Payoff

The only way to cope with the changes on the Internet—the number of hosts, types of applications, and growing security concerns—is to implement a new version of the Internet protocol to succeed IPv4. The IETF formed the IP next-generation (IPng) Working Group to define this transitional protocol, and the result was IP version 6 (IPv6)—designed as an evolution from IPv4, rather than as a radical change.

Introduction

The Internet is historically linked to the ARPANET, the pioneering packet-switched network built for the US Department of Defense in 1969. Starting with four nodes that year, the ARPANET slowly grew to encompass many systems across the US, and connected to hosts in Europe and Asia by the end of the 1970s. By the early 1980s, many regional and national networks across the globe started to become interconnected, and their common communications protocols were based on the TCP/IP suite. By the late 1980s, the number of host systems on these primarily academic and research networks could be counted in the hundreds or thousands. In addition, most of the traffic was supporting simple text-based applications, such as E-mail, file transfers, and remote log-in.

By the 1990s, however, users discovered the Internet and commercial use, previously prohibited or constrained on the Internet, was actively encouraged. Since the beginning of this decade, new host systems are being added to the Internet at rates of up to 10% per month, and the Internet has been doubling in size every 10-12 months for several years. By January 1997, there were more than 16 million hosts on the Internet, ranging from PC-class systems to supercomputers, on more than 100,000 networks worldwide.

The number of connected hosts is only one measure of the Internet's growth. Another way to quantify the change, however, is in the changing applications. On today's Internet it is common to see hypermedia, audio, video, animation, and other types of traffic that were once thought to be anathema to a packet-switching environment. As the Internet provides better service support, new applications will spark even more growth and changing demographics. In addition, nomadic access has become a major issue with the increased use of laptop computers, and security concerns have grown as a result of the increased amount of sensitive information accessible via the Internet.

IPv6 Background and Features

The Internet protocol (IP) was introduced in the ARPANET in the mid-1970s. The version of IP commonly used today is version 4 (IPv4), described in RFC 791. (See the Appendix at the end of this article for a listing of RFCs related to IPv6.)

Although several protocol suites (including Open Systems Interconnection) were proposed over the years to replace IPv4, none succeeded because of IPv4's large and continually growing installed base. Nevertheless, IPv4 was never intended for today's Internet in terms of the number of hosts, types of applications, or security concerns.

In the early 1990s, the Internet Engineering Task Force (IETF) recognized that the only way to cope with these changes was to design a new version of IP to become the successor to IPv4. The IETF formed the IP next-generation (IPng) Working Group to
define this transitional protocol, ensuring long-term compatibility between the current and new IP versions and support for current and emerging IP-based applications.

Work started on IPng in 1991 and several IPng proposals were subsequently drafted. The result of this effort was IP version 6 (IPv6), described in RFCs 1883 to 1886; these four RFCs were officially entered into the Internet Standards Track in December 1995.

**Differences Between IPv4 and IPv6**

IPv6 is designed as an evolution from IPv4 rather than as a radical change. Useful features of IPv4 were carried over in IPv6 and less useful features were dropped. According to the IPv6 specification, the changes from IPv4 to IPv6 fall primarily into the following categories:

- **Expanded addressing capabilities** The IP address size is increased from 32 bits to 128 bits in IPv6, supporting a much greater number of addressable nodes, more levels of addressing hierarchy, and simpler autoconfiguration of addresses for remote users. The scalability of multicast routing is improved by adding a scope field to multicast addresses. A new type of address, called anycast, is also defined.

- **Header format simplification** Some IPv4 header fields have been dropped or made optional to reduce the necessary amount of packet processing and to limit the bandwidth cost of the IPv6 header.

- **Improved support for extensions and options** IPv6 header options are encoded to allow for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future. Some fields of an IPv4 header are optional in IPv6.

- **Flow labeling capability** A new quality-of-service (QOS) capability has been added to enable the labeling of packets belonging to particular traffic “flows” for which the sender requests special handling, such as real-time service.

- **Authentication and privacy capabilities** Extensions to support security options, such as authentication, data integrity, and data confidentiality, are built into IPv6.

**Improved Terminology of IPv6**

IPv6 also introduces and formalizes terminology that, in the IPv4 environment, are loosely defined, ill-defined, or undefined. The new and improved terminology includes:

- **Packet** This is an IPv6 protocol data unit (PDU), comprising a header and the associated payload. In IPv4, this would have been termed “packet” or “datagram.”

- **Node** This is a device that implements IPv6.

- **Router** This is an IPv6 node that forwards packets, based on the IP address, not explicitly addressed to itself. In former TCP/IP terminology, this device was often referred to as a gateway.
Host This represents any node that is not a router. Hosts are typically end-user systems.

Link This is a medium over which nodes communicate with each other at the data link layer (e.g., an automated teller machine, a frame relay, a switched multimegabit data service wide area network, or an Ethernet or Token Ring local area network).

Neighbors These are nodes attached to the same link.

IPv6 Header Format

The format of an IPv6 header is shown in Exhibit 1. Although IPv6 addresses are four times the size of IPv4 addresses, the basic IPv6 header is only twice the size of an IPv4 header, thus decreasing the impact of the larger address fields. The fields of the IPv6 header are:

- **Version** This represents the IP version number (4 bits). This field's value is 6 for IPv6 and 4 for IPv4. This field is in the same location as the version field in the IPv4 header, making it simple for an IP node to quickly distinguish an IPv4 packet from an IPv6 packet.

- **Priority** This enables a source to identify the desired delivery priority of the packet (4 bits).

- **Flow label** This is used by a source to identify associated packets needing the same type of special handling, such as a real-time service between a pair of hosts (24 bits).

- **Payload length** This is the length of the portion of the packet following the header, in octets (16 bits). The maximum value in this field is 65,535; if this field contains zero, it means that the packet contains a payload larger than 64K bytes and the actual payload length value is carried in a jumbo payload hop-by-hop option.

- **Next header** This identifies the type of header immediately following the IPv6 header and uses the same values as the IPv4 protocol field, where applicable (8 bits). The next header field can indicate an options header, higher layer protocol, or no protocol above IP. Sample values are listed in the following table:

<table>
<thead>
<tr>
<th>Value</th>
<th>Contents of the next header</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Internet Control Message Protocol (ICMP)</td>
</tr>
<tr>
<td>6</td>
<td>Transmission Control Protocol (TCP)</td>
</tr>
<tr>
<td>17</td>
<td>User Datagram Protocol (UDP)</td>
</tr>
<tr>
<td>43</td>
<td>Routing header</td>
</tr>
<tr>
<td>44</td>
<td>Fragment header</td>
</tr>
<tr>
<td>58</td>
<td>Internet Control Message Protocol version 6 (ICMPv6)</td>
</tr>
<tr>
<td>59</td>
<td>Nothing; this is the final header</td>
</tr>
<tr>
<td>60</td>
<td>Destination Options header</td>
</tr>
<tr>
<td>89</td>
<td>Open Shortest Path First (OSPF)</td>
</tr>
</tbody>
</table>
- **Hop limit** This specifies the maximum number of hops that a packet may take before it is discarded (8 bits). This value is set by the source and decremented by one by each node that forwards the packet; the packet is discarded if the hop limit reaches zero. The comparable field in IPv4 is the time to live (TTL) field; it was renamed for IPv6 because the value limits the number of hops, not the amount of time that a packet can stay in the network.

- **Source address** This is the IPv6 address of the originator of the packet (128 bits).

- **Destination address** This is the IPv6 address of the intended recipients of the packet (128 bits) (Exhibit 1).

### IPv6 Header Format

**IPv6 Addresses**

To accommodate almost unlimited growth and a variety of addressing formats, IPv6 addresses are 128 bits in length. This address space is probably sufficient to uniquely address every molecule in the solar system.

IPv6 defines three types of addresses:

- A unicast address specifies a single host.

- An anycast address specifies a set of hosts, such as a set of FTP servers for a given organization. A packet sent to an anycast address is delivered to one of the hosts identified by that address, usually the “closest” one, as defined by the routing protocol.

- A multicast address also identifies a set of hosts; a packet sent to a multicast address is delivered to all the hosts in the group.

There is no broadcast address in IPv6 as in IPv4, because that function is provided by multicast addresses.

IPv4 addresses are written in dotted decimal notation, where the decimal value of each of the four address bytes is separated by dots. The preferred form of an IPv6 address is to write the hexadecimal value of the eight 16-bit blocks of the address, separated by colons (:), such as FF04:19:5:ABD4:187:2C:754:2B1. The leading zeros do not have to be written and each field must have some value.

IPv6 addresses often contain long strings of zeros because of the way in which addresses are allocated. A compressed address form uses a double colon (::) to indicate
multiple 16-bit blocks of zeros; for example, the address FF01:0:0:0:0:0:0:5A could be written as FF01::5A. To avoid ambiguity, the “::” can only appear once in an address.

An alternative, hybrid address format has been defined to make it more convenient to represent an IPv4 address in an IPv6 environment. In this scheme, the first 96 address bits (six groups of 16) are represented in the regular IPv6 format and the remaining 32 address bits are represented in common IPv4 dotted decimal; for example, 0:0:0:0:0:199.182.20.17 (or ::199.182.20.17).

**Address Prefix Allocation**

One of the goals of the IPv6 address format is to accommodate many different types of addresses. The beginning of an address contains a 3- to 10-bit format prefix defining the general address type; the remaining bits contain the actual host address, in a format specific to the indicated address type. This table represents an address prefix allocation (from RFC 1884):

<table>
<thead>
<tr>
<th>Allocation</th>
<th>Prefix (Binary)</th>
<th>Fraction of Address Space</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reserved</td>
<td>0000 0000</td>
<td>1/256</td>
</tr>
<tr>
<td>Unassigned</td>
<td>0000 0001</td>
<td>1/256</td>
</tr>
<tr>
<td>Reserved for NSAP Allocation</td>
<td>0000 001</td>
<td>1/128</td>
</tr>
<tr>
<td>Reserved for IPX Allocation</td>
<td>0000 010</td>
<td>1/128</td>
</tr>
<tr>
<td>Unassigned</td>
<td>0000 011</td>
<td>1/128</td>
</tr>
<tr>
<td>Unassigned</td>
<td>0000 1</td>
<td>1/32</td>
</tr>
<tr>
<td>Unassigned</td>
<td>0001</td>
<td>1/16</td>
</tr>
<tr>
<td>Unassigned</td>
<td>001</td>
<td>1/8</td>
</tr>
<tr>
<td>Provider-Based Unicast Address</td>
<td>010</td>
<td>1/8</td>
</tr>
<tr>
<td>Unassigned</td>
<td>011</td>
<td>1/8</td>
</tr>
<tr>
<td>Reserved for Geographic-Based Unicast Addresses</td>
<td>100</td>
<td>1/8</td>
</tr>
<tr>
<td>Unassigned</td>
<td>101</td>
<td>1/8</td>
</tr>
<tr>
<td>Unassigned</td>
<td>110</td>
<td>1/8</td>
</tr>
<tr>
<td>Unassigned</td>
<td>1110</td>
<td>1/16</td>
</tr>
<tr>
<td>Unassigned</td>
<td>1111 0</td>
<td>1/32</td>
</tr>
<tr>
<td>Unassigned</td>
<td>1111 10</td>
<td>1/64</td>
</tr>
<tr>
<td>Unassigned</td>
<td>1111 110</td>
<td>1/128</td>
</tr>
<tr>
<td>Unassigned</td>
<td>1111 1110 0</td>
<td>1/512</td>
</tr>
<tr>
<td>Link Local Use Addresses</td>
<td>1111 1110 10</td>
<td>1/1024</td>
</tr>
<tr>
<td>Site Local Use Addresses</td>
<td>1111 1111 11</td>
<td>1/1024</td>
</tr>
<tr>
<td>Multicast Addresses</td>
<td>1111 1111</td>
<td>1/256</td>
</tr>
</tbody>
</table>
The Provider-Based Unicast Address

The provider-based unicast address is an IPv6 address that might be assigned by an Internet service provider (ISP) to a customer. Exhibit 2 shows a provider-based unicast address format. This type of address contains a number of subfields, including the following:

- **Format prefix** This indicates the type of address as provider-based unicast. It is always 3 bits, coded “010.”

- **Registry identifier** This identifies the Internet address registry from which the ISP obtains addresses.
- **Provider identifier** This identifies the ISP. This field contains the address block assigned to the ISP by the address registry authority.

- **Subscriber identifier** This identifies the ISP’s subscriber. This field contains the address assigned to this subscriber by the ISP. The providerID and subscriberID fields together are 56 bits in length.

- **Intrasubscriber** This contains the portion of the address assigned and managed by the subscriber.

### Provider-Based Unicast Address Format

**IPv4-Compatible Addresses**

Another particularly important address type is the one that indicates an IPv4 address. With more than 16 million hosts using 32-bit addresses, the public Internet must continue to accommodate IPv4 addresses even as it slowly migrates to IPv6 addressing.

IPv4 addresses are carried in a 128-bit IPv6 address that begins with 80 zeros (0:0:0:0:0). The next 16-bit block contains the compatibility bits, which indicate the way in which the host/router handles IPv4 and IPv6 addresses. If the device can handle either IPv4 or IPv6 addresses, the compatibility bits are all set to zero (0) and this is termed an “IPv4-compatible IPv6 address”; if the address represents an IPv4-only node, the compatibility bits are all set to one (0xFFFF) and the address is termed an “IPv4-mapped IPv6 address.” The final 32 bits contain a 32-bit IPv4 address in dotted decimal form.

**Multicast Addresses**

IPv6 multicast addresses provide an identifier for a group of nodes. A node may belong to any number of multicast groups. Multicast addresses may not be used as a source address in IPv6 packets or appear in any routing.

All multicast addresses, as shown in Exhibit 3, begin with 8 ones (0xFF). The next 4 bits are a set of flag bits (flgs); the 3 high-order bits are set to zero; and the fourth bit (T-bit) indicates a permanently assigned (“well-known”) multicast address (T=0) or a nonpermanently assigned (“transient”) multicast address (T=1). The next 4 bits indicate the scope of the address, or the part of the network for which this multicast address is relevant; options include node-local (0x1), link-local (0x2), site-local (0x5), organization-local (0x8), or global (0xE).

**Multicast Address Format**

The remaining 112 bits are the group identifier, which identifies the multicast group, either permanent or transient, within the given scope. The interpretation of a permanently assigned multicast address is independent of the scope value. For example, if the World Wide Web (WWW) server group is assigned a permanent multicast address with a group identifier of 0x77, then:

- FF01:0:0:0:0:0:0:77 would refer to all WWW servers on the same node as the sender.
- FF02:0:0:0:0:0:0:77 would refer to all WWW servers on the same link as the sender.
- FF05:0:0:0:0:0:0:77 would refer to all WWW servers at the same site as the sender.
- FF0E:0:0:0:0:0:0:77 would refer to all WWW servers in the Internet.

Finally, a number of well-known multicast addresses are predefined, including:

- **Reserved multicast addresses** These are reserved and are never assigned to any multicast group. These addresses have the form FF0x:0:0:0:0:0:0:0, where x is any hexadecimal digit.

- **All nodes' addresses** These identify the group of all IPv6 nodes within the given scope. These addresses are of the form FF0t:0:0:0:0:0:0:1, where t =1 (node-local) or 2 (link-local).

- **All routers' addresses** These identify the group of all IPv6 routers within the given scope. These addresses are of the form FF0t:0:0:0:0:0:0:2, where t =1 (node-local) or 2 (link-local).

- **The dynamic host configuration protocol (DHCP) server/relay-agent address** This identifies the group of all IPv6 DHCP servers and relay agents with the link-local scope; this address is FF02:0:0:0:0:0:0:C.

**IPv6 Extension Headers and Options**

In IPv6, optional IP layer information is encoded in separate extension headers that are placed between the IPv6 basic header and the higher-layer protocol header. An IPv6 packet may carry zero, one, or more such extension headers, each identified by the next header field of the preceding header and each containing an even multiple of 64 bits (see Exhibit 4). A fully compliant implementation of IPv6 includes support for the following extension headers and corresponding options:

- **The hop-by-hop options header** This header carries information that must be examined by every node along a packet's path. Three options are included in this category. The pad1 option is used to insert a single octet of padding into the options area of a header for 64-bit alignment, whereas the padN option is used to insert two or more octets of padding. The jumbo payload option is used to indicate the length of the packet when the payload portion is longer than 65,535 octets. This option is employed when the payload length field is set to zero.

- **The routing header** This header is used by an IPv6 source to list one or more intermediate nodes that must be visited as part of the packet's path to the destination; this option is functionally similar to IPv4’s loose and strict source routing options. This header contains a list of addresses and an indication of whether each address is strict or loose. If an address is marked strict, it means that this node must be a neighbor of the previously addressed node; if an address is marked loose, this node does not have to be a neighbor of the previous node.

- **The fragment header** This header is used by an IPv6 source to send packets that are larger than the maximum transmission unit (MTU) on the path to the destination. This header contains a packet identifier, fragment offset, and final fragment indicator. Unlike IPv4, where fragmentation information is carried in every packet header, IPv6 only
carries fragmentation/reassembly information in those packets that are fragmented. In another departure from IPv4, fragmentation in IPv6 is performed only by the source and not by the routers along a packet's path. All IPv6 hosts and routers must support an MTU of 576 octets; it is recommended that path MTU discovery procedures (per RFC 1981) be invoked to discover, and take advantage of, those paths with a larger MTU.

- **The destination options header** This header carries optional information that has to be examined only by a packet's destination node(s). The only destination options defined so far are pad1 and padN, as described above.

- **The IP authentication header (AH) and IP encapsulating security payload (ESP)** These are IPv6 security mechanisms (a section on IPv6 security appears later in this article).

With the exception of the hop-by-hop option, extension headers are only examined or processed by the intended destination nodes. The contents of each extension header determine whether or not to proceed to the next header and, therefore, extension headers must be processed in the order that they appear in the packet.

### IPv6 Extension Header Examples

#### IPv6 Quality-of-Service (QOS) Parameters

The priority and flow label fields in the IPv6 header are used by a source to identify packets needing special handling by network routers. The concept of a flow in IP is a major departure from IPv4 and most other connectionless protocols; flows are sometimes referred to as a form of connectionless virtual circuit because all packets with the same flow label are treated similarly and the network views them as associated entities.

Special handling for nondefault quality of service is an important capability for supporting applications that require guaranteed throughput, end-to-end delay, and jitter, such as multimedia or real-time communication. These QOS parameters are an extension of IPv4's type-of-service (TOS) capability.

The priority field allows the source to identify the desired priority of a packet. Values 0 through 7 are used for congestion-controlled traffic, or traffic that backs off in response to network congestion, such as TCP segments. For this type of traffic, the following priority values are recommended:

- Zero is recommended for uncharacterized traffic.
- One is recommended for “filler” traffic (e.g., Netnews).
- Two is recommended for unattended data transfer (e.g., E-mail).
- Three is recommended for reserved traffic.
- Four is recommended for attended bulk transfer, such as FTP or hypertext transfer protocol (HTTP).
- Five is also recommended for reserved traffic.
Six is recommended for interactive traffic (i.e., telnet).

Seven is recommended for Internet control traffic (i.e., routing protocols and SNMP [simple network management protocol]).

Values 8 through 15 are defined for noncongestion-controlled traffic, or traffic that does not back off in response to network congestion, such as real-time packets being sent at a constant rate. For this type of traffic, the lowest priority value (8) should be used for packets that the sender is most willing to have discarded under congestion conditions (e.g., high-fidelity video traffic) and the highest value (15) should be used for those packets that the sender is least willing to have discarded (e.g., low-fidelity audio traffic).

The flow label is used by a source to identify packets needing nondefault QOS. The nature of the special handling might be conveyed to the network routers by a control protocol, such as the resource reservation protocol (RSVP), or by information within the flow packets themselves, such as a hop-by-hop option. There may be multiple active flows from a source to a destination, as well as traffic that is not associated with any flow (i.e., flow label=0). A flow is uniquely identified by the combination of a source address and a nonzero flow label. This aspect of IPv6 is still in the experimental stage and future definition is expected.

**IPv6 Security**

In the early days of TCP/IP, the ARPANET user community was small and close, and security mechanisms were not the primary concern. As the number of TCP/IP hosts grew, and the user community became one of strangers (some nefarious) rather than friends, security became more important. As critical and sensitive data travels on today's Internet, security is of paramount concern.

Although many of today's TCP/IP applications have their own devices, security should be implemented at the lowest possible protocol layer. IPv4 has few, if any, security mechanisms, and authentication and privacy at lower protocol layers is largely absent. IPv6 builds two security schemes into the basic protocol.

**IP Authentication Header**

The first mechanism is the IP authentication header (RFC 1826), an extension header that can provide integrity and authentication for IP packets. Although many different authentication techniques are supported, use of the keyed message digest 5 (MD5, described in RFC 1321) algorithm is required to ensure interoperability. Use of this option can eliminate a large number of network attacks, such as IP address spoofing. This option is also valuable in overcoming some of the security weaknesses of IP source routing.

IPv4 provides no host authentication. It can only supply the sending host's address as advertised by the sending host in the IP datagram. Placing host authentication information at the Internet layer in IPv6 provides significant protection to higher-layer protocols and services that currently lack meaningful authentication processes.

**IP Encapsulating Security Payload**

The second mechanism is the IP encapsulating security payload (ESP, described in RFC 1827), an extension header that can provide integrity and confidentiality for IP packets. Although the ESP definition is algorithm-independent, the Data Encryption Standard using cipher block chaining mode (DES-CBC) is specified as the standard encryption scheme to
ensure interoperability. The ESP mechanism can be used to encrypt an entire IP packet (tunnel-mode ESP) or just the higher-layer portion of the payload (transport-mode ESP).

These features add to the secure nature of IP traffic while actually reducing the security effort; authentication performed on an end-to-end basis during session establishment provides more secure communications even in the absence of firewall routers.

**ICMPv6**

The Internet control message protocol (ICMP) provides error and information messages that are beyond the scope of IP. ICMP for IPv6 (ICMPv6) is functionally similar to ICMP for IPv4 and also uses a similar message format and forms an integral part of IPv6. ICMPv6 messages are carried in an IPv6 datagram with a next header field value of 58.

ICMPv6 error messages include:

- **Destination unreachable** This is sent when a packet cannot be delivered to its destination address for reasons other than congestion.

- **Packet too big** This is sent by a router when it has a packet that it cannot forward because the packet is larger than the MTU of the outgoing link.

- **Time exceeded** This is sent by a router when the packet's hop limit reaches zero or if all fragments of a datagram are not received within the fragment reassembly time.

- **Parameter problem** This is sent by a node that finds some problem in a field in the packet header that results in an inability to process the header.

ICMPv6 informational messages are echo request and echo reply (used by IPv6 nodes for diagnostic purposes), as well as group membership query, group membership report, and group membership reduction (all used to convey information about multicast group membership from nodes to their neighboring routers).

**Migration to IPv6**

When IPv4 became the official ARPANET standard in 1983, use of previous protocols ceased and there was no planned interoperability between the old and the new. This is not the case with the introduction of IPv6.

Although IPv6 is currently being rolled out for the Internet backbone, there is no scheduled date of a flash cut from one to the other; coexistence of IPv4 and IPv6 is anticipated for many years to come. The sheer number of hosts using IPv4 today suggests that no other policy even begins to make sense. IPv6 will appear in the large ISP backbones sooner rather than later, and some smaller service providers and local network administrators will not make the conversion quickly unless they perceive some benefit from IPv6.

The coexistence of IPv4 and IPv6 in the network means that different protocols and procedures need to be accommodated. In one common short-term scenario, IPv6 networks will be interconnected via an IPv4 backbone (see Exhibit 5). The boundary routers will be IPv4-compatible IPv6 nodes and the routers' interfaces will be given IPv4-compatible IPv6 addresses. The IPv6 packet is transported over the IPv4 network by encapsulating the packet in an IPv4 header in a process is called tunneling. Tunneling can also be performed
when an organization has converted a part of its subnet to IPv6. This process can be used on host-host, router-router, or host-router links.

**Common Short-Term Scenario Where an IPv4 Network Interconnects IPv6 Networks**

Although the introduction of IPv6 is inevitable, many of the market pressures for its development have been rendered somewhat unnecessary because of parallel developments that enhance the capabilities of IPv4. The address limitations of IPv4, for example, are minimized by use of classless interdomain routing (CIDR). Nomadic user address allocation can be managed by the DHCP servers and relay agents. QOS management can be handled by the RSVP protocol. And the IP authentication header and encapsulating security payload procedures can be applied to IPv4 as well as to IPv6.

This is not meant to suggest that IP vendors are waiting. IPv6 has already started to appear in many new products and production networks. Support for IPv6 on several versions of UNIX have been announced by such organizations as Digital Equipment Corp., IBM Corp., INRIA (Institut National de Recherche en Informatique et en Automatique, or The French National Institute for Research in Computer Science and Control), Japan’s WIDE Project, Sun Microsystems, Inc., the Swedish Institute of Computer Science (SICS), and the US Naval Research Laboratory.

Other companies have announced support for IPv6 in other operating environments, including Apple Computer, Inc.’s MacOS, FTP Software, Inc.’s DOS/Windows, Mentat's STREAMS, Novell, Inc.’s NetWare, and Siemens Nixdorf, Inc.’s BS2000. Major router vendors that have announced support for IPv6 include Bay Networks, Inc., Cisco Systems, Inc., Digital Equipment Corp., Ipsilon Networks, Penril Datability Networks, and Telebit Corp.

**6bone Trials**

One of the important proving grounds of IPv6 is the 6bone, a testbed network spanning North America, Europe, and Japan, which began operating in 1996. The 6bone is a virtual network built on top of portions of today's IPv4-based Internet, designed specifically to route IPv6 packets. The goal of this collaborative trial is to test IPv6 implementations and to define early policies and procedures that will be necessary to support IPv6 in the future. In addition, it will demonstrate IPv6's new capabilities and will provide a basis for user confidence in the new protocol.

For most users, the transition from IPv4 to IPv6 will occur when the version of their host's operating system software is updated; in some cases, it means running dual-stacked systems with both versions of IP. For larger user networks, it may make sense to follow the model of the larger global Internet—in particular, to redesign the IPv6 network topology and addressing scheme, to build a testbed IPv6 network with routers and a DNS, and then slowly to migrate applications, users, and subnetworks to the new backbone. The lessons learned from the 6bone activity are useful for individual networks as well as for the Internet backbone.

**Conclusion**

The transition to IPv6 has already started, even though most Internet and TCP/IP users have not yet seen new software on their local systems or on local networks. Before IPv6
can be widely deployed, the network infrastructure must be upgraded to employ software that accommodates the new protocol.

In addition, the new address format must be accommodated by every TCP/IP protocol that uses addresses. The domain name system (DNS), for example, has defined an AAAA resource record for IPv6 128-bit addresses (IPv4’s 32-bit addresses use an A record) and the IP6.INT address domain (IPv4 uses the ARPA address domain). Other protocols that must be modified for IPv6 include dynamic host configuration protocol (DHCP), the address resolution protocol (ARP) family, and IP routing protocols such as the routing information protocol (RIP), open shortest path first (OSPF) protocol, and the border gateway protocol (BGP). Only after the routers and the backbones are upgraded will hosts start to transition to the new protocol and applications be modified to take advantage of IPv6’s capabilities.

Author Biographies

Gary C. Kessler
Gary C. Kessler is a senior member of technical staff and chief information officer at Hill Associates, a telecommunications training, education, and consulting firm located in Colchester VT. He is the coauthor of ISDN (New York: McGraw-Hill, 1996), author of more than 40 articles, and a frequent speaker at industry conferences. He can be reached via E-mail at kumquat@hill.com.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>Version number of the IP packet</td>
</tr>
<tr>
<td>Prio.</td>
<td>Prioritization of the packet</td>
</tr>
<tr>
<td>Flow Label</td>
<td>Flow label for DS tunneling</td>
</tr>
<tr>
<td>Payload Length</td>
<td>Length of the payload data</td>
</tr>
<tr>
<td>Next Header</td>
<td>Next header type</td>
</tr>
<tr>
<td>Hop Limit</td>
<td>Maximum number of hops</td>
</tr>
</tbody>
</table>

**Source Address**

**Destination Address**
Note:
The left-hand column represents a TCP segment encapsulated in IP without additional options, the middle column represents a TCP segment following a routing header, and the right-hand column represents a TCP segment fragment following a fragment header following a routing header.