JASON G. ANDRESS

IPv6: the next Internet protocol

Jason Andress works as a system administrator for Agilent Technologies. He is currently wrapping up his master's degree in CS and will soon be starting on his doctorate. He is also a recent Debian convert.

- *Jason.Andress@Agilent.com*

The follow-on to IPv4, IPv6 has not yet seen wide deployment. This article discusses the motivations for IPv6, its history, its design criteria, and some of its new features. Finally, a look at future deployment and applications is presented.

IPv6 is the network protocol follow-on to the popular IPv4,[1] the network transport layer of the TCP/IP protocol that runs the majority of the Internet. IPv6 was designed with the knowledge of all of IPv4's shortcomings and with 20 good years of experience running the Internet. IPv6 addresses the Internet's current and anticipated problems with elegant solutions.

IPv4

IPv4 was designed in 1980 to replace the already archaic NCP protocol on the ARPANET as it then existed. When first deployed, fewer than 1,000 computers were linked by IPv4. Who would have guessed that a 32-bit address space whose theoretical maximum connectivity was about two billion computers would not be enough?

Two decades after its first implementation, the explosive growth of the Internet exposed some of IPv4's limitations, the most serious of which is limited address space. The problems of expanding the address space drove the design of IPv6. IPv4 had several other problems, however:

- Its header
- Routing
- Configuration
- Security
- Quality of Service (QoS)

IPV4 ADDRESS SPACE

Two problems exist in the IPv4 address space. First, the 32-bit address does not allow sufficient address space; second, the address allocation is not granular enough. In the original allocation scheme there are five classes of addresses: A, B, C, D, and E. Of these classes, only A, B, and C are used during normal operation. These classes are broken out like so:

- Class A—125 networks, 16 million hosts per network, ~2 billion hosts total
- Class B—16,382 networks, 65,534 hosts per network, ~1.1 billion hosts total
- Class C—2 million networks, 254 hosts per network, ~508 million hosts total

NOTE

[1] The effort to develop the Internet Protocol Next Generation was started in 1994 [2]. One of the fields carried forward from IPv4 was the version field. IPv4 used version number 4; another protocol, the Internet Stream Protocol, was already using version number 5. Thus, the first available version number was 6 and the name "IPv6" was born.

Note that 125 (0.006%) of the 2,016,507 networks constitute more than half of the available addresses.

One solution to IPv4's address-space problems is Classless Inter-Domain Routing (CIDR) [9]. CIDR replaces the previous A, B, and C address classes with an addressing scheme that enables the full IP address space to be partitioned much more finely. CIDR enables addresses to be assigned to networks as large as 500,000 hosts or as small as 32 hosts. The smallest block of addresses assignable under class-ful routing was 254 addresses (a class C), which was one of the contributing factors in the 3% usage rate of assigned addresses. (The other two addresses of the 256 possible are used as broadcast addresses.)

In addition to the address allocation changes brought about by CIDR, Network Address Translation (NAT) technology enables multiple systems to share a single IP address by carefully routing the combination of IP address and port number on local networks. The advantages of having a unique address for every computer on the Internet are obvious. Coupled with the proliferation of small appliances that exploit very inexpensive networking technologies, the addressing problem continues to fester.

IPV4 HEADER

The IPv4 header has two main problems that slow throughput:

- A checksum must be computed for each packet being processed.
- Each router that processes the packet must process the option field.

Unfortunately, without restructuring the header (redesigning the protocol), neither of these problems is particularly fixable.

IPV4 ROUTING

CIDR also addresses the problem with the growing size of the global routing tables. Under the previous class-ful system, the global routing tables were growing toward their maximum theoretical size of 2.1 million entries. In addition to restructuring address conventions, CIDR also implemented Hierarchical Routing Aggregation with a logically tiered structure to reduce entries in routing tables. Under this system, each router keeps only the routing information for the next routers in its own logical hierarchy. This change has reduced the number of entries in the global routing tables to approximately 35,000.

IPV4 CONFIGURATION

Under IPv4, TCP/IP-based networking requires several pieces of data to configure a network. An administrator or user must supply the IP address(es), routing gateway address, subnet mask, DNS server(s), and possibly other information. In order to simplify configuration, some networks utilize Dynamic Host Configuration Protocol servers and then enable local area network clients to request appropriate network configuration from a central server as network services are configured on that client. Although this eases configuration for the end user, it really only moves the burden to the network's administrators.

IPV4 SECURITY

The IPv4 protocol was created in an age of cooperation among research and development institutions that composed the network. The goal was to create a protocol that enabled the network to succeed; the twin notions of hostile environments or noncooperative, even destructive, users were not strongly considered. Unfortunately, such attacks need to be taken into consideration today.

The lack of integral security in the design of IPv4 enabled the wide variety of attacks that are commonly seen today. Spoofing attacks, attacks that exploit protocol implementations to crash or disable the host or slow other connections, and a variety of others are commonplace in today's network environment.

Mechanisms to secure IPv4 do exist, but no requirements for their use are in place and no one standard exists. One of these methods, IPSec [10], sees common use in securing packet payloads. IPSec exploits cryptographic security services to provide:

- Confidentiality (messages cannot be read in transit)
- Integrity (messages cannot be altered in transit)
- Authentication (the origin of the sender is known with total confidence)

Confidentiality is provided via the use of encryption, integrity by means of a cryptographic checksum that incorporates the encryption key, and authentication by digitally signing with the encryption key.

IPV4 QOS

Quality of service (QoS) enables the priority of traffic to be adjusted to suit the type of traffic that is being handled. When IPv4 was designed, most Internet traffic was text-based. As the Internet has expanded and technology has progressed, new types of traffic such as streaming video and multiplayer gaming have created a need to prioritize traffic that is dependent on speed of delivery over traffic which does not depend on speed, such as email.

While QoS standards exist for IPv4, real-time QoS support relies both on the type of service (TOS) field and on identification of the contents of the packets. Unfortunately, the IPv4 TOS field has limited functionality and is interpreted differently by different vendors. Additionally, it is not possible to identify the contents of encrypted packets.

Design Considerations for IPv6

By 1990 it had become clear that the protocols then in use would not be able to hold up under the explosive growth of the Internet. A January 1991 meeting of the Internet Activities Board (IAB) and the Internet Engineering Steering Group (IESG) put forth five main categories as the focus for development efforts on future protocols [11]:

- Routing and addressing
- Multi-protocol architecture
- Security architecture
- Traffic control and state
- Advanced applications

Those groups completed design of the specifics of the IPv6 (then termed IPng) protocol exactly four years later [12].

IPV6 HEADER

The IPv6 header design reduces routing and processing overhead by moving nonessential and option fields to extension headers placed after the IPv6 header. The new header is only about twice as large as the IPv4 header, even with the new features and (relatively) huge 128-bit addresses. The increased header size does not cause any appreciable delay in traffic, due to the improvements made to the header in order to ease processing.

IPv4 headers and IPv6 headers can coexist on a network, although IPv6 is not backward compatible with IPv4. A host or router must support both the IPv4 and IPv6 protocol stacks in order to process both header formats.

IPV6 ADDRESSING

IPv6 sports 128-bit addresses, in contrast to the 32-bit addresses of IPv4. This gives IPv6 an address space of 3.4 x 10^{38} machines, theoretically enough to assign three trillion addresses for every human on earth and 10,000 trillion other planets. However, this large space is not intended to be used in that way. Many of the address bits are used less efficiently in order to simplify addressing configuration dramatically.

Only a small percentage of IPv6 addresses are currently allocated for use by hosts, with a huge number of addresses available for future use. The address space that IPv6 provides obviates address-conservation techniques (e.g., NAT).

IPV6 ROUTING

IPv6 routing is almost identical to CIDR IPv4 routing. The IPv6 address design facilitates an efficient, hierarchical routing system that enables smaller routing tables, which, in turn, permit routing of more hosts than is possible under IPv4.

IPV6 CONFIGURATION

IPv6 supports a new stateless address configuration scheme that dramatically simplifies host configuration. In IPv6, hosts automatically configure themselves with addresses created by combining prefixes advertised by local routers with information local to the host. Even without a router, hosts on the same link can automatically configure themselves with local addresses and communicate on that local link without need for manual configuration. This new configuration system not only removes a menial task from the network administrator, but also allows renumbering of an entire network by changing local address information on the local routers [2].

IPV6 SECURITY

Compliance with IPSec [10] is mandatory in IPv6, and IPSec is actually a part of the IPv6 protocol. IPv6 provides header extensions that ease the implementation of encryption, authentication, and Virtual Private Networks (VPNs). IPSec functionality is basically identical in IPv6 and IPv4, but one benefit of IPv6 is that IPSec can be utilized along the entire route, from source to destination.

IPSec in IPv6 is implemented using two extension headers: the authentication extension header and the Encrypted Security Payload (ESP) extension header. The authentication extension header provides integrity and authentication of source, protection against replay attacks, and protection for the integrity of the header fields. The ESP extension header provides confidentiality, authentication of source, protection against replay attacks, and limited traffic flow confidentiality [14].

IPV6 QOS

The IPv6 header has new fields to define how traffic is handled and identified. By using a flow label field in the header, traffic identification enables a router to identify and potentially provide special handling for packets that belong to a flow (a series of packets between a source and destination). Because the traffic is identified in the header, support for QoS can be provided even when the contents of the packet are encrypted with IPSec.

The Urgency of IPv6 Deployment

NAT and CIDR have somewhat eased the address space issue for the current time frame; however, address space is not allocated evenly across the globe. "Some regions of the world were allocated fewer IPv4 addresses than others. The most populated part of the world, the Asia-Pacific region, was allocated the smallest amount of the remaining IP addresses: 2%, compared with 5% for the Americas and 4% for Europe. Some countries in Asia-Pacific have virtually run out of addresses already, others are close. The European Union has predicted that address space in Europe will become critical in 2005." [13] Using IPv4, China's allocation amounts to only about 22 million IP addresses. With a population of 1.3 billion people and 17 million Internet subscribers, China will shortly be entirely out of IPv4 space.

These observations, among others, are prompting many organizations to examine the transition to IPv6 in the near future. One of the largest and most visible organization with firm plans for the transition to IPv6 is the United States Department of Defense. According to a DOD memorandum on IPv6, "The DOD goal is to complete the transition to IPv6 for all inter- and intra-networking across the DOD by 2008." [6] In accordance with this memo, any network assets that are put into place as of October 1, 2003, must be both IPv6 and IPv4 capable. For those forward thinkers, there is great significance to this. If the DOD plans to be entirely on IPv6 by 2008, any company that interfaces with the networks of the DOD must be able to accommodate IPv6. This seems to be an excellent setup for a rather swift chain reaction of IPv6 conversions.

Wide IPv6 Deployment

The pain of upgrading to facilitate migration to IPv6 can be reduced by performing as much of the work as is feasible in advance. Almost all of the required changes fall into this category, making the final switchover to IPv6 an anti-climactic event. Forward-looking organizations such as the DOD are already taking these steps.

Network infrastructure changes can be phased in over time with minimum disruption by switching to routing and related equipment that supports both IPv4 and IPv6. This activity alone removes a great deal of the work in making the transition and can be accomplished fairly simply by eschewing equipment that does not support IPv6. In theory, the natural turnover of network equipment will cause IPv6 hardware compatibility to become a non-issue over time.

Much work for the transition to IPv6 involves the software and operating systems in use on clients and servers.

Almost all major operating systems have had at least some level of support for IPv6 for the last five years. Upgrading a corporate network, however, is not so simple as changing a configuration parameter and requires extensive planning in order to ensure a smooth rollout.

Migrating to IPv6 does not need to be painful, but it does need advance preparation and identification of networked applications that require major investment (vs. simple changes). Aside from making hardware and software changes, what better way to prepare for a new technology than hands-on experience?

Further Research on IPv6

Useful experience in running IPv6 networks can be gained in one of two ways: experimenting with an IPv6-based machine on the Internet, or setting up an offline test lab.

Several options exist for running a live IPv6 machine on the Internet:

- The "6bone" is an experimental Internet facility for tunneling IPv6 packets over the IPv4 Internet. See the Web site [4] to learn how to run IPv6 in general and obtain proper IPv6 addresses to use with the IPv6 Testing Address Allocation experimental protocol [7].
- Several ISPs and companies also have functioning IPv6 network connections. Connecting an IPv6 machine to the Internet poses no great difficulty given an IPv6 address, proper equipment, and a configuration [5].
- O'Reilly's *Ipv6 Essentials* [1] is a good guide to configuring various operating systems to use IPv6 and testing IPv6-oriented applications and utilities.

Appendix E in the Microsoft Press *Understanding IPv6* [3] is a guide to setting up an IPv6 test lab on Windows, including clients, routers, and a DNS server. Although intended specifically for Microsoft platforms, the main concepts translate easily to other operating systems. As specified in the book, the test lab cycles through pinging, static routing, name resolution, IPSec, and some of the IPv6 security features. Although limited, this lab setup enables experimentation without concern for security threats or other issues related to connecting to a live IPv6 network.

Practical Implications

The majority of the issues related to IPv6 fall into the categories of economics and adopter comfort level.

Economics plays a large part when looking at a migration to IPv6, not only in the sense of capital expenditure, but also in manpower, time, and other resources.

The main economic factor that needs to be considered when looking at a migration to IPv6 is the timeline for the migration. The speed of the migration can have a large effect on the cost of the project.

In the long term, migrating to IPv6 is not an expensive proposition. Over time, network infrastructure equipment will be replaced, software will be upgraded, and most of the other changes that are needed for a migration can be integrated with the normal upgrade process.

Given a very short timeline for a migration to IPv6, the cost can increase dramatically. If upgrades to network infrastructure, client software, servers, and other associated items are attempted concurrently and over a short period, not only does the cost increase, but so does the impact on users, which brings us to adopter comfort level.

The comfort level of potential users of IPv6 may not seem to be a large issue, but it definitely has the potential to be. If, during the transition to IPv6, a security issue or other problem of sufficient magnitude were publicized, the impact on large-scale migration could be significant and far-reaching. This is another case where carefully planning migrations to IPv6 can help to avert problems.

The Future

From a high-level view, the major benefits of IPv6 are its scaling and increased security. The global deployment of IPv6 will be an enabling factor in redefining the Internet as we now know it.

With IPv6, the Internet can continue its dramatic growth while embracing mobile telephones, PDAs, home appliances, automobiles, intelligent buildings, and a plethora of other devices.

Looking to the longer-term future, the ability to address and fully access any networked device has the potential to lead to new technologies and the renewal of existing ones. Consider the opportunity to take "single sign-on" a step further by addressing individuals as well as machines. An implanted chip [8] could carry an address for a particular individual and facilitate the use of cell phones, PDAs, workstations, etc. Such devices would read the user's address from the implanted chip and configure themselves accordingly. Such a technology would facilitate routing of email, retrieval of data, and other tasks that currently inconvenience users by fragmenting their data by geographical location.

Conclusion

IPv6, still in its initial stages of deployment after several years of availability, is definitely coming. It will renormalize the Internet by removing stopgap measures such as NAT, by providing a standard security mechanism for packet payloads, and by effectively removing the cap on address space. It will reduce, in the long term, the load of day-to-day administration tasks currently required just to keep networks running at a basic level, and it will relegate most network configuration to just plugging in the cable.

In the end, worry and hand-wringing over the transition to IPv6 will likely rise to the level of headline-making, but, with a little planning, the transition will be as anticlimactic as the Y2K problem.

REFERENCES

[1] Hagen, S., *IPv6 Essentials*, O'Reilly Media, Inc., 2002.

[2] Loshin, P., *IPv6 Clearly Explained*, Morgan Kaufmann Publishers, Inc., 1999.

[3] Davies, J., *Understanding IPv6*, Washington: Microsoft Press, 2003.

[4] Fink, B., "6Bone testbed for deployment of IPv6," retrieved December 2, 2004, from http://www.6bone.net/, 2004.

[5] Hinden, R., "IPng implementations," retrieved December 4, 2004, from http://playground.sun.com/pub/ipng/html/ipng-implementations.html, 2002.

[6] Stenbit, J., "Internet Protocol Version 6 (IPv6)" [electronic version], Department of Defense Memorandum, 2003.

[7] Hinden, R., Fink, R., & Postel, J., "IPv6 Testing Address Allocation," retrieved December 1, 2004, from ftp://ftp.isi.edu/in-notes/rfc2471.txt, 1998.

[8] Digital Angel Corporation, "FDA Clears Verichip for Medical Applications in the United States," retrieved December 15, 2004, from http://www.4verichip.com/nws_10132004FDA.htm, 2004.

[9] Fuller, V., Li, T., Yu, J., & Varadhan, K., "Classless Inter-domain Routing (CIDR): An Address Assignment and Aggregation Strategy," retrieved December 17, 2004, from ftp://ftp.rfc-editor.org/in-notes/rfc1519.txt, 1993.

[10] "Internet Protocol," retrieved December 16, 2004, from ftp://ftp.rfc-editor.org/in-notes/rfc2401.txt, 1998.

[11] Clark, D., Chapin, L., Cerf, V., Braden, R., & Hobby, R., "Towards the Future Internet Architecture," retrieved December 19, 2004, from http://www.rfc-editor.org/cgi-bin/rfcdoctype.pl?loc=RFC&letsgo=1287&type=ftp&file_format=txt, 1991.

[12] Bradner, S., Mankin, A., "The Recommendation for the IP Next Generation Protocol," retrieved December 19, 2004, from http://www.rfc-editor.org/cgi-bin/rfcdoctype.pl?loc=RFC&letsgo=1752&type=ftp&file_format=txt, 1995.

[13] Holder, D., "Upgrading the Net," *British Computer Bulletin*, retrieved December 19, 2004, from http://www.bcs.org/BCS/Products/Publications/JournalsAndMagazines/ComputerBulletin/OnlineArchive/may02/digitalworld.htm, 2002.

[14] Cisco, "Implementing Security for IPv6," retrieved December 19, 2004, from http://mail.cat.or.th/ipv6/sa_secv6.pdf, 2004.