



How To Prepare for IPv6 Networking

ReadWriteWeb

BY ED TITTEL AND JEFF CARRELL

SPONSORED BY



CenturyLinkTM
Business

Case Study: A Sample SMB IPv6 Set-up Scenario

Without going into all of the details involved in set-up and configuration, let's review a recent case in point in converting a small company from IPv4 only to dual-stack IPv4/IPv6 networking and show you how it was done and the time and issues dealt with along the way. We consider a network that enabled Windows 7 clients to run in dual-stack mode, with IPv6 used when available, and IPv4 otherwise. Total expenditures involved were around \$2,000 to replace an older (Rev A) D-Link DIR-655 combo device (firewall, single WAN port, 4-port GbE switch, and wireless access point with RevA3 firmware) with a Fortinet Fortigate 80C device (firewall, gateway, 6-port GbE switch, dual WAN ports with comprehensive and complete IPv6 support).

STEP 1: SOLVE THE ISP BARRIER (ONE HOUR)

Because local native IPv6 ISP service was not available from the company's chosen ISP, a tunnel-based approach was set up with well-known IPv6 service provider Hurricane Electric (HE) as part of the overall solution. HE offers a free [IPv6 Tunnel Broker](#) solution that support native IPv6 Internet access by tunneling over IPv4 connections through a non-native IPv6 ISP from an in-house IPv6 enabled host computer or boundary device to an HE IPv6 router.

Though tunneling does impose a performance impact, HE routers are extremely fast and efficient. And because the company peers with major backbone providers at its datacenters, we didn't notice any perceptible slowdowns when comparing Internet interactions with dual-stack services for IPv6 as compared to using IPv4 instead. So far, users at the company have noticed no change in Internet behavior or performance, even though they're using IPv6 for up to 35% of their network communications, according to our traffic analyses.

STEP 2: MAKE THE NETWORK IPV6-READY (THREE HOURS)

Once we replaced the D-Link boundary device with the Fortinet Fortigate 80C, we simply had to enable IPv6 on that device, and set up protocol filters for HTTP/HTTPS, SMTP, POP3, remote access, and ICMP, then set up the HE tunnel broker. We were immediately able to use IPv6 on devices attached directly to the Fortinet box through one of the switch ports. The total time and effort involved was under two hours, including a mix of GUI/Web and command-line-based setup and configuration activities on the Fortinet device.

The next step was to configure our HP/3COM Layer 3 switches to support IPv6 VLANs to set up the switched equivalent of subnets on these devices.

STEP 3: CREATING AN IPV6 FRIENDLY ENVIRONMENT (ONE HOUR-PLUS)

Configuring the HE tunnel broker automatically handled the DNS issue: we simply linked to HE's DNS servers which run dual-stack and resolve IPv4 and IPv6 name resolution requests. In other cases, we've found that configuring Microsoft or BIND DNS for IPv6 takes some study and preparation, but that the actual activity usually takes less than 15 minutes to complete. The first time can be challenging but it gets progressively easier after that.

The Fortinet Fortigate 80C includes a simple DHCPv6 server as part of its IPv6 configuration options. We needed only to provide it with a suitable address range for assignment, and to note static address assignments for servers, routers, switches, and so forth, and address management was good to go.

Finally, we also modified an Exchange Server 2010 to enable IPv6 support. All of the IPv6 related issues and details are completely explained and illustrated in the TechNet article [Understanding IPv6 Support in Exchange 2010](#) so this proved relatively easy and straightforward. IIS 7 supports IPv6 as-is, so unless you've turned off IPv6 features on the servers on which it runs, though it is necessary to download FTP for IIS 7.0 if you want to support IPv6 FTP connections for IIS (see this [SoftLayer forum post](#) for details). Depending on your installation, this could take an hour or more.