# A Case study of IPv4 and IPv6

Ms. P.S.Kharche[1], Dr. P.M.Jawandhiya[2],
*Department of Computer Science And Engineering, PLITMS, Buldana[1, 2]*
*Email: kharche.priyanka8@gmail.com[2], pmjawandhiya@rediffmaill.com[3]*

**Abstract**- As networks are expanding day by day, IPv6 is gaining more and more popularity. Different transition mechanisms have been established and yet a lot of research is to be carried out. Network security is another very important area of research and needs special attention in the era of network expansions. In this paper, we have discussed different transition mechanisms from IPv4 to IPv6, and various security issues, as well. We have presented a comprehensive review of various security measures proposed by different researchers.

**Index Terms-** IPv4, IPv6

## INTRODUCTION

Internet protocol IPv4 was developed as a research project by the Defense Advanced Research Projects Agency (DARPA), a United States Department of Defense agency, before becoming the foundation for the Internet and the World Wide Web. IPv4 included an addressing system that used numerical identifiers consisting of 32 bits. These addresses are typically displayed in quad-dotted notation as decimal values of four octets, each in the range 0 to 255, or 8 bits per number.

Internet protocol version 6 was first publicly used version of protocol IPv6 is an Internet Layer protocol for packet-switched internetworking and provides end-to-end datagram transmission across multiple IP networks, closely adhering to the design principles developed in the previous version of the protocol, Internet Protocol Version 4 (IPv4). IPv6 was first formally described in Internet standard document RFC 2460, published in December 1998. It simplifies aspects of address assignment (stateless address autoconfiguration), network renumbering, and router announcements when changing network connectivity providers. It simplifies processing of packets in routers by placing the responsibility for packet fragmentation into the end points. The IPv6 subnet size is standardized by fixing the size of the host identifier portion of an address to 64 bits to facilitate an automatic mechanism for forming the host identifier from link layer addressing information (MAC address).

### 1.1. *Comparison with IPv4*

On the Internet, data is transmitted in the form of network packets. IPv6 specifies a new packet format, designed to minimize packet header processing by routers.[2][11] Because the headers of IPv4 packets and IPv6 packets are significantly different, the two protocols are not interoperable. However, in most respects, IPv6 is an extension of IPv4. Most transport and application-layer protocols need little or no change to operate over IPv6; exceptions are application protocols that embed Internet-layer addresses, such as FTP and NTP, where the new address format may cause conflicts with existing protocol syntax.

- Larger address space

The main advantage of IPv6 over IPv4 is its larger address space. The length of an IPv6 address is 128 bits, compared with 32 bits in IPv4.[2] The address space therefore has 2128 or approximately 3.4×1038 addresses.

The longer addresses simplify allocation of addresses, enable efficient route aggregation, and allow implementation of special addressing features. In IPv4, complex Classless Inter-Domain Routing (CIDR) methods were developed to make the best use of the small address space. The standard size of a subnet in IPv6 is 264 addresses. Thus, actual address space utilization rates will be small in IPv6, but network management and routing efficiency are improved by the large subnet space and hierarchical route aggregation.

Renumbering an existing network for a new connectivity provider with different routing prefixes is a major effort with IPv4.[13][14] With IPv6, however, changing the prefix announced by a few routers can in principle renumber an entire network, since the host identifiers (the least-significant 64 bits of an address) can be independently self-configured by a host.[15]

- Multicasting

Multicasting means , the transmission of a packet to multiple destinations in a single send operation. In IPv4 this is an optional although commonly implemented feature.[16] 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 multicasting to address 224.0.0.1. IPv6 also provides for new multicast implementations, including embedding rendezvous point addresses in an IPv6 multicast group address, which simplifies the deployment of inter-domain solutions.[17]

In IPv4 it is very difficult for an organization to get even one globally routable multicast group assignment, and the implementation of inter-domain solutions is arcane.[18] Unicast address assignments by a local Internet registry for IPv6 have at least a 64-bit routing prefix, yielding the smallest subnet size available in IPv6 (also 64 bits). With such an assignment it is possible to embed the unicast address prefix into the IPv6 multicast address format, while still providing a 32-bit block, the least significant bits of the address, or approximately 4.2 billion multicast group identifiers. Thus each user of an IPv6 subnet automatically has available a set of globally routable source-specific multicast groups for multicast applications.[19]

- Stateless address autoconfiguration (SLAAC)

IPv6 hosts can configure themselves automatically when connected to an IPv6 network using the Neighbor Discovery Protocol via Internet Control Message Protocol version 6 (ICMPv6) router discovery messages. When first connected to a network, a host sends a link-local router solicitation multicast request for its configuration parameters; routers respond to such a request with a router advertisement packet that contains Internet Layer configuration parameters.[15]

If IPv6 stateless address auto-configuration is unsuitable for an application, a network may use stateful configuration with the Dynamic Host Configuration Protocol version 6 (DHCPv6) or hosts may be configured manually using static methods.

Routers present a special case of requirements for address configuration, as they often are sources of autoconfiguration information, such as router and prefix advertisements. Stateless configuration of routers can be achieved with a special router renumbering protocol.[20]

- Network-layer security

Internet Protocol Security (IPsec) was originally developed for IPv6, but found widespread deployment first in IPv4, for which it was re-engineered. IPsec was a mandatory specification of the base IPv6 protocol suite,[2][21] but has since been made optional.[2

- 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,[2][11] because less processing is required in routers. This furthers the end-to-end principle of Internet design, which envisioned that most processing in the network occurs in the leaf nodes.

The packet header in IPv6 is simpler than the IPv4 header. Many rarely used fields have been moved to optional header extensions.

IPv6 routers do not perform IP fragmentation. IPv6 hosts are required to either perform path MTU discovery, perform end-to-end fragmentation, or to send packets no larger than the default Maximum transmission unit (MTU), which is 1280 octets.

The IPv6 header is not protected by a checksum. Integrity protection is assumed to be assured by both the link layer or error detection and correction methods in higher-layer protocols, such as TCP and UDP. In IPv4, UDP may actually have a checksum of 0, indicating no checksum; IPv6 requires a checksum in UDP. Therefore, IPv6 routers do not need to recompute a checksum when header fields change, such as the time to live (TTL) or hop count.

The TTL field of IPv4 has been renamed to Hop Limit in IPv6, reflecting the fact that routers are no longer expected to compute the time a packet has spent in a queue.

- Mobility

Unlike mobile IPv4, mobile IPv6 avoids triangular routing and is therefore as efficient as native IPv6. IPv6 routers may also allow entire subnets to move to a new router connection point without renumbering.[23]

- Options extensibility

The IPv6 packet header has a minimum size of 40 octets. Options are implemented as extensions. This provides the opportunity to extend the protocol in the future without affecting the core packet structure.[2] However, recent studies indicate that there is still widespread dropping of IPv6 packets that contain extension headers.[24]

- Jumbograms

IPv4 limits packets to 65,535 (216−1) octets of payload. An IPv6 node can optionally handle packets over this limit, referred to as jumbograms, which can be as large as 4,294,967,295 (232−1) octets. The use of jumbograms may improve performance over high-MTU links. The use of jumbograms is indicated by the Jumbo Payload Option header.[25]

- Privacy

Like IPv4, IPv6 supports globally unique IP addresses by which the network activity of each device can potentially be tracked. The design of IPv6 intended to re-emphasize the end-to-end principle of network design that was originally conceived during the establishment of the early Internet. In this approach each device on the network has a unique address globally reachable directly from any other location on the Internet.

Network prefix tracking is less of a concern if the user's ISP assigns a dynamic network prefix via DHCP.[26][27] Privacy extensions do little to protect the user from tracking if the ISP assigns a static network prefix. In this scenario, the network prefix is the unique identifier for tracking and the interface identifier is secondary.

In IPv4 the effort to conserve address space with network address translation (NAT) obfuscates network address spaces, hosts, and topologies. In IPv6 when using address auto-configuration, the Interface Identifier (MAC address) of an interface port is used to make its public IP address unique, exposing the type of hardware used and providing a unique handle for a user's online activity.

It is not a requirement for IPv6 hosts to use address auto-configuration, however. Yet, even when an address is not based on the MAC address, the interface's address is globally unique, in contrast to NAT-masqueraded private networks. Privacy extensions for IPv6 have been defined to address these privacy concerns,[28] although Silvia Hagen describes these as being largely due to "misunderstanding".[29] When privacy extensions are enabled, the operating system generates random host identifiers to combine with the assigned network prefix. These ephemeral addresses are used to communicate with remote hosts making it more difficult to track a single device.[30]

Privacy extensions are enabled by default in Windows (since XP SP1), OS X (since 10.7), and iOS (since version 4.3).[31][32] Some Linux distributions have enabled privacy extensions as well.[33]

In addition to the "temporary" addresses mentioned above, there are also "stable" addresses:[34] Interface Identifiers are generated such that they are stable for each subnet, but change as a host moves from one network to another. In this way it is difficult to track a host as it moves from network to network, but with-in a particular network it will always have the same address (unless the state used in generating the address is reset and the algorithm is run again) so that network access controls and auditing can be potentially be configured.

**1.2.** Packet format:IPv6

An IPv6 packet has two parts: a header and payload.

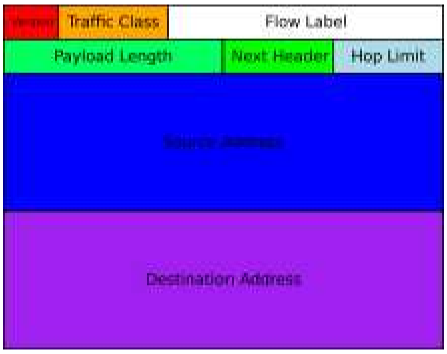
The header consists of a fixed portion with minimal functionality required for all packets and may be followed by optional extensions to implement special features.

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 the type of the optional extension or payload which follows the header. This Next Header field tells the receiver how to interpret the data which follows the header. If the packet contains options, this field contains the option type of the next option. The "Next Header" field of the last option, 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.

Without special options, a payload must be less than 64KB. With a Jumbo Payload option (in a Hop-By-Hop Options extension header), the payload must be less than 4 GB.

Unlike with IPv4, routers never fragment a packet. Hosts are expected to use Path MTU Discovery to make their packets small enough to reach the destination without needing to be fragmented.



**1.3.** *Addressing*:IPv6

Compared to IPv4, the most obvious advantage of IPv6 is its larger address space. IPv4 addresses are 32 bits long which provides approximately 4.3×109 (4.3 billion) addresses.[35] IPv6 addresses are 128 bits long, resulting in an address space of 3.4×1038 (340 undecillion) addresses. Such a large space is sufficient for the future.[36]

IPv6 addresses are written in eight groups of four hexadecimal digits. The groups are 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.[3

- Stateless address autoconfiguration (SLAAC)

An IPv6 host may generate its own IP address and test the uniqueness of a generated address in the addressing scope intended. IPv6 addresses consist of two parts. The most-significant 64 bits are the subnet prefix to which the host is connected, and the least-significant 64 bits are the identifier of the host interface on the subnet. This means that the identifier need only be unique on the subnet to which the host is connected, which simplifies the detection of duplicate addresses.[38]

| part | Subnet prefix | Interface identifier |
|---|---|---|
| bits | 64 | 64 |

Link local address

All IPv6 hosts require a link-local address. This is derived from the MAC address of each interface and the link-local prefix FE80::/10. The process involves filling the address space with prefix bits left-justified to the most-significant bit, and filling the MAC address in EUI-64 format into the least-significant bits. If any bits remain to be filled between the two parts, those are set to zero.[38]

The uniqueness of the address on the subnet is tested with the Duplicate Address Detection (DAD) method.[39]

Address uniqueness

Hosts verify the uniqueness of addresses assigned by sending a neighbor solicitation message asking for the Link Layer address of the IP address. If any other host is using that address, it responds. However, MAC addresses are designed to be unique on each network card which minimizes chances of duplication.[40]

The host first determines if the network is connected to any routers at all, because if not, then all nodes are reachable using the link-local address that already is assigned to the host. The host will send out a Router Solicitation message to the all-routers[41][42] multicast group with its link local address as source. If there is no answer after a predetermined number of attempts, the host concludes that no routers are connected. If it does get a response from a router, there will be network information inside that is needed to create a globally unique address. There are also two flag bits that tell the host whether it should use DHCP to get further information and addresses:

- The Manage bit, that indicates whether or not the host should use DHCP to obtain additional addresses

- The Other bit, that indicates whether or not the host should obtain other information through DHCP. The other information consists of one or more prefix information options for the subnets that the host is attached to, a lifetime for the prefix, and two flags:[40]

    - On-link: If this flag is set, the host will treat all addresses on the specific subnet as being on-link, and send packets directly to them instead of sending them to a router for the duration of the given lifetime.

Global addressing

The assignment procedure for global addresses is similar to local address construction. The prefix is supplied from router advertisements on the network. Multiple prefix announcements cause multiple addresses to be configured.[40]

Stateless address autoconfiguration (SLAAC) requires a /64 address block, as defined in RFC 4291. Local Internet registries are assigned at least /32 blocks, which they divide among subordinate networks.[43] The initial recommendation stated assignment of a /48 subnet to end-consumer sites (RFC 3177). 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 were given a single /64 network.[44]

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 loopback, 6to4 tunneling, and Teredo tunneling, as outlined in 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.

- IPv6 in the Domain Name System

In the Domain Name System, hostnames are mapped to IPv6 addresses by AAAA resource records, so-called quad-A records.

- Address representation

The 128 bits of an IPv6 address are represented in 8 groups of 16 bits each. Each group is written as 4 hexadecimal digits and the groups are separated by colons (:). The address 2001:0db8:0000:0000:0000:ff00:0042:8329 is an example of this representation.

**1.4.** Transition mechanisms

IPv6 is not foreseen to supplant IPv4 instantaneously. Both protocols will continue to operate simultaneously for some time. Therefore, some IPv6 transition mechanisms are needed to enable IPv6 hosts to reach IPv4 services and to allow isolated IPv6 hosts and networks to reach each other over IPv4 infrastructure.[47]

Many of these transition mechanisms use tunneling to encapsulate IPv6 traffic within IPv4 networks. This is an imperfect solution, which reduces the maximum transmission unit (MTU) of a link and therefore complicates Path MTU Discovery, and may increase latency.[48] Tunneling protocols are a temporary solution for networks that do not support native dual-stack, where both IPv6 and IPv4 run independently.

- Dual IP stack implementation

Dual-stack (or native dual-stack) IP implementations provide complete IPv4 and IPv6 protocol stacks in the same network node. This facilitates native communications between nodes using either protocol. The method is defined in RFC 4213.[49]

This is the most desirable IPv6 implementation during the transition from IPv4 to IPv6, as it avoids the complexities of tunneling, such as security, increased latency, management overhead, and a reduced PMTU.[50] However, it is not always possible, since outdated network equipment may not support IPv6.

Dual-stack software design is a transitional technique to facilitate the adoption and deployment of IPv6. However, it might introduce more security threats as hosts could be subject to attacks from both IPv4 and IPv6. It has been argued that dual-stack could ultimately overburden the global networking infrastructure by requiring routers to deal with IPv4 and IPv6 routing simultaneously.[51]

- Tunneling

Many current Internet users do not have IPv6 dual-stack support, and thus cannot reach IPv6 sites directly. Instead, they must use IPv4 infrastructure to carry IPv6 packets. This is done using a technique known as tunneling, which encapsulates IPv6 packets within IPv4, in effect using IPv4 as a link layer for IPv6.

IP protocol 41 indicates IPv4 packets which encapsulate IPv6 datagrams. Some routers or network address translation devices may block protocol 41. To pass through these devices, UDP packets may be used to encapsulate IPv6 datagrams. Conversely, on IPv6-

only Internet links, when access to IPv4 network facilities is needed, tunneling of IPv4 over IPv6 protocol occurs, using the IPv6 as a link layer for IPv4.

Automatic tunneling

Automatic tunneling refers to a technique by which the routing infrastructure automatically determines the tunnel endpoints. Some automatic tunneling techniques are below.

6to4 is recommended by RFC 3056. It uses protocol 41 encapsulation.[52] Tunnel endpoints are determined by using a well-known IPv4 anycast address on the remote side, and embedding IPv4 address information within IPv6 addresses on the local side. 6to4 is the most common tunnel protocol currently deployed.

Teredo is an automatic tunneling technique that uses UDP encapsulation and can allegedly cross multiple NAT nodes.[53] IPv6, including 6to4 and Teredo tunneling, are enabled by default in Windows Vista[54] and Windows 7. Most Unix systems implement only 6to4, but Teredo can be provided by third-party software such as Miredo.

ISATAP (Intra-Site Automatic Tunnel Addressing Protocol)[55] uses the IPv4 network as a virtual IPv6 local link, with mappings from each IPv4 address to a link-local IPv6 address. Unlike 6to4 and Teredo, which are inter-site tunneling mechanisms, ISATAP is an intra-site mechanism, meaning that it is designed to provide IPv6 connectivity between nodes within a single organization.

Configured and automated tunneling (6in4)

6in4 tunneling requires the tunnel endpoints to be explicitly configured, either by an administrator manually or the operating system's configuration mechanisms, or by an automatic service known as a tunnel broker;[56] this is also referred to as automated tunneling. Configured tunneling is usually more deterministic and easier to debug than automatic tunneling, and is therefore recommended for large, well-administered networks. Automated tunneling provides a compromise between the ease of use of automatic tunneling and the deterministic behavior of configured tunneling.

- Proxying and translation for IPv6-only hosts

Hosts newly added to the Internet might only have IPv6 connectivity. For these clients to have backward-compatible connectivity to existing IPv4-only resources, suitable IPv6 transition mechanisms must be deployed.

One form of address translation is the use of a dual-stack application-layer proxy server, for example a web proxy.

NAT-like techniques for application-agnostic translation at the lower layers in routers and gateways have been proposed.

**1.5.** IPv6 readiness

Compatibility with IPv6 networking is mainly a software or firmware issue. However, much of the older hardware that could in principle be upgraded is likely to be replaced instead. The American Registry for Internet Numbers (ARIN) suggested that all Internet servers be prepared to serve IPv6-only clients by January 2012

- Software

Host software may have only IPv4 or only IPv6 networking software, or it may support dual-stack, or hybrid dual-stack operation. The majority of personal computers running recent operating system versions support IPv6. Many popular applications with networking capabilities are compliant.

IPv4-mapped IPv6 addresses

Hybrid dual-stack IPv6/IPv4 implementations recognize a special class of addresses, the IPv4-mapped IPv6 addresses. These addresses consist of an 80-bit prefix of zeros, the next 16 bits are one, and the remaining, least-significant 32 bits contain the IPv4 address. These addresses are typically written with a 96-bit prefix in the standard IPv6 format, and the remaining 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. A deprecated format for IPv4-compatible IPv6 addresses is ::192.0.2.128.[59]

Because of the significant internal differences between IPv4 and IPv6, some of the lower-level functionality available to programmers in the IPv6 stack does not work the same when used with IPv4-mapped addresses. Some common IPv6 stacks do not implement 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).[60] On these operating systems, a program must open a separate socket for each IP protocol it uses. On some systems, e.g., the Linux kernel, NetBSD, and FreeBSD, this feature is controlled by the socket option .

- Shadow networks

One side effect of IPv6 implementation may be the emergence of so-called shadow networks caused by IPv6 traffic flowing into IPv4 networks when IPv6 enabled nodes are added to the existing network, and the IPv4 security in place is unable to properly identify it. This may occur with operating system upgrades, when the newer OS enables IPv6 support by default, while the older one did not. Failing to update the security infrastructure to accommodate IPv6 can lead to IPv6 traffic bypassing it.Shadow networks have been found occurring on business networks in which enterprises are replacing Windows XP systems that do not have an IPv6 stack enabled by default, with Windows 7 systems, that do.

Advantages of IPv4:

- **Reliable security**
- **Large routing tasks**
- **Flexible**

Advantages of IPv6:

- No more checksums, better performance
- Encryption and IPsec built in
- Multiple network addresses assigned to the same device
- Client-side IP address assignment, no need for DHCP

Conclusion:

- In this paper, we discuss about the Internet protocol version IPv4 and IPv6. Internet protocol version 6 was first publicly used version of protocol which provides end-to-end datagram transmission across multiple IP networks, built in Encryption and IPsec, Multiple network addresses assigned to the same device,Client-side IP address assignment, However, in most respects, IPv6 is an advantgeous.

References:

1 J. Bound. Assignment of IPv4 Global Addresses to IPv6 Hosts (AIIH). Work In Progress.
2 R. E. Gilligan, S. Thomson, J. Bound, and W. R. Stevens. Basic Socket Interface Extensions for IPv6. Work In Progress.
3 J. Mogul and S. Deering. Path MTU Discovery, RFC 1191, November 1990.
4 J. McCann, S. Deering, and J. Mogul. Path MTU Discovery for IP version 6, RFC 1981, Aug. 1996.
5 J. Postel. Internet Control Message Protocol. RFC 792, Sep. 1981.
6 H. Custer. Inside Windows NT. Microsoft Press. 1993.
7 Y. Rekhter, B. Moskowitz, D. Karrenberg, and G. de Groot. Address Allocation for Private Internets. RFC 1597, March 1994.