Published on *InfoWorld* (http://www.infoworld.com)

IPv6 transition framework for the enterprise

By Brian Heder
Created *2011-06-10 03:54AM*

If all the excitement about IPv6 [1] has finally convinced you to take a serious look at what's involved in the transition, you'll want to start with this framework. After all, transitioning to IPv6 can be daunting given it will affect every networked device on the planet and it is more than just a transition of technology, it's also a transition of people and culture and the way we think.

When you do a Google search trying to find guidance on transitioning to IPv6, you come across all sorts of down-in-the-weeds technical information on IPv6 transition techniques -- think tunnel broker [2], ISATAP, NAT64 [3], CGN [4], dual-stack [5], DS-Lite [6], ALG, NAT-PT, IPv4-mapped addressing, SLAAC [7], etc. These are all important topics, and there is a time and place to consider the technologies, but when you are just beginning to plan your transition, you need a bigger-picture perspective.

[Also on InfoWorld: 8 security considerations for IPv6 deployment [8]. | Also: Your handy IPv6 checklist [9]. | Get your websites up to speed with HTML5 today using the techniques in InfoWorld's HTML5 Deep Dive [10] PDF how-to report. | Learn how to secure your Web browsers in InfoWorld's "Web Browser Security Deep Dive [11]" PDF guide.]

ANALYSIS: World IPv6 Day: Tech industry's most-watched event since Y2K [12]

Whether you are a small nonprofit with a couple employees and a basic website, or a multinational corporation with a globally distributed data center [13] architecture, the framework presented here will help you bring your organization into the 21st century.

Before going any further, let me lay out three basic assumptions I'm making about the reader:

1) You are already convinced (or at least your boss is!) that your organization needs to move toward IPv6 [14]. It is not my intent to make the case for IPv6 transition or even for IPv6 in general.

2) Your organization's ultimate goal is an end-to-end IPv6 computing infrastructure. In other words, though you may rely on temporary transition techniques in the short term (some of which you may already have deployed), you don't want to rely on them forever. After all, eventually the whole world will transition to IPv6 and there will be no more need for IPv4. Now that may not happen for another century or two, but the point is you want a comprehensive plan that covers the entire organization.

3) You can't simply flip the magic IPv6 switch and make the whole world IPv6 at once, so you'll need to make provisions to operate IPv4 and IPv6 side-by-side for the foreseeable future [15]. Think of it as "indefinite coexistence."

The strategy

Every good coach knows you can't win without a strategy, and transitioning to IPv6 requires a two-part strategy that will set the foundation for a successful rollout.

The first part of the strategy is itself divided into two phases:

Phase 1. Customer-facing content. Anything that is exposed to the Internet should be transitioned first. This is especially true for enterprises that rely on the Internet as a means of doing business. As time goes on, more and more IPv6-only clients will be popping up on the Internet as ISPs run out of IPv4 addresses [16]. While any smart ISP will provide some sort of transition mechanism to ensure their IPv6 customers have the ability to access IPv4 content, you cannot rely on this as your only means of reaching those customers. If a particular ISP's transition mechanism doesn't work well with your content, who is the IPv6 customer going to blame? You of course! If your website fails to load properly or in a timely manner [17] in the customer's browser, chances are he will get annoyed and move on to your competitor. Therefore you need to make a priority of getting your Internet-facing content onto the IPv6 Internet.

(As an aside, getting your content on IPv6 isn't as simple as just running dual-stack on your Web server [18]. You most likely have an entire infrastructure that will need to transition prior to sending and receiving IPv6 packets on that server. We will discuss this more later.)

Phase 2. Internal systems. Once your customer-facing content is available to the IPv6 Internet, you can now direct your attention to internal systems. Internal system communications includes anything that doesn't typically leave your organizational boundary, such as system-to-system traffic and management traffic. This phase also includes internal client PCs.

This two-phased approach makes the transition more manageable and is similar to what all Federal agencies are doing (see this OMB mandate from September 2010 [19]). By focusing on customer-facing content first, you can ensure your organization won't lose visibility as more and more IPv6 users come online. The remaining steps in this article will ultimately be performed twice, once for each phase.

Transition areas

The second part of the strategy is really the linchpin of the entire framework: transition areas (TAs). This is where all transition-related activities take place, forming the foundation of your enterprise rollout.

The basic concept behind TAs is to break the enterprise into several functional categories. The exact number of areas may vary from one organization to another, but many will overlap. Some TAs are 100% technical, while others are more people and process oriented.

Here is a sample list of TAs that will apply to most enterprises. Your list may be bigger or smaller depending on your needs.

- communications infrastructure
- servers [18] and operating systems
- IPv6 address space
- tools

- security [20]
- storage [21]
- people and processes

Each TA is assigned a lead (ideally a senior-level SME in his functional area) and a number of contributors. There should be a large number of contributors, for reasons that will become apparent below. For larger or more complex TAs, a multi-level hierarchy may be desirable.

The benefits are numerous:

- Activities are divided into manageable, definable chunks. This is critical because the IPv6 transition touches so many aspects of your organization.
- The work is spread around. The IPv6 transition is too much for any one person. The idea is to use only a small slice of many people's time as opposed to all of a few people's time.
- You might get hit by a bus, so you don't want to be a single point of failure.
- Everyone gets involved. IPv6 is more than just a transition of technology. By getting everyone involved, there is a sense of collective ownership, and everyone starts thinking and learning about IPv6.
- The collective knowledge and skills of a wide variety of people are effectively utilized.
- Nothing gets missed.

The actual activities of the TAs will be outlined next, but before we get to that, one note: When assigning TA leads, be sure the individuals are reliable and excited about IPv6. You will be leaning on them a lot throughout the transition, so choose them carefully.

Reconnaissance

Now that the basic strategy is laid out, and the TA team structure is in place, it's time to get to work.

Before you can "flip the switch" and start running IPv6, you first need to assess the IPv6 readiness of your systems. Therefore the first task for your TA teams will be a reconnaissance mission. The TA leads will define a list of all the components within the scope of their TA, and assign one information gathering worksheet per component to a TA team contributor.

QUIZ: How prepared are you for IPv6? [22]

What exactly defines a "component" may differ depending on the TA, but a component should be a measurable, definable unit. For example, if one of your TAs is Communications Infrastructure, a component could be a particular router [23] (for example, a Cisco [24] ASR 1013, or a Juniper MX480). If one of your TAs is Processes, a unit might be one process (for example, a subnet request process).

For the technical TAs, components can typically be broken down into two types:

1) Box-level components: typically a physical or virtual device with CPU and memory resources. These should be assigned to more junior-level contributors, as they are typically simpler and more straightforward. Examples: a particular router, a physical or virtual server, etc.

2) System-level components: a protocol or application that abstracts the underlining hardware on which it

runs. These should be assigned to more senior-level contributors, as they can be quite complex. Examples: a routing architecture, a network or server monitoring solution, etc.

Defining scope

During the first phase of the transition (Internet-facing content), it is important for you to clearly define the scope of the information gathering exercise to your TA leads, and likewise for your TA leads to clearly define the scope to the contributors on their teams. As contributors fill out their worksheets, they will more than likely run into gray areas in the scope definition ("Is this component in scope or not?").

BY THE NUMBERS: Lack of IPv6 traffic stats makes judging progress difficult [25]

It is important to have an open line of communication between the contributors and their TA lead, and likewise between the TA leads and you. You will undoubtedly run into scope questions that will force you to draw a line in the sand as a particular component may not clearly fall in or out of scope.

Don't bite off more than you can chew in the first transition phase. Rather, just focus on the minimal subset of components needed to meet your Phase 1 goal. Everything else can be addressed during the second phase, after you already have a successful first phase transition under your belt.

Once all the worksheets are completed and turned in, you can use them to paint a picture of IPv6 readiness across the enterprise, and to reveal exactly what you will need to do to execute the rollout. This picture is critical in the next step of your IPv6 rollout.

If your organization is like most, you will probably be pleasantly surprised to find that many of your components are ready to support IPv6 with only minor changes, and that very little (if any) capital expenditure will be required. The main reason for this is the fact that vendors have been rolling out support for IPv6 [26] for the past 10 years or so, and most organizations will have already been incorporating this support over the past few cycles.

With IPv6 readiness fully assessed, you are now equipped to dive in and begin planning and executing the rollout.

Plan and execute

It is now time for the fun part: planning and executing your transition. In this task, you will use the information gathered to develop a step-by-step plan for making the transition happen. There is nothing magical or mysterious about this step. Like any other project, proper management and organization are going to be keys to success.

The first thing to do is to sit down with your TA leads, either as a group or individually, and create a complete list of all the steps necessary to enable IPv6 in the various parts of the enterprise as revealed in the component worksheets. With all the steps listed, start identifying dependencies and milestones, and begin to develop a timeline. You may be thinking, "This seems a lot like Project Management 101," and you would be absolutely right! There is nothing magical or mysterious about this step.

You will come to rely even more heavily on your TA leads and TA contributors as you plan and execute the transition. They will be responsible for coming up with the configurations and actually enabling IPv6 across the enterprise. Use the same people who filled out the reconnaissance worksheets to build and implement the required changes.

What follows is essentially a list, in no particular order, of lessons learned and key things to watch out for as you plan and execute the transition:

- Identify any requirement that may need capital funding up front. This may be hardware or software

upgrades, training, or new systems. Where upgrades are necessary, if you can get capital funding, plan for native IPv6. If you can't get capital funding, you may have to come up with another plan for that component, such as an alternate transition mechanism (for example, tunneling or translation).

● Lab and/or prototype testing should be performed whenever possible. Begin lining up the resources early, such as lab space, vendor demo gear, etc.

● Coming up with an IPv6 addressing scheme [7] is one of the most important of all your efforts. When else do you get a second chance to correct all the mistakes made with your IPv4 addressing plan? Rather than just doling out subnets sequentially, you should think through the implications and come up with a plan that will be flexible enough to take your enterprise into the foreseeable future and beyond. Perhaps you only have two or three sites, but what will your organization look like in 50 years? Perhaps now your organization is limited to one geographic territory, but who knows what will happen in 50 years? The point is, before you begin throwing IPv6 space at your network, come up with the overarching principles that will guide all your IPv6 assignments.

● Prior to acquiring IPv6 address space from a service provider [27], be sure you understand the differences between provider independent (PI) and provider assigned (PA) address space. This concept is fundamentally new in IPv6, so be sure you understand all the implications of which type you acquire.

● I recently read [28] that nearly half of all organizations track IPv4 space manually. This is clearly unsustainable in IPv6. If you do not have an IPAM (IP address management) [29] solution deployed, now is the time to find one. If you do have an IPAM, IPv6 readiness should have been assessed during the reconnaissance task described.

● Don't forget the WAN [30]. You need to understand your options for connecting to the IPv6 Internet. Different service providers offer different options, so be sure to consider them all. Sadly, many service providers do not yet have IPv6 connections available for customers yet. In this case, you may want to consider finding another provider, or alternately using a tunnel broker.

● Don't overlook your tools. One of the weakest links right now in terms of vendor IPv6 support is in the category of tools. This includes network node management, packet capture and analysis, server management, SNMP management, IDS/IPS solutions, etc. Be sure to focus early in the game on enabling IPv6 on your tools wherever possible.

● Pay special attention to anything that is fundamentally different between IPv6 and IPv4 [31]. You may want to instruct your TA leads and contributors to make a list of these items as they learn more about IPv6. I already mentioned the PI vs. PA address space issue as one fundamental difference. A few others include: EUI-64 addressing, stateless auto configuration, ARP replaced by neighbor discovery, no more broadcast, no more fragmentation by intermediate devices, and all subnets are /64s. These are just a few of the things that make IPv6 different than IPv4.

● IPv6 support among vendors is not nearly as mature as IPv4. Because of this, there may be bumps along the road as IPv6 is rolled out, so be sure expectations are properly set.

● Don't forget the need to properly train your staff. This is especially critical for the operations folks who will be working with IPv6 on a day-to-day basis.

● Lather, rinse, repeat. Don't forget that the steps in this chapter and the previous are meant to be performed twice, once for each phase of the transition as described in Chapter 2.

Much more can be said about IPv6 transitions, but the intent of this article is to help you see the forest through the trees. As the IPv6 transition lead, you need to stay out of the weeds so you can help guide

everyone else through the sometimes difficult-to-navigate terrain that is IPv6.

Though IPv6 has been around for a while, it is still considered a new technology. In many cases vendor support for IPv6 is not as mature as it is for IPv4. However, enough organizations have made the transition to demonstrate that IPv6 is ready to begin replacing IPv4 as the dominant protocol on the Internet. Though there may be some bumps along the road to IPv6, with a solid strategy and proper planning, your organization can make a successful transition into this new era.

Heder, CCIE No. 24788, is a senior network engineer specializing in large-scale enterprise and data center network design for the Department of Defense, as well as organizationwide IPv6 transitions. Heder holds a master's degree with a concentration in network architecture and design, and has a patent filed for an IPv6 transition technology. He can be reached at brian.heder@gmail.com [32].

Read more about LAN and WAN [30] in Network World's LAN & WAN section.

Networking Internet IPv6

Links:
[1] http://www.networkworld.com/news/2009/073009-ipv6-guide.html
[2] http://www.networkworld.com/news/2010/050610-ipv6-tunnel-basics.html
[3] http://www.networkworld.com/community/blog/testing-nat64-and-dns64
[4] http://www.networkworld.com/community/node/44989
[5] http://www.networkworld.com/community/node/42436
[6] http://www.networkworld.com/community/node/46600
[7] http://www.networkworld.com/community/blog/ipv6-address-design
[8] http://www.infoworld.com/d/security/8-security-considerations-ipv6-deployment-902?source=fssr
[9] http://www.infoworld.com/d/data-explosion/your-handy-ipv6-checklist-232?source=fssr
[10] http://www.infoworld.com/d/mobilize/best-laptop-money-cant-buy-496?source=fssr
[11] http://www.infoworld.com/d/security-central/the-infoworld-expert-guide-web-browser-security-892?isource=ifwelg_fssr
[12] http://www.networkworld.com/news/2011/060711-ipv6-expect.html
[13] http://www.networkworld.com/topics/data-center.html
[14] http://www.networkworld.com/news/tech/2011/012511-enterprise-ipv6-address-planning.html
[15] http://www.networkworld.com/news/2011/013111-as-ipv4-disappears-transition-poses.html
[16] http://www.networkworld.com/news/2011/041411-apnic-ipv4-gone.html
[17] http://www.networkworld.com/news/2011/060711-ipv6-problems.html
[18] http://www.networkworld.com/topics/server.html
[19] http://www.cio.gov/documents/IPv6MemoFINAL.pdf
[20] http://www.networkworld.com/topics/security.html
[21] http://www.networkworld.com/topics/network-storage.html
[22] http://www.networkworld.com/slideshows/2011/011411-ipv6-quiz.html
[23] http://www.networkworld.com/news/2009/120909-network-router-cheat-sheet.html?ts0hb&story=rtrcheat
[24] http://www.networkworld.com/subnets/cisco/
[25] http://www.networkworld.com/news/2011/052411-ipv6-traffic.html
[26] http://www.networkworld.com/news/2007/060707-8-mgmt-vendors-ipv6.html
[27] http://www.networkworld.com/news/tech/2008/030508-tech-update.html
[28] http://www.businesswire.com/news/home/20110606005403/en/Survey-Enterprises-Ready-IPv6-Transition
[29] http://www.networkworld.com/reviews/2007/120307-ip-address-management-test.html
[30] http://www.networkworld.com/topics/lan-wan.html
[31] http://www.networkworld.com/news/2007/102607-arguments-ipv4-ipv6.html
[32] mailto:brian.heder@gmail.com