IPv6 Operations
Internet-Draft
Expires: January 10, 2005

T. Chown
University of Southampton
July 12, 2004

IPv6 Campus Transition Scenario Description and Analysis
draft-chown-v6ops-campus-transition-00

Status of this Memo

Copyright Notice

Abstract

In this document we consider and analyse the specific scenario of IPv6 transition and deployment in a large department of a university campus network. The department is large enough to operate its own instances of all the conventional university services including (for example) web, DNS, email, filestore, interactive logins, and remote and wireless access. The scenario is a dual-stack one, i.e. transition to IPv6 means deploying IPv6 in the first instance alongside IPv4. This analysis will both identify the available (and still missing) components for IPv6 transition, and also test the applicability of the recently completed IPv6 Enterprise Network

Scenarios document.

Table of Contents

1. Introduction 4
2. Discussion of Scenarios Network Infrastructure Components . 5
2.1 Component 1: Enterprise Provider Requirements 5
2.2 Component 2: Enterprise Application Requirements 6
2.3 Component 3: Enterprise IT Department Requirements 6
2.4 Component 4: Enterprise Network Management System 8
2.5 Component 5: Enterprise Network Interoperation and Coexistence 8
3. Discussion of Network Infrastructure Component Requirements 9
3.1 DNS 9
3.2 Routing 9
3.3 Configuration of Hosts 9
3.4 Security 9
3.5 Applications 9
3.6 Network Management 10
3.7 Address Planning 10
3.8 Multicast 10
3.9 Multihoming 10
4. Specific Scenario Component Review 10
4.1 Network Components 10
4.1.1 Physical connectivity (Layer 2) 10
4.1.2 Routing and Logical subnets (Layer 3) 11
4.1.3 Firewall 11
4.1.4 Intrusion Detection System 11
4.1.5 Management 11
4.1.6 Monitoring 11
4.1.7 Remote access 11
4.1.8 IPv6 External Access 12
4.2 Address Allocation Components 12
4.2.1 IPv6 network prefix allocation 12
4.2.2 IPv6 Address allocation 12
4.3 Services 13
4.3.1 Email 13
4.3.2 Web Hosting 13
4.3.3 Databases 13
4.3.4 Directory Services 13
4.3.5 DNS 13
4.3.6 PKI 14
4.3.7 NTP 14
4.3.8 USENET News 14
4.3.9 Multicast 14
4.3.10 Remote login 14
4.3.11 File serving 14

4.4 Host and Device Platforms 14
4.4.1 Server platforms 14
4.4.2 Desktop/laptop platforms 15
4.4.3 PDA platforms 15
4.5 User Tools 15
4.5.1 Hardware 15
4.5.2 Mail Client 16
4.5.3 Web Browser 16
4.5.4 Conferencing systems 16
4.5.5 Other collaboration tools 16
4.5.6 Usenet news client 16
4.5.7 Host communications 17
4.6 Hard-coded address points 17
5. Analysis 18
5.1 Philosophy 18
5.2 Current deployment 18
5.3 Planned transition steps 18
5.4 Missing components 18
5.5 Considerations beyond the Scenarios Document 19
6. Summary 20
7. Acknowledgements 20
8. Security Considerations 20
9. Informative References 20
Author's Address 21
Intellectual Property and Copyright Statements 22

1. Introduction

The scope of the enterprise network transition scenarios is very large, much more so than that of the other three IPv6 transition areas under study within the IETF. The IPv6 Enterprise Network Scenarios [13] have been defined. In this document we present a specific case study area for IPv6 transition, namely a large department (1,500 staff and students, over 1,000 hosts) in an academic campus network. The purpose of this document in its current form is to both define and analyse the IPv6 transition of such a network, but also to test the applicability of the IPv6 Enterprise Network Scenarios document to a specific example.

Our campus study falls under "Scenario 1" of the IPv6 Enterprise Network Scenarios [13] document, i.e. the campus network is an existing IPv4 network, where IPv6 is to be deployed in conjunction with the IPv4 network.

"Scenario 1" has the assumption that the IPv4 network infrastructure used has an equivalent capability in IPv6. This document will analyse that assumption. The Scenario also has requirements, i.e. that the existing IPv4 network infrastructure is not disrupted, and that IPv6 should be equivalent or better than the network infrastructure in IPv4. The Scenario also notes that it may also not be feasible to deploy IPv6 on all parts of the network immediately.

These assumptions and requirements will be discussed later in this text.

It should also be noted why Scenarios 2 and 3 did not apply to this campus transition scenario. Scenario 2 talks of specific applications, but in the campus case we wish to deploy IPv6 pervasively, in wired and wireless networks, as an enabler for education and research, to encourage new application development. Scenario 3 focuses on using IPv6 as the basis for most network communication, but in the campus we already have a significant IPv4 deployment that will be utilised for the foreseeable future (Scenario 3 would perhaps be more appropriate for a greenfield deployment).

This document is very much a work in progress, and thus this first instance of this document is not intended to be complete or comprehensive. Some sections are empty at this stage. We make no claims that this campus scenario is typical, but believe the lessons leanrt and analysis undertaken may be of wider interest. Feedback is sought on scope and the required level of detail.

2. Discussion of Scenarios Network Infrastructure Components

In this section, we look at the issues raised by following the Scenarios Network Infrastructure Components of the IPv6 Enterprise Network Scenarios [13] document, section 3.2.

2.1 Component 1: Enterprise Provider Requirements

The answers to the questions posed in this section of the IPv6 Enterprise Network Scenarios document are as follows:

- There is external access to/from the campus network, regional MAN and National Research Network beyond.
- There are needs for access by remote staff, student and researchers.
- It is a single site, with four buildings.
- There are no leased lines or wide-area VPNs between remote buildings.
- The department has 12 IPv4 Class C's, the campus has a Class B, independent from its provider (assigned prior to use of CIDR).
- The IPv4 and IPv6 provider is the National Research and Education Network (JANET in the UK). JANET provides a /48 prefix for the university. The university offers a /52 prefix for the department.
- The university and department make their own prefix allocations for subnets.
- There is no multihoming, and thus no multihomed clients.
- The only IPv6 service offered by the provider to date is a 6to4 [3] relay.
- There is no exteral IPv6 routing protocol needed due to the use of static route configuration.
- There is no external data centre.
- IPv6 runs over the same access links to campus (the JANET backbone uses true dual stack, the regional MAN uses 6PE [14]. On campus, the IPv4 traffic to the department is received through a Nokia IP740 firewall, the IPv6 traffic is received through a BSD firewall. Thus the access links into the department for IPv4 and

IPv6 are different, though the goal is to make them the same.

2.2 Component 2: Enterprise Application Requirements

Answers to the next IPv6 Enterprise Network Scenarios section are as follows:

- The application inventory is discussed in the specific component review in the next section.
- We expect the first applications to be moved will be the support services, including DNS. The first applications should be the common IPv4 applications, e.g. web, remote login and email, such that IPv6 offers as least an equivalent service to IPv4 for the important applications.
- The academic environment has a good mix of open source and commercial software, predominantly either Microsoft or Linux, but with a growing number of Mac OS/X users. Specific platforms are reviewed in the component review in the next main section. Most open source applications have been upgraded to allow IPv6 operation; others can be upgraded given time.
- The general goal is for applications to support both IPv4 or IPv6 operation, i.e. to be IP agnostic.
- There is no use of NAT in the department's network. Home users, or users access into the network remotely from certain locations, may experience NAT at their client side.
- NAT issues are relevant from the end-to-end perspective, for establishment of end-to-end security where desired, and in relation to IPv6 transition (remote access) mathods that may be run through NATs.
- There is a mix of internal and external applications. Where limitations occur, it is mainly by policy not technology, e.g. as implemented in firewall restrictions.

2.3 Component 3: Enterprise IT Department Requirements

Here we list responses to the next IPv6 Enterprise Network Scenarios section on IT Department Requirements:

- Ownership and support is all in-house.

- Remote VPNs are supported.
- No inter-site networking is required.
- No network mobility support is needed at this point, though we expect to use Mobile IPv6 between the department network and a local community wireless network.
- The IPv6 address plan for the department requires a /52 prefix.
- There is no detailed asset database, though one is being built.
- There are no geographically separate sites.
- The internal IPv4 address assignment mechanism is DHCP for clients, with manual configuration for servers. We thus expect to use DHCPv6 for at least some IPv6 clients.
- Internal IPv4 routing is static or uses RIP. We thus expect to use RIPng internally.
- We expect our IPv6 network management policy to be very similar to that for IPv4.
- There is no QoS provision at present, largely due to the ample campus bandwidth (1Gbit/s uplink).
- Security is applied through many technologies implementing our policies, e.g. firewall, email scanning, wireless LAN access controls. We expect similar policies for IPv6, but need to analyse differences.
- Training will be done in-house.
- The impacted software components are discussed in the next main section. Not all functions are upgradeable to IPv6; those that are not are discussed in the analysis section. Some are, e.g. use of OpenLDAP in place of MS Active Directory.
- The impacted hardware components are discussed in the next main section. Not all hardware is upgradeable, e.g. network printers. There are no load balancing systems in use. There are wireless LAN hosts in the network that are mobile, but currently the wireless network is a flat IPv4 subnet. There may be nodes moving to external wireless networks (the local community wireless network.

2.4 Component 4: Enterprise Network Management System

The responses to the next IPv6 Enterprise Network Scenarios section are as follows:

- No performance management is required.
- There are a number of network management and monitoring tools in use, which will need to be used in a dual stack or IPv6 mode, e.g. the nocol availability monitring tools, and SNMP-based management.
- The configuration management may include use of tools to configure services including DNS and email.
- No policy management and enforcement tools are required.
- No detailed security management is required, though we expect to manage the implementations including firewalls and intrusion detection.
- We may need to manage the deployed transition tools and mechanisms.
- We need to analyse the considerations IPv6 creates for network management, e.g. use (or not) of RFC3041 privacy addresses.

2.5 Component 5: Enterprise Network Interoperation and Coexistence

Answers to the final IPv6 Enterprise Network Scenarios section on Coexistence are as follows:

- The platforms that are required to be IPv6 capable are listed in the next main section.
- There is only one network ingress and egress point to the site that needs to be IPv6 capable; this is a Gigabit Ethernet interface.
- The required transition mechanisms are discussed in the analysis section. We expect to mainly use the VLAN [7] mechanism for internal IPv6 transport, with a parallel IPv6 routing infrastructure based on BSD routers.
- The transition to IPv6 will be enabled on the wire first, enabling clients, with a phased introduction of service capability, as discussed below in the analysis section.

- 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.

3. Discussion of Network Infrastructure Component Requirements

In this section, we discuss the network infrastructure component requirements raised in the IPv6 Enterprise Network Scenarios [13] document, in section 4.

3.1 DNS

BIND9 is used for our three internal name servers. The servers will be made dual stack, to be available for IPv6 transport for local dual-stack or IPv6-only nodes.

3.2 Routing

Internal 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 IPv4, and thus is likely to be statically configured for IPv6.

3.3 Configuration of Hosts

IPv4 clients use DHCP for address and other configuration options. We expect to use Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [4] 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 [1], and these nodes will need support for Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6 [5] for other configuration options, including the IPv6 address of a local DNS resolver.

3.4 Security

We need to identify new IPv6 related security considerations, and those associated with transition mechanisms [15]. Site policies may need to be updated as a result.

3.5 Applications

The Application Aspects of IPv6 Transition [12] document describes best porting practice for applications. There should also be

consideration for any required application proxies.

3.6 Network Management

The network management and monitoring systems will need to embrace IPv6, and any transition mechanisms used to deploy IPv6. Monitoring includes usage tracking (e.g. via MRTG) and availability monitoring (e.g. via nocol).

3.7 Address Planning

The department receives 12 Class C prefixes for IPv4 use, and uses only globally routable addresses internally. The IPv4 address space for the campus was obtained prior to CIDR, but the IPv6 address space is allocated from the UK National Research Network (JANET) address space under 2001:0630::/32. The university receives a /48 prefix, which is 2001:0630:d0::/48. The department has a /52 allocation within this block of 2001:0630:d0:0:/52.

3.8 Multicast

IPv4 multicast is used for a number of applications, including the AccessGrid. Connectivity is provided via the local campus and regional network. We expect to use both IPv6 ASM (i.e. PIM-SM), and may seek to make use of the Embedding the Address of RP in IPv6 Multicast Address [11] technique. For briding between IPv4 and IPv6 multicast, we believe an IPv4 - IPv6 multicast gateway [16] may prove valuable. Finally, we expect to make use of source specific multicast (SSM) more heavily in IPv6, bringing IPv6 and SSM together in one deployment cycle.

3.9 Multihoming

The site is not multihomed.

4. Specific Scenario Component Review

Here we describe specific technology in use now in the department. Later in this section we discuss any items not included in the above section, i.e. those not explicitly mentioned in the IPv6 Enterprise Network Scenarios document. In the next main section we analyse these for missing technologies, as a form of gap analysis.

4.1 Network Components

4.1.1 Physical connectivity (Layer 2)

- Switched Ethernet
- Gigabit Ethernet
- Wireless networking (802.11b)

4.1.2 Routing and Logical subnets (Layer 3)

The hybrid Layer 2/3 routing equipment has approximately 20 internal IPv4 subnets (in effect, routed VLANs). There is no specific internal routing protocol used. There is a static route via the site firewall to the main upstream provider (academic) running at 1Gbit/s.

4.1.3 Firewall

The firewall is currently CheckPoint Firewall-1 running on a Sun Solaris platform, just migrating to a Nokia IP740 hardware platform. There is one internal facing interface, one external facing interface, and two .DMZ. interfaces, one for wired hosts and one for the Wireless LAN provision.

4.1.4 Intrusion Detection System

- Snort

4.1.5 Management

Some network management is performend by SNMP; there is no specific package for this. There is a greater emphasis on monitoring than explictly in management.

4.1.6 Monitoring

A number of tools are used, to monitor network usage as well as systems availability, e.g. nocol, nagios and MRTG. The IBM AWM tool is used for network testing, along with iperf, rude and crude.

4.1.7 Remote access

- Livingston Portmaster 56K/ISDN dialup
- RADIUS server
- (Microsoft) VPN server

4.1.8 IPv6 External Access

- IPv6 connectivity comes via 6PE from our regional network.

4.2 Address Allocation Components

The department receives its IPv4 and IPv6 address allocations from the University. For IPv4, the University has a Class B allocation which is not aggregated under the JANET NREN. For IPv6, the University receives its allocation from JANET.

4.2.1 IPv6 network prefix allocation

For IPv6, JANET has the prefix 2001:630::/32 from RIPE-NCC, as the national academic ISP in the UK. The University has been allocated 2001:630:d0::/48 by JANET. The department transitioning will be allocated a /52 size prefix under 2001:630:d0::/48, i.e. 2001:630:d0:0::/52.

In the initial deployment, we expect that IPv4 and IPv6 subnets will be congruent (and share the same VLANs). The advantage for IPv6 is that subnets will not need to be resized to conserve or efficiently utilise address space as is the case currently for IPv4 (as subnet host counts rise and fall for administrative or research group growth/decline reasons).

4.2.2 IPv6 Address allocation

It is expected that the network devices will use a combination of address allocation mechanisms:

- Manually configured addresses (in some servers)
- Stateful DHCPv6 (probably in fixed, wired devices and some servers)
- Stateless address autoconfiguration (probably in wireless and mobile devices)
- RFC3041 privacy addresses (in some client devices)

For devices using stateless or RFC3041 mechanisms, a Stateless DHCPv6 server will be required for other (non-address) configuration options, e.g. DNS and NTP servers.

4.3 Services

4.3.1 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 for mail access, using the UW-IMAP open source code. There is an MS Exchange server used by up to 100 users (generally those wanting shared access to mail spools, e.g. professors and secretaries). MailScanner is used for anti-spam/ anti-virus. This uses external services including various RBLs for part of its spam checking. Successful reverse DNS lookup is required for sendmail to accept internal SMTP connections for delivery.

4.3.2 Web Hosting

Web content hosting is provided either with Apache 1.3.x (open source) 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.

4.3.3 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 department systems to the campus systems. Databases include: finance records, people, projects and publications (offered using ePrints).

4.3.4 Directory Services

The following are used:

- NIS (6 servers, all Solaris)
- LDAP
- Active Directory
- RADIUS

4.3.5 DNS

The three DNS servers have recently been upgraded to BIND9. A DNS secondary is held at another UK university site.

4.3.6 PKI

The department has at least 10 SSL certificates from Thawte, including Web-signing certificates. No personal certificates are supported by the department (though users may have their own).

4.3.7 NTP

The JANET NREN offers a stratum 0 NTP server. The department also has a GPS-based NTP server built-in to its own RIPE NCC test traffic server.

4.3.8 USENET News

The news feed is delivered using dnews.

4.3.9 Multicast

There is PIM-SM IPv4 multicast via a dedicated Cisco 7206 router. This supports applications including the IPv4 AccessGrid conferencing system. A number of bugs in the existing IPv4 equipment prevent heavy use of IPv4 Multicast within the department network (thus an IPv6 Multicast solution is highly desirable). An IPv4 Multicast beacon is used for monitoring Multicast.

4.3.10 Remote login

Remote login access is offered via ssh, with sftp for file transfer. Remote use of telnet and ftp is denied by the firewall.

4.3.11 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. The content distribution server is hosted on such a system (e.g. containing MS software licenced under the Campus Agreement).

4.4 Host and Device Platforms

4.4.1 Server platforms

These include:

- Windows 2003 server
- Windows 2000 server

- Windows NT
- Solaris 8
- Solaris 9
- RedHat Linux
- SGI Origin 300 (Irix 6.5.x)

4.4.2 Desktop/laptop platforms

These include:

- Windows 98, 2000, ME, XP
- Linux (various flavours)
- MacOS/X
- BSD (various flavours)

4.4.3 PDA platforms

These include:

- Windows CE/.NET, Pocket PC
- PalmOS
- Familiar Linux on iPaQ
- Zaurus (Linux)

4.5 User Tools

These are non-exhaustive but representative application/platform lists

4.5.1 Hardware

- Networked printers
- Networked webcams

4.5.2 Mail Client

- Outlook (various versions)
- Eudora
- Mutt
- Pine

4.5.3 Web Browser

- MS Internet Explorer
- Mozilla
- Safari
- Opera

4.5.4 Conferencing systems

- AccessGrid
- A dedicated H.323 system
- MS Netmeeting

4.5.5 Other collaboration tools

- IRC
- Jabber
- MSN Messenger
- cvs

4.5.6 Usenet news client

- nn
- Mozilla

4.5.7 Host communications

- X11
- VNC
- PC Anywhere

4.6 Hard-coded address points

Usage of IPv4 hard-coded addresses is interesting for at least two reasons. One is that it illustrates where IPv6 hard-coded addresses may appear, and thus secondly it is useful to analyse which hard-coded addresses may be barriers to smooth IPv6 renumbering. A procedure for renumbering has been described in Procedures for Renumbering an IPv6 Network without a Flag Day [6]. A non-exhaustive list of instances of such addresses includes:

- Provider based prefix(es)
- Names resolved to IP addresses in firewall at startup time
- IP addresses in remote firewalls allowing access to remote services
- IP-based authentication in remote systems allowing access to online bibliographic resources
- IP address of both tunnel end points for IPv6 in IPv4 tunnel
- Hard-coded IP subnet configuration information
- IP addresses for static route targets
- Blocked SMTP server IP list (spam sources)
- Web .htaccess and remote access controls
- Apache .Listen. directive on given IP address
- Configured multicast rendezvous point
- TCP wrapper files
- Samba configuration files
- DNS resolv.conf on Unix

- Nocol monitoring tool
- NIS/ypbind via the hosts file
- Some interface configurations
- Unix portmap security masks
- NIS security masks

5. Analysis

To be added.

5.1 Philosophy

To be added. Essentially dual-stack is a path to allowing IPv6-only devices to be added later, and preferred external IPv6 communications.

Some mechanisms will be needed for remote access from staff or student homes in the absence of their ISP not supporting IPv6, e.g. Tunnel broker [2], 6to4 [3] or Teredo [9]. These are to be analysed, and the support implications (where appropriate).

5.2 Current deployment

To be added.

5.3 Planned transition steps

To be added.

5.4 Missing components

An initial gap analysis for technology highlights the following missing components:

- No IPv6 Layer 3 functionality on the department's current Ethernet switch/routing equipment (this will be worked around using the parallel VLAN method, until new IPv6-capable equipment is deployed);
- Lack of NFS/Samba IPv6 support;
- Lack of MS Exchange, Outlook or Eudora IPv6 support;

- AccessGrid is IPv4-only (IPv6-enabling work is to be undertaken in 6NET);
- Some Apache 2 modules lack Apache 1.3 functionality, hence migrating is a problem in a small number of cases;
- No IPv6 support for Active Directory;
- No IPv6 dnews, so one would have to use inn as a Usenet news server;
- Lack of supported IPv6 for Windows 98/2000/ME;
- Lack of supported IPv6 for Irix;
- Lack of supported IPv6 for various PDA platforms;
- No method available to offer reverse IPv6 DNS for sendmail to verify autoconfiguring hosts (prepopulating a 64 bit subnet space is a problem, some wildcard method is required);
- Lack of MLDv2 snooping in Ethernet switch equipment (thus IPv6 Multicast will flood subnets);
- No available IPv6-enabled X11 (there is an xfree but it is encumbered by an unpopular copyright statement that most distributors find unnacceptable);
- No support for IPv6 hotspot access control via web-redirection systems.

5.5 Considerations beyond the Scenarios Document

Here we mention issues or scenario components that were not explicitly listed in the IPv6 Enterprise Network Scenarios document. Due to the scope, that document could not embrace all details. We mention here components that other sites may also wish to consider:

- Support for WLAN and other access control. One solution is to use 802.1x which is IP-agnostic as a Layer 2 port control mechanism.
- Consideration for hard-coded addresses.
- ..To be completed..

6. Summary

In this document we will analyse the specific campus transition scenario for the author's site, and report the analysis for the benefit of others who may be in a similar scenario, or for whom parts of the scenario are relevant. The basic IPv6 deployment is doable now, but there are still missing components that prevent a full dual-stack deployment.

7. Acknowledgements

Discussions with fellow participants on the 6NET and Euro6IX projects have been valuable.

8. Security Considerations

There are no specific new considerations from this scenario description and analysis.

9 Informative References

[1] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.

[2] Durand, A., Fasano, P., Guardini, I. and D. Lento, "IPv6 Tunnel Broker", RFC 3053, January 2001.

[3] Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, February 2001.

[4] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C. and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[5] Droms, R., "Stateless Dynamic Host Configuration Protocol (DHCP) Service for IPv6", RFC 3736, April 2004.

[6] Baker, F., "Procedures for Renumbering an IPv6 Network without a Flag Day", draft-baker-ipv6-renumber-procedure-01 (work in progress), October 2003.

[7] Chown, T., "Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks", draft-chown-v6ops-vlan-usage-00 (work in progress), October 2003.

[8] Chown, T., "IPv4 and IPv6 Dual-Stack Issues for DHCPv6", draft-chown-dhc-dual-stack-00 (work in progress), February 2004.

[9] Huitema, C., "Teredo: Tunneling IPv6 over UDP through NATs", draft-huitema-v6ops-teredo-00 (work in progress), June 2003.

[10] Chown, T., "IPv4 and IPv6 Dual-Stack Issues for DHCPv6", draft-ietf-dhc-dual-stack-00 (work in progress), March 2004.

[11] Savola, P. and B. Haberman, "Embedding the Address of RP in IPv6 Multicast Address", draft-ietf-mboned-embeddedrp-00 (work in progress), October 2003.

[12] Shin, M., "Application Aspects of IPv6 Transition", draft-ietf-v6ops-application-transition-00 (work in progress), December 2003.

[13] Bound, J., "IPv6 Enterprise Network Scenarios", draft-ietf-v6ops-ent-scenarios-00 (work in progress), October 2003.

[14] Clercq, J., "Connecting IPv6 Islands across IPv4 Clouds with BGP", draft-ooms-v6ops-bgp-tunnel-00 (work in progress), October 2002.

[15] Savola, P., "IPv6 Transition/Co-existence Security Considerations", draft-savola-v6ops-security-overview-00 (work in progress), June 2003.

[16] Venaas, S., "An IPv4 - IPv6 multicast gateway", draft-venaas-mboned-v4v6mcastgw-00 (work in progress), February 2003.

Author's Address

Tim Chown
University of Southampton

School of Electronics and Computer Science
Southampton, Hampshire SO17 1BJ
United Kingdom

EMail: tjc@ecs.soton.ac.uk

Intellectual Property Statement

Disclaimer of Validity

Copyright Statement

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.