Transition of Ipv4 to Ipv6

By

Anita Kanuganti

Hemanth Rao

Under The Able
Guidance Of Professor
Dr.Mohamed Khalil

Abstract: The Internet Engineering Task force began an effort to develop a successor to the IPv4 protocol. A prime motivation for this effort was the realization that the 32-bit IP address space was beginning to be used up, with new networks and IP nodes being attached to the internet(and being allocated unique IP addresses) at a breathtaking rate. To respond to this need for a large IP address space, a new IP protocol was developed. But as the saying goes, that every action has a equal and opposite reaction, this solution lead to a more serious problem, of how to make this transition of changing all the IPv4 enabled nodes into IPv6 enabled nodes.
The different methods in which these transitions can be implemented is the main point of discussion in this paper. We will discuss all the methods and their respective advantages and disadvantages. We will also give a brief description of the IPv6 Protocol.

I. Introduction

The format of the IPv6 packet is shown in the below described figure.

Version	Traffic Class	Flow label	
Payload		Next Hdr	Hop limit
Source Address (128 bits)			
Destination Address (128 bits)			
Data			

Expanded addressing capabilities: IPv6 increases the size of the IP address from 32 to bits to 128 bits. In addition to unicast and multicast address, it also implements a new type of address called the any cast address. This allows a packet addressed to an any cast address to be delivered to any one of group of hosts. The IPv6 datagram has the following fields defined.

1. *Version* This four bit field identifies the IP version number. The IPv6 carries a value of "6" in this field. Note that putting a "4" in this field does not create a valid IPv4 datagram.
2. *Traffic Class* The eight-bit field is similar in spirit to the ToS field that we saw in the IPv4
3. *Flow label* This 20 bit field is used to identify a "flow" of data grams
4. *Payload length* This 16 bit value is treated as an unsigned integer giving the number of bytes in the IPv6 data grams following the fixed length, 40 byte packet header.
5. *Next header* This field identifies the protocol to which the contents (data field) of this datagram will be delivered. The field uses the same value as the protocol field in the IPv4 header.
6. *Hop limit* The contents of this field are decremented by one by each router that forwards the datagram. If the hop limit count reaches zero, the datagram is discarded.
7. *Source destination address* The various formats of the IPv6 128 bit address
8. *Data* This is the payload portion of the IPv6 datagram.

There is also a new ICMP for IPv6. The ICMP message is used by IP nodes to report error conditions and provide limited information for the end system. A new version of the ICMP has been developed

for IPv6. This is discussed in the RFC 2463. In addition to reorganizing the existing ICMP type and code definitions, ICMPv6 also added new types and codes required by the new IPv6 functionality. These include the “Packet too big” type and many more.

II. Requirements for Smooth Transitions

When we talk about the transition from IPv4 to IPv6, we have to take into consideration every component in the network.
What we exactly mean here is that, every node, every router in the network must be made IPv6 compatible. But that does not mean that they will be losing their IPv4 datagram processing capabilities.

The actual transition process from IPv4 to IPv6 can be compared to the migration processes of smaller scale that take place all the time. Operating system and software development environment version changes are good examples of such migration. The main constraints set for the IPng transition should be generally the same as in any smaller scale migration. However, for the global Internet community the fulfillment of the constraints is much more important, and few shortcuts can be tolerated.

Constraints for the Transition:

Step wise transition: We are already aware of that the transition cycle will take years and there is no way to synchronize the process on different sites. A distributed approach is necessary. Presumably only the smallest user organizations are able to switch over to IPv6 in a single step. All others must be able to make their own staged transition plan, and proceed in it with as few interdependencies as possible. IPv4 and IPv6 network equipment must be allowed to coexist and interoperate. It should even be realized that some old, small-scale systems may never be capable of running IPv6. They will maintain the old protocol suite in the network to the end of the old hardware usage time

Coexistence and internetworking: The transition independency means that the order of migration on unique computers and network devices is not tied to the upgrade of some other systems in the network. The release dates of new computer systems, routers and application software cannot be commonly synchronized. Old equipment and software will be used in the network while the IPng-based systems and applications are deployed. The old systems should run without modifications and be able to communicate with both the old and new systems. In practice this means a strict requirement for simultaneous support for both IPv4 and IPv6 on all new systems.

Feasible address mapping scheme: IPng brings the advantage of a very large address space where even multiple addresses can be easily reserved for each host. In addition to the complex scheme of 128-bit IPv6 address distribution, a simplified method is necessary. To make the transition process easier an optional simple mapping from an old IPv4 address is desirable. Since it is not possible to assume that all IPv4 addresses used are globally unique, the mapping may be site-specific in some cases instead of a fixed prefix.

Smart management tools: During the transition and existence of dual protocol networks the demand for a whole set of management tools is clear. The new tools must be clever enough to separate IPv4 and IPv6 characteristics on multiple levels. Detection of different routes and possible translation points must be implemented. A mechanism for checking the IPng