



IPv6-Enabling Your Web Environment

Begin Migration to IPv6 with your Internet-Facing Services

The 30-year-old pool of unique IPv4 addresses is quickly drying up. As a result, makers of laptops, tablet computers, smart phones, netbooks and other user devices will soon be shipping products that contain newer IPv6 addresses only.

When that happens, how do you make sure that the new IPv6-only devices can access your public Web site that is built on IPv4? Similarly, how can internal users access IPv6 content out in the Internet or at an extranet partner's site? IPv6 and IPv4 aren't interoperable, so you'll have to upgrade at least some of your Web environment to become IPv6-capable.

Of course, you'll want to continue serving the billions of IPv4-enabled devices already in use while also accommodating the newer equipment. That means you'll need to run two host-protocol stacks, IPv4 and IPv6, wherever possible, on Web and email servers and supporting network, security and operations equipment.

Plan Now

It's a recommended best practice that enterprises begin to plan their transition to IPv6 now. The recommended Phase One of the migration is to get IPv6 connectivity on public-facing Internet services first, in order to be able to serve external users who may be using shiny new IPv6-only access devices.

In addition to the traditional public Internet connections, many companies now use the public Internet as their extranet transport network for collaborating with business partners and customers. If that's the case in your organization, it is further justification for IPv6-enabling your Web infrastructure to ensure your extranet connections also remain functional.

Your long-term objective is to eventually get everything migrated to running both protocols, referred to as "dual-stack". What's holding back some companies is that not all makers of the equipment they run offer IPv6 software. If not, enterprises have to turn to interim solutions such as tunneling – encapsulating IPv6 packets in IPv4 packets to be sent across portions of the network that haven't yet been upgraded to IPv6.

Eventually, many years from now, when the world is IPv6-dominated with a few pockets of what will then be "legacy" IPv4 devices remaining, the reverse will be happening: IPv4 will be tunneled through IPv6.

Consider Dual-Stack Challenges and Solutions

There's a bit of sticking point with running the IPv4/IPv6 dual stack in the Web environment, especially for very large content providers. One challenge, particularly expressed by some of the largest Web content providers, is to ensure that IPv4 devices can continue to access content without users experiencing delays as the host environment decides whether to return an IPv4 or an IPv6 address to the client device.

Below are some explanations and suggested steps to take in handling this issue and determining which components of your Web environment to IPv6-enable first.

1. Create a DNS Strategy that Avoids 'Brokenness'

IPv6-enabling your Web environment has to account for the way Domain Network System (DNS) host environments work. As you know, when users want to visit a particular Web site, they type a domain name into their browser. An interconnected, distributed worldwide DNS database of domains and IP addresses maps (or "resolves") that domain name, such as "example.com," to its underlying unique IP address, and the connection gets made.

For many years, that IP address was exclusively an IPv4 address. Now, however, you also need an IPv6 address, which requires that you publish what is called an "AAAA" address resource record (AAAA RR) for the address. For their part, IPv4 sites have already published "A" RRs at the IP address's host site.

With both protocols now enabled in the Web environment, then, there will be both the older A RRs and new AAAA RRs. When both protocols are running at both ends of the connection – meaning the connection can be established using either IPv4 or IPv6 – the DNS world is set up so that the AAAA RR stored by the IPv6 protocol is the default record that is returned.

Protect Your Existing Primary Domain

Because an IPv6-enabled Web site will likely return the AAAA RRs if given a choice, an interim best practice is not to associate AAAA RRs with your primary Web domain name, such as "example.com."



The reason is that for the next few years, there will be far more IPv4-speaking devices that attempt to access your Web site than IPv6-enabled devices. You don't want to suddenly break the IPv4 connections to your well-known domain name.

As noted, when both protocols are running at both ends of the connection, the IPv6 protocol is the default record that is returned. The perceived problem here is that there can be a delay, possibly as long as 30 seconds, while the DNS servers assess the situation and default to the IPv6 protocol. That pause in response time has the world's largest content providers worried about users' experiences in a mixed IPv4-IPv6 environment.

Create IPv6-only Domain with Prefix

One interim option to alleviate the delay problem is adding a special prefix to your domain name to differentiate IPv6 connections. In this scenario, if the host detects that the incoming request is sent from an IPv4-only device, it will return an A RR. If it detects only an IPv6-enabled device, it will return an AAAA RR.

Your IPv6 environment, then, could be accessed via something like "ipv6.example.com," which is associated strictly with AAAA (IPv6) records and content. Note, though, that users will need to know and specifically use this URL to get to the IPv6 content.

You could choose to return different content to user devices, depending on whether they are communicating via IPv4 or IPv6 to avoid the potential latency mentioned earlier. That's a strategic decision to make that's, in part, based on the fact that at this moment, IPv6 is not universally deployed.

Stay on Top of DNS Whitelisting Developments

There is also a movement afoot that you should be aware of. Currently under consideration at the Internet Engineering Task Force (IETF) is

an Internet-Draft (a work in progress that may or may not become standard) called the DNS Whitelist for IPv6. This project aims to create a list of IP addresses that have IPv6 capabilities. The idea is that content providers would share the DNS Whitelist to serve content to IPv6-capable access devices. Web site visitors not listed on the DNS Whitelist for IPv6 would receive IPv4-based content.

2. Upgrade Incrementally

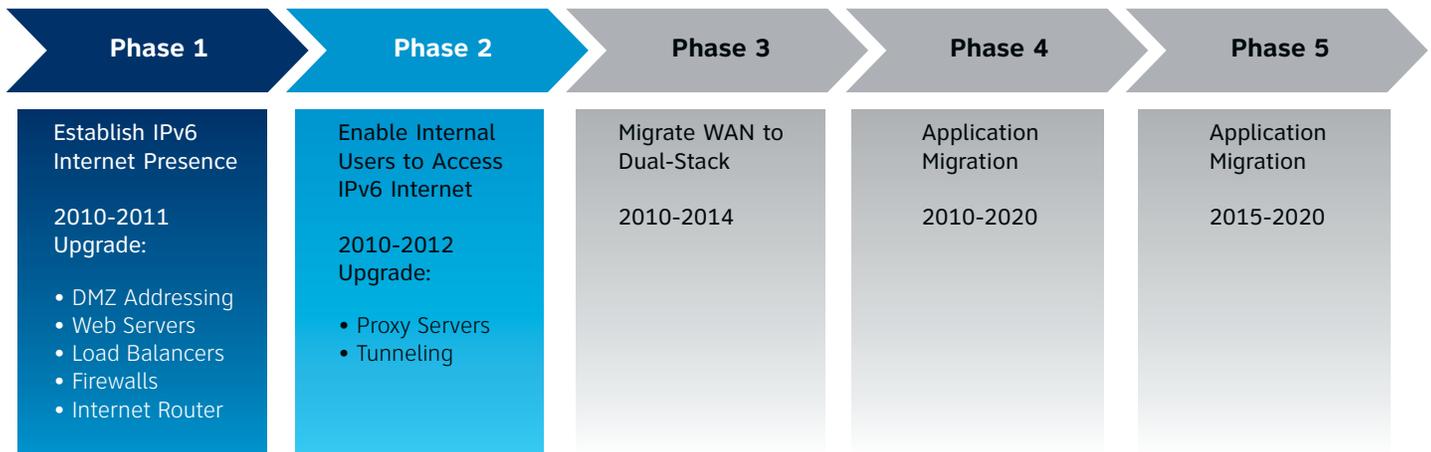
Your entire Web environment doesn't need to be upgraded to support IPv6 all at once. The components of the Web environment needing to speak IPv6 are those that will directly interact with IPv6 content requests from the Internet. The following components will need to run both IPv4 and IPv6 addresses:

- Firewall. Avoid tunneling, mentioned earlier, on this network component to prevent unwanted and unidentifiable access in and out of the Web environment
- Proxy servers and reverse proxy servers
- Web load balancing equipment
- Web servers that you want to serve up content to IPv6 connections. This might include all your Web servers or just a portion of them to start – with a strategy to upgrade the entire Web server farm gradually as you see an increase IPv6 content requests from site visitors

On the other hand, you don't need to upgrade your databases and application servers right away, because they have a trusted relationship with your Web servers at the back end over your existing IPv4 environment.

Below is a sample recommended migration plan.

IPv6 Migration, Phases 1 & 2: Internet



3. Optimize Apps and Web Servers

It's important to ensure that your Web applications are optimized for functioning in a dual-protocol world going forward. One aspect of this is to be sure that Web developers use fully qualified domain names (FQDNs) for making calls between databases, rather than IP addresses. This approach minimizes the risk of broken connections because of application code.

For software that has been developed in recent years – particularly open source Web server software such as Apache HTTP – IPv6-enabling applications might be quite simple. You might need to enter IPv6

addressing information into configuration files and screens. Some programs will need to be restarted, while more sophisticated ones will simply require notification to function in both IPv6 and IPv4 mode.

Summary

Enterprises don't need to panic over the imminent depletion of the IPv4 address pool. However, they should feel a sense of urgency in getting the Internet-facing side of their network environments to a point where it is IPv6-capable and begin planning for that now, if they haven't already.

For more information on how AT&T can help you with your IPv6 transition, please visit http://www.business.att.com/enterprise/online_campaign/ipv6/.