IPv6 - The Future is Forever

Seminar Topic

Submitted in partial fulfilment of
the course

CS497S : SEMINAR

Submitted by

Dhandeep M Lodaya
B080569CS

Department of Computer Science & Engineering
National Institute of Technology Calicut
Kerala - 673601
Monsoon 2011

ABSTRACT

Internet Protocol version 6 (IPv6) is the current version of the Internet Protocol. It is designed to succeed the older Internet Protocol (IPv4). The growth of the Internet has created a need for more addresses than are possible with IPv4, hence the IPv6 version known to never exhaust. IPv6 with 10^{29} times the number of IPv4 addreses, boasts the Future Forever.

IPv6 in DNS, Address format, IPv4- IPv6 mapping, Tunneling and Deployment are the major topics discussed under IPv6.

REPORT

Internet Protocol version 6 (IPv6) is a version of the Internet Protocol (IP). It is designed to succeed the Internet Protocol version 4 (IPv4).IP (the Internet Protocol) is one of the most important protocols for networks, including the Internet. It is responsible for identifying each machine on the network by a unique address (the IP address) and routing data packets from their source to their destination machine through this addressing. The actual version of the IP protocol being used is IPv4 (IP version 4).

1 The Limitations of IPv4

The structure of a current IP (IPv4) address is four numbers ranging between 0 and 255, each separated by a dot. An example is 192.168.66.1; since each number is represented in binary by an 8-bit word, an IPv4 address is made up of 32 binary digits (bits). The maximum number you can make with 32 bits is 4.3 billion (2 raised to power 32).

Each machine on the Internet should have a unique IP address - no two machines can have the same address. This therefore means that the Internet can theoretically hold only 4.3 billion machines, which is quite a lot. But in the early days of IP, due to lack of vision and some business flair, many IP addresses were squandered. They were sold to companies, which underutilize them. They cannot be claimed back. Some others have been restricted to purposes other than public use, like research, technology-related uses etc. The remaining addresses are dwindling and, considering the amount of user computers, hosts and other devices that are connected on the Internet, we will soon run out of IP addresses! During the first decade of operation of the Internet (by the late 1980s), it became apparent that methods had to be developed to conserve address space. In the early 1990s, even after the redesign of the addressing system using a classless network model, it became clear that this would not suffice to prevent IPv4 address exhaustion, and that further changes to the Internet infrastructure were needed. and hence the concept of PAT(Port address translation) was introduced,[widely knows as NAT(Network Address Translation)]. The simplest type of NAT provides a one to one translation of IP addresses. RFC 2663 refers to this type of NAT as basic NAT. It is often also referred to as one-to-one NAT. In this type of NAT only the IP addresses, IP header checksum and any higher level checksums that include the IP address need to be changed. The rest of the packet can be left untouched (at least for basic TCP/UDP functionality, some higher level protocols may need further translation). Basic NATs can be used when there is a requirement to interconnect two IP networks with incompatible addressing.

2 NAT

However it is common to hide an entire IP address space, usually consisting of private IP addresses, behind a single IP address (or in some cases a small group of IP addresses) in another (usually public) address space. To avoid ambiguity in the handling of returned packets, a one-to-many NAT must alter higher level information such as TCP/UDP ports in outgoing communications and must maintain a translation table so that return packets can be correctly translated back. RFC 2663 uses the term NAPT (network address and port translation) for this type of NAT. Other names include PAT (port address translation), IP masquerading, NAT Overload and many-to-one NAT. Since this is the most common type of NAT it is often referred to simply as NAT.

In the mid-1990s NAT became a popular tool for alleviating the consequences of IPv4 address exhaustion. It has become a common, indispensable feature in routers for home and small-office Internet connections. Most systems using NAT do so in order to enable multiple hosts on a private network to access the Internet using a single public IP address.

Network address translation has serious drawbacks on the quality of Internet connectivity and requires careful attention to the details of its implementation. In particular all types of NAT break the originally envisioned model of IP end-to-end connectivity across the Internet and NAPT makes it difficult for systems behind a NAT to accept incoming communications. As a result, NAT traversal methods have been devised to alleviate the issues encountered.

3 IPv6's Birth

By the beginning of 1992, several proposals appeared and by the end of 1992, the IETF announced a call for white papers.The Internet Engineering Task Force adopted the IPng model on July 25, 1994, with the formation of several IPng working groups. By 1996, a series of RFCs was released defining Internet Protocol version 6 (IPv6), starting with RFC 1883 IPv6 Described

IPv6 specifies a new packet format, designed to minimize packet header processing by routers. Because the headers of IPv4 packets and IPv6 packets are significantly different, the two protocols are not interoperable. However, in most respects, IPv6 is a conservative extension of IPv4. Most transport and application-layer protocols need little or no change to operate over IPv6;

4 Larger address space

The most important feature of IPv6 is a much larger address space than in IPv4. The length of an IPv6 address is 128 bits, compared to 32 bits in IPv4. The address space therefore supports 2128 or approximately 3.41038 addresses. As a small example of the potential in the new protocol there is a quote in one of Microsofts articles written by a Joseph Davies 6.6 x 10 addresses for every square meter of the Earths surface. The exact number of IPv6 addresses available is.

340,282,366,920,938,463,463,374,607,431,768,211,456

By comparison, this amounts to approximately $5*10^{28}$ addresses for each of the 6.8 billion people alive in 2010. In addition, the IPv4 address space is poorly allocated, with approximately 14% of all available addresses utilized. While these numbers are large, it was not the intent of the designers of the IPv6 address space to assure geographical saturation with usable addresses. Rather, the longer addresses simplify allocation of addresses, enable efficient route aggregation, and allow implementation of special addressing features.

5 Multicasting

Multicasting, the transmission of a packet to multiple destinations in a single send operation, is part of the base specification in IPv6. In IPv4 this is an optional although commonly implemented feature. IPv6 multicast addressing shares common features and protocols with IPv4 multicast, but also provides changes and improvements by eliminating the need for certain protocols. IPv6 does not implement traditional IP broadcast, i.e. the transmission of a packet to all hosts on the attached link using a special broadcast address, and therefore does not define broadcast addresses. In IPv6, the same result can be achieved by sending a packet to the link-local all nodes multicast group at address ff02::1, which is analogous to IPv4 multicast to address 224.0.0.1. IPv6 also supports new multicast solutions, including embedding rendezvous point addresses in an IPv6 multicast group address which simplifies the deployment of inter-domain solutions.

6 Mandatory support for network layer security

Internet Protocol Security (IPsec) was originally developed for IPv6, but found widespread deployment first in IPv4, into which it was back-engineered. IPsec is an integral part of the base protocol suite in IPv6. IPsec support is mandatory in IPv6 but optional for IPv4.

7 Simplified processing by routers

In IPv6, the packet header and the process of packet forwarding have been simplified. Although IPv6 packet headers are at least twice the size of IPv4 packet headers, packet processing by routers is generally more efficient, thereby extending the end-to-end principle of Internet design. Specifically:
The packet header in IPv6 is simpler than that used in IPv4, with many rarely used fields moved to separate optional header extensions. IPv6 routers do not perform fragmentation. IPv6 hosts are required to either perform path MTU discovery, perform end-to-end fragmentation, or to send packets no larger than the IPv6 default minimum MTU size of 1280 octets. The IPv6 header is not protected by a checksum; integrity protection is assumed to be assured by both link layer and higher layer (TCP, UDP, etc.) error detection Therefore, IPv6 routers do not need to recompute a checksum when header fields (such as the time to live (TTL) or hop count) change.
The TTL field of IPv4 has been renamed to Hop Limit, reflecting the fact that routers are no longer expected to compute the time a packet has spent in a queue.

8 Mobility

Unlike mobile IPv4, mobile IPv6 avoids triangular routing and is therefore as efficient as native IPv6. IPv6 routers may also support network mobility which allows entire subnets to move to a new router connection point without renumbering.

9 Packet format

The IPv6 packet is composed of two parts: the packet header and the payload. The header consists of a fixed portion with minimal functionality required for all packets and may contain optional extension to implement special features. The fixed header occupies the first 40 octets (320 bits) of the IPv6 packet. It contains the source and destination addresses, traffic classification options, a hop counter, and a pointer for extension headers if any. The Next Header field, present in each extension as well, points to the next element in the chain of extensions. The last field points to the upper-layer protocol that is carried in the packet's payload.
Extension headers carry options that are used for special treatment of a packet in the network, e.g., for routing, fragmentation, and for security using the IPsec framework. The payload can have a size of up to 64KB without special options, or larger with a jumbo payload option in a Hop-By-Hop Options extension header.
Unlike in IPv4, fragmentation is handled only in the end points of a communication session; routers never fragment a packet, and hosts are expected to use Path MTU Discovery to select a packet size that can traverse the entire communications path.

10 Addressing

IPv6 addresses are written in eight groups of four hexadecimal digits separated by colons, for example, $2001 : 0db8 : 85a3 : 0000 : 0000 : 8a2e : 0370 : 7334$. IPv6 unicast addresses other than those that start with binary 000 are logically divided into two parts: a 64-bit (sub-)network prefix, and a 64-bit interface identifier.
For stateless address autoconfiguration (SLAAC) to work, subnets require a /64 address block as defined in RFC 4291section 2.5.1. Local Internet registries get assigned at least /32 blocks, which they divide among ISPs. The obsolete RFC 3177 recommended the assignment of a /48 to end consumer sites. This was replaced by RFC 6177, which "recommends giving home sites significantly more than a single /64, but does not recommend that every home site be given a /48 either." /56s are specifically considered. It remains to be seen if ISPs will honor this recommendation; for example, during initial trials Comcast customers have been given a single /64 network.
IPv6 addresses are classified by three types of networking methodologies: unicast addresses identify each network interface, anycast addresses identify a group of interfaces, usually at different locations of which the nearest one is automatically selected, and multicast addresses are used to deliver one packet to many interfaces. The broadcast method is not implemented in IPv6. Each IPv6 address has a scope, which specifies in which part of the network it is valid and unique. Some addresses are unique only on the local (sub-)network; Others are globally unique. Some IPv6 addresses are reserved for special purposes, such as the address for loopback, 6to4 tunneling, Teredo tunneling and several more. See RFC 5156. Also, some address ranges are considered special, such as link-local addresses for use on the local link only, Unique Local addresses (ULA) as described in RFC 4193 and solicited-node multicast addresses used in the Neighbor Discovery Protocol.

11 Address Format

IPv6 addresses have two logical parts: a 64-bit network prefix, and a 64-bit host address part. (The host address is often automatically generated from the interface MAC address.) An IPv6 address is represented by 8 groups of 16-bit hexadecimal values separated by colons (:) shown as follows:
A typical example of an IPv6 address is $2001 : 0db8 : 85a3 : 0000 : 0000 : 8a2e : 0370 : 7334$
The hexadecimal digits are case-insensitive.
The 128-bit IPv6 address can be abbreviated with the following rules:

Rule 1: Leading zeroes within a 16-bit value may be omitted. For example, the address $fe80 : 0000 : 0000 : 0000 : 0202 : b3ff : fe1e : 8329$ may be written as $fe80 : 0 : 0 : 0 : 202 : b3ff : fe1e : 8329$

Rule 2: One group of consecutive zeroes within an address may be replaced by a double colon. For example,$fe80 : 0 : 0 : 0 : 202 : b3ff : fe1e : 8329$ becomes $fe80 :: 202 : b3ff : fe1e : 8329$
A single IPv6 address can be represented in several different ways, such as $2001 : db8 :: 1 : 0 : 0 : 1$ and $2001 : 0DB8 : 0 : 0 : 1 :: 1$. RFC 5952 recommends a canonical textual representation.

12 Dual IP stack implementation

The dual-stack protocol implementation in an operating system is a fundamental IPv4-to-IPv6 transition technology. It implements IPv4 and IPv6 protocol stacks either independently or in a hybrid form. The hybrid form is commonly implemented in modern operating systems supporting IPv6. Dual-stack hosts are described in RFC 4213.
Modern hybrid dual-stack implementations of IPv4 and IPv6 allow programmers to write networking code that works transparently on IPv4 or IPv6. The software may use hybrid sockets designed to

accept both IPv4 and IPv6 packets. When used in IPv4 communications, hybrid stacks use an IPv6 application programming interface and represent IPv4 addresses in a special address format, the IPv4-mapped IPv6 address. IPv4-mapped IPv6 addresses Hybrid dual-stack IPv6/IPv4 implementations support a special class of addresses, the IPv4-mapped IPv6 addresses. This address type has its first 80 bits set to zero and the next 16 set to one, while its last 32 bits are filled with the IPv4 address. These addresses are commonly represented in the standard IPv6 format, but having the last 32 bits written in the customary dot-decimal notation of IPv4; for example, ::ffff:192.0.2.128 represents the IPv4 address 192.0.2.128. It substitutes the old and deprecated IPv4-compatible IPv6 address formed by ::192.0.2.128.

Because of the significant internal differences between IPv4 and IPv6, some of the lower level functionality available to programmers in the IPv6 stack do not work identically with IPv4 mapped addresses. Some common IPv6 stacks do not support the IPv4-mapped address feature, either because the IPv6 and IPv4 stacks are separate implementations (e.g.,Microsoft Windows 2000, XP, and Server 2003), or because of security concerns (OpenBSD) . On these operating systems, it is necessary to open a separate socket for each IP protocol that is to be supported. On some systems, e.g., theLinux kernel, NetBSD, and FreeBSD, this feature is controlled by the socket option IPV6 ONLY as specified in RFC 3493.

13 Tunneling

In order to reach the IPv6 Internet, an isolated host or network must use the existing IPv4 infrastructure to carry IPv6 packets. This is done using a technique known as tunneling which consists of encapsulating IPv6 packets within IPv4, in effect using IPv4 as a link layer for IPv6.

The direct encapsulation of IPv6 datagrams within IPv4 packets is indicated by IP protocol number 41. IPv6 can also be encapsulated within UDP packets e.g. in order to cross a router or NAT device that blocks protocol 41 traffic. Other encapsulation schemes, such as used in AYIYA or GRE, are also popular.

Conversely, on IPv6-only internet links, when access to IPv4 network facilities are needed, tunneling of IPv4 over IPv6 protocol occurs, using the IPv6 as a link layer for IPv4.

REFERENCES

1. RFC 1833

2. RFC 2633

3. RFC 3177

4. RFC 4291

5. RFC 4193

6. RFC 4213

7. RFC 5952

8. RFC 5156

9. RFC 6177

10. http://www.en.wikipedia.org/wiki/IPv6

11. http://www.ipv6.com

12. http://www.ipv6forum.org.in