Building an Enterprise IPv6 Test Lab

ReadWriteWeb

BY JEFF CARRELL AND ED TITTEL

SPONSORED BY

CenturyLink™ Business

According to recent studies of IPv6 market penetration and use, somewhere between 25% and 33% of enterprises are doing "something" with IPv6. It's not always clear what this really means. Even on World IPv6 Day, native IPv6 usage didn't surpass 1.5% of overall traffic at its highest peaks (though it did briefly cross 4% if you include IPv4 tunneling protocols for IPv6 such as Teredo and 6in4), as shown in Figure 1. Clearly, the Internet has a long way to go before IPv6 comprises a substantial portion of Internet traffic.

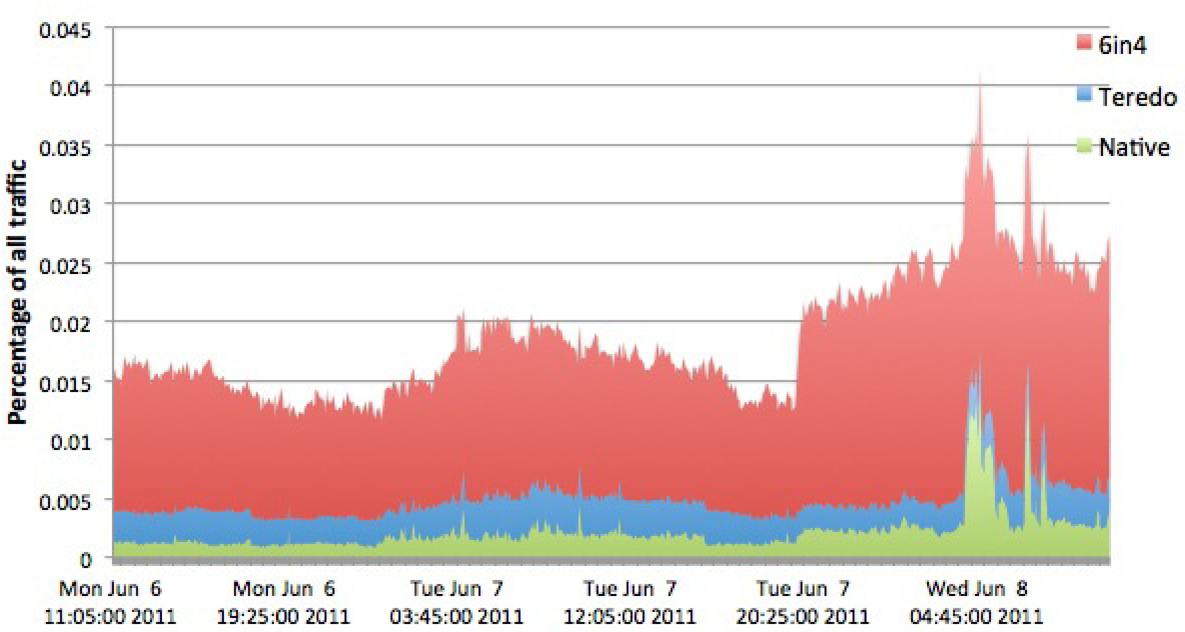

Figure 1: IPv6 Traffic leading up to World IPv6 Day (Source "The World IPv6 Day Report Card," courtesy of Arbor Networks)

WHY A TEST LAB IS NEEDED FOR IPV6

Recent studies indicate that while as many as one-third of organizations are using IPv6 in at least some limited kind of way, up to 85% of all organizations plan to roll out IPv6 before the end of 2013. Given that many business networks will be starting from scratch, and have a substantial learning curve to climb along the way, we believe that these timelines could easily stretch into 2014 or even further out.

We strongly recommend that an early step on the way to IPv6 investigation, migration assessment and planning, pilot testing and deployment must include the design, installation, configuration and use of an IPv6 test lab. A test lab provides an ideal learning and experimentation environment, because, if properly designed, mistakes or misconfigurations will produce much-needed experience without wreaking havoc on users, production networks or Internet access.

The purposes of an IPv6 test lab are as follows:

- **To select and test network components for IPv6 compatibility**, while maintaining IPv4 addresses, mechanisms, services and configurations intact
- **To train IT staff** in installing, configuring, and maintaining IPv6 connectivity alongside IPv4, ultimately for production use
- **To document and specify device or component upgrades** or replacement operations to add IPv6 connectivity to existing IPv4 networks
- **To provide a forward-looking learning and experimentation environment** where new devices, appliances, services and network infrastructure components can be tested and documented outside production environments

In our case, we are not only revising a book to include substantial Wireshark-based protocol traces of IPv6 protocols and services (see the Guide to TCP/IP), we also teach hands-on lab courses at IPv6 SIG meetings, Sharkfest, gogoNET Live! and other gatherings. Because we are on a pretty stringent budget, and have access to surplus equipment from HP and Dell, we were able to put our current test lab configuration together for under $50,000. Were all of its components to be purchased at rock-bottom prices on-line, the whole shebang could still be assembled for under $100,000 (not including software licenses, which likely double both numbers, nor the MRV box mentioned elsewhere here).

Part 1: Choosing IPv6 infrastructure elements

When it comes to setting up an IPv6 test lab, numerous elements require investigation for IPv6 compatibility. Though this article will address some typical devices and network infrastructure components, any test lab you design must match (or exceed) current IPv4 capabilities to be both usable and workable. While you're redesigning a network to add IPv6 capability, it never hurts to keep asking (and answering) questions such as "What could we do better or differently?" "What kinds of consolidation, upgrade or improvements can we enact?" or "What other tools and technologies could we use to improve network efficiency, throughput, bandwidth or user experience metrics?"

Table 1 provides a summary of the most typical devices and network components that must accommodate IPv6 to ensure a smooth and workable upgrade, with no interruption or degradation of user services and experiences. And for your own test lab, you'll want to include all infrastructure and boundary elements that must handle IPv6, including security and other appliances, remote access devices or software, WAN optimization and load-balancing appliances, network management consoles, servers and clients. Please note that representative virtual machines or real end-user client platforms play an important role in an IPv6 test lab, as well as networking components and network servers and services.

Table 1: Typical IPv6 Test Lab Components Model Production Environments

Item	Category	Notes/Remarks
Router	Network infrastructure	Most routers built after 2004 only need firmware/sw upgrades
Switch (Layer 2)	Network infrastructure	Used to set up and manage IPv6 VLANs, collapsed VLANs, etc.
Switch (Layer 3)	Network infrastructure	Used to set up and manage IPv6 VLANs, collapsed VLANs, etc.
Firewall	Network infrastructure	Careful checks for compatibility and features required, new rules or policies must be defined
Security and other appliances	Network infrastructure	Careful checks for compatibility and features required
Remote access	Network infrastructure	Testing of IPv6 native and tunneled protocols required
WAN optimization and load-balancing appliances	Network infrastructure	Careful checks for compatibility and features required
Network consoles	Network management	Compatibility, metrics, configuration, and display changes inevitable
Servers	Network services	Installation and configuration of new IPv6 services necessary for all server OSes and versions in production use
Clients	Network users and access	Test native and tunneled IPv6 addressing, connectivity, services for all client platforms and OS versions in production use

Figure 2 shows our IPv6 test lab layout. It's configured so that in/out links in the Hands-On Lab and Author Lab areas may be used to install, configure and test virtual (software-based) Fortinet FortiGate firewalls/appliances. Also, students can establish and check their work in setting up switches and firewalls for IPv6 use. We run a separate lab for router configuration (using virtual router software) and make virtual clients and servers available as well.

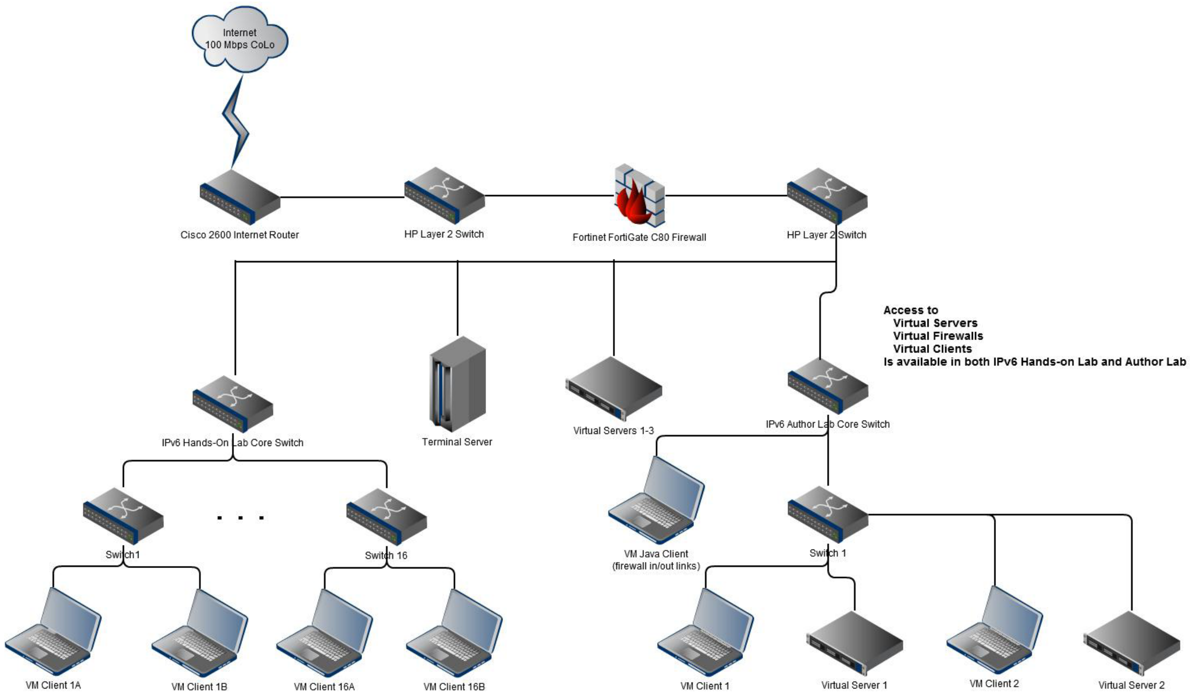

Figure 2: A sample IPv6 test lab layout

Some interesting learning in setting up the physical lab at Hurricane Electric came from figuring out when to route patch cables from interior switches in the Hands-On Lab (used for teaching students in our classes) and the Author Lab (which we use to capture protocol traces for our book project) to Layer 2 switches on either side of the firewall. This allows us to set up both inbound and outbound connections to test configurations to make sure they are working properly and as expected.

In addition, we use virtual router and firewall software — namely the Vyatta Open Source Virtual Router and Fortinet's FortiGate virtual firewall/security appliance — to permit students and authors alike to set up complete, end-to-end Internet-facing or internal network configurations. There's no doubt that virtualization not only makes test lab set-ups easier and more flexible, but also exerts significant cost controls as well. When working with virtualized components, it's important that interface and configuration details be identical to the production components that will ultimately be used, and that changes to step-by-step instructions and how-to's be carefully documented to take note of such differences. (See Table 2 for a list of what equipment our own test lab contains.)

In our case, we decided to put our IPv6 Test Lab at Hurricane Electric in Fremont, California. Because we wanted to provide native IPv6 access to the lab, with fast Internet access, and to use IPv6 throughout, we had to choose among a relative handful of providers and locations in the United States where we could obtain native IPv6 service, lease rack space in a well-run datacenter and keep costs to a minimum. Though our monthly costs average under $1,000 for connectivity and rack space, we were pleased to obtain a tolerable monthly rate from a leading provider of IPv6 Internet access and services.

As a final concluding note to this section, it's absolutely essential that infrastructure components work well when IPv6 is turned on, and that their set-up and configuration be well-documented, and demonstrably repeatable so that IT professionals can learn what they must to prepare for future production roll-outs. Even though a device or component might work with IPv6, those that require jumping through lots of hoops or involve long, drawn out set-up and configuration maneuvers might be better off retired and replaced with newer or more capable replacements that are easier to work with. Though capital budgets will exert profound control over some such choices, management must also understand that time and effort have their costs as well, and may need to be factored into planning and deployment along with acquisition costs. Over time, there is no doubt that upkeep and maintenance, particularly personnel-related expenses, dwarf purchase costs.

Table 2: Devices Used in the IPv6TestLabs Data Racks

Vendor	Model	Qty	Description	IPv6 Characteristics and Set-up
HP	E3500	3	20-port GbE switch	Enable IPv6 (dual-stack), set up IPv6 VLANs, use RIP
HP	E4800	10	44-port GbE switch	Enable IPv6 (dual-stack), set up IPv6 VLANs, use RIP
HP	ProLiant G5 DL380 Server	1	2x Xeon 5160, 16 GB RAM, 280 GB HD	Enable and configure IPv6 for DNS, Exchange, VMware ESXi 4.1
Cisco	C2561XM	1	24-port Layer 3 switch (acts as terminal srvr)	Enable IPv6 (dual-stack), set up IPv6 VLANs, use RIP
Cisco	WS-CS3560 WS-3750	2 3	48-port Layer 3 switch 48-port Layer 3 switch	Enable IPv6 (dual-stack), set up IPv6 VLANs, use RIP
Cisco	2621XM	1	Edge router	Flash IOS to 12.3 or higher, enable IPv6 (dual stack), define IPv6 routes: boundary/internal
Fortinet	FortiGate C80	1.p 8.v	Firewall/security appliance	Enable IPv6 (automatic dual-stack), set up DHCPv6, configure DNSv6, establish IPv6 protocol filters (DHCP, DNS, HTTP/S, SFTP, Remote Access, etc.)

Notes:

1. Student lab stations get primarily 20-port switches, backbone and author stations get primarily 44-port switches, wiring is flexible but requires manual recabling for configuration changes (the MRV will make this unnecessary).
2. The lab features a single physical FortiGate C80 at the network boundary, but makes virtual versions available for both student and author stations (up to eight may be in simultaneous use).
3. Cisco switches are sometimes available to students (24-port models) but the 48-port model is reserved for lab backbone use only.
4. We plan to add two more servers like those listed to provide more virtual client and server access to users for more advanced uses.

Part 2: Configuring IPv6 services

Beyond setting up and configuring physical or virtual devices for IPv6, it's also important to get comfortable with installing, configuring and maintaining various IPv6 services on an organization's networks. When we teach our IPv6 Hands-On Lab classes, we emphasize installation, set-up and configuration (or turning on IPv6 and making necessary configuration changes, as is often the case with many modern applications and services) for:

- **Domain Name Services**: set-up and configuration to add IPv6 support to DNS on Windows Server 2008 and 2008 R2 (other platforms covered on a case-by-case basis)
- **Microsoft Exchange Server**: set-up and configuration for IPv6 email transfer and forwarding
- **Web servers**: set up and configuration for IPv6 on Internet Information Services (IIS) versions 7.0 and 7.5

Basic testing and access to these services (or to the data or content they provide) is essential to make sure things are working properly. In some of our hands-on labs, we observe that students are as interested in good testing techniques as they are in set-up and configuration details. There's no doubt that careful, patient testing has to be part of what the test lab is used to teach and do, and that such skills and knowledge must also be rolled out for any pending IPv6 production deployments as well.

Beyond the basics, organizations will want to make an audit of the IP services and protocols they use to see what must be updated, upgraded or replaced to add IPv6 compatibility, and what remains stuck at IPv4-only network service levels. Fortunately, companies like Datatek make black boxes like their Transformer product) that provide protocol translation from IPv4 (inside the black box) to IPv6 (from outside the black box), so that IPv6 clients remain able to access protocols and services for which no other direct migration or upgrade path is available.

Once the audit has been conducted, virtual servers in the test lab should be created so that necessary services and related protocols can be installed, then set up and configured for access using IPv6. This is bound to be a time-consuming and learning-intensive proposition. Some organizations that have large application and service portfolios and are starting an IPv6 network from scratch might find this process longer and more drawn out than they initially expected they would be. The end result should be well-documented set-up and configuration information, with step-by-step instructions on how to proceed, what inputs or settings to create, and how to troubleshoot the inevitable gotchas that are bound to pop up along the way.

Part 3: Implementing remote access

Larger organizations may operate multiple data centers, and will have to decide if they want to build more than one IPv6 test lab. But medium and smaller organizations will seldom be inclined to consider multiple labs. We designed our lab for remote access from the get-go, and suspect that most organizations will find this appealing, given that the number of sites (and locations from which IT staff work) usually exceed the number of data centers available by a pretty wide margin.

To some extent, the rising tide of virtualization for most aspects of IT will soften the unsatisfied desire for hands-on access to physical hardware for those who work in or with the test lab. It can be frustrating to work remotely for IT professionals used to getting down and dirty with the devices they operate. Indeed, there will be some situations where data center or collocation staff must interact directly with hardware. But IT professionals must also get used to doing and managing things remotely, not only because it's a good way to bring widely dispersed staff together with resources they must manage, but also because that's the way the entire IT industry is trending nowadays.

That is why we want to recommend one particular piece of hardware you don't see in Figure 2 (we're in the process of acquiring one used and won't be installing it for another three to six months because of timing and cost issues). It's called a physical layer 1 switch, made by MRV Communications in Chelmsford, MA. This device permits users to connect any port on the switch to any other port using a non-blocking matrix through software controls (which means it works as well remotely as it does locally). Because you never know how you want to chain devices together in a test lab, this switch offers the ultimate in any-to-any connectivity. While such devices are expensive (for 96 ports and with 10 Gbps or 40 Gbps interconnects, it's easy to spend over $100,000 on this box alone), they can turn troublesome recabling operations into quick, easy software reconfigurations. Given that investigating new technologies means you can't possibly foresee all the device interconnections you might want to make in your lab, this box is a godsend.

Part 4: Finishing touches and debugging

When it came to getting our own test lab up and running, we did hit some interesting snags. We ran into a strange external ground issue for a Cisco Async Card cable that wouldn't talk to our firewall until we broke the external ground connection (and only interminable trial-and-error helped us find and fix this problem). We also discovered that our Java-based VPN Web client wouldn't work on Macintosh Safari but worked fine with Firefox. It also worked perfectly with Safari on the iPhone, and with all major browsers on Windows and Linux client machines.

But once we got the bugs shaken out, we have been able to access and run IPv6 networking tools and services on our test networks, and teach others how to do likewise. The most interesting part has been working through the various services we must also make sure work properly with IPv6, especially when (as is far too often the case) set-up and configuration values and settings are not well documented. But that's what makes our work so important, and why organizations must go through the same motions before they can take IPv6 onto production networks.

Ed Tittel and Jeff Carrell are longtime computing industry veterans, former Novell employees and co-authors, with Laura Chappell, of a college textbook entitled "Guide To TCP/IP." Jeff develops and delivers training on HP network switches and routers, and teaches hands-on IPv6 labs for Sharkfest and all kinds of IPv6 task forces and organizations. Ed makes his living as a freelance writer and researcher. Together, they operate IPv6HoL.com, an IPv6 portal that includes a virtual IPv6 training lab, IPv6 content and information and pointers to most imaginable kinds of IPv6 resources.