

1. ARIN IPv6 Wiki Acceptable Use	3
2. IPv6 Info Home	3
2.1 Explore IPv6	5
2.1.1 The Basics	6
2.1.1.1 IPv6 Address Allocation BCP	6
2.1.2 IPv6 Presentations and Documents	9
2.1.2.1 ARIN XXIII Presentations	11
2.1.2.2 IPv6 at Caribbean Sector	12
2.1.2.3 IPv6 at ARIN XXIII Comment	12
2.1.2.4 IPv6 at ARIN XXI	12
2.1.2.4.1 IPv6 at ARIN XXI Main-Event	13
2.1.2.4.2 IPv6 at ARIN XXI Pre-Game	14
2.1.2.4.3 IPv6 at ARIN XXI Stats	14
2.1.2.4.4 IPv6 at ARIN XXI Network-Setup	18
2.1.2.4.5 IPv6 at ARIN 21	21
2.1.3 IPv6 in the News	21
2.1.3.1 Global IPv6 Survey	23
2.1.3.2 IPv6 Penetration Survey Results	23
2.1.4 Book Reviews	25
2.1.4.1 An IPv6 Deployment Guide	25
2.1.4.2 Day One: Advanced IPv6 Configuration	25
2.1.4.3 Day One Exploring IPv6	25
2.1.4.4 IPv6 Essentials	26
2.1.4.5 Migrating to IPv6	26
2.1.4.6 Running IPv6	26
2.1.4.7 IPv6, Theorie et pratique	26
2.1.4.8 Internetworking IPv6 With Cisco Routers	26
2.1.4.9 Guide to TCP/IP, 4th Edition	26
2.1.4.10 Understanding IPv6, Third Edition	27
2.1.5 Educating Yourself about IPv6	27
2.1.5.1 HashIPv6	29
2.1.6 IPv6 Resource Sites	29
2.2 Prepare For IPv6	29
2.2.1 Broadband CPE	30
2.2.2 Carrier Support	36
2.2.3 Designing an IPv6 Lab Environment	36
2.2.4 Device Support	37
2.2.5 DNS Registrars IPv6 Support Status	38
2.2.6 Enabling IPv6 on a Mail Server	38
2.2.7 First Steps for ISPs	39
2.2.8 Guidelines for the Secure Deployment of IPv6	41
2.2.9 How do I get IPv6 from ARIN	41
2.2.10 How do I get IPv6 from an ISP	41
2.2.11 Investigate Middleboxes	42
2.2.12 IPv6 Addressing Plans	42
2.2.13 IPv6 Consulting Resources	45
2.2.14 IPv6 Firewalls	45
2.2.15 Operational transition information	46
2.2.16 Planning IPv6 Deployment	46
2.2.16.1 United States	47
2.2.16.1.1 NIST	47
2.2.16.1.2 US Civilian Agency Networks	48
2.2.16.1.3 US Department of Defense	49
2.2.16.1.4 US IPv6 Policy	50
2.2.17 Porting Applications	51
2.2.18 Providers Currently Selling IPv6 Transit	51
2.2.19 Transparent Internet Access	52
2.2.20 US Government - USGv6 Technical Infrastructure	52
2.2.21 Vendors in the ARIN Region	52
2.2.21.1 Vendors in the ARIN Region 6connect	53
2.2.21.2 Vendors in the ARIN Region Acme Packet	53
2.2.21.3 Vendors in the ARIN Region Adtran	53
2.2.21.4 Vendors in the ARIN Region Airspan	54
2.2.21.5 Vendors in the ARIN Region APC	54
2.2.21.6 Vendors in the ARIN Region Calix	55
2.2.21.7 Vendors in the ARIN Region Cisco	55
2.2.21.8 Vendors in the ARIN Region Comtrend	55
2.2.21.9 Vendors in the ARIN Region Ericsson	56
2.2.21.10 Vendors in the ARIN Region Hostik	56
2.2.21.11 Hostik	56
2.2.21.12 Vendors in the ARIN Region HP	56
2.2.21.13 Vendors in the ARIN Region Procera Networks	57

2.2.21.14 Vendors in the ARIN Region RG Nets	57
2.2.21.15 Vendors in the ARIN Region TiVO	58
2.2.21.16 Vendors in the ARIN Region Yamaha	58
2.3 Implement and Manage IPv6	58
2.3.1 Apache HTTPD	59
2.3.2 Customer problems that could occur	59
2.3.3 Providers of IPv6 Services	67
2.3.4 DNS and Naming Issues	68
2.3.5 Implementing 6PE	70
2.3.6 IPv6 Management Tools	72
2.3.7 ISP IPv6 Implementations	72
2.3.8 Relay Services	73
2.3.8.1 Cisco 6to4 Relay Service	75
2.3.8.2 FreeBSD Teredo Relay	81
2.3.8.3 Juniper 6to4 Relay Service	81
2.3.8.4 Linux or BSD 6to4 Relays	82
2.3.8.5 ISPs currently announcing a 6to4 prefix	85
2.3.8.6 Miredo	86
2.3.8.7 Transitioning__6to4	87
2.3.8.8 Transitioning__NAT64	88
2.3.8.9 Transitioning__NAT-PT	88
2.3.8.10 Transitioning__Teredo	88
2.3.8.10.1 ISPs currently announcing a teredo prefix	88
2.3.9 Renumbering an IPv6 Network	88
2.3.10 Troubleshoot IPv6 Issues	89
2.3.11 FreeBSD	92
2.3.12 Linux Support	93
2.3.13 Solaris IPv6 Sites	93
2.3.14 Warning broken users with JavaScript	93
2.3.15 3GPP Mobile Networks	95
2.3.16 IPv6 Consulting and Training Services	100
2.3.16.1 A Wireshark IPv6 Configuration Profile	104
2.3.16.2 IPv6 Training and Consulting Services	105
2.3.17 IPv6 Hosting and DNS Providers	105

ARIN IPv6 Wiki Acceptable Use

Role of the Collective Community

Acceptable Use Policy (AUP)

The content of this website is generated and maintained, in part, by the Internet number resource community members through consensus and open collaboration. Its purpose is to provide interested individuals in the community an opportunity to collaborate on subject matter pertaining to IPv6. Anything posted to this website must relate to IPv6 issues and topics generally considered to be current and relevant. The focus of this website is implementation and migration of IPv6 in the ARIN region, but content related to experiences outside the ARIN region is allowed.

The following policies have been established to allow for the effective exchange of information in a responsible way by interested parties. These policies must be strictly adhered to in order to keep this website as an effective open forum and useful resource.

- All articles and content must relate specifically to IPv6 topics and issues. Postings not directly related to the use of IPv6 and/or Internet number resource policies as they relate to IPv6 are prohibited.
- Independent issues not affecting the larger Internet number resource community are not appropriate, nor are comments of a personal nature.
- Use or distribution of others' comments or content of this site for any purpose other than to discuss relevant issues pertaining to IPv6, or for the free and unrestricted distribution of the content of this site is not permissible.
- Any unprofessional or confrontational comments showing a lack of respect, such as using foul or abusive language or attacking someone's character, will not be tolerated.
- Overuse of the privilege of posting content or making comments, flooding of articles or comments/e-mails to registered users of the site, contacting other registered users for the purpose of sales or marketing of services, or any other form of spamming is strictly prohibited.
- Marketing of products or advertising of any kind, whether for business or employment purposes, is not allowed.
- The promotion of political views is not appropriate.
- Attempts to obtain e-mail addresses for any purpose other than for which the wiki was designed is prohibited.
- Content that is the owned intellectual property of a specific user or organization, and that is posted without the explicit permission of the owner of the intellectual property, is strictly prohibited.

Violators of any of the above policies will be contacted and asked to adhere to the policy. Offensive content will be removed. If a user persists in violating the policy, ARIN staff will take steps to prohibit the user, whether associated with a registered user account or IP address, from participating on this website . Thank you for your participation and cooperation.

IPv6 Info Home



Welcome to the ARIN IPv6 Wiki!

This site is hosted by ARIN to facilitate discussion and the sharing of information on IPv6 topics and issues. The site has been recently updated and if you have never used a Confluence-based wiki before, please consult the [Help Pages](#) for information on using the wiki software. Also, the links below will help you get started in adding content and using this site.

Before adding any content to this website, please review this site's [Privacy Policy](#) and [Disclaimers](#) documents. Links are provided at the bottom of every page. Also, users and contributors must review the [Acceptable Use Policy](#) .

Explore IPv6

- [The Basics](#)
- [IPv6 Presentations and Documents](#)
- [IPv6 in the News](#)
- [Book Reviews](#)
- [Educating Yourself about IPv6](#)
- [IPv6 Resource Sites](#)

ARIN & IPV6

Highlights

- NEW: IPv6 Consulting and Training Services
- IPv6 Hosting and DNS Providers



Connect to the Whole Internet with IPv6

Recent space activity



- **Torbjörn Eklöv**
 - [Troubleshoot IPv6 Issues](#) updated 25 Mar 2016 • [view change](#)
- **Tim Martin**

Prepare for IPv6

- Broadband CPE
- Carrier Support
- Designing an IPv6 Lab Environment
- Device Support
- DNS Registrars IPv6 Support Status
- Enabling IPv6 on a Mail Server
- First Steps for ISPs
- Guidelines for the Secure Deployment of IPv6
- How do I get IPv6 from ARIN
- How do I get IPv6 from an ISP
- Investigate Middleboxes
- IPv6 Addressing Plans
- IPv6 Consulting Resources
- IPv6 Firewalls
- Operational transition information
- Planning IPv6 Deployment
- Porting Applications
- Providers Currently Selling IPv6 Transit
- Transparent Internet Access
- US Government - USGv6 Technical Infrastructure
- Vendors in the ARIN Region

Relevant IPv6 Information at ARIN.NET

If you would like more information about ARIN's policies and procedures related to IPv6, or a look at community discussions and other materials, we encourage you to make use of the [ARIN website](#). We've provided some links below to highlighted information.

- ARIN's IPv6 Info Center
- IPv4 Depletion / IPv6 Adoption Slide Deck
- IPv6 section of Number Resource Policy Manual
- Instructions-Initial IPv6 Allocation from ARIN
- Instructions-Requesting Additional IPv6 Allocations from ARIN
- Instructions-Requesting a Direct IPv6 Assignment from ARIN
- ARIN Fee Schedule
- ARIN Registration Statistics
- ARIN Public-facing Services



Preparing Applications for IPv6

A Software Developers Guide to Writing and Migrating Network Applications for Use

on IPv6 Networks



- IPv6 Consulting Resources updated 25 Mar 2016 • [view change](#)



Torbjörn Eklöv

- DNS Registrars IPv6 Support Status updated 25 Mar 2016 • [view change](#)



- IPv6 Consulting Resources updated 25 Mar 2016 • [view change](#)



- IPv6 Hosting and DNS Providers updated 25 Mar 2016 • [view change](#)

ARIN is pleased to present "Preparing Applications for IPv6," a software developers guide to writing and migrating networked applications for use on IPv6 networks. This guide focuses on software application needs when making the migration to IPv6, and covers some common assumptions made when developing software for an IPv4-only Internet.

Implement and Manage IPv6

- [Apache HTTPD](#)
- [Customer problems that could occur](#)
- [Providers of IPv6 Services](#)
- [DNS and Naming Issues](#)
- [Implementing 6PE](#)
- [IPv6 Management Tools](#)
- [ISP IPv6 Implementations](#)
- [Relay Services](#)
- [Renumbering an IPv6 Network](#)
- [Troubleshoot IPv6 Issues](#)
- [FreeBSD](#)
- [Linux Support](#)
- [Solaris IPv6 Sites](#)
- [Warning broken users with JavaScript](#)
- [3GPP Mobile Networks](#)
- [IPv6 Consulting and Training Services](#)
- [IPv6 Hosting and DNS Providers](#)

Results from Global IPv6 Deployment Monitoring Surveys: 2013, 2012, 2011, and 2010 are also available online.

Explore IPv6

This category is for article pages dealing with educational resources available for deploying IPv6. Before adding an article about a new resource, please check to see if a reference to it already exists on another page.

- [Book Reviews](#)
 - [An IPv6 Deployment Guide](#)
 - [Day One: Advanced IPv6 Configuration](#)
 - [Day One Exploring IPv6](#)
 - [Guide to TCP/IP, 4th Edition](#)
 - [Internetworking IPv6 With Cisco Routers](#)
 - [IPv6, Theorie et pratique](#)
 - [IPv6 Essentials](#)
 - [Migrating to IPv6](#)
 - [Running IPv6](#)
 - [Understanding IPv6, Third Edition](#)
- [Educating Yourself about IPv6](#)
 - [HashIPv6](#)
- [IPv6 in the News](#)
 - [Global IPv6 Survey](#)
 - [IPv6 Penetration Survey Results](#)
- [IPv6 Presentations and Documents](#)
 - [ARIN XXIII Presentations](#)
 - [IPv6 at ARIN XXI](#)
 - [IPv6 at ARIN XXI Main-Event](#)
 - [IPv6 at ARIN XXI Pre-Game](#)
 - [IPv6 at ARIN XXI Stats](#)
 - [IPv6 at ARIN XXI Network-Setup](#)
 - [IPv6 at ARIN 21](#)
 - [IPv6 at ARIN XXIII Comment](#)
 - [IPv6 at Caribbean Sector](#)

- [IPv6 Resource Sites](#)
- [The Basics](#)
 - [IPv6 Address Allocation BCP](#)

External Links

[The Power of 6 - Learn why and how to prepare for an IPv6 transition - Video from Cisco](#)

The Basics

What is an IP Address?

"IP" stands for Internet Protocol. Internet Protocol provides the methodology for communication between devices on the Internet. An Internet Protocol address (IP address) is a number that uniquely identifies a device on a computer network and, using transport protocols, moves information on the Internet. Every device directly connected to the Internet must have a unique IP address.

Background: IPv4 and Depletion

IPv4 (Internet Protocol version 4) is the first widely used standard defining how the Internet and its connected devices operate and communicate with one another. When IPv4 became the Internet standard, the 4.2 billion possible IP addresses were never intended to house a global commercial Internet. It was 1981, there were only a limited number of computers that needed to connect to the Internet (mostly American government and research entities), and web-capable phones were far from being invented. This pool of IP addresses has been in use for the entire history of the commercial Internet, but recent technology has driven the available [IP address pool very close to depletion](#).

Nowadays, in addition to every computer, nearly every cellular telephone and gaming console is connected to the Internet, not to mention the infrastructure hardware required to make these devices work. As a result of this rapid growth, IPv4 addresses are running out, and fast. According to the Number Resource Organization, less than ten percent of them remained in the [Internet Assigned Numbers Authority \(IANA\)](#) free pool as of the beginning of 2010. Through the use of tools like [Network Address Translation \(NAT\)](#), users have extended the life of IPv4, because NAT allows multiple devices to speak to the Internet through a single IP address, while the router in that particular household or business keeps track of which device(s) are receiving and sending information.

Why IPv6?

The solution to IP address depletion is simple: developing a more robust numbering system will allow for far more IP addresses. [IPv6 \(the newer Internet Protocol\)](#) holds 340,282,366,920,938,463,463,374,607,431,768,211,456 IP addresses. This exponentially larger pool of IP addresses is the key to the future growth of the Internet, and companies that use and distribute IP addresses will need to adapt their networks and systems to use IPv6. Without IPv6, the Internet's expansion and innovation could be limited, and the underlying infrastructure will become increasingly complex to manage. The additional costs from delaying deployment will make life harder for Internet operators, application developers, and end users everywhere.

An excellent [presentation on IPv6 is available](#). It covers both the high-level basics, as well as in-depth technical details, especially as related to security and privacy.

IPv6 Address Allocation BCP

Best Current Practices in for IPv6 Address Allocation

This Best Practices document aims to provide IPv6 Address allocation guidelines that a network operator can follow while planning the IPv6 subnetting for its network (based on the issues faced and learning's from IPv6 implementation in NKN and NIC network).

Best Current Practice:

1. Subnetting

IPv6 addresses generally written in Hex format. Each Hex number represents 4 bit, commonly known as nibble. A nibble boundary is a network mask that aligns on a 4-bit boundary. Subnetting the v6 address at nibble boundary improves efficiency and make it easier to understand for humans* (Machine will anyway read it binary format).

Nibble Aligned Prefixes



Non-Nibble Aligned Prefixes



Example of Nibble and non-Nibble Boundaries Subnetting

From the above example, we can clearly see that Subnetting at the Nibble boundaries is easier to manage and do the subnetting.

* Condition may arise where you may have to do non-Nibble based subnetting. It depends on case-to-case basis But Nibble boundaries based subnetting is the recommended one.

2. Every LAN segment should be assigned /64 prefix

A /64 IPv6 segment provides 64 bits for network and hosts both. Every LAN segment should be provided /64 prefix regardless the size of the same. An IEEE's 64-bit Extended Unique Identifier **EUI-64** format (method by which host can automatically assign itself a unique ipv6 address) needs a LAN segment of /64.

/64 subnet is also required for Stateless Address Auto Configuration (SLAAC, refer [RFC 4862](#)).

3. Point-to-point Network

In case of point-to-point network, there is a flexibility of using /64 or /126 or /127 segment. As ip addresses are generally assigned manually in point-to-point link, so no benefit in using /64. If addresses are assigned to point-to-point link through SLAAC or EUI-64, then /64 is the only available option.

In case of manual assignment, /127 is the subnet which comes in mind. In some cases, we may face an issue called "subnet-router anycast" in routers while using /127 for point-to-point link (refer [rfc 3627](#) for more details). The best available option will be using /126 for Point-to-point Links.

4. /48 blocks for every Site/Region/Customer

For multi-homing in IPv6, minimum /48 segment is required. Every customer/Site should be allocated a /48 segment, irrespective of the size/LAN of the Region/Customer. Next /48 should be reserved for every Customer/Site so as to allocate the same if needed in future.

5. Hierarchical address planning

There should always be a scope for further expansion of the network. Inefficient planning and little or no scope for expansion will lead to an end up in inefficient v6 address allocation and will also lead to an increase in the v6 routing table. As mentioned above, every site/region should be allocated a /48 v6 block. In addition to this next /48 block should be reserved for that site. Continuous allocation helps in aggregation of two /48 into a single /47 segment (which will help us in minimizing the size of the v6 routing table).

6. Infrastructure Segment

Infrastructure incl. Loopback addresses, WAN Links and others. First /48 from ISP resource pool should be reserved for this. We can further subnet this /48 into multiple /64 segments.

a. Loopback Addresses

Loopback is the most common address and in majority of times, it is used in configuration. It should be as concise as possible so as to help human remember the same. Using first /48 from an ISP pool of /32 or /30 (or whatever the pool is) helps in suppressing the address to the maximum extent.

As for example, Suppose 2405:8A00::/32 is the ISP IPv6 address block, then we will have the following /48 subnet from the same :-

2405:8A00::/32
2405:8A00::/48
2405:8A00:0001::/48
2405:8A00:0002::/48
(snip)
2405:8A00:FFFF::/48

As clearly visible in the above example, the first /48 contains all zeros which can be combined to represent the segment in the best concise manner. Loopback address needs to be /128 only. First /48 can be further segmented into multiple /64 and the first /64 block will be used for loopback address allocation.

By using /64 segment, a scope is there for 2^{64} unique loopback v6 addresses (which is more than enough for the whole internet). As per current practice, use numeral only in the last octet and leave alphabets altogether.

For e.g.:- Suppose loopback segment is 2405:8A00::/64. Loopback addresses will be 2405:8A00::1/128, 2405:8A00::2/128, 2405:8A00::3/128, 2405:8A00::9/128. The next sequential address will be 2405:8A00::A/128. But as per best practice, this will be ignored (having alphabet in the last octet).

Useful loopback addresses will be like:-

2405:8A00::/64
2405:8A00::1/128
2405:8A00::2/128
(snip)
2405:8A00::9/128
2405:8A00::10/128
(snip)

2405:8A00::9999/48

b. WAN Links

Point-to-point links or WAN links requires only 2 useful addresses. Here any of the /127 or /126 or /64 can be used. It depends on the network design altogether. Whatever be used, uniformity should be maintained. As per practice, /126 is the optimal option as it save us from 'subnet-router anycast' and also use the address space from efficiently. /64 can be separated out from the Infrastructure pool for this purpose.

For e.g.:-

2405:8A00:0:1::/64
2405:8A00:0:1::0/126
2405:8A00:0:1::4/126
(snip)
2405:8A00:0:1::C/126
2405:8A00:0:1::10/126
(snip)
2405:8A00:0:1::1C/126

IPv6 Presentations and Documents

The following are links to documents/presentations with useful information on IPv6:

- [Why you need IPv6: Chris Grundemann's "Carrier Grade NAT – Observations and Recommendations" slides](#)
- [NRO's IPv6 Deployment Survey](#)
- [latest version of NIST's Guidelines for the Secure Deployment of IPv6](#)
- [Survey of IPv6 Support in Commercial Firewalls](#)
- [Results of a Security Assessment of the Internet Protocol version 6 \(IPv6\)](#)
- [IPv6 Deployment for Service Providers](#)
- [Managing 100 million IP addresses: Comcast is one of the first operators to adopt IPv6 as a strategic activity with an aggressive roll-out plan.](#)
- [IPv6 primer videos Intro Address-Space v6Header IPv4-v6 EUI-64 Addressing](#)
- [ATIS Report and Recommendation on IPv6](#)
- [Clara.Net describe how they deployed IPv6 services.](#) Presentation was given at UKNOF in September 2007.
- [Going Native Hurricane Electric, a well-known provider of IPv6 tunnel-broker services for many years, describe what they learned as they transitioned their backbone to extensive native IPv6 peering.](#)
- [Randy Bush did an excellent presentation on issues with IPv6 implementation](#)
- [Sharing a single IPv4 address for multiple customers using double NAT and IPv6](#)
- [Nathan Ward's NZNOG tutorial on IPv6 Deployment for ISPs](#)
- [This site maintains a list of Major Networks and their IPv6 transition status](#) Scroll down to see the table of information.
- [An inventory of practical implementations Business case perspective on actual implementations.](#)
- [IPv6: What, Why, How \(60 slides, by Jen "Furry" Linkova\) - covers both "executive" and highly technical topics, with a slight bias on security and privacy \(online-with-"live"-data and PDF versions\)](#)
- [A document on IPv6 deployment strategy at the University of Pennsylvania](#)
- [Interview with Martin Levy of Hurricane Electric on enabling IPv6](#)

Most Up To Date Books

- [Migrating to IPv6](#) by Marc Blanchet
- [IPv6 Essentials](#) by Silvia Hagen
- [IPv6, Theorie et pratique](#) (French)
- [Running IPv6](#) by Ilijitsch van Beijnum
- [Day One: Exploring IPv6](#) (Juniper/Junos specific) by Chris Grundemann
- [Day One: Advanced IPv6 Configuration](#) (Juniper/Junos specific) by Chris Grundemann
- [IPv6 Security](#) by Scott Hogg, Eric Vyncke

- IPv6 Fundamentals by Rick Graziani
-

Internet2/ESnet Joint Techs Workshops Presentations

- <http://www.internet2.edu/presentations/jt2010july/20100714-whinery-roguerasniping.pdf> Rogue RA Sniping with Scapy, July 2010 (Alan Whinery - lightning talk)]
- Making Your Campus Safe for Google DNS Whitelisting, July 2010 (David Farmer - lightning talk)
- Monitoring IPv6 Content Reachability and Accessibility, July 2010 (Roch Guerin, Shumon Huque)
- IPv6 Campus Deployment Updates panel, February 2010 (Shumon Huque, Alan Whinery, Randy Bush)
- IPv6 SNMP Network Management, February 2010 (Jon Dugan)
- DREN IPv6 Update, February 2010 (Ron Broersma)
- IPv6 in the UNAM Campus, February 2010 (Azael Fernandez)
- IPv6 Deployment in the Greek Student Network
- IPv6 Challenge: Coming Soon to a Network Near You!
- Migration or Stagflation: IPv6, Protocol Number Resource Management, and the Future of the Internet
- If We Deploy IPv6, Will It Help or Hurt Our Security?
- Campus IPv6 Deployment
- IPv6 Transition Experience
- Campus IPv6 Addressing Plans
- Enabling IPv6 in Products and Services
- Forcing the Issue: A Campus's (Ongoing) Experience in IPv6 Deployment
- IPv6 Autoconfiguration: Plug & Play Dream or Security Nightmare?

Internet2/ESnet Joint Techs - DREN IPv6 Implementation Updates

- Summer 2009
- Winter 2009
- Summer 2008
- Winter 2008
- Summer 2007
- Winter 2007
- Winter 2006
- Summer 2005
- Winter 2005
- Summer 2004

Joint NANOG/ARIN IPv6 Tutorials and Workshop Presentations

- NANOG 41 / ARIN XX Joint IPv6 Program

Relevant NANOG Presentations

Following is a list of IPv6 presentations given at NANOG meetings over the past several years. All the links go to the NANOG conference page which usually contains a link to presentation slides as well as recorded video of the presentation.

This list was selected from the NANOG presentations archive.

- IPv6 Transition & Operational Reality, Randy Bush, IJ. NANOG 41, October 2007.
- IPv6 Technical Issues Panel, Moderator: Joel Jaeggli. NANOG 41, October 2007
- IPv6 Multihoming, by Marla Azinger, Frontier Communications. NANOG 38, October 2006.
- Pragmatismv6: a Grown-up, Critical Examination of IPv6, by Todd Underwood Renesys, moderator; Daniel Golding, Tier 1 Research; David Meyer, Cisco, University of Oregon; Jason Schiller, Verizon Business. NANOG 38, October 2006.
- Open issues with ipv6 routing/multihoming, by Jason Schiller, UUNET/Verizon. NANOG 37, June 2006.
- IAB IPv6 Multihoming BOF, Dave Meyer, Cisco, moderator. NANOG 35, October 2005.
- IPv6 Deployment Issues: A Tier 1 Perspective, by Stewart Bamford, Level3. NANOG 35, October 2005.
- Tutorial: Getting Started with IPv6. Level: Introductory. Jordi Palet, Consulintel. NANOG 35, October 2005.
- Inter-AS Traffic Engineering Case Studies as Requirements for IPv6 Multihoming Solutions, by Jason Schiller, UUNET.
- IPv6 - Evolutionary Issues and Challenges, by Udo Steinegger, Cable & Wireless. NANOG 34, May 2005.
- Tutorial: IPv6 Deployment and Case Studies, by Salman Asadullah and Ciprian Popoviciu, Cisco. Level: Introductory/Intermediate. NANOG 32, October 2004.
- Network Augmentation Panel: Experiences in Adding IPv6 Services & Support to Existing IPv4 Networks. Bill Manning, moderator; Rob Rockell, Sprint; Brent Sweeny, Internet2 NOC; Ed Lewis, ARIN. NANOG 31, May 2004.
- IPv6 IPv4 Threat Comparison, by Darrin Miller and Sean Convery, Cisco. NANOG 31, May 2004.
- Overview of the Global IPv6 Routing Table, Gert Doering, SpaceNet AG, Munich, author. Cathy Wittbrodt, presenter. NANOG 29,

October 2003.

- Tutorial: Issues in IPv6 Deployment, by Jeff Doyle. Level: Introductory. NANOG 28, June 2003.
- IPv4/IPv6 Dual-Stack on Abilene, by Grover Browning, Indiana University. NANOG 28, June 2003.
- Operational Testing of DNS Resources - IPv6/DNS Symbiosis, by Bill Manning. NANOG 27, February 2003.
- IPv6 Deployment Concepts, by Tony Hain, Cisco. Tutorial, NANOG 27, February 2003.
- Commercial IPv6 Deployment by ISPs in Japan, by J. Hagino, IJ/KAME. NANOG 26, October 2002.
- Experiences With Developing, Testing, Planning, and Operating IPv6-Enabled Nameservers, by Paul Vixie, ISC. NANOG 26, October 2002.
- IPv6 Impressions: ARIN Update and Routing Table Overview, by Cathy Wittbrodt, Packet Design. NANOG 26, October 2002.
- IPv6 Basics (Tutorial), by Tony Hain, Cisco. NANOG 26, October 2002.
- Operational Experience with IPv6 Migration, by Akira Kato, ISI. NANOG 22, May 2001.
- IPv6 in Mobile Wireless Networking, by Dana Blair, Cisco. NANOG 21, February 2001.
- IPv6: Why, What, When, Where? (Tutorial), by Steve Deering, Cisco. NANOG 19, June 2000.
- IPv6 Update / ARIN IPv6 Delegation Status, by Bill Manning, ISI, and Michael O'Neill, ARIN. Presentation includes "Penetration Rate of Private Address Space," "Current Use of IPv6 Address Space," and "ARIN IPv6 Delegation Status." NANOG 19, June 2000.
- Panel: Operational Experience with IPv6. Bob Fink, Lawrence Berkeley National Lab (moderator), Rob Rockell, Sprint, Greg Miller, MCI WorldCom, Bill Maton, Communications Research Centre, Sean Mentzer, Qwest. NANOG 19, June 2000.

Google Tech Talks

- Google IPv6 Conference 2008 (video)

IETF v6ops Working Group RFCs

This working group is chartered to develop and publish guidelines for operation of a shared v6/v4 Internet. There are also some Internet Drafts available at the WG website which may be useful.

- Transition Scenarios for 3GPP Networks (RFC 3574) (23359 bytes)
- Unmanaged Networks IPv6 Transition Scenarios (RFC 3750) (48153 bytes)
- Survey of IPv4 Addresses in Currently Deployed IETF Sub-IP Area Standards (RFC 3793) (11624 bytes)
- Introduction to the Survey of IPv4 Addresses in Currently Deployed IETF Standards (RFC 3789) (22842 bytes)
- Survey of IPv4 Addresses in Currently Deployed IETF Internet Area Standards (RFC 3790) (102694 bytes)
- Survey of IPv4 Addresses in Currently Deployed IETF Routing Area Standards (RFC 3791) (27567 bytes)
- Survey of IPv4 Addresses in Currently Deployed IETF Security Area Standards (RFC 3792) (46398 bytes)
- Survey of IPv4 Addresses in Currently Deployed IETF Transport Area Standards (RFC 3794) (60001 bytes)
- Survey of IPv4 Addresses in Currently Deployed IETF Application Area Standards (RFC 3795) (92584 bytes)
- Survey of IPv4 Addresses in Currently Deployed IETF Operations & Management Area Standards (RFC 3796) (78400 bytes)
- Evaluation of Transition Mechanisms for Unmanaged Networks (RFC 3904) (46844 bytes)
- Security Considerations for 6to4 (RFC 3964) (83360 bytes)
- Application Aspects of IPv6 Transition (RFC 4038) (69727 bytes)
- Scenarios and Analysis for Introducing IPv6 into ISP Networks (RFC 4029) (64388 bytes)
- IPv6 Enterprise Network Scenarios (RFC 4057) (33454 bytes)
- Procedures for Renumbering an IPv6 Network without a Flag Day (RFC 4192) (52110 bytes)
- Analysis on IPv6 Transition in Third Generation Partnership Project (3GPP) Networks (RFC 4215) (52903 bytes)
- Basic Transition Mechanisms for IPv6 Hosts and Routers (RFC 4213) (58575 bytes)
- Use of VLANs for IPv4-IPv6 Coexistence in Enterprise Networks (RFC 4554) (23355 bytes)
- ISP IPv6 Deployment Scenarios in Broadband Access Networks (RFC 4779) (188511 bytes)
- IPv6 Enterprise Network Analysis - IP Layer 3 Focus (RFC 4852) (76199 bytes)
- Recommendations for Filtering ICMPv6 Messages in Firewalls (RFC 4890) (83479 bytes)
- Using IPsec to Secure IPv6-in-IPv4 Tunnels (RFC 4891) (46635 bytes)
- Local Network Protection for IPv6 (RFC 4864) (95448 bytes)
- Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status (RFC 4966) (60284 bytes)
- IPv6 Neighbor Discovery On-Link Assumption Considered Harmful (RFC 4943) (16719 bytes)
- IPv6 Transition/Co-existence Security Considerations (RFC 4942) (102878 bytes)

Relevant RIPE NCC Presentations

- [RIPE Labs - IPv6 CPE survey|<http://www.ripe.net/meetings/regional/moscow-2010/presentations/MH-LABS-CPE-20100905.pdf>] (213 KB)
- IPv6 implementation AS8359 (281 KB)

Please add links to other useful documents and presentations.

ARIN XXIII Presentations

Sunday, 26 April 2009

- How To Run IPv6 When All You Have Is IPv4

- [IPv6 Session](#) by Mark Kusters
- [Network Setup](#) by Darren Kara
- [IPv6 Tunnel Brokers](#) by Matt Ryanczak
- [A Dive into IPv6 Implementation for ISP's - Is it that deep?](#) by Aaron Hughes
- [Dual-prong Approach: IPv6 and Dual-stack Lite](#) by Alan Duraid and Yiu Lee

IPv6 at Caribbean Sector

This is the Comment Area for the Caribbean Sector Event

informational comment:

this morning, before the v6 test, I upgraded to Firefox V:3.0.1, and it worked on v6 without any changes! /Lea

Under XP while most websites worked AVG cannot reach its update server. /PLA

Man Climbs Worlds 14 Tallest Peaks

Hirota Takeuchi has gotten official certification for his feat of climbing the worlds 14 tallest mountains. Hes the 30th person ever and the first Japanese person to accomplish the feat.

[Man Climbs Worlds 14 Tallest Peaks](#)

[GoodvilleNews.com](#) - good, positive news, inspirational stories, articles

7 Reasons Why Not Making Mistakes Is The Biggest Mistake

The FEAR of being nothing, achieving nothing and becoming nothing should be way bigger than the fear of making mistakes. A life spent making mistakes is not only more honorable, but more useful than a life spent doing nothing. ~ George Bernard Shaw

[7 Reasons Why Not Making Mistakes Is The Biggest Mistake](#)

[GoodvilleNews.com](#) - good, positive news, inspirational stories, articles

5 Easy Steps to Turn Your Life Into an Abundant Garden

Dont judge each day by the harvest you reap but by the seeds that you plant. ~ Robert Lewis Stevenson It has been my experience that life is what you make of it. You can look at it many ways. It can be like a cup of coffee it is all in how you make it. I have decided to look at my life as a garden because your harvest all depends on what seeds you plant.

[5 Easy Steps to Turn Your Life Into an Abundant Garden](#)

[GoodvilleNews.com](#) - good, positive news, inspirational stories, articles

Mr. Happy Man

For six hours each day, Bermudas Johnny Barnes stands at a busy traffic intersection telling all who pass that he loves them. His delight and sincerity are infectious, and the people of the island love him back. His service is a simple reminder of the power of happiness and loving-kindness to change any day for the better

[Mr. Happy Man](#)

[GoodvilleNews.com](#) - good, positive news, inspirational stories, articles

Cat Saves Owner Hours After Adoption

A newly-adopted cat repaid his owners loving gesture earlier this month by saving her from a medical emergency just hours after he was brought home, the Green Bay Press Gazette reports.

[Cat Saves Owner Hours After Adoption](#)

[GoodvilleNews.com](#) - good, positive news, inspirational stories, articles

IPv6 at ARIN XXIII Comment

Use this page to provide feedback and information about your user experience.

IPv6 at ARIN XXI

Helpful links with IPv6 configuration information:

[NANOG IPv6 Hour - February 2008](#)

[IETF71 IPv4 Outage User Experiences](#)

[APRICOT 2008 Lessons](#)

IPv6 Information Websites:

ARIN's own IPv6 Information Portal

[SixXS IPv6 Deployment & Tunnel Broker](#)

[go6 The IPv6 portal](#)

IPv6 Pre-Game Show:

[Pre-Game Comment Area](#)

IPv6 Main Event:

[Main-Event Comment Area](#)

Network Setup:

[Network Setup Overview](#)

Statistics from the ARINXXI IPv6 Event:

[IPv6 Network Statistics](#)

IPv6 at ARIN XXI Main-Event

Vista

- Still "just works".
- Same caveats as in the [pre-game](#) .
- Google Earth works, although it's almost certainly not native.

Windows XP

- Brand new XP install connected without issue to the XP network.
 - IM (AOL/Trillian) or MSN (Native Client) didn't connect
 - PPTP does not work
 - Youtube videos do not play
 - Firefox and IE seem fine.
 - IMAP/SMTP via Thunderbird using SSL/TLS works
 - Windows Media Player 10 can stream audio (http/mp3) from a native IPv6 web server
- Was able to connect only after the following:

```
Microsoft Windows XP Version 5.1.2600
(C) Copyright 1985-2001 Microsoft Corp.

C:\Documents and Settings\cgrundemann>netsh interface ipv6 install
An extended error has occurred.
C:\Documents and Settings\cgrundemann>esentutl /p %windir%\security\Database\secedit.sdb
...
Operation completed successfully in 5.141 seconds.

C:\Documents and Settings\cgrundemann>netsh interface ipv6 install

Ok.

C:\Documents and Settings\cgrundemann>
```

- Firefox and IE both working
- As expected: no IM (Pidgen with AIM, Yahoo and Google accounts), corporate VPN not available
- Downloaded a PDF from APNICs site
- Was able to login (both individual and chapter admin) and navigate [www.ISOC.org](#) - everything seems to work!
- Was able to log in and post to a Word Press weblog hosted by [NearlyFreeSpeech.net](#)

MacOS

- See [pre-game](#) for already-known issues.

Linux

- Add a comment!

Other OSes

- Add a comment!

Misc

- Note: The link for the linux NAT-PT software in the preso was wrong. Correct URL is <http://www.lucastomicki.net/naptd.php>
- Flash details: Flash Media Server 3 will support v6, but I can't find evidence that the client will anytime soon.

IPv6 at ARIN XXI Pre-Game

OS X 10.5 and 10.4(.11)

- works after following instructions in handout and also disabling v4
- native software update works
- Fix for Firefox works
- The Cisco VPN version 4.9 has error 51. Says to make sure there is an active network interface with an IP address
- Mac Mail works for IMAP/SSL and SMTP/SSL
- [Mulberry mail](#) does not work (confirmed by author)
- Youtube videos don't play. I'm guessing the flash plugin is v4 only.

Vista

- "just works".
- IM protocols (AIM, YIM) cannot connect.
- Windows Update is broken.
- SSH works
- Citrix does not work (blocked?)
- YouTube videos won't play on Vista either.

Linux/Ubuntu 7.10 Gutsy Gibbon

- not working – anyone have it running???
- I got this to work (finally) by completely disabling the GNOME network manager. You can disable network manager by doing the following:

Stop network manager

```
sudo /etc/dbus-1/event.d/26NetworkManagerDispatcher stop
sudo /etc/dbus-1/event.d/25NetworkManager stop
```

Create these files:

```
echo "exit" > /etc/default/NetworkManager
echo "exit" > /etc/default/NetworkManagerDispatcher
```

Once you do this you will have to setup your machines network manually.

IPv6 at ARIN XXI Stats

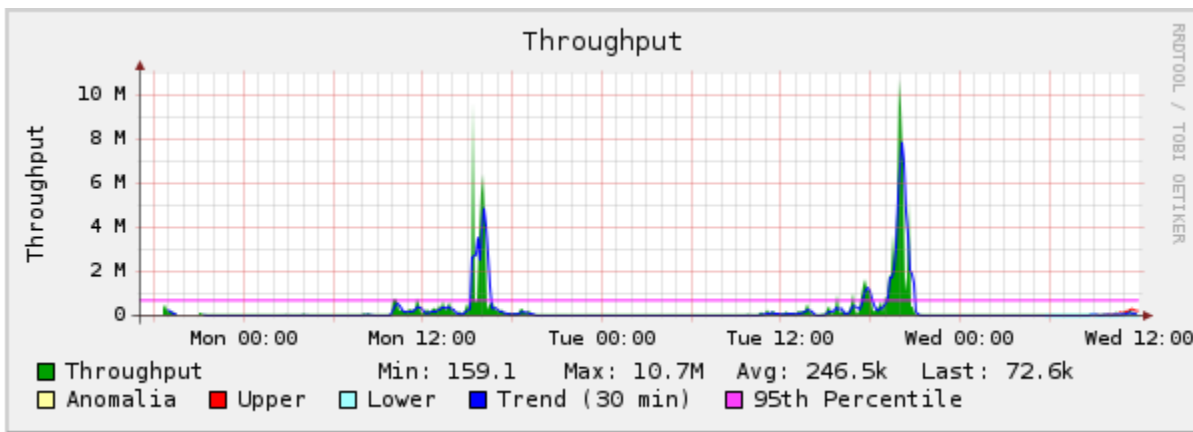
We actively monitored the IPv6 networks throughout the meeting and we have some statistics to share as a result.

Everyone likes lists so we'll start with the top 25 domains queried on the IPv6 networks during the meeting. The results are not purely indicative of where people were pointing their web browsers to because of reverse DNS which accounts for arin.net being the number one domain on the list.

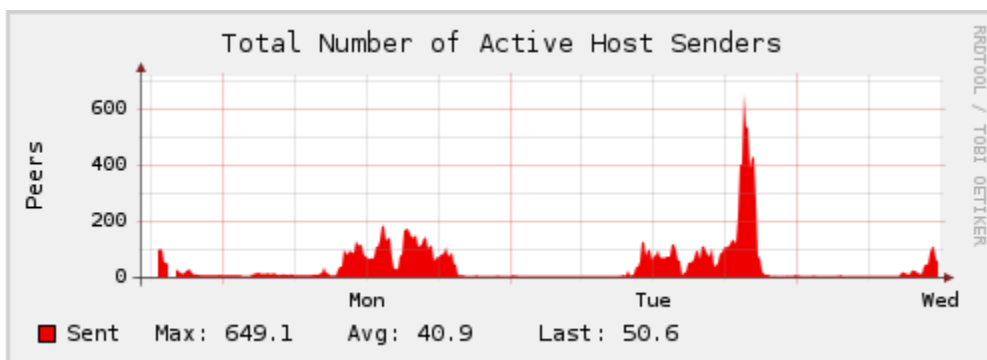
Top 25 Domains

- arin.net
- google.com
- savvis.net
- integer.com
- gov.ms
- hotmail.com
- yahoo.com
- aol.com
- wayport.net
- sover.net
- facebook.com
- cnn.com
- mac043.local
- es.net
- boeing.com
- google-analytics.com
- atdmt.com
- microsoft.com
- co.uk
- revsci.net
- verizon.com
- apple.com
- windows.com
- msn.com
- wired.com

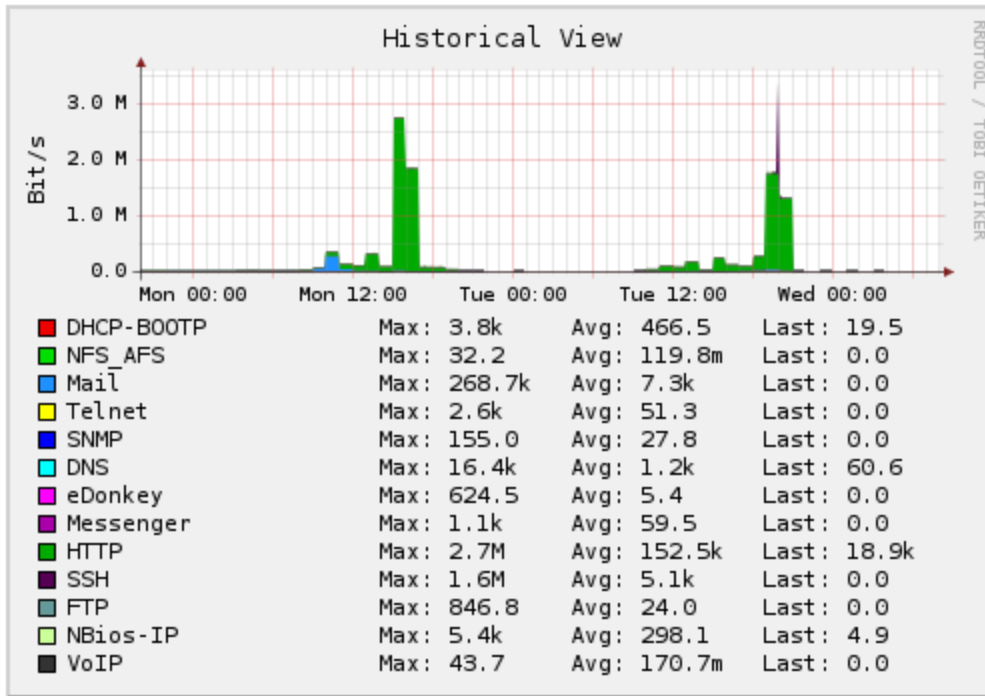
The most widely used protocol was HTTP following by DNS and various mail and instant messaging protocols. We saw very little SSH and other such traffic which implies that not many people were attempting to do work over the IPv6 networks. The fact that NAT-PT breaks most (if not all) VPN clients probably has something to do with that. Throughput on the IPv6 networks was greatest during the IPv6 Main Event on Tuesday evening though the following throughput graph does make it apparent that people were using the IPv6 only networks throughout the meeting.



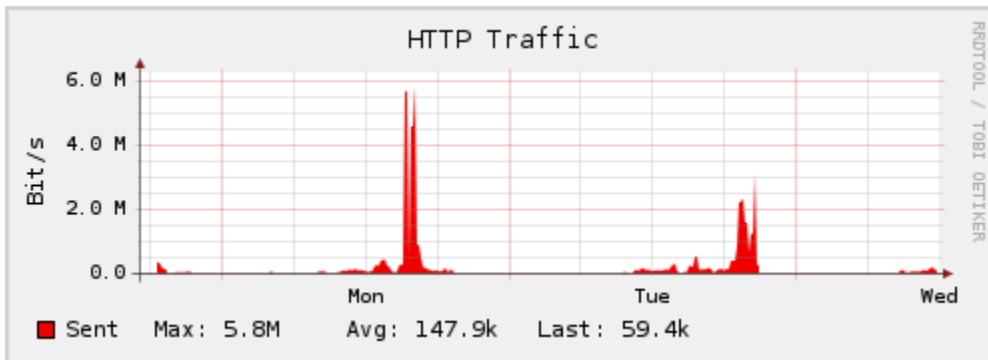
This next graph shows the number of hosts sending data over the IPv6 networks. It shows both local and remote hosts. This gives a clear picture of when the network was in use during the meeting. You can clearly see the spike in usage during the IPv6 Main Event.



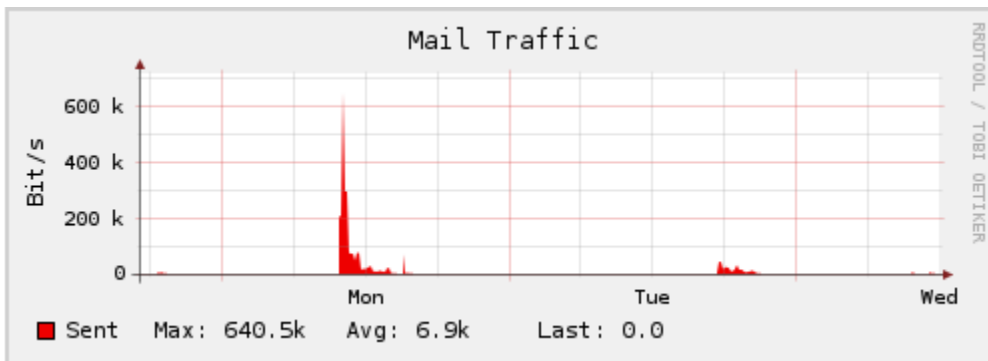
The next graph shows protocol usage. Unfortunately HTTP dominates this graph making it difficult to determine what other protocols were used. We'll post individual protocol graphs in an attempt to make up for that.



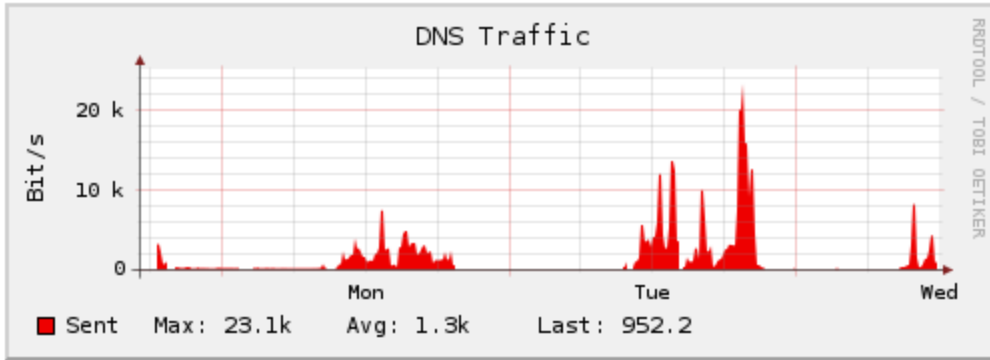
Here's a graph of HTTP traffic only. HTTP was the dominate protocol in use. The huge spike on Monday was a certain systems admin downloading Linux ISOs.



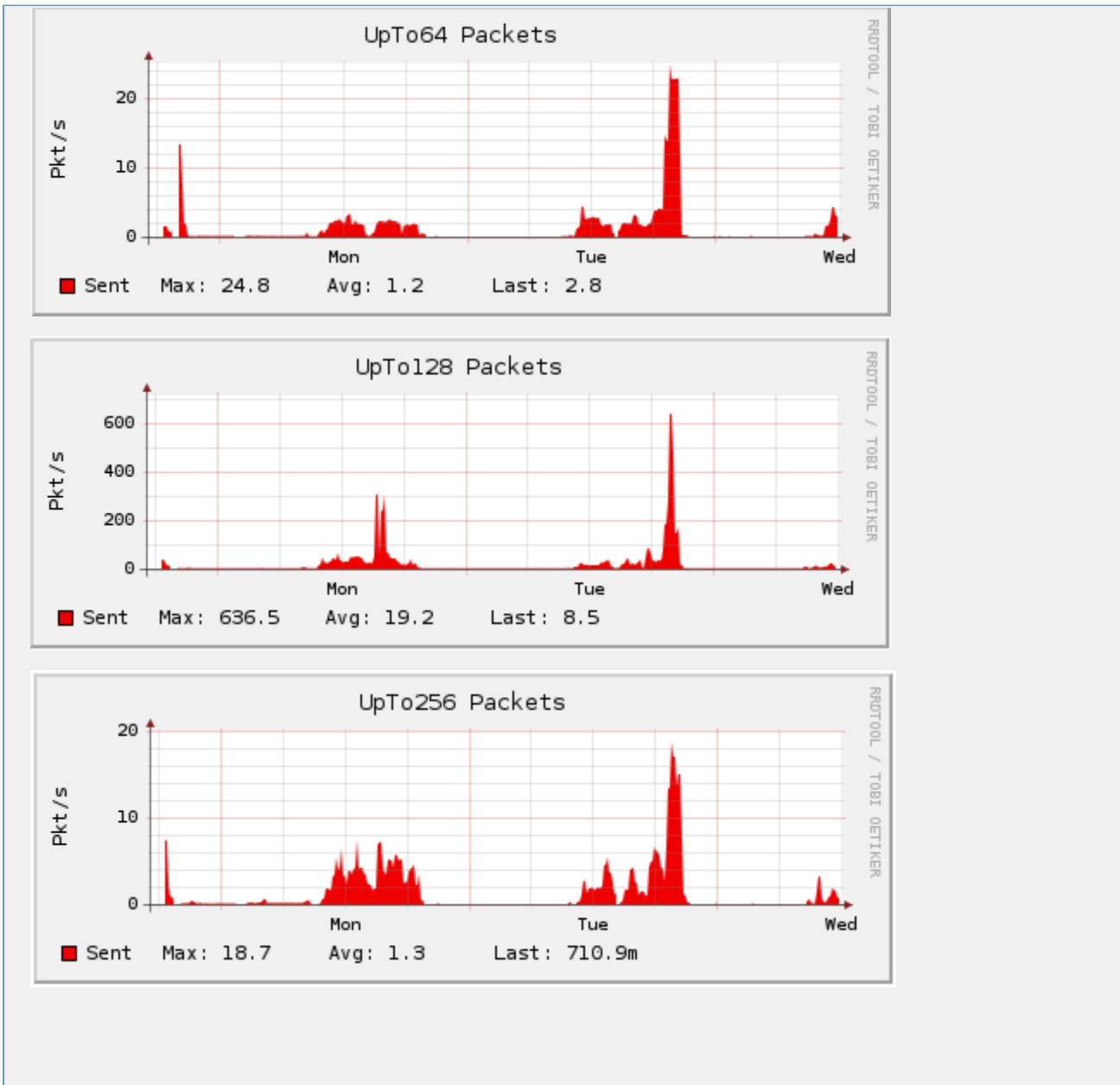
Email protocols were the second most popular application protocol used on the IPv6 network. The following graphs show traffic for SMTP, POP3 and IMAP.

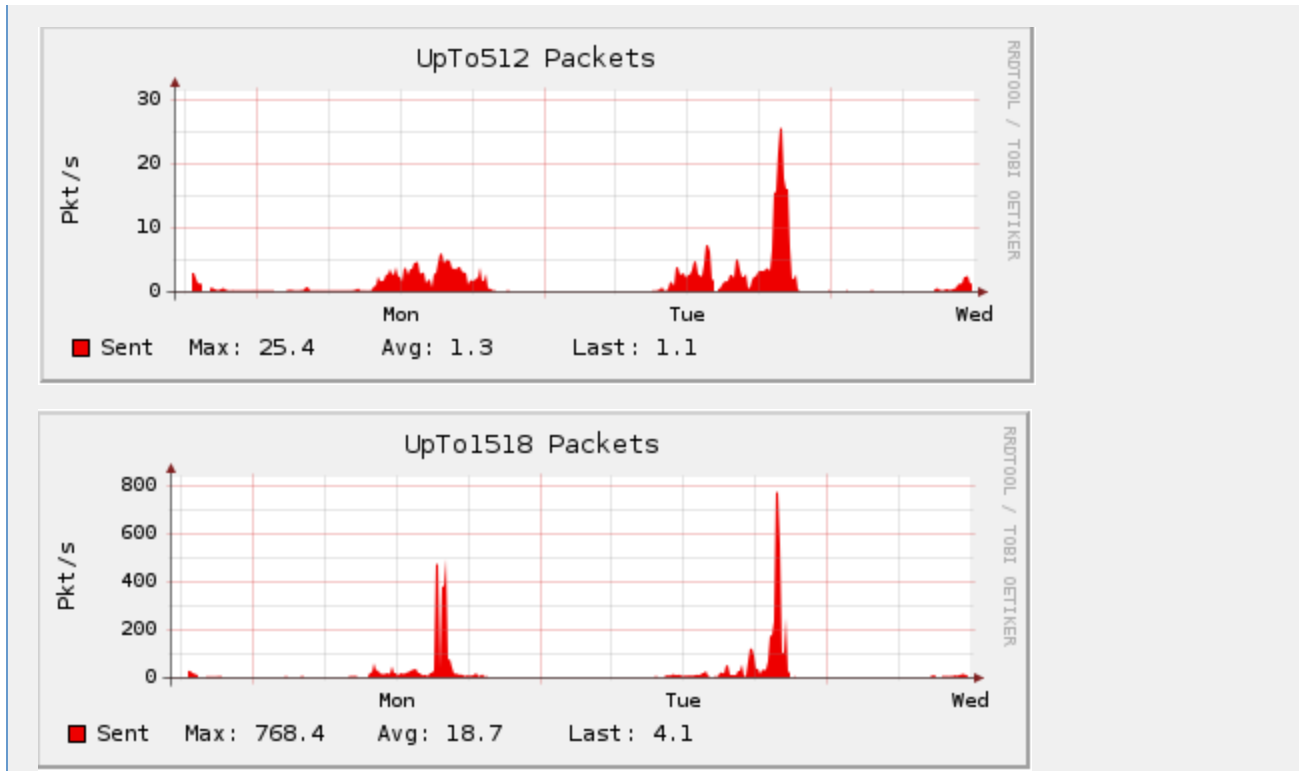


Here's a graph depicting DNS traffic during the meeting. Again, there is a clear spike during the IPv6 Main Event.



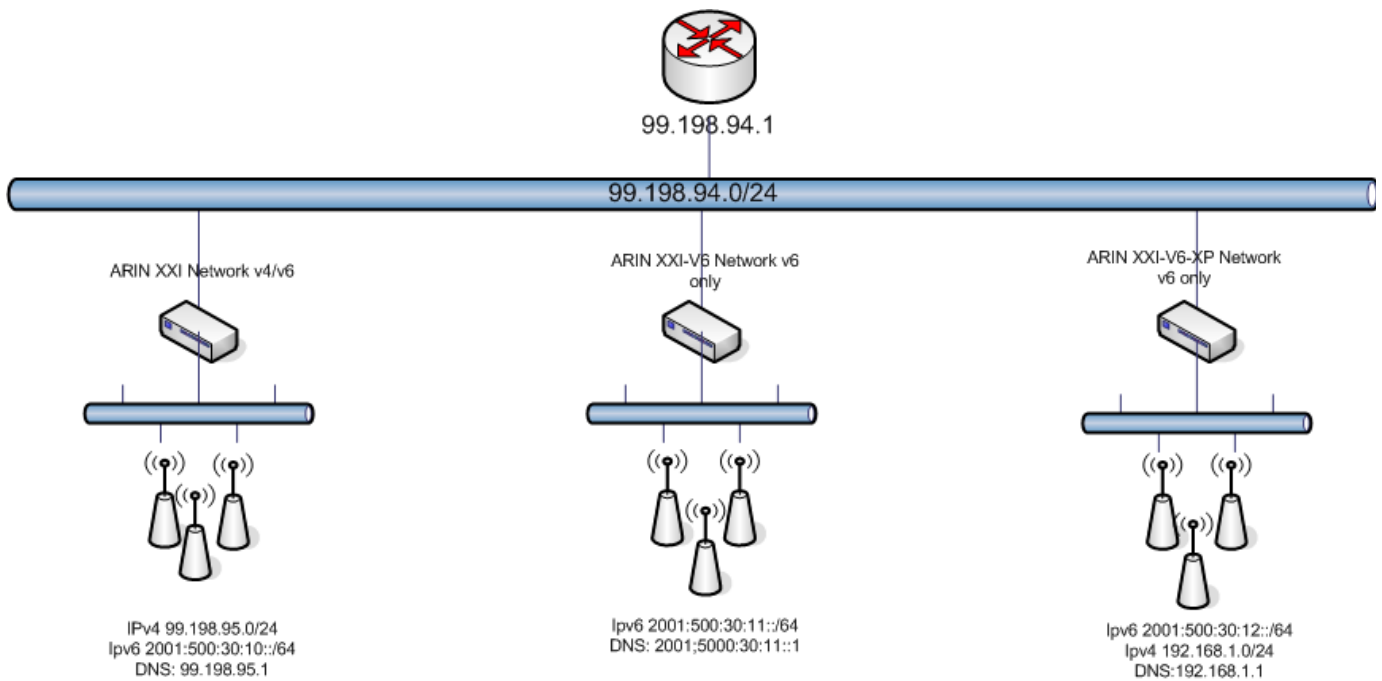
The following graphs show the various packet sizes seen during the meeting.



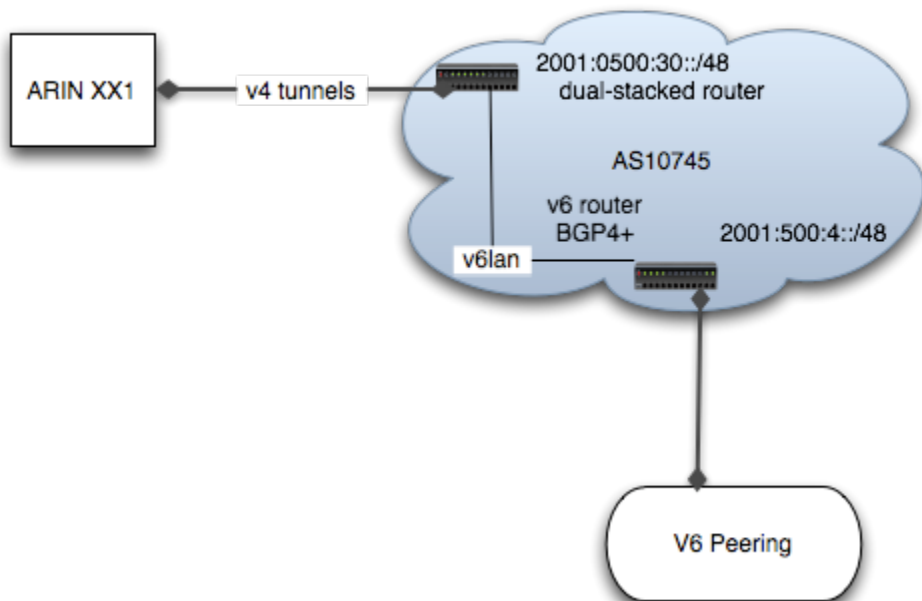


IPv6 at ARIN XXI Network-Setup

The network at ARIN XXI was a bit more complex than a typical ARIN meeting network. In order to facilitate the IPv6 event we designed what amounts to three separate networks for ARIN XXI. These networks had three separate SSIDs: ARINXXI, ARINXXI-V6 and ARINXXI-V6-XP. The following diagram gives a view of the network topology.



IPv6 transit on each network was provided by tunnels back to the ARIN offices in Virginia where we have IPv6 transit through OCCAID via the Equinix IPv6IX. The following diagram depicts the IPv6 tunnel configuration.



ARINXXI: The primary network supported both IPv4 and IPv6. IPv4 addresses and DNS servers were assigned via DHCPv4 while IPv6 addresses were assigned using RA. IPv4 address space and transit was provided by our sponsor, Wild Blue. IPv6 address space and transit was provided by a tunnel back to the ARIN offices. This machine did not have any special configuration. It was set up as a Linux based router with radvd providing IPv6 addresses advertisements to clients and BIND 9 providing DNS services. The IPv6 tunnel and routing were handled using standard Linux mechanisms.

IPv4 and IPv6 packet forwarding were enabled:

```
echo "1" > /proc/sys/net/ipv6/conf/all/forwarding
echo "1" > /proc/sys/net/ipv4/conf/all/forwarding
```

The IPv6 Tunnel was setup:

```
ifconfig sit0 up
ifconfig sit0 inet6 tunnel ::199.43.0.65
ifconfig sit1 up
ifconfig sit1 inet6 add 2001:500:30::2/64
route -A inet6 add ::0 dev sit1
```

You also need to assign an IPv6 address to the internal Ethernet Interface:

```
ifconfig eth0 inet6 add 2001:500:30:10::1/64
```

radvd.conf contained:

```
interface eth0
{
  AdvSendAdvert on;
  MinRtrAdvInterval 5;
  MaxRtrAdvInterval 15;
  prefix 2001:500:30:10::/64
  {
    AdvOnLink on;
    AdvAutonomous on;
  };
};
```

Bind was setup as a recursive name server listening on both IPv4 and IPv6.

ARINXX-V6: The ARINXX-V6 network was configured to support only IPv6 on the local network segment (No IPv4 for clients at all). This network provided connectivity to the IPv4 Internet by using NAT-PT and the TOTd DNS gateway. The IPv6 transit and address space for this network was provided by a tunnel to the ARIN offices. The IPv4 transit which was required for NAT-PT was provided by the meeting sponsor. We used a Linux box as the gateway device for this network. DHCPv6 services were used to provide clients which supported DHCPv6 a DNS server.

Those clients that did not support DHCPv6 were required to be configured their DNS server manually. The Linux box ran an implementation of NAT-PT which is available from <http://www.lucastomicki.net/naptd.php>. The Linux machine also ran a DNS application layer gateway (DNS ALG) named TOTd, or Trick or Treat Daemon. The TOTd application is basically a DNS proxy that provides a NAT-PT compatible AAAA record for hosts that do not return a valid AAAA record when a DNS query is performed. This allows the NAT-PT daemon to provide the translation necessary to connect to an IPv4 only resource from an IPv6 only client. While the basic configuration of this Linux gateway was pretty standard things get a bit complicated when using the naptd daemon. The following configuration details will hopefully help you along if you would like to set this up yourself.

IPv6 packet forwarding must be enabled:

```
echo "1" > /proc/sys/net/ipv6/conf/all/forwarding
```

The IPv6 Tunnel was setup (You will need to have your own tunnel endpoint to define in line two):

```
ifconfig sit0 up
ifconfig sit0 inet6 tunnel ::199.43.0.65
ifconfig sit1 up
ifconfig sit1 inet6 add 2001:500:30::2/64
route -A inet6 add ::0 dev sit1
```

and an IPv6 address was assigned to the internal Ethernet Interface:

```
ifconfig eth0 inet6 add 2001:500:30:10::1/64
```

radvd.conf contained:

```
interface eth0
{
  AdvSendAdvert on;
  AdvManagedFlag off;
  AdvOtherConfigFlag on;
  MinRtrAdvInterval 10;
  MaxRtrAdvInterval 30;
  prefix 2001:500:30:11::/64
  {
    AdvOnLink on;
    AdvAutonomous on;
  };
};
```

We found that radvd had to be up and running in order for DHCPv6 to work properly. It appeared the ISC dhcpd (4.1.0a1) wanted to see an RA before it would do its thing.

dhcpd.conf:

```
default-lease-time 1800;
max-lease-time 1800;
ddns-update-style none;
authoritative;
log-facility local7;
option dhcp6.name-servers 2001:500:30:11::1;
subnet6 2001:500:30:11::/64 { }
```

dhcpd was also started with the following command line options:

```
dhcpd -6 -cf /usr/local/etc/dhcpd.conf
```

The DNS ALG (TOTd) was configured as follows:

```
; DNS Server to use for resolution
forwarder 99.198.94.4 port 53
; Prefix to use for nat-pt hosts
prefix 2000:ffff::
; port to listen on
port 53
pidfile /var/run/totd5005.pid
totuser nobody
; 6to4 reverse lookup setting
stf
```

The nat-pt application does not use text based configuration files. It provides a tool that generates a binary configuration file. What follows is a log of the answers we supplied to the configuration generator for our network. We tried a lot of the different setups in our lab and we found the the only setup the worked reliably was a very basic configuration (we accepted the defaults).

naptd-confmaker log:

```

Ataga IPv4/IPv6 NAPT Configuration Maker
(c) 2005 by Lukasz Tomicki <tomicki@o2.pl>
Do you want to create a new configuration? Y/n
y
Do you want IPv4 addresses from the outside interfaces to be automatically used as part of the NAT pool? Y/n
y
Do you want to configure additional address as part of your NAT pool? y/N
n
Do you want to create a pool of public IPv4 addresses that will allow incoming connections to be dynamically mapped to appropriate IPv6 addresses? y/N
n
Do you want to create static mappings of public IPv4 addresses that will allow incoming connections to reach IPv6 hosts? y/N
n
Enter the name of the first inside (IPv6) interface that you want NAT-PT to listen on.
interface (eth0 eth1 sit0 sit1): eth0
eth0
Do you want to enter more interfaces? y/N
n
Enter the name of the first outside (IPv4) interface that you want NAT-PT to listen on.
interface (eth0 eth1 sit0 sit1): eth1
eth1
Do you want to enter more interfaces? y/N
n
Enter the TCP translation timeout in seconds 86400:
Enter the UDP translation timeout in seconds 3600:
Enter the ICMP translation timeout in seconds 30:
Enter the IPv6 prefix that will be used as the destination for translations.
prefix 2000:ffff
Please enter the IPv4 address of the DNS server you are currently using.
IPv4 DNS server: 99.198.94.4
99.198.94.4
You can configure hosts for automatic DNS translation by using the DNS server below.
IPv6 DNS Server: 2000:ffff::63c6:5e04
Thank you for choosing Ataga as you IPv4/IPv6 NAT-PT solution.
Setup is now complete. Type 'naptd' to start NAT-PT.

```

Several iptables rules are required to make the NAT-PT daemon work properly. This is because the daemon is running in use ... \n

IPv6 at ARIN 21

1. REDIRECT IPv6 at ARIN XXI

IPv6 in the News

IPv6 in the News – Google News Hits

Could not retrieve <http://www.google.com/news?q=IPv6&ie=UTF-8&output=rss> - Page not permitted.

Archived News Items

28-Sep-10	Federal Government IPv6 transitions in 2012 and 2014 (PDF)
14-Aug-10	IPv6 accessibility & address for your IPv4 website
01-Oct-09	IPv6 support for cloud computing services by 3Tera
16-Sept-08	
11-Sept-08	
16-Apr-08	Sound the alarm, IPv6 execs say
16-Apr-08	Industry execs sound IPv6 alarm—is the sky really falling?

16-Apr-08	IPv6 exec says sound the alarm	
2-Apr-08	U.S. carriers quietly developing IPv6 services (Network World)	
1-Apr-08	Work on IPv6 integration and migration surges	
1-Apr-08	IPv6: It's Time to Make the Move	
29-Mar-08	IPv6... A Pre-Game Show in Denver and Featured at the Geneva Auto Show	
28-Mar-08		
28-Mar-08	[No More IP's for Web?	http://www.webpronews.com/topnews/2008/03/31/no-more-ip%E2%80%99s-for-web
14-Mar-08	The Internet's Space Shortage	
12-Mar-08	Nigeria: Use of IPv4 Declines - Report	
12-Mar-08	What the U.S. is missing by ignoring IPv6	
11-Mar-08	The IPv6 experience: Are you experienced yet?	
13-Feb-08	Could IP address plan mean another IPv6 delay?	
4-Feb-08	Overhaul of net addresses begins	
4-Feb-08	IP Version 6 switches on	
4-Feb-08	IP addresses: A wasted resource?	
28-Jan-08	EU Ponders Privacy of Internet Addresses	
23-Jan-08	Get IPv6 skills now rather than later	
23-Jan-08		
17-Jan-08		
17-Dec-07	How feds are dropping the ball on IPv6	
26-Oct-07		
29-Aug-07	IPv6 Checkup Time	
6-Aug-07		
3-Aug-07	For online users, a looming shortage of IP addresses	
29-Jun-07	IPv6 D-Day is coming up fast	
27-Jun-07	IP address timebomb	
18-Jun-07		
15-Jun-07	Concerns grow over IPv6 migration	
14-Jun-07	More IPv6 Warnings on Why Organizations Must Plan Transition Now	
29-May-07	The Internet is Running Out of Addresses	
25-May-07	ARIN Urges IPv6 Upgrades	
22-May-07		
21-May-07	ARIN: It's time to migrate to IPv6	

21-May-07	
5-Feb-07	DOD to allocate its IPv6 addresses
(dates vary)	

Global IPv6 Survey

ARIN and the Cooperative Association for Internet Data Analysis (CAIDA) worked together to conduct a survey to capture global IPv6 penetration data. The survey took place in September of 2008 and an analysis of the results was presented by kc claffy of CAIDA during the ARIN XXII meeting in Los Angeles, California on October 15, 2008.

Below are links to kc claffy's presentation of the results, and a copy of the survey questions and possible responses. Both documents are in PDF format.

- [Presentation of Global IPv6 Penetration Survey Results](#)
- [Global IPv6 Penetration Survey Questions and Possible Responses](#)

[<< Back to Main Page](#)

IPv6 Penetration Survey Results

ARIN and the Cooperative Association for Internet Data Analysis (CAIDA) worked together to conduct a survey to capture IPv6 penetration data in the ARIN region. The survey took place in March of 2008 and an analysis of the results was presented by kc claffy of CAIDA during the ARIN XXI meeting in Denver, Colorado, last week.

Below are links to kc claffy's presentation of the results, and a copy of the survey questions and possible responses. Both documents are in PDF format.

- [Presentation of IPv6 Penetration Survey Results](#)
- [IPv6 Penetration Survey Questions and Possible Responses](#)

Dynamically updated information on IPv6 penetration:

- [LACNIC's IPv6 graph dashboard aggregating graphs from multiple sites](#)
- [DE-CIX's graph of IPv6 traffic](#)
- [NIST's report on U.S. Government, Industry, Education, and Departmental deployment of IPv6 on dns, mail and web domains](#)
- [AMS-IX's graph of traffic by Ethertype](#)
- [BGPmon's IPv6 weathermap](#)
- [Martin Levy's \(Hurricane Electric\) Google IPv6 statistics](#)
- [Google's IPv6 statistics](#)
- [Eric Vyncke's estimation of IPv6 brokenness \(since yesterday, week, month, and all time\)](#)
- [RIPE graph that shows percentage of networks \(ASes\) that announce an IPv6 prefix](#)
- [IPv6 Matrix](#)
- [AAAA and IPv6 connectivity statistics of top websites according to Alexa](#)
- [Percentage of top-100 Alexa sites worldwide and major countries that are IPv6 accessible by Lars Eggert \(dynamically updated daily\)](#)
- [Wikimedia IPv6 stats](#)
- [IPv6 Measurements by Geoff Huston \(dynamically updated\)](#)
- [Tore Anderson of Redpill Linpro AS "IPv6 dual-stack client loss in Norway" \(dynamically updated regularly\)](#)
- [Hurricane Electric "Global IPv6 Deployment Progress Report" \(dynamically updated\)](#)
- [IPv6 BGP Operational Report from UNINETT \(dynamically updated\)](#)
- [IPv6 DFP visibility by SixXS \(dynamically updated\)](#)
- [Comcast "IPv6 Adoption Monitor" \(dynamically updated\)](#)
- [IPv6 BGP Table Size by Geoff Huston \(dynamically updated\)](#)
- [IPv6/IPv4 Comparative AS Statistics by Geoff Huston \(dynamically updated\)](#)

- IPv6 allocations and prefixes on RIPE's IPv6 ACT NOW (dynamically updated)
- University of Pennsylvania "IPv6 Adoption Monitor" (dynamically updated)
- IPv6 Status Survey (dynamically updated)
- IPv6 Deployment Aggregated Status (dynamically updated)
- IPv6 deployment in Swedish municipalities (dynamically updated)
- IPv6 deployment in Swedish authorities (dynamically updated)
- (Older) RIPE page that tracks eight sites (dynamically updated)

Reports or write-ups on IPv6 penetration:

- Google presentation at RIPE 65
- The Measurement Factory: "IPv6 SURVEY: OCTOBER 2011"
- Arbor Networks report "Six Months, Six Providers and IPv6" (April 2011)
- RIPE Labs "Members and Number Resources, One Year Later" (March 2011)
- BGPExpert's 2010 IPv6 Address Use Report
- RIPE Labs "Interesting Graph - Networks with IPv6 over Time" (November 2010)
- Executive summary of IPv6 matrix presented at INET London (September 2010)
- New Zealand "IPv6 Readiness Survey 2010"
- Percentage of global top-30 websites (based on Alexa traffic ranking) that offer services on IPv6 networks
- RIPE Labs "IPv6 Ripeness - First Steps"
- RIPE Labs "IPv6 Allocations since 1999"
- RIPE "Measuring IPv6 usage at web clients and DNS resolvers"
- "IPv6 at web clients and caching resolvers" from RIPE 60 (May 2010)
- Renesys "IPv6: Are we there yet?" (April 2010; excerpts from their Market Intelligencer)
- ISOC column by Geoff Huston (April 2010)
- OECD report "INTERNET ADDRESSING: MEASURING DEPLOYMENT OF IPv6" (April 2010)
- Passive and Active Measurement Conference paper by Google "Evaluating IPv6 Adoption in the Internet" (April 2010)
- Tore Anderson of Redpill Linpro AS' posting on IPv6 brokenness
- RIPE Labs "Measuring IPv6 at Web Clients and Caching Resolvers" (March 2010)
- isc.sans.org IPv6 support (January 2010)
- RIPE Labs "IPv6 Deployment Survey" from RIPE 59 (October 2009)
- Google "IPv6 at Google: a case study" (July 2009)
- NRO "Measuring IPv6 Deployment" by Geoff Huston & George Michaelson (June 2009)
- BGPmon "New IPv6 deployment statistics" (April 2009)
- Elliott Karpilovsky, Alexandre Gerber, Dan Pei, Jennifer Rexford, and Aman Shaikh, "Quantifying the extent of IPv6 deployment," in Proc. Passive and Active Measurement Conference (April 2009)
- Google "IPv6 at Google" from RIPE 58 (May 2009)
- Google "Global IPv6 statistics" from RIPE 57 (October 2008)
- "AMS-X IPv6 traffic trends" from RIPE 57 (October 2008)
- "IPv6 usage in Sweden" from RIPE 57" (October 2008)
- Arbor Networks report "Tracking the IPv6 migration" (August 2008)
- "The End is Near, but is IPv6?" by Craig Labovitz (August 2008)
- "IPv6 Deployment: Just where are we?" by Geoff Huston & George Michaelson (April 2008)

- [A macroscopic snapshot of the IPv6 Internet topology - CAIDA report \(2008\)](#)
- [RIPE Labs "IPv6 Measurements - A compilation" \(links to other reports\)](#)

IPv6 routing table

- [Snapshot comparison of IPv6 routing table sizes](#)

[<< Back to Main Page](#)

Book Reviews

There are a variety of books on IPv6, some of which are obsolete, and others which discuss IPv6 from a particular point of view. We would like this site to develop a comprehensive set of reviews of all these books to help people choose which ones are most appropriate to fill gaps in their knowledge.

Please feel free to add any comments to these pages based on your experience of the book. Also, please feel free to include links to publisher sites, but do not include links to booksellers.

Printed Books

Note that these may also be available in downloadable versions from the publisher

- [Migrating to IPv6](#)
- [IPv6 Essentials](#)
- [IPv6, Theorie et pratique](#)
- [Running IPv6](#)
- [Guidelines for the Secure Deployment of IPv6](#)
- [Guide to TCP/IP, 4th Edition](#)
- [Understanding IPv6, Third Edition](#)

Free or Downloadable Books

- [An IPv6 Deployment Guide](#)
- [Internetworking IPv6 With Cisco Routers](#)
- [Review__Day One__Exploring IPv6](#)

An IPv6 Deployment Guide

An IPv6 Deployment Guide *edited by Martin Dunmore*

This is a free publication by the European 6NET consortium and is [available as a downloadable PDF](#).

The information contained in this book is taken from the project's deployment cookbooks and other deliverables. Since each cookbook/deliverable generally concentrates only on specific IPv6 features or deployment scenarios (e.g. site transition, multicast, mobility, DHCP, routing etc.), we believe that providing all the important information in a single reference book is much more preferable to the reader than negotiating our multitude of project deliverables.

Day One: Advanced IPv6 Configuration

Day One: Advanced IPv6 Configuration is an ebook published by Juniper Networks. You can download a free PDF copy [here](#). If you are not a J-Net member, you must create an account for the download.

Chris Grundemann wrote this ebook as a follow up to [Day One Exploring IPv6](#). The material resumes where the previous guide concluded. The author enhances the test bed used in the first book. The topics covered in this ebook follow.

- BGP Routing with IPv6 (native + IPv6 over IPv4 peering)
- DHCPv6
- VRRP for IPv6
- Class of Service (COS) for IPv6
- Multicast Listener Discovery

If you enjoyed the first book, this book is worth perusing. You can quickly get up to speed on intermediate IPv6 topics and their configuration in JUNOS.

Day One Exploring IPv6

Day One: Exploring IPv6 is an ebook published by Juniper Networks. You can download a free PDF copy [here](#). If you are not a J-Net member, you must create an account for the download.

Chris Grundemann, the author the book, covers IPv6 topics such as addressing, neighbor discovery, and stateful autoconfiguration before delving into IPv6 configuration and troubleshooting in JUNOS. For example purposes, the author uses a test bed that progresses into a more production-like environment with the introduction of dynamic routing protocols.

The book is a great way for network operators to get familiar with IPv6 and configuration/troubleshooting in JUNOS. Readers who enjoy Chris's presentation of the material can read his follow-up book on IPv6, [Day One__Advanced IPv6 Configuration](#) .

IPv6 Essentials

IPv6 Essentials *by Silvia Hagen*

Recommended by Brian Carpenter, former chair of the IETF and former IAB member, as being pretty much up to date.

Migrating to IPv6

Migrating to IPv6 *by Marc Blanchet*

Recommended by Brian Carpenter, former chair of the IETF and former IAB member, as being pretty much up to date.

Running IPv6

Running IPv6 is a book published in 2006 which includes detailed information for implementers of IPv6 on [Cisco](#), [Windows](#), [Linux](#), [FreeBSD](#), and [MacOS X](#). It was written in English by [Iljitsch van Beijnum](#) and published and distributed by [Apress](#). The ISBN is **1-59059-527-0**.

The book focuses on implementation specifics including in certain applications such as the [ISC BIND name server](#). It also contains references to the appropriate [RFCs](#) and technical details about the protocol, and has a troubleshooting section designed to assist individuals and organizations working to roll out IPv6 on their systems and networks. It does not cover programming.

External links

- [The book's official website](#)
- [Apress website](#)

IPv6, Theorie et pratique

IPv6, Théorie et Pratique *by Gisèle Cizault*

This book, published by [O'Reilly](#) is being maintained up to date on the web in a [wiki version](#).

Internetworking IPv6 With Cisco Routers

Internetworking IPv6 With Cisco Routers *by Silvano Gai*

This book is being made available in full on the web [here](#) with the following warning:

The book has not been updated to the most recent version of the IPv6 standards

It is also available [in Italian](#).

Guide to TCP/IP, 4th Edition

Guide to TCP/IP, 4th Edition *by Jeffrey L Carrell, Laura Chappell, Ed Tittel, James Pyles*

Published by Cengage Learning, Sept 2012

ISBN-13: 9781133019862

http://www.cengage.com/search/productOverview.do?Ntt=1418371055155368746018982760831253759204&N=16+4294922389+4294966692&Ns=P_Product_Title|0&Ntk=P_EPI

Guide to TCP/IP, Fourth Edition introduces students to the concepts, terminology, protocols, and services that the Transmission Control Protocol/Internet Protocol (TCP/IP) suite uses to make the Internet work.

This text stimulates hands-on skills development by not only describing TCP/IP capabilities, but also by encouraging students to interact with protocols.

It provides the troubleshooting knowledge and tools that network administrators and analysts need to keep their systems running smoothly.

Guide to TCP/IP, Fourth Edition covers topics ranging from traffic analysis and characterization, to error detection, security analysis and more. Both IPv4 and IPv6 are covered in detail.

Lots of packet capture examples and the trace files are available for download.

What's New since 3rd Edition:

- Significant increase in IPv6 coverage since 3rd Ed!
- New primary focus on IPv6 includes: IPv6 addressing, subnetting, and automatic addressing facilities, IPv6 header architecture, MTU and packet handling, IPv6 routing, ICMPv6, NDP in IPv6, changes in TCPv6, plus upper-layer IPv6 protocols.
- Hands-on protocol analysis now utilizes Wireshark.
- Improved analysis problems, study/review questions, and updated labs to reinforce learning and retention of key material.

Understanding IPv6, Third Edition

Understanding IPv6, Third Edition *by Joseph Davies*

Published by Microsoft Press, June 2012

ISBN-13: 9780735659148

<http://www.microsoft.com/learning/en-us/book.aspx?ID=15814>

Your essential guide to deploying IPv6 on Windows® networks

Get in-depth technical information to put IPv6 technology to work—including networks with hardware running Windows 8 and Windows Server® 2012. Written by a networking expert, this reference explains IPv6 features and benefits, and provides detailed information to help you implement this protocol. You will learn best practices for using IPv6 services in your Windows network, whether you are an IT professional, a network administrator, or an IT student. Discover how to:

- Use Windows features and tools to implement IPv6 on your network
- Set up a test lab to experiment with IPv6 configuration and functionality
- Understand dynamic routing and the IPv6 routing protocols
- Use IPv6 transition technologies to support both IPv4 and IPv6 during deployment
- Implement IPv6 security features and measures
- Deploy native IPv6 connectivity to an IPv4-only intranet
- Apply best practices from the Microsoft corporate network case study
- Test your understanding of IPv6 concepts with end-of-chapter quizzes

Educating Yourself about IPv6

At this point in time, there are not enough people with both IPv6 experience, and training skills, to provide you with IPv6 training in the same way that you earn a CCIE. Of course, router vendors can teach you how to configure their devices and they do provide a wealth of published material that covers some of the experience of IPv6 pioneers. However, we are just beginning to see significant deployment of IPv6 in the real world harsh operational conditions of the Internet. This is likely to raise any number of issues which were unknown to the people who wrote existing books and training materials.

Documenting the problem: IPv4 exhaustion/depletion

- [Geoff Huston](#) (more conservative)
- [Hurricane Electric](#) (more aggressive)
- [The IPv4 depletion site](#) (most aggressive)
- [InfoWeapons](#) (must complete form to download whitepaper) (more aggressive)
- [Cisco's Tony Hain](#)
- [CAIDA](#) (older analysis)

Papers and Presentations

You must make a commitment to seek out the up-to-date experience of other people who are on the same journey as you, scaling up IPv6 to replace IPv4 in the Internet. A lot of this up-to-date material will be in published papers and conference presentations. We hope that you will share links to that material here.

There are about 200 papers and presentations on IPv6 available from [the IPv6 Eprints Server](#).

The Defense Research and Engineering Network (DREN) has published an [IPv6 Security Assessment](#).

Since IPv6 was first introduced, there have been many changes to the protocol with many RFCs updated or deprecated. Unfortunately, this means that some books have incorrect information, and even recent authors may have the wrong impression about how IPv6 should be implemented/deployed. Brian Carpenter from the IETF recommends these two books as containing the most up to date explanations of IPv6.

- IPv6 for all (free book). Available in English and other languages.
- Migrating to IPv6 by Marc Blanchet
- IPv6 Essentials by Silvia Hagen
- IPv6, Theorie et pratique (French)

The 6DEPLOY project makes available about 25 tutorials in PDF format that cover a variety of IPv6 topics such as Multicast, Network Management, Addressing and so on.

There is an Internet draft available clarifying how the IPv6 subnet model differs from IPv4.

Home Labs

Here are a couple of articles about setting up a small-scale IPv6 test lab for educational purposes.

- [Part 1](#)
- [Part 2](#)

Here is a brief overview of the tools used to set up an IPv6 lab using virtual machines on a virtual network.

NetKit bills itself as the poor man's system to experiment with computer networking. Downloads are available.

Here is a Usenix paper on building a virtual IPv6 lab using UserMode Linux virtualization. UserMode Linux (UML) has been widely used to build virtual network lab environments.

If you have Cisco licences then you might want to use DynaGen, a front end for DynaMIPS, the Cisco emulator. DynaGen makes it easier to run multiple instances of simulated routers for lab training purposes. Here is the DynaGen tutorial.

Build an IPv6 Router on Linux with NAT-PT and use this between your home IPv6 PCs and your IPv4 Internet access connection. Although the IETF has deprecated NAT-PT to historical status, it does work and some people feel that it is superior to 6to4 Relay. The best way to find out is to experience both of them for yourself.

Free Books

It's always better if you can get your employer to buy a full library of IPv6 books for you, but if you are trying to come up to speed on your own dime, you might want to read a free book on IPv6 and Internetworking with Cisco routers.

If you know of any other books that can be freely downloaded, please add them here.

- [An IPv6 Deployment Guide](#)
- [Day One: Exploring IPv6](#) (Junos specific, free login required, mobile versions available)
- [IPv6 eBook Series: Part 1 — The Basics](#)
- [IPv6 eBook Series: Part 2 — Network Preparations](#)
- [IPv6 eBook Series: Part 3 — Migration](#)
- [IPv6 eBook Series: Part 4 — Provisioning](#)

E-Learning Tools

- Introductory tutorial available at 6DISS Website (no longer updated, replaced by 6DEPLOY).
- Numerous tutorials are downloadable from 6DEPLOY including such topics as addressing case studies, IPv6 routing, multicast, security, deployment scenarios, and so on.
- US DoD High-Performance Computing Educational materials - [DoD HPC IPv6 Training and Learning](#)

Training

There's a lot of generic IPv6 training out there, but here's a few worth highlighting:

- CellStream, Inc. and The Online School of Network Sciences offers Hands On IPv6 training, plus check out these free how to's:
 - [Experimenting with DHCPv6](#)
 - [Experimenting with ICMPv6](#)
 - [A Wireshark IPv6 Configuration Profile](#)
 - [Setting Up an IPv6 Teredo Tunnel in Windows 7](#)
 - [Setting up an IPv6 ISATAP Tunnel in Windows 7](#)
 - [Setting up a 6to4 Tunnel in Windows 7](#)
 - [Neighbor Discovery \(ND\) Table in IPv6 Windows, Linux and MAC Machines](#)
 - [Links to Ubuntu IPv6 How To's](#)
 - [IPv6 Windows Command Line Examples](#)
 - [IPv6 MAC OSx Command Line Examples](#)
 - [IPv6 Linux Command Line Examples](#)
- MAAWG has a free hour-long video regarding e-mail for senders

- SCTE has both online and in-person [training](#)
- Global Knowledge has an [introductory](#) and [advanced](#) course
- If their training is anything like their [wiki](#) then NIL Associates' IPv6 [courses](#) are probably worth looking into
- RIPE has a [list of training sources and experts](#)
- [Erion](#) has been doing IPv6 training since 1999
- [Nephos6](#) has certified courseware, built by the guys from [Native6](#)
- [Training4IPv6](#) has a [list and categorization of trainers](#)
- [My IPv6 tutor](#) has free video-based self-training
- Hurricane Electric has [online training videos](#)
- Sixscape Communications has free [online IPv6 training](#)
- [SI6 Networks](#) offers hands-on [IPv6 security training](#)
- [Consulintel](#) host many documents and books.
- [Network Utility Force](#) has certified trainers, engineers and a certified course

Other informational sources

ARIN maintains some IPv6 information on their [V6-Info pages](#) and they also run tutorials at their twice yearly meetings. Here is the [Sunday V6 schedule for the Albuquerque meeting](#) which will happen on the 14th of October. In between V6 day and the main ARIN meeting there will be a [N ANOG meeting](#). NANOG and ARIN have one joint conference per year like this.

APNIC has a nice wiki too:

<http://icons.apnic.net/display/IPv6/Home>

HashIPv6

This page relates to the #ipv6 IRC channel on Freenode (irc.freenode.net). (Mediawiki does not allow "#" in page names, so we needed to substitute that character with something so as to be clear we were referring to the IRC channel and not IPv6 in general.) Other suggested references were [PoundIPv6](#), [TicTacToeIPv6](#), and [OctothorpeIPv6](#).

The channel offers free but unwarranted guidance, support, and answers to general IPv6 questions, typically related to:

- connectivity issues
- deployment strategy
- network stack theory
- other subjects?

The channel sees a lot of cross-posting with the [/r/ipv6](#) subreddit due to a substantial number of common users.

IPv6 Resource Sites

The following web sites contain a wide variety of information for organizations of any size.

- [ARIN IPv6 Info Center](#)
- [DoD HPCMP/DREN IPv6 Knowledge Base](#)
- [ISOC Deploy360 Programme/IPv6](#)
- [RIPE NCC IPv6 Act Now](#)
- [IPv6 Hackers Mailing-List](#)
- [SI6 Networks' publications](#)
- [IPv6 @ APNIC](#)
- [6DEPLOY](#)
- [Consulintel IPv6 Resources](#)
- <https://dnssecandipv6.se/>

Prepare For IPv6

This category is intended to be a repository for information on how to plan for IPv6 deployment and transition.

Relevant presentation regarding making the business case for IPv6: "[Some Predictions about IPv4, IPv6, and Your Boss](#)"

- [Broadband CPE](#)
- [Carrier Support](#)
- [Designing an IPv6 Lab Environment](#)
- [Device Support](#)
- [DNS Registrars IPv6 Support Status](#)
- [Enabling IPv6 on a Mail Server](#)
- [First Steps for ISPs](#)
- [Guidelines for the Secure Deployment of IPv6](#)
- [How do I get IPv6 from ARIN](#)
- [How do I get IPv6 from an ISP](#)
- [Investigate Middleboxes](#)
- [IPv6 Addressing Plans](#)
- [IPv6 Consulting Resources](#)

- IPv6 Firewalls
- Operational transition information
- Planning IPv6 Deployment
 - United States
 - NIST
 - US Civilian Agency Networks
 - US Department of Defense
 - US IPv6 Policy
- Porting Applications
- Providers Currently Selling IPv6 Transit
- Transparent Internet Access
- US Government - USGv6 Technical Infrastructure
- Vendors in the ARIN Region
 - Vendors in the ARIN Region 6connect
 - Vendors in the ARIN Region Acme Packet
 - Vendors in the ARIN Region Adtran
 - Vendors in the ARIN Region Airspan
 - Vendors in the ARIN Region APC
 - Vendors in the ARIN Region Calix
 - Vendors in the ARIN Region Cisco
 - Vendors in the ARIN Region Comtrend
 - Vendors in the ARIN Region Ericsson
 - Vendors in the ARIN Region Hostik
 - Hostik
 - Vendors in the ARIN Region HP
 - Vendors in the ARIN Region Procera Networks
 - Vendors in the ARIN Region RG Nets
 - Vendors in the ARIN Region TIVO
 - Vendors in the ARIN Region Yamaha

Broadband CPE

Standards and Standard Organizations

While the IETF working groups have been working on IPv6 standards for many, many years, documents that describe what standards and features should be in broadband CPE devices have only started to materialize in 2010.

Broadband Forum

The [Broadband Forum](#) (formerly DSL Forum) has included IPv6 in its BroadbandSuite specification X.X which was intended to be released in 2009-2010.

- [TR-124 Issue 2: Functional Requirements for Broadband Residential Gateway Device](#)
 - [TR-187: IPv6 for PPP Broadband Access](#)
 - [TR-177: IPv6 in the context of TR-101](#)
 - [WT-181 Issue 2 Amendment 2](#) extends Issue 2 of the TR-069 Device data model in order to support IPv6
- For more information on IPv6, contact the chairs of the [Architecture & Transport WG](#). They may be able to share with you draft text.

CableLabs

- [IPv4 and IPv6 eRouter Specification](#)

IETF

- [RFC 7084: "Basic Requirements for IPv6 Customer Edge Routers"](#)
- [IETF draft: "Advanced Requirements for IPv6 Customer Edge Routers"](#)

RIPE

- [Requirements For IPv6 in ICT Equipment](#)

NIST

- [A Profile for IPv6 in the U.S. Government – Version 1](#)

The New Hampshire's InterOperability Laboratory performed an IPv6 CE test, and as an exception to their general rule, published some [test results](#). No vendors are named (to protect the guilty).

Other listings

Marco Hogewoning gave a [presentation](#) at RIPE 60 covering various vendors' support and progress with various DSL and router CPE. This has

now been followed up with a [page](#) at the RIPE Labs to document IPv6 CPE. A complete listing of every survey can be found [here](#).

Adapters

Adapter CPEs allow an ISP to offer subscribers immediate access to IPv6 over an existing IPv4 access network. Neither the existing IPv4 access CPE nor the ISPs IPv4 access network gear (DSLAM, etc.) need to be changed, nor have their firmware updated, if an Adapter CPE is used at the subscriber premise. As in Dual-Stack implementations, the ISP issues the subscriber a /48 prefix, or smaller space, using the ISPs own IPv6 allocation which the Adapter CPE advertises over the subscriber's home or office LAN.

The Adapter CPE practically works by plugging into any free ethernet port on an existing routers or modem at the subscribers premise. It encapsulates IPv6 traffic on the subscribers LAN in an IPv4 tunnel and sends it over an IPv4 network to the ISPs IPv6 enabled core. Regular IPv4 traffic at the subscriber premise follows its normal path on the existing CPE to the ISP core. Adapter CPEs can work behind nested NATs if the appropriate IPv6-in-IPv4 protocol is used. The ISP is expected to have a tunnel server to decapsulate the IPv6 traffic at their core network. One tunnel server should be able to handle thousands of Adapter CPEs, and such a server can be supplied by the Adapter CPE vendor.

Adapter CPEs can also reverse tunnel IPv4-in-IPv6 to serve subscribers operating an IPv6 modem but need a private IPv4 address tunneled within IPv6.

For users on a 3G, LTE or WiMax wireless connection via a USB style modem, a software version of the Adapter CPE can be used to connect the user to the same IPv6 tunnel server at the ISP core.

- gogo6 Adapter CPE [gogoCPE](#)
 - Supports 6RD (RFC 5969), TSP (RFC 5572) and L2TP (RFC 2661) for IPv6-in-IPv4 tunneling
 - If implementing IPv6 tunneling behind NATs then TSP protocol is recommended for tunneling across all types of NATs
 - An Adapter CPE version that enables DS-Lite over IPv6 CPEs by using IPv4-in-IPv6 tunneling is available
 - Adapter CPE using DS-Lite helps conserve IPv4 by deploying v4 private addresses to subscribers over IPv6
- gogo6 Adapter Software Client [gogoCLIENT](#)
 - Graphical interface works on Windows XP, Vista, 7, Server 2003/2008
 - Command line version for Mac OS X, Linux and BSD
 - Trial version of Adapter Software Client can be downloaded from the [Freenet6](#) site
- gogo6 Tunnel Server [gogoSERVER](#)
 - Server supports both Adapter CPE and Software Client users
 - One server can support different IPv6 migration protocols, including TSP, 6RD, DS-Lite and DSTM

Cable

For cable, this is simple because all gateway devices certified by Cablelabs at DOCSIS 3.0 CM or CMTS will have IPv6 support. An example such device is the [Cisco Systems DPC3939](#) Of course, having a compliant cable modem or gateway only matters if the cable company's CMTS also supports IPv6.

- [Comcast IPv6 Information Center](#)

The new 'DOCSIS 2.0 + IPv6' standard also supports IPv6, which may on the cable modem side only require a firmware upgrade [<http://www.rmv6tf.org/2008-IPv6-Summit-Presentations/Dan%20Torbet%20-%20IPv6andCablev2.pdf>].

DSL

Most of the newest models released since Q3 2010 either have some level of IPv6 support, especially those models that support VDSL2. Many of the vendors with IPv6 implementations use Broadcom's chipset, and it's code has been lacking. That code has improved over the last few months to the point that in Q2 2011 that it's almost feature complete.

- [AVM Fritz!Box WLAN 3270](#) and [3370](#), [FRITZ!Box Fon WLAN 7240](#), [7270](#) (only v2, v3 and international, no IPv6 on 7270 v1), [7320](#), [7340](#), [7390](#) and [7570](#) (upgrade to latest firmware might be required):
 - IPv6 now supported by most (if not all) current AVM modem routers
 - Support for native IPv6 as well as SixXS heartbeat, 6RD, 6in4 and 6to4 tunnels
 - MTU can be set manually
 - Support for ULA
 - IPv6 firewall
 - DHCPv6 support
- [BEC 7800TN R2](#)
 - Has the Billion 7800NL code on the bottom of the box
 - When PPPoEv6 configured on WAN
 - DHCPv6-PD works
 - Stateful DHCP works and retrieves DNS servers
 - SLAAC with stateless DHCP works and retrieves DNS servers
 - handles non /64 prefix delegations
 - verifying if it has stateful packet inspection firewall support
 - IPoE requires manually entering default WAN gateway
- [BEC 8800N](#) (IPv6 implementation not fully complete, i.e. requires entering default gateway on WAN interface)

- Billion BiPAC 7402R2 ADSL2+ VPN Firewall Router (seems to be vanished from the face of the earth or at least is not supported)
- Billion 7800NL
- Cisco 87x and 88x SOHO routers, so not residential consumer-grade
- Comtrend CT-5374
 - When PPPoEv6 configured on WAN
 - DHCPv6-PD works
 - SLAAC with stateless DHCP works
 - handles non /64 prefix delegations
 - stateful packet inspection firewall support
 - GUI doesn't expose much of the IPv6 addresses
 - GUI uses confusing terminology to describe IPv6 features
- Comtrend AR-5384u
 - When PPPoEv6 configured on WAN
 - DHCPv6-PD works
 - SLAAC with stateless DHCP works
 - handles non /64 prefix delegations
 - stateful packet inspection firewall support
 - GUI doesn't expose much of the IPv6 addresses
 - GUI uses confusing terminology to describe IPv6 features
- Draytek Vigor 120, 2130 and 2750
- Funkwerk Enterprise Communications
 - bintec RS-Series
 - bintec Rxxx2-Series
- NetComm NB6Plus4
- NetComm NB6Plus4W
- NetComm 3G16WV
- Technicolor TG582n and also the TG789vn, TG789vn v3, TG788vn, TG787, TG784n v3, TG784n, TG784, TG712, TG670, TG589vn v2, and TG587n v3
 - Firmware r10.2 should be ready by the end of January, 2012.
 - IPv6 on the WAN side
 - Link-Local only
 - Static IPv6
 - SLAAC
 - Stateful DHCPv6
 - IPv6 over PPPoE
 - 6to4 tunneling
 - IPv6 in IPv4 tunneling
 - 6rd
 - DSLite
 - stateful firewall for IPv6
 - IPv6 on the LAN side
 - Link-Local only
 - Stateful DHCPv6 server
 - SLAAC
 - Prefix delegation
 - DNSv6 server
 - DNSv4/v6 proxy
- Technicolor TG789vn
 - When PPPoEv6 configured on WAN
 - DHCPv6-PD works
 - SLAAC with stateless DHCP works
 - handles non /64 prefix delegations
 - GUI for IPv6 configuration is incomplete
- VisionNet 505N (IPv6 implementation not fully complete)
- ZyxEL VSG1432 is in a testing phase with their IPv6 code (may be available from your ZyXEL SE)
 - When PPPoEv6 configured on WAN
 - DHCPv6-PD works
 - Stateful DHCP works
 - SLAAC with stateless DHCP works
 - handles non /64 prefix delegations
 - stateful packet inspection firewall not currently supported, vendors says it will soon
- Zoom X7N
- via OpenWRT
 - IPv6 with OpenWRT 3rd party firmware
 - [Comcast custom built IPv4/IPv6 OpenWRT firmware <http://sourceforge.net/p/dslite-6rd/home/>]
- via DD-WRT
 - Many Linksys, Buffalo and D-Link Routers with DD-WRT 3rd party firmware
 - [A ready-to-use IPv6 firmware build of dd-wrt that will fit in a 4MB flash WRT54G, Buffalo WHR-HP-G54, WRT600N, etc.] <http://www.dd-wrt.com/phpBB2/viewtopic.php?t=34022&postdays=0&postorder=asc&start=0>]
- via TomatoUSB
 - TomatoUSB build features IPv6 no GUI

Routers/Wireless Access Points

- D-Link's presentation ([http://www.ipv6.org.tw/docu/summit2009/1028 Session 4/01.2009%20Summit D-Link's%20View%20on%20IPv6.pdf](http://www.ipv6.org.tw/docu/summit2009/1028%20Session%204/01.2009%20Summit%20View%20on%20IPv6.pdf)) on their commitment to IPv6 and [blog entry](#) listing some IPv6 ready products. D-Link is currently working on adding Dual-Stack Lite (DS-Lite) support.
- [Airport Extreme \(later model\) details here](#)
 - ****WARNING: Apple will NOT support IPv6, if it works it works, if it doesn't, their support will not talk to you**
 - IPv6 on the WAN side
 - Static IPv6
 - DHCPv6 (stateful) with PD
 - DHCPv6 (stateless) with PD
 - 6to4 tunneling
 - IPv6 on the LAN side
 - stateless DHCPv6
 - no stateful DHCPv6
- [Buffalo WZR-AG300NH](#)
 - Implementation details unknown
- [D-Link DIR-601 \(Hardware Revision A1, look \[//ftp.dlink.com/Gateway/dir601/Firmware/\]\(http://ftp.dlink.com/Gateway/dir601/Firmware/\) here for updates\)](#)
 - supports DHCP-PD
 - IPv6 on the WAN side
 - Link-Local only
 - Static IPv6
 - SLAAC
 - Stateful DHCPv6
 - IPv6 over PPPoE
 - 6to4 tunneling
 - IPv6 in IPv4 tunneling
 - IPv6 on the LAN side
 - Link-Local only
 - Stateful DHCPv6
 - SLAAC
- [D-Link DIR-615 \(Hardware Revision C\)](#)
 - supports DHCP-PD (requires 3.12 or greater firmware [//ftp.dlink.com/Gateway/dir615 revC/Firmware/dir615 revC FW 313NA.zip](http://ftp.dlink.com/Gateway/dir615%20revC/Firmware/dir615%20revC%20FW%20313NA.zip) here)
 - IPv6 on the WAN side
 - Link-Local only
 - Static IPv6
 - SLAAC
 - Stateful DHCPv6
 - IPv6 over PPPoE
 - 6to4 tunneling
 - IPv6 in IPv4 tunneling
 - IPv6 on the LAN side
 - Link-Local only
 - Stateful DHCPv6
 - SLAAC
- [D-Link DIR-615 \(Hardware Revision E1-E4, all new IPv6 features will be developed on this hardware revision, look \[//ftp.dlink.com/Gateway/dir615 revE/Firmware/\]\(http://ftp.dlink.com/Gateway/dir615%20revE/Firmware/\) here for updates; some features listed may be only available in private beta\)](#)
 - supports DHCP-PD
 - IPv6 on the WAN side
 - Link-Local only
 - Static IPv6
 - SLAAC
 - Stateful DHCPv6
 - IPv6 over PPPoE
 - 6to4 tunneling
 - IPv6 in IPv4 tunneling
 - 6rd
 - Stateless DHCP to retrieve options
 - IPv6 on the LAN side
 - Link-Local only
 - Stateful DHCPv6
 - Stateless DHCPv6/SLAAC
 - RFC 6106 (previously RFC 5006)/SLAAC
- [D-Link DIR-632 \(Hardware Revision A1; some features listed may be only available in private beta\)](#)
 - supports DHCP-PD
 - IPv6 on the WAN side
 - Link-Local only
 - Static IPv6
 - SLAAC
 - Stateful DHCPv6

- IPv6 over PPPoE
 - 6to4 tunneling
 - IPv6 in IPv4 tunneling
 - 6rd
 - Stateless DHCP to retrieve options
- IPv6 on the LAN side
 - Link-Local only
 - Stateful DHCPv6
 - Stateless DHCPv6/SLAAC
 - RFC 6106 (previously RFC 5006)/SLAAC
- **D-Link DIR-655** (Hardware Revision B1, look [//ftp.dlink.com/Gateway/dir655_revB/Firmware/](http://ftp.dlink.com/Gateway/dir655_revB/Firmware/) here for updates; some features listed may be only available in private beta)
 - supports DHCP-PD
 - stateful packet inspection firewall on WAN
 - IPv6 on the WAN side
 - Link-Local only
 - Static IPv6
 - SLAAC
 - Stateful DHCPv6
 - IPv6 over PPPoE
 - 6to4 tunneling
 - IPv6 in IPv4 tunneling
 - 6rd
 - DS-Lite (in development)
 - Stateless DHCP to retrieve options
 - IPv6 on the LAN side
 - Link-Local only
 - Stateful DHCPv6
 - Stateless DHCPv6/SLAAC
 - RFC 6106 (previously RFC 5006)/SLAAC
 - DNS Search List support
- **D-Link DIR-815** (Hardware Revision A1)
 - supports DHCP-PD
 - stateful packet inspection firewall on WAN
 - IPv6 on the WAN side
 - Link-Local only
 - Static IPv6
 - SLAAC
 - Stateful DHCPv6
 - IPv6 over PPPoE
 - 6to4 tunneling
 - IPv6 in IPv4 tunneling
 - 6rd
 - DS-Lite (in development)
 - Stateless DHCP to retrieve options
 - IPv6 on the LAN side
 - Link-Local only
 - Stateful DHCPv6
 - Stateless DHCPv6/SLAAC
 - RFC 6106 (previously RFC 5006)/SLAAC
- **D-Link DIR-825** (Hardware Revision B and [//ftp.dlink.com/Gateway/dir825_revB/Firmware/dir825_revB FW 205NA.zip](http://ftp.dlink.com/Gateway/dir825_revB/Firmware/dir825_revB_FW_205NA.zip) latest firmware; some features listed may be only available in private beta)
 - supports DHCP-PD
 - IPv6 on the WAN side
 - Link-Local only
 - Static IPv6
 - SLAAC
 - Stateful DHCPv6
 - IPv6 over PPPoE
 - 6to4 tunneling
 - IPv6 in IPv4 tunneling
 - 6rd
 - Stateless DHCP to retrieve options
 - IPv6 on the LAN side
 - Link-Local only
 - Stateful DHCPv6
 - Stateless DHCPv6/SLAAC
 - RFC 6106 (previously RFC 5006)/SLAAC
- **D-Link DIR-825** (Hardware Revision C1)
 - supports DHCP-PD
 - stateful packet inspection firewall on WAN (in development)
 - IPv6 on the WAN side

- Link-Local only
 - Static IPv6
 - SLAAC
 - Stateful DHCPv6
 - IPv6 over PPPoE
 - 6to4 tunneling
 - IPv6 in IPv4 tunneling
 - 6rd
 - DS-Lite (in development)
 - Stateless DHCP to retrieve options
- IPv6 on the LAN side
 - Link-Local only
 - Stateful DHCPv6
 - Stateless DHCPv6/SLAAC
 - RFC 6106 (previously RFC 5006)/SLAAC
- [D-Link DHP-1320](#) (Hardware Revision A1)
 - supports DHCP-PD
 - IPv6 on the WAN side
 - Link-Local only
 - Static IPv6
 - SLAAC
 - Stateful DHCPv6
 - IPv6 over PPPoE
 - 6to4 tunneling
 - IPv6 in IPv4 tunneling
 - 6rd
 - Stateless DHCP to retrieve options
 - IPv6 on the LAN side
 - Link-Local only
 - Stateful DHCPv6
 - Stateless DHCPv6/SLAAC
 - RFC 6106 (previously RFC 5006)/SLAAC
- [FireBrick Ltd](#) A range of SOHO/Office routers built with IPv6 from the start.
 - [FireBrick 2500](#)
 - [FireBrick 2700](#)
- [Funkwerk Enterprise Communications](#)
 - [bintec RS-Series](#)
- [Linksys E4200](#) (needs [1.0.02 \(Build 13\)](#) or later)
 - supports DHCP-PD
 - IPv6 on the WAN side
 - SLAAC (likely, but not verified)
 - Stateful DHCPv6
 - manual or automatic 6rd
 - IPv6 on the LAN side
 - Stateless DHCPv6/SLAAC
 - supports IPv6 on guest network if there are more than two available IPv6 subnets
- [Linksys RVS4000](#) has a NAT-PT bug
 - IPv6 on the WAN side
 - 6to4 tunneling
 - IPv6 on the LAN side
 - Stateless
 - Stateful (DHCPv6)
- [Linksys WRVS4400N](#) is the wireless version of the above
 - IPv6 on the WAN side
 - 6to4 tunneling
 - IPv6 on the LAN side
 - Stateless
 - Stateful (DHCPv6)
- [NetComm NP805N](#)
- [Netgear WNR1000v2](#) Latest [firmware](#) explicitly supports IPv6
- [Netgear WNR3500v2](#) Latest [firmware](#) explicitly supports IPv6
- [Netgear WNR3500L](#) Latest [firmware](#) explicitly supports IPv6
- [Netgear WNDR3700v1](#) Latest [firmware](#) explicitly supports IPv6
- [Netgear WNDR3700v2](#) Latest [firmware](#) explicitly supports IPv6
 - supports DHCP-PD
 - IPv6 on the WAN side
 - Static IPv6
 - Stateful DHCPv6
 - IPv6 over PPPoE (creates a separate session for IPv6. Issue has been reported to Netgear)
 - 6to4 tunneling
 - Stateless DHCP to retrieve options
 - Pass Through

- IPv6 on the LAN side
 - Stateful DHCPv6 (whether WAN was PPPoE or DHCP, the LAN-attached Windows 7 machine did obtain an IP, but unable to ping past WAN interface; could be the fact that the delegated prefix was a /56. Bug has been reported to Netgear.)
 - Stateless DHCPv6/SLAAC (the full /56 delegated prefix is used, rather than a /64, which results in a Windows 7 machine not obtaining IP information, consistent with RFC2462. Bug has been reported to Netgear.)

Trial and Test devices

In addition to the commercial products, some people are rolling their own using Linux/BSD servers or upgrading the firmware of existing devices. The typical broadband gateway currently on the market is a standard computer design loaded with custom firmware according to the spec of the company whose plastic case and logo are used. But in actual fact, all devices whatever the brand, are manufactured by factories in the Far East using a small set of standard hardware designs. Virtually all of these designs can be adapted to use IPv6 by simply changing the software, i.e. uploading a different set of firmware. The brand name sellers are using this fact to have very short product cycles to adjust to market demand. This means that as soon as there is any significant demand for IPv6 support, they could update their software and have new products on the market in two to three months.

The Far East

The Japanese market has many more IPv6 devices and services than most other countries. A good way to track what is going on there is to read through the announcements at [IPv6Style](#) in Japan. Don't click on the English version of the site since that is outdated and doesn't contain the product announcements. Instead, use a web translator to read the site. You can use [Babelfish](#) to produce an adequate Japanese-to-English translation for learning about new products. While many articles will still be almost incomprehensible, new product announcements are so formulaic that you can usually understand what the product will do, and the product name and model for further inquiries.

If you want to deploy IPv6 and cannot find CPE on the market to support your needs, it is worthwhile to send a detailed RFQ to the major brand name sellers like Linksys, Netgear, etc. Japanese or Korean brand name sellers are more likely to have already done the IPv6 development so make sure that companies like Billion and Buffalo get your RFQ.

Carrier Support

- **Global Crossing** - AS3549 - Dual Stack Support
- **Hurricane Electric** - AS6939 - Dual Stack Support
- **Qwest** - AS209 - Supports "Test" IPv6 connections over dedicated circuit. No Dual Stack

Also see the [Providers Currently Selling IPv6 Transit](#) page.

Designing an IPv6 Lab Environment

Because IPv6 has new features, i.e. it is not just IPv4 with more bits, you will need to build a test lab environment to experiment with IPv6 anycast, mobile IP, transition technologies, and so on. Given the amount of work that must be done before IPv6 can be fully deployed in production, and the short time before the global free pool of IPv4 addresses runs out in 2010, every ISP should be building their test labs today.

This page is for information that will help ISPs set up their in-house test labs, not for educational labs which are covered on the [Educating Yourself about IPv6](#) page.

OSS Considerations

Even though it is not necessary to manage your network over IPv6 it is likely that you will want to trial [IPv6 Management Tools](#) in your lab. Part of your lab trials should be to determine what management functions need to be done on IPv6 and what can be done with other protocols such as IPv4.

IPv6 Internet Access

Because you need to trial IPv6 peering and you are likely to be unable to interconnect your lab with other ISP labs, you should build a multi-AS environment in your lab network. Merit [describes the lab environment for their IPv6 workshop](#) in April 2007.

On the other hand, you might want to isolate your IPv6 test lab from your normal test-and-certify environment so that you CAN connect to the live IPv6 Internet complete with IPv6 peering. Collect volunteers who will run IPv6 on their workstations/laptops and connect them to the IPv6 lab in such a way that this is their only Internet access. You might want to go so far as to block their IPv4 addresses in web proxies and Internet firewalls so that they are forced to eat the company's new dog food. With a crew of technically knowledgeable users you will be able to shakedown corner cases much quicker.

IPv6 Security and Potentially Disruptive Testing

Enterprise IPv6 lab environments should be isolated for the production networks whenever they are used for configuration and testing of security mechanisms or other infrastructure components that may be disruptive or introduce security risk.

There is a Python extension library called SCAPY that can be used to generate IPv6 packets, both correctly formed and incorrectly formed. Because it is built on Python it is a fully programmable test data generator.

Read this presentation to see what it can do:
[SCAPY and IPv6 Networking](#)
and Google for SCAPY6 to find more info.

Fun Stuff

IPv6 network fax service anyone? Even colour copiers now do IPv6.

```
(We got a new colour photocopier at work today - it's IPv6 capable.
None of us techs asked for it as a feature, and I don't think any of us
actually got a look at the datasheet for it before it was bought. The
first we knew of it supporting IPv6 was when the photocopier tech asked
us if we wanted it enabled. I suspect the photocopier tech didn't even
quite appreciate what he was asking. To him, it was probably just another
photocopier networking option that the customer might want turned on.)
```

Any other IPv6 gadgets that you know of which might be fun to try out on the lab network?

Device Support

Without rich support from our common hardware vendors IPv6 deployment will never become a reality. While core network equipment and Operating Systems are finally showing mature IPv6 implementations what good does that do us if our Printers, LAN switches, Battery Backup Systems, etc. don't support IPv6. All hardware and vendors which need to be IPv6 capable should be listed on this page so that if their implementations are lacking, market pressure can be put forth by the customers of their product.

Operating Systems

A very complete page on configuring IPv6 on a multitude of operating systems can be found [here](#)

- [Miredo](#)
- [Renumbering an IPv6 Network](#)
- [Operating System Support](#)
 - [Linux Support](#)
 - [Solaris IPv6 Sites](#)

Routing and Switching

- [Adtran](#) - Development rumored to begin in Q109 with code shipping by Q409
- [Alcatel-Lucent](#) - In SR OS 10.0 & 11.0 they made a lot of IPoE access model BNG improvements such chained relay of LDRA DHCPv6 packets and link based dynamic pool selection.
- [Cisco](#) - Increasing support in IOS 12.4T. Limitations such as BVI support exist. Cisco also has a [documented list](#) of specific IPv6 features for each IOS release.
- [Juniper Networks](#) - Fully supported in M/T series.
- [Relay Services](#)
 - [Cisco 6to4 Relay Service](#)
 - [Juniper 6to4 Relay Service](#)
 - [Linux or BSD 6to4 Relays](#)

Network Infrastructure

- American Power Conversion - No Support.
- Falcon UPS - Supports IPv6
- HP UPS Management - Supports IPv6

VoIP

- Sonus Networks - No current support. Vendor hinted at 2009 but no definite roadmap.

DSL and Cable Modems

Also see the [Broadband CPE](#) page for more supported devices.

External Lists of IPv6-Supporting Devices

- [IPv6 Portal](#) - List of devices claiming support
- [DoD Device List](#) - DoD's list from its IPv6 mandate
- [Comparison of IPv6 application support](#) - List of applications and their support (or lack of) IPv6
- [IPv6 Forum "IPv6 Ready Logo Program Approved List"](#)

DNS Registrars IPv6 Support Status

List of Registrars and their IPv6 Glue Support Status

Sites below list either domains supported or "NONE" for no support. If your registrar is not listed, their status is unknown. Please find out and contribute back here.

See also similar list at SIXXS [and Hurricane Electric <http://bgp.he.net/report/dns>].

<http://www.frobbit.se>

Registrar	URL	IPv6 Glue Support Level
Checkdomain	http://www.checkdomain.de	
DomainDiscover	http://www.domaindiscover.com	
Dotster	http://www.dotster.com	
DynDNS	http://www.dyndns.com	In progress
EDUCAUSE	http://www.educause.edu	
Enom/BulkRegister	http://www.enom.com	
EPAG	http://www.epag.de	
Frobbit	https://frobbit.se/	Supported
GKG.NET Inc.	http://www.gkg.net	
GoDaddy	http://www.godaddy.com	
Mythic Beasts	http://www.mythic-beasts.com	Supported
OnlineNIC	http://www.onlinenic.com	
OpenSRS	http://www.opensrs.org	
Tiger Technologies	http://www.tigertech.net	
Name	http://www.name.com	

Enabling IPv6 on a Mail Server

You need to think through all the interactions before enabling IPv6 on a mail server.

Ket Crispin posted this to the IETF list:

I was presenting what I thought was an interesting example of a subtle problem that can come up in ipv6 deployment.

The mailserver in question uses a default redhat enterprise build (actually centos). ipv6 is either enabled by default, or just has a single check box, with no further information. The fact that ipv6 is enabled so trivially carries the implication that just enabling ipv6 won't actually damage anything.

Now I know different. Just enabling ipv6 on an otherwise correctly configured and functioning ipv4 box **will** cause damage – it will cause mail that would have been delivered to not be delivered. I could be wrong, but this strikes me as a trap that lots of people could fall into.

As I mentioned, my servers actually do reject mail if they can't find a reverse dns for the senders IP. Some of those servers use ipv6; in light of all this I'm going to have to rethink that decision. For a server, the combination of enabling ipv6 and using this particular anti-spam technique may drastically increase the number of false positives – especially as ipv6 gets more widely deployed.

Paul Warren adds:

Google mail servers reject mail with no IPv6 reverse DNS. This means that a) if you adopt this measure then you're in good company, and b) if you enable IPv6 on your mail server, then it's very important that you have working IPv6 reverse DNS.

When enabling IPv6 on a mail server, you need to consider all the places where you might have IP-based access restrictions in place, as even if you don't modify add any AAAA records to point at your server, it will start using IPv6 for outgoing connections. One place to consider is SPF records for any domains for which your server sends mail.

First Steps for ISPs

The first steps for ISPs to take today, do not involve planning IPv6 rollout or even testing IPv6 in the lab. Many users on the IPv4 Internet are already using IPv6 today through various types of tunneling schemes. For the past few years, many new computers (Apple PCs, Solaris servers, Linux servers) have had IPv6 support installed by default. Devices like the Apple Airport WiFi gateway already set up 6to4 relay tunnels for IPv6 devices on end user networks.

So the first step to take is to make sure that your network facilitates the use of these tunneling technologies. There are three separate steps to take.

See [IPv6 Transition Mechanism](#) for a comparison of the various IPv6 Transition mechanisms, outside of providing native connectivity.

Get IPv6 Transit

If you are going to get, or have your own IPv6 allocation from ARIN, you will either have a large network yourself and peer with everybody, or you will need to get Transit (i.e., an upstream ISP). See [IPv6 Transit Providers](#) for ISPs who are offering IPv6 Transit possibilities in the various parts of the world.

Like IPv4 Transit, you will most likely want to have at least two upstream providers over diverse paths to ensure that either of them goes down that the other can take over. If you only have one upstream, you may simply have static routes to direct IPv6 traffic to you, and a default route outbound. If you have two upstream, you will use BGP to announce routes, and can either set up a separate BGP session for your IPv6 route, or add your IPv6 route to your IPv4 BGP session.

If your IPv6 connectivity is different than your IPv4 connectivity, be careful when sizing the bandwidth needed. Even though today IPv6 traffic is fairly minimal for pretty much everyone, it has the potential to grow quickly now that more stuff comes with IPv6 support out of the box. If someone then adds an AAAA record to a service that generates a lot of traffic, a noticeable amount of traffic can move from IPv4 to IPv6 over night. You'll want to be able to add additional bandwidth on fairly short notice or else supplement the native IPv6 access with an IPv6 tunnel over your IPv4 access connection to the upstream who provides IPv6 service.

Setup a peering with GRH

Setup peering with [GRH](#) and provide your routing tables to the system. This tool allows you to see easily which prefixes you are missing in your network and where you might want to improve IPv6 Transit. It also provide the community with a look into the quality of your network and ability to have a shot of debugging when something looks wrong.

Consider Transition Options

Setup A 6to4 Relay

This allows your customers to use your globally registered IPv4 addresses to create a globally unique /48 prefix in the reserved 6to4 prefix 2002::/16. This makes the site behind the IPv4 address able to communicate using IPv6. The method is even workable across NAT devices since it leverages your network addresses, not the customers.

First, you might want to review RFC's [3056](#) and [3068](#). Also, it would be good to read your router vendor's documentation on 6to4 relays because you set up the 6to4 relay service on routers which respond to the 6to4 anycast address assigned in RFC 3068.

A complete description of 6to4, how to setup clients (in case you don't want the automatic configuration) and how to setup a 6to4 Relay in different platforms, is available at [The IPv6 Portal](#).

Check the following pages for more details on specific vendors:

- [Cisco 6to4 Relay Service](#)
- [Juniper 6to4 Relay Service](#)
- [Linux or BSD 6to4 Relays](#)

Configure 6to4 relay service on two well-connected IPv6-enabled routers in your network and make sure you see a route to the 192.88.99.1 address propagated in your IGP.

Assuming you have already configured your normal IPv6 connectivity then don't forget to route 2002::/16 and sprinkle some "redistribute connected" over your favorite routing protocols.

If you want to run a public gateway, announce 192.88.99.0/24 and 2002::/16 over BGP.

No need to do tunneling at leaf nodes (i.e., ones where all the traffic goes into one direction) and if you have at least two in your network one location can be backup for another, so then one per location would be enough. If I had some old 7200s lying around I'd use those, in locations where replacing drives isn't a huge deal a BSD box (Linux if you insist) would be a good choice because they give you a bigger CPU for your money.

But doing it on non-dedicated routers is fine as well as long as you're sure an excess of IPv6 traffic isn't going to cause problems.

Here is a list of [ISPs currently announcing a 6to4 prefix](#). Add yourself to the list after you start announcing one.

Setup a Teredo Relay

Teredo is an alternative IPv6 transition technology specifically for providing IPv6 connectivity behind a NAT device by using UDP tunneling. The protocol is described in RFC 4380. ISPs should run a Teredo Relay to optimize IPv6 connectivity for Teredo clients accessing the ISPs native IPv6 hosts. Establishing a local relay does not require any modification of Teredo clients - Teredo relay discovery is built-in to the protocol.

Teredo client functionality is built-in to Windows. Macintosh and UNIX systems can use [Miredo](#).

- [Microsoft Teredo Overview](#)
- [Brief description of Teredo tunneling](#)
- [FreeBSD Teredo Relay Setup](#)

Setup A Tunnel Broker

Tunnel Brokers can be set up using a variety of different software, including Microsoft Windows. [RFC 3053](#) defines the role of a tunnel broker. Here are some pointers to various HowTo documents.

- [OpenVPN Howto](#)
- Buy and install Gateway6 from [Hexago](#)
- The CSELT Tunnel Broker software, ipv6tb, is widely advertised on the web at [and <http://carmen.ipv6.tilab.com/>] however I was not able to reach either of the two sites. If anyone succeeds, please edit this page.
- [SixXS](#) can provide a *gratis* Tunnel Broker in your own network, one only needs to provide hardware, power and connectivity, define a policy on who can use it. Custom web/console interfaces and API's are available on request. Contact them for more information.
- [The IPv6 Portal](#) has a list of Tunnel Brokers around the world.
- [Tunnelbroker.net](#) provides a free Tunnel Broker service. Registration & management via web form. Example configurations and forums provided.

Note that some Tunnel Brokers require that you have your own address space from your RIR and arrange, setup and maintain routing and transit, which leads to the biggest advantage over 6to4/Teredo: the network it is in your control, not in the control of others.

Advise Your Customers

Tell your customers what you have set up and point them to some resources that explain how to best make use of 6to4, Teredo and tunnel brokers. In addition, let them know about the [Customer problems that could occur](#) and provide some advice on how to address these problems.

- [Hurricane Electric](#) in April 2008, sent out this [notice](#) to their customers about IPv6. Configuration guides for many different operating systems are available at [The IPv6 Portal](#).

Work Toward Native IPv6

After you have accomplished this, it is time to begin the planning and education process which will result in offering native IPv6 Internet access services at all PoPs where you currently offer IPv4 Internet access. You will need to run dual-stack on your backbone and servers, and will need to push IPv6 all the way to the edge. Here are some pages which will help with that.

- [Implementing Dual Stack](#)
- [Educating Yourself about IPv6](#)
- [Planning IPv6 Deployment](#)
- [Designing an IPv6 Lab Environment](#)
- [DNS and Naming Issues](#)
- [Troubleshoot IPv6 Issues](#)
- [Implementing 6PE](#)
- [Investigate Middleboxes](#)
- [Article on ISP IPv6 planning](#)

Guidelines for the Secure Deployment of IPv6

Guidelines for the Secure Deployment of IPv6, Dec. 2010, SP 800-119

Available from the main site: <http://csrc.nist.gov/publications/nistpubs/800-119/sp800-119.pdf>

Recommended by Henrik Kramshoej, for having a great introduction and detailed description of IPv6 - including security issues. No sizable IPv6 network should be built without browsing this first.

How do I get IPv6 from ARIN

There are six simple steps to take to receive IPv6 address space directly from ARIN.

1. Review ARIN policy requirements in the [Number Resource Policy Manual](#).
2. Set up an [ARIN Online account](#) and complete/submit the appropriate request forms.
3. ARIN evaluates the request, and asks for additional information as needed to verify eligibility.
4. ARIN approves the request.
5. Pay applicable fees and sign the Registration Services Agreement.
6. Receive notification that the resources are available for use.

Detailed information on this process is available on the [Requesting A Resource](#) page on the ARIN website.

How do I get IPv6 from an ISP

First, make sure your [equipment supports IPv6](#) and is properly configured to handle IPv6 traffic. Along with the benefits of adding IPv6 to your network it can also introduce new problems so [prepare for some common issues](#).

Use [Hurricane Electric's World Report](#) (seems to be auto-generated) and pull a report for the country you're in. Then compare ISPs that are available to you. The 'Adjacencies v6' column refers to how many other IPv6 connections to other companies they have (peering) which will improve IPv6 performance. The 'Routes v6' column refers to the part of their network that is available over IPv6. Both columns you can compare to the related v4 columns to get an idea how far along their IPv6 implementation is at. Now if the ISP has no v6 routes listed then they just don't offer any form of IPv6 to their customers currently. If the ISP has a very low ratio of v6 to v4 routes then they may have a limited IPv6 deployment where only available in IPv6 trials (e.g. limited to certain areas or types of technology used or even on an opt-in only basis) or just via [Relay Services](#).

Some other things to consider when evaluating ISP's IPv6 offerings:

- Fully native IPv6 end to end support is best vs. using tunnels since those would limit the routes you would be able to access inside the ISP's backbone network and therefore potentially impact performance
- If only tunneled connections available then confirm if you would be connecting to a POP that is local enough to you (at least in same country if in a smaller country or the same region if a larger country)
- If the size of the IPv6 subnets they can offer are enough for your needs without having to pay more to get the equivalent of what you already have with IPv4

If you are a current customer of an ISP without native IPv6 connectivity then make sure to tell them of your interest in this. If no IPv6 options are offered by contacting who handles your account then make sure they send up your expressed interest/inquiry to someone with some decision making influence.

If your current ISP doesn't support native IPv6 *and* there aren't other reasonable IPv6 offerings from other ISPs in your area then in the interim you could consider:

- Using a managed IPv6 over IPv4 tunnel through a tunnel broker. There could be noticeably reduced performance/reliability if using a technology that has to deal with NAT traversal or tunneled to a non-local POP or even if using a free service could be an overloaded/busy server so make sure to shop around.

- Do some tests or ask your ISP if they have their [own 6to4 or Teredo relays setup](#) & enable use of them for IPv6-only traffic and use IPv4 for everything else (note: with IPv4 preferred for dual-stack and IPv4 content). Don't bother using those transition technologies from public servers since they are usually not reliable enough.

Other useful resources:

[Network World article: Finding an IPv6 ISP](#)

Investigate Middleboxes

For a long time, estimated to be between 10 and 20 years, the Internet will have a mixture of IPv4 and IPv6 which will need to communicate with each other. Many of these communications needs can be facilitated through middleboxes of one sort or another. It is difficult to give general advice about which middleboxes to install in your network, but you should survey the possibilities and see whether or not one of them will work for you.

Application Proxies

This is just a variation on the ALG [Application Layer Gateway](#) but instead of addressing the need for security, it bridges the gap between IPv4 and IPv6. It can be as simple as an SMTP relay server that functions on both IPv4 and IPv6 simultaneously.

NAT-PT

This is a form of NAT with additional features that are needed to bridge the gap between IPv4 and IPv6 hosts. It is defined in [RFC 2766](#). Although the IETF doesn't particularly like this solution, it has been implemented by some vendors such as Cisco, and it will be helpful to many ISPs during the transition to a pure IPv6 Internet.

Web Proxies with CONNECT Support

This might be a general solution for you if you have a userbase which will be satisfied with operating behind a web proxy. There are more details in [this Internet Draft](#) written by Iljitsch van Beijnum.

IPv6 Addressing Plans

This page is for developing a best practice guide to IPv6 addressing plans for an ISP allocation. These are the allocations that are a /32 prefix or shorter. To some extent, a company that receives a /20 or /22 will be doing some things a bit differently due to scale, nevertheless, the same principles apply to developing the plan.

Where possible, a guideline should give its rationale and reference any supporting documentation.

Discussion can occur within the comments section below. In some cases, where there is no clear consensus on some aspect of the guidelines, we will post both positions on this page and copy the discussion material to a separate background page that focuses on the one issue.

General Guidelines

Template:Alertbox|Draft document!|Although this document contains input from several people including discussions on the NANOG list, it is not necessarily the last word in IPv6 addressing plans. If you have suggestions for improvement, please post it to the discussion page (see the tab above).

There are several approaches to an "optimal" plan, but one [website](#) follows RFC 3531 and a [book's](#) perspective.

Additional points:

1. Separate address block for infrastructure from other uses (enterprise, loopbacks)
 - May mean two /48s per PoP
 - Document so that you can justify it in your Host Density ratio
2. Each individual site should receive plenty of subnets, such as between a /48 and /56. See RFC 6177.
3. Summary aggregates for groups of sites where it makes sense, but watch your HD ratio
4. Any prefixes shorter than /48 will only be assigned when there is written justification to show that this prefix will meet the RIR HD ratio guidelines within 5 years.
5. Each PoP is a site therefore assign a /48 for infrastructure
6. No subnets will use prefixes longer than /64.
7. Separate address block for router loop-back interfaces
 - Generally number all loopbacks out of one /64
 - /128 per loopback
 - *Note that this recommendation violates RFC 4291 - "IP Version 6 Addressing Architecture", which states that for addresses with other than binary 000 as their first 3 bits, the Interface Identifier must be 64 bits long. It isn't really necessary to save IPv6*

address space by using /128s on loopbacks. For example, out of a /48, if you allowed for 16384 /64s for loopbacks, you'd still have 49 152 subnets left for links. If your network is big enough that that sort of addressing plan is not going to be large enough, then you probably won't have any issues with getting multiple /48s e.g. a /47 or /46.

8. Assign a /64 per LAN / VLAN / subnet
9. Organizations with multiple /48 allocations should consider enterprise-wide aggregation levels of /60 or larger blocks for the administration of enterprise policies for common functions such as:
 - DMZ
 - Realtime traffic, such as voice & video
 - Network loopback addresses and Link space
10. IETF expects that you will assign a /64 for point-to-point links
 - Fewer typos because all subnets are the same size
 - You can use longer prefixes but what's the point?
 - /126 will break Mobile IPv6 Home Agent discovery
 - /112 leaves final 16 bits free for Node IDs
 - Use /64 unless you have read and understand RFC 3627
 - Note: on pure point-to-point links (e.g., SONET) anything shorter than /127 is vulnerable to ping-pong packet amplification as described in [Maz's APNIC 26 presentation](#). (On Ethernet, this is at most a neighbor cache DoS)
11. The enterprise network should receive a prefix sufficient to provide a /48 allocation for each site (office/campus/PoP) at which the company has employees or systems.
12. All customers get one /48 unless they can show that they need more than 65k subnets.
 - Host count is irrelevant.
 - Do not assign to customers from PoP aggregates
 - Define aggregate areas which contain several PoPs
 - Carry customer networks in iBGP
 - Aggregate only in eBGP
 - If you have lots of consumer customers you may want to assign /56s to private residence sites.
13. Expect the registry to allocate a /32 and reserve one /32
 - Plan for the time when you get a second allocation giving you a /31 aggregate.
 - If you get more than /32 first time round, ask the RIR how much is reserved so you can plan appropriately.
14. If you need private addresses, generate a ULA prefix as defined in [RFC 4193](#)
 - Use [this handy web tool](#) to generate one
 - Add it to the registry at the above site, if you want people to know that this is your private space
 - Make sure your internal registry people are aware of your ULA prefix(es) so that everybody uses it.

Specific Situations

1. Point-to-point links may be assigned a /126 prefix if there is written assurance that the drawbacks documented in [RFC 3627](#) will not occur.

RFC 5375

Five people have written RFC 5375 for the IETF's [v6ops working group](#). It has a lot of detail.

The following is an excerpt from RFC 5375, section 2.4:

IPv6 provides network administrators with a significantly larger address space, enabling them to be very creative in how they can define logical and practical address plans. The subnetting of assigned prefixes can be done based on various logical schemes that involve factors such as:

- o Using existing systems
 - translate the existing subnet number into IPv6 subnet id
 - translate the VLAN id into IPv6 subnet id
 - o Rethink
 - allocate according to your need
 - o Aggregation
 - Geographical Boundaries - by assigning a common prefix to all subnets within a geographical area
 - Organizational Boundaries - by assigning a common prefix to an entire organization or group within a corporate infrastructure
 - Service Type - by reserving certain prefixes for predefined services such as: VoIP, Content Distribution, wireless services, Internet Access, Security areas etc. This type of addressing may create dependencies on IP addresses that can make renumbering harder if the nodes or interfaces supporting those services on the network are sparse within the topology.

The above draft has a lot more on designing addressing plans including some detailed case studies in an appendix.

NANOG Postings

Bill Herrin

Bill Herrin posted the following explanation of aggregation on the NANOG mailing list.

If I remember right, this came from a discussion on the ARIN PPML list.
I don't clearly remember the discussion, so my apologies in advance if I get some of it wrong.

During discussion and analysis, allocation of addresses by POP was found to be incompatible with a couple goals deemed more important. The general consensus was that you should establish areas consisting of multiple POPs and aggregate by area instead. However, ARIN is not in the business of recommending routing best practices so the recommendation was narrowed to just "don't aggregate by POP" meaning "don't fine-tune your aggregation all the way down to the POP level; stop somewhere above it."

The first problem with aggregating by POP was customer mobility. When a customer moves from the suburbs 10 miles east of the city to the suburbs 10 miles west of the city, he should keep his addresses and that shouldn't cause you any hardship. If your aggregation area includes the city and its suburbs, that's no problem for you. If you've aggregated by the CO where their DSL connects to, then over time as customers migrate around the city you'll end up with an awful mess.

Another problem was that there is a temptation to implement security features at the aggregation points. For example, you might put your egress source address filtering and spoofing protection there to catch anything where you couldn't for whatever reason filter directly on the customer link. If the aggregation point covers a large area, there are a very small number of customer movements for which that will be a problem. If its a single POP you end up screwing a lot of customers. A canonical example of this sort of error is Verizon Business's Ashburn data center. Customers of the data center can't leave the building and keep their IP addresses. Verizon Business (UUnet/MCI) can't attach them anywhere else on the network.

Another problem was DOS attacks. If someone DOSes a network that has moved since its inception then it'll first take out the specific route, then take out the covering route. If you've aggregated by area, there's a good chance the covering route is far enough upstream to handle the DOS. If the covering route is an alternate POP, it probably doesn't so you've allowed the attacker to crush two POPs with one DOS.

Another problem was sparse allocation. Sparse allocation for IPv6 addresses is strongly recommended. If allocated address blocks are not adjacent to each other then when a customer says, "I need more addresses," there is a strong probability that you can grant the request by simply changing the prefix length. This keeps your routing table small and tidy. You get lots and lots of IPv6 addresses, so if you only break them up into a dozen pools you still have plenty with which to do sparse allocation. If you break them up into pools for each of the hundreds or even thousands of POPs that you have and/or create two levels of aggregation (first by POP, second by area), you won't have enough to do effective sparse allocation.

There were other points disfavoring aggregation by POP but I can't remember what they were. I think there was also an assumption that traditional dynamic-IP customers would not each get a static block of IPv6 addresses. If that fails to hold true then it changes the character of the aggregation problem.

Ryan Harden

Ryan Harden posted this to the NANOG mailing list:

Our numbering plan is this:

1. Autoconfigured hosts possible? /64
2. Autoconfigured hosts not-possible, we control both sides? /126
3. Autoconfigured hosts not-possible, we DON'T control both sides? /64
4. Loopback? /128

Within our /48 we've carved it into (4) /50s.

- First, Infrastructure. This makes ACLs cake.
 - Within this /50 are smaller allocations for /126s and /128s and /64s.
- Second, User Subnets (16k /64s available)
 - All non-infrastructure subnets are assigned from this pool.
- Third, Reserved.
- Fourth, Reserved.

We believe this plan gives us the most flexibility in the future. We made these choices based upon what works the best for us and our tools and not to conserve addresses. Using a single /64 ACL to permit/deny traffic to all ptp at the border was extremely attractive, etc.

Matthew Petach

Matthew Petach said on the NANOG list:

As I mentioned in my lightning talk at the last NANOG, we reserved a /64 for each PtP link, but configured it as the first /126 out of the /64. That gives us the most flexibility for expanding to the full /64 later if necessary, but prevents us from being victim of the classic v6 neighbor discovery attack that you're prone to if you configure the entire /64 on the link. All someone out on the 'net needs to do is scan up through your address space on the link as quickly as possible, sending single packets at all the non-existent addresses on the link, and watch as your router CPU starts to churn keeping track of all the neighbor discovery messages, state table updates, and incomplete age-outs. With the link configured as a /126, there's a very small limit to the number of neighbor discovery messages, and the amount of state table that needs to be maintained and updated for each PtP link.

It seemed like a reasonable approach for us--but there's more than one way to skin this particular cat.

IPv6 Consulting Resources

The following organizations/individuals offer IPv6 consulting services (please add your link here if applicable):

- <http://brooksconsulting-llc.com/>
- <http://chrisgrundemann.com/>
- <http://www.consulintel.es/>
- <http://www.hoggnet.com/>
- <http://www.netuf.net/>
- <http://tocici.com/>
- <http://www.steffann.nl/>
- <http://www.si6networks.com>
- <http://www.nephos6.com>
- <http://www.nodo6.com>
- <https://www.aptient.com/>
- <http://goo.gl/SGBHgx>
- Consulintel
- <https://www.interlan.se/>

IPv6 Firewalls

Some people have claimed that they cannot yet sell IPv6 Internet access because there is no IPv6 firewall support. According to [this ICANN study](#) this is not quite true. At least 30% of the 42 vendors surveyed, had IPv6 support.

According to [this talk](#) many open-source and commercial firewalls supporting IPv6 are available.

- MFFirewall based on Linux is a free/opensource IPv6/IPv4 fully functional Firewall <http://code.google.com/p/mf-firewall/>
- m0n0wall is based on FreeBSD <http://m0n0.ch/wall/screenshots.php>
- pfSense is also based on FreeBSD <http://pfsense.com/index.php?id=26>
- FWBuilder is a management tool that builds filter setups for several different firewalls http://www.fwbuilder.org/archives/cat_screenshots.html

- Checkpoint FW1 NGX R65 on SecurePlatform supports IPv6
- FortiGate/Fortinet supports IPv6 in FortiOS 3.0 and up. Read [this technote](#) for more info.
- Juniper SSG (formerly Netscreen) supports IPv6 in ScreenOS 5.4 and up.
- Cisco ASA (formerly PIX) supports IPv6 in version 7.0 and up (Does not currently support Failover)
- Stonesoft has committed to [rolling out IPv6 support in 2008](#) across its StoneGate product line.

Commercial firewall support may be lagging behind OS and router support, but not by much.

The Campus IPv6 Wiki has a more detailed rundown of IPv6 firewall testing and hints for their use [here](#).

You can [Build an IPv6 Firewall with OpenBSD](#).

You can [also build an IPv6 firewall with Windows Server 2008](#).

Vyatta and it's open-source core both fully support IPv6

ip6tables is used to build IPv6 firewalls in both openwrt and dd-wrt. Although dd-wrt and openwrt are built for wireless routers, you can turn off the wireless interface on these routers and use them as ethernet-to-ethernet routers.

DD-WRT supports IPv6 and runs on a lot of hardware, including the Linksys WRT 160N, IPv6 support is discussed [here](#). (IPv6 firewall support not in the GUI, only from command line as of March 2011)

OpenWRT also supports IPv6 with both tunnelling and native, and also runs on a large amount of hardware, including both the Netgear WGR614L and Linksys WRT54GL. In the US, the WGR614L is stocked at [www.amazon.com](#) and the WRT54GL is stocked at Fry's Electronics and is available at [www.frys.com](#) IPv6 support is discussed [here](#).

Read about other people's experience using an Enterprise IPv6 firewall/IDS <http://www3.ietf.org/proceedings/07mar/slides/v6ops-6/v6ops-6.ppt>

Operational transition information

- There is a site on operations transition information at <http://civil-tongue.net/clusterf/>
- V6 Ops Transition Reality Presentation - <http://rip.psg.com/~randy/080312.cenic-v6-op-reality.pdf>
- Many ISPs will find NAT-PT to be useful. Iljitsch Beijnum describes [a modified NAT-PT](#).
- Most ISPs should set up various [Relay Services](#) to give the best connectivity to the v4/v6 Internet.
- There is some excellent [guidance on IPv6](#) from the APNIC community
- Proxying will be useful to allow v4 and v6 hosts to communicate. However it is not necessary to implement a special proxy for every protocol if you have a [web proxy that supports the HTTP CONNECT method](#).
- There are some subtle issues with [Enabling IPv6 on a Mail Server](#).
- The IETF has published [RFC 5211](#) by John Curran which outlines one possible timeline for transition of the Internet to IPv6.
- Andy Davidson, of NetSumo ISP Consultancy in the UK, discusses the IPv6 deployment they have done within their own organisation and for their customers. [Video here on YouTube](#)
- Voxel's blog provides perspective into a Internet Infrastructure/hosting company IPv6 migration <http://www.voxel.net/blog/2009/10/blog6-voxel-ipv6-update>
- Zahid Ghadialy's [Blog entry on IPv6 Transition for 3G and 4G cellular networks](#)
- [Cisco Tutorial on IPv6 Transition](#)
- [Discussion of IPv6 Deployment and Performance](#)

Planning IPv6 Deployment

This RIPE presentation covers the highlights [IPv6 Tutorial](#).

Google has a number of videos of Google tech talks on Youtube such as [Google IPv6 Conference 2008: Planning for the IPv6 Integration](#).

There is a good [blog on deploying IPv6](#) by the authors of O'Reilly's book on IPv6 Network Administration. Following this you get a good sense of the kinds of [corner cases](#) that you will need to deal with.

For an effective and successful IPv6 transition it is important to [collect and track metrics](#) measuring: The impact of IPv6 on IPv4, The user experience for IPv6 enabled services compared to the user experience for the existing IPv4 enabled services. Baselining the existing environment and services and then monitoring both IPv4 and IPv6 throughout IPv6 enablement will avoid the default finger pointing and will provide the metrics needed in reporting on the progress and success of the project.

In addition to planning the IPv6 transport network deployment, you also need to consider [DNS and Naming Issues](#) carefully. DNS servers will send AAAA records to hosts which may have IPv6 capability on the host, but not on their access network. For many years, Apple Macs, Linux Machines and Solaris servers have supported IPv6 out of the box. If they try to use the IPv6 addresses that you advertise, but their access network does not support IPv6, your site will appear to be malfunctioning.

You need to collect a knowledgebase of how to [Troubleshoot IPv6 Issues](#) so that your helpdesk staff and your NOC staff are prepared for the inevitable queries that will come in.

In addition to your own needs for [IPv6 Firewalls](#), you should prepare to help customers with information about new IPv6 firewall vendors as the market changes.

It is important to look at the different transition mechanisms and understand how and why you can implement these in your network to improve service to customers during the transition period when many Internet flows will have to travel over both IPv4 and IPv6.

- [Transitioning__6to4](#)

- [Transitioning__NAT64](#)
- [Transitioning__NAT-PT](#)
- [Transitioning__Teredo](#)
- [Transitioning__Tunnel Broker](#)

There is more info on the [Relay Services](#) page.

You should also evaluate [IPv6 Firewalls](#) both for your own use and to recommend to customers.

Look for transit providers here: [Providers Currently Selling IPv6 Transit](#)

United States

United States Government

The United States federal government has taken a three prong approach to IPv6.

- Military networks: Transition mandated by the Department of Defense
- Civilian government agency networks: Transition mandated by the White House
- Private networks: The Department of Commerce concluded in 2005 that the transition should be left to market forces, with the believe that US government transition efforts (DOD and civilian) would help drive the market.

In the process of transition, the US Government has produced a significant amount of documentation concerning implementation, testing, security, and other issues, that may be useful to other networks. These documents have been listed and linked on this wiki.

Area	Federal Agency with Responsibility
Military Networks	US Department of Defense
US Civilian Agency Networks	White House <ul style="list-style-type: none"> • CIO Council • IPv6 Task Force

[Specifications](#) | [NIST](#) |

[Testing](#) | [NIST](#) |

[Security](#) |

- [NIST](#)
- [DHS](#)
- [NSA](#) |

[Procurement Rules](#) | [Government Services Administration](#) |

[Private Networks \(US IPv6 Policy\)](#)

- [Department of Commerce, National Telecommunications and Information Agency](#)
- [Federal Communications Commission](#)
 - [Office of Strategic Planning and Policy Analysis](#)
 - [Office of Engineering and Technology Technology Advisory Committee](#) |

[International \(ITU\)](#)

- [NTIA Office of International Affairs](#)
- [Department of State](#) |

NIST

In 2005, the White House Office of Management and Budget (OMB) directed the National Institute of Standards and Technology (NIST) to develop standards and testing necessary to support adoption of IPv6 by US Government agencies. The NIST project is known as USGv6. NIST has developed a technical standards profile for US Government acquisition of IPv6 hosts and routers, and a specification for network protection devices. NIST is also actively establishing a testing program in order to test the compliance of products and vendors with the profile.

NIST IPv6 Documentation

- [IPv6 Economic Impact Assessment](#), RTI International for NIST (Oct. 2005)

USGv6 Profile

- NIST: Special Publication (SP) 500-267: A Profile for IPv6 in the U.S. Government - Version 1.0, July 2008
- NIST Issues Draft IPv6 Technical Profile, NIST 2/6/2007
 - [Frequently Asked Questions list](#)
 - [2007-01-31 Announcement of public comment period on Draft 1](#)
- Second Draft Profile
 - **Notice** : NIST has released a second draft of a proposed standards profile to support the implementation of Internet Protocol Version 6 (IPv6) by government agencies. NIST developed the "profile" to help ensure that IPv6-enabled federal information systems are interoperable, secure and able to co-exist with the current IPv4 systems. An initial draft of the NIST profile was released for comment one year ago (see "NIST Issues Draft IPv6 Technical Profile"). The second draft of A Profile for IPv6 in the U.S. Government - Version 1.0 develops a long-term strategy for 2010 and beyond. It incorporates the feedback from meetings with industry and government groups and input including more than 500 comments. The profile recommends technical standards for common network devices, such as hosts, routers, firewalls and intrusion detection systems. It also outlines the compliance and testing programs that NIST will be establishing to ensure that IPv6-enabled federal information systems are interoperable and secure, and that they work with existing IPv4 systems. NIST is calling for comments on the draft report by Feb. 29. For more information on the profile and to contribute comments, go to www.antd.nist.gov/usgv6 .

Security

- [Special Publication 800-119](#), Guidelines for the Secure Deployment of IPv6 This document is intended to help with the deployment of the next generation Internet Protocol, IPv6. It describes and analyzes IPv6's new and expanded protocols, services, and capabilities, including addressing, DNS, routing, mobility, quality of service, multihoming, and IPsec. For each component, there is a detailed analysis of the differences between IPv4 and IPv6, the security ramifications and any unknown aspects. It characterizes new security threats posed by the transition to IPv6 and provides guidelines on IPv6 deployment, including transition, integration, configuration, and testing. It also addresses more recent significant changes in the approach to IPv6 transition. Dec. 28, 2010
 - [Feb. 22, 2010 SP 800-119 DRAFT Guidelines for the Secure Deployment of IPv6](#)
- [Secure Domain Name System \(DNS\) Deployment Guide](#)

Testing

- NIST: Special Publication (SP) 500-273: IPv6 Test Methods: General Description and Validation - Version 1.0, August 2009
- [2007-05-04 IPv6 Testing Meeting Presentation Materials](#)
- [2007-04-17 Federal Register Announcement of IPv6 Testing Meeting](#)

NIST Presentations

- Doug Montgomery, IPv6: Hope, Hype and (Red) Herrings, NIST (2006) (presentation on the promise and misunderstandings surrounding IPv6)

References

- [CIO Council IPv6 Transition Guidance Sec. 5.2.6.1](#) "As the Federal government technical standards-making body, NIST will work with OMB and the IPv6 Working Group to evaluate the need for common standards and technical guidance. NIST will work with stakeholders to ensure any standards/guidance developed is in alignment with existing industry standards and is in the best interest of the Federal government. Furthermore, NIST will provide the IPv6 Advisory Group and OMB with additional guidance as necessary and maintain representation on the IPv6 Advisory Board."
- [OMB Memorandum 05-22](#) - Transition Planning for Internet Protocol Version 6 (IPv6) (August 2, 2005) ("The National Institute for Standards and Technology (NIST) will develop, as necessary, a standard to address IPv6 compliance for the Federal government.")

US Civilian Agency Networks

In 2005, the [United States](#) Office of Management and Budget (OMB) mandated that federal agencies initiate the transition to IPv6. According to the CIO Council:

The Office of Management Budget issued Memorandum M-05-22, "Transition Planning for Internet Protocol Version 6 (IPv6)", establishing the goal of enabling all Federal government agency network backbones to support the next generation of the Internet Protocol Version 6 (IPv6) by June 30, 2008. The memorandum required the agency's network backbone to be ready to transmit both IPv4 and IPv6 traffic, and support IPv4 and IPv6 addresses, by June 30, 2008. . . . The requirements for June 30, 2008 were for the network backbone (core) only. IPv6 did not actually have to be operationally enabled (i.e. turned on) by June 30, 2008. However, network backbones must have been ready to pass IPv6 traffic and support IPv6 addresses. Applications, peripherals, and other IT assets which are not leveraged in the execution of the functions mentioned above are not required for the June 30, 2008 deadline. CIO Guidance 2006

Moving the government's information technology from "ready" to "operational" will require additional work. On September 28, 2010, at a Department of Commerce IPv6 Workshop, OMB released a further memo Transition to IPv6 setting forth additional deadlines for the federal IPv6 transition:

In order to facilitate timely and effective IPv6 adoption, agencies shall:

- Upgrade public/external facing servers and services (e.g. web, email, DNS, ISP services, etc) to operationally use native IPv6 by the end of FY 2012;
- Upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 2014.

In 2005, OMB created an IPv6 Advisory Group and tasked the CIO Council with publishing transition planning guidance. The CIO Council established an Interagency IPv6 Working Group, headed by Peter Tseronis, Senior Advisor, US Department of Energy.

OMB also directed the National Institute of Standards and Technology (NIST) to develop standards and testing necessary to support adoption of IPv6 by US Government agencies. The NIST project is known as USGv6. NIST has developed a technical standards profile for US Government acquisition of IPv6 hosts and routers, and a specification for network protection devices. NIST is also actively establishing a testing program in order to test the compliance of products and vendors with the profile. The Government Services Administration updated the Federal Acquisition Regulation (FAR) to reflect the IPv6 specifications, and is assisting agencies with IPv6 procurement needs.

Documents

- **Office of Management and Budget**
 - Karen S. Evans, Administrator, Office of E-Government and Information Technology, [Transition Planning for Internet Protocol Version 6 \(IPv6\)](#), M-05-22 (Aug. 2, 2005).
 - Vivek Kundra, [Transition to IPv6](#), Memorandum for Chief Information Officers and Executive Departments and Agencies, Executive Office of the President, Office of Management and Budget (Sept. 28, 2010).
- **CIO Council**
 - [IPv6 Transition Guidance](#), Federal CIO Council Architecture and Infrastructure Committee, CIO Council (Feb. 2006).
 - [Federal CIO Council IPv6 Transition Guidance](#) (Mar. 4, 2008).
 - [Planning Guide/Roadmap Toward IPv6 Adoption within the US Government](#), The Federal CIO Council Architecture and Infrastructure Committee Technology Infrastructure Subcommittee Federal IPv6 Working Group (May 2009)
 - [IPv6 Frequently Asked Questions \(FAQ\)](#)
- **National Institute of Standards and Technology (NIST)**
 - [USGv6 Technical Infrastructure](#), Advanced Networks Division, NIST.
 - [USGv6 Testing Program](#), Advanced Network Technologies Division, NIST.
 - [IPv6 Economic Impact Assessment](#), RTI International for NIST (Oct. 2005).
 - [A Profile for IPv6 in the US Government – Version 1.0](#), Recommendations of NIST, NIST SP500-267 (Jul. 2008).
 - [Discussion Draft](#) (Feb. 22, 2007).
 - [Special Publication \(SP\) 500-273: IPv6 Test Methods: General Description and Validation - Version 2.0](#) (Nov. 30, 2009).
 - [Version 1](#) (Aug. 6, 2009).
 - [Discussion Draft](#)
 - [Special Publication 800-81r1, Secure Domain Name System \(DNS\) Deployment Guide](#) (Apr. 2010).
 - [Special Publication 800-119, Guidelines for the Secure Deployment of IPv6](#) (Dec. 28, 2010).
 - [Estimating USG IPv6 External Service Deployment Status](#).
- **Government Services Administration**
 - [GSA – IPv6](#)
 - [Federal Acquisition Regulation; FAR Case 2005-041, Internet Protocol Version 6 \(IPv6\)](#), Final Rule, 74 Fed. Reg. 65605 (Dec. 10, 2009) ("The Civilian Agency Acquisition Council and the Defense Acquisition Regulations Council (Councils) are issuing a final rule amending the Federal Acquisition Regulation (FAR) to require Internet Protocol Version 6 (IPv6) compliant products be included in all new information technology (IT) acquisitions using Internet Protocol (IP)".).
- **National Security Agency**
 - "Internet Protocol version 6 (IPv6) is being considered and deployed throughout the U.S. Government and private industry. The Information Assurance Directorate, Systems and Network Analysis Center (SNAC) of NSA is providing general guidance to make the implementation of IPv6 more secure."
 - [Firewall Design Considerations for IPv6](#) (Oct. 3, 2007).
 - [A Filtering Strategy for Mobile IPv6](#) (Sep. 19, 2007).
 - [Router Security Configuration Guide Supplement - Security for IPv6 Routers](#), Report No. I33-002R--6 (May 23, 2006).
- **Government Accounting Office**
 - [Internet Protocol Version 6: Federal Agencies Need to Plan for Transition and Manage Security Risks](#), GAO (May, 27 2005)
"Transitioning to IPv6 is a pervasive and significant challenge for federal agencies that could result in significant benefits to agency services. But such benefits may not be realized if action is not taken to ensure that agencies are addressing key planning considerations or security issues. Accordingly, we are recommending, among other things, that the Director of the Office of Management and Budget (OMB) instruct the federal agencies to begin addressing key IPv6 planning considerations, and that federal agency heads take immediate actions to address the near-term security risks."
- **NASA Research & Engineering Network: IPv6**

US Department of Defense

The US Department of Defense (DOD), with its network-centric operations, has high network address demands and therefore places a priority on the expanded address space. In 2003, it was the first government branch to announce an IPv6 transition policy, declaring that: "The achievement of net-centric operations and warfare, envisioned as the Global Information Grid (GIG) of inter-networked sensors, platforms and other Information Technology/National Security System (IT/NSS) capabilities, depends on effective implementation of IPv6 in concert with other aspects of the GIG architecture." (DOD Memo 2003) The DOD set 2008 as the deadline by which it should complete its IPv6 transition. DOD's transition to IPv6 has been described as "aggressive" and DOD has operational plans that would require a high demand on a network address space.

Documentation

- DOD Memo for Secretaries of the Military Departments, From Dept of Defense Chief Information Officer, [Internet Protocol version 6 \(IPv6\)](#) (Jun. 9, 2003).
- [Marine Corps Internet Protocol version 6 \(IPv6\) Policy](#).
- Priscilla E. Guthrie, Deputy Assistant Secretary of Defense, Deputy CIO, [Transition Planning for Internet Protocol version 6](#) (Aug. 16, 2005).
- [DOD IPv6 Generic Test Plan Version 4](#), DISA (May 2009).
- [Special Interoperability Certification for IPv6 Capability](#), Joint Interoperability Test Command (listing products tested for IPv6 Capability).
 - [DoD IPv6 Standards Profiles for IPv6 Capable Products, Version 4](#).
 - [DoD IPv6 Standards Profiles for IPv6 Capable Products, Version 5](#).
 - [DoD IPv6 Generic Test Plan, Version 4](#).
- [IPv6 Template - IPv6 Letter of Compliance Template \(XLS\)](#) DISA.
- [Defense Research and Engineering Network IPv6 Backbone](#).
- [DoD HPCMP: IPv6 Pilot Information](#).

US IPv6 Policy

From [Potential Impacts on Communications from IPv4 Exhaustion & IPv6 Transition FCC Working Paper](#), December 2010 (public domain)

In 2004, the Department of Commerce (the National Telecommunications and Information Administration (NTIA) and the National Institute of Standards and Technology (NIST)) initiated an investigation into the US Government's policy response to IPv6. This culminated with the release of the 2006 Report [Technical and Economic Assessment of Internet Protocol, Version 6 \(IPv6\)](#). In the Report, the Department of Commerce stated:

Industry stakeholders and Internet experts generally agree that IPv6-based networks would be technically superior to the common installed base of IPv4-based networks. The vastly increased IP address space available under IPv6 could potentially stimulate a plethora of new innovative communications services. Deployment of IPv6 would, at a minimum, "future proof" the Internet against potential address shortages resulting from the emergence of new services or applications that require large quantities of globally routable Internet addresses.

Current market trends suggest that demand for unique IP addresses could expand considerably in future years. The growing use of the Internet will likely increase pressures on existing IPv4 address resources, as more and more people around the globe seek IP addresses to enjoy the benefits of Internet access. In addition, the potential development of new classes of networked applications (e.g., widely available networked computing in the home, the office, and industrial devices for monitoring, control, and repair) could result in rapid increases in demand for global IP addresses.

Over time, IPv6 could become (as compared to IPv4) a more useful, more flexible mechanism for providing user communications on an end-to-end basis. The redesigned header structure in IPv6 and the enhanced capabilities of the new protocol could also simplify the configuration, and operation of certain networks and services. These enhancements could produce operations and management cost savings for network administrators. In addition, auto-configuration and other features of IPv6 could make it easier to connect computers to the Internet and simplify network access for mobile Internet users.

Addressing the appropriate role for the government in promoting the transition, the Department of Commerce at that time concluded,

The Task Force finds that no substantial market barriers appear to exist that would prevent industry from investing in IPv6 products and services as its needs require or as consumers demand. The Task Force, therefore, believes that aggressive government action to accelerate deployment of IPv6 by the private sector is not warranted at this time. The Task Force believes that, in the near term, private sector organizations should undertake a careful analysis of their business cases for IPv6 adoption and plan for the inevitable emergence of IPv6 traffic on both internal and external networks.

In 2010, the Department of Commerce [announced](#) that grantees for the Comprehensive Community Infrastructure Awards, which are part of the NTIA Broadband Technology Opportunity Program (BTOP) stimulus grants, must report on "Internet protocol address utilization and IPv6 implementation." Recipients are required to file quarterly reports until the end of their funding.

On September 28, 2010, NTIA convened an [IPv6 Workshop](#), during which Assistant Secretary of Commerce for Communications and Information Lawrence Strickling stated,

(F)or industry in particular – smart-phone and router manufactures, transport providers, Internet service providers, and chief information and technology officers throughout the industry – action is needed. Today we want to impress upon everyone that this is an urgent issue, but one that can be successfully handled with good planning. And we want to encourage companies to share best practices on IPv6 uptake for all businesses to benefit, particularly for small- and medium-sized enterprises.

The NTIA event, which was moderated by US CTO Aneesh Chopra and US CIO Vivek Kundra, highlighted the importance of industry and government working together, sharing information and best practices that could facilitate the transition. At the event, the CIO Council released its new memo with the new deadlines for the federal IPv6 transition.

Fundamental to the US IPv6 policy is the belief that the US Governments' procurement of IPv6 equipment and services for [US Civilian Agency Networks](#) will help drive the mark forward to IPv6.

In December 2010, the Federal Communications Commission released a working paper entitled [Potential Impacts on Communications from IPv4 Exhaustion & IPv6 Transition FCC Working Paper](#), December 2010. The FCC's [Technology](#)

Advisory Committee is also examining IPv6. Discussion of IPv6 was noticeably absent from the FCC's [Broadband Plan](#).

The FBI has been active in the ARIN Government Working Group, represent the concerns of law enforcement with the IPv6 transition.

Documents

- Department of Commerce
 - [Technical and Economic Assessment of Internet Protocol, Version 6 \(IPv6\)](#), IPv6 Task Force, Department of Commerce (Jan. 2006).
 - [NTIA Report: Technical and Economic Assessment of IPv6](#) (Jul 2004) (Discussion Draft).
 - [Notice of Funds Availability \(NOFA\) and Solicitation of Applications](#), Broadband Technology Opportunities Program, National Telecommunications and Information Administration, US Department of Commerce, 75 Fed. Reg. 3792 (Jan. 22, 2010).
 - [Agenda, Internet Protocol Version 6 \(IPv6\) Workshop: The Impact of the Adoption and Deployment of IPv6 Addresses for Industry, the US Government, and the Internet Economy](#), US Department of Commerce, National Telecommunications and Information Administration, September 28, 2010.
- Federal Communications Commission
 - [Potential Impacts on Communications from IPv4 Exhaustion & IPv6 Transition](#) FCC Working Paper, December 2010.
 - FCC Office of Engineering and Technology, [Technology Advisory Committee](#)
- Department of Homeland Security
 - [Malware Tunneling in IPv6](#) (May 26, 2005).

Porting Applications

This page is intended to track resources that will aid in porting Applications from IPv4 only code to IPv4/IPv6 dual stack capable applications.

Owen DeLong's porting presentation

http://meetings.apnic.net/__data/assets/pdf_file/0011/18848/Porting-IPv4-Applications-to-Dual-Stack_Owen-Delong.pdf

Jun-ichiro itojun Hagino's preso

www.ipv6.or.kr/summit2003/presentation/II-2.pdf

Mark Blanchet Presentation - May 2000

<http://www.viagenie.qc.ca/en/ipv6/presentations/IPv6%20porting%20appl v1.pdf>

Indiana University presentation - June 2004

http://www.cu.ipv6tf.org/pdf/IPv6_Porting_Issues.pdf

Eva Castro's web page and presentation from 2003

<http://gsyc.escet.urjc.es/~eva/IPv6-web/ipv6.html>

http://www.usipv6.com/2003arlington/presents/Eva_Castro.pdf

IETF RFCs:

RFC 3493 - Basic Socket Interface Extensions for IPv6

<http://www.ietf.org/rfc/rfc3493.txt>

RFC 3542 - Advanced Sockets Application Program Interface (API) for IPv6

<http://www.ietf.org/rfc/rfc3542.txt>

RFC 4038 - Application Aspects of IPv6 Transition

<http://www.ietf.org/rfc/rfc4038.txt>

RFC 5014 - IPv6 Socket API for Source Address Selection

<http://www.ietf.org/rfc/rfc5014.txt>

Providers Currently Selling IPv6 Transit

This is a list of companies that are known to currently sell native IPv6 transit (in alphabetical order).

(for a global list with region details, see: [SixXS: Where can I get native IPv6 transit?](#) and [SixXS: Where can I get native IPv6 / Which ISP's provide IPv6?](#) for native link providers)

- [bit \(Europe NL\)](#)
- [Cogent](#)
- [Flag \(Asia\)](#)
- [Global Crossing](#)
- [Hurricane Electric](#)
- [Internap \(US, Europe, Asia\)](#)
- [LambdaNet Communications](#)
- [Mythic Beasts Ltd \(UK\)](#)
- [NTT Communications \(fka NTT/Verio\)](#) (Asia, Europe, US, Australia) Global Website (v4 or v6): <http://www.ntt.net>
- [Opentransit / Orange / France Telecom](#) (US, Europe, Singapore) <http://www.orange.com/wholesalesolutions/oursolutions/internetbandwidth/oti.html>

- Qwest
- Sprint
- Tele2 / SWIPNet (Europe, US) <http://ipv6.tele2.net>
- Teleglobe
- TeliaSonera IC (native in select cities, via Layer2 tunneling in others)
- Tinet (formerly, Tiscali International): selling IPv6 worldwide: <http://www.tinet.net>
- UnitedLayer

This is not an advertisement for these companies, and should not be interpreted as any kind of endorsement. Buyer beware. Your mileage may vary.

Also see the [Carrier Support](#) page.

Transparent Internet Access

John Curran commented in a message to NANOG:

There are companies which would like to be connecting new customers with IPv6 as we approach IPv4 depletion and then handle v translation for IPv4 site connectivity in their network i.e. customers connecting to "The Internet" via only IPv6 with the expectation of reaching all Internet destinations (IPv4 and IPv6) without any hassles.

While making the backbone networks dual-stack is going to be serious work, it's at least an understandable goal that operators can make plans to hit. That's not the case with the requirement to provide transparent connectivity to IPv4 destinations via IPv6 transport. NAT-PT wasn't exactly an elegant solution, but it's now precisely what some providers are looking for (so connecting customers via just IPv6 is at least viable). Without it, every provider is going to come up with ad-hoc customer connection models with various IPv4 tunnelling and translation games once IPv4 address blocks become generally unavailable.

The irony is that the I* rationale for moving NAT-PT to historic was "to restore the end-to-end transparency of the Internet" and yet the only real chance we have to restore end-to-end transparency is to first have a transition to the IPv6 (using dual-stack, NAT-PT, and every other tool at our disposal) and then over time let present IPv4 destination sites add IPv6 for end-to-end transparency based on their actual need for it. Instead, central planning may have effectively killed the very tool that's needed to allow providers to provision new Internet customers over a pure IPv6-only model, and create the right motivation for existing Internet sites to go dual-stack and actually gain "end to end transparency" via IPv6.

In a nutshell, we need to be able to provide IPv6 connected users with a transparent view of all Internet resources regardless of whether those resources use IPv4 or IPv6 access. And we also need to provide IPv4 Internet users with the same kind of transparent view. Without this last capability in our networks, we will not be able to convince hosting customers to use IPv6 network access services.

Implementing the transition strategies documented in [First Steps for ISPs](#) will only solve part of this puzzle. To make a fully transparent Internet access service will also require implementing protocol translation (NAT-PT) or proxy services (ALG). Some resources for this are available on the [Operational transition information](#) page, but this is an area that needs a lot more effort to trial technologies and document how best to implement them. The existing technologies are discussed on the [Relay Services](#) page.

Some have suggested that a good way to do this work would be to prepare and plan for supporting an Internet community meeting such as IETF or NANOG with only IPv6 Internet access. If transparent access is successfully deployed, it means that all the IPv4 users at the meeting, and at home, will not notice the fact that there is no IPv4 Internet access at the meeting. This goes beyond tunneling IPv4 over IPv6 because applications will make DNS queries for the wrong kind of record (A or AAAA) in order to make a connection. These queries need to be spoofed in order for successful transparent communication to occur.

US Government - USGv6 Technical Infrastructure

As a part of the [United States](#) Government's transition of [US Civilian Agency Networks](#) to IPv6, OMB Memorandum M-05-22 directed the National Institute of Standards and Technology (NIST) to develop the technical infrastructure (standards and testing) necessary to support wide scale adoption of IPv6 in the US Government (USG). In response NIST developed a technical standards profile for US Government acquisition of IPv6 Hosts and Routers, and a specification for Network Protection Devices. The Host and Router profile includes a forward looking set of RFCs published by the Internet Engineering Task Force (IETF), encompassing basic IPv6 functionality, and specific requirements and key optional capabilities for routing, security, multicasting, mobility, network management, and quality of service. The Network Protection Device profile contains a NIST established set of capability requirements for IPv6 aware firewalls and intrusion detection systems.

Additional information is available on the [Technical Infrastructure for USGv6 Adoption](#) page. Information on [Participating Test Laboratories and Accreditors](#) is also available.

Vendors in the ARIN Region

This page was created in response to the following discussion: <http://lists.arin.net/pipermail/arin-discuss/2009-September/001525.html>

- [Vendors in the ARIN Region 6connect](#)
- [Vendors in the ARIN Region Acme Packet](#)
- [Vendors in the ARIN Region Adtran](#)
- [Vendors in the ARIN Region Airspan](#)
- [Vendors in the ARIN Region APC](#)
- [Vendors in the ARIN Region Calix](#)
- [Vendors in the ARIN Region Cisco](#)

- [Vendors in the ARIN Region Comtrend](#)
- [Vendors in the ARIN Region Ericsson](#)
- [Vendors in the ARIN Region Hostik](#)
- [Hostik](#)
- [Vendors in the ARIN Region HP](#)
- [Vendors in the ARIN Region Procera Networks](#)
- [Vendors in the ARIN Region RG Nets](#)
- [Vendors in the ARIN Region TIVO](#)
- [Vendors in the ARIN Region Yamaha](#)

Vendors in the ARIN Region 6connect

Datacenter management has grown to encompass more and more of IT and Facilities- but the tools haven't really matured. Generally, solutions are costly to implement, come with expensive licensing and can't be customized to your business. Our team dealt with these market dynamics and finally decided to build our own solution. 6connect's DCIM is purpose built from the ground up to be simple, easy to use, secure, and scalable.

Whether you are looking for better tools to manage your datacenter, or finding resources to help optimize and automate your business processes -from IPv6 strategy to distributed computing and facility integration, our team can help.

6connect
 548 Market St, #39313
 San Francisco, CA 94104

Telephone: +1-408-329-6901
 Email: webinfo@6connect.com

Online at: <http://www.6connect.com/>

Vendors in the ARIN Region Acme Packet

Acme Packet enables the delivery of trusted, first-class interactive communications—voice, video and multimedia sessions—and data services across IP network borders. Our Net-Net family of session border controllers, multiservice security gateways and session routing proxies supports multiple applications in service provider, enterprise and contact center networks—from VoIP trunking to hosted enterprise and residential services to fixed-mobile convergence. They satisfy critical security, service assurance and regulatory requirements in wireline, cable and wireless networks; and support multiple protocols—SIP, H.323, MGCP/NCS, H.248 and RTSP—and multiple border points—service provider access and interconnect, and enterprise access and trunking.

Acme Packet
 71 Third Avenue
 Burlington, MA 01803 USA
 Telephone (781) 328-4400
 Fax (781) 425-5077
info@acmepacket.com

<http://www.acmepacket.com>

Vendors in the ARIN Region Adtran

ADTRAN, Inc. is a leading global provider of networking and communications equipment with an innovative portfolio of more than 1,700 solutions for use in the last mile of today's telecommunications networks. Widely deployed by carriers, distributed enterprises and Small- and Medium-sized Businesses (SMBs), ADTRAN solutions enable voice, data, video, and Internet communications across copper, fiber, and wireless network infrastructures. ADTRAN solutions are currently in use by every major U.S. service provider and many global ones, as well as by thousands of

public, private and governmental organizations worldwide. ADTRAN is headquartered in Huntsville, Alabama, with sales offices strategically located throughout the United States and around the world.

Contact ADTRAN
ADTRAN, Inc.
901 Explorer Boulevard
P.O. Box 140000
Huntsville, AL 35806

800-9ADTRAN

<http://www.adtran.com>

Vendors in the ARIN Region Airspan

Airspan has been a leading vendor of wireless products and solutions since 1992. Today we have more than 500 customers in 100 countries around the world.

Airspan has been at the forefront of developing these new wireless standards. Furthermore, by creating in-house expertise in WiMAX, Wi-Fi and VoIP, Airspan is able to exploit synergies and come up with innovative products and solutions that closely integrate these technologies in the most beneficial ways for our customers.

Headquarters:
Airspan Networks Inc.
777 Yamato Road
Suite 310 Boca Raton
FL 33431 USA
Tel: +1 561 893-8670
Fax: +1 561 893-8671

<http://www.airspan.com>

Vendors in the ARIN Region APC

In today's "always on, always available" world where businesses can't stop and downtime is measured in dollars, American Power Conversion (APC) provides protection against some of the leading causes of downtime, data loss and hardware damage: power problems and temperature. As a global leader in network-critical physical infrastructure (NCPi) solutions, APC sets the standard in its industry for quality, innovation and support. Its comprehensive solutions, which are designed for both home and corporate environments, improve the manageability, availability and performance of sensitive electronic, network, communications and industrial equipment of all sizes.

132 Fairgrounds Road
W. Kingston , RI 02892
UNITED STATES

<http://www.apcc.com>

Vendors in the ARIN Region Calix

Calix: The Largest Communications Equipment Supplier Focused Solely on Access

Several hundred service providers operating tens of millions of access lines depend on Calix to power their access networks. Industry-leading solutions deployable throughout the access network enable a rich set of information, communication, and entertainment services over any combination of fiber and copper, thus helping Calix customers gain a competitive edge. And an extremely high degree of integration and robust service management allow Calix customers to operate their access networks at the lowest possible cost. Massive service capacity over extreme operational efficiency—these are what make Calix an ideal access partner.

But Calix goes beyond innovative, future-hedging access network solutions; we simplify all aspects of the service deployment process. A tightly integrated vertical supply chain improves quality and scale while reducing lead times. A broad set of Calix Compatible partners ensure smooth and fast deployment of leading-edge, IP-based services. And a host of no-cost service and support functions dramatically simplify training, troubleshooting, and network upgrades. Calix makes it simple.

They can be contacted at:

Petaluma Headquarters
1035 N. McDowell Blvd.
Petaluma, CA 94954
Phone: 707-766-3000
Fax: 707-766-3100
Email: info@calix.com

<http://www.calix.com>

Vendors in the ARIN Region Cisco

Cisco is a networking equipment vendor. They can be contacted at:

Cisco Systems, Inc.
170 West Tasman Dr.
San Jose, CA 95134
USA
(408) 526-4000
(800) 553-NETS
(800) 553-6387

<http://www.cisco.com>

Vendors in the ARIN Region Comtrend

With more than 10 million products installed, COMTREND CORPORATION is a leading global supplier of advanced networking solutions. Comtrend is a ISO-9001/14001 certified company that designs, manufactures, and markets a wide range of networking equipment integrating

ADSL, ADSL2+, Bonded ADSL2+, VDSL2, VOIP, IP STB Multimedia, Residential Wi-Fi, Auto Configuration Systems, Digital Signage Applications and High-Speed PLC technology. Comtrend is committed to a vision of bringing people together through technology and continues to realize this vision through a focus on innovation and superior service.

You can reach us by:
Phone: 1-877-COMTREND
Tel: 1-949-753-9640
Fax: 1-949-753-9020
Mail: 15375 Barranca Parkway, Suite C-104 Irvine, CA 92618, USA

<http://www.comtrend.com>

Vendors in the ARIN Region Ericsson

Ericsson is a world-leading provider of telecommunications equipment and related services to mobile and fixed network operators globally. Over 1,000 networks in more than 175 countries utilize our network equipment and 40 percent of all mobile calls are made through our systems. We are one of the few companies worldwide that can offer end-to-end solutions for all major mobile communication standards.

Peter Olofsson
Head of Industry Analyst Relations, Global
Phone: +46 10 7191880
E-mail: industry.analysts@ericsson.com

Rob Elston
Industry Analyst Relations, Americas
Phone: +1 972 583 0982
E-mail: industry.analysts@ericsson.com

Kathy Egan
Industry Analyst Relations, Americas
Phone: +1 212 843 8422
E-mail: industry.analysts@ericsson.com

Colleen Rosander
Industry Analyst Relations, Americas
Phone: +1 724 742 7794
E-mail: industry.analysts@ericsson.com

<http://www.ericsson.com>

Vendors in the ARIN Region Hostik

Lanset America Corp. offers dual stack/Native IPv6 connectivity at their Colocation facility DataNOC in Sacramento California. Please visit DataNOC.com and Hostik.com for more information.

Hostik

Lanset America Corp. DBA Hostik Provides IPv6/IPv4 Dual Stack/Native connectivity. Please visit Hostik.com or DataNOC.com

Vendors in the ARIN Region HP

Networks are growing in importance and scope for today's organizations.

As a longtime networking industry leader, HP ProCurve is a safe choice for the best available products, solutions and customer care (services and technical support) to meet those challenges.

HP should be encouraged to implement IPv6 on their printers.

Hewlett-Packard Company
3000 Hanover Street
Palo Alto, CA 94304-1185 USA
Phone: (650) 857-1501
Fax: (650) 857-5518
Open between 8:00 a.m. and 5:00 p.m. Pacific Time, Monday - Friday.

<http://www.hp.com>

Vendors in the ARIN Region Procera Networks

Procera Networks develops Evolved DPI solutions that provide the most accurate traffic awareness, control and protection for complex networks. Its PacketLogic™ product suite was purpose-built for DPI and leverages the company's advanced identification engine, DRDL™. DRDL delivers previously unseen accuracy and an unchallenged low false-positive rate even as applications get encrypted.

Most important to making the right decision is to have access to, and rely on, accurate intelligence – this is where PacketLogic stands out from the competition. PacketLogic is deployed at more than 400 broadband service providers, telcos, governments and higher education campuses worldwide.

Corporate Offices

Procera Networks, Inc.
100 Cooper Court
Los Gatos, CA 95032

Phone:
+1 408-890-7100
1-877-PROCERA (776-2372)

E-mail: info@proceranetworks.com

Fax: +1 408-354-7211

<http://www.proceranetworks.com>

Vendors in the ARIN Region RG Nets

RG Nets is the leading provider of gateways and centralized-authentication appliances designed to manage, provision, and protect revenue-generating networks. rXg turn-key gateways offer customer networks of all sizes a single integrated network-provisioning appliance for cost-effective and scalable network deployments. All of the functions and features required in today's revenue-generating policy-enforcement networks are bundled in one rXg device. Headquartered in Carson City, NV, RG Nets has a worldwide sales and technical support organization, along with a global network of resellers and integrators. With over a decade of experience in this space, the team at RG Nets delivers unparalleled solutions to maximize the profitability of your network.

info@rgnets.com
+1 408 441 0100

<http://rgnets.com>

Vendors in the ARIN Region TiVO

TiVO desperately needs encouragement to implement IPv6 in their products.

TiVO Inc.
2160 Gold Street
P.O. Box 2160
Alviso, CA 95002-2160

408-519-9100
Fax: 408-519-5330

<http://www.tivo.com>

Vendors in the ARIN Region Yamaha

Yamaha produces very nice audio components, some of which are controllable via IP. Unfortunately, according to Yamaha, they have no plans to support IPv6.

It would be nice if they were encouraged to do so.

Yamaha Electronics Corporation, USA
6660 Orangethorpe Avenue
Buena Park, CA 90620

Fax: 714-522-9832

<http://www.yamaha.com>

Implement and Manage IPv6

This category is for articles covering issues related to actual in-production usage of IPv6. This can include network management, troubleshooting, or other topics involved in supporting IPv6 on a network, as well case studies of IPv6 deployments.

- [Apache HTTPD](#)
- [Customer problems that could occur](#)
- [Providers of IPv6 Services](#)
- [DNS and Naming Issues](#)

- Implementing 6PE
- IPv6 Management Tools
- ISP IPv6 Implementations
- Relay Services
 - Cisco 6to4 Relay Service
 - FreeBSD Teredo Relay
 - Juniper 6to4 Relay Service
 - Linux or BSD 6to4 Relays
 - ISPs currently announcing a 6to4 prefix
 - Miredo
 - Transitioning__6to4
 - Transitioning__NAT64
 - Transitioning__NAT-PT
 - Transitioning__Teredo
 - ISPs currently announcing a teredo prefix
- Renumbering an IPv6 Network
- Troubleshoot IPv6 Issues
- FreeBSD
- Linux Support
- Solaris IPv6 Sites
- Warning broken users with JavaScript
- 3GPP Mobile Networks
- IPv6 Consulting and Training Services
 - A Wireshark IPv6 Configuration Profile
 - IPv6 Training and Consulting Services
- IPv6 Hosting and DNS Providers

External links

- [ISP IPv6 Service Comparison](#)
- [Status of IPv6 in various OS'es](#)
- [Wiki for testing single stack IPv6 \(IPv6-only\)](#)
- [Discussion of IPv6-enabled mail systems](#)
- [C Language examples of IPv4 & IPv6 raw socket calls](#)

Apache HTTPD

Detecting IPv6 Clients

You can configure Apache HTTPD to set an environment variable if the client is using IPv6:

1. httpd.conf
2. Set an environment variable if access is IPv6

```
SetEnvIfNoCase REMOTE_ADDR "^0-9a-f+$" IPV6_USER=1
```

If [Server Side Includes](#) are enabled, you can modify page content based on whether the client is using IPv4 or IPv6:

```
Hello client from
<!--#echo var="REMOTE_ADDR" -->
<br>
<!--#if expr="$IPV6_USER" -->
<b>You are using IPv6. Good!</b>
<!--#else -->
<b>You are not using IPv6.</b>
<!--#endif -->
```

Customer problems that could occur

If you know of any issues that customers might encounter during the transition to IPv6, please add a subheading to this page and explain both the problem and how to address it.

Broken users unable to access dual-stacked content

A small number of users have some kind of misconfiguration or bug in their internet connection that makes them unable to properly access dual-stacked web sites. More often than not, these users have no problems accessing IPv4-only sites, which causes them to perceive the dual-stacked site as the one having problems. A web site operator can detect these users using JavaScript and potentially warn them about the problem, see [Warning broken users with JavaScript](#).

The existence of these users is unfortunately causing content providers to put off enabling IPv6. For more information, see these presentations by Yahoo (https://sites.google.com/site/ipv6implementors/2010/agenda/07_Fesler_Y!atGIPv6ImpConf.pdf?attredirects=0), [Google](#), and [Redpill Linpro](#). There's also an [article about the problem](#) in Wikipedia.

This section attempts to document the most common causes as to why this happens, and how end users can solve it. It is based on real operational experience from running dual-stacked web sites.

Use of transitional IPv6 connectivity

Transitional IPv6 connectivity (6to4 or Teredo), is usually less reliable than IPv4. For this reason, the end user's web browser should prefer to use IPv4 when attempting to access dual-stacked site. This is well documented in [I-D.vandeveldede-v6ops-harmful-tunnels](#), as well as by researchers [E mile Aben](#) and [Geoff Huston](#).

6to4 router functionality is implemented and often enabled by default in a large number of home gateway products made by several different vendors. This is unfortunately in accordance with Microsoft's [requirements for Windows-compatible home routers](#). Due to the fact that not all operating systems and applications de-prefer transitional IPv6 connectivity, it is recommended to disable it (especially 6to4) whenever possible.

Due to the operational problems with 6to4, the IETF has recently moved towards deprecating it and discouraging any further use of it, by adopting [I-D.ietf-v6ops-6to4-to-historic](#) as a IETF v6ops Working Group document.

Android

Earlier versions of Android preferred transitional IPv6 connectivity above IPv4, as its system resolver did not implement RFC 3484.

Solution: Upgrade Android to version 2.2 Froyo or later.

Apple Mac OS X

Mac OS X, in versions earlier than 10.6.5, do not de-prioritize 6to4 compared to IPv4.

Solution: Upgrade Mac OS X to the latest available version.

Versions predating 10.6.x «Snow Leopard»

At the time of writing, the patch that de-prioritizes 6to4 is only available for the «Snow Leopard» series (10.6.x). Avoiding 6to4 entirely is the best solution, but might not always be possible or feasible when another device in the network is announcing itself as a 6to4 router. Users on old PowerPC systems have no upgrade path from 10.5.

Work-around: Use the latest version of [Google Chrome](#), which will mask the underlying problem.

Work-around: Disable IPv6 completely in the operating system: *System Preferences -> Network -> Advanced -> TCP/IP -> Configure IPv6 -> Off*.

GNU/Linux

The GNU C Library will de-prefer transitional IPv6 connectivity if the local IPv4 address is not a private one (RFC 1918), due to a strict interpretation of RFC 3484 (see [SW#11438](#)).

Solution: Upgrade the Linux distribution to [Debian Squeeze](#), [Fedora 13 Goddard](#), [Ubuntu 10.04 Lucid Lynx](#), [Mandriva 2010.1 Spring](#), [openSUSE 11.3](#), [Gentoo 2010-04-25](#), or any later versions.

Alternative solution: Add the following lines to the file `/etc/gai.conf` (create it if it doesn't exist):

```
scopev4 ::ffff:169.254.0.0/112 2
scopev4 ::ffff:127.0.0.0/104 2
scopev4 ::ffff:0.0.0.0/96 14
```

Microsoft Windows

MS Windows automatically enables Teredo and 6to4 whenever possible. The system resolver library will de-prioritize their use, but not all applications use the system resolver library and will therefore end up preferring the less reliable transitional IPv6 connectivity.

Solution: Disable 6to4 and Teredo, by entering the following commands in an Administrator shell:

```
netsh interface ipv6 6to4 set state disabled
netsh interface teredo set state disabled
```

Alternatively, visit [Microsoft KB#929852](#), and choose the **Disable IPv6 tunnel interfaces** fix (solution 50443).

Internet Connection Sharing

If Internet Connection Sharing is enabled on **any** interface (it doesn't even have to be connected), the Windows hosts will announce itself as an IPv6 router to the local network. This will in turn cause problems for other operating systems that doesn't de-prioritize transitional IPv6 connectivity, notably Mac OS X (see above).

Solution: Disable 6to4 and Teredo as described above, and also ensure Internet Connection Sharing is disabled whenever unused.

Opera web browser

The Opera web browser uses its own resolver library, and would in versions earlier than 10.50 (on Microsoft Windows) and 10.63 (on Mac OS X and Linux) prefer transitional IPv6 connectivity above IPv4.

Solution: Upgrade Opera to the latest available version.

Home gateways and broadband routers

Apple

The AirPort and Time Capsule wireless base stations will advertise the prefix `::/64` on their LAN interfaces if they are set up with IPv6 mode **tunnel** while having a private (RFC 1918) address assigned to their WAN interfaces. As the resulting auto-configured addresses are invalid, hosts on the LAN will suffer dual-stack breakage. The bug was last reported in firmware version 7.4.2, and is confirmed to be fixed in firmware version 7.5.2).

Solution: Upgrade the firmware of the AirPort/Time Capsule to the latest available version ([instructions](#)).

AVM

Certain AVM FRITZ!Box models (at least 7270 International v2) is known to have ULA (RFC 4193) functionality based on recommendations from IETF [-D.ietf-v6ops-ipv6-cpe-router](#) revision 07 or earlier (the advertised router lifetime is greater than 0). When IPv6 is enabled on the device, it will announce a ULA prefix, which is withdrawn as soon as a global prefix is available, including a 6to4-derived one. Like ULA, 6to4 is enabled by default by the overall IPv6 configuration setting.

If the device is used in a IPv4-only environment with CGNAT/NAT444 where the WAN interface is numbered using RFC 1918 addresses, 6to4 is never activated and the ULA addresses will continue to be announced. Because ULAs are globally scoped addresses that are not special-cased in RFC 3484, this will cause hosts on the LAN to attempt to use them when connecting to dual-stacked destination, which cannot work.

Solution: Ensure ULA functionality is disabled. This can be done from the router's web interface - instructions follows:

1. Open <http://fritz.box/> with your web browser.
2. Enter your FRITZ!Box password.
3. Click *Settings* (towards the top of the window).
4. Click *Internet*.
5. On the left, click *Account Information*.
6. Select the *IPv6* tab on the right side, towards the top of the window, under the heading *Account information*.
7. You are now on the IPv6 settings page. The last section of this page is called *Unique Local Addresses*. In this section, select **do not assign unique local addresses (ULA) (not recommended)**.
8. Click *Apply*.

Cisco Linksys

E2000, E3000, and E4200

These models (and possibly others which share the same code) offers by default DHCPv6 service that assigns addresses to the LAN hosts from the documentation prefix 2001:db8::/32. However, no ICMPv6 Router Advertisements are being sent in this case, which causes the LAN hosts to not have a default route, thus causing the host operating stack to generate fast internal failures when IPv6 is attempted.

They also enable 6to4 router functionality by default. If 6to4 is active (i.e. if the WAN interface is numbered using a public IPv4 address), ICMPv6 Router Advertisements will be transmitted to the LAN segment, containing a Prefix Information Option for the 6to4 prefix.

Luckily, the networking stack in Microsoft Windows will immediately remove the DHCPv6-assigned bogon address from 2001:db8::/32 upon receiving an ICMPv6 Router Advertisement. As Microsoft Windows is the only major operating system that supports DHCPv6 (and uses it even when there are no ICMPv6 RAs), end users are unlikely to experience brokenness due to this issue.

The recent firmware revisions disable both 6to4 and the DHCPv6 service with the bogon addresses by default, solving all known problems.

Solution: Upgrade the router firmware to the firmware version indicated below (or newer):

- E2000: [1.0.04 \(build 07\)](#)
- E3000: [1.0.04 \(build 06\)](#)
- E4200: [1.0.04 \(build 07\)](#)

Select the *Downloads* tab on the pages linked to above in order to acquire the latest firmware image and its corresponding release notes.

As of 10/8/2011, the E2000 link above is 404 and the E4200 link leads to firmware 1.0.03 (released 9/28/11).

Firmware 1.0.03 of E4200 suffers from the same problem as the Fritz in that it provides ULA addresses which Windows 7 uses as source addresses. There does not appear to be a way to disable ULA on the E4200 router in 1.0.03.

On a related note: Firmware 1.0.00, which performs tunneling by default, but does not provide ULA, works out of the box. Do not update to 1.0.03 if your configuration is working.

IPv6/6to4 settings can be configured from (assuming 192.168.1.1 is the IPv4 address of the device):

- E4200: <http://192.168.1.1/SystemConfig.asp>
- E3000: <http://192.168.1.1/System.asp> (the on/off toggle is labeled *Vista Premium*)
- E2000: Unknown - probably one of the above.

WRVS4400N

This model (and possibly others) uses the bogon range 2005:123:456:789::/64 as its default DHCPv6 pool. These addresses cannot be used to communicate with the IPv6 internet, and their presence on end-user hosts will cause end-user brokenness.

Solution: Ensure the router is operating in IPv4-only mode. This setting is found under *Setup -> IP Versions* in its web interface.

D-Link

Several D-Link models from the *DSL* series (at least DSL-584T, DSL-G604T, DSL-G624T, DSL-G664T, and DSL-G684T), do not correctly forward DNS responses for hostnames with both A and AAAA records published. What it does is to stuff the first 32 bits of the AAAA record into the A record that's being returned to the end user's computer. In other words, *getip6.info* will incorrectly resolve to 32.1.5.0 (the *2001:0500:* part of the IPv6 address). If the operating system or web browser prefers to use IPv4, it will be unable to connect to the destination.

Italian ISP Wind/Infostrada is reported to have distributed the DSL-G624T to its customer base over a period of several years.

It doesn't happen all the time - it appears to be timing-dependent. Older Mozilla Firefox browsers are hit particularly bad, due to the fact that they will request AAAA lookups even if the local host does not have an IPv6 address.

Work-around: Disable DNS forwarding support in the router. This will cause the D-Link to advertise the ISP's upstream DNS resolvers (instead of itself) in DHCPv4, and the hosts on the LAN will query them directly. Instructions follows:

Log in to your D-Link box as user 'admin'.

On the Home page, select DNS from the left hand menu.

[This is not shown in the documentation, and may not be in the same menu in all devices. If you cannot find it, there may be no easy solution for this model.]

On the DNS page, select DNS Relay Selection/Disable DNS Relay

Then click Apply and Save.

To make the change permanent, go back to the Home page, select Tools/System/Save & Reboot. Your D-Link will then take a minute or so to restart itself.

Bugs in operating system TCP/IP stacks

Apple iOS

No fallback from IPv6 to IPv4

Apple iOS is not able to fall back from IPv6 to IPv4, if the initial IPv6 connection attempt fails due to blackholing. An error message is displayed after a timeout of about 60 seconds instead. If errors are generated by the network, on the other hand, it will successfully fail over; either instantly (TCP RSTs), or after four seconds (ICMPv6 unreachables).

Short of ensuring that any IPv6 connectivity present work perfectly, there is no known workaround. IPv6 cannot be disabled in iOS.

This bug is reported to Apple in #8702877. The latest iOS version the bug has been confirmed to be present in is 4.3.

Solution: Upgrade iOS to the latest available version - it is reported to be fixed in iOS 5, which includes an «Happy Eyeballs» implementation.

Apple Mac OS X

Use of IPv6 with only link/site-local addresses

When attempting to connect to a dual-stacked destination when the system has only link-local IPv6 addresses (but at the same time a default IPv6 route), a 75 second timeout is incurred per AAAA record. IPv6 is preferred over IPv4 in this case due to lack of support for RFC 3484 in Mac OS X's system resolver. A system will be vulnerable to this bug if it has received an ICMPv6 Router Advertisement message that does not contain any Prefix Information Options, for example.

Portugese ISP SAPO is known to distribute a CPE to its customers (Pirelli A1000G) that emits such RAs by default, and the D-Link DIR series of routers will do so as well (at least DIR-635, DIR-655, DIR-825, and DIR-855).

Hosts running Microsoft Windows (at least Vista) with Internet Connection Sharing enabled can also emit such prefix-less RAs, in certain situations (possibly limited to when two network interfaces are bridged).

This will especially affect users of Mozilla Firefox older than version 4.0, as it will request AAAA records even though the system does not have any global IPv6 addresses (see [bug #614526](#)), and will attempt to connect to the IPv6 addresses in preference to falling back to IPv4. Safari also suffered from this problem up until Mac OS X 10.6.4. It will also affect users of the virtualisation software Parallels Desktop (regardless of the browser used), because its virtual network interfaces have site-local IPv6 addresses assigned, in turn making the `AI_ADDRCONFIG` flag to `getaddrinfo()` ineffective.

Similarly, the "ssh" client application (accessible in a MacOS X shell) initiates connections to global scope IPv6 addresses even if the OS only has link-local addresses in its interfaces. Bug with ID 8820407 is open with Apple.

Solution: Upgrade to Mac OS X 10.6.8. The bug is fixed there by sorting IPv6 addresses last in `getaddrinfo()`'s result set when there's only link-local IPv6 addresses present on the host.

Versions predating 10.6.x «Snow Leopard»

There is no fix this bug available for older versions of Mac OS X like «Tiger» and «Leopard». While it is preferred to upgrade to «Snow Leopard» to get the bug fixed properly, this might be undesired due to it not being a free upgrade, or entirely impossible if the hardware used is PowerPC-based. One of the following work-arounds might help for users of old Mac OS X versions:

Work-around: If the user is using Mozilla Firefox, ensure it is upgraded to [version 4.0](#) or newer. This *might* avoid the problem by suppressing AAAA lookups.

Work-around: Use the latest version of [Google Chrome](#), which will mask the underlying problem.

Work-around: Disable IPv6 completely in the operating system: *System Preferences -> Network -> Advanced -> TCP/IP -> Configure IPv6 -> Off*

Handling of Router Advertisements with a lifetime of 0

When receiving an Router Advertisement packet with a lifetime of 0, Mac OS X-based hosts will incorrectly install a default route. It appears that a Prefix Information Option must be present in the RA packet for the bug to take effect.

The technique of using a lifetime of 0 to announce an IPv6 router without global connectivity is used by devices conforming to RFC 6204 in the case where ULA addressing are used within the residential site. In this situation the Mac OS X host will attempt to use ULA IPv6 addresses for global connectivity, leading to timeouts towards dual-stacked content.

Apple bug ID: 8705091.

Solution: Upgrade to Mac OS X 10.6.8, where this bug is fixed.

Versions predating 10.6.x «Snow Leopard»

There is no fix this bug available for older versions of Mac OS X like «Tiger» and «Leopard». While it is preferred to upgrade to «Snow Leopard» to get the bug fixed properly, this might be undesired due to it not being a free upgrade, or entirely impossible if the hardware used is PowerPC-based. One of the following work-arounds might help for users of old Mac OS X versions:

Work-around: Use the latest version of [Google Chrome](#), which will mask the underlying problem.

Work-around: Disable IPv6 completely in the operating system: *System Preferences -> Network -> Advanced -> TCP/IP -> Configure IPv6 -> Off*

Handling of ICMPv6 Destination Unreachable

When a router in the network responds to a TCP SYN packet with an ICMPv6 Destination Unreachable, Mac OS X will re-transmit the TCP SYN packet five times with intervals of one second before giving up, even though the ICMPv6 code indicates that the situation is permanent and further attempts are pointless (e.g. Code 2 - Beyond scope of source address). In other words, an avoidable four-second timeout is incurred for every outgoing TCP connection.

Work-around: Use the latest version of [Google Chrome](#), which will mask the underlying problem.

Work-around: Upgrade to Mac OS X 10.7 «Lion», which will mask the underlying problem (only works if Safari is used)

Microsoft Windows

No «un-deprecation» of SLAAC-assigned IPv6 addresses

If a Windows Vista/7 machine has a SLAAC-assigned IPv6 address that becomes deprecated (due to its Valid Lifetime countdown timer reaching zero), it fails remove the **deprecated** flag after receiving an RA with a Valid Lifetime for the same prefix of >0 (the timers themselves will however be refreshed). This could happen for example if the user's CPE router intentionally deprecated the prefix in response to a WAN link failure event (and later attempted to un-deprecate it after the WAN link came back up and was assigned the same prefix), or if the computer was suspended/hibernated for a duration longer than the remaining Valid Lifetime and then woken up again (while remaining connected to the same network as before).

In the typical case, the problem will cause IPv4 to be used in preference to IPv6 in situations where it should have been the other way around. It will therefore not cause a «dual-stack brokenness» problem for content providers, however it might lead to a performance impact in the case where the IPv4 connectivity is inferior to IPv6 (for example if there's a CGN in the IPv4 path).

Solution: Install update KB2563894. This is available through Windows Update as an important update, and may also be downloaded from [security bulletin MS11-064](#).

Handling of ICMPv6 Destination Unreachable

Microsoft Windows appears to ignore received ICMPv6 Destination Unreachable completely, instead falling back on the overall connection timeout mechanism. This causes a completely avoidable 21 second long timeout to occur for every outbound TCP connection.

Bugs in web browsers

Mozilla Firefox

Mozilla Firefox does not set the AI_ADDRCONFIG flag when looking up names using the system getaddrinfo() library function, which causes it to solicit AAAA records even though the system has no IPv6 addresses (non-loopback and non-linklocal). This can trigger other problems, such as the D-Link AAAA mangling bug and the Mac OS X bug regarding the use of link-local IPv6 addresses when connecting to global destinations. The bug is fixed as of Firefox 4.0, see the [bug report](#)

Solution/work-around: Upgrade to Firefox [version 4.0](#).

Opera

When Opera, in versions older than 11.10, is used on a Mac OS X machine that has Parallels Desktop installed, it is unable to connect to dual-stacked web sites (except if the machine in question also has connectivity to the IPv6 internet). This is Opera Software bug DSK-326913.

Solution: Upgrade Opera to [version 11.10](#) or later.

Problematic network deployments

NTT NGN (Japan)

The NTT Next Generation Network includes the physical last-mile infrastructure (the local loop) to the customer's premises. Other ISPs lease these lines in order to provide internet service, similar to a [LLU](#) arrangement.

However, the NGN infrastructure also includes a walled-garden IPv6 deployment, which is used to deliver IPTV services, at least. While this IPv6 connectivity cannot communicate with the Internet at large, it uses globally scoped IPv6 addresses that looks just like ordinary IPv6 internet connectivity to the devices on the residential LAN. To compensate for this, the NGN centrally spoofs TCP RST packets for all connections that attempt to cross the walled garden boundary and get out to the global Internet. While this limits the impact on end users, it still is known to cause at least 1-second connection timeouts and failed image loading on (older) MSIE browsers. There's also a concern that the central TCP RST generators won't be able to keep up with the load, once a significant number of popular destinations on the Internet deploy IPv6.

Work-around: Use the latest version of [Google Chrome](#), which will mask the underlying problem.

Work-around: Install a modified RFC 3484 policy table that specifically de-prefers the use of the NGN IPv6 prefixes for communication with global destinations, see <http://www.attn.jp/maz/p/i/policy-table/> for more information.

Alternate work-around: Disable IPv6 in the operating system.

Firewall Config Issues

Especially if you have users on Vista.
It does this IPv6 tunnelling thing that on the surface appears really cool. When you try and talk IPv6 to something other than link-local: (in order)

- If you have a non-RFC1918 (ie. 'public') address, it fires up 6to4.
- If you have an RFC1918 address, it fires up Teredo.
Seems cool in theory, and you'd think that it would really help global IPv6 deployment - I'm sure that's how it was intended, and I applaud MS for taking a first step. But in practice, however, this has essentially halted any IPv6 /content/ deployment that people want to do, as user experience is destroyed.

You can help, though - here's the problem:

6to4 uses protocol 41 over IP. This doesn't go through NAT, or stateful firewalls (generally). Much like GRE.

Because of this, if you're a enterprise-esque network operator who runs non-RFC1918 addresses internally and do NAT, or you do stateful firewalling, PLEASE, run a 6to4 relay on 192.88.99.1 internally, but return ICMPv6 unreachable/admin denied/whatever to anything that tries to send data out through it. Better yet, tell your firewall vendor to allow you to inspect the contents of 6to4 packets, and optionally run your own 6to4 relay, so outgoing traffic is fast.

Even if you don't want to deploy IPv6 for some time, do this at the very least RIGHT NOW, or you're preventing those of us who want to deploy AAAA records alongside our A records from doing so. If you need configs for <vendor/OS B/C/J/L>, post a message to the [NANOG list](#) and I'll write some templates.

I see this sort of IPv4 network quite commonly at universities, where students take their personal laptops and throw them on the campus 802.11 network. While disabling the various IPv6 things in Vista at an enterprise policy level might work for some networks, it doesn't for for a university with many external machines visiting. So, if you're a university with a network like this (ie. most universities here in NZ, for example), please spend a day or two to fix this problem in your network - or better yet, do a full IPv6 deployment.

--Nathan Ward

Allow ICMPv6 through firewalls

Ensure that your firewalls allow through ICMPv6 types 1-4 and 128/129 as per NIST recommendation. In particular if you inadvertently block type 2 (Packet too big), you may find that users behind tunnels can connect to a web site but not get any content back.

--John Gibbins

Increased Latency to your IPv6 Content

If you do deploy an IPv6 network for your content, [set up a Teredo relay](#), and point 2001::/32 at it. Your viewers/users will automatically use this relay when accessing your content, and their traffic to you will be over IPv4, all they way from their PC to your network - so, equivalent performance as IPv4. Note that I say relay here, not server.

Mozilla.org are doing this for example. Cue Matthew Zeier.

--Nathan Ward

Check out [Enabling IPv6 on a Mail Server](#).

Unfortunately, not all Domain Registrars are providing IPv6 Glue yet

It may be tough to get IPv6 AAAA records for your nameservers into the DNS Glue records, depending on your registrar.

Check out [DNS Registrars IPv6 Support Status](#), let's build a list of who does and does not.

Troubleshooting Steps

The following steps should be followed in order. After each step, try testing again to see if your problem has been resolved. In general, keep your operating system and software up to date.

Update your Operating System

Windows

Go to <http://update.microsoft.com> for the latest version.

Mac OS X

Go to the Apple menu, choose Software Update, and update all available updates.

Update your browser or application

Internet Explorer

Go to <http://update.microsoft.com> and follow the instructions.

Mozilla Firefox

Firefox is normally updated automatically, but you can easily check. In Firefox, click Help, then Check for Updates. Get the New Version, then Restart Firefox.

Chrome

If a wrench icon appears on the browser toolbar, click it. Select "Update Google Chrome" then Restart.

Opera

Go to <http://www.opera.com/download/> to get the latest version, and follow the prompts.

Safari

Should have been updated when you updated your operating system: Go to the Apple menu, choose Software Update, and update all available updates.

Update your home gateway

Check the website of your gateway vendor to learn how to update it.

Disable transition technologies

Windows

Go to <http://support.microsoft.com/kb/929852> and select the "Disable IPv6 tunnel interfaces" fix.

Or, from a Windows command prompt: Click Start > Run > cmd (enter).
Then type (without the quotation marks) "netsh interface ipv6 6to4 set state disabled" and press enter.
Finally, type (without the quotation marks) "netsh interface teredo set state disabled" and press enter.

Mac OS X

Teredo is not commonly used by Mac OS X. Updating to the latest version of OS X should resolve any problems with 6to4, but if you cannot upgrade, you may have to disable IPv6 altogether. Continue troubleshooting, until you have no other choice.

Configure your firewall

Ensure that your firewalls allow through ICMPv6 types 1-4 and 128/129 as per NIST recommendation. In particular if you inadvertently block type 2 (Packet too big), you may find that users behind tunnels can connect to a web site but not get any content back.

If you are using tunnels intentionally, permit protocol 41 traffic.

Special cases

If you are using an AVM FRITZ!Box, follow the directions above to disable ULA.

If you are using a Linksys WRVS4400N, follow the directions above to disable IPv6 on the gateway.

If the problem still isn't fixed

Use Mac OS X 10.7 «Lion» (Safari only)

Mac OS X 10.7 «Lion» has high-level APIs that implement Happy Eyeballs-ish parallel connections, which efficiently mask any connection problems related to IPv6 (or IPv4 for that matter). More information about this [here](#). Currently, Safari is the only major browser to utilise these APIs.

Use Google Chrome

The latest version of [Google Chrome](#) has built-in robustness (Happy Eyeballs) when it comes to dual-stack brokenness, which will in the worst case result in a 300ms delay once per host, instead of long timeouts for every single connection. While it doesn't cure the underlying problem, it will mask the symptoms in a very efficient manner.

Disable IPv6

If no other workaround or attempted fix has remedied the problem, the last thing to try is to disable IPv6 outright. While this will prevent the user from successfully using IPv6 once the underlying problem has been fixed, it is likely to help improve the user experience in the short term.

Windows

Go to <http://support.microsoft.com/kb/929852> and select the "Disable IPv6 except for loopback" fix.

Mac OS X

Go to the Apple menu, select System Preferences, then Network (make sure Built-In Ethernet is selected) and choose Advanced, TCP/IP, then Configure IPv6 and select "off." Then choose OK and Apply.

Providers of IPv6 Services

This page is intended to list providers of various IPv6 service other than IPv6 transit to the public Internet because that is likely to be the core vanilla IPv6 service that everyone will eventually provide. There is a separate page to list [Providers Currently Selling IPv6 Transit](#).

Consulting Services including Network Design

- [NODO 6](#) provides IPv6 consulting and transition project management

Training and Education Services

- [Erion](#) provides IPv6 training courses
- [NODO 6](#) provides IPv6 Forum training and certification courses
- [ipv6.he.net](#) is a free IPv6 certification course provided by Hurricane Electric

IPv6 VPNs (all flavors)

IPv6 Gateway's Tunneled over IPv4

- [Hexago's](#) IPv6 gateways allow IPv6 to be tunnelled across any IPv4 network
- [tunnelbroker.net](#) is a free IPv6 tunnel service provided by Hurricane Electric

6PE over MPLS core network

Ethernet WAN Solutions

- [BT](#) announced their Etherflow product in Spring 2008

Anything Else?

DNS and Naming Issues

Basics

When you start deploying IPv6 services for outside users, you will need to add AAAA record for those hosts in your DNS and set up proper delegation for ip6.arpa to handle PTR records. Before you do this, it is a good idea to make sure that you have reasonable IPv6 connectivity so that IPv6 users won't be diverted to high-latency indirect paths when they start using the AAAA records. Also, to help users on your network, set up the IPv6 services described in [First Steps for ISPs](#). It wouldn't hurt to do an audit of customers who are using other tunnel broker servers and contact them, pointing out that you have a local tunnel broker service. If you don't do this, it is likely that the new AAAA records for your service will cause some of your users to experience much higher latency because they get their IPv6 packets from a distant tunnel broker. It will appear that your network is suffering from strange latency problems since the server with the AAAA record is on your network.

Special Hostnames

One way to avoid such issues and allow testing without disrupting production services is to set up special domain names. Initially, you can add a name which only returns an AAAA record. This assures that connectivity is IPv6 and does not require change to the existing host name. (Note: You may have to configure your service to recognize the new name, e.g. add a ServerAlias directive to an Apache virtual host.) To switch to production IPv6 use, add an AAAA record to the primary host name. Adding another name that only returns an A record will provide a way to test with IPv4 only.

```
Initial testing:
  www.your.domain          (Original name. A record only.)
  www.ipv6.your.domain     (AAAA record only.)
Production:
  www.your.domain          (A and AAAA record.)
  www.ipv6.your.domain     (AAAA record only.)
  www.ipv4.your.domain     (A record only.)
```

Substitute `www` with whatever hostname you are using. The above form is what is in general use around the internet and what some people will try in cases where a DNS name has both an AAAA and A records and one of them does not work.

Reverse DNS

Reverse DNS works via PTR records in your zones. For IPv4, the bits are reversed, such that a PTR record for **192.168.0.0** would look like **0.0.168.192 IN PTR your.hostname..** The same is true for IPv6, except that you must separate each character with a `..`. This means that a PTR record for **2008:64:128::ee:1** would look like **1.0.0.0.e.e.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.8.2.1.0.4.6.0.0.8.0.0.2 IN PTR your.hostname.** or a PTR record for

DNSBLs

While there are a plethora of [DNSBLs](#) for IPv4 addresses, they are only a few for IPv6.

- [Roaring Penguin](#)
- [Bit's Virbl](#)

One of the specific challenges of a DNSBL for IPv6 is the large address space and whether /128's or /64's should be the smallest entry.

Mailserver Whitelists

Somewhat the opposite of the above, IPv6-capable email servers are registered.

- [IPv6 Mailserver Whitelist](#)

Implementing 6PE

Please add tips about implementing 6PE to provide IPv6 access services across an MPLS core.

6PE is described in [RFC 4798](#). It is very similar to BGP/MPLS IP VPNs [RFC 4364](#) (obsoleted RFC 2547).

The first key difference is that the IPv6 traffic is not within an IP VPN in the MPLS PE router, it is in the Global Routing Table (GRT). Like with BGP/MPLS IP VPNs the traffic forwarding between PEs is based on label swapping the top MPLS label in the label stack as the packet is forwarded across the network, which besides for the PE routers does not have to be dual-stacked. In a correctly configured BGP/MPLS IP VPN network these labels will already exist and have been signalled by LDP or RSVP-TE. The specific label switched paths (LSPs) of interest are between the BGP next-hop addresses of the PEs. The second difference is that unlike with BGP/MPLS IP VPNs there is no automatic signalling of an inner service label for the IPv6 packet. The BGP configuration for the IPv6 address family in BGP must be explicitly configured to send this label.

Note that the BGP neighbors are IPv4 and the LSPs are based on IPv4 signalling protocols, thus IPv4 and IPv6 traffic between pairs of PEs will follow congruent paths. The ease with which this can be configured and that it is based on BGP/MPLS IP VPNs which service providers are highly familiar with, makes 6PE an attractive and low risk way to start supporting IPv6 in the core network before making a later transition to native IPv6 interior routing protocol (IGP) support. The priority for service providers at this stage of the IPv6 transition should be to connect IPv6 users at the edge.

Cisco example

The key extra bit of configuration is [send-label](#). This will result in traffic to destinations learned from PEs (that also have the [send-label](#) neighbor argument) being label swapped across the network.

The network statement is used to advertise an IPv6 loopback address to have an end-point to use with ping testing.

```
interface Loopback0
description *** Loopback Address for PE4***
ip address 10.99.99.4 255.255.255.255
ipv6 address 2001:DB8:C:4::1/64

router bgp 5466
neighbor REFLECTOR update-source Loopback0
neighbor REFLECTOR version 4
neighbor 10.99.99.9 peer-group REFLECTOR
neighbor 10.99.99.9 description ipv4 peering to rrl
address-family ipv6
neighbor REFLECTOR send-label
neighbor 10.99.99.9 activate
network 2001:DB8:C:4::/64
exit-address-family
```

Note in the above example a BGP Route Reflector is used. The RR should also have the [send-label](#) command so that it reflects the inner service label of the IPv6 packet.

Alcatel-Lucent Example

With ALU the extra bit of configuration is the [advertise-label ipv6](#) command.

```

configure router
interface "system"
address 172.16.0.11/32
ipv6
address 2001:DB8:A:11::1/128
exit
exit all

configure router policy-options
begin
prefix-list "ipv6-system"
prefix 2001:DB8:A::/48 through 128
exit
policy-statement bgp_internal_out
entry 10
from
protocol direct
prefix-list "ipv6-system"
exit
action accept
origin incomplete
exit
exit
commit
exit all

configure router
bgp
group "internal"
family ipv4 ipv6
min-route-advertisement 2
next-hop-self
type internal
export "bgp_internal_out"
neighbor 172.16.0.31
advertise-label ipv6
exit
exit
exit all

```

Note when using Route Reflector with ALU SR OS it is necessary to enable MPLS on the RR even though the RR is not involved in the forwarding process.

Juniper JUNOSe Example

```

license ipv6 "v6$Ru5le!s"
ipv6

interface loopback 0
ip address 10.99.99.17 255.255.255.255
ipv6 address 2001:db8:e:17::1/128

mpls
mpls ldp
mpls ldp advertise-labels host-only

router bgp 5466
address-family ipv6 unicast
no auto-summary
neighbor REFLECTOR activate
no neighbor REFLECTOR shutdown
neighbor REFLECTOR description Standard Route Reflector
neighbor REFLECTOR graceful-restart
neighbor REFLECTOR send-label
neighbor 172.16.0.31 peer-group REFLECTOR
no neighbor 172.16.0.31 shutdown
network 2001:db8:e:17::1/128
exit-address-family

```

There is also something called 6VPE which runs over MPLS and is used to provide VPN routing. More info is available in [RFC 4659](#).

This is even easier to use as inner service label exchange is automatic.

IPv6 Management Tools

On this page, please link to information about commercial or Open Source tools that can manage networks over IPv6, or help with management and troubleshooting of IPv6 networks.

IPv6 Security Assessment & Troubleshooting

- [SI6 Networks' IPv6 Toolkit](#)

OSS tools

- [SMARTS IPv6 Availability Manager](#)
- [Jeff Doyle reports on OPNET's IPv6 module](#)
- [Reference implementation of the Shim6 multihoming protocol for IPv6](#)
- [NetDot \(NETwork DOcumentation Tool\)](#) can handle IPv6 addressing and also export data to Bind, DHCP, Nagios, etc.

Managing IPv6 Networks with SNMP and the new IPv6 MIBS

- [IPv6 MIBs Technical Training Videos](#)

Monitoring IPv6 Enabled Services

- [Assess, Baseline, Monitor and Troubleshoot IPv6 Enabled Services. Measure the Effectiveness of IPv6 Enablement](#)

IPv6 Address calculators and manipulators

- [v6decode.com](#): Display addresses in various representations
- [IPv6 subnet calculator](#)
- [IPv6 RFC 5952 validator](#)
- [Perl script 'IPv6canonical'](#) formats IPv6 addresses in the format as written in "A Recommendation for IPv6 Address Text Representation"
- [IPv6 Subnetting card](#)
- [IPv6 subnetting cheat sheet / table](#)
- [IPv6 subnet calculator and hierarchical subnet planner](#)
- [ip6calc](#) by Peter Bieringer ([link broken as of 7/31/2011](#))
- [RFC3531 IPv6 address plan and allocation tool](#) ([link broken as of 7/31/2011](#))
- [ip6addr](#) ([link broken as of 7/31/2011](#))

IP Address Management (IPAM)

- [Alcatel-Lucent VitalQIP® IPAM](#)
- [BlueCat Networks IPAM](#)
- [Crypton UK - EasyIP\(TM\)](#)
- [EfficientIP IPAM](#)
- [FreeIPdb](#)
- [GestióIP](#)
- [HaCi](#)
- [Incognito Address Commander](#)
- [IPal](#)
- [6connect, IPv6/IPv4 IPAM Tool suite \(ARIN RESTful integration\) and Network Automation](#)
- [BT Diamond IP - IPControl\(TM\)](#)
- [Infoblox IPAM \(freeware version\)](#)
- [IPAT \(IP Allocation Tool\) \(2011/02/12: Downloads disabled\)](#)
- [IPplan Open Source IPAM](#)
- [mihap's IPAM](#)
- [NetDot](#)
- [phpipam](#)

ISP IPv6 Implementations

On this page, please link to information about ISP Implementations of IPv6

Hurricane Electric

[Hurricane Electric Letter Regarding World IPv6 Day](#)

[Tunnel broker Service](#)

Comcast

[Comcast Activates First Users with IPv6 native Dual-Stack over DOCSIS](#)

[Comcast IPv6 Information Center](#)

Qwest

[Qwest announces IPv6 Internet Address](#)

XO

[XO Support for IPv6 Connectivity](#)

Verizon

[Verizon Begins Testing IPv6 on FIOS service](#)

Sonic.net

[IPv6 Tunneling Service](#)

Sprint

[Sprint Native IPv6 Overview](#)

NTT America

[NTT America IPv6 Service](#)

Global Crossing

[Global Crossing IPv6](#)

SiXXS

[SiXXS Main Page](#)

Gogonet Freenet6

[Freenet6 Service](#)

Defense Research and Engineering Network (DREN)

[History of IPv6 Support and Implementation](#)

Relay Services

IPv6 Transmission Mechanisms

IPv4 and IPv6 networks are not directly interoperable, which means that a transition mechanism is needed in order to permit hosts on an IPv4

network to communicate with hosts on an IPv6 network, and vice versa. The links below are links to videos developed by RIPE NCC will help you understand some of these techniques.

6in4



6in4 is a tunneling technique. You can manually set up a 6in4 tunnel. Watch this video to learn more.

2:05


6RD



6RD is a tunneling technique in which the IPv4 and IPv6 addresses come from the Internet Service Provider (ISP). Some ISPs offering DSL or cable services are implementing 6RD to connect their customers over IPv6.

2:52


NAT64



NAT64 is a transition mechanism based on Network Address Translation (NAT) that makes it possible for IPv6-only hosts to talk to IPv4-only servers. NAT64 can be useful for mobile providers.

4:09

DS-Lite



DS-Lite allows an ISP to give access to IPv4-only services for customers that have only native IPv6. This mechanism could be useful for DSL or cable providers.

2:37

Additional Materials

There are several relay services that are of interest to ISPs because they can set up tunnel relay servers to either provide better service to a mixed v4/v6 Internet, or to enable full reachability regardless of the end-user's version of IP. The following pages deal with the main automatic tunnel/relay technologies:

- [Cisco 6to4 Relay Service](#)
- [FreeBSD Teredo Relay](#)
- [Juniper 6to4 Relay Service](#)
- [Linux or BSD 6to4 Relays](#)
- [ISPs currently announcing a 6to4 prefix](#)
- [Miredo](#)
- [Transitioning__6to4](#)
- [Transitioning__NAT64](#)
- [Transitioning__NAT-PT](#)
- [Transitioning__Teredo](#)

There is also useful information about these technologies on these pages:

- [Operational transition information](#)
- [Planning IPv6 Deployment](#)
- [Transparent Internet Access](#)

The following conversation from the NANOG list explains how effective placement of 6to4 relays in content-provider networks can greatly reduce the likelihood of latency issues in a mixed v4/v6 Internet.

```
> 2) If Teredo relays are deployed close to the service (ie. content,  
> etc.) then performance is almost equivalent to IPv4. 6to4 relies on  
> relays being close to both the client and the server, which requires  
> end users' ISPs to build at least *some* IPv6 infrastructure, maintain  
> transit, etc. When you consider that this infrastructure and transit  
> is quite likely to be over long tunnels to weird parts of the world,  
> this is a bad thing. Putting relays close to the content helps for the  
> reverse path (ie. content -> client), however the forward path (client  
> -> content) is likely to perform poorly.
```

Not quite correct. 6to4 does not require transiting a relay if the target is another 6to4 site. What this means is that a clueful content provider will put up a 6to4 router alongside whatever native service they provide, then populate the dns with both the native and 6to4 address. A properly implemented client will do the longest prefix match against that set, so a 6to4 client will go directly to the content provider's 6to4 router, while a native client will take the direct path. The only time an anycast relay needs to be used is when the server is native-only and the client is 6to4-only.

And here is a brief Q&A that makes it clear that installing proper relays gives you greater visibility of your IPv6 traffic.

On Thu, 30 Oct 2008, David W. Hankins wrote:

```
> I don't know how to ask this question without sounding mean, but did  
> the graph spike out of zero, or did you start collecting two months ago?
```

It spiked out of zero as we put up our 6to4 and teredo relays approx two months ago. I don't know where the traffic was before, probably at other peoples 6to4 relays.

--

Mikael Abrahamsson email: swmike@swm.pp.se

Cisco 6to4 Relay Service

An ISP can set up a 6to4 relay service by configuring at least two well-connected IPv6-enabled routers to set up automatic 6to4 tunnels.

A 6to4 tunnel is an automatic IPv6 tunnel where a 6to4 border router in an isolated IPv6 network creates a tunnel to a 6to4 border router in another isolated IPv6 network over an IPv4 infrastructure. The tunnel destination is determined by the globally unique, 32-bit IPv4 address of the remote 6to4 border router that is concatenated to the prefix 2002::/16. 6to4 tunnels are configured between 6to4 border routers or between 6to4 border routers and hosts.

A 6to4 relay service is a 6to4 border router that offers traffic forwarding to the IPv6 Internet for remote 6to4 border routers. A 6to4 relay forwards packets that have a 2002::/16 source prefix.

6to4 tunnels and connections to a 6to4 relay service need not be requested or negotiated between customers and the ISP. The ISP simply configures the 6to4 relay service and customers can automatically connect to the service whenever they like. Because of the one-to-many relationship between the 6to4 relay service and each 6to4 tunnel (each customer), there is low maintenance and management overhead associated with 6to4 tunnels and a 6to4 relay service. However, given that customers use the IPv4 address of their border router to construct the 6to4 address that they use to connect to the 6to4 relay service (they are not delegated a /48 prefix from the ISP), the ISP may want to manage the IPv4 routing announcements for the relay service to control its use (the ISP will need IPv4 traffic statistics if it wants to identify and charge individual customers for using the service).

Reverse 6to4 delegation can be requested at: <http://6to4.nro.net>, please check the instructions at http://6to4.nro.net/6to4_reverse/non_2002/index.html.

Brief Example

Here is a minimal config fragment. Check Cisco's documentation for full details. This should be configured on a dual-stack router that has good

IPv4 and IPv6 connectivity. To minimize latency, it should be on the border between your IPv4-only network and your dual-stack network. This configuration can be duplicated to additional dual-stack routers for increased reliability.

```
! Your unique Router ID
! Use your own real IP addresses here instead of 192.0.2.1 and 2001:db8::1
! The 6to4 relay anycast address 192.88.99.1 (see RFC 3068) should be
! configured as a secondary address on the loopback interface
interface Loopback0
    ip address 192.88.99.1 255.255.255.0 secondary
    ip address 192.0.2.1 255.255.255.255
    ipv6 address 2001:db8::1/128
!
interface Tunnell
    description 6to4 Tunnel
    no ip address
    ipv6 unnumbered Loopback0
    tunnel source loopback0
    tunnel mode ipv6ip 6to4
!
ipv6 route 2002::/16 Tunnell
```

WARNING: The 192.88.99.1 address on the loopback interface may be selected as your router ID during a subsequent reboot or an OSPF or BGP process restart. To prevent this (particularly if you are running multiple 6to4 gateways for reliability) you should explicitly specify your OSPF or BGP router ID.

A 6to4 gateway provides routing in two different directions. First, it provides a route for packets from native IPv6 (non-6to4) devices within an IPv6 network to reach 6to4 devices which do not have native IPv6 connectivity. The 2002::/16 route should be distributed to other IPv6 routers using an IPv6-capable IGP (eg. OSPFv3 or RIPv6).

The gateway also allows packets from 6to4 devices which have only IPv4 connectivity to reach native IPv6 devices on the IPv6 network. The route to the anycast address 192.88.99.1 should be distributed via an IPv4 IGP (eg. OSPF or EIGRP) to other IPv4 routers.

For example, if you run OSPFv3 and OSPF on your routers:

```
ipv6 router ospf 10
    ! Redistribute the 2002::/16 static route
    redistribute static
!
router ospf 10
    ! Redistribute the 192.88.99.1 route
    redistribute connected subnets
```

If the router will be a public 6to4 gateway, then the 192.88.99.0/24 network and/or the 2002::/16 network should also be announced via BGP to other networks (see RFC 3068, section 4.3). Depending on your BGP peering policy and configuration, accomplishing this may require one or more of the following:

- Adding a 'network 192.88.99.0' and/or 'network 2002::/16' to your BGP configuration
- Adjusting your BGP filters to permit the outgoing announcements
- Coordinating with your BGP peer(s) to accept the 192.88.99.0/24 and/or 2002::/16 prefixes and propagate them
- Adjusting your border interface ACLs to permit the traffic

Detailed Example

Jordi Palet Martinez posted the following example on the AfriNIC mailing list:

Details of the example configuration

The examples below is assuming that the public IPv4 address in the WAN

interface of the router is 192.1.2.3. You should replace that with the right information for your own case, same with other data used in the examples.

Also, you need to understand how to calculate the 6to4 IPv6 address for your router. This is done using the IPv4 address and the IPv6 6to4 prefix.

The 6to4 prefix 2002::/16 is taking the first 16 bits. Then the bits 17 to 48 are the nibble notation for your IPv4 address. So in our example it will be:

```
192 = c0
1 = 01
2 = 02
3 = 03
```

So consequently:

```
2002:c001:0203::/48
```

We will use the first address of the prefix for the WAN interface, so

```
2002:c001:0203::1/128
```

Also, the anycast address for 6to4 is: 192.88.99.1

Following the same example as above, in IPv6 will be:

```
2002:c058:6301::/128
```

For our example using a Loopback, we use 192.3.2.3, which in IPv6 will be

```
2002:0c03:0203::/128
```

We show below two options for the 6to4 Relay. One basic configuration and another using the anycast address for 6to4. You just need to configure one of them (A or B).

A Example configuration of a basic 6to4 Relay

This relay will only be reachable for hosts or routers with a manual configuration pointing to it.

A1) Enable IPv6 in the router

```
ipv6 unicast-routing
```

A2) Ethernet0/0 interface configuration (obviously you can use another interface)

```
interface Ethernet0/0
  description 6to4 Relay Service
  ip address 192.1.2.3 255.255.255.0
```

A3) tunnel 6to4 virtual interface

```
interface Tunnel2002
description 6to4 Relay Interface
no ip address
no ip redirects
ipv6 address 2002:c001:0203::1/128
tunnel source Ethernet0/0
tunnel mode ipv6ip 6to4
```

A4) 6to4 prefix route

```
ipv6 route 2002::/16 Tunnel2002
```

B Example configuration of a 6to4 Relay with anycast support

B1) Enable IPv6 in the router

```
ipv6 unicast-routing
```

B2) We use the loopback (recommended), but you could use an Ethernet Interface or any other one

```
interface Loopback0
description 6to4 Anycast Relay Service
ip address 192.88.99.1 255.255.255.0 secondary
ip address 192.3.2.3 255.255.255.255
ipv6 address 2002:c003:0203::1/128
ipv6 mtu 1480
no ipv6 mfib fast
```

Note: When using IPv4 anycast addresses is recommended to configure explicitly the BGP/OSPF ID with a unicast address, otherwise, the router may take by default the anycast address as the ID.

B3) tunnel 6to4 virtual interface

```
interface Tunnel2002
description anycast 6to4 Relay Interface
no ip address
no ip redirects
ipv6 address 2002:C058:6301::/128 anycast
ipv6 unnumbered Loopback0
no ipv6 mfib fast
tunnel source Loopback0
tunnel mode ipv6ip 6to4
tunnel path-mtu-discovery
```

C Configuration for a public Relay

If you choose the anycast option (B), then you can also make the relay public via the following steps.

C1) You need to announce the 2002::/16 prefix usually via BGP. The example below will help you. You should add this to the normal unicast IPv6 configuration and replace the right information for your own case.

```
router bgp myASN
  no bgp default ipv4-unicast
  bgp log-neighbor-changes
  neighbor remotepeer_IPv6_address remote-as remoteASN
  neighbor remotepeer_IPv6_address description Peer to remoteISP

  address-family ipv6
  neighbor remotepeer_IPv6_address activate
  neighbor remotepeer_IPv6_address route-map remoteISP_in in
  neighbor remotepeer_IPv6_address route-map remoteISP_out out
  network my_IPv6_prefix
  network 2002::/16
  exit-address-family

  ipv6 route 2002::/16 Null0

  ipv6 prefix-list 6to4_prefix seq 5 permit 2002::/16

  route-map remoteISP_out permit 10
  match ipv6 address prefix-list 6to4_prefix
```

Note: Of course, you need to replace some of the parameters with your specific data, such as myASN, remotepeer_IPv6, my_IPv6_prefix, remoteASN, remoteISP, remoteISP_in and remoteISP_out.

C2) Additionally you need to configure the announce of the 6to4 anycast prefix, 192.88.99.0/24, to your neighbor ISPs.

Once you have started announcing this prefix, add yourself to the list of [ISPs currently announcing a 6to4 prefix](#).

D Configuration for a Private Relay

Alternatively, if you only want to offer the relay to your own customers, you need to announce the 192.88.99.0/24 prefix only to them. Then you will need to use example A) and use something adapted to your own network/routing protocol.

For example, if you are using OSPF as your IGP, you will add something such as:

```
router ospf 1
  log-adjacency-changes
  auto-cost reference-bandwidth 10000
  network 192.88.99.0 0.0.0.255 area 0
```

E Real-life configuration for 6to4 public relay on a Cisco 7600 platform

In addition to the scenarios above it could be really tricky to debug all of the associated problems. If you're using a Cisco 7600 platform it is worth

checking out the following:

- 1) DO NOT put 192.88.99.1 as a secondary address on a Loopback interface. Otherwise you will not enable cef fully.
- 2) Additional addressing on Loopback ('normal' IPv4- and IPv6-loopbacks on Lo64 below) is not obligatory, though it will allow for proper diagnostics from the router towards 6to4 clients.
- 3) In an MPLS environment CHECK OUT for "mls mpls tunnel-recir" in the running-conf. It is mandatory to ensure bi-directional traffic flows.

Below is a real-life configuration that delivers (appears courtesy of CCIE #10389), IGP part is omitted for clarity. Feel free to ask questions/comment at aa916-ripe contacts.

```
!
mls mpls tunnel-recir
!
interface Loopback64
 ip address 192.168.2.155 255.255.255.255 secondary
 ip address 192.88.99.1 255.255.255.0
 no ip redirects
 ipv6 address 2002:C0a8:029B::1/128
 ipv6 enable
 ipv6 mtu 1280
 no ipv6 redirects
 no ipv6 unreachable
!
interface Tunnel64
 no ip address
 no ip redirects
 ipv6 address 2002:C058:6301::/128 anycast
 ipv6 unnumbered Loopback64
 ipv6 enable
 ipv6 mtu 1280
 no ipv6 redirects
 tunnel source Loopback64
 tunnel mode ipv6ip 6to4
 tunnel path-mtu-discovery
!
ipv6 route 2002::/16 Tunnel64
!
router bgp xxxx
!
 address-family ipv4
  redistribute connected route-map to-bgp
!
 address-family ipv6
  redistribute static route-map to-bgp6
!
route-map to-bgp permit 10
 match ip address prefix-list xxxx:6to4-anycast
 set local-preference 200
 set community xxxx:yy xxxx:zz
!
route-map to-bgp6 permit 10
 match ipv6 address prefix-list xxxx:6to4
 set local-preference 200
 set community xxxx:yy xxxx:zz
!
ip prefix-list xxxx:6to4-anycast seq 5 permit 192.88.99.0/24
ipv6 prefix-list xxxx:6to4 seq 5 permit 2002::/16
```


FreeBSD Teredo Relay

Miredo is a Teredo implementation that runs on FreeBSD. The FreeBSD system should already have functional dual-stack connectivity before installing Miredo. You'll need root privileges to run most of the commands below.

Install Miredo

Do one of the following

```
pkg_add -r miredo
```

or

```
cd /usr/ports/net/miredo  
make install
```

Configure Miredo

Enable Miredo during system startup.

```
echo miredo_enable=YES >> /etc/rc.conf
```

Enable IPv6 forwarding.

```
echo net.inet6.ip6.forwarding=1 >> /etc/sysctl.conf  
sysctl net.inet6.ip6.forwarding=1
```

Edit the Miredo config:

- Uncomment RelayType and change it to relay
- Comment out any ServerAddress

Start and test Miredo

Before starting Miredo, check the IPv6 route table for the lack of a 2001::/32 route

```
netstat -rn | grep 2001::/32
```

You should get no output from the above.

Ping6 and traceroute6 to a known Teredo client (eg. teredomon.mucip.net or mire.remlab.net). The client will be multiple hops away.

```
ping6 teredomon.mucip.net  
traceroute6 teredomon.mucip.net
```

Now startup Teredo relaying.

```
/usr/local/etc/rc.d/miredo start
```

Recheck the IPv6 route table and traceroute6 paths. You should now see a 2001::/32 route and the Teredo client will be 0 hops away.

```
> netstat -rn | grep 2001::/32  
2001::/32 teredo ULS teredo  
> traceroute6 teredomon.mucip.net  
1 2001:0:53aa:64c:3c10:f226:af0b:cba 710.172 ms 240.230 ms 240.489 ms
```

Redistribute the Teredo 2001::/32 route

To allow your FreeBSD Teredo relay to be useable by the rest of your IPv6 network, you'll need to add a 2001::/32 route to your routers. Two ways to do that are:

- Add a static route on your router to 2001::/32 with your FreeBSD system IPv6 address as the gateway address and propagate the static route to your network.
- Run a dynamic routing protocol on the FreeBSD system compatible with your existing network routers.

Juniper 6to4 Relay Service

Jordi Palet Martinez reported on the NANOG list:

```
Unfortunately, Juniper doesn't support 6to4, only in Netscreen
boxes. This is ridiculous and I already asked Juniper several
times about this ..., but never got a positive feedback about
when it will be supported.
```

```
Regards,
Jordi
```

Linux or BSD 6to4 Relays

All you need is a Linux or BSD box configured as a router, for instance [Quagga](#) or [BIRD](#).

As someone who is building little compact flash and USB flash based BSD boxes for various tasks, I can quite happily say its entirely possible to build diskless based Linux/BSD routers which are upgraded about as easy as upgrading a Cisco router (ie, copy over new image, run "save-config" script, reboot.) Its been that way for quite some time.

If there's interest I'll hack up a FreeBSD nanobsd image with ipv6 support, a routing daemon (whatever people think is good enough) and whatever other stuff is "enough" to act as a 6to4 gateway.

You too can build diskless core2duo software routers for USD \$1k.

Nathan Ward has packaged up a [FreeBSD image that runs on Soekris boxes](#) which incorporates 6to4 and Teredo. A binary TUI release can be [downloaded from Nathan's website](#), as well as a nice [article by Geoff Huston](#).

Reverse 6to4 delegation can be requested at: <https://6to4.nro.net>, please check the instructions at https://6to4.nro.net/6to4_reverse/non_2002/index.html.

If you announce a 6to4 prefix, make sure to add your ASN to the list of [ISPs currently announcing a 6to4 prefix](#).

Jordi's AfriNIC posting

This info provides the steps required in order to configure your BSD box as a 6to4 Relay.

In order to proceed, you need to have a public IPv4 address on that box, your own IPv6 prefix (provided by AfriNIC in this case) and IPv6 transit.

The BSD box need to support stf pseudo-interface, FreeBSD 5.4 or higher version is recommended, for FreeBSD 4.9 you need to recompile the kernel adding "pseudo-device stf". NetBSD 1.5 supports stf pseudo-interface compiling the kernel. Also need to have IPv6 support and IPv6 routing enabled.

If you need help in order to acquire your IPv6 prefix from AfriNIC, let us know and we can help even with the request form.

Similarly, we are able to help in making sure you have the right configuration for IPv6 in your BSD and you can get IPv6 transit (native or tunneling) either from your upstream, or alternatively, if that's not possible, we will be able to provide free IPv6 transit to third party networks.

Regards,

Jordi

Running a 6to4 relay on Linux

Tested on 2.6.24-19-generic (ubuntu hardy).

Create this bash script

```
#!/bin/bash

echo 1 > /proc/sys/net/ipv6/conf/default/forwarding
echo 1 > /proc/sys/net/ipv6/conf/all/forwarding
echo 1 > /proc/sys/net/ipv6/conf/eth0/forwarding

ip -4 addr add 192.88.99.1/32 dev eth0
# enabling forwarding makes the RA added default gateway disappear, so
# it has to be added manually.
ip -6 route add ::/0 via YOUR_GATEWAY dev eth0

ip route flush dev tun6to4 2>/dev/null
ip link set dev tun6to4 down
ip tun del tun6to4

ip tunnel add tun6to4 mode sit ttl 100 remote any local 192.88.99.1
ip link set dev tun6to4 up

ip -6 route add 2002::/16 dev tun6to4
ip -6 route add ::/96 dev tun6to4 metric 1
```

Remember that you need to update access lists for the network the 6to4 relay is on. Allow 192.88.99.1 into the network. As it sends packets from 2002:: you need to allow spoofed outgoing packets.

IMPORTANT NOTE

If you are running a Linux based 6to4 relay you should consider applying [this patch](#).

Create an stf interface

In case it doesn't exist, create an stf interface.
Run these commands in a terminal:

```
ifconfig stf create
```

By default the stf interface is not enabled.

Add local 6to4 address to interface (note: prefix length 16 is very important!)

```
ifconfig stf0 inet6 6to4addr prefixlen 16
```

```
ifconfig stf0 inet6 2002:c001:0203::1 prefixlen 16
```

Configure IPv6 connectivity

Because we are configuring a 6to4 relay it should have IPv6 connectivity (either native or via a tunnel) through an IPv6 gateway (for our example we use 2001:7f9:1::1 as GW address). After having configured an IPv6 address on the corresponding interface, the default route should be configured:

If our IPv6 interface is interface ne0:

To configure the IPv6 address:

```
ifconfig ne0 inet6 alias 2001:7f9:1::2
```

To add a default route:

```
route add -inet6 default 2001:7f9:1::1
```

Configure prefix advertisements

Somewhere on the Relay network, the device in charge of announcing prefixes (typically a BGP router) should announce 2002::/16 prefix to its IPv6 peerings.

This would allow native IPv6 nodes to reach 6to4 nodes (2002::/16 addresses).

Regarding the IPv4 reachability of the Relay there are two options:

1. Configure the 6to4 anycast IPv4 address (192.88.99.1) and announce the anycast prefix (192.88.99.0/24) to the site IPv4 peerings.
2. 6to4 hosts will be able to find it automatically, with no need for any manual configuration.
3. Use another public IPv4 address.
4. Some kind of advertisement of the IPv4 address is needed (usually a FQDN-Fully Qualified Domain Name) in order to allow others to configure our relay.

This will allow 6to4 nodes (2002::/16 addresses) to reach native IPv6 nodes through our relay.

Making your configuration persistent

In order to make your configuration persistent, a script could be used that is executed at boot time. The idea is to have a script that executes all the commands needed to configure everything as desired.

This example for Linux takes the local host public IPv4 address as an argument:

```
#!/bin/sh

IPV4=$1
PARTS=`echo $IPV4 | tr . ' '`
PREFIX48=`printf "2002:%02x%02x:%02x%02x" $PARTS`

STF_IF="stf0"
STF_NET6="$PREFIX48":0000
STF_IP6="$STF_NET6"::1

ifconfig $STF_IF inet6 $STF_IP6 prefixlen 16 alias

ifconfig ne0 inet6 alias 2001:7f9:1::2
route add -inet6 default 2001:7f9:1::1
```

For FreeBSD add this to /etc/rc.conf:

```
stf_interface_ipv4addr="public_v4addr"

ipv6_defaultrouter="2001:7f9:1::1"
```

Configuration examples may vary for other BSD distributions.

Remove a 6to4 tunnel using "ip" and a dedicated tunnel device

Remove a 6to4 interface address

```
ifconfig stf0 inet6 -alias 2002:c001:0203::1
```

Remove 6to4 prefix route

First we can see the route table with:

```
netstat -rn
```

Now we can delete the route entry for 2002::/16 prefix via <gateway_IPv6> with:

```
route delete -inet6 2002::/16 <gateway_IPv6>
```

ISPs currently announcing a 6to4 prefix

Oceania/Asia

Australia:

- 1221 Telstra

Korea:

- 17832 NISA

Viet Nam:

- 7643 VDC

Europe

Denmark:

- 1835 FSK Net

Estonia:

- 3327 Linxtelecom

Finland:

- 1741 FUNET

France:

- 1257 Tele2

Germany:

- 286 kpn.de
- 1257 Tele2
- 5430 Freenet
- 12816 mwn
- 15598 IP Exchange
- 20640 Titan
- 35244 kms.de

Ireland

- 42227 Airwire

Italy:

- 12779 itgate.net

Netherlands:

- 1101 SURFNet
- 1257 Tele2
- 8954 InTouch
- 26943 Your.Org
- 31383 Computel
- 5615 Telfort
- Ziggo

Portugal:

- 1930 FCCN

Spain:

- 8903 BT Spain
- 16206 Abared

Sweden:

- 1257 Tele2
- 16150 GlobalTransit

Switzerland:

- 559 switch.ch

United Kingdom:

- 5400 BT

North America

USA:

- 59 University of Wisconsin
- 109 Cisco
- 1239 Sprint
- 3344 Kewlio
- 5050 Pittsburgh Supercomputing Center
- 6175 Sprint
- 6939 Hurricane Electric
- 7019 NTT
- 10533 Ottawa Internet Exchange
- 19255 Your.Org
- 19782 Indiana University
- 25795 ARP Networks

Miredo

Miredo is an open-source Teredo IPv6 tunneling software, for the Linux, BSD and OS/X operating systems. It includes functional implementations of all components of the Teredo specification (client, relay and server). It is meant to provide IPv6 connectivity even from behind NAT devices.

There is more info, and software to download at [the Miredo website](#).

Note that Miredo supports Teredo server, Teredo relay and Teredo client. From an ISP perspective, the Teredo client is not of interest since non-Windows clients generally get better results using 6to4 relaying.

Various ISPs will however announce a teredo prefix, to improve quality of users using teredo. Here is a list of [ISPs currently announcing a teredo prefix](#).

Teredo server

A Teredo server needs two consecutive public IPv4 addresses, and global IPv6 connectivity.

Lets say the addresses are 192.0.2.100 and 192.0.2.101, on network interface

eth0. Typically, you will already have configured 192.0.2.100 as the "normal" IP address on eth0. On Linux, you can add 192.0.2.101 with iproute2:

```
# /sbin/ip -4 address add 192.0.2.101/32 dev eth0
```

As regards miredo-server, you simply have to put this single directive into miredo-server.conf:

```
ServerBindAddress 192.0.2.100
```

On the firewall side, miredo-server requires UDP port 3544 to be "open" on the server, on both server's IPv4 addresses.

On the IPv6 side, no special setting should be needed. The server should simply have a working IPv6 connectivity. It must be allowed to emit ICMPv6 packets with source in range 2001:0::/32 and destination within 2000::/3.

Teredo relay

The Teredo relay requires a single (public) IPv4 address and IPv6 connectivity. In miredo.conf, the "RelayType restricted" directive should be sufficient (please comment out the ServerAddress directive if present). You can optionally select a port number (BindPort 12345) if a fixed UDP port is needed, e.g. for firewalling purposes. IPv6 forwarding should be enabled on the host:

```
# echo -n 1 > /proc/sys/net/ipv6/conf/all/forwarding
```

Miredo will take care of adding required Teredo IPv6 routing and addressing on the host. However because IPv6 forwarding is enabled on the host, IPv6 autoconfiguration will no longer work, so you will have to setup the **non-Teredo** IPv6 addressing/routing manually.

An IPv6 route toward 2001:0::/32 should be exported to the other IPv6 routers. Miredo does NOT take care of that; it can be done with the usual mechanisms, either with manual routing configuration on the other routers, or with a dynamic routing protocol (BGP, OSPFv3, IS-IS, RIPng...). In the latter case a routing daemon will be needed in addition to Miredo (typically [Quagga/Zebra](#) or [BIRD](#)).

N.B.: it is perfectly ok to run miredo and miredo-server on the same host.

Specific relay setup instructions:

- [FreeBSD Setup](#)

Transitioning ___6to4

This is a transition mechanism in which the user configures a 6to4 client in their PC or home gateway. The 6to4 client receives dynamic tunnel services from a 6to4 server which is found via the anycast address prefix 192.88.99.0/24 allocated in [RFC 3068](#). This tunnel then attaches the IPv4 host to the IPv6 network using the IPv6 address 2002::V4ADDR::/48. The mechanism is documented in [RFC 3056](#). Most 6to4 implementations allow a relay router to be configured as an alternative to the RFC 3068 well-known relay router address. That address is exactly 192.88.99.1.

A complete explanation about 6to4 is available at [The IPv6 Portal](#).

ISPs can improve connectivity for their customers who are currently running IPv6 on their PCs by [setting up a 6to4 relay](#). This avoids the increased network latency caused by a trombone path to the IPv6 destination through a distant 6to4 relay. For an ISP's customers to find that relay it either needs to be explicitly configured in their client stacks, or it needs to be numbered 192.88.99.1 and the clients need to use the RFC 3068 address.

In addition, a content provider can also add IPv6 access to their services by configuring 6to4 on their network. Again, by shortening the path taken by one of the protocols, you ensure that there is no tromboning of the path and network latency is close to the minimum possible. Of course, you need to configure all the servers and related infrastructure responsible for those services to use IPv6, using a 6to4 prefix. Note that this is not particularly different from any other kind of IPv6 transit a content provider might decide to arrange.

For more info on specifics using Cisco, Linux and BSD, have a look at the [First Steps for ISPs](#) page.

Transitioning__NAT64

After seeing the interest in deploying NAT-PT in spite of its flaws, work was done on a cleaner IPv6 to IPv4 NAT solution known as NAT64. This is now gaining steam as the preferred option over [NAT-PT](#).

- An open source NAT64 implementation is available [here](#).

Transitioning__NAT-PT

This is a transition mechanism in which a gateway server fills a role similar to an IPv4 NAT box, except that it is also translating protocols as well as addresses.

The mechanism is defined in [RFC 2766](#) and although the IETF has deprecated it to historical status, it is likely to be widely used until the balance of Internet sites are accessible through IPv6.

- [NAT-PT Transition Study and Test Report](#)
- [An article on setting up NAT-PT on Linux](#).
- [Guide to Building a Linux IPv6 Router with NAT-PT](#) Good Howto document for setting up your own lab or home trial of NAT-PT
- Cisco supports [Express Forwarding for NAT-PT](#) in IOS 12.4

There are alternatives to NAT-PT being developed such as [IVI \(roman numerals for iv and vi\)](#). This was developed in China where there is already a large IPv6-only Internet backbone covering 18 cities. For more check [these slides from IETF OPSAREA](#). Also, [Kernel patches are available](#) for an IVI server for Linux 2.6.12 and 2.6.18.

NATPT is likely to be replaced by [NAT64](#) now that the IETF is taking this type of transition gateway seriously.

Transitioning__Teredo

A complete explanation about Teredo is available at [The IPv6 Portal](#).

ISPs currently announcing a teredo prefix

Oceania/Asia

Europe

Ireland

- 42227 Airwire

North America

- 6939 Hurricane Electric

Renumbering an IPv6 Network

Before you design your network layout and addressing plan, it is a good idea to find out what needs to be done to simplify future renumbering.

The following message from an ARIN mailing list, recounts one person's experience with IPv6 renumbering:

My organization recently changed IPv6 numbers. We had used EUI64 addressing on servers and used a "subnetting" scheme that was logical and sustainable. It did not require actually touching any servers to change IPs. It was done as such: Add IP prefix to appropriate router interfaces, run find-replace script to fix prefixes in DNS, wait, remove old IP prefixes from router interfaces.

While I am not trying to diminish the valid conversation about difficulties involved in renumbering, etc., I am actually doing, and have done this. IPv6 is not IPv4, and there are some aspects of it that change the ways things are/can be done. In our experience, the largest hurdle involved in using IPv6 effectively is getting folks to break out of the IPv4 way of thinking. With larger address spaces come the ability to address interfaces, etc. in a more logical way, that when added to some of the nice things like EUI64 addressing, can make "re-numbering" considerably easier.

We do not terminate VPNs, and in fact, because of limitations associated with traditional VPN-V4 L3 MPLS where services like Multicast and IPv6 have been concerned, we don't use that technology (much - we have the luxury of being able to not use it for the most part). We do have a great many downstream members (members to us, most would call them "customers") who use our IP space. One of them is very active with IPv6 (a larger community college of all places, not a major university), and I understand they simply made prefix changes much as we did, as they planned for this eventuality when they initially deployed.

You might also want to have a look at RFC 4192 entitled *Procedures for Renumbering an IPv6 Network without a Flag Day* to better understand how the process differs from IPv4.

Troubleshoot IPv6 Issues

- [Verifying the IPv6 Experience](#)
 - [Identify your IPv6 address](#)
 - [Test your IPv6-based browsing connectivity](#)
 - [Test your e-mail server connectivity](#)
 - [Test webmail](#)
 - [Test FTP access](#)
 - [Test NTP access](#)
 - [Test Telnet access](#)
 - [Test Performance](#)
 - [Test Network Connectivity](#)
 - [Test PMTUD](#)
 - [Test support of Extension Headers](#)
 - [Test Website](#)
 - [Test IPv6 readiness of a domain](#)
 - [Test for open ports](#)

Use this page to collect tips on how to troubleshoot IPv6 issues. For instance, adding an AAAA record for a service to your DNS may result in a small percentage of end-users losing connectivity and others experiencing unusually high latency. The root cause for connectivity loss is usually that the end user is on another network with IPv6 on their PC but no form of IPv6 connectivity. In fact, their company may be blocking Teredo and 6to4 traffic. The root cause for high latency is usually that the end user is using some form of tunnel (ISATAP, tunnel broker, 6to4, Teredo) that causes their traffic to trombone out to a distant tunnel endpoint and then come back again, or perhaps the tunnel endpoint is on a network that has poor IPv6 connectivity.

As you deploy IPv6 and as other networks deploy IPv6, your helpdesk will see new and different problems. Also, problems that seem familiar will turn out to have different root causes from before. You will need to deal with this issue even if you are delaying implementation of IPv6 in your own network.

In order to debug connectivity issues, you can easily traceroute from various places to your network by setting up an IPv4-only host and setting up various kinds of transition technologies on it (6to4, Teredo, gogo6 and SixXS tunnels, etc.)

Verifying the IPv6 Experience

It may not be initially obvious, but your IPv6 throughput may not be the same as your IPv4 throughput.

- Service providers may have IPv6 transit or peering, but those connections may not be dual-stacked and so IPv6 operates over a

- separate physical interface than the IPv4 traffic.
- The IPv6 path is more circuitous than IPv4 because of sub-optimized routes to get to the target node. Because there are so (comparatively) few IPv6 links, the physical path to the target node may be indirect.
- The service provider may have less-optimized transit or peering links than IPv4, and so while they may have IPv4 peering with Company A and B, they may not have IPv6 peering with Company B.
- An intermediate router(s) may not be able to route IPv6 in hardware but only in software, and relatively low levels of traffic may bring the router to a very high level of CPU utilization resulting in lower IPv6 throughput.
- The service provider may be using tunneling for IPv6.

In addition to their service provider's topology, an end-user's local IPv6 environment may result in poor IPv6 throughput.

- The end-user's PC could be using Teredo and all the traffic is being tunneled through a remote host positioned sub-optimally in the path to the target node.
- The end-user's router tunnels to a remote host that is also not in the path to the target node.
- The end-user's router is performing IPv6to4 and the network stack is not well-optimized.

Identify your IPv6 address

- ipv6.whatismyv6.com
- ip6.me
- Traceroute6.net Also provide AAAA lookup and traceroute features
- whatismyipv6address.com
- runningipv6.net
- IPv6-test.com
- <http://test-ipv6.se/> and <http://test-ipv6.com/>

Test your IPv6-based browsing connectivity

- [Akamai IPv6 connectivity check](#)
- [IPv6 eye chart](#) hosted by RIPE that check IPv6 access to websites that are participating in World IPv6 Day
- [Test IPv6](#) in several different ways
- [onlyv6.com](#) only accessible if your client has IPv6 connectivity AND configured DNS servers with IPv6 connectivity.
- [Test IPv4, IPv6, and 6to4](#) in several different combinations
- <http://test-ipv6.se/> and <http://test-ipv6.com/> test your IPv6 connectivity

Test your e-mail server connectivity

- [E-mail reflector](#) helps email users identify whether or not they're sending over IPv6 and also clues them in to what their DNS looks like from the outside world. It will reply to the email showing the Received headers as well as dig -t mx output for the domain.
- This is a tool for testing if your mail setup is capable of sending IPv6 emails. To use this tool simply send an email to bouncer@freenet6.net and if your mail is IPv6 enabled, you should receive an instant reply. If you do not receive a reply, that means that your mail system is probably not IPv6 enabled. You can leave subject field and body of the message empty, or you can put something in the subject field that will help you identify reply email. The body of the message can be empty and will be replaced in the reply with some helpful information (the date the message was received and the path of the message). Please note that the bouncer is only reachable over IPv6, however, the reply message may be mailed to you over IPv4. Check message headers of the reply message. Missing the reply message? Check your spam folder.
- Anyone can send an e-mail to echo@v6address.com and get a dual stack reply - if the sending e-mail system is IPv6 ready the response will return over IPv6. if not, it will come back over IPv4. The reply contains the message headers (as the message body) of the message that was sent (the message body is discarded). More [here](#).

Test webmail

- Free [webmail](#) service that's accessible over IPv6 (and IPv4). Open account [here](#) (note: site is in German)

Test FTP access

- ftp.ipv6.debian.org
- ftp6.netbsd.org
- ftp-v6.cuhk.edu.hk
- ftp.snt.ipv6.utwente.nl
- ftp6.rrze.uni-erlangen.de
- ftp6.uni-erlangen.de
- ftp.ipv6.uni-muenster.de

Test NTP access

- ntp.ipv6.uni-leipzig.de
- ntp.freenet6.net
- ntp.hexago.com
- ntp.sixxs.net
- ntp6.space.net
- time.join.uni-muenster.de
- time6.ipv6.uni-muenster.de

Test Telnet access

- ipv4.test-ipv6.com 79 for IPv4 only
- ipv6.test-ipv6.com 79 for IPv6 only
- ds.test-ipv6.com 79 for either

Test Performance

The only way to know the actual 'goodput' of your IPv6 link is to measure that with an IPv6-based test. Here are some IPv6 "speed test" sites:

- [University of Maine \(US\)](#)
- [Bredbandskollen: warning Swedish language](#)
- [IPv6-speedtest.net \(UK\)](#)
- [Speedtest6.com: Located in Japan & Hong Kong, Test IPv6 traffic in Asia](#)
- [InspireNet Bandwidth \(NZ\)](#)
- [Premier Communications' \(US\)](#)
- [Westland Cable Clan \(NL\)](#)
- [thinkbroadband \(UK\)](#)
- [aissp \(UK\)](#)
- [lava.net \(US\)](#)
- [Harry's Seite \(DE\)](#)
- [Parque Tecnológico de Bizkaia \(BR\)](#)
- [ipv6-test.com \(ES, FR, RO, IN\)](#)
- [Baseline, Monitor, Troubleshoot User Experience over IPv6](#)

Here are some large files accessible over IPv6:

- [Tele2: 10 GbE connection to their core, capable of at least 5Gbps](#)

Here are some IPv6-capable throughput software tools:

- [Distributed Internet Traffic Generator \(D-ITG\) with Java-based GUI](#)
- [Iperf](#)

Test Network Connectivity

Thorough diagnostic tests of network links (both require Java)

- [International Computer Science Institute's Netalyzer](#)
- [University of Maine's Network Diagnostic Test \(NDT\)](#)

Without Java - <http://test-ipv6.se/> and <http://test-ipv6.com/>

Test PMTUD

- The [WAND network research group](#) provides a set of PMTUD Tests. See also this [guide to interpreting the test results](#). For background, consult [this presentation](#)
- Based on [WAND network research group](#) scamper <https://interlan.se> created <https://IPv6alizer.se> to test PMTUD for websites.
- The web server at <http://www.ipv6chicken.com> uses a large MTU on its own interface to provide a quick test of PMTUD operation in the path from them to your local network.
- <http://test-ipv6.se/> and <http://test-ipv6.com/> test your IPv6 and PMTUD

Test support of Extension Headers

- The path6 tool of [SI6 Networks' IPv6 Toolkit](#) is an IPv6-enabled traceroute-like tool with full support for IPv6 Extension Headers.

Test Website

If you host a website and want to test your end users' IPv6 access:

- IPv6 Test Analyse (warning: in Dutch)
- Tag site and track (Andrew Yourtchenko)
- IPv6 test widget
- IPv6 dual-stack client loss in Norway
- HTML/iframe include to check IPv6 brokenness
- IPv6 validation in JavaScript
- Crisp's IPv6 validation
- Warning broken users with JavaScript
- Geoff Huston's integration with Google Analytics
- Compare IPv6 and IPv4 User Experience

Test IPv6 readiness of a domain

- IPv6 status check
- FQDN and prefix status check
- IPv6 Readiness Checker
- chair6' basic IPv6 checks
- IPv6 Health Check
- <http://go6.se/check/>

Test for open ports

Here are some web sites that use an NMAP scan over IPv6 to test for open ports on the visitor's address

- IPv6 Endpoint Open Ports Check
- SCANIPV6.com - Online Port Scanner (for IPv4 and IPv6)
- Hurricane Electric's Portscan (requires Tunnelbroker account)
- Online Open-source IPv6 Firewall tester (see [source at github](#))
- Tim Chappell's IPv6 Ping & Portscan (open to all IPv6 hosts)

FreeBSD

FreeBSD is a 4.4BSD-Lite2 based operating system. It is free for all, and licensed under the BSD license. It contains a mature IPv6 stack. The first version to contain IPv6 support was FreeBSD 4, which included the *KAME* stack.

Ports

Several ports to support IPv6 users are included in the FreeBSD ports collection, which includes a variety of free and open-source software. These include *net/sixxs-aiccu*, *net/ipv6calc*, *net/ipv6gen*, *net/radvd*, *net/gateway6*, *net/openvpn*, and more.

Tunnel support

Several types of tunnels are supported. Generally, these use the **gif** or **tun** devices, depending on the type of tunnel used.

Kernel drivers

IPv6 is supported in the GENERIC kernel which is installed when you install FreeBSD from release media. In order to explicitly compile IPv6 support into your kernel, the configuration must include the **INET6** option directive. You may also wish to include support for the **gif** or **faith** devices.

Building ports and/or world

The following line can be added to your */etc/make.conf* to enable IPv6 by default when building ports or world:

- WITH_IPV6='true'

Related pages

- [Linux or BSD 6to4 Relays](#)

External links

- [FreeBSD official website](#)
- [The FreeBSD handbook section on IPv6](#)
- [A reference from O'Reilly - Note: out-dated, references 6bone.](#)

Linux Support

This page contains information about support for IPv6 on Linux

Linux IPv6 Sites

- [Deepspace6 Linux IPv6 Project](#) - Good Summary of Linux Application IPv6 Support
- Peter Beiringer's [Linux IPv6 HOWTO Pages](#)
- The [USAGI Project](#) bringing standard IPv6 support into Linux kernel code tree

Solaris IPv6 Sites

This page contains links to various useful sites about IPv6 on Solaris and OpenSolaris.

Solaris and OpenSolaris IPv6 Sites

- [Good overview of IPv6 in Solaris 8,9,10 and OpenSolaris 2009.6](#)
- [Configuring an OpenSolaris 6to4 router](#)
- [Security issue in Solaris 10 and OpenSolaris build 102-107](#)
- [Chapter from Sysadmin guide on Enabling IPv6 on a Network](#)
- [How to configure IPv6 on OpenSolaris compared to Slackware](#)
- [IPv6 in Shared Stack Zones](#)
- [DTrace Network Provider supporting IPv6 tracing](#)

Warning broken users with JavaScript

Introduction

The main concern for a web site operator that wants to deploy dual-stack service on his site, is the existence of *broken users*, i.e., users that could access his site fine while it was available over IPv4 only, but for some reason have problems accessing it when it is made available over IPv6 as well. A list of the most common causes for this is found in [Customer problems that could occur](#)

At the time of writing, measurements done by several organisations indicate that at least 1 in 2000 users currently have this problem, see:

[Google's presentation at RIPE 61](#)

[Redpill Linpro's presentation at RIPE 61](#)

[Yahoo's presentation at IETF 77](#)

One thing a web site operator can do about this problem, is to automatically identify these users whenever they visit his web site (which presumably is IPv4-only at that point), and display a warning of some kind that informs the users that they have a problem, and preferably how to fix it, too. That way, when the site is finally dual-stacked, the users will have had ample warning.

It is also useful to warn broken users in this way even after the site has been dual-stacked, as they will in most cases be able to load a dual-stacked page if they are patient enough to endure an initial connection timeout over IPv6.

A much more comprehensive (and probably better) solution for testing the user's IPv6 connectivity is available from [falling-sky](#), the open-source variant of Jason Fesler's [test-ipv6.com](#).

JavaScript code

Add this code near the bottom of your HTML pages. It should work as-is, but see below for some more discussion about how to adapt it better to your site.

```

<!-- these are the test elements that will be loaded by the JavaScript below -->
<IMG id="1x1_ds_testing_1" class="1x1_ds_testing" width="1" height="1">
<IMG id="1x1_ds_testing_2" class="1x1_ds_testing" width="1" height="1">
<IMG id="1x1_ds_testing_3" class="1x1_ds_testing" width="1" height="1">
<IMG id="1x1_v4_testing_1" class="1x1_v4_testing" width="1" height="1">
<IMG id="1x1_v4_testing_2" class="1x1_v4_testing" width="1" height="1">
<IMG id="1x1_v4_testing_3" class="1x1_v4_testing" width="1" height="1">

<!-- Remove the line below if you're already loading the jQuery library -->
<SCRIPT
src="https://ajax.googleapis.com/ajax/libs/jquery/1.4.2/jquery.min.js"></SCRIPT>

<SCRIPT language="javascript" type="text/javascript">
$(window).load(function() {
    // Defines for how many milliseconds we're willing to wait for the test elements
load before
    // considering it a failure. Should not be more than 21 seconds, as that's
Microsoft Windows'
    // connect() timeout.
    var timeout = 5000;

    // Records the number of dualstack and ipv4-only successes.
    var ds_ok = 0;
    var v4_ok = 0;

    $('#1x1_ds_testing').load(function() {
ds_ok++;
    });

    $('#1x1_v4_testing').load(function() {
v4_ok++;
    });

    // Load the test images while trying to avoid caches.
    var rand = Math.random();
    $('#1x1_ds_testing_1').attr('src', 'http://<dualstacked hostname
1>/lib/1x1.png?rand=' + rand);
    $('#1x1_ds_testing_2').attr('src', 'http://<dualstacked hostname
2>/lib/1x1.png?rand=' + rand);
    $('#1x1_ds_testing_3').attr('src', 'http://<dualstacked hostname
3>/lib/1x1.png?rand=' + rand);
    $('#1x1_v4_testing_1').attr('src', 'http://<ipv4-only hostname
1>/lib/1x1.png?rand=' + rand);
    $('#1x1_v4_testing_2').attr('src', 'http://<ipv4-only hostname
2>/lib/1x1.png?rand=' + rand);
    $('#1x1_v4_testing_3').attr('src', 'http://<ipv4-only hostname
3>/lib/1x1.png?rand=' + rand);

    // Check the result of the test after the timeout have expired.
    var t = setTimeout(function() {
        // We take the conservative approach here. 100% success with
// IPv4 combined with 0% success with dualstack is necessary
// to give user a warning about broken IPv6.
        if(v4_ok == 3 && ds_ok == 0) {
            alert("You have a problem accessing dual-stack sites!");
        }
    }, timeout);
});
</SCRIPT>

```

Improving the warning

The code above will just throw a JavaScript `alert()` pop-up, which is likely not what you want. You probably want to replace this with a nicer-looking error box/banner that gives a warning in the same language as the rest of the site, and giving pointers to further information so that the user will be able to solve the problem himself, or alternatively contact you for help.

Hosting of the test elements

You should make sure to use different hostnames for each URL, preferably pointing to different IP addresses. This prevents browsers from doing clever optimisations which could trick the test.

Changing the timeout and number of test elements

The timeout setting should be higher than the time required by a normal client to load the test images, but lower than the systemic connect() timeout of the common operating systems. The lowest such timeout is, to the best of my knowledge, 21 seconds (Microsoft Windows).

You can also modify the number of test elements loaded if you feel that six of them makes the test too heavy-weight. I would not go below one ipv4-only PNG though, because otherwise you might be testing whether or not the machine that hosts the test elements is up or not; or below two dual-stacked PNGs, because a single load failure could be caused by a number of unrelated things, such as the user having a congested Internet connection.

Author and copyright information

The code was written by me, [Tore Anderson](#), and is released into the public domain. Do with it what you wish.

Sites who have this or something similar in production

Please add your site here if you add such a test, so that others can have a look at it for inspiration!

- [Brian Carpenter's home page](#)
- [Consulintel web site](#)

3GPP Mobile Networks

Audience

The intended audience is Mobile Packet Core engineers that wish or need to deploy IPv6.

3GPP networks is an acronym rich field. For more general audiences [RFC 6459](#) is an excellent primer.

The introduction of IPv6 to the 3GPP Standards and Mobile Networks

The 3GPP maintains the standards for [General Packet Radio Service](#) (GPRS) based 2G/3G wireless access networks and its [System Architecture Evolution](#) (SAE) for LTE and LTE-Advanced wireless access. 3GPP Release 8 introduced Evolved-UMTS Terrestrial Radio Access (E-UTRA), which is designed to provide a single evolution path for many different radio access technologies: [GSM/ EDGE](#), [UMTS/ HS PA](#), [CDMA2000/ ED-VO](#), [TD-SCDMA](#) to LTE and beyond. Release 8 defines a new Evolved Packet Core (EPC) which must be implemented when deploying LTE access.

IPv6 was first introduced into the 3GPP standards with release 99 (in year 1999) but was not widely implemented by equipment vendors or deployed by Mobile Network Operators.

3GPP Release 9 is considered a minor update to Release 8 but it introduced support in GPRS for dual-stack IPv4v6 [PDP contexts](#) on a single shared radio access bearer. Release 9 also resolved the anomalous situation with Release 8 where dual-stack was supported for LTE access but not supported for GPRS access. Others are of the view that the anomaly was with software implementations of the standards. In any case all new equipment is free of the problem. Release 10 introduced DHCPv6-PD to the standards.

User and Transport Planes

IPv6 must be enabled in the user-plane so that subscribers can start using the IPv6 Internet. This is the PDP/PDN bearer from the mobile device to an IP gateway in the Mobile Network Operator's core network. Operators and equipment vendors are therefore prioritising the deployment of IPv6 in the user-plane.

User IP traffic from the mobile device (User Equipment) is in a separate logical user-plane transported over the network. The transport, signalling, OAM, or charging interfaces within the network are hidden from the User Equipment (UE) and initially can continue to use IPv4

while the user-plane is providing IPv4v6 or IPv6 (with IPv4 translated through a local NAT46 clatd) connectivity to the subscriber. Many newer Release 9 networks will have user-plane IPv6 enabled by default even though they have not configured their GGSN/PGWs to assign IPv6 /64s & their HLR/HSS subscriber profiles to allow IPv6 PDP/PDN bearers. It is also important that user-plane IPv6 is allowed for visiting subscribers to get back to their home network that has adopted IPv6. In June 2014 Telenor of Norway started roaming by default using IPv6 for customers with the Samsung S5.

The Radio Access Networks & Mobile Packet Cores

The SGSN and GGSN are the core network elements for GERAN/UTRAN (2G/3G) APN access.

The SGW, PGW and MME are the EPC network elements for E-UTRAN (LTE) APN access.

Real nodes combine these functions to support multiple RAN and core types. For example the SGSN-MME and S/P-GW are common combinations. To ensure data session continuity the GGSN function is also combined with the P-GW function so that there is a common anchor point for the PDP/PDN connection.

PDN Types must match when inter-SGSN RAU (Routing Area Updates) or intra-RAT (Radio Access Technology) handovers for the mobile UE (User Equipment) takes place. All SGSN/MMEs where this can occur in an operator's network must therefore be on Release 9 compliant software for PDP/PDN Type IPv4v6 to be possible.

The PGW

The PGW (also known as the PDN-GW) is the EPC network element that assigns the IP addressing information to the mobile UE. Individual IPv4 addresses are assigned and/or an IPv6 /64 prefix is assigned.

Typically the addresses or prefixes come from pools configured in the PGW. They may also however come from other sources such as the HLR/HSS, PCRF or RADIUS AAA server.

To facilitate inter-RAT the PGW may also support GGSN functionality if a Gn/Gp SGSN is used initially instead of an S4-SGSN. See 3GPP TS23.401 Annex D (GPRS enhancements for EUTRAN access, Release 9).

SLAAC is used to assign the prefix to the UE, therefore only a /64 prefix can be used. This is prefix size not a configuration option because SLAAC mandates that it be /64. The host bits should change with each connection. DoS protection against attacks on the /64 may be implemented.

3GPP Release 10 allows the UE to request a delegated prefix (IA_PD) using DHCPv6. Note that UEs do not yet implement support for DHCPv6-PD.

Single or Dual-Stack PDP/PDN Bearers

PDP/PDN bearer may be: IPv4 (the existing legacy setting), IPv4v6 (Dual-Stack in a single radio bearer) or IPv6 (without a parallel IPv4 bearer, the target solution).

The transition guidelines of the IETF and 3GPP ([TR23.975](#)) is dual-stack first and then IPv6-only as IPv4 is phased out. However there are a couple of issues with dual-stack in 3GPP networks that do not apply to fixed networks (discussed further in this page). There are operators using IPv4v6 (e.g. Verizon Wireless) and IPv6-only (e.g. T-Mobile USA, Orange Poland, Telenor Norway) PDP/PDN bearers.

As the situation currently stands there are many operators with 2G/3G access networks on pre-release 9 and LTE access networks on release 8/9. This rules out the use of dual-stack PDP/PDN bearers in such PLMNs as session continuity (uninterrupted data access) during inter-Radio Access Technology (inter-RAT) handovers is not possible. This situation will improve with time as equipment is software upgraded or decommissioned, however it is currently the main networking issue preventing IPv4v6 PDP/PDN type roaming and inter-RAT handovers.

To make IPv6-only PDP/PDN bearer a viable migration strategy, the operator must provide NAT64/DNS64 service to the UE and the UE must support a [RFC 6877](#) NAT46 clatd. The clat has been standard in Android since 4.4 (or 4.3 in T-Mobile USA's case) and it was introduced in Windows Phone 8.1. Apple iOS is the notable exception. Here is a video <http://youtu.be/XI-hlyZSAmA> of Cameron Byrne from T-Mobile US talking about how they are using this to "break free" of IPv4.

Dual-Stack using two separate bearers

This is possible but it: consumes more radio resources, consumes more PDP licences, generates two sets of billing CDRs and can cause session continuity issues with LTE handovers where IPv4_OR_IPv6 is the allowed PDN type. Therefore it is not a desirable configuration for the network operator. To occur: the HLR configuration must allow IPv4 and IPv6 for the APN but not allow dual-stack within a single bearer, the RAN must allow multiple simultaneous radio bearers from the UE and the UE itself must set up separate PDPs for IPv4 and IPv6. This situation may occur where the HPLMN wants to provide home IPv6 access but does not have a means of preventing the sending PDP-Ext-Type (signalling dual-stack within a single radio bearer) to visited SGSNs. A Release 9 compliant HPLMN providing dual-stack within a single bearer is incompatible with roaming to a pre-release 9 visited SGSN that does not fall back gracefully to IPv4. The HLR/HSS needs the capability to allow separate home and roaming PDP/PDN protocol types to avoid these related problems.

vvvvvv	CALLID	MSID	USERNAME	IP
TIME-IDLE				


```

-----
-----
IUCNAI 160e0eec 27203----- 35385-----@testdata 100.127.248.16
00h00m09s

VUCNAT 160e0eed 27203----- 35385-----@testdata 2a01:b340:ee0:e51:0:16:e0e:ed01
00h00m04s

```

The above GGSN/PGW CLI output shows two separate PDP bearers from a single UE (a Samsung S4 based on Android 4.4.2). The UE APN protocol was set to "IPv4/IPv6" and the HLR was set to allow both IPv4 and IPv6 bearers for the APN. In the HLR APN configuration the extended PDP indicator to allow dual-stack on single radio bearer was not set (see example of this in the HLR/HSS section below).

The Dual Address Bearer Flag

If all the SGSNs in an operator's network can support dual-stack PDP then the DAF flag should be set in the node properties of all the SGSN/MMEs concerned. Otherwise dual-stack PDN connections will not be brought up by the PGW. This is even if the HLR/HSS & PGW are configured for IPv4v6 and the mobile UE requests IPv4v6. Instead, the PGW may bring up an IPv4 or an IPv6 PDN bearer.

Roaming Issues

As IPv6 is deployed mobile operators will need to update their roaming agreements to indicate their ability to support visitors with IPv4v6 and/or IPv6 PDP/PDN connections. The GSMA RAEX IR.21 Roaming Database has fields to take this information. What seems to be happening in the real world is that operators are just doing it without comprehensively updating all their documentation.

They also need a way of controlling the PDP type signalled to visited SGSNs when their subscribers roam. Dual-stack is not possible in roaming situations where the visited pre-release 9 SGSN does not gracefully fallback to an IPv4 PDP session if it receives an Extended PDP type flag from the roaming subscriber's HLR. These problems are currently the subject of an [Internet Draft](#) in the IETF v6ops WG. Currently the 3GPP standards do not allow for per VPLMN subscriber profiles depending on the visited operator's ability to correctly handle IPv6. Since IPv4 and IPv6 PDP types were introduced to the standards at the same time support for IPv6 PDP is more widespread. Android provides an APN roaming protocol field which may be set to IPv4. In combination with a subscriber profile allowing IPv6 (used when home) and IPv4 (used when roaming) this Android APN configuration option provides a way for operators to deploy IPv6 at home for maximum impact and leaves the roaming issues for another day when IPv6 is more widely adopted by other PLMNs.

At least one (well known) HLR vendor has a feature to suppress the sending of the Extended PDP Type flag based on SGSN IP address but they have not made it a standard feature included without extra cost.

In at least one vendors SGSN/MME, user plane IPv6 needs to also be explicitly allowed in the case of another PLMNs subscribers visiting the network. It is more straightforward to make the network ready for visitors using IPv6 PDP/PDN connections than it is to allow the IPv6 friendly operator's own subscribers set-up an IPv6 PDP/PDN back to their home network.

The HLR/HSS

The HLR uses SS7/MAP over the Gr interface to send the user profile to the SGSN.

An S4-SGSN uses Diameter and the S6d interface. The HSS uses Diameter and the S6a interface to send the LTE user profile to the MME.

An S4-SGSN is also likely to have been implemented with Release 9 support.

```

<hgppp:pdpcp=240;
HLR PACKET DATA PROTOCOL CONTEXT PROFILE DATA
PDPCH  APNID  EQOSID  VPAA  PDPTY  PDPID  EPDPIND
240    80     1      NO    IPV4    25     NO
      76     1      NO    IPV4    26     NO
      74     1      NO    IPV4    31     NO
      73     1      NO    IPV4    32     NO <-- testdata APN V4
      73     1      NO    IPV6    50     NO <-- testdata APN V6

```

The above HLR configuration example shows a single APN (ID = 73) with both IPv4 and IPv6 PDP allowed but the Extended PDP indicator (epdpind) not set. In this situation the desirable APN protocol setting in the UE is IPv6 instead of IPv4/IPv6 because of the reasons listed in the section on single or dual-stack bearers above.

The PDN type options in the HSS with LTE are better: IPv4, IPv6, IPv4_or_IPv6 and IPv4v6.

3GPP Release 10 clarified that when a user profile has PDP/PDN Type IPv4v6, types IPv4 or IPv6 are also allowed if requested by the mobile device.

Large-Scale or so-called Carrier Grade NAT

The use of NAT44 is very widespread in 3GPP networks. Typically all subscribers will go through the provider NAT. Besides preventing end-to-end connectivity the NAT causes performance degradations such as limits on TCP ports and applications that are broken by NAT. With IPv6, customers get improved service as all applications using it end-to-end will bypass the restrictions of the NAT. As the deployment of IPv6 proceeds traffic growth through the NAT should slow and eventually start declining. There is a strong incentive to eliminate all legacy IPv4 applications in new devices in particular as otherwise NAT subscriber host state may continue to grow as billions more devices are added to the Internet.

Migration Strategies for the PDP/PDN IP Connection

IP on link to UE	Main Pros	Main Cons
IPv4-only (Do Nothing)	Waiting while innovators and early adopters solve any remaining technical barriers to IPv6 adoption	Does nothing to solve the internal private IPv4 addressing problem
		Increasingly inferior service for customers as the ratio of IPv6 to IPv4 grows
		No cost savings from bypassing CGN
		Missed opportunities/lost customers, no one wants to be last to adopt IPv6
IPv4v6 (Dual-stack)	iPhone/iOS works at home with it (with restrictions on roaming)	Does nothing to solve the internal private IPv4 addressing problem
	Allows CGN bypass by IPv6 traffic	Dual-stack is not well supported when roaming. Fallback to IPv4 or proprietary features needed in HLR/HSS to workaround old pre-Release 9 visited Gn/Gp SGSNs that can't handle dual-stack in a single bearer
	New opportunities/new customers	Retains all of the IPv4 network operations overhead and much of the resource consumption of IPv4
IPv6-only (using RFC6877 backwards compatibility for IPv4)	Solves the internal private IPv4 addressing problem	RFC6877 IPv4 "clat" not yet supported by Apple iOS
	Stock Android 4.4+ works with it	
	Allows CGN bypass by IPv6 traffic	
	New opportunities/new customers	

Billing Domain & Charging

Mobile Packet Core elements (SGSN, GGSN, SGW, PGW) can all generate Charging Data Record (CDR) files which can be used, after further processing, for billing.

The SGSN produces S-CDRs, the SGW produces SGW-CDRs, the PGW can also produce PGW-CDRs.

There are a number of fields in the CDRs where IPv6 related information will appear. The mediation system which processes these CDRs for billing or a pre-processing script stage may be needed to deal with these minor changes to prevent the case of a 128-bit value being loaded into a 32-bit field. Usually the billing domain CDRs (e.g. TAP3) do not use the IP address information in the CDRs coming from the network elements. 3GPP TS 32.251 (Charging management; Packet Switched (PS) domain charging) describes the fields.

From Release 9, S-CDRs contain the following relevant fields, concerned with the mobile devices IP-CAN bearer.

S-CDR field	Values	Comment
PDP Type	IPv4, IPv6, IPv4v6, PPP, IHOSS:OSP	
Served PDP Address	IPv4 address when PDP Type is IPv4, IPv6 address when PDP Type is IPv6 or IPv4v6	Note this field can hold an 32 bit IPv4 or 128bit IPv6 address depending on PDP Type. A system processing this field may need to be updated accordingly
Served PDP/PDN Address extension	IPv4 address of the PDP when the PDP Type is IPv4v6	The generation of this field may be a configuration option (e.g. it is with Cisco Star OS)

SGW-CDRs & PGW-CDRs contain 3 similar fields. The CDRs produced by the elements may be proprietary and not 3GPP compliant.

If on-line charging (e.g. using PCEF function in the PGW and the Gy interface) is used then the above CDR considerations mainly apply to roaming and the ability of the visited PLMN to process CDRs containing IPv6 addresses.

IMS & VoLTE

VoLTE implements VoIP using IMS instead of using Circuit Switched Fallback (CSFB). IPv6 support was in IMS from the start. It is straightforward to use IPv6 with VoLTE. IMS (GSMA IR.92) requires a separate APN from the Internet APN therefore the inter-RAT and roaming issues with Internet access APNs do not arise. IPv6 is mandatory with VoLTE. All VoLTE phones have Radio Interface Layers that support IPv6.

The evolution to VoLTE should act as a further stimulus to user-plane IPv6 deployment because the UE will require at least two IP addresses at the PGW, one for Internet access and the other for VoLTE.

Proxy Mobile IPv6 is not used for 3GPP access

Proxy Mobile IPv6 (RFC 5213) is not used in any production 3GPP networks and is not involved in the transition of user-plane services to IPv6. The existing GTP based transport mechanisms are used.

Mobile Operating Systems

Android, Apple iOS, Windows Phone, Blackberry

Operating System	Supported PDP/PDN APN Protocols	Separate Control of APN Roaming Protocol	RFC6877 NAT46 clat when APN Protocol is IPv6
Android 4.4*	IPv4, IPv4v6, IPv6	Yes	Yes
iOS 8.0	IPv4, IPv4v6	?	No
iOS 9.0	IPv4, IPv4v6, IPv6	?	No, but bump-in-API approach for IPv4 literals
Windows Phone 8.1	IPv4, IPv4v6, IPv6	?	Yes
Blackberry	IPv4, ?	?	No
SailfishOS/Jolla Phone	IPv4, IPv4v6, IPv6	No?	No?

Android 4.4 and beyond has a [464xlat](#) clat, running as a daemon, that works in combination with a [NAT64](#) CGNAT box in the provider's network. It presents an IPv4 interface to the mobile device and other devices tethered off of it. Using the stateful translation algorithm of [RFC 6145](#) IPv4 packets are translated into IPv6 packets so that they may be sent over an IPv6-only PDP/PDN connection. Note that these packets are translated, not encapsulated, it is easier for the charging functions in GGSN/PGWs to be agnostic to 464xlat translated IPv4 traffic or native IPv6 traffic. This has been verified in production networks. MAP-T also uses the translation algorithm of RFC6145 and has the advantage of distributing the NAPT state away from the CGNAT box to the access device. Unlike 464xlat there is no client implementation. It also needs a means of communicating the allowed port range to the client; such as PCP or DHCPv6.

3GPP TS 24.301 says LTE devices must first request IPv4v6 but in practice this is controlled by operator/carrier configuration files. In Android it may be edited and separate home and roaming PDP/PDN types may be set. However as mentioned in the roaming section above this functionality alone is not enough to deal with the problem of old SGSNs.

Apple iOS supports dual-stack tethering when the PDP/PDN connection is IPv4v6. At [WWDC 2015 Apple announced](#) upcoming improvements in IPv6 support in iOS 9. App developers will be required to verify their App with IPv6-only and NAT64+DNS64. iOS 9 will work with IPv4 literals when using the NSURLSession API on a NAT64+DNS64 network. The API will bump in an IPv6 literal synthesized according to RFC 7050. They do not support under-the-sockets bump-in-API (RFC 3338) or 464XLAT (RFC 6877).

*The clatd was introduced in Android 4.3 but the phone needed to be rooted to add the /etc/clatd.conf configuration file or it needed to be an operator specific build (initially T-Mobile US).

Windows Phone 8.1 has recently [introduced support for RFC 6877](#).

Discussion of Sailfish <https://together.jolla.com/question/89966/use-dual-stack-ipv4-and-ipv6-on-mobile-data-by-default/> here.

Smartphone APN editing functionality that assists the transition to IPv6

Stock Android 4.4.2 is very IPv6 transition friendly and a number of operators consequently list smartphones based on it amongst the first devices that they support when deploying IPv6. e.g. The Google Nexus 5 and Sony Xperia Z. With these UEs it is possible to edit the APN protocol and APN roaming protocol in the APN settings. At the early stages of the transition being able to select IPv4 or IPv4/IPv6 APN protocol instead of IPv6 is conducive to supporting the small number of subscribers using IPv4 only VPN access protocols.

Samsung's policy since Android 4.4 (KitKat) is that editing of APN protocol and APN roaming protocol is not blocked (option appears greyed out when it is blocked or unavailable). However for operator locked phones the operator needs to request that the new default (unblocked) applies to their CSC.

Tethering IPv6 off a 3GPP Internet connected device

This is documented in [RFC 7278](#). It should next be implemented in stock Android together with support for [RFC 6106](#).

IPv6 Internet tethering of devices using the 3GPP /64 was implemented in a number of devices prior to the creation of an RFC e.g. Apple iOS LTE iPhones on Verizon Wireless, Samsung and Sony devices.

Stock Android 4.4.2 (KitKat) currently only supports single-stack IPv4 tethering when the PDP/PDN connection is IPv4v6 or IPv6. When the PDP/PDN connection is IPv6, IPv4 traffic from the tethered IPv4 RFC 1918 prefix is forwarded through the 464xlat clat4 interface.

Samsung Android 4.4.2 smartphones support dual-stack tethering when the PDP/PDN bearer is IPv4v6 or IPv6. On the latest builds, the availability of which will depend on the operator, IPv4 tethering is supported through the 464xlat clatd on a PDP/PDN IPv6 bearer. All new Samsungs starting with the S5 support IPv4 tethering through the clatd.

Sony Xperia Z phones also support IPv6/464xlat, IPv4v6 and tethering of IPv4 and the shared /64 prefix.

Huawei E5372 3GPP WiFi hotspots also support /64 prefix sharing. The Huawei E3272 USB Stick also works by sharing the /64 prefix.

VPN Access Methods

OpenVPN is the working method because it uses TCP or UDP to transport SSL/TLS traffic. It is compatible with the RFC 6877 464xlat clat4 interface and does not require Application Layer Gateways in the NAT or use GRE as a tunnel transport protocol. OpenVPN 2.3 also introduced support for IPv6 inside the tunnel and as the tunnel transport.



Currently most OpenVPN tunnel providers only offer IPv4 connectivity through the tunnel and use IPv4 as the tunnel transport.

The Cisco VPN client in devices tethered through a UE doing 464xlat works.

IPv6 Consulting and Training Services

Do you know it is time to add IPv6 to your network, but you aren't sure where to start? Let us help. Below is a growing list of companies and individuals who have represented that they offer IPv6 consulting and training services.




If you or your organization provides IPv6 network consulting or training and would like to be included on this list, please [request a GetIPv6.info wiki account](#) and add your entry to the list in alphabetical order.



Company Name	Type of Training Offered	Service Area	Website and/or Public contact Email
	<ul style="list-style-type: none"> Hands On IPv6 Training (fundamentals and advanced) Using IPv6 with Wireshark IPv6 Consulting Online School of Network Sciences 	US, North America & International	www.netscionline.com www.cellstream.com
	<ul style="list-style-type: none"> IPv6 Consulting and training since 2001, worldwide - English and Spanish. Worked already in +110 countries. 	Worldwide	Consulintel
	<ul style="list-style-type: none"> IPv6 - Training, Strategy, Planning, Design, Consulting IPv6 - Security audit, Penetration testing IPv6 Forum Certified Course (Gold), CCIE and IPv6 Forum Certified (Gold) Trainer(s) 	Norway, Nordics, Europe, International	salg@datamatrix.no www.datamatrix.no

Get6!

In order to keep the Internet growing, organizations must "Get6" now to ensure their future success in a changing web environment. Find out how to make the case for the transition to IPv6 at the [TeamARIN.net website!](#)

<p>"Next Generation Security for the Next Generation Internet & IoT"</p> <ul style="list-style-type: none"> Joe Klein, CEO 	<p><i>Training:</i></p> <ul style="list-style-type: none"> IPv6 Hacking, Defense & Security Architecture Training <p><i>Services:</i></p> <ul style="list-style-type: none"> IPv6 Integration into Security Operations Center's (SOC) technology & processes IPv6 security audit & penetration testing <p><i>Product:</i></p> <ul style="list-style-type: none"> IPv6 (and dual stack) Cyber Threat Intelligence IPv6 IDS, Sensors & Analytics 	<p>US, North America & International</p>	<p>www.disrupt6.com sales@disrupt6.com</p>
 <p>Europalab Networks</p> <p><i>"Network, Software, and Hardware engineering for telco and industry"</i></p> <p>Michael Schloh von Bennewitz</p>	<p><i>Consulting</i></p> <ul style="list-style-type: none"> IPv6 planning and testing IPv6 design and deployment <p><i>Services</i></p> <ul style="list-style-type: none"> IPv(4 6) dual stack migration IPv6 penetration testing 	<p>North America, Europe, Asia, five languages spoken</p>	<p>dev.europalab.com ipvsix@europalab.com</p>
<p>Florian Consulting Inc.</p>	<ul style="list-style-type: none"> IPv6 Consulting, Design and Deployment 	<p>Calgary, AB, Canada</p>	<p>www.florian.ca info@florian.ca</p>
 <p>HexaBuild, Inc.</p>	<ul style="list-style-type: none"> IPv6 Consulting, Design and Deployment IPv6 Address Planning IPv6 Allocation Requests IPv6 Training and IT Support Integration IPv6 Security Auditing Hardware and Software IPv6 Support Auditing Cloud Architecture and Practice On-site and remote IPv6 Training options with full labs Skilled IPv6 trainers - all materials created by published IPv6 authors who are international IPv6 speakers and experts in IPv6 	<p>International</p>	<p>https://hexabuild.io info@hexabuild.io</p>

Hoyos Consulting LLC	<ul style="list-style-type: none"> IPv6 Consulting, Design and Deployment 	USA & International	www.hoyosconsulting.com info@hoyosconsulting.com
	<ul style="list-style-type: none"> IPv6 Consulting, Design and Deployment Planning, training, using IPv6 IPv6 - Security audit, Penetration testing IPv6 Email, DNS, and Network Deployment Secure IPv6 broadband and enterprise networks 	Sweden	https://secureenduserconnection.se/ https://dnssecandipv6.se/ https://www.interlan.se/ info@interlan.se
InterServer	<ul style="list-style-type: none"> IPv6 Cloud Hosting 	NJ, USA	www.interserver.net support@interserver.net
IPv6 Now	<ul style="list-style-type: none"> Planning, training, using IPv6 - basic to advanced IPv6 Forum Gold Certified training and courses Australian and Asian specialist focus 	Australia, Asia, international	6now.net services@6now.net
DeLong Consulting Owen DeLong	<ul style="list-style-type: none"> IPv6 Training IPv6 Forum Gold Certified Instructor We bring the training lab to you 	SF Bay Area World (with T&E)	owen@delong.com
Jacob D Evans, Consulting	<ul style="list-style-type: none"> IPv6 Email, DNS, and Network Deployment IPv6 Consulting for Private Datacenter IPv6 Consulting for Hosting Providers and Internet Service Providers. 	PA, USA	www.jacobdevans.com linkedin.jacobdevans.com ipv6@jacobdevans.com
Megawire Inc	<ul style="list-style-type: none"> IPv6 Network Deployment 	Ontario, Canada	ipv6@megawire.ca
	<ul style="list-style-type: none"> IPv6 Fundamentals Hands-On Workshop (2 days) IPv6 Advanced Topics Hands-On Workshop (2 days) 	Worldwide	https://www.menandmice.com/support-training/training/ info@menandmice.training
	<ul style="list-style-type: none"> IPv6 - Engineering, Consulting IPv6 - Planning, Design, Implementation IPv6 - Security auditing, Penetration testing 	USA	www.ncom.com ipv6@ncom.com
Network Utility Force	<ul style="list-style-type: none"> IPv6 Forum Certified Training IPv6 Architecture, Planning, Design, Deployment and Consulting IPv6 Security 	Global	http://www.netuf.net/p/ipv6.html ipv6@netuf.net

<p>NODO 6</p> 	<ul style="list-style-type: none"> • IPv6 Consulting • IPv6 Transition Project Management • IPv6 Forum Training, Courses & Certifications: <ul style="list-style-type: none"> • Network Engineer (Silver) • Network Engineer (Gold) • Security Engineer (Gold) • Trainer (Gold) 	<p>Worldwide</p>	<p>www.nodo6.com info@nodo6.com</p>
<p>Teach Me IPv6 Jeff Carrell</p>	<ul style="list-style-type: none"> ▪ IPv6 Forum Certified Training ▪ IPv6 Consulting, Design and Deployment 	<p>US & International</p>	<p>www.teachmeipv6.com jeff.carrell@teachmeipv6.com</p>
<p>TeKnowledgey, Inc.</p>	<ul style="list-style-type: none"> ▪ IPv6 Design, Deployment, and Management 	<p>UT, USA</p>	<p>www.tknow.com sales@tknow.com</p>
<p>Auspex Technologies</p>	<ul style="list-style-type: none"> • IPv6 Consulting, Design, Deployment, Management, Training, and Security 	<p>USA & International</p>	<p>www.auspextech.com dgeesey@auspextech.com</p>
<p>S.J.M. Steffann</p>	<ul style="list-style-type: none"> • IPv6 Consulting (Strategic, Planning, Architecture, Security, Design, Labs, Deployment) • IPv6 Training (Beginner, Advanced, Custom, Hands-on) 	<p>EU & International</p>	<p>www.steffann.nl sander@steffann.nl</p>
<p>Sunny Connection AG</p> 	<ul style="list-style-type: none"> • IPv6 Consulting (Strategy, Planning, Architecture, Labs) • IPv6 Training <ul style="list-style-type: none"> • IPv6 Essentials Workshops for Architects, Engineers and Developers • IPv6 Planning Workshops for Decision Makers 	<p>Based in Switzerland All services offered internationally</p>	<p>www.sunny.ch silvia.hagen@sunny.ch</p>
<p>Tim Martin</p>	<ul style="list-style-type: none"> • IPv6 Enterprise Design, Planning, Consulting • Cisco training for organizations with an active IPv6 plan 	<p>US Public Sector</p>	<p>www.cisco.com/ipv6 tmartin@cisco.com</p>
<p>runningdownstream consulting, LLC</p>	<ul style="list-style-type: none"> • IPv6 strategy, readiness assessment, roadmap development • Business case development • Training 	<p>USA - mid-large scale enterprise deployment</p>	<p>ebrierley@att.net</p>

	<ul style="list-style-type: none"> • Hands-on IPv6 Hacking Training Courses • Hands-on IPv6 Deployment Training Courses • IPv6 consulting 	International	www.si6networks.com/education/ipv6/ www.si6networks.com fgont@si6networks.com
	<ul style="list-style-type: none"> • IPv6 Network Design, Planning and Consulting for Enterprise, Service Providers and Data Centers • IPv6 Training 	Norway / Northern Europe	www.nlogic.no post@nlogic.no
	<ul style="list-style-type: none"> • IPv6 Consulting (Strategy, Planning, Architecture, Design, Deployment) • IPv6 Certified Training <ul style="list-style-type: none"> • IPv6 Foundations (Instructor led, lab based, on site or remote) • IPv6 eLearning (Learn IPv6 or prepare for IPv6 Certification) • IPv6 Forum Certification • Tools for measuring, assessing and troubleshooting IPv6 services. Make the transition deterministic! 	US & International	www.nephos6.com www.v6sonar.com contact@nephos6.com
	<ul style="list-style-type: none"> • Service-provider IPv6 Consulting, Design and Deployment with an emphasis on Juniper Networks 	US & International	www.aptient.com ipv6@aptient.com
Portlandia Cloud Services 	<ul style="list-style-type: none"> • IPv6 webhosting, Consulting, Cisco Systems expertise, Linux & Windows server management 	Portland, OR	www.portlandiacloudservices.com

The IPv6 consultants and trainers listed above have represented that they provide IPv6 services and wish to be included on this list. ARIN neither endorses nor guarantees the services provided by these organizations. ARIN makes no representation as to the quality or suitability of services offered. ARIN is not responsible nor is it liable for any content, data, products, goods or services provided by or through these organizations. We suggest that you undertake a reasonable amount of due diligence and research into any potential provider that you deem necessary or appropriate before engaging any such provider. If you seek additional information regarding any entity on this list, we invite you to please contact them directly.

A Wireshark IPv6 Configuration Profile

For those of you who love Wireshark and are supporting IPv6, we would like to offer a great default profile for IPv6. Consider for a moment what would be important in your network administration in IPv6:

- Certainly anything having to do with ICMPv6
- Being able to find packets with certain extension headers
- Being able to detect tunneled packets
- Being able to note packets with certain IPv6 Addresses

All this would be a great starting point, and you would want to great colorization of things like neighbor discovery, ICMPv6 errors, etc.

Click here: <https://www.cellstream.com/reference-reading/tipsandtricks/280-a-wireshark-ipv6-profile>

IPv6 Training and Consulting Services

Thanks to the publication of a study by the NRO (Number Resource Organization) that is the official representative of the five RIRs (Regional Internet Registries) that oversee the allocation of all Internet number resources, we learned the following:

- Over 50% of respondents note that the cost of deployment of IPv6 is a major barrier to adoption and deployment.
- Over 45% of respondents report inability to find IPv6 knowledgeable technical staff to support deployment.

The survey polled over 1,500 organizations from 140 countries.

It is time to bring yourself and your staff up to speed on IPv6.

Supporting IPv6 begins with understanding IPv6.

CellStream has been supporting IPv6 for many years and with the 2 Day [Hands On IPv6 standard course](#), or the 2 Day [Ethernet and IPv6 course](#), or the more detailed 3 Day [Hands on IPv6 course](#), you can begin to build the knowledge base within your technical staff. Hands on training is the best training as students not only understand, but they "do". In the class, we take an IPv4 network and build an IPv6 network - from scratch, and then we learn how the various migration options can be used to support both IPv4 and IPv6 in the near future.

We also offer our [Advanced IPv6 course](#) that covers IPv6 over MPLS, and other subjects.

Visit our Online School of Network Sciences at <http://netscionline.com/>! Creating a user there is free. And there are so many free resources you can leverage once your user is created: <https://netscionline.com/course/index.php?categoryid=21>.

We look forward to helping.

IPv6 Hosting and DNS Providers

Ready to make your website available over IPv6 and looking for a hosting and DNS provider that supports IPv6? Let us help. Below is a growing list of providers who have represented that they offer IPv6 services. If you represent a hosting or DNS provider that offers IPv6 services and would like to be included on this list, please [request a GetIPv6.info wiki account](#) and add your entry to the list in alphabetical order.

Company Name	Reported IPv6 Services	Service Area	Public contact email
1uHost	<ul style="list-style-type: none">• IPv6 Hosting• IPv6 DNS• AAAA records	Low Cost Web Hosting, Domain Name Registration, VPS, WebMail, and SHOUTcast Radio	support@1uhost.com
American Data Technology, Inc. (ADTI)	<ul style="list-style-type: none">• IPv6 Hosting (native)• IPv6 DNS• AAAA records	Web Hosting, Cloud Hosting, Dedicated and Managed Hosting, VPS, IaaS/PaaS, Web Hosting, Email Hosting, DNS, Colocation Services	IPv6@localweb.com
ARP Networks, Inc.	<ul style="list-style-type: none">• IPv6 Hosting (native)• IPv6 DNS• AAAA records• IPv6 Transit	VPS, Dedicated Servers, Colocation, IP Transit	sales@arpnetworks.com
Atlantech Online, Inc.	<ul style="list-style-type: none">• IPv6 Hosting (native)• IPv6 DNS• AAAA records• IPv6 Transit	Washington, DC Metro Region	sales@atlantech.net
Broadband Networks	<ul style="list-style-type: none">• IPv6 Hosting (native)• IPv6 DNS• AAAA records	Hosting	hosting@broadbandnetworks.com
Castlegem Inc	<ul style="list-style-type: none">• IPv6 Hosting (native)• IPv6 DNS• AAAA records• IPv6 Transit	Internet Service Provider (VPS, Dedicated, Colocation, IaaS) in New York City	office@castlegem.com

Get6!

In order to keep the Internet growing, organizations must "Get6" now to ensure their future success in a changing web environment. Find out how to make the case for the transition to IPv6 at the [TeamARIN.net website!](#)

Cloudflare, inc.	<ul style="list-style-type: none"> • IPv6 CDN • IPv6 DDoS mitigation on • IPv6 DNS 	Global. (for DDoS mitigation, DNS, and Content Delivery Network - CDN)	sales@cloudflare.com +1 (650) 319 8930
ColoGuard Enterprise Solutions	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 Transit 	New York	andy@cologuard.com
Comlink, LLC	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 DNS • AAAA records • IPv6 Transit 	Midwest: Michigan, Ohio, Indiana, Illinois, Wisconsin	sales@comlink.net
DataChambers	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 DNS • AAAA records • IPv6 Transit 	North Carolina, South Carolina	info@datachambers.com
Dyn, Inc.	<ul style="list-style-type: none"> • IPv6 DNS • AAAA records 	Global	info@dyn.com
EAS Enterprises LLC	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 DNS • AAAA records 	US	ipv6sales@easent.net
Energy Group Networks	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 Transit 	Dedicated Servers, Colocation, Transit	sales@egihosting.com
FiberPeer Networks	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 Hosting (tunneled) • IPv6 DNS • AAAA records • IPv6 Transit 	Everywhere	sales@fiberpeer.com
FullHost	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 DNS • AAAA records 	Canada (Vancouver, BC and Toronto, ON data centers)	sales@fullhost.com
GlowHost	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 DNS • AAAA records 	Worldwide	hosting.sales@glowhost.com
GT.net	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 Transit 	Managed Hosting, Private Cloud, IaaS	info@gt.net
Handy Networks, LLC	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 DNS • AAAA records • IPv6 Transit 	Denver Metro	sales@handynetworks.com
Host TugaTech 	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 DNS • AAAA records 	Europe (Portugal, Germany, France, UK)	host@tugatech.com.pt
Hurricane Electric	<ul style="list-style-type: none"> • IPv6 Transit (native) • IPv6 Tunnelbroker • IPv6 DNS • AAAA records 	Global Backbone Network, Dual Stack IP Transit, Colocation, Dedicated Servers, Managed Servers Free DNS, Free IPv6 Tunnelbroker, Free IPv6 Certification	sales@he.net
Inertia Networks, LLC	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 DNS • AAAA records 	cPanel Hosting, VPS Hosting (Located in Los Angeles, CA)	sales@inertianetworks.com

INIZ	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 DNS • AAAA records 	Worldwide	sales@iniz.com
	<ul style="list-style-type: none"> • IPv6 VSP hosting • IPv6 DNS • IPv6 mail services 	Sweden but serving the globe DNS slave service located in Sweden (three places), London and Amsterdam Native IPv6 since 2007	info@interlan.se
Kevin McCarthy	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 Hosting (tunneled) • IPv6 DNS • AAAA records 	Worldwide	support@dlhost.com
Lanset America Corp. DBA Hostik	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 DNS • AAAA records 	Located in Sacramento California serving the globe	sales@hostik.com
Media-Hosts Inc.	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 DNS • AAAA records • IPv6 Transit 	Hosting, Dedicated Servers, Virtual Serves, Colocation, IP Transit	sales@media-hosts.com
MetroInternet	<ul style="list-style-type: none"> • IPv6 DNS • AAAA records • IPv6 Transit 	Quebec and Ontario	info@metrointernet.ca
Mythic Beasts Ltd	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 DNS • AAAA records • IPv6 Transit 	UK	sales@mythic-beasts.com
NETRIPLEX GLOBAL DNS	<ul style="list-style-type: none"> • IPv6 DNS • AAAA records 	Worldwide	sales@netriplex.com
Netsolus.com Inc.	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 Hosting (tunneled) • IPv6 DNS • AAAA records • IPv6 Transit 	Worldwide	info@netsolus.com
NetSource Communications, Inc.	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 DNS • AAAA records 	Data Center Hosting	sales@netsource.com
NetToGo, Inc.	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 DNS • AAAA records 	Managed Colocation, Private Cloud & Data Center Hosting Miami, FL USA	rmedina@nettogo.net
New Continuum Data Centers	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 Transit 	Colocation & Data Center Hosting (1U-42U)	tom@continuumdatacenters.com
Packet Host, Inc.	<ul style="list-style-type: none"> • IPv6 Hosting (bare metal servers) • IPv6 Transit 	Bare metal hosting & IP transit in: New York Metro Amsterdam, NL San Jose, CA Tokyo, JP	help@packet.net
Query Foundry	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 Transit 		sales@queryfoundry.com

Roller Network	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 DNS • AAAA records • IPv6 Transit 	Worldwide (Colocation, DNS); Reno/Sparks, Northern Nevada (Transit)	sales@rollernet.us
ServedBy The Net	<ul style="list-style-type: none"> • IPv6 Hosting (native) • AAAA records • IPv6 Transit 	USA	info@servedby.net
Sheldon Networks, Inc. DBA: ACT USA	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 DNS • AAAA records 	United States of America	sales@actusa.net
Stealthy Hosting	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 Transit 	Seattle, WA	Sales@StealthyHosting.com
Total Uptime Technologies	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 Hosting (tunneled) • IPv6 DNS • AAAA records • IPv6 Transit 	Global	sales@totaluptime.com
Vivid-Hosting	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 Hosting (tunneled) • IPv6 DNS • AAAA records • IPv6 Transit 	Los Angeles	kchau@vivid-hosting.net
WebTuga 	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 DNS • AAAA records 	Europe (Portugal)	info@webtuga.pt
Yellowknife Wireless Company LLC	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 DNS • AAAA records • IPv6 Transit 	Oregon (Deschutes, Crook, Jefferson, North Klamath Counties)	info@ykw.com
Zenith Media Canada 	<ul style="list-style-type: none"> • IPv6 Hosting (native) • IPv6 DNS (native) • AAAA Records 	Canada (Montreal, Quebec) Europe (Strasbourg, France) United States (Virginia)	info@zenithmedia.ca 1-855-ZENITH-0

The hosting and DNS providers above have represented that they provide IPv6 services and wish to be included on this list. ARIN does not endorse or guarantee the services provided by these organizations, nor make a representation as to the quality or suitability of services offered. We suggest that you undertake a reasonable amount of due diligence and research into any potential provider. If you seek additional information regarding any entity on this list, we invite you to please contact them directly.