# Cisco IT Expands IPv6 Web Presence

Cisco IT Methods

## Introduction

Integrating IPv6 into the global Cisco® network began in 2010 with two overarching strategic design goals: 1) develop IPv6 web presence, and 2) provide ubiquitous IPv6 connectivity within the Cisco corporate network. In the past few years, Cisco IT has been steadily increasing users' IPv6 access and working toward its web presence target state of an end-to-end, dual-stack design that extends IPv4 and IPv6 connectivity to public-facing web servers. Deployment progress is detailed in the case study, How Cisco Is Implementing IPv6.

In September 2013, Cisco greatly expanded its IPv6 web presence by providing customers and partners IPv6 access to more than 800 ordering, support, and other externally facing cisco.com applications. A centerpiece of this implementation, which uses a dual-stack design to the web servers, is Cisco Commerce Workspace residing on tools.cisco.com. The primary web portal used by Cisco partners to configure, quote, and order Cisco products and services, Cisco Commerce Workspace has an annual run rate of US$40 billion.

In December 2013, an estimated 3.67 percent of traffic on tools.cisco.com was coming over IPv6. "That percentage represents an annual revenue run rate of $1.5 billion realized via IPv6," says E. Marie Brierley, IPv6 program manager, Global Infrastructure Services at Cisco. "We're not only running large applications over IPv6, but we're starting to realize revenue through traffic relying on IPv6 connectivity. This traffic is expected to grow as adoption of IPv6 increases."

The revenue potential, and a transparent IPv6 user experience, would not be possible without well-planned, upfront application testing and validation of the IPv6 addresses and connectivity.

## Solution

IPv6 is not the concern of network teams alone. The entire IT organization, including network, server, product development, security, application, and senior leadership teams, must adopt the IPv6 migration plan. With more than 800 applications to test for the September launch and 33 cross-functional teams representing them, Cisco IPv6 program leads kicked off the web presence effort by holding recorded, web-conferencing sessions with all the teams. They discussed relevant IPv6 concepts, application migration objectives, and a process for identifying IPv6-related impacts.

Program leads devised a comprehensive checklist to assist stakeholders with determining the impacts, if any, that IPv6 would have on their applications. Application impacts were gleaned from IP address- and connectivity-centric use cases and corresponding special-handling requirements described on the checklist (Figure 1).

**Figure 1.** Excerpt from IPv6 Impact Checklist

| Use Case | Impact |
|---|---|
| I store IP addresses in a database | IPv6 addresses are 128-bit hexadecimal, with colons separating the octets. IPv4 addresses are 32-bit, written in decimal, with periods separating the octets. You may need to adjust your database fields. |

The project charter included keeping business stakeholders apprised of the impacts and overall status of the migration.

“IPv6 isn’t a business capability change. It’s a technology change. From a business stakeholder’s perspective, IPv6 should roll out without any business or customer impact,” says Kaali Dass, IT architect, Connected IT Services at Cisco. “We kept regular communication with IT and business to update key milestones and progress. Also, we had periodic and regular communication with our stakeholders to avoid any surprises.”

Using input gathered from the checklists, application teams performed a thorough impact analysis to identify:

- All applications and services associated with a particular domain
- Remediation required
- Sanity or development testing method:
  - If no change is required in the product’s code, simple sanity testing will check key functionality and whether the application is performing as expected.
  - If code change is required, the application will undergo full development lifecycle testing (How is the IP address coming into the domain? Where is it coming from? Is the IP address correct and posted properly? Is it passing the IP check logic parameters? How is the address being stored?).

During pre-testing activities, Dass’s team collaborated with multiple subject-matter experts to create a small block of common code that would capture and validate IPv6 addresses. Now, internal teams can insert the ready-made block of code where they need it instead of recreating the code multiple times.

Test planning and logistics were carefully laid out and communicated over several weeks. The window for actual IPv6 testing, however, was only a few days. Testers were required beforehand to:

- Ensure IPv6 was enabled on their laptops or desktops. A wiki page contained configuration instructions, and additional testing resources were centralized on the internal Cisco enterprise collaboration platform.
- Verify IPv6 connectivity and check their IPv6 address on the cisco.com platform. IPv6 access was mandatory for all development, testing, and quality assurance (QA) teams. Third-party browser plug-ins allowed the testers to view IPv6 addresses on cisco.com webpages.

“How laptops and other client devices choose which IP protocol to use for connecting to a web-based application was our biggest area of training and documentation,” says Dass. “Extensive instructions and guidelines were needed. We had to provide a process with explicit steps for testers to follow, to ensure that they would be coming through as IPv6 for the testing.”

Pre-testing safeguards were replicated for many of the application teams. Program leads used an email alias and other collaboration tools to address testing issues and provide troubleshooting support.

## Security

Architectural elements of the Cisco IPv6 web presence include a reverse proxy, dual-stack production network, Domain Name System (DNS) and name resolution, content delivery service, web analytics system, availability and performance monitoring, and security.

In a dual-stack environment, security breaches can arise with new IPv6 devices as well as with the technologies that enable IPv4 and IPv6 to coexist. The shared environment calls for a few basic security measures:

- Replicate IPv4 security configuration settings for IPv6.
- Configure host security controls to block and inspect traffic from both IP versions.
- Get familiar with all the possible entry points for IPv6 traffic, especially on new devices.

Additionally, visibility is paramount to security monitoring between IPv4 and IPv6. “If a machine is running both protocols and all we can see is IPv4, we have no way to fully protect that machine, or to know whether a virus is infecting the system,” says Rich West, information security architect at Cisco.

“Our number 1 security message is parity between IPv4 and IPv6 monitoring and log collection capabilities,” says West. “Secondly, it’s important to understand the risks a new protocol might introduce into our networks. Tunnel traffic security holes, stack and endpoint vulnerabilities, etc., increase as more and more devices come online.”

## Lessons Learned

Cisco IT offers the following tips for planning IPv6 application migration:

- Look beyond the applications themselves, and identify external dependencies. Are your network service providers and cloud service providers IPv6 ready? During its migration, Cisco IT had to devise a workaround for a cloud storage provider that did not support IPv6.
- Ensure that testing is done using IPv6, not just IPv4. How are you enabling laptops and other devices for IPv6? That is, how does a client identify itself as using one protocol over the other? Provide testers with clear documentation, guidelines, and tools such as plugins and patches for setting up their laptop or desktop for IPv6.
- Initially deploy IPv6 in test environments (a lab or pilot network) that represent the applications and devices targeted for integration. Keep all IT and business stakeholders informed, solicit their input, and analyze the operational metrics.

## For More Information

Cisco IPv6 deployment guides for enterprises: Design Zone for IPv6 (cisco.com login required).

Cisco IT case study: How Cisco Is Implementing IPv6.

To read additional Cisco IT case studies about a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT.

To view Cisco IT webinars and events about related topics, visit Cisco on Cisco Webinars & Events.

## 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.**