Enabling IPv6 on a Mail Server

You need to think through all the interactions before enabling IPv6 on a mail server.

Ket Crispin posted this to the IETF list:

> I was presenting what I thought was an interesting example
> of a subtle problem that can come up in ipv6 deployment.
>
> The mailserver in question uses a default redhat enterprise
> build (actually centos). ipv6 is either enabled by default,
> or just has a single check box, with no further information.
> The fact that ipv6 is enabled so trivially carries the implication
> that just enabling ipv6 won't actually damage anything.
>
> Now I know different. Just enabling ipv6 on an otherwise
> correctly configured and functioning ipv4 box **will** cause
> damage – it will cause mail that would have been delivered
> to not be delivered. I could be wrong, but this strikes me
> as a trap that lots of people could fall into.
>
> As I mentioned, my servers actually do reject mail if they
> can't find a reverse dns for the senders IP. Some of those
> servers use ipv6; in light of all this I'm going to have
> to rethink that decision. For a server, the combination of
> enabling ipv6 and using this particular anti-spam technique may
> drastically increase the number of false positives – especially
> as ipv6 gets more widely deployed.

Paul Warren adds:

Google mail servers reject mail with no IPv6 reverse DNS. This means that a) if you adopt this measure then you're in good company, and b) if you enable IPv6 on your mail server, then it's very important that you have working IPv6 reverse DNS.

When enabling IPv6 on a mail server, you need to consider all the places where you might have IP-based access restrictions in place, as even if you don't modify add any AAAA records to point at your server, it will start using IPv6 for outgoing connections. One place to consider is SPF records for any domains for which your server sends mail.