

IPv6: Near Term Priorities

IPv6 Forum President Latif Ladid talks to InterComms about the countdown on IPv4 address space



Latif Ladid, IPv6 Forum President.

Q: What's most troubling for you in the world of IP?

A: The address space has gone down to ten percent. We only have 26 blocks left. This will serve us for a maximum of 24 months if not 18. Soon, there will be a run on the bank because a lot of the ISPs think that if they have IPv4 address space, they will be better prepared for the transition. This is not easy to do. If you take the investment in the US alone, as of 2008, there was something like \$200 billion in ICT investment of which something like 80 percent or \$140 billion was spent on the management and maintenance of the installed base, which means that the legacy networks are getting harder and harder to manage and maintain. With 20 percent spent on managing new equipment, that tells you that new technologies are very difficult to introduce into a large scale legacy network. This is one of the new hurdles and the new roadblocks to introduce large scale innovation.

Q: Who have overcome those roadblocks?

A: Those who have been smart and agile have already introduced these new technologies. Companies in the US like Verizon now have sufficient deployment of IPv6 for LTE and have mandated IPv6 into it. This is brand new. No-one has done this, even in Asia. They are using standards that have not yet been decided upon by 3GPP or 3GPP2. These are big signs that the US can pick up the ball and run with it a lot faster than Asia or Europe. This is the dynamic, that the US always teaches us new rules when things are really tough. This is reinforced by the announcement of the US' new broadband policy, or what they have called the Broadband Stimulus Package; a \$5 billion package announced in June for which they are now asking for proposals. That is designed to give an incentive to ISPs to extend broadband to rural areas and amazingly, IPv6 is mandated into it. There is an irony that for the first time some of poorer and rural areas in that country will have the latest technology. This is where the government can play a dramatic role in introducing new technologies. I would expect the same thing that has occurred in the US to happen in other countries too. Another example is in green, smart grids in which the US has also decided on IPv6. IPv6 will be used to connect to any device, in this case to a metre at home to manage energy more efficiently. Networking energy installation is a fundamental shift into faster easier collection of data about how energy is used and where it is used poorly. New models of energy saving are going to come out of this. New networks are going to go into these sectors, where the management of these sectors has hitherto not done very well, using proprietary solutions that were typically very expensive.

These stimulus packages are a good place to position IPv6 so that the equipment is going to be future

proofed, especially in these rural areas where often the cheapest technology has been installed in the past.

Q: Why are government customers important?

A: We see the government being the prime customer for large scale technologies because they are the largest customers. In one case in Germany, the Germany Online initiative has 26,000 networks. It is the project of Chancellor Merkel, in which citizens can access anything they need from the government. They have found that these 26,000 networks in Germany have been installed using private addressing. When you have private addressing it's like having the same 'phone number' multiple times within these 26,000 strong networks. They cannot call each other because they have the same phone numbers. When these numbers are used in these 26,000 networks, when you want to connect them to each other directly, then you have a IP address collision because it's the same number calling each other. If you want to do secure email between the two, the security protocol believes you are calling yourself and stops the connection. For these networks to send emails to each other, they have to go through an ISP. As a consequence of this, they have decided to use IPv6 to give each network its own unique prefix so that they will be able to send emails directly to each other within their own network.

This is the same everywhere, including the US. What we need is an end to end model; which is an IP address connecting to another IP address which are unique. With IPv6, we will be able to do end to end and in this case end to end security. In the future when we have smart guys to link IPv6 and IPv4 we will be able to switch the old stuff as well. It is only a matter of time.

Any email server will require a unique IP address, in this case IPv6 and spammers will not be allowed to use

- ▶ IPv4's hidden addresses so that we will be able to trace them, wherever they are. If all governments agree on this one then we will be able to trace anyone sending spam.

Q: What are the organisation's priorities for the next twelve months?

A: The prime objective is to get these big customers – governments – on board. We have to get the big customers to adopt IPv6 and the biggest customers are the governments themselves and this is working very well. The second objective is to get ISP to give IPv6 service to their customers. They play a major role. The ISPs are very much focused on a day to day bread winning cycle. To them, any investment that does not bring money right away is not going to be considered. With the address space reduction and with only a maximum 24 month timeline available, they will soon hit the wall.

The smart guys have already announced that they are making the changes and they have already delivered new services. In Japan you already have 75 big ISPs who are delivering IPv6 and some of them have up to five million users such as NTT, Softbank or IJ. In France in 2002, one ISP called Nerim told the IPv6 community that if they could collect 10,000 signatures, they would give them IPv6 for free. They now have now 1.5 M users using IPv6 from their 5 Million user base. <http://www.nerim.fr/ipv6>

You find different models of how different ISPs are delivering services. However, ISPs are realising that leaving your 'IP tank' empty in the middle of the highway is not a smart thing to do. Most of the engineers understand the issue but CTOs and CEOs don't always appreciate it.

Q: What are the Killer Apps for IPv6?

A: One of the biggest things that has come out is Microsoft's Direct Access. Its objective goes beyond

the Virtual Private Network (VPN) model. VPN is a model that has been designed so that you can use the current infrastructure to build secure tunnels across the Internet back to your corporate server. This model however is only good for corporations that require their people to use VPNs to access their email or business data. When using VPNs you can only use it to access primarily your corporate network but you cannot use it to access the Internet easily because of the security measures. VPNs are also expensive because of the security software that has to be used.

Now with IPv6 we have end to end capabilities. Using IPv6 and IPSEC, when you connect to the internet from anywhere in the world, MS' Direct Access will connect

you automatically to the Corporation's network and you can still use your laptop to access the Internet and do private stuff. The software allows the user to choose at any time to connect to any of their customers or suppliers with zero pain. This is end-to-end security. This is what IPv6 brings to the table. This is a major magic brought to everyone by IPv6.

MS' model is open, although it is proprietary to MS. I think the security software providers are going to have a very hard time adapting to this new model. The internet is going to be used for faster, better communication and it is going to be very interesting to see who has the first killer application for IPv6.

