What's the big deal about IPv6?

A PLAIN-ENGLISH GUIDEBOOK FOR NON-TECHNICAL MANAGERS
WHY SHOULD I CARE ABOUT IPV6?

Your network administrators will tell you that IPv6 is the future of the Internet technology and you’ve got to be ready.

You’ve probably assumed that any shift in technology will cost a zillion dollars and you don’t really see the business case for IPv6 yet.

So let’s put it in simple, non-technical terms:

1. We’re running out of IPv4 addresses

We’re dangerously close to running out of IPv4 addresses—those funny little 32-bit numbers (something like 192.0.2.76) that help bits of information find their way to the right destination on the Web.

IPv4 has only 4 billion addresses. For the whole planet. Easy to see how we’d run out when everybody—and their mama—has a PC, a laptop, a video game console and a smartphone, right?

IPv6 has a whopping 340 undecillion addresses, give or take a few. Imagine 340, then imagine 36 zeroes right after it and you begin to see just how many unique IP addresses that represents.

That means you can grow and keep on growing, adding new customers (and all their connected devices) just as fast as you can.

2. We’re all going to IPv6

As we run out of IPv4 addresses, two things will happen:

First, it will be REALLY difficult to qualify for more IPv4 addresses to assign to your customers, so you won’t be able to grow your business much. Second, service and content providers will begin to use IPv6 addresses for websites and other network services.

So, we may not all go at once and we’ll probably keep IPv4 around for awhile, but we are all going to IPv6.

3. Your customers pay for the whole Internet, so you’d better deliver it

If you don’t deploy IPv6 in your network in some way/shape/form, your customers will have a heck of a time trying to access sites and content that have IPv6 addresses.

See, IPv4 and IPv6 don’t play nice. In fact, they’re not compatible at all. Equipment and software running IPv4 cannot “talk” to equipment or software running IPv6 without some sort of intermediary.

Here’s the bottom line: Your customers pay you for access to the Internet. They expect access to the whole Internet, not just the IPv4 parts of it. If you want to keep those paying customers happy, then your network will have to support IPv6. How do I prepare for IPv6 deployment?

As you begin planning for IPv6 deployment it is critical to consider how all parts of your business will be affected.
HOW DO I PREPARE FOR IPV6 DEPLOYMENT?

As you begin planning for IPv6 deployment it is critical to consider how all parts of your business will be affected.

Core Network

You may have to upgrade or replace certain pieces of equipment in your network, particularly Layer 2 devices like DSLAMs, wireless access points and routers. The best way to figure out which equipment is capable of running IPv6 is to test it by sending IPv6 packets through your normal traffic flows.

Based on those findings, you can work with equipment vendors to determine if upgrades are available, or if replacement is necessary. The long-term goal is to run IPv6 natively across your network, instead of IPv4. In the short-term, your goal should be to implement IPv6 in stages so that you can plan for replacing incompatible equipment as your budget permits.

Residential CPE

Cable networks have the advantage over DSL and fiber networks for IPv6 readiness in CPE devices. DOCSIS 3.0-certified cable modems are capable of receiving a firmware upgrade for IPv6. DOCSIS cable operators have a standard method for upgrading modem firmware, so they’ll have an easier time getting their CPE devices upgraded than telcos.

Almost no DSL or fiber CPE devices are ready for IPv6. And, even if that equipment could be upgraded, most independent telcos haven’t adopted TR-069, so they have no mechanism for a mass automatic upgrade.

As you plan for IPv6 deployment, you’ll need to audit all the CPE devices in your network and determine which ones can be upgraded remotely, which ones will require technician to complete a manual upgrade on-site, and which ones will need to be replaced.

Even if you haven’t adopted TR-069, ask your modem vendors if they can help you with mass automatic upgrades. Their equipment may have a default setting that you can use to run an upgrade, instead of dispatching technicians to those customers or replacing their modems.

Replacing modem equipment gives telcos an opportunity to institute a mass upgrade mechanism. When you order modems, ask the manufacturer to activate TR-069 and set the default URL to a private IP address on your network. Then, the next time you need to upgrade modem firmware on those devices, you can place configuration and upgrade instructions there for the modem to retrieve automatically.

Commercial CPE & Services

You’ll need to audit commercial devices in the same way that you audited residential CPE. Determine if the equipment you’ve deployed can be upgraded or if it needs to be replaced. And, if they haven’t called already, you should expect your commercial customers to start asking you run (tunnel, in tech-speak) IPv6 over their existing IPv4 connection.

Your business customers also have additional internal items to consider, such as preparing their mail servers or Microsoft exchange servers and making arrangements for applications or equipment that require a static IP address.
Business users will look to you to supply an IPv6 connection, but they may also seek your help in implementing IPv6 in their local network. Be ready to answer those questions, or refer them to a network consultant you trust.

Web Hosting

If you provide web hosting services, users with IPv6 addresses will want to access the sites you’re currently hosting in IPv4. You’re going to need to give those sites IPv6 addresses, or implement translation (NAT, in tech-speak).

Other IP Services

If you offer voice or video services over IP, be sure to check with your upstream providers regarding their IPv6 deployment. Ask about timelines and any equipment or software upgrades and then work to plan any changes with minimal service disruptions.

WHAT ARE MY OPTIONS FOR DEPLOYMENT?

There is no line in the sand for IPv6, so adoption will be gradual and we’ll be running IPv4 and IPv6 simultaneously for quite some time. That means you’ll need to move both kinds of traffic across your network. It will also be necessary to translate v4 to v6 and vice versa.

Following are slightly technical descriptions of highly technical deployment methods. This info won’t make you an expert, so use it as a starting point for a discussion with your network engineers (or a consultant, if you prefer) about the best choices for your network and budget. Bear in mind that your network may require the use of more than one deployment method.

Dual Stack

Running a dual stack means that IPv4 and IPv6 are running simultaneously on the same interface. Devices running dual stacks (meaning they have both an IPv4 and an IPv6 address) can send and receive both kinds of packets.

This is the least complex method of deploying IPv6 and works best in transition plans that begin by implementing IPv6 in the core network, then expanding outward to the edge.

Of course, this method only works if you have sufficient IPv4 addresses. So, make sure you’re managing your inventory carefully.

Tunnels

Think of tunnels as a shell formed around an IPv6 packet so that it can pass through an IPv4 connection. Tunnels work in reverse, too, moving IPv4 packets in a shell over an IPv6 connection.
Though they add a layer of complexity to your network, tunnels are a viable option if you need to deploy IPv6 quickly. This may be the case if you’ve got a business customer requesting an IPv6 connection, in which case you’re deploying at the edge first, then moving toward the core of your network.

To configure an IPv6 tunnel over an IPv4 connection for a business customer, for example, you’ll manually configure the routers at either end of the connection with the IPv4 source and destination addresses.

Tunnels can also be configured automatically and require an application to query a server to set up a tunnel, then take it down when the session is complete. While this is certainly more scalable than creating manual tunnels, automatic tunnels can be less secure and, because they are built and discarded on-demand, troubleshooting is more difficult.

Translators

Translation is the most complex method of deployment. Instead of putting an IPv6 packet in an IPv4 shell, like a tunnel, translation actually re-writes the header on one of the packets. This is called NAT, or network address translation, and is sort of like translating an English sentence into a Spanish one before you send it on across the Internet.

Many service providers, particularly telcos, will find that carrier-grade NAT (CGN, also referred to as Large Scale NAT or LSN) is the most viable option for IPv6 deployment. CGN hides the end user addressing behind a NAT middleware device in your network.

While CGN is a viable option for short-term IPv6 deployment, there are drawbacks.

First, management of the network becomes more cumbersome. You’ll have to consider the placement of DNS servers relative to the NAT middleware. IMCP messages (ping, in non-geek speak—it’s one of many tools used to monitor networks) are challenging to translate.

Second, installing NAT middleware creates a single point of failure. If the middleware fails, your customers lose connectivity.

Third, CGN assigns a translated address for the public side of each customer’s home network. Then, each device on that network receives a translated address to use inside the customer’s home network. This means that end user traffic is passing through two layers of NAT architecture, slowing the connection and increasing the chance of translation failure.

Like any IP technology, CGN also faces security, scalability and reliability challenges. Record-keeping for the purposes of compliance with law enforcement regulations also becomes more difficult.
WHAT DO I DO NOW?

Now that you understand why IPv6 is important, it’s time to figure out how you’re going to deploy it.

1. Use this paper as a starting point for a discussion with your network engineers, or a network consultant, if you have one. Enlist their help in applying for an IPv6 allocation and investigating an IPv6 backbone connection.

2. Test the readiness of your network and CPE gear to figure out which pieces may need upgrades or replacement to run IPv6.

3. Determine what training is necessary to prepare your staff to run, secure and support an IPv6 network, in addition to your IPv4 network.

4. Work with your engineers to determine which transition method(s) are best for your network and best address the needs of your customers.

5. Communicate with vendors and customers to coordinate any service changes.

For more information on IPv6, or to request help with testing the readiness of your network, please visit ZCorum.com/ipv6.