IPv6: The Next Generation Internet Protocol

2. New Features in IPv6

Harsha Srinath

Harsha Srinath is currently pursuing his MS degree in Computer Science at the Center for Advanced Computer Studies (CACS) in University of Louisiana at Lafayette, USA. His research interests include networking with an emphasis on wireless networks, distributed databases and data mining.

Part 1, IPv4 and its shortcomings, *Resonance*, Vol.8, No.3, pp.33-41, 2003.

IPv4, the workhorse protocol of the currently popular TCP/IP protocol suite, is fast becoming obsolete. The exponential growth of the Internet is the main reason that has required the creation of the next generation of Internet Protocol-IPv6. IPv6 is much more flexible and promises to take care of the address space and security issues in the foreseeable future.

In this part we explain the new features introduced in the emerging Internet Protocol standard and why they have been introduced.

Keywords
Computer network, expanded addressing, new generation internet.

Birth of IPv6

As mentioned in Part 1[1] of the paper, the growth of the global Internet was exponential since its inception in the 1980's. The designers of this Internet Protocol (IPv4) never envisioned the scale of the Internet, nor could they imagine its potential for growth. Unfortunately, this unprecedented growth apart from benefiting millions of users was not without ill consequences. It posed a potential threat that a day might come when virtually all IP address are exhausted. Further, with increasing monetary transactions being done using the Internet, there was a need for more security features in the Internet Protocol.

A development of a potential solution for this problem began during the late 1990s.The creation of a new version of the Internet Protocol, IPv6, the next-generation Internet Protocol (IPng), was approved by the Internet Engineering Steering Group on November 17, 1994 as a proposed standard.

Since 1994, a large number of end-user organizations, standards groups, and network vendors have been working together on the

specification and testing of early IPv6 implementations. Standards work on IPv6 has now come so far that vendors have already committed to a considerable number of development and testing projects. All of the major router vendors have committed to adding IPv6 to their products.

With increasing monetary transactions being done using the Internet, there was a need for more security features in the Internet Protocol.

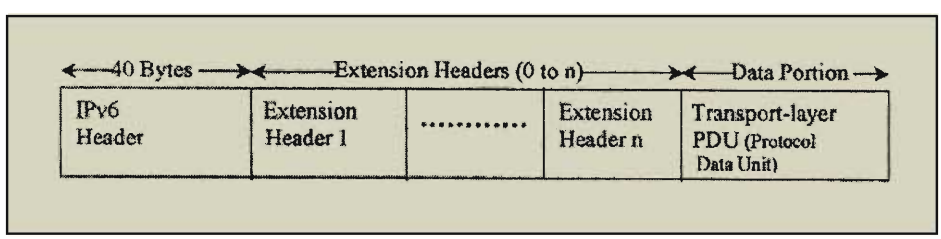
Internet Protocol Version 6.0

The best way to begin our study of IPv6 would be to start analyzing the datagram format of this protocol. This can then lead to a closer look at the header changes in IPv6 and finally the addressing format will complete our study of IPv6.

As *Figure* 1 shows, the most notable change in the IPv6 datagram format is its fixed header size of 40 bytes. This allows the network software developers to optimize the parsing of IPv6 headers along fixed boundaries. We will look at the fields of IPv6 in the following section. The elimination of the Options field that existed in IPv4 gave rise to the need for Extension Headers in IPv6. Following these optional extension headers, the IPv6 datagram will have the transport layer protocal data unit (PDU). IPv6 standards have defined the following Extension headers and recommends they be used in the following order (These headers are looked at closely later):

1. Hop-by-hop options header
2. Destination options header-1
3. Source routing header
4. Fragment header
5. Authentication header
6. Encryption header
7. Destination options header-2

Figure 1. Generic IP Datagram.



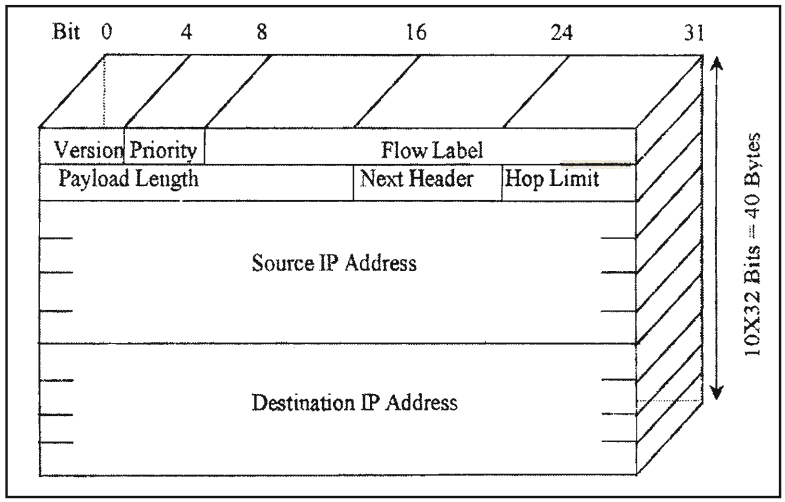


Figure 2. IPv6 (Primary) Header.

Ipv6 Header Structure

Figure 2 reveals the much-streamlined format of the IPv6. Many fields that existed in IPv4 have been dropped and some made optional. This simplified structure is expected to offset to a certain extent the bandwidth cost of the longer IP address of IPv6.

The fixed header size of 40 bytes in IPv6 has eliminated the header length field of IPv4. The time-to-live field of IPv4 has been renamed to the *hop limit* field in IPv6. Hop-limit value is decremented by one every router which forwards the packet. The hop-limit field is set to the appropriate value by the source node. When the value in the hop limit field is decremented to zero, the packet is discarded. The IPv6 hop limit field will store a value of up to 8 bits or 255 hops, which should be more than adequate for even the largest of networks.

The time-to-live field of IPv4 has been renamed to the *hop limit* field in IPv6.

The *Next Header* allows an arbitrary number of additional option headers to be appended to the primary IPv6 header. The fact that these headers are only optional makes packet transmission flexible. The *payload length field* contains almost the same information, as did the total length field in IPv4. The only difference being that this field does not include the length of the IPv6 header, which is 40 bytes. The new payload length field can

accommodate packets up to 64 KB in length. IPv6 routers will forward even larger packets, called *'jumbo-grams'*, if the payload length field is set to zero and a special extension header is added, as discussed below.

The other IPv4 header fields that have been eliminated are the service-type, fragment offset, identification, flags and checksum. The extension headers of IPv6 take care of all the work done by these older headers.

The new IPv6 fields: *flow label* and *priority* have taken over the functions of the older IPv4 service-type field. The optional extension headers (explained below) have taken over the work of the fragmentation headers of IPv4 viz., offset, identification, and flags fields. IP provides a connectionless and unreliable service that is; IP does not guarantee that all data will be delivered, or that the delivered data will arrive in the proper order. It is the responsibility of the next higher layer (usually TCP) or lower layers, to recover from any errors that occur. Thus, the IPv4 checksum field now stands abandoned in IPv6.

The Extension Headers of IPv6

The discarded options field of IPv4 was originally meant to carry information about source routing, security, and other optional parameters. IPv6 achieves all functions of the options field in a more reformed and systematic way by the use of *extension headers*. IPv6 extension headers are optional and provide a powerful means to support security, fragmentation, source routing, network management, and many other functions. An IPv6 packet can carry virtually any number of extension headers between the initial header and the higher layer payload.

IPv6 extension headers are optional and provide a powerful means to support security, fragmentation, source routing, network management, and many other functions.

The extension headers also impact the *protocol* field of the older IPv4 by using a *next header* field that indicates the protocol carried in the next extension or payload header. The IPv6 standards groups have already defined a number of extension headers and have also created a suggested (but not mandatory) guideline for the order of header insertion. We will briefly study

Presently, one such defined application of the hop-by-hop extension header is the Router Alert option, which is used to inform the router that it must process the packet completely before it can forward it to the next hop.

each of these extension headers to understand how they make IPv6 a much more powerful protocol compared to its predecessor.

1. Every router along the forwarding path will examine the *hop-by-hop options header*, when present. The most obvious use of such a feature would be to check routes, and transmit management commands to routers. Presently, one such defined application of the hop-by-hop extension header is the Router Alert option, which is used to inform the router that it must process the packet completely before it can forward it to the next hop.

2. The *destination options header* can occur either at the start or end in the chain of extension headers. When found at the start, (called *Destination options header-1*), it will be directly behind hop-by-hop options header (if any). This is used to carry information to the first destination listed in the address field. When found at the end (called *Destination options header-2*) of the extension header chain, it is used to carry information meant only for the final destination router.

3. *Source routing header* is an improved version of the *source routing* option of IPv4. This feature can be used to route the datagrams along user specified paths and helps to control the network traffic.

Figure 3 shows how the Source Routing Header can be used to route network traffic along specific paths. The dashed lines

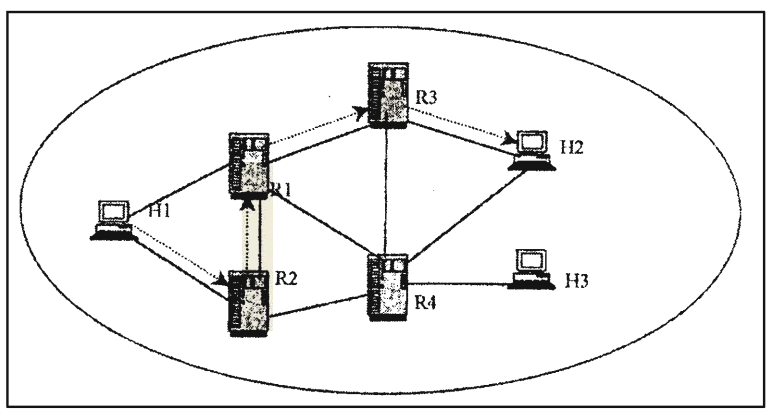


Figure 3. Source Routing Header used to route along specific paths.

indicate the specific path used to route datagrams. In the figure, although H2 (Host2) can be reached through R4 (Router4) we send the datagrams through R3.

The intermediate nodes cannot fragment IPv6 packets, improving the router performance and reducing the network traffic.

4. IPv4 allows fragmentation anywhere along the path of a datagram depending on the capacity of the intermediate links. This fragmentation and reassembly along the path is clearly an overhead and has been curtailed to the source and ultimate destination in IPv6.The intermediate nodes cannot fragment IPv6 packets, improving the router performance and reducing the network traffic. Most of the present networks have the ability to transmit large packets. But in unusual cases where fragmentation is inevitable, we make use of the *fragmentation header*. A node uses a path discovery algorithm to find the MTU (Maximum Transmission Unit). Using this, the source node will fragment, as needed for the appropriate destination address.

The next two extension headers can be the subjects of much discussion because of the lack of standardized network layer level security in IPv4. In the current discussion we will focus only on the main features of IPv6 that makes it much more secure compared to its predecessor.

5. The *authentication header* is used to guarantee network applications that the data they receive is from the original sender. In the earlier version of IP, we had frequent occurrences of hacking and other kinds of unauthorized access. Such malicious accesses have often caused huge losses to many corporations. IPv6 prevents all such security issues by using the authentication header.

Using IPv6 authentication headers, hosts can establish a standards-based security understanding using algorithm-independent secret keys. Both the sender and the receiver agree upon using a key. The sender forms a checksum and sends it in the authentication header. This checksum is verified on the receiver side using the secret key, thus authenticating the sender.

The *authentication header* is used to guarantee network applications that the data they receive is from the original sender.

6. The *encryption header* is also called the Encapsulating Security Payload (ESP) service of IPv6. Along with the authentication

The IPv6 addresses are assigned to individual interfaces on nodes, not to the nodes themselves as in IPv4. The interfaces can also have multiple IP addresses.

header, this encryption header can be used to provide very high level of privacy and integrity. This feature is a boon to all application level programs since they can use this network layer level encryption and streamline their security features. Non-disruptive reading also called sniffing and snooping that was rampant in IPv4, can be blocked using the encryption header. But more importantly, these headers provide security against disruptive reading (hacking) and thus make IPv6 even secure.

Addressing Architecture of IPv6

IPv6's addressing has been the topic of considerable IP research recently. As with the security issues of IP, in the present discussion, the addressing features have been dealt only in an abstract level bearing in mind an audience of varied backgrounds. The Suggested Reading will be useful to those who want to explore this further.

The IPv6 addresses are assigned to individual interfaces on nodes, not to the nodes themselves as in IPv4. The interfaces can also have multiple IP addresses (a similar concept is present in multi-homed hosts in IPv4). This would permit a subscriber using multiple access providers across the same interface to have separate addresses aggregated under each provider's address space.

Primarily, IPv6 has three kinds of addressing formats viz., Unicast address format, Multicast address format and Anycast address format

1. Unicast address format: This kind of addressing is used to reach individual interfaces and this format is further divided into five types.

a. *Provider-based global unicast addressing* is used for global addressing across the entire universe of connected hosts.

b. *Link-local unicast addresses* are to be used for addressing on a single link or sub-network.

c. Although *Site-local address format* is used for local addressing,

it can be integrated into the global addressing scheme. This scheme can reduce burden on global network traffic since such addresses can be used immediately by an organization that expects to transition to the use of global addresses only later.

d. One of the most important challenges for IPv6 is the transition from IPv4 to IPv6. During the transition, there will be a point when both formats co-exist and IPv4-compatible IPv6 format is expected to play a important role during this period. This format supports a technique known as automatic tunneling that can to be used forward such traffic through IPv4 routing topologies.

e. As in IPv4, IPv6 supports a *loopback address format* that can be used by a node to send an IP packet to itself. Symbolically this address can be represented as 0:0:0:0:0:0:0:1.Generally, IPv6 addresses are represented as x:x:x:x:x:x:x:x, where each x is the hexadecimal value of a 16-bit portion of the address.

2. Multicast address format: One of the drawbacks of IPv4 was that time sensitive data was difficult to negotiate during times of heavy network traffic. *Multicast addressing format* overcomes the problem to some extent by using 'multicast groups'. A new member becomes part of a multicast group by sending a 'join' message to a nearby router. A multicast server sends the usually time sensitive data to suitable host/hosts. A multicast-capable network can automatically replicate the server's packets and route them to each destination in the multicast group using an efficient path. This forwarding is done only as needed and thus saves network resources compared to IPv4.

3. Anycast address format: Concept wise, anycast address format has some features of both unicast and multicast. An 'anycast group' will consist of two or more interfaces on a group of nodes. A packet addressed to the group's anycast address is delivered to only one of the interfaces, typically the 'nearest' interface in the group, according to current routing protocol metrics. This is in contrast with multicast services, which deliver packets to all members of the multicast group. This new IP feature promises

One of the drawbacks of IPv4 was that time sensitive data was difficult to negotiate during times of heavy network traffic. *Multicast addressing format* overcomes the problem to some extent by using 'multicast groups'.

considerable improvements in network traffic control.

Transition to IPv6 and Conclusions

The most obvious question that arises would be the shift from IPv4 to IPv6. IPv6 surely promises a lot of new avenues for research and technological developments in the field of computer communications. But, like any new technology, IPv6 also throws open new problems and challenges. As such, it would be unjust to expect a quick and trouble free transition.

The upgrading process must be flexible enabling the network administrators to make incremental changes to the existing IPv4 networks. Also, the cost of building new IPv6 networks must not be high compared to building an IPv4 network. To facilitate transition, the IETF has set up a work group called NGTRANS (Next Generation TRANSition). One of the main problems considered by the NGTRANS is that during the process it is crucial for IPv6 to co-exist with IPv4 until the transition is complete. A considerable number of transition mechanisms like *Dual Stack* and *Tunneling* have already been put forward in this regard.

Acknowledgements

I thank Dr Y Narahari, Dr S S Iyengar, Mr C J Jagadeesha for support and help.

Suggested Reading

[1] W Richard Stevens, *TCP/IP Illustrated*, Pearson Asia, 2001.
[2] Andrew S Tanenbaum, *Computer Networks*, 3rd Edition, Prentice Hall of India, 2000.
[3] E Britton, J Tavs, and R Bournas, TCP/IP: The Next Generation, *IBM Sys. J.*, No. 3, 1995.
[4] S Bradner and A Mankin, *IPng: Internet Protocol Next Generation*, Reading, MA: Addison-Wesley, 1996.
[5] C Huitema, *IPv6: The New Internet Protocol*, Prentice Hall, 1996.
[6] Vasudev Navellar, *IPv6 Transition Mechanisms*, IIT, Kanpur, April 1999. [URL:http://www.cse. iitk.ac.in/users/dheeraj/reports/ipv6-trans.ps.gz]
[7] http://www.ietf.org/ (RFC's 2460,1933)

Address for Correspondence
Harsha Srinath
#44, 'Dwaraka'
39th Cross
Jayanagar 8th Block
Bangalore 560082, India.
Email:
harshasrinath@hotmail.com