

SFWR ENG 4C03 Research Project

Emergence of new Internet Protocol Standard (IPv6)

Researcher: Ramez Mousa, 0055465 - Revision Date: March 29, 2004

1.0 Need for IPv6

Currently, the Internet Protocol in use is IPv4. IPv4 has been around since the late 1970s and has remained almost unchanged since its inception. This clearly demonstrates that the design is powerful and flexible. However, LAN technologies have greatly improved and the number of hosts on the Internet has skyrocketed in the past few years. In fact, reports indicate that a new host appears on the Internet every minute. Consequently, the current 32-bit IP address space employed with IPv4 can no longer accommodate the rapid growth of the Internet and it is expected to be completely exhausted by the year 2010. Moreover, IPv4 did not provide sufficient security features. Thus, IPv6 with a 128-bit IP address space and enhanced security features, have emerged.

2.0 New features provided by IPv6

2.1 Larger Addresses

The most significant and noticeable new feature offered by IPv6 is the larger address space. The size of the IPv6 address space is 128-bit, which is four times as large as the 32-bit address space of IPv4. This allows as many as 256 billion address spaces for internet users, which is 64 times as much as the address space provided by IPv4. Thus, IPv6 has sufficient address space to handle the growth of the Internet for decades to come. Moreover, this abundance of address space allows many more devices such as cell phones and PDAs (Personal Data Assistants), and even IP phones in the near future, connection to the internet without any limitations.

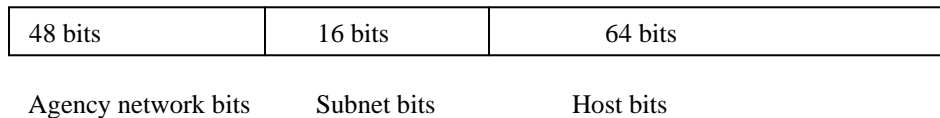
2.2 Enhanced Security Features

IPv6 has many new built-in security features over its predecessor IPv4. IPv6 comes with a function called IPsec which provides two different extension headers that are used to enhance authentication and security. The first extension header is the Authentication Header which provides host authentication. Host authentication increases the security level and helps prevent host masquerading attacks and maintain data integrity. The second extension header is the IP Encapsulating Security Payload (ESP). ESP allows a datagram to be transmitted confidentially from the source to the destination. The source can encapsulate the datagram and encrypt the packet. A new clear text header is then attached to the ESP. When the destination receives the packet, it discards the clear text header, decrypts the ESP, and process the ESP header. At that point, the data may be accessed as normal.

2.3 Extended Address Hierarchy

IPv6 uses the larger address space to create additional levels of addressing hierarchy. It is based on a 3 level hierarchy, whereas IPv4 used a 2 level hierarchy. The top level identifies the agency the address is registered with and the provider of the address. The next level identifies the subnet address and the lowest level identifies the specific host. This technique is called subnet addressing and allows a single network to span multiple physical networks. Moreover, IPv6 can define a hierarchy of ISPs as well as a hierarchical structure within a given site allowing each site to customize the IP address according to the

number of hosts and sub-networks on the site. The following is an illustration of the IPv6 address format.



2.4 Support for Autoconfiguration And Renumbering

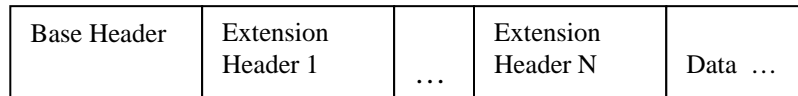
IPv6 provides facilities that allow computers on an isolated network to assign themselves addresses and begin communicating without requiring administrators to manually assign the address to be used. Once a host is connected to the internet, they are assigned an address automatically and are instantly connected to the internet, similar to plug and play. Moreover, the protocol also includes a facility that permits a manager to renumber networks dynamically.

2.5 Provision for Protocol Extension

A very significant new feature added to IPv6 is that it easily allows for future changes. IPv4 is a protocol that fully specifies all details of the underlying network. Thus it restricts its users from making any changes to the network. IPv6 on the other hand, is a protocol that can easily permit additional features since it does not specify all the details of the underlying network. It also has an extension capability that allows the IETF (Internet Engineering Task Force) to adapt the protocol to changes in underlying network hardware or to new applications.

3.0 IPv6 Datagram

The IPv6 datagram has been completely redesigned and is quite different from its IPv4 predecessor. An IPv6 datagram has a fixed size base header followed optional extension headers.



IPv6 Datagram: only the base header is necessary. Extension headers are optional.
Obtained from Comer, p. 603.

3.1 IPv6 Base Header Format

The following is an illustration of the IPv6 header. It contains less information and been greatly simplified from the IPv4 datagram header.



Format of the IPv6 base header. Obtained from Comer, p.604

The following is a brief explanation of the purpose of each field.

- Version field specifies the version of the protocol being used. For IPv6, the version field contains a 6.
- Traffic class indicates the priority of this packet, relative to other packets from the same source. Higher priority packets will be transmitted first.
- The 24-bit Flow Label field in the IPv6 header may be used by a source to label sequences of packets for which it requests special handling by the IPv6 routers, such as non-default quality of service or "real-time" service.
- Payload length field specifies the number of octets carried in the datagram excluding the header itself.
- Next Header identifies the type of header immediately following the current header. This allows the receiving application to determine if this is the last header to expect or if there are more extension headers to receive.
- Hop Limit gives a strict bound on the maximum number of hops a datagram can make before being discarded.
- Source Address and Destination Address give the 128-bit IPv6 source and destination address of the transmitted header.

3.2 IPv6 Extension Headers

IPv6 extension headers are similar to IPv4 options. Each datagram includes extension headers for only those facilities that the datagram uses. Essentially, IPv6 has moved the options and some of the fixed fields that appear in an IPv4 datagram header to extension headers. This modification provides IPv6 the required mechanisms to support functions such as fragmentation, source routing, and authentication (as discussed above under IP security), while greatly simplifying the base header. Moreover, this modification is much more efficient because most datagrams do not use all these functionality. Thus, it is much more efficient to exclude them from the base header and include them in extension headers whenever necessary.

3.3 IPv6 Source Routing

IPv4 provides the sender the ability to specify a loose source route whereby the source specifies that the datagram must visit one or more intermediate nodes on the way to its destination. IPv6 retained this ability; however it uses a separate extension header for source routing when IPv4 offered it through the options field. As described above, such a modification is an improvement since most datagrams do not use this functionality; therefore, it is more efficient to include them in extension headers, where they may be used when necessary.

4.0 Final Remarks

IPv6 includes many new and useful features over its predecessor IPv4. Most significantly, it has a much larger address space that is capable to handle the growth of the internet for decades to come. IPv6 also provides features such as an extended address hierarchy, support for autoconfiguration and renumbering, and provision for protocol extension. All these features were not available through IPv4 and are very useful to IPv6 users. The transition between IPv4 and IPv6 is still in the early stages. However, some countries such as Japan have taken the initiative and have begun adapting the new protocol. It appears very likely that many other countries will follow and adapt IPv6 as it is the future of Internet Protocol.

4.0 References

Comer, Douglas E. INTERNETWORKING with TCP/IP: Principles, Protocols, and Architectures, 4th Edition. New Jersey: Prentice Hall, 2000.

Deering & Hinden. Network Working Group: “IPv6 Specification”.
<ftp://ftp.isi.edu/in-notes/rfc2460.txt>. Last accessed: March 29, 2004.

Goodin, Dan. The Wall Street Journal Online: “New Net Traffic Snarled”.
<http://zdnet.com.com/2100-11-529686.html>. Last accessed: March 29, 2004.

R. Hinden. “IP version 6”. <http://playground.sun.com/pub/ipng/html/ipng-main.html>. Last accessed: March 29, 2004.