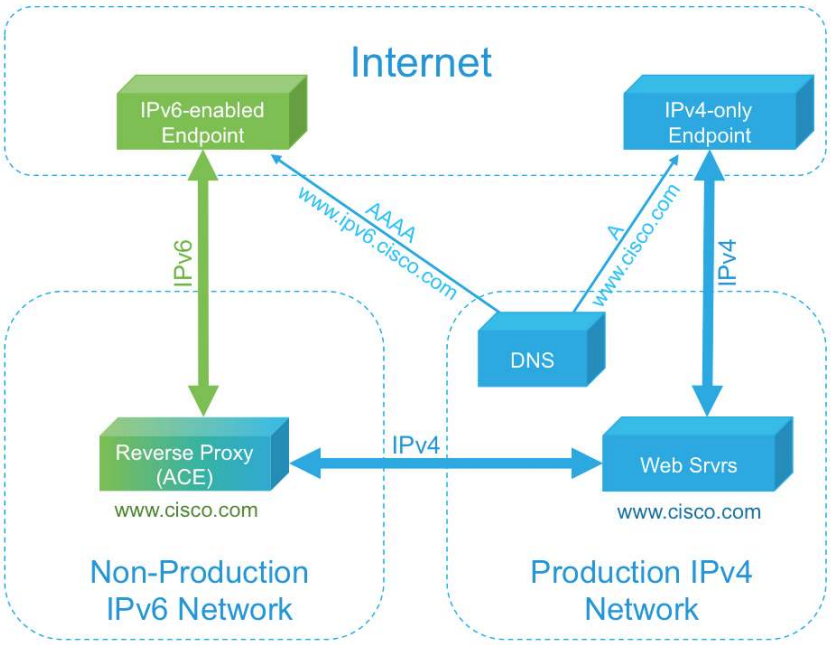


Step 2. Participated in World IPv6 Day

Held on June 8, 2011, World IPv6 Day was a one-day global event to test global readiness for IPv6. Cisco IT participated by making www.cisco.com accessible by IPv6. To complete the project in time for the event, the team decided to use a reverse-proxy design, also known as Server Load Balanced IPv6-to-IPv4 (SLB64). The reverse proxy directs incoming IPv6 connections to a backend IPv4-only web server. The solution is based on the Cisco ACE 30 Application Control Engine Module for Cisco Catalyst Switches (Figure 7). “We chose the reverse-proxy architecture because we didn’t have much time, and this approach minimized the impact on our data center, network, server, and application teams,” says Woolwine. More detail about the reverse-proxy design appears later in this case study.

No major issue occurred during World IPv6 Day, and the event was widely regarded as a success for Cisco and the industry at large.

Figure 7. Reverse-Proxy Architecture for World IPv6 Day

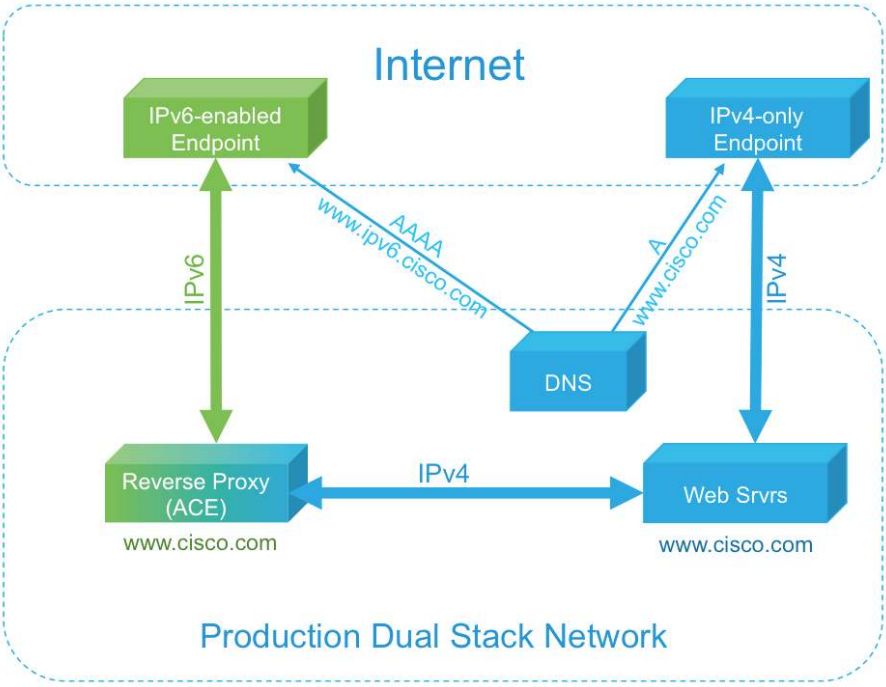


Step 3. Participated in World IPv6 Launch

World IPv6 Launch followed a year after World IPv6 Day, on June 6, 2012. The goal was for content providers and network operators to turn on IPv6 and leave it on permanently. Cisco IT decided to participate in World IPv6 Launch by permanently enabling IPv6 access to www.cisco.com. Goals included:

- No significant incremental costs: This led to the decision to continue using the reverse-proxy architecture implemented for World IPv6 Day (Figure 8).
- End-user experience comparable to the IPv4 experience: Cisco IT used the same caching and acceleration solution used for the IPv4 web presence. To gain visibility into the user experience for customers and partners outside the United States, the team used a third-party web analytics tool with dual-stack support to analyze NetFlow v9 information.
- Same SLAs for availability provided for IPv4 web presence: This required redundant service provider circuits and continual monitoring of availability and performance.
- Operational readiness: Operations teams received the education and tools to support and troubleshoot the IPv6 web presence in the same way that they already supported the IPv4 web presence.

Figure 8. Production Dual-Stack Network for IPv6 Web Presence



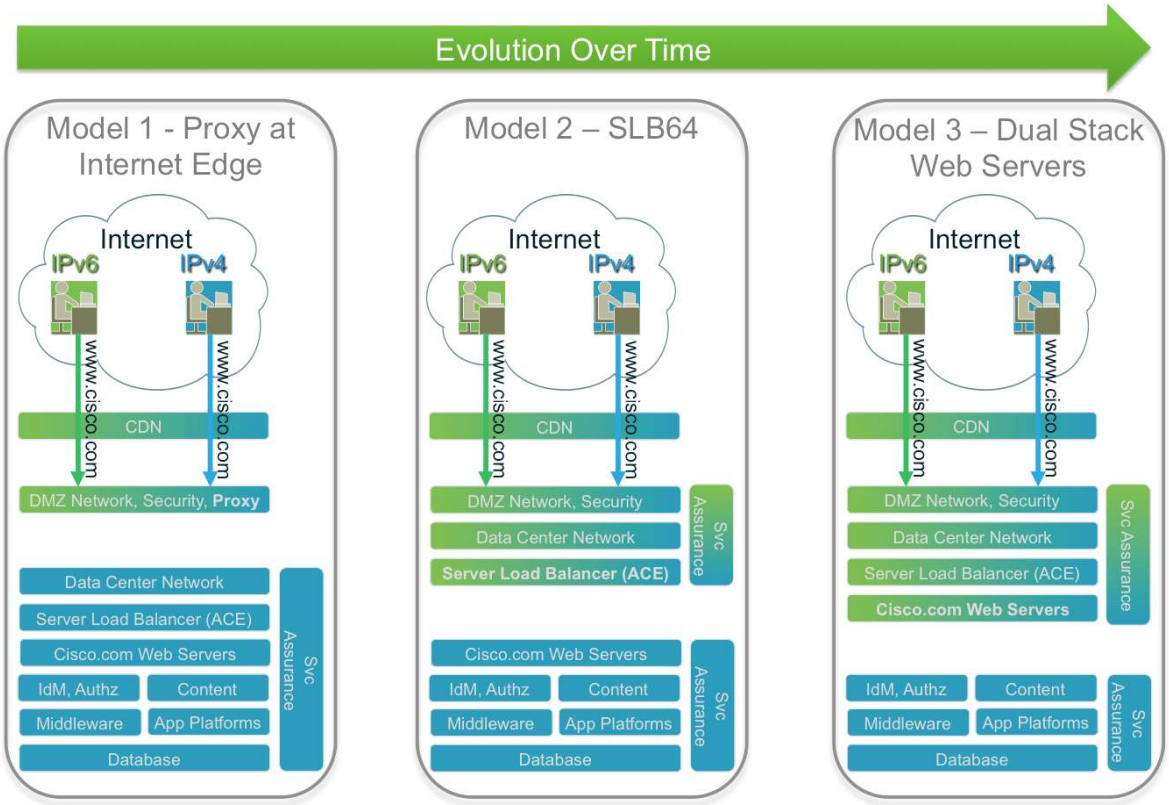
"World IPv6 Launch was a major success for Cisco and the industry," says Manville. "No major glitches occurred during the event, and Cisco IT is sharing lessons learned about architecture, design, and operations with our customers as they continue their own IPv6 journeys."

Step 4. Continued Working Toward Web Presence Target State

The target state for Cisco IT's web presence is an end-to-end dual-stack design that extends IPv4 and IPv6 connectivity all the way to the web servers. In Figure 9, the left side shows the design for World IPv6 Day, the middle shows the design for World IPv6 Launch, and the right side shows the target state. The backend platforms and systems are currently IPv4-only. Later Cisco IT will migrate these platforms to dual-stack.

"Enabling cisco.com to support IPv6 helps Cisco better serve our customers, increase our competitive advantage, comply with global compliance needs, and bring thought leadership to the IPv6 community," says Sheila Jordan, senior vice president for communications and collaboration, Cisco IT.

Figure 9. Target State: End-to-End Dual-Stacked Infrastructure to Support Internet Presence



Architecture for IPv6 Internet Presence

Architectural elements for the Cisco IPv6 Internet presence include a reverse proxy, dual-stack production network, DNS and name resolution, content delivery service, web analytics system, availability and performance monitoring, and security.

Reverse Proxy

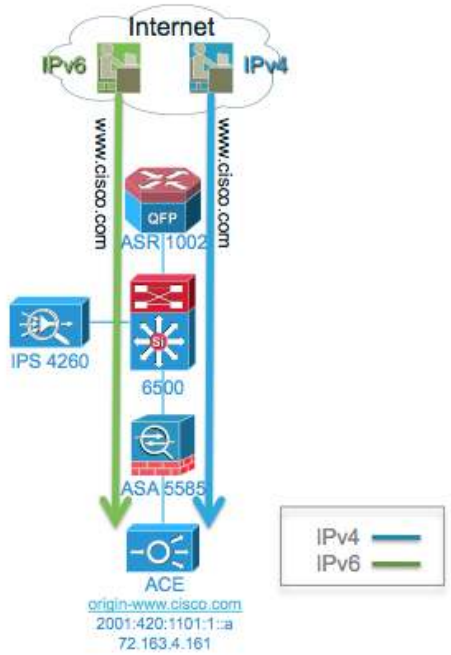
Cisco IT chose the reverse-proxy design (labeled SLB64 in Figure 9) for two reasons. One was that the relative ease of implementation would help the team make the deadline to participate in the World IPv6 Launch. The other rationale was to avoid the need to extend IPv6 connectivity all the way to the web servers, eliminating concerns about whether the web server OS and business applications supported IPv6. “We view the proxy-based approach as a stepping stone to the target state, which is dual-stacking all the way to web servers,” says Woolwine. “We recognized that bringing IPv6 all the way to the web servers would introduce unknowns and require a greater time commitment from systems administrators and web administrators. The reverse-proxy design gave us the best opportunity to move quickly and minimize risk.”

“Starting with a proxy-based design also bought time for cross-platform IPv6 support to mature,” says Khalid Jawaid, Cisco IT network engineer. “Organizations that start their transition later might find it easier to use dual-stack from the beginning.”

> “We view the proxy-based approach as a stepping stone to the target state, which is dual-stacking all the way to web servers. We recognized that bringing IPv6 all the way to the web servers would introduce unknowns and require a greater time commitment from systems administrators and web administrators. The reverse-proxy design gave us the best opportunity to move quickly and minimize risk.”
>
> **—Jon Woolwine, Chief Architect for IPv6 Program, Cisco IT**

Cisco ACE 30 Application Control Engine Modules act as the proxy. The web server farm has virtual IPv6 and IPv4 addresses hosted on the reverse proxy, while the physical web servers have an IPv4 address only. Figure 10 shows a traffic flow from an IPv6 endpoint accessing www.cisco.com. The DNS server advertises an AAAA record for the website, and the record points to the virtual IPv6 address hosted on the Cisco ACE30 module. When IPv6-enabled endpoints initiate a web connection to www.cisco.com, the proxy server terminates the connection and then initiates an IPv4 session to the production server. The proxy remains in this middleman role for all traffic between IPv6-enabled endpoints and the production IPv4 web servers. Traffic from IPv4-only endpoints flows as it would without the proxy service. “With the reverse-proxy approach, making Internet-facing services IPv6-accessible only requires changes to the web server, not the underlying application servers and management software,” says Woolwine.

Figure 10. IPv6 Internet Presence Using Reverse Proxy



The Cisco ACE30 module also provides server load balancing over IPv4. Cisco IT configured the Internet Point of Presence (iPoP), DMZ, and data center networks for dual-stack support, allowing IPv6 traffic to flow from the Internet to the 6to4 proxy.

Dual-Stack Production Network

To test the reverse-proxy design before the launch, Cisco IT needed a production network. The team enabled IPv6 end to end: on the Internet, gateways to existing service providers, the iPoP/DMZ segment, WAN backbone, core network, and desktop infrastructure.

DNS and Name Resolution

Cisco IT uses the same name-resolution process used previously for the IPv4-only web presence. Solution elements include:

- DNS services within Cisco IT
- Cisco Global Site Selector (GSS), used for global server load balancing
- DNS services within the content delivery network (CDN) provider's network

To provide name resolution in a dual-stack environment, Cisco IT added support for AAAA records into Cisco GSS and the CDN provider network.

CDN Provider's Service

Cisco IT's web team worked with the CDN provider to make sure the provider could support downloads to IPv6 clients, with an experience comparable to the IPv4 client experience. The CDN provider inserts the IPv6 source address when proxying HTTP requests back to the origin.

Web Analytics System

The team continues to use the same web analytics system used when the web presence was IPv4 only. The vendor modified the system to also collect and report IPv6 address data.

Availability and Performance Monitoring

Cisco IT enabled IPv6 support on its internal management tools and Cisco Prime products. "From the start, we had the capability to track both IPv6 and IPv4 performance," says Jeff Lehman, project lead for IPv6 web team. The team made a few changes at the application layers to accommodate IPv6 and the proxy-based design.

The web team is adding IPv6 support to applications in other web server environments one by one. For each application, the team first makes sure that it can monitor availability and performance over IPv4 only, IPv4 and IPv6, and IPv6 only. The tools report historical trending for IPv4, IPv6, and both. Alerts about availability issues indicate whether the device or application is IPv4 or IPv6.

To monitor availability and performance of web services from outside the enterprise, Cisco IT works with its existing vendor, which connects from many points on the Internet and reports how long it takes to load pages.

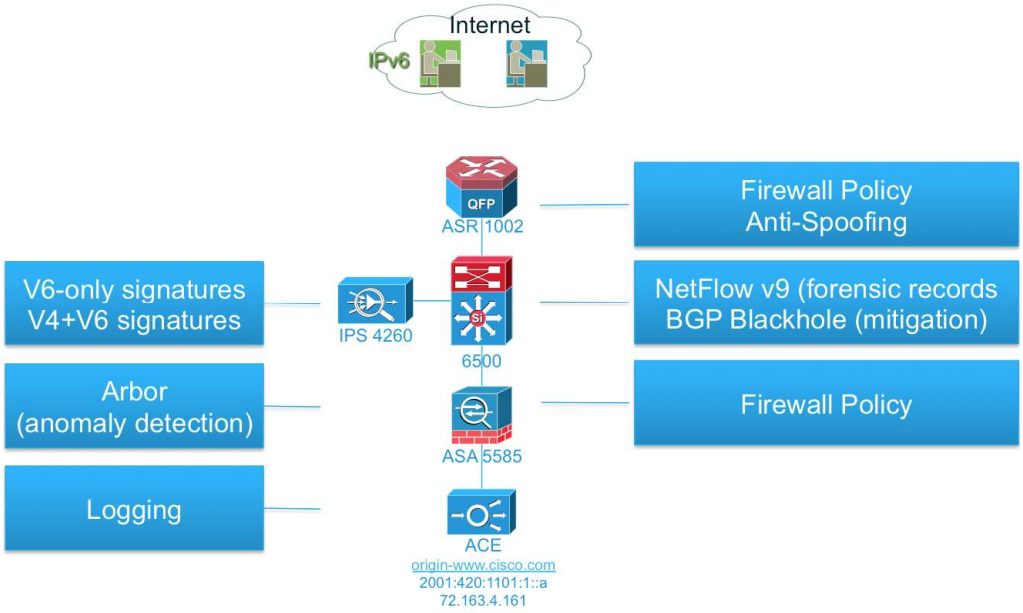
Security

The security design for the proxy architecture included the following elements (Figure 11):

- IPv6 address anti-spoofing policy in the network
- NetFlow v9 for forensic analysis

- Anomaly detection
- Traffic blackholing for mitigation of security events

Figure 11. Security Design for IPv6 in Proxy Setup



Partnering with Service Providers for IPv6 Services

When Cisco IT first embarked on its journey to IPv6, most IPv6 service providers provided IPv6-over-IPv4 tunnels. As services providers begun offering dual-stack services, Cisco IT worked with its existing service providers to plan the transition.

Initially, the service providers installed temporary IPv6 Internet circuits that were physically separate from production circuits. Later, the providers decommissioned the temporary circuits and deployed production dual-stack circuits, still in use. “We worked with all of our service provider partners to make sure the IPv6-based services we would receive were comparable to our current IPv4-based services,” says Christensen. During the transition, Cisco IT worked closely with Cisco engineering teams and Cisco Services to fine-tune the Cisco IOS Software. Recommendations from Cisco IT have been implemented in Cisco network devices for the benefit of customers.

Providing Ubiquitous IPv6 Access

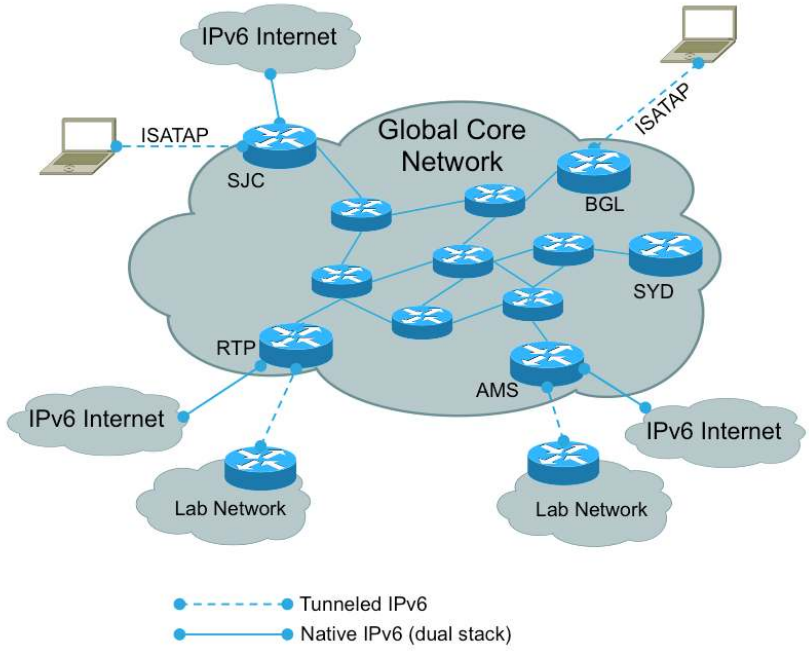
In parallel with introducing an IPv6 Internet presence, Cisco IT worked to provide access from IPv6-enabled devices from anywhere on the Cisco global network. The team decided to take an inside-out approach. “The plan was simple: extend from the core outwards across the distribution and access layers to the desktop,” says Jawaid.

Step 1. Improved Tunnel Overlay Performance

In the original design, all 6in4 and ISATAP tunnels terminated at a single hub at San Jose headquarters. But as engineering groups accelerated IPv6 product development and testing, backhauling all traffic to San Jose began

to degrade performance. “To provide consistent performance, we modified the tunnel design by placing tunnel hubs in each region around the globe and distributing IPv6 Internet access into some of these locations,” Woolwine says (Figure 12).

Figure 12. Regional IPv6 Tunnel Hubs Avoid Congestion from Backhauling Traffic to One Hub



Step 2. Extended IPv6 Connectivity Across Core

When preparing for World IPv6 Day in 2011, Cisco IT began upgrading the core links to support dual-stack traffic, starting with the heavily trafficked core links connecting San Jose and Bangalore. In the upgraded parts of the network, all network services, including quality of service (QoS) and multicast, apply to both IPv4 and IPv6. “The dual-stack strategy enabled us to move one step at a time toward end-to-end IPv6,” says Christensen.

The team first enabled iPv6 on primary network devices, and then on backup devices. This approach gave Cisco IT the confidence to extend IPv6 into the core, because the team knew that they could fall back to IPv4 if something did not work as expected. Soon after, Cisco IT added dual-stack support to iPoPs and DMZs.

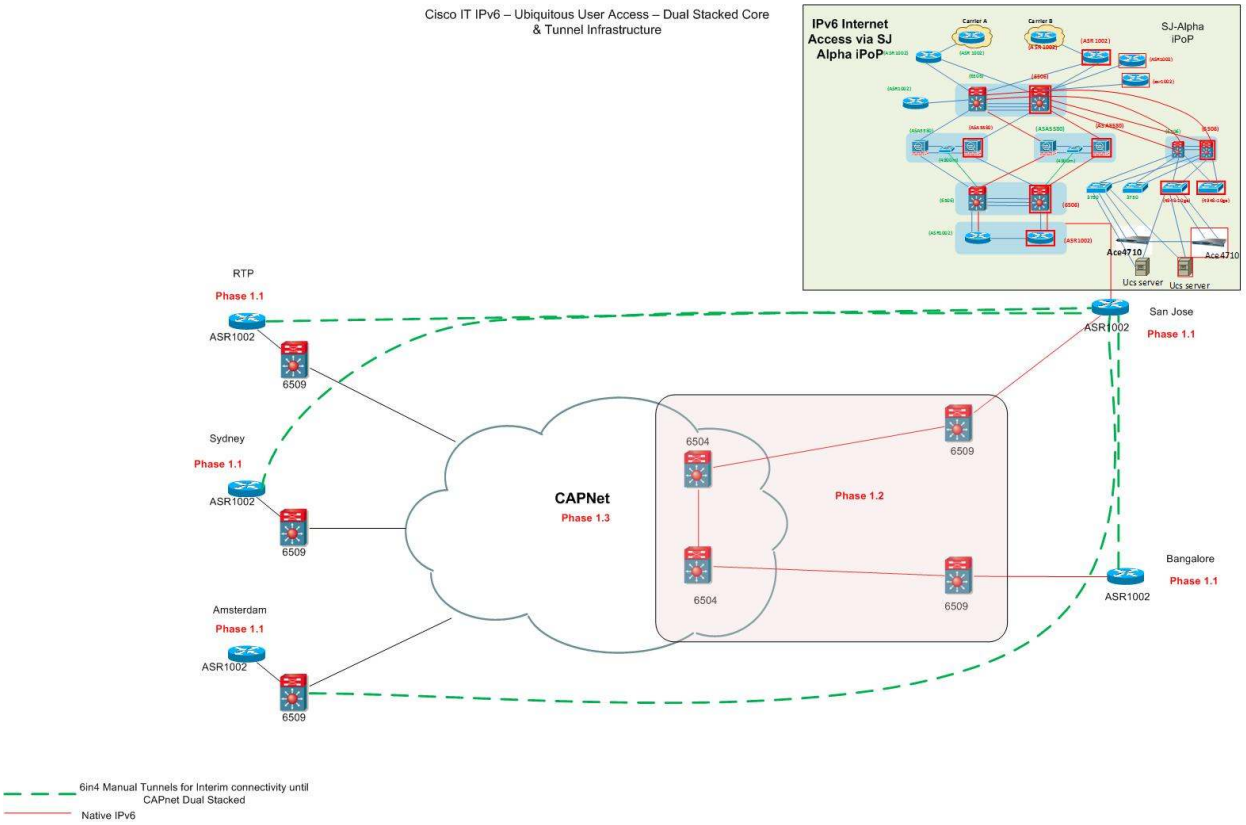
To avoid incremental costs for integrating IPv6 into the network, Cisco IT implemented IPv6-capable hardware and software through the Fleet Upgrade Program. Early in the IPv6 transition project, the design team updated the design standards for the Fleet Upgrade Program to include IPv6 requirements. “We chose to introduce IPv6 gradually, to not incur incremental costs,” says Jawaid. “By following the normal hardware and software refresh cycle in the Fleet Upgrade Program, we didn’t have to make a big one-time investment to IPv6-enable the infrastructure. The key to success is aligning the deployment timeline with change control windows and release cycles.”

> “We chose to introduce IPv6 gradually, to not incur incremental costs. By following the normal hardware and software refresh cycle in the Fleet Upgrade Program, we didn’t have to make a big one-time investment to IPv6-enable the infrastructure. The key to success is aligning the deployment timeline with change control windows and release cycles.”
>
> **—Khalid Jawaid, Network Engineer, Cisco IT**

The core network is now dual-stack, as shown in Figure 13. In locations that previously used 6in4 tunnels to a headend, Cisco IT retired the tunnels.

Cisco IT used Enhanced Interior Gateway Routing Protocol (EIGRP) for IPv4 and continues using it today, with the dual-stack network. “It’s a good idea to use the same routing protocol for IPv4 and IPv6 to simplify support activities for operational teams,” says Woolwine.

Figure 13. Ubiquitous IPv6 Access: Dual-Stacked Core and Tunnel Infrastructure



Step 3. Extended IPv6 to the Desktop

Since 2003, Cisco users have had the option of turning on ISATAP to acquire IPv6 connectivity through an Anycast regional ISATAP router. Labs could request IPv6 tunnels through the same regional headends.

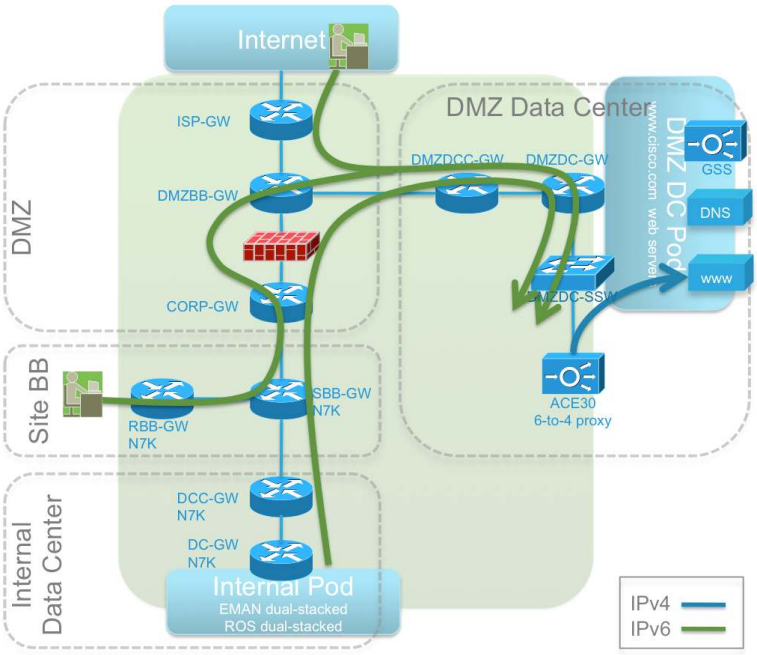
More recently, Cisco IT began providing native IPv6 support through a dual-stack network in dozens of global sites. The program started with the wired network and then expanded to wireless networks in conjunction with the Fleet Upgrade Program. Extending IPv6 to the desktop involved:

- Enabling IPv6 on the devices.
- Turning on IPv6 on the various operating systems used in the Cisco enterprise after extensively testing the operating systems: The Cisco IT client services team, which maintains all approved OS images, was engaged early in the process of extending IPv6 to the desktop. Employees were told that a building supported IPv6 only after the client services team provided an approved build.
- Making sure that printers could use DHCPv6 for IPv6 address assignment: Cisco IT set the affinity options to make sure that printers always received the same IPv6 address.

Step 4. Extended IPv6 Into Data Centers

Extending IPv6 into data centers required two actions. One was turning on IPv6 in the Cisco Nexus® Switches and Cisco Catalyst® Switches, which were already certified for dual-stack operations (Figure 14). The other action was configuring management software, Including Cisco Network Registrar, to monitor the IPv6 Internet presence and automatically assign addresses to IPv6-capable desktops.

Figure 14. Extending IPv6 to Data Center



Operational Readiness

Operational support requirements increased during the journey to IPv6. At the outset, monitoring was limited to 6in4 tunnels to regional headends and a small number of IPv6-enabled devices. As Cisco IT began adding dual-stack support across the end-to-end infrastructure, the team had to prepare to support IPv6 with the same SLAs offered for IPv4. “We expect our network devices to remain dual-stack for years, so we don’t immediately need to move management services entirely to IPv6,” says Woolwine. “We can continue to use IPv4 for SNMP queries and traps and for configuration management processes.”

To identify internal and third-party tools and processes that needed updates to support IPv6, Cisco IT conducted a Fault, Configuration, Accounting, Performance, and Security (FCAPS) evaluation. The Operations Command Center (OCC) management and escalation process has remained the same, and the team supports the same SLA for IPv6 and IPv4 devices.

Cisco IT engaged Cisco Services for IPv6 design reviews, software version recommendations, security recommendations, and testing. “Cisco Services shared best practices for the IPv6 transition, helping us avoid pitfalls that other companies have experienced,” says Jawaid.

Results

“As Cisco continues its journey towards becoming a borderless enterprise, our IPv6 deployment is enabling many of the infrastructure requirements mandated by our present and future business strategies,” says Manville. “It has become clear that for enterprises large and small, IPv6 is not just a side thought, but a core technology evolution that will play an important role in the future of business and IT strategies.”

“As Cisco continues its journey towards a borderless enterprise, our IPv6 deployment is enabling many of the infrastructure requirements mandated by our present and future business strategies. It has become clear that for enterprises large and small, IPv6 is not just a side thought, but a core technology evolution that will play an important role in the future of business and IT strategies.”

John Manville, Senior Vice President, Global Infrastructure Services, Cisco IT

Cisco IT has permanently IPv6-enabled popular external websites, including www.cisco.com, home.cisco.com, and www.webex.com.

The team has also made significant progress toward ubiquitous IPv6 Internet access:

- One hundred percent of the core network is IPv6-enabled, using Cisco Catalyst 6000 Series Switches and Cisco ASR 1000 Series Routers. This includes:
  - DMZs in the Richardson, Texas data center and at San Jose headquarters. These DMZs connect to the same service provider circuits as before.
  - Interconnect between the Cisco WebEx® data center and the Cisco network: When Cisco users join a WebEx collaboration session using an IPv6 device, the traffic flows directly to the WebEx cloud instead of taking a detour over the public Internet.

  - Richardson data center and other global pods.
- Applications that monitor devices and applications: These applications are IPv6-enabled in Richardson; Research Triangle Park, North Carolina; Bangalore; and Sydney, Australia.
- Approximately one-third of Cisco's global offices. In these offices, employees and contractors can access hosts and applications that have an IPv6 address. More than 88 global sites are scheduled to have IPv6 connectivity by August 2013.
- More than 90 labs, which connect to the tunnel infrastructure: IPv6 connectivity for labs enables Cisco business units to develop IPv6-capable products. "In fiscal year 2013, we are removing the tunnels and extending IPv6 natively down to the lab gateways," says Jawaid. Cisco IT offers formal operational support for IPv6-enabled labs, as well as a formal process to request IPv6 connectivity using existing support tools.

Additional progress includes:

- Enabling DHCPv6 in Cisco Network Registrar version 7 in EMAN, Cisco's Enterprise Management software. EMAN is used for network performance monitoring; application support; and rapid activation of home office network access, voicemail, and other productivity tools.
- Adding more sites with dual-stacked capabilities to the desktop network.
- Implementing IPv6 First Hop Security (FHS) to prevent malicious or unintentional traffic from causing issues. FHS is a suite of security features including Router Advertisement (RA) Guard, IPv6 snooping, and others.
- Upgrading WLAN clusters to the newest hardware, using Cisco Prime Network Control System to monitor wireless IPv6 traffic.

Next Steps

Cisco IT continues to resolve vendor dependencies and gaps in third-party network management tools and security software. The project team is developing an IPv6 blueprint that vendors can use to IPv6-enable their software.

During 2013, Cisco IT expects to expand the cisco.com IPv6 web presence by providing IPv6 access to ordering, support, marketing, and software download services. To save time and minimize resource requirements, the initial design will use the reverse-proxy architecture. Other plans include:

- Delivering end-to-end IPv6 in more locations
- Adding IPv6 support to internal monitoring applications
- Providing an IPv6 Internet presence for all Cisco websites
- Extending IPv6 support to branch offices
- Enabling IPv6 for the 27,000 Cisco teleworkers who use Cisco Virtual Office
- Providing dual-stack support in the desktop environment for the remaining Cisco offices
- Continuing to integrate IPv6 with other borderless network services through the Extended Enterprise Network (E2N) program
- Providing dual-stack support for the infrastructure as a service (IaaS) platform, called Cisco IT Elastic

Infrastructure Service (CITEIS), and the Cisco extranet

- Completing the transition at all IT-owned data center and DMZ sites

Lessons Learned

Cisco IT shares the following advice with other organizations migrating to IPv6:

- Engage early with IT teams outside the core networking team, including the applications, security, and web teams.
- Consider the effect of IPv6 addresses on external parties, including Internet service providers, CDN providers, and third-party application providers.
- Account for lead time from vendors in your project plans. Some of Cisco IT's vendors have not yet formulated a plan for IPv6. Lead time considerations are especially important for organizations that have compliance requirements for IPv6.
- Realize that end-device operating systems behave differently with IPv6. For this reason, Cisco IT plans to test the various smartphone and tablet operating systems in use by the company's mobile workforce.
- Certify new hardware and software in advance of the need: Cisco IT implemented an ongoing certification cycle so that if an issue is identified with existing hardware or software, a new version is already or almost certified. Cisco IT uses the Network Optimization Service from Cisco Services for hardware and software certification, freeing the internal team for other activities.
- Take advantage of prescheduled release windows when possible: It was challenging to align the deployments schedule for World IPv6 Launch with available release windows. "The only solution is to begin planning the IPv6 transition as early as possible," says Sharma. "Taking advantage of release windows helped us minimize downtime required for upgrades."

For More Information

To read additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit.

To read more about Cisco IPv6 Solutions, visit www.cisco.com/go/ipv6.

Note

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

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.**