TELECOM LAB ITALIA
www.telecomitalialab.com

Cod. Doc. DPC 2001.02904

TILAB contribution to IPv6 Task Force - Actions for IPv6

Version: 1.0

Date: 25.09.2001

Number of pages: 6

AUTHOR: Leonardo FERRACCI (NS/NS)

REVISION: Paolo FASANO (NS/NS)

APPROVAL: Paolo FASANO (NS/NS)

Executive summary

A number of papers have been submitted to the IPv6 Task Force which examine the reasons behind the design of IPv6 and the benefits of its deployment; this document is based on such works and aims at highlighting some points of attention the IPv6 Task Force should keep into account and some initiatives it could suggest to the EC in order to support actual IPv6 deployment in production environments.

Contents

1 Introduction

A number of papers have been submitted to the IPv6 Task Force which examine the reasons behind the design of IPv6 and the benefits of its deployment; this document is based on such works and aims at highlighting some points of attention the IPv6 Task Force should keep into account and some initiatives it could suggest to the EC in order to support actual IPv6 deployment in production environments.

This paper is organized as follows: first some points are outlined which could ease IPv6 introduction in client hosts; then the network side is taken into account, focusing separately on issues concerning ISPs and manufacturers.

2 Client side

The minimum requirement for IPv6 acceptance among end users is to keep the effort of updating (if needed) and configuring terminals as little as possible. This means:

- Operating systems:
  - If an update of existing versions of operating systems is needed to enable IPv6 support, this should be performed by an automated script/program with minimum or no intervention from the user;
  - Newer versions of operating systems should be encouraged to install and enable IPv6 software by default; as long as software footprint is not a concern, having all “IPv6/IPv4 nodes” hosts seems a wise solution for enabling both dual stack strategies (in the transition period) and IPv6-only functionality (in the future: this would be done simply by not binding any address to the IPv4 interface);
- System configuration:
  - IPv6 host autoconfiguration features should be used to the maximum extent possible (of course this has to be supported by autoconfiguration services provided by the network);
  - Automated “wizards” should help the user to set those network parameters not provided by autoconfiguration.

After that, it is important to provide users with applications; this a key point for two main reasons:

- Users are familiar with a number of applications and services (such as WWW, e-mail, chat, newsgroups, and so on) which they expect to be still available when upgrading to IPv6. It is arguable that in the first steps of IPv6 deployment, porting of IPv4 applications to IPv6 may not seen as a primary issue, as it could be likely that enough IPv4 addresses are still available to have most or all new IPv6 terminals implementing dual-stack; notwithstanding this, availability of IPv6-aware applications is definitely an issue to monitor, as lack of IPv6 support in widespread applications may seriously jeopardize the deployment of IPv6-only terminals in the near future.
- On the other hand, new features of IPv6 can be exploited to build brand-new classes of applications and services; in this way, user demand for such services would be a strong market driver for IPv6 deployment. For example, unlike IPv4 dial-up connections and

private addressing, IPv6 makes it possible to assign to each user a permanent, globally unique address, which is an important feature for emerging peer-to-peer applications.

3 Network side

3.1 ISPs & Network Infrastructure

A reasonable requirement for ISPs wishing to offer IPv6 connectivity is to have all main services for both residential users and corporate costumers (such as DNS, mail, news, WWW) hosted on dual-stack servers, or alternatively available from both IPv4 and IPv6 servers; this seems a more flexible solution than NAT-PT/ALG and does not require host stacks to implement transition mechanisms still in the draft state such as DSTM. For example, the need for a root name server and TLD servers accessible via IPv6 has already been outlined (up to date, this the case for .jp and .cc TLDs only). A desirable result of the TF could be a set of recommendations aimed at UE governments to support ISPs in server and network infrastructure updates (new version and patches of operating systems and applications on servers; new software releases on routers, and maybe HW upgrades to support them if needed). Supporting ISPs in the migration effort could help in building critical mass for IPv6, hopefully leading to a snowball effect that forces even more ISPs to adopt IPv6 just to avoid giving ground to the most innovative of their competitors.

As for network infrastructure, we can make different considerations for:

- Backbone infrastructure: ISPs can choose whether to deploy an overlay infrastructure (where IPv6 traffic is tunnelled over the existing IPv4 network) or to gradually introduce a separate IPv6 native network, in addition to the IPv4 infrastructure;

- Access infrastructure: even though issues related to IPv6 access are similar to those existing in IPv4, some points of attention are still to monitor as there seems to be a lack of access devices (such as NAS's) featuring IPv6 support.

Peering between IPv6 ISPs, through tunneling on the existing IPv4 network or native IPv6 connections, should be encouraged too, as well as the deployment of transition mechanisms to allow IPv6-only hosts to access any service available on IPv4-only servers. Anyway, great care should be taken in addressing the latter problem, as emerging but not yet fully standardized solutions (such as DSTM) are to be taken into account against existing standards (NA(P)T-PT/ALG) which are not transparent to all applications and upper-layer protocols. Besides mandating dedicated servers deployment, some of such transition mechanisms (namely SIIT and DSTM) require changes in the implementation of the IPv6 protocol stack of clients; as stated earlier, attention should be paid to make sure that such an update (if needed) is performed in the less painful way possible for the user. Thus with regard to the transition mechanisms issue, too, cooperation and sharing of operational experience between ISPs should be encouraged.

There is also an important social and political benefit in spreading IPv6 support as widely as possible in network infrastructures: in facts, due to the limited number of IPv4 addresses available for many developing countries, IPv6 seems a great chance of reducing the "digital divide"; anyway, risk exists of actually enlarging such gap if the new protocol is not widely and readily supported in the communication infrastructure of developed countries.

3.2 Motivations for ISPs

An analysis has been carried out at TILAB, aimed at highlighting advantages from which IPv6 ISPs can benefit, depending on their size and target market. Such considerations are summarized below.

3.2.1 Backbone ISPs

A backbone ISP (which provides wholesale Internet connectivity to downstream ISPs in the international market) can achieve significant benefits from IPv6 adoption if:

- It plans to expand within developing countries, where the lack of IP addresses is a big issue;
- It wants to offer transit services to local and regional ISPs which already started IPv6 experiments and deployment;
- It wishes to increase its relationships with other peer or upstream providers which decided to start with IPv6 experiments and deploymenton their own;
- It has interest in participating to the creation of the new Internet since the beginning.

3.2.2 Wired ISPs in the corporate market

In this case, ISPs are more likely to benefit from offering IPv6 support if:

- They are facing a growing number of costumers who cannot get all the global IP address they ask for;
- They do not like the growing number of NATs within their own networks, which is making any new service design and offering more and more complex;
- They are interested in R&D cooperation with actual as well as potential customers sensible to innovation.

3.2.3 Wired ISPs in the residential market

ISPs offering connectivity to end users should be interested in IPv6 if they are aware that:

- The demand for always-on services is dramatically increasing;
- IPv6 may prove as a key enabler for new, not-yet-conceived services (e.g. peer-to-peer);
- Innovation oriented users, whose interest for IPv6 is already enthusiastic, may turn in a large number of new costumers.

3.2.4 Wireless ISPs

The most significant advantages deriving from IPv6 adoption can probably be achieved by wireless operators and ISPs:

- The process of introducing IP networking in mobile terminal, which has just started with GPRS deployment, may be seriously jeopardized by the shortage of global IPv4 addresses;
- IPv6 enables new services such as mobile-terminated calls, always-on services and transparent roaming;
- IPv6 is a core component in the 3G and Beyond-3G architecture;

- Wireless applications and terminals can benefit of optimised Mobile IPv6 features.

3.3 Network equipment manufacturers

Lately, IPv6 support is spreading among commercially available network devices from the main manufacturers; anyway, some points of attention are still to be taken carefully into account:

- US loose commitment to IPv6 could reduce implementation and support efforts from vendors; it is important to build synergies with Asian countries in order to make the joint European and Asian market valuable for manufacturers;

- Manufacturers of equipment for 2.5G (and 3G) mobile networks seem to still have a gap to close with respect to wired network equipment.

4 Software vendors

Most network applications which are released under open source licences have been readily updated by research institutes and early IPv6 enthusiasts; such software includes the most widespread server-side implementations of the main Internet application protocols (such as HTTP, IRC, NNTP, SMTP), so that a firm basement for IPv6 Internet application deployment is now available. Thus with application software the focus should be moved to:

- Server software based on proprietary protocols (maybe SAP, LotusNotes, …) or released under commercial/closed source licence (e.g. Microsoft IIS web server);

- Client software for both standard and proprietary protocols.

Introduction of IPv6 support into clients of standard protocols can be pushed by two factors: the spreading of the relevant IPv6-enabled servers and the availability of open source clients, which can be patched or modified by “anyone” to support IPv6 (this in facts turns into a competitive advantage which competitors releasing commercial/closed source applications may wish to close, implementing IPv6 on their clients too).

On the other hand, network applications based on proprietary protocols are more likely to defer IPv6 implementation until its support is felt as a mandatory requirement for the survival of the software product on the market.

Thus, the Task Force approach towards software vendors should be aimed at the development of a widespread understanding that the few lines of code required to add IPv6 support in existing applications are not only a future proof solution but may even turn into a competitive advantage – or, conversely, that lacking IPv6 support may suddenly become a hard-to-close negative gap with respect to the competitors.