http://www.cbronline.com/blogs/cbr-rolling-blog/ipv6-top-10-tips-for-cios

IPv6: Top 10 tips for CIOs

CBR Rolling Blog

CBR Staff WriterPublished 08 June 2011

In this guest blog published exclusively on CBR, Nicolas Fischbach, director network strategy and architecture, Colt, offers some hints and tips for CIOs worried about IPv6 migration

Today is World IPv6 Day, organised The Internet Society (ISOC) and backed by tech giants such as Google and Facebook. It is designed to raise awareness of the switch from IPv4 to IPv6. Here *Colt*'s director network strategy and architecture, **Nicolas Fischbach** offers his guidance to CIOs worried about the new protocol:

1. **Be prepared**: the sky isn't falling, but if you have not yet started to plan for IPv6 you had better start soon. 2011 is the year when most businesses will need to do at least some research, planning and budgeting for IPv6. How quickly you need to execute will mostly depend on the nature of your business and which region of the world you serve. Those doing business on the Internet or running their own public infrastructure will have to act sooner than those who mostly only consume Internet services.
2. **It's not like Y2K, there is no D-day**: there won't be a switchover day nor a specific deadline to meet to support IPv6 which makes planning (and the business case) more difficult. But a number of things are already clear: there are only a limited amount of IPv4 addresses available - this varies between a matter of months and a matter of years, dependant on in which part of the world you are based; and IPv4 and IPv6 will coexist for many years.
3. **Train your staff**: IPv6 isn't just a simple address format change, it's a new protocol suite that has wider implications than just the network. Make sure people on your payroll who deal with networks, systems, applications development and security are fully trained. And prepare your support staff as well, as your users will encounter IPv6 related issues at some point sooner or later. Even if you don't deploy IPv6 now, others on the Internet are.
4. **Is it time for an infrastructure review?** IPv6 will introduce a new numbering scheme to your network, and may be a good opportunity to finally get rid of some of the older legacy equipment or refresh part of your IT infrastructure. Why not use this chance to start again afresh, even if only in some segments of the network such as the external facing environment?
5. **IPv6 will be driven by consumer demand**: Most CIOs and subsequently CISOs have learned the hard way that users drive IT and not the other way around anymore. Most recent mobile devices come equipped with some sort of IPv6 support and as such, IPv6 traffic is likely to grow by itself on your LAN even if you don't "officially" deploy and support IPv6 yet. It is important to make sure you have the right tools in place to visualise and enforce traffic on your network or you risk ending up with an unmanaged internal overlay network that puts your data at risk.
6. **IPv6 isn't more or less secure than IPv4, it's how your organisation handles security which matters most**: as a rule, security policies should be protocol agnostic and you should apply similar rules to IPv4 and IPv6 traffic. Of course, we will see vulnerabilities in IPv6 implementations, and some of those will remind us of good old IPv4 bugs. But on the whole, the security capabilities aren't changing radically, even in the LAN where the mode of operation has changed the most. There is a common misconception that because IPv6 supports IPsec natively all communications will be encrypted, but this is not the case.
7. **Do a proper technology assessment**: feature parity between IPv4 and IPv6, as well as the performance of devices, still varies greatly. You might be looking at a serious impact on performance if you don't validate technology properly.
8. **It's not all about cloud and virtualisation**: while various "as a Service" offerings rightly sit at the top of the priority list for most CIOs at the moment, you shouldn't forget that the network is an enabler, and if you want your applications to perform you need to adequately invest in your infrastructure at all levels.

9. **Work with your Service Provider**: Obviously, the majority of businesses will depend on their Service Provider to deliver native IPv6 connectivity. This could be a great opportunity to work closely together and build on their experience rolling out IPv6 across their own infrastructure.
10. **An opportunity to say thank you? Finally, we come to every company's most important asset**: your employees. Throughout my career I've managed a number of engineering and operation teams and there's nothing more rewarding than a simple 'thank you' coming from your CIO. The upcoming IPv6 introduction project you are going to kick-off might be the right opportunity to show the team some gratitude.

CBR has already taken a look at what various industry experts have to say on the matter. You can read that post here.

Comments

Post a comment

Comments may be moderated for spam, obscenities or defamation.

-
- Disqus
  - Login
  - About Disqus
- Like
- Dislike
-

F5 Networks EMEA 3 weeks ago

- Good tips and we would really emphasise the importance of the first point about preparation. Companies would do well to remember that preparing now is not only likely to be much less costly, but it will also make any retraining easier for the workforce.

The changeover from IPv4 to IPv6 will affect everyone, but smaller businesses who outsource their IT may not notice the difference. Network providers will take care of the transition for hosted services such as email and instant messaging, making sure that equipment is IPv6-compatible.

However, for larger enterprises or rapidly growing businesses the conversion could be more complicated. It’s long been lamented that IPv6 is not backwards compatible with IPv4 – essentially, they can’t ‘talk’ to each other. Although this does seem like a glaring error; particularly since the two networks will need to run in parallel for a number of years. However, this does mean that larger organisations will need to put measures in place to integrate the two networks, and take care to correctly secure networks.