

An ATIS Whitepaper on Information & Communication Technologies (ICT) and IPv6 Readiness

January 2011
Release 1.0

The Study of IPv6 Readiness

Those parties involved in the Information and Communication Technologies (ICT) industry are acutely aware of the media attention focused on the impending depletion of IPv4 addresses; in fact, the need for transition to IPv6 is almost a daily media story. Fueling these stories are announcements from organizations such as the Number Resources Organization (NRO) and the American Registry for Internet Numbers (ARIN) warning all Internet stakeholders to take *immediate action* and begin necessary preparations to deploy IPv6.¹

IPv6 advocates have been waving “yellow flags” for years with respect to the imminent depletion of IPv4 addresses and the dire need to enable IPv6. With 2 percent of IPv4 addresses unallocated by Internet Assigned Numbers Authority (IANA), as of December 2010, a sense of urgency has finally taken root. Current predications state that the IANA free pool of IPv4 addresses may be depleted by the end of January 2011.² When that happens, the level of uncertainty will rise significantly. The next milestone for IPv4 address exhaust is the depletion of the inventory held by the five individual Regional Internet Registries (RIRs) to include the ARIN. Without a timely and orderly transition to IPv6, the Internet is likely to become fragmented with domains of IPv4 only endpoints, domains of IPv6-enabled endpoints and multiple layers of network address translation and tunneling to stitch them together. In sum, the growth and deployment of new services will become increasingly more complex.

On an upside, the “yellow-flag strategy” has been successful in preparing parties for the impending depletion of IPv4 addresses. Significant attention is now being given to the topic and most new hardware and software supports IPv6. To examine the current IPv4/v6 landscape based on all these activities, senior executives from ICT companies, as represented by the ATIS Board of Directors, tasked ATIS and its IPv6 Task Force (IPv6TF) to reassess IPv6 readiness. This paper represents the ATIS IPv6TF’s assessment of the IPv4/v6 landscape, industry’s preparedness for the depletion of IPv4 addresses and subsequent readiness for IPv6. This assessment is intended for ATIS member companies, but may also be of interest to the broader ICT community.

State of IPv6 Readiness

Since the ATIS IPv6TF last reviewed IPv6 in 2008, industry standards supporting transition technologies have undergone significant advancement due to new industry and technical developments. In 2006, it was anticipated that most organizations would likely deploy a “dual-stack” (i.e., running simultaneous IPv4 and IPv6 networks) approach to the transition to IPv6. Today, most North American service providers have a plan for supporting IPv6. These plans include supporting dual-stack, tunneling (e.g., 6rd, DS-lite), and NAT64 protocol translation. Regardless of the approach, many service providers and large enterprises (e.g., US Federal Government) are well down the path of implementing their IPv6 transition strategies. Network and consumer electronics equipment vendors, which have been expanding their IPv6-enabled equipment portfolio for a number of years, are actively working with their partners to advance their IPv6 offerings. In some cases, service providers have started field trials of IPv6 with consumer premises

¹ Number Recourse Organization (NRO), Media Center, Remaining IPv4 Address Space Drops Below 5%, 18 Nov. 2010, <http://www.nro.net/media/remaining-ipv4-address-below-5.html>

² IPv6 Forum, IPv4 Exhaustion Counter, Web, December 2010, < <http://www.ipv6forum.com/>>

equipment (CPE), mobile handsets, and edge gateway routers upgraded to support IPv6. These field trials are intended to validate IPv6 transition plans for consumer and enterprise services, and are a key step toward enabling IPv6 in core networks, on edge routers and on CPE.

The transition to IPv6 is complex and the process will differ for organizations in different industries. For small companies whose main concern is serving internal users and customers, deploying dual-stack will suffice into the foreseeable future provided IPv4 addresses can be allocated for growth. Service providers, content providers, large enterprises and government entities have a much bigger task. While most of these organizations have been dealing with the IPv6 transition for some time now, there remain complex interoperability and security issues associated with the transition.

With the uptick in publications noting the actions of larger service providers' and enterprises' transition to IPv6, bordering organizations are beginning to heed the importance of IPv6 in their own business and network planning strategy and are consequently accelerating their implementation and deployment of IPv6 capabilities. By way of example, the impact of the Federal Government's recent mandate that all consumer-facing Federal websites must be IPv6 compliant by September 2012³ has caused a ground-swell of activity around IPv6 throughout the entire federal supply-chain.

Also contributing to the need to quickly advance the deployment and availability of an IPv6-enabled infrastructure is the exponential growth of wireless service offerings and the proliferation of IP-based wireless data systems such as ubiquitous sensor networks and evolving wireless services and applications to support next generation smart-devices and technologies (e.g., smart-meters, smart-appliances, and smart-buildings). A gating issue to fully realizing the "Internet of Things" is the enablement of native IPv6, as there are not enough IPv4 resources available to bring these innovative services online. IPv6 must be readily available to ensure real-world objects and sensors are an integral, operational part of the Internet. The output from objects and sensors becomes more valuable the more networked they are, making it possible to know information or interact and influence objects, electrical systems, people, from any location. Machine-to-Machine (M2M) –which refers to machine-to-machine communications (i.e., automated data exchange between machines) – is a large contributor to causing an entire "Internet of Things", or Internet of intelligent objects, to emerge.⁴

While momentum builds to enable IPv6, there is no uniform approach or Internet-wide mandated timeframe to complete the task. Each company will transition to IPv6 at its own pace thereby creating varying levels of IPv6 capabilities and readiness. Where companies are in their transition or strategy depends on a number of factors. In some cases, companies continue to struggle with identifying the financial value-add for transitioning to IPv6; looking at IPv6 from a purely return on investment (ROI) perspective and less on ensuring business continuity or growth. Assisting these organizations to better grasp the impact of IPv4 address depletion on the continued growth of their Internet traffic is of paramount importance to enabling a true IPv6 Internet.

Other areas needing attention with respect to their transition to or availability of IPv6 are in the operations support systems (OSS) and application space. Publicly available information reports that operating systems such as Windows 7, XP, Vista, OS X, Unix, and Linux are IPv6-ready or enabled. By comparison to other necessary IPv6 functions, the readiness of applications to support IPv6 is less known.

³ Vivek Kundra, Federal Chief Information Officer, Executive Office of the President, MEMORANDUM FOR CHIEF INFORMATION OFFICERS OF EXECUTIVE DEPARTMENTS AND AGENCIES, <
<http://www.cio.gov/Documents/IPv6MemoFINAL.pdf>>

⁴ M2M.com, White Papers, m2m alliance, Implementing M2M applications via GPRS, EDGE and UMTS, Website, 16 Nov. 2010, <http://m2m.com/community/resources/white_papers_and_reports>

Information on IPv6 transition tools, strategies, challenges and best practices is readily available on the Internet for parties seeking guidance. The IPv6 Forum⁵ maintains a testing tool for IPv6 compliant websites. The U.S. Federal Government also maintains a number of useful documents and materials which includes test plans, certification procedures and listing of certified/approved IPv6 product and services.⁶

Industry-accepted specifications and standards from organizations such as the IETF are readily available or under development to enable the transition to IPv6 with a great amount of work done on mechanisms for the transition from IPv4 to IPv6. While dual-stack continues to be a recommended path for the transition, it is recognized that not all parts of the network (including customer premise equipment (CPE)) will move to IPv6 support at the same rate. Therefore, transition techniques will continue to be supported to allow for different parts of the network to transition at different times. In addition, it is understood that not all web content will move to IPv6 at the same rate.

Several types of tunneling mechanisms and NATs have been proposed to enable different transition strategies. Much of this work is occurring in the Behavior Engineering for Hindrance Avoidance (behave)⁷ and Softwires (software)⁸ working groups in IETF. Recently, the IETF's IPv6 Operations (v6ops) Working Group⁹ has taken up the discussion of transition scenarios and strategies for service providers.

As efforts continue to enable IPv6 capabilities, parties are being increasingly aware that current estimates for the RIRs to run out of unallocated IPv4 address space is January 2012. Since each RIR community has different consumption rates, depletion of each RIR's free pool will occur at different times. Based on rate of consumption, it appears APNIC will be the first RIR to run out of unallocated IPv4 addresses.¹⁰ Within a RIR, depletion will occur first for the largest carriers and enterprises when the RIR is unable to fulfill a request for a large allocation. RIR's will be able to meet the needs of smaller and medium sized organizations for a longer period. Service providers will continue to be able to allocate IPv4 addresses to customers out of their unallocated pool as long as it lasts. Being able to allocate IPv4 address space post depletion will likely become a competitive advantage. Organizations may find incentive to restructure existing assignments and better utilize existing IPv4 resources.

Under current RIR policies, organizations are supposed to return unneeded IPv4 address space to the RIR for reallocation. The rate of voluntary return of IPv4 address space to RIR's is low. An aspect of the run-out of IPv4 address space that has been researched for the last few years is the creation of a market for IPv4 addresses where an organization that needs IPv4 address space provides financial incentive to an organization to renumber out of under-utilized space. The RIRs are evaluating policies to deal with this situation and in some cases, facilitate it. The possibility exists for a stronger black market for address space to develop, especially for address space not under control of a RIR. Black market trading of address space is debilitating to stability of networks and internet security. Service providers can play an important role in preventing the black market trading of address space by refusing to route address space traded on the black market, thus making such space unusable. Processes for verifying the proper users of address space are still under investigation.

⁵ IPv6 Forum, IPv6 Ready Program Logo, Web, November 2010, < <http://www.ipv6ready.org/>>

⁶ See "Additional Resources" section

⁷ IETF, datatracker.ietf.org, Behavior Engineering for Hindrance Avoidance (behave), Description of Working Group, web, 1 January 2011, < <http://datatracker.ietf.org/wg/behave/charter/>>

⁸ IETF, datatracker.ietf.org, Softwires (software), Description of Working Group, web, 1 January 2011, <<http://datatracker.ietf.org/wg/software/charter/>>

⁹ IETF, datatracker.ietf.org, IPv6 Operations (v6ops), Description of Working Group, web, 1 January 2011, <<http://datatracker.ietf.org/wg/v6ops/charter/>>

¹⁰ An analysis of the run-out of IPv4 addresses can be found in Geoff Huston's "IPv4 Address Report" at <http://ipv4.potaroo.net/>

The Internet community has been working to develop policy within the RIR's to manage the depletion of IPv4 addresses and transition to IPv6. These policies include methods for managing the allocation of the last few address blocks and how to manage returned address space. Samples of the policies the RIRs have developed are included in the appendix of this paper.

The Need to Drive Broader Adoption and Transition to IPv6

For the past several years ATIS and its member organizations have worked to elevate awareness of the development and deployment of IPv6. Today, as IANA IPv4 address depletion is nearing, companies need to renew their sense of urgency and inspire the entire Internet community to quickly deploy IPv6 for all public Internet services. Many ATIS members are leading the transition to IPv6, but the widespread adoption of IPv6 is still far from being complete and this poses a near term risk to the health of the Internet and businesses that operate on the Internet. Leading Internet companies join ARIN in urging the quick and orderly deployment of IPv6 services, especially for publicly addressed services like web content and email services.

IPv6-only deployments will be the *de facto* for high-growth markets like machine-to-machine (SmartGrid, e-Readers, etc.) communications as well as increasingly rich and complicated consumer any-to-any multimedia services such as mobile two-way or n-way video calling. Based on this growth, it is anticipated that U.S. mobile/wireless market break through the 100% barrier in 2013 to hit 105% by the end-2013.¹¹ Without a timely and orderly transition to IPv6, services might be degraded as traffic will have to traverse multiple layers of NATs, protocol translators and tunnels for endpoints to communicate with each other.

Organizations are committed to deploying IPv6 services as the strategically correct choice for enabling long-term service delivery. In the near to mid-term, Internet services must be available as dual-stack IPv4 and IPv6 since the IPv6-only networks will begin to be deployed to consumers in 2011. The IETF softwire and behave working groups have created *DS-Lite* and *NAT64* technologies to deal with IPv6-only endpoints communicating with IPv4-only Internet content and vice versa.

These technologies have strong support from service providers and carriers as a bridge between a growing user base and the long-tail of Internet content; but these technologies cannot sustain the pace of innovation on the Internet. Only IPv6 end-to-end connectivity can be the long term solution to ensure content, services, and users can continue to connect seamlessly and take the Internet to the next level of communication innovation.

Challenges in Transitioning to IPv6

It has long been understood that transitioning to IPv6 would present a host of challenges. In 2007, ATIS released its second IPv6 related report entitled "*ATIS Internet Protocol version 6 (IPv6) Task Force Report on IPv6 Transition Challenges, July 2007*", wherein a number of challenges were identified including: the need to ensure Quality of Service (QoS); network security; interoperability between IPv4 and IPv6 native networks; Network Address Translators (NATs); and the potential impacts on network traffic and routing. While many of the challenges identified back in 2007 have been resolved over time, others remain and new ones have appeared.

¹¹ Intelligence Centre Channels, 4G, Mobile Broadband and Emerging Devices Key at CTIA Wireless 2010, <http://www.intelligencecentre.net/2010/03/26/4g-mobile-broadband-and-emerging-devices-key-at-ctia-wireless-2010/>

Notwithstanding the numerous challenges with IPv6, a key area where people need to focus their attention is to understand IPv6. That is, to study the business impact of the depletion of IPv4 addresses and the transition to IPv6; to carefully evaluate existing infrastructure to assess its readiness for the new protocol; and to create high-quality transition plans. The task of transitioning to IPv6 is far from easy and the learning curve is huge. Organizations may be overly cautious because of the possibility of unintended consequences. It is complicated and there is a fear factor for IT staffs.

After almost three years since ATIS' report, the need for organizations to make key internal business decisions with respect to IPv6 continues to be a gating factor to their transition. More precisely, while IPv6 is unquestionably important to the industry, its wide-scale advancement continues to be preempted by more pressing operational priorities. Announcements from organizations such as the NRO with respect to the depletion of IPv4 address and publications noting the IPv6 deployment by larger organizations, however, have started to accelerate the transition to IPv6.

Other pressing challenges (aside from the constant concern with capital expenses associated with transitioning) include: the possible deployment of "large scale carrier NATs"; the large number of NATs deployed in residential gateways which are not IPv6-capable; the lack of broad consumer or user demands; and overall IPv4-to-IPv6 interworking. It is widely understood that during the transition to IPv6 different networks will be at different phases of migration. In addition, different applications and services will be at different stages of migration. As such, multiple scenarios have to be considered for interconnection and interworking between IPv4-only applications, IPv6-only applications, IPv4 networks and IPv6 networks. The ability of IPv6-only networks to interconnect with legacy IPv4 networks will likely remain a concern in the foreseeable future.

Another challenge facing businesses shifting over to IPv6 is ensuring that all their back-office equipment and applications are IPv6 capable. This is especially important if a company relies on "home-grown" ordering systems to track their orders. In this case, companies will need to redesign their back-office systems to make sure they can send and receive IPv6 traffic. These scenarios lead some people to believe they have to completely "forklift-upgrade" their entire infrastructure in order to handle the new protocol. In reality, there may be certain segments that don't need native IPv6 support immediately and can be supported by tunneling over an IPv6 infrastructure. These considerations must be part of careful transition planning.

Businesses must also make sure that special-purpose appliances used in the network (e.g., Firewalls, Intrusion Detection Systems, Load-balancers) support IPv6 and are configured correctly for IPv6 support. Some policies might need to be revised to support IPv6, e.g., Firewalls must pass ICMPv6 "packet too big" packets in order for IPv6 Path MTU discovery to work.

When considering whether or not to use tunneling technologies, issues like delay, troubleshooting and MTU sizing should be taken into account.

IPv6 Implementation and Deployment Challenges

As ICT companies continue down the path of preparing for the depletion of IPv4 addresses and implementing transition strategies or deploying IPv6 capabilities, a few deployment challenges to note include: interoperability across vendors; interworking between IP versions; Domain Name Server (DNS) strategies; network support and troubleshooting; and impacts to network services and applications.

As efforts continue to implement and deploy IPv6, ensuring interoperability of CPE and infrastructure equipment across vendors will be a challenge as it relates to key technologies like the 6rd and NAT64. A

good example is ensuring that 6rd can be deployed to Residential Gateways (RGs) and other customer premise devices. At present, the necessary standards to support these individual solutions (e.g., 6rd, NAT64) appear to be in place. Enabling interoperability in a multiple vendor environment becomes more about the interpretation of standards and ensuring consistent implementation across devices. To that end, identifying and or establishing a venue for IPv6 interoperability testing can help to minimize many of these types of technical and operations challenges companies will certainly face in their of deployment of IPv6.

As work continues on enabling IPv4 and IPv6 internetworking, ensuring that hardware and software developers optimize their devices to minimize disruption at the v4/v6 hand-off point will also be important. Some technologies -- like VoIP, may have to use Application Layer Gateways (ALG) to assist in the hand-off; however, there are draft IETF specifications warning of possible side effects of the use of ALG and recommend turning off ALG in certain scenarios.¹²

In maintaining a dual-stack deployment strategy, companies should prepare for and be ready to resolve potentially conflicting IPv4 and IPv6 routing and address records. For example, DNS might return a AAAA record containing an IPv6 address for a destination, but there might not be an IPv6 route to that destination. Defining a strategy to minimize this and similar problems associated with Domain Name System (DNS) A versus AAAA (or quad-A) records should be part of the deployment discussion. A possible approach may be to take steps to optimize DNS configurations and “lookup” queries. As an illustration, some new Operating Systems (OS’), as well as some networks, will first do an AAAA lookup for IPv6 and then will only do the IPv4 A lookup if the AAAA failed while others will perform the A and AAAA DNS lookups in parallel and then use the first one returned. The IETF v6ops working group is considering strategies and recommendations on how best to manage this situation.

Finally, but by no means of less importance, impact assessments when deploying IPv6 must be performed on core service provider services (i.e., IPTV, VoIP, other IP-related services) and applications . Today, there is minimal information available on preparedness of applications for IPv6. There has been some dialogue on how to design transition-friendly applications, e.g., use of fully qualified domain names (FQDN), removal of IPv4 literals, and adjustment of field sizes when IP capture and storage is needed, but there isn’t much information in terms of best practices. Best Practices would describe at a high level application guidelines (e.g., RFC 3235-NAT friendly application guidelines). One proposal under consideration in the IETF is entitled “*Happy Eyeballs: Trending Towards Success with Dual-Stack Hosts, draft-wing-v6ops-happy-eyeballs-ipv6-01*” (work in progress). This document provides a mechanism for applications to use in order to determine the most optimal connection (IPv6 or IPv4) to a server.¹³

IPv6 Readiness Summary

As efforts continue in and across companies, based on the information provided, examined and discussed, indicators show that the ICT industry, as represented in ATIS, is taking appropriate measures to be ready for IPv4 depletion. It is widely accepted that the advent and deployment of 4G mobile devices will increase the need to switch over to IPv6, since each of those devices will require its own IP address. Consequently, if any company wants to push its content out to mobile devices over the next few years, they are going to need some capability to handle IPv6 traffic. It is also recognized that necessary standards

¹² “Common requirements for IP address sharing schemes”, draft-nishitani-cgn-05, <<http://tools.ietf.org/html/draft-nishitani-cgn-05>>

¹³ IETF Tools, IETF Documents, Web, November 2010, < <http://tools.ietf.org/html/draft-wing-v6ops-happy-eyeballs-ipv6-01>>

and specifications are readily available or under development to support a number of different transition technologies and strategies to IPv6.

Service providers also need to continue with efforts to educate their clients and consumers on the advantages of transitioning to IPv6. A key advantage to note is the enablement of innovative applications, which can leverage the demand for global public IP addresses by potentially billions of devices to advance for example the "Internet of things." Improvements in business process, optimized outsourcing efficiency, and continued globalization are additional benefits which leverage IPv6-based integrated information processing systems, embedded automation capabilities, and collaborative tools such as immersive multimedia services.

A number of ATIS' member companies provide their view of IPv6 through publically available statements or position papers. Readers of this paper may find this additional material of interest. References to access this material as well as other information are available in the following appendix "IPv6 Resources."

Companies/Parties Contributing to this Whitepaper: AT&T, Alcatel-Lucent, Cisco Systems, Qwest Communications, Telcordia Technologies, T-Mobile USA, US Cellular, and Verizon Communications.

IPv6 Resources & References

ATIS IPv6 Reports (<http://www.atis.org>)

- “ATIS Internet Protocol version 6 (IPv6): Report & Recommendation, May 2006”
- “ATIS Internet Protocol version 6 (IPv6) Task Force Report on IPv6 Transition Challenges, July 2007”
- “ATIS Readiness Plan for IPv6 Transition, June 2008”

Company Position Papers on IPv6

- AT&T, *AT&T Position on IPv6*, http://www.business.att.com/content/whitepaper/WP-IPv6_18359_v1_5-11-09.pdf
- Verizon, *Benefits for IPv6 Enterprises*, http://www.verizonbusiness.com/resources/whitepapers/wp_benefits-of-ipv6-for-enterprises%20_en_xg.pdf
- Cisco, <http://www.cisco.com/ipv6>

U.S. Federal Mandates & Public Law

- *Office of Management and Budget, M-05-22*:
- By June 2008 “All agency infrastructures (network backbones) must be using IPv6 and agency networks must interface with this infrastructure” “ensure that all new IT procurements are IPv6 compliant. Any exceptions to the use of IPv6 require the agency's CIO to give advance, written approval.” <http://www.whitehouse.gov/omb/memoranda/fy2005/m05-22.pdf>
- *Public Law 109-163, SEC 221* requires “A certification by the Chairman of the Joint Chiefs of Staff that the conversion of Department of Defense networks to Internet Protocol version 6 will provide equivalent or better performance and capabilities than that which would be provided by any other combination of available technologies or protocols” <http://www.dod.gov/dodgc/olc/docs/PL109-163.pdf>
- *Public Law 108-375, SEC 331* states “To determine whether a change to the use of Internet Protocol version 6 will support Department of Defense requirements, the Secretary of Defense shall provide for rigorous, real-world, end-to-end testing of Internet Protocol version 6” <http://www.dod.mil/dodgc/olc/docs/PL108-375.pdf>

U.S. Federal Guidelines and Resources

- *DoD IPv6 Generic Test Plan, Version 4, May 2009*. Defines the test plan to be used by JITC to test COTS and GOTS (government off-the-shelf) IPv6 products. http://jitc.fhu.disa.mil/adv_ip/register/docs/ipv6v4_may09.pdf
- *DoD IPv6 Standard Profiles for IPv6 Capable Products, Version 4.0, July 2009* http://jitc.fhu.disa.mil/apl/ipv6/pdf/dsr_ipv6_product_profile_v4.pdf. Provides engineering-level definition of “IPv6 Capable” products necessary for interoperable use throughout the U.S. Department of Defense (DoD). Defines product classes, base requirements (applicable to all product classes) and functional requirements applicable to specific product classes.
- *DISA, Joint Interoperability Test Command (JITC)* provides test, evaluation, and certification services to support global net-centric warfighting capabilities. JITC tests and certifies IPv6 products and maintains an up to date list here: <http://jitc.fhu.disa.mil/apl/ipv6.html> - the list spans the following product categories HOST, NETWORK APPLIANCES, ROUTER, LAYER 3 SWITCH, SECURITY DEVICE, ADVANCED SERVER and APPLICATION.
- *NIST Special Publication (SP) 800-119, DRAFT Guidelines for the Secure Deployment of IPv6, Feb 2010*. Detailed analysis of the differences between IPv4 and IPv6, characterization of security ramifications and threats posed by transition and deployment to IPv6. http://csrc.nist.gov/publications/drafts/800-119/draft-sp800-119_feb2010.pdf
- *NIST Special Publication (SP) 500-267: A Profile for IPv6 in the U.S. Government – Version 1.0, Recommendations of the National Institute of Standards and Technology, July 2008*. <http://www.antd.nist.gov/usgv6/usgv6-v1.pdf>. Analysis to determine significant near-term technical

gaps for IPv6 deployment and recommendation of additional standards and testing infrastructures and processes needed to assist Federal agencies.

IETF RFCs

- Gilligan, R. and E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005. <http://www.rfc-editor.org/rfc/rfc4213.txt>
"This document specifies IPv4 compatibility mechanisms that can be implemented by IPv6 hosts and routers. Two mechanisms are specified, dual stack and configured tunneling."
- Shirasaki, Y., Miyakawa, S., Yamasaki, T., and A. Takenouchi, "A Model of IPv6/IPv4 Dual Stack Internet Access Service", RFC 4241, December 2005. <http://www.rfc-editor.org/rfc/rfc4241.txt>
"This memo is a digest of the user network interface specification of NTT Communications' dual stack ADSL access service, which provide a IPv6/IPv4 dual stack services to home users. In order to simplify user setup, these services have a mechanism to configure IPv6 specific parameters automatically."
- Carpenter, B. and K. Moore, "Connection of IPv6 Domains via IPv4 Clouds", RFC 3056, February 2001. <http://www.rfc-editor.org/rfc/rfc3056.txt>
"This memo specifies an optional interim mechanism for IPv6 sites to communicate with each other over the IPv4 network without explicit tunnel setup, and for them to communicate with native IPv6 domains via relay routers."
- Huitema, C., "Teredo: Tunneling IPv6 over UDP through Network Address Translations (NATs)", RFC 4380, February 2006. <http://www.rfc-editor.org/rfc/rfc4380.txt>
".here a service that enables nodes located behind one or more IPv4 Network Address Translations (NATs) to obtain IPv6 connectivity by tunneling packets over UDP; we call this the Teredo service."
- Templin, F., Gleeson, T., Talwar, M., and D. Thaler, "Intra-Site Automatic Tunnel Addressing Protocol (ISATAP)", RFC 5214, October 2005 <http://www.rfc-editor.org/rfc/rfc5214.txt>
"The Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) connects dual-stack (IPv6/IPv4) nodes over IPv4 networks."
- Despres, R., "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd)", RFC 5569, January 2010. <http://www.rfc-editor.org/rfc/rfc5569.txt>
"IPv6 rapid deployment on IPv4 infrastructures (6rd) builds upon mechanisms of 6to4 to enable a service provider to rapidly deploy IPv6 unicast service to IPv4 sites to which it provides customer premise equipment"
- Davies, E., Krishnan, S., and P. Savola, "IPv6 Transition/Co-existence Security Considerations", RFC 4942, September 2007. <http://www.rfc-editor.org/rfc/rfc4942.txt>
"The transition from a pure IPv4 network to a network where IPv4 and IPv6 coexist brings a number of extra security considerations that need to be taken into account when deploying IPv6 and operating the dual-protocol network and the associated transition mechanisms. "
- Tsirtsis, G. and P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)", RFC 2766, February 2000. <http://www.rfc-editor.org/rfc/rfc2766.txt>
"This document specifies an IPv4-to-IPv6 transition mechanism, in addition to those already specified in [TRANS]."
- Aoun, C. and Davis, E., "Reasons to Move the Network Address Translator - Protocol Translator (NAT-PT) to Historic Status", RFC 4966, July 2007. <http://www.rfc-editor.org/rfc/rfc4966.txt>
"This document discusses issues with the specific form of IPv6-IPv4 protocol translation mechanism implemented by the Network Address Translator - Protocol Translator (NAT-PT) defined in RFC 2766."
- Huitema, C., "An Anycast Prefix for 6to4 Relay Routers", RFC 3068, June 2001. <http://www.rfc-editor.org/rfc/rfc3068.txt>
"This memo introduces a "6to4 anycast address" in order to simplify the configuration of 6to4 routers."
- W. Townsley, O. Troan, IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification, RFC 5969 (PROPOSED STANDARD), August 2010, <http://tools.ietf.org/html/rfc5969>
- De Clercq, J., Ooms, D., Prevost, S., Le Faucheur, F., "Connecting IPv6 Islands over IPv4 MPLS Using IPv6 Provider Edge Routers (6PE)", RFC 4798, February 2007. <http://www.rfc-editor.org/rfc/rfc4798.txt>

IETF Internet Drafts

- Wing, D., "Port Control Protocol (PCP)", draft-ietf-pcp-base-02 (work in progress), January 4, 2011. <http://datatracker.ietf.org/doc/draft-ietf-pcp-base/>
"Port Control Protocol is an address-family independent mechanism to control how incoming packets are forwarded by upstream devices such as network address translators (NATs) and simple IPv6 firewalls."
- Yamagata, I., Shirasaki, Y., Nakagawa, A., Yamaguchi, J., and H. Ashida, "NAT444," draft-shirasaki-nat444-02 (work in progress), July 12, 2010. <http://datatracker.ietf.org/doc/draft-shirasaki-nat444/>
"This document describes one of the network models that are designed for smooth transition to IPv6. It is called NAT444 model. NAT444 model is composed of IPv6, and IPv4 with Large Scale NAT (LSN)."
- Yamaguchi, J., Shirasaki, Y., Miyakawa, S., Nakagawa, A., and H. Ashida, "NAT444 addressing models", draft-shirasaki-nat444-isp-shared-addr-04 (work in progress), <https://datatracker.ietf.org/doc/draft-shirasaki-nat444-isp-shared-addr/>
"This document describes addressing models of NAT444."
- Bush, R. (ed.), "The A+P Approach to the IPv4 Address Shortage," draft-ymbk-aplusp-06 (work in progress), October 18, 2010. <http://datatracker.ietf.org/doc/draft-ymbk-aplusp/>
"We are facing the exhaustion of the IANA IPv4 free IP address pool. Unfortunately, IPv6 is not yet deployed widely enough to fully replace IPv4, and it is unrealistic to expect that this is going to change before we run out of IPv4 addresses."
- Durand, A., Droms, R., Haberman, B., Woodyatt, J., and Y. Lee, "Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion", draft-ietf-softwire-dual-stack-lite-06 (work in progress), August 2010. <http://datatracker.ietf.org/doc/draft-ietf-softwire-dual-stack-lite>
"This document revisits the dual-stack model and introduces the dual-stack lite technology aimed at better aligning the costs and benefits of deploying IPv6."
- Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", draft-ietf-behave-v6v4-xlate-stateful-12 (Work in Progress), July 2010. <http://datatracker.ietf.org/doc/draft-ietf-behave-v6v4-xlate-stateful/>
"This document describes stateful NAT64 translation, which allows IPv6- only clients to contact IPv4 servers using unicast UDP, TCP, or ICMP."
- Penno, R., Saxena, T., Boucadair, M., and S. Sivakumar. "Analysis of 64 Translation", draft-penno-behave-64-analysis-05 (Work in Progress), October 2010, <https://datatracker.ietf.org/doc/draft-penno-behave-64-analysis/>
"Due to specific problems, NAT-PT was deprecated by the IETF as a mechanism to perform IPv6/IPv4 translation.."
- Li, X., Bao, C., Chen, M., Zhang, H., and J. Wu, "The CERNET IVI Translation Design and Deployment for the IPv4/IPv6 Coexistence and Transition", draft-xli-behave-ivi-07 (work in progress), January 6, 2010. <http://datatracker.ietf.org/doc/draft-xli-behave-ivi/>
"This document presents the China Education and Research Network (CERNET)'s IVI translation design and deployment for the IPv4/IPv6 coexistence and transition."

Samples of RIR Policies:

- ARIN, "ARIN Number Resource Policy Manual", Version 2010.3, September 2010. <https://www.arin.net/policy/nrpm.html>
- RIPE NCC, "IPv4 Address Allocation and Assignment Policies for the RIPE NCC Service Region". RIPE-498. October 2010. <http://www.ripe.net/ripe/docs/ripe-498.html>
- RIPE NCC, "IPv6 Address Allocation and Assignment Policy", RIPE-481. September 2009. <http://www.ripe.net/ripe/docs/ripe-481.html>
- APNIC, "APNIC transfer, merger, acquisition, and takeover policy", APNIC-123. Version 1. 10 February 2010. <http://www.apnic.net/policy/transfer-policy>
- LACNIC, "LACNIC Policy Manual" _V1.4. 06/12/2010. <http://www.lacnic.net/en/politiclas/manual.html>
- APNIC, "Policies for IPv4 address space management in the Asia Pacific region", APNIC-086, Version 11, 8 November 2010. <http://www.apnic.net/policy/add-manage-policy>
- APNIC, "IPv6 address allocation and assignment policy", APNIC-089. Version 009. 8 November 2010. <http://www.apnic.net/policy/ipv6-address-policy>
- AfriNIC, "IPv4 Allocation Policy", AFPUB-2005-v4-001, 17-05-2006, <http://www.afrinic.net/docs/policies/AFPUB-2005-v4-001.htm>

- AfriNIC, “IPv6 Allocation Policy”, AFPUB-2004-v6-001. 30-06-2004. <http://www.afrinic.net/docs/policies/AFPUB-2004-v6-001.htm>
- ICANN. “Global Policy for the Allocation of the Remaining IPv4 Address Space”, 6 March 2009, <http://www.icann.org/en/general/allocation-remaining-ipv4-space.htm>
- ICANN. “Internet Assigned Numbers Authority (IANA) Policy For Allocation of IPv4 Blocks to Regional Internet Registries”, 8 April 2005. <http://www.icann.org/en/general/allocation-IPv4-rirs.html>
- ICANN. “Internet Assigned Numbers Authority (IANA) Policy For Allocation of IPv6 Blocks to Regional Internet Registries”, 7 September, 2006. <http://www.icann.org/en/general/allocation-IPv6-rirs.htm>