

New Generation of the Internet Protocol

For more than 20 years the Internet has been based on Version 4 of the Internet Protocol (IPv4). IPv4 was designed to accommodate approximately four billion potential Internet addresses using 32-bits each, which seemed more than adequate back in the 1980s.¹

As the Internet grew, blocks of Internet addresses were assigned to various organizations and countries. However, by 1995 and 2000 about one-quarter and one-half of all potential Internet addresses were taken, respectively. With the fast growth in the number of Internet devices, it looked as if IPv4 addresses would be exhausted. However, researchers and technologists in the Internet standards organizations anticipated this problem in the early 1990s and developed methods to extend the life of IPv4. Meanwhile, they also initiated the development of the “next generation” of IP, an effort that led to the development and standardization of IPv6 (version 6 of the Internet Protocol).

Prolonging the Use of IPv4

The principal methods developed for prolonging the use of IPv4 include network address translation (NAT), classless interdomain routing (CIDR) and PPP/DHCP address sharing.

- Using NAT, a single device, such as a router, acts as an agent between the Internet and a local network, so that only a single IP address is required to represent an entire group of endpoints.
- Although the main motivation of CIDR was to reduce the size of routing tables carried by ISPs, it also permit smaller allocations of addresses to customers and ISP. In particular, it lets a grouping of separate IP networks appear as part of a single subnet, allowing service providers to conserve addresses by divvying up pieces of a full range of IP addresses to multiple customers.
- Besides these technical approaches for further extending the life of IPv4, unused, but assigned, addresses have been reclaimed for use. Another major driver is action by the Regional Internet Registries to prevent waste of IP addresses. PPP and DHCP are more auto-configuration aids; as more and more people move to always-on broadband connections, the address-conservation aspects of this will decrease.

Unfortunately, the conservation of IPv4 addresses has undesirable effects that penalize performance and increase operating costs. The measures used make system administration more complex and error prone. In particular, to configure NAT to support remote administration entails high operating costs. The lack of transparency of NAT makes reliable diagnoses of problems difficult. When NAT is used, the on-the-fly manipulation of IP packet headers, necessary for establishing a link between a private network and the public network, makes end-to-end IPsec security very difficult, as NAT’s modification of packet headers leads to a rejection of packets during IPsec controls. Moreover, NAT degrades performance, which is especially important for applications sensitive to transit times.

Perhaps worst of all, NAT is a stumbling block for launching peer-to-peer applications, which have recently emerged as key applications for both end users and businesses. For such applications, it is necessary to know the correspondent address in the private network, requiring complex application-related mechanisms for locating the address of the final correspondent. IPv6 provides end-to-end connectivity that is lost with the use of NATs and offers a better long-term solution for the delivery of services over IP.

While the interim measures taken to prolong the life of IPv4 has created other problems, the most immediate challenge driving migration to a new protocol is that the number of Internet endpoints is growing explosively, with the result that it is doubtful that IPv4 can meet future needs. Technologists in many industry sectors are predicting or actually designing complex applications for devices that will require IP addresses for a vast number of endpoints. More than one billion PCs, more than one billion mobile Internet endpoints (including mobile phones), more than one billion cars, billions of home-based voice-over-IP gateways, as well as the growing numbers of gaming stations and home appliances that may each need their own Internet addresses.

The Creation of IPv6

By the early 1990s researchers anticipated the need for more Internet addresses and began work on a new generation of the Internet protocol. The result is Internet Protocol Version 6, IPv6. IPv6 supports 128-bit addresses and the number of addresses available for Internet

endpoints is vast⁴, exceeding the number needed for any scenario yet devised. IPv6 was approved by the IETF as a Proposed Standard in 1995 and was approved as a standard in 2000.

Although the original impetus for the creation of IPv6 was to increase the address space, the opportunity to design a new Internet Protocol made it possible to introduce additional enhancements. IPv6 was designed with an architecture more consistent than that of IPv4, with hooks that can be used for improved support for improved security, multicasting and anycasting, and mobility, as well as potentially for enhanced quality of service. One particular security-related advantage of IPv6 is the inclusion of the secure neighbor discovery protocol, which protects neighbor discovery messages through the use of cryptographically generated addresses.²

Although IPv6 brings many benefits, it is not a panacea for all challenges the Internet faces. IPv6 does add several layers of built-in security and once employed, it will help to stop certain classes of attacks by making it difficult to spoof, or masquerade, as a different computer. However, IPv6 has no ability to close most known network vulnerabilities, which usually exploit security weaknesses above the IP layer. Yet it is a key part of the solution to establishing a “culture of networking security.”

IPv6 enables better traffic flow than IPv4 and enables automatic connectivity. In particular, IPv6 offers “neighbor” discovery and address autoconfiguration capabilities supporting mobility, allowing hosts to operate anywhere without special support. Using these capabilities, a host can be reached no matter where it is connected to the Internet. This is accomplished by binding the current “care-of address” of a mobile host to its home address.

A Phased Adoption

Although IPv6 offers advantages, its adoption has been slowed by the complexity and costs associated with the move from IPv4 to IPv6. Because of this, the migration from IPv4 to IPv6 will require the coexistence of these protocols for some time.

The key strategies used in deploying IPv6 at the edge of such a network involve carrying IPv6 traffic over the IPv4 network, allowing isolated IPv6 domains to communicate with each other before the full transition to a native IPv6 backbone. It is also possible to run IPv4 and IPv6 throughout the network, from all edges through the core, or to translate between IPv4 and IPv6 to allow hosts communicating in one protocol to communicate transparently with hosts running the other protocol. A fourth option in a phased migration strategy is the delivery of IPv6-based services over an MPLS core network.³ All techniques allow networks to be upgraded, and IPv6 to be deployed incrementally with little to no disruption of IPv4 services.

Market Interest in IPv6

The heaviest demand for new IPv6 addresses is in Asia, because that continent has struggled with a minimal allocation of IPv4 addresses. Enterprises in Asia are planning to adopt IPv6 technology because no IPv4 addresses are available to meet their current and future needs. Moreover, Japan, South Korea and China have federal mandates and incentives for the private sector to adopt IPv6 on an accelerated

schedule. China is testing IPv6 networks in some big cities around the country. Japan has already implemented an IPv6 production network, which is used by every service provider in the country. South Korea is working with the European Union to develop applications and services using IPv6.

Not only does IPv6 provide a way that the shortage of Internet addresses in Asia can be met, but there is a growing opinion that early adoption of IPv6 offers a competitive advantage for Asia relative to the U.S. for technological leadership in the Internet. This view is also held within the European Union.

The migration to IPv6 is slower in Europe than in Asia, but the European Union has mandated that in the next few years, network devices must support IPv6. Also, in January 2004, the EU launched a large research IPv6 network. Currently, IPv6 is used extensively on several large research networks in Europe and Asia. Commercial IPv6 service is available in Japan, Korea, Malaysia, Taiwan, Hong Kong and Australia, as well as in Europe, including the U.K., the Netherlands, France, Germany and Spain.

There has also been a lot of interest in IPv6 in the U.S. among the research, vendor communities and the federal government. While the high cost of rolling it out has deterred service providers from introducing it, the federal government’s mandate to move to this upgraded protocol is spurring demand in the public sector. Implementing IPv6 requires replacing the IP stacks on routers, switches, and other networking equipment and supporting IPv6 on servers, hosts, and other end devices. Some industry analysts have said that it will be a long time before IPv6 will be used by North American carriers, as measures such as NAT extend the life of IPv4.

The 2003 announcement by the Department of Defense (DoD) of its decision to switch to IPv6 had a considerable influence on the movement to IPv6 in the U.S. DoD’s goal is to transition all DoD networking to IPv6 by 2008. The Office of Management and Budget has also set 2008 as the goal for transitioning all government agencies to the newer protocol. Agencies have already been instructed to develop an analysis of the impact from the transition and to inventory IPv6-ready devices. So far only DoD has made significant preparations for the transition, since this technology will help enable the execution of military strategy and tactics.

At the present time, IPv6 is running on large-scale research networks in the U.S. and commercial IPv6 service is available in several places in the U.S. The DoD is actively pushing the adoption of IPv6. They are part of the Moonv6 Project, which set up the largest IPv6 network in the world in March 2004. The goal of the Moonv6 Project is to drive the adoption of IPv6 in the U.S.

A key area for the adoption of IPv6 is for use by digital mobile devices. The use of IPv6 is mandated in Release 5 of the Universal Mobile Telecommunications System standard (UMTS) from the 3rd Generation Partnership Project (3GPP), which develops standards for advanced mobile networks. Specifically, UMTS Release 5 mandates IPv6 in all handsets and the 3G Internet Multimedia Subsystem is defined to run only on IPv6.

Key Points

- **Internet Protocol Version 4 (IPv4) has been a standard since 1981, and currently forms the foundation of most Internet transactions.**
- **IPv4 suffers from several important shortfalls, chief of which include a lack of sufficient address space (fewer than four billion addresses, a problem compounded by inefficient allocation), as well as inadequate security, multicasting, and Quality of Service (QoS) features.**
- **Methods devised to overcome IPv4 shortcomings, such as Network Address Translation (NAT), often introduce obstacles to seamless Internet connectivity.**
- **Greatest impetus for adoption of IPv6 comes from the Asia Pacific region, owing to the acute shortage of allocated IPv4 addresses; and in the U.S. from the Department of Defense and the Office of Management and Budget.**
- **Methods to prolong the use of IPv4 have been devised, such as Network Address Translation (NAT), allowing multiple endpoints to share one IPv4 address. While these industry supported “workarounds” have extended the availability of addresses, there are other limitations created in using NAT for some important applications, such as peer-to-peer applications, and potentially other future applications.**
- **Work began in the mid-1990s to develop a “next generation” Internet protocol. The result, IPv6 (sometimes called IPng), was approved as a standard in 2000.⁴ IPv6 brings several benefits: it supports a vast number of Internet addresses, enough to meet all current needs; in addition, a fully implemented IPv6 offers the ability for applications providers to offer users with improved performance, guaranteed quality of service capabilities, manageability, scalability, data protection and multicast support.**
- **Cost and complexity of upgrading from IPv4 to IPv6 is significant. More development is required to smooth the transition and coexistence between legacy IPv4 networks and IPv6 networks to provide businesses and suppliers a smooth transition path. These issues, and the workarounds extending the life of IPv4, have delayed IPv6 implementation, especially in the United States.**
- **Some analysts believe that IPv4 and IPv6 will coexist and that IPv4 not totally be replaced until some years following. However, AT&T’s view is that many customers will be slow to move to IPv6. It is quite likely that IPv6 will need to operate in parallel with IPv4 for a very long time.⁵**

DoD and IPv6 - The Key to Net-Centric Combat Operations

The greatest challenges facing the DoD in terms of the internet is how to leverage the ubiquitous internet with the warfighter for secure end-to-end mobile communications, improved performance, QoS and real-time situational awareness.

Net-centric operations and warfare requirements dictate that there are increased IP address allocation so that the globe can be divided into a global address location grid – IPv6 is slated to be able to support 1000 address for each square meter of the earth’s surface. This can be used as coordinates for the identification of every component in the warfight. In this environment information systems, soldiers, military vehicles and their component parts, mobile devices, decision makers, sensors and systems, become an integrated entity on the global information grid (GIG), allowing for collaboration with precision and speed. In this fully networked environment, command and control now moves from a hierarchical model to an integrated networked model for improved agility, flexibility and accurate, decisive responses. IPv6 is the foundation of interoperability across the DoD GIG.

The potential benefits of IPv6 are great. However, transitioning will be a daunting task. The majority of hardware and software systems will need to be upgraded or replaced. While most of this could occur through normal technology-refresh cycles, IPv4 and IPv6 systems will need to interoperate for a long time because of the immaturity of IPv6 advanced capabilities, e.g. transition mechanisms, tactical wireless, security and QoS. The financial and technical impact of the 2008 mandate may undoubtedly change the “mandate” to a “goal” especially for the civilian agencies, where the customer benefits are not as apparent.

Navy and Marines

FORCENet is the operational construct and architectural framework that will provide the Navy-Marine Corp team with the capability to deliver persistent secure and accurate battlespace intelligence for rapid and coordinated decision making. It binds warriors, sensors, networks, C2, platforms and weapons into a tightly integrated distributed combat force. This enables dispersed, human, decision-makers to leverage military capabilities and achieve dominance across the entire mission landscape with joint, allied and coalition partners. FORCENet is the future implementation of Network Centric Warfare in the Naval Services, extending the web to basic devices, using the IPv6 protocol capabilities.

Air Force

The Air Force requires global network connectivity, network-enabled platforms/weapons, fused Intel and real-time C2 and SA. With IPv6 the Air and Space Ops center can have global network connectivity to – every airman, aircraft, tool or piece of equipment across the constellationNet in real-time. This will increase efficiency of operations by shortening time for decisions, improve accuracy on the battlefield and improve collaboration and information sharing for decision making, while reducing collateral damage in warfare.

Army

Mandated operation capabilities dictate network-centric battle command. Examples of areas critical to net-centricity and the Future

Force concept that are being explored for potential operational benefits include enhanced capabilities for mobility, end-to-end security, multicast and auto-configurations. The army is therefore working to incorporating IPv6 into all of its Enterprise Architectures – LandWarNet, Business Enterprise Architecture and Battle Command Architecture. They will gradually migrate to a dual-stack backbone, with a “native v6” switch beginnings after the ‘08 guidelines.

About AT&T Government Solutions

Every day, thousands of experienced AT&T Government Solutions professionals go beyond expectation, deploying visionary solutions that serve our citizens, defend our nation and prepare for the future.

We serve the federal government as a trusted provider, backed by a proven performance record in delivering mission-enabling solutions. Fusing our core networking capabilities and our professional services expertise along with innovation from AT&T Labs, we are driven to meet the toughest agency demands today, while establishing a path to emerging technologies.

Underpinning every solution we build are the global resources and assets of one of the largest providers of communications services in the world. Our dynamic service management tools, advanced technology and an experienced staff modernize operations and enhance our customers' experience, enabling agencies to focus on their mission – not their IT challenges.

For more information contact:

AT&T Government Solutions
1900 Gallows Road
Vienna, VA 22182
www.att.com/gov

References

1. Not all bit strings of length 32 are valid Internet addresses. IPv4 has three classes of addresses, Class A, Class B, and Class C, and also supports services such as multicasting. Because of the way these addresses are specified, only around 3 billion IPv4 addresses are available for use by Internet endpoints. Moreover, because the way IPv4 addresses are assigned to endpoints, in practice, only about 250 million IPv4 addresses can be used.
2. IPv6 nodes use the Neighbor Discovery Protocol (NDP) to discover other nodes on the link, to determine their link-layer addresses to find routers, and to maintain reachability information about the paths to active neighbors. If not secured, NDP is vulnerable to various attacks. See: RFC 3971.
3. AT&T was the first major networking provider to delivery MPLS services and today offers a single, seamless MPLS-enabled infrastructure.
4. The IPng directorate was formed in 1993; there was a Proposed Standard – which carries a great deal of significance in the IETF – in 1995.
5. Security expert Steve Bellovin estimates that IPv4 cannot start to die out until at least five years after Microsoft ships a fully IPv6-capable end-user system. He feels there will be much greater installed base of IPv4-only machines until then, especially given that most machines are never upgraded. He notes, however, that Windows XP SP2 is fully v6-capable and that within five years, we may start to see the tipping point.

To learn more about our full array of products and services, contact your AT&T Client Business Manager at: 1.800.862.0926 or www.att.com/gov.

