“12 Steps to Enable IPv6 in an ISP Network”

This document isn’t intended to be a comprehensive and detailed technical digest of how to deploy IPv6 in an ISP network that currently has IPv4, but rather an executive summary of the 12 fundamental steps, not including services (DNS, web, email, etc.), for native IPv6 support and the maintenance of IPv4 as a transparent service.

1. How many customers (home+corporate) your network has and what is the expected growth in the short/medium term? If the total is smaller than 50.000 customers, we recommend you to request a /32 to APNIC, /31 if you have up to 100.000 customers, /30 for up to 200.000 customers, and so on. If you already got a /32 and have more than 50.000 customers, you can request an upgrade of your actual prefix. To request your IPv6 prefix, visit Get IPv6.

2. Audit your network, as you need to know what equipment has the right IPv6 support, what need to be updated or replaced. Is important to have a detailed inventory, from your upstream connections to the customers CPEs. If your vendors don’t provide the right support, you should push them. Generally, the market is big and free …

3. Get a professional training with companies that have a demonstrated experience in IPv6 deployment in ISPs. IPv6 is not more difficult, but IPv4 and IPv6 are different and the difficulty may be “changing your mindset”: It is necessary to “unlearn” IPv4 to correctly understand IPv6. Possibly will be convenient that you agree on a consultancy service together with the training. It may seem excessive, however, you will save a lot of time, as the transition to IPv6 will become more important and urgent and that time will cost much more in terms of business losses and problems with IPv4 than the cost of that training and consultancy.

4. Confirm with your upstream providers that they have IPv6 support and enable it in your BGP with them. Same for CDNs, caches and IXs. If the actual upstream providers don’t have IPv6 support, you really need to look for better partners. This part of your network must be dual-stack. In the worst case, if there is no way to get dual-stack from one or several of your upstreams, you may need to use a tunnel, typically by means of 6in4 (protocol 41, manually configured) or GRE, but you should consider this only as a temporary bypass.

5. Review your security policies. They should be equivalent to what you apply with IPv4, but remember that you should not filter ICMP with IPv6, among other related details that will avoid the correct flow of traffic across your network. Review also the IPv6 prefix filtering in your BGP peers; again, those are policies conceptually equivalent to what you already know for IPv4, but with a different protocol.

6. Configure IPv6 support in all your monitoring systems. IPv6 has the same importance as IPv4, so any system that allows, either from inside or outside your network, view the traffic quality, quantity, stability, visibility of your prefixes, etc., must support with the same conditions IPv4 and IPv6.

7. Now that you already know the differences between IPv4 and IPv6, you’re ready for designing your detailed addressing plan, nevertheless possibly the overall overview has been already done in the consultancy. This is master piece for the correct IPv6 deployment, very different from IPv4 and for sure you will need an IPAM (IP Address Management) device or tool, as it

is impossible to manage millions of IPs with the traditional text file or spreadsheet as you did before with IPv4.

8. Deploy IPv6 in your core and distribution networks. Possibly dual-stack will be sufficient in a first phase. In a follow-up stage, maybe you will be able to supress IPv4 in part of those networks, so you can reuse those addresses in more relevant places of your network.

9. It will be very convenient to start some small trial, in your own corporate network. Remember that /64 is the minimum for each LAN or VLAN, that the golden rule is to keep dual-stack in the LANs/VLANs (even if using private IPv4 addresses) and that is easier to use SLAAC and RDNNS. DHCPv6 is an extra option, most of the time unnecessary, moreover, Android doesn't support it. Also in this phase, it may be interesting to involve in the pilot some of your corporate customers, even some residential ones. It is not so relevant if at this stage, manually provisioning is required.

10. Prepare your access network as well as the provisioning system. Your billing systems may be affected too. Is time to define what transition mechanism is the right one. My recommendation is 464XLAT[1], at least for the residential customers and cellular networks. It is a must to have good support from the CPE vendors. For the provisioning the best will be to use DHCPv6-PD. Use the RIPE BCOP in order to understand how to number your customers.

11. Configure PLAT (NAT64+DNS64) in your network. Don't use CGN, it will bring you much more problems, higher cost (not only the CGN itself, but also the logging systems). If you've a cellular network, with the PLAT deployment, and setting up an IPv6-only APN, you will have all done for the smartphones and other 3G/LTE devices. In the case of Android and Windows, they come with the CLAT, while iOS/Apple only use the PLAT, because all their apps are mandatorily supporting IPv6.

12. Update the CPEs. Try again with some customers, once updated; this is the most critical and complex part of all the process. There are many ways to approach it. Once done, you're ready for a massive IPv6 activation (maybe in phases, regions, etc.) and do a commercial announcement.

Your network is ready for the future!

Now, you need to start considering how to take profit of IPv6 with new services and applications, IoT is the key hint, sure you will find other advantages.

Author: Jordi Palet, "The IPv6 Company"

[1] 464XLAT is one of the most recent transition mechanism (and the most used one, with millions of users in 3G/4G networks), which has the advantage of using IPv6-only in the access network, so the ISP doesn't require IPv4 addresses there; despite that, provides IPv4 private addresses to the users (by means of the CLAT), so that devices and applications still work in a transparent way.