IPv6 Campus Transition Experiences

Tim Chown
School of Electronics and Computer Science
University of Southampton
Southampton SO17 1BJ, United Kingdom
tjc@ecs.soton.ac.uk

Abstract

IPv6 is now a mature standard, with the core protocols defined by the Internet Engineering Task Force (IETF). Over the past two years a number of national research networks and academic network backbone providers have deployed IPv6 in production, using dual-stack networking. The challenge ahead now is to push IPv6 deployment into the universities and end sites in the academic networks. This paper presents an overview of the current state of IPv6 transition at one such site, the University of Southampton (UK), drawing on experience gained from participation on the 6NET and Euro6IX projects.

1. Introduction

In the past two years a significant number of National Research and Education Networks (NRENs) have deployed a production IPv6 service. Such dual-stack deployments now mean that native IPv6 connectivity is available between diverse points on the Internet, spanning areas including North America, Europe and South East Asia.

In Europe the GÉANT network has offered a production unicast IPv6 dual-stack service since mid-2003, and the majority of the European NRENs have also enabled IPv6 on their backbones. These efforts in Europe have been accelerated by the results produced by the 6NET [1] and Euro6IX [13] IST-funded research projects, each of which have invested over 1,000 man months in a three-year period.

2 Transition Philosophy

With IPv6 widely available natively between most worldwide academic networks, and the myriad of unreliable and unpredictable tunnelled connections having been removed, IPv6 performance end to end is largely every bit as good as IPv4. While connectivity on commercial IPv6 networks is yet to catch up, the challenge now is to deploy IPv6 into the end sites (universities) and encourage and demonstrate innovative new IPv6 applications and services.

Our view is that IPv6 transition is inevitable, and thus an early deployment is prudent. A university should anyway deploy network services to support teaching and research, and is an ideal seeding ground for innovation, where technologies are presented to staff, students and researchers.

3 Transition Scenario

A site may choose to deploy IPv6 in different ways, as described in the IETF Enterprise Scenarios work [12]. A site may seek to deploy IPv6 dual-stack throughout its infrastructure, may seek an early dual-stack deployment in sparse nodes, or may consider deploying an IPv6-dominant solution.

In the School of Electronics and Computer Science we are deploying a pervasive dual-stack IPv6 environment. The goal is to support IPv6 operation where applications, services or hosts choose to select it, and to enable the introduction of IPv6-only devices into the network that are able to use both the traditional IP infrastructure (DNS, mail, etc) and also begin to take advantage of new IPv6 protocols (Mobile IPv6, IPv6 Source-Specific Multicast, etc).

The deployment is not necessarily straightforward. A site wishing to deploy IPv6 is unlikely to have current commercial network infrastructure that can support dual-stack, wire-speed operation, without considering a potentially expensive upgrade. However, one would expect IPv6 capability to follow through natural network infrastructure procurement cycles. As an interim step, we have deployed a parallel IPv6 routing infrastructure on site for unicast and multicast, as described in this paper.

The deployment experience of the projects is captured in the project deliverables online. For 6NET this includes the "IPv4 to IPv6 Transition Cookbook for end-sites" [2], in which the theory and practice of transition tools such as

ISATAP, NAT-PT, 6to4, tunnel brokers and Teredo is explained. Our experience has also been fed into IETF work, including IPv6 Campus Transition [6], and IPv6 Enterprise Analysis, [11]. We expect an update of our Cookbook to version D2.3.4 by the time of the SAINT workshop.

3.1 Specific scenario

Our School network spans some 20 or so IPv4 subnets of varying sizes from /23 to /28, containing over 1,000 DNS-registered hosts and over 1,500 users. The IPv4 connectivity to our NREN (JANET) comes via our regional network (LeNSE) and the campus.

There is only one network ingress and egress point to the site that needs to be IPv6 capable; this is a Gigabit Ethernet interface. IPv4 campus connectivity into the School routes via a Nokia firewall, passes through an IDS system (Snort) and is then broken out by existing switch-router equipment (mainly Alcatel-based) that does not support Layer 3 IPv6 operation.

Given there is no available network infrastructure for IPv6 routing, we require an appropriate mechanism to deploy IPv6 on the wire until a new procurement allows IPv6 operation. We have 802.1q VLAN support within the network, internally and also to span our network to remote buildings across the campus; this is the tool we have selected to use to enable our parallel IPv6 deployment.

The preferred mechanism for interoperation with legacy nodes is to use dual-stack and thus IPv4 to communicate to IPv4 nodes and IPv6 to communicate to IPv6 nodes. We have not identified any in-house, non-upgradeable legacy applications, e.g. our specific financial and administrative applications are presented via Web interfaces.

4 Network Infrastructure Components

Here we discuss the generalised network infrastructure components that need to be considered in transition:

- *DNS*. BIND9 is used for our three internal name servers, which are acting as local dual-stack resolvers for IPv4 or IPv6 transport for local dual-stack or IPv6-only nodes. The three servers carry AAAA records, and AAAA glue is being added. JANET supports IPv6 transport DNS lookups to .ac.uk.

- *Routing*. Internal IPv4 routing is either statically configured or uses RIP. We thus expect to use RIPng for internal IPv6 routing. The external routing is statically configured for IPv6, as per IPv4. The site is not multihomed.

- *Configuration of Hosts*. IPv4 clients use DHCP for address and other configuration options. We expect to use Dynamic Host Configuration Protocol for IPv6 (DHCPv6) for IPv6 clients. This will require analysis of the IPv4 and IPv6 Dual-Stack Issues for DHCPv6 [10]. We expect some clients, especially in wireless LANs, to use IPv6 Stateless Autoconfiguration, and thus need DHCPv6 for other configuration options, including the local IPv6 DNS resolver. Although IPv6 offers Stateless Autoconfiguration, it is expected that the managed environment will continue, driven from our asset database, for some time, thus DHCPv6 is required. We expect to support hosts using RFC3041 Privacy Extensions.

- *Security*. We are identifying new IPv6 related security considerations, and those associated with transition mechanisms.

- *Applications*. The IETF Application Aspects of IPv6 Transition work [5] describes best IP version independent porting practice for applications. Application proxies should generally also be enabled.

- *Network Management*. The network management and monitoring systems need to embrace IPv6 and transition mechanisms used to deploy IPv6. IPv6 monitoring includes usage tracking (e.g. via MRTG) and availability monitoring (e.g. via Nagios).

- *Address Planning*. IPv6 address space is allocated from JANET's prefix of 2001:0630::/32. The university receives a /48 prefix, which is 2001:0630:d0::/48. The School has a /52 allocation within this block, of 2001:0630:d0:0::/52, starting with a /56 but with reserved space to grow into. The IPv6 allocation was made based on us using a similar percentage of IPv4 address space.

- *Multicast*. IPv4 multicast is used for a number of applications. We expect to make use of source specific multicast (SSM) more heavily in IPv6, bringing IPv6 and SSM together in one deployment cycle.

5 Deployment Methodology

As described in the IPv6 Enterprise Analysis document [11], our scenario is one of wide-scale dual-stack deployment. The plan for deployment follows the guidelines of Section 7 of that text, i.e.:

1. *Gaining initial connectivity*. In our case, the connectivity is native IPv6 from JANET, via the regional MAN (using 6PE) and the campus (using a VLAN to carry IPv6 natively across the campus).

2. *Obtaining global IPv6 address space, and formulating an address plan*. With our /56 prefix we can create in theory up to 256 IPv6 subnets initially. However, because the School runs an IPv6 tunnel broker for remote access, allocations from the /52 will be taken up early. Note this means we cannot broker /48 networks.

3. *Deploying basic external connectivity, while ensuring IPv6 security.* This is a function of site policy, which needs to be updated for IPv6-specific issues, e.g. privacy addresses, and implemented, via an IPv6 firewall, IDS and other measures.

4. *Deploying basic internal network services*: DNS, routing, and host configuration support. We are using the VLAN-based method for parallel IPv6 routed deployment described in [9]. At this point we have IPv6 routed on the wire almost pervasively in the School.

5. *Supporting IPv4-IPv6 interworking*. As there are not (yet) any IPv6-only links, interworking methods are not required. Should IPv6-only devices be deployed on the dual-stack infrastructure, we anticipate using proxy tools (web cache, SMTP relay, etc) to support their access to legacy IPv4 services. Exceptions are hardware like IPv4-only printers, WLAN access points and webcams.

6. *Supporting remote users*. See the next section.

7. *Deploying wider IPv6 application, management and service support*. This is an ongoing task.

6 Transition Toolbox

We are using the following mechanisms in our department transition plan, one to support internal IPv6 routing, the others to support remote IPv6 access:

1. *Internal*. We use VLANs to distribute IPv6 connectivity over the existing non-dual-stack network infrastructure [9]. When dual-stack infrastructure is available, and the next procurement due, we will upgrade the core network infrastructure to dual-stack. The VLAN solution is an interim step.

2. *Remote access*. We have three options; IPv6 access over an IPv4 VPN solution (we are using OpenVPN for this), or running a Tunnel broker for remote access, or offering a 6to4 relay for remote access, where users can manually configure the relay's IPv4 address.

Our IPv6 native connectivity comes in via a BSD firewall to an IPv6-only access router (Cisco 7206), which feeds internal connectivity to BSD router(s) that break IPv6 routing out to internal IPv4 subnets by injecting IPv6 Router Advertisements into congruent VLANs.

We do not currently see a requirement for:

1. NAT-PT, because we are dual-stack with no IPv6-only networks (yet), and as we introduce such networks, or IPv6-only nodes in the dual-stack networks, we expect to use application layer gateways and proxies for legacy IPv4 access;

2. ISATAP, because we prefer to use a structured internal IPv6 deployment, and are doing so in a pervasive fashion (i.e. not as a sparse deployment);

3. Teredo, as our remote users are capable of using other access methods. However, we may deploy a Teredo relay in due course to support home users behind NATs if they report problems with using other access methods.

7 Services and Status

Our experience of the deployment of IPv6 services on site have been fed into project cookbooks, e.g. the 6NET ”IPv6 Network Management Cookbook” [4] and the 6NET ”Routing, DNS, intra-domain multicast, inter-domain multicast, and security cookbook” [3].

Specific examples of our other services are:

- *Email*. There are three MX hosts for inbound email, and two main internal mail servers. Sendmail is the MTA. POP and IMAP (and their secure versions) are used, based on open source code, and there is an MS Exchange server. MailScanner is used for anti-spam/ anti-virus, which uses external services including various RBLs for part of its spam checking, which are not available over IPv6.

- *Web Hosting*. Web content hosting is provided either with Apache 1.3.x or Microsoft IIS 5.0. Common components used to build systems with are MySQL, PHP 4 and Perl 5; these enable local tools such as Wikis to be run. An upgrade to Apache 2 has IPv6-enabled the bulk of our School's web presence.

- *Databases*. All database systems are presented via a web interface, including the financial systems. In some cases, e.g. student records, ODBC-like access is required/used in to/out from the School systems to the campus systems.

- *Directory Services*. We use NIS, LDAP, MS Active Directory and RADIUS. Only AD does not support IPv6.

- *NTP*. The JANET NREN offers a stratum 0 NTP server, but it is not IPv6 enabled. The School has two IPv6-enabled NTP servers, via its RIPE NCC test traffic server and a dedicated unit from Meinberg. Client support is currently lacking on some platforms.

- *USENET News*. The news feed is delivered using dnews; a change to INN would be required to support IPv6.
- *Remote login*. Remote login access is offered via ssh, with sftp for file transfer, both of which support IPv6.
- *File serving*. The main file servers are SGI systems, hosting large (multi-TB) standalone RAID arrays. The files are offered via NFS and Samba to client systems; these do not yet support IPv6.
- *Backups*. Backups are run over SSH, which is IPv6-enabled.

8 IPv6 specific features

We are beginning to offer new IPv6 services, e.g. we support internal use of MIPv6, and MIPv6 between the School and our local IPv6-enabled community WLAN (SOWN). We support PIM-SSM for IPv6 on our parallel IPv6 BSD routing infrastructure.

We are studying advantages of IPv6 management, e.g. resilience to port scanning [7], and the removal of requirements to resize subnets to utilise address space efficiently. We are studying new challenges, like graceful IPv6 renumbering [8].

9 Current Gap Analysis

Here we highlight examples of current gaps in our deployment plans; with dual stack these are not critical, however to support IPv6-only nodes in the network, these become important.

- No IPv6 Layer 3 functionality on the School's current Ethernet switch/routing equipment (hence we use the parallel VLAN method for now);
- Lack of NFS/Samba IPv6 support;
- No IPv6 support for MS Active Directory;
- Lack of supported IPv6 for Windows 98/2000/ME;
- Lack of supported IPv6 for Irix;
- Lack of supported IPv6 for various PDA platforms;
- Lack of MLDv2 (or MLDv1) snooping in Ethernet switch equipment;
- Lack of detailed feature support on firewalls;
- No available IPv6-enabled X11 (there is an xfree but it carries a debated copyright statement).
- No support for IPv6 hotspot access control via web-redirection systems;
- Few DHCPv6 server implementations, very few client implementations.

10 Conclusions and Future Work

We have deployed IPv6 pervasively on our School network, via an interim parallel router infrastructure. Many local services, tools and applications are now IPv6-enabled. We have not observed any noticeable negative impact on our IPv4 behaviour. We are beginning to take advantage of new IPv6 services, including MIPv6 and SSM. The gaps in deployment are shrinking, perhaps most notable being the commercial, vendor-specific applications.

References

[1] 6NET Project. http://www.6net.org/.

[2] 6NET Project Deliverable 2.3.3-bis: IPv4 to IPv6 transition Cookbook for End Sites, August 2002. http://www.6net.org/publications/deliverables/D2.2.3bis1.pdf.

[3] 6NET Project Deliverable 3.1.2: Routing, DNS, intra-domain multicast, inter-domain multicast, and security cookbook, August 2002. http://www.6net.org/publications/deliverables/D3.1.2.pdf.

[4] 6NET Project Deliverable 6.3.1: IPv6 Network Management Cookbook, July 2002. http://www.6net.org/publications/deliverables/D6.3.1.pdf.

[5] Application Aspects of IPv6 Transition. IETF Internet Draft (work in progress), June 2004. draft-ietf-v6ops-application-transition-03.

[6] T. Chown. IPv6 Campus Transition Scenario Description and Analysis. IETF Internet Draft (work in progress), October 2004. draft-chown-v6ops-campus-transition-01.

[7] T. Chown. IPv6 Implications for TCP/UDP Port Scanning. IETF Internet Draft (work in progress), July 2004. draft-chown-v6ops-port-scanning-implications-01.

[8] T. Chown. Things to think about when Renumbering an IPv6 Network. IETF Internet Draft (work in progress), October 2004. draft-chown-v6ops-renumber-thinkabout-00.

[9] T. Chown. Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks. IETF Internet Draft (work in progress), October 2004. draft-chown-v6ops-vlan-usage-02.

[10] DHCP: IPv4 and IPv6 Dual-Stack Issues. IETF Internet Draft (work in progress), October 2004. draft-ietf-dhc-dual-stack-02.

[11] IPv6 Enterprise Network Analysis. IETF Internet Draft (work in progress), October 2004. draft-ietf-v6ops-ent-analysis-00.

[12] IPv6 Enterprise Network Scenarios. IETF Internet Draft (work in progress), July 2004. draft-ietf-v6ops-ent-scenarios-05.

[13] Euro6IX Project. http://www.euro6ix.org/.