CHAPTER 2

BACKGROUND OF INTERNET PROTOCOL

This chapter presents the background and the using of Internet Protocol version 4 (IPv4). The IPv4 addresses have some problems and limitations. Several solutions are deployed to alleviate the problems of IPv4. This chapter explains the ways and concepts of solutions to extend time for IPv4 address usage. It also presents the fundamentals of the new IP which is the long-term solution.

The background of IPv4 address space and the addresses consumption are introduced in section 2.1. The ways to extend IPv4 address usage, CIDR and NAT are presented in section 2.2 and 2.3 respectively. The overview of IPv6 and the comparison of IPv4 with IPv6 are described in section 2.4. A summary of this chapter is in section 2.5.

2.1 Introduction

The Internet is in wide use for communications between people. It uses the Internet Protocol (IP) to deliver the communication data. IP uses addresses like a house number to identify a place somewhere. In the Internet, an IP address is required for each computer or device which is attached to a link of the network. It is used to identify a node that is connected to a network. And it is used to arrange the appropriate path between a sender and receiver(s).

The current IP is IP version 4 (IPv4) [1]. It was created with an address size of 32 bits so the absolute maximum number of IP addresses is a little more than 4.29×10^9. The survey of address space by Asia Pacific Network Information Centre (APNIC) in March 2005 is shown in Figure 2.1.

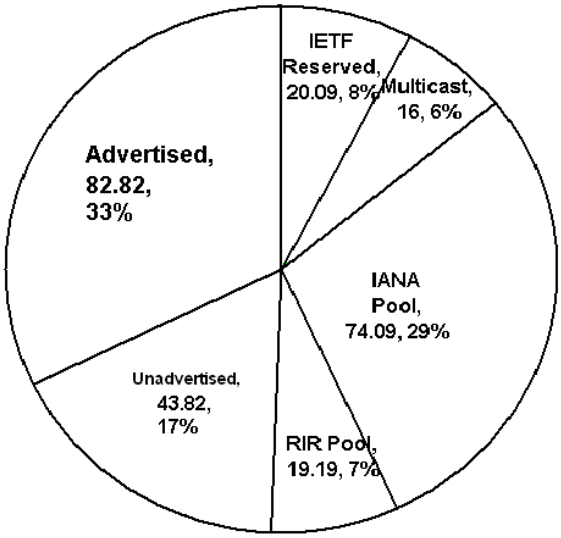

Figure 2.1 IPv4 address space snapshot – from APNIC March 2005. From: [11]

It is found that not all of the IPv4 addresses are available to be used. Some blocks of address are assigned for other particular uses. The IETF has reserved some 8% of the address space (or equivalent of 20.09 of the 256 /8 network blocks.) A further 6% or 16 /8 blocks are reserved for use in multicast context or routing aggregation. The leaves a little under 220 /8 blocks, or 86% of the total IPv4 address spaces available for general use.

There are millions of hosts, computer servers, mobile phones, communication devices, conference services and online electronic devices which each need an IP address as a requirement for their communications. In addition, new technology, for instance Mobile IP, Voice over IP, IP telephony and 3GPP are intending to use IP in their components. The number of IPv4 address is limited by its structure. As IP addresses have been rapidly consumed, address space will become a problem for the Internet in the near future.

We can analyze the demand for address space across the global Internet by using the growth of the routing system. We can derive a model of the demand and make some tentative predictions as to the lifetime of IPv4 address space. IPv4 address consumptions were investigated by APNIC as shown in Figure 2.2.

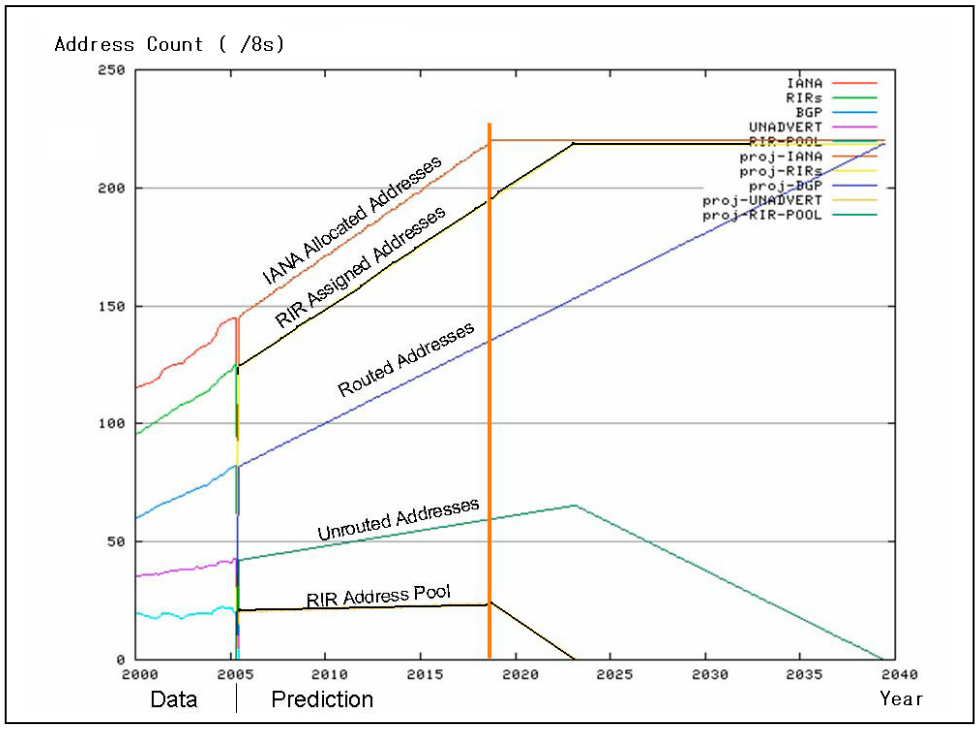

Figure 2.2 IPv4 address consumption – from APNIC March 2005. From: [11]

The number of routed addresses, the addresses that can be reached, has continuously increased. In year 2005, this implies that about 146 /8 address blocks are in used. The remaining 74 /8 address blocks would provide about a further 12 years or until 2018.

IPv4 address space will be critical in the near future because of the limitation of IPv4 number and the address consumption which is continuously increasing. There are two elements, CIDR and NAT that have been allowed to extend using IP addresses in IPv4.

2.2 Classless Inter Domain Rou ting

The report project of C. Sricharan and S. Hussain [12] explained the cause and motivation that Classless Inter Domain Routing (CIDR) [3] is deployed to extend the life time of IPv4 address usage for the Internet. IPv4 addresses suffer from two factors: wasteful address assignment, and excessive routing overhead. They said as shown in the following two paragraphs

“First of all, the standard IPv4 address assignment system is inherently very wasteful.

Following the IPv4 rules as they were originally conceived, any medium-sized company with more than 256 computers would apply for a Class B address, and consequently tie up 64 thousand values. Large companies claiming Class A addresses tie up (and grossly underutilize) about 16 million of IPv4's available addresses. Had certain emergency measures not been taken a few years ago, the TCP/IP community would already be out of host numbers, with most claimed addresses going unused! As it stands, the stopgap introduction of CIDR a few years ago, which (among other things) permits the assignment of Class C addresses in consecutive blocks (aggregates) to build mini-Class-B networks, has bought some time for the IPv4 address pool.

Secondly, classifying millions of computers with just two hierarchical levels results in very large routing tables incurring enormous processing overhead in the Internet's interior routers. As originally conceived, an IP packet's network number identifies the organization that reserved it, and its host number identifies a specific network interface within that organization. This was a workable idea in the 70's, when relatively few network numbers identified the paths to most of the world's computers, and Internet routers needed to advertise and maintain only a few thousand entries in their routing tables. If the original IPv4 architecture were in place today, the Internet's routers would be melting under the strain of maintaining millions of paths to Class C networks in individual households. Again, CIDR to the rescue: its address aggregation scheme flattened the growth of the Internet's routing tables, and bought some more time for IPv4.

So how much time do we have left? Not much. Even with CIDR in place, various estimates now foresee IPv4's collapse occurring somewhere between the years 2000 and 2018. The future of the Internet demands nothing less than the immediate and fundamental reconsideration of the Internet Protocol. "

2.3 Address translator

Network Address Translation (NAT) [6] is a solution to solve this problem. Although it is a short term solution, NAT can slow down use of globally unique IPv4 address. It allows multiple systems on a private network to share one public IP address.

The concept of NAT is to assign private IP addresses for connections inside the local network and allocate a global IP address for connections to the Internet. In addition, the global address can be reused for translation by the other internal hosts. NAT acts as a translator to map from private to global and vice versa. A node in a network which deploys NAT is assigned with a

private IPv4 address. It uses the address connect to other nodes inside network only. When the node wants to connect to the Internet, its IP address is mapped to a global IPv4 address. NAT uses an address translation mechanism to allow hosts in a private network to communicate with others in an external network.

This mechanism is placed at a border router. Each NAT box has a mapping table that contains pairs of private and globally unique addresses. The IP addresses inside the stub domain are not globally unique and are used independently in other domains to solve the address depletion problem.

NAT often must cooperate with application level gateways (ALG) [13] because the NAT function cannot handle applications which include IP addresses or TCP/UDP ports in the payload. ALG and NAT may interact to keep state, use NAT state information, modify applications' payload and perform anything which is necessary to run the application across different realms.

There are many types of NAT which have the same basic properties as follows: transparent address assignment, transparent routing through address translation (routing here refers to forwarding packets, not exchanging routing information) and Information Control Message Protocol (ICMP) [14] error packet payload translation.

1. Transparent address assignment

NAT provides transparent routing when a packet within private network is sent to an external destination by binding the private address with a global address. In some cases, the binding may extend to transport level identifiers – Transfer Control Protocol (TCP) [15] and User Datagram Protocol (UDP) [16] ports. There are two sorts of address assignments.

Static: In this case, a private IP address is mapped to global. The mapping is assigned manually in a table permanently or for the lifetime NAT operation. When a host with a private IP address connects to an external host, the address is translated to a global IP address following the rule in the table. As long as the binding is not changed, NAT continues to use the existing address mapping to translate between private and global IP addresses. These addresses cannot be changed to others unless they are modified by an administrator.

Dynamic: In this case, a private address is bound to a global but it is not processed manually. NAT cooperates with ALG to allocate an address for mapping. It works automatically. It is based on usage requirements and session flow. The global address could be reused after the

address binding of a session is terminated when NAT would free that binding.

2. Transparent routing through address translation

NAT can route packet into the right path because it translates IP address and changes the header of the packet. The phases of translation are as follows:

a) **Address binding:** this is the initiation phase of translation. A private IP address is associated with an external address or vice versa. After the connection is established, all subsequence packets of the same connection will use the same binding for session packet translation. A single host may have many simultaneous sessions from or to itself.

b) **Address lookup and translation:** In order to forward packets between two the realms, NAT will look at the information of address or transport identifier translation which was recorded as state information when the session was established.

c) **Address unbinding:** This phase is the end of session. It is terminated when a TCP FIN is received, or by the timeout. The address binding is terminated after which the global address can be reused for another private address mapping.

3. ICMP error packet payload translation

It is necessary to modify ICMP [14] error messages because the original IP address of the packet was changed. Then IP address within ICMP payload needs to be changed in order that it refers to the address of the origin node. NAT needs to completely translate to end host so IP address, checksum field and relevant transport header must all be modified.

2.3.1 Overview of NAT

There are many variations of NAT which are used in different applications. This document presents only two variations: traditional NAT and bi-directional NAT.

a) **Traditional NAT or outbound NAT**

Traditional NAT would allow hosts which have only private addresses to transparently communicate with hosts with global addresses. NAT makes the external network visible to internal hosts but hides the existence of the internal hosts from the outside world. Since the private

addresses are not externally visible the same set can be used independently at many sites. The only requirement is that the private addresses must not duplicate any global addresses.

In traditional NAT, a session is only initiated from the private network to an external destination. There are two variations of traditional NAT which are Basic NAT and NAPT (Network Address Port Translation).

Basic NAT: Basic NAT allocates a global address from its address pool to an internal host that initiates communication with an external destination. All packets for the connection (or session) must pass through the NAT router. For outbound packets only the source IP address, plus the header checksum, and transport layer checksum are altered.

When the external host responds to the internal, the reply packet is routed toward the NAT router. For inbound packets, the router checks destination address only and looks for this number in the mapping table. If the destination address is in the table, NAT translates the address and updates checksum of the inbound packet. When the connection is terminated, the pair of address translation is removed from the mapping table. The allocated global address is returned to the address pool.

Network Address Port Translation (NAPT): A global IP address in address pool of NAT can be used to map to several private IP addresses of internal hosts. When they communicate with the other hosts in the Internet, their addresses are translated to the identical global address. NAT allows sharing a global address with many private addresses. It uses the address with the port number for translation.

Normally, an IP packet carries either a TCP or UDP packet as its payload. The transport layer has source port and destination port fields to identify local end point of a connection. Each port has 16 bits integers which indicate where the connection begins and ends.

Address and port translation is suitable for an organization that has a private network with a single service provider assigned global IP address. For example, a company has many computers with private addresses 172.30.20.0/24 but it has a globally unique address 100.30.20.10 which is registered with its service provider.

When an internal host with address 172.30.20.x and using source port number 3500 connects to an external host, an outgoing packet passes through the NAT router. The private address is mapped to the address 100.32.20.10. However, it is possible that the same source port number is used by the other hosts which connect outside. So it is necessary to also translate the port

number to identify the different sending processes.

NAPT would allow mapping private IP address, local TCP/UDP port number and related fields into a global address. Then it adds the address mapping into the mapping table and changes header of the outgoing packet to be the global address. TCP/UDP header checksum must be recalculated and inserted into the packet.

When the external host sends a reply packet to the internal host, the incoming packet passes through NAT router. The router relies on the mapping table to check and translate address and port of the packet to the original values. The address and port translation are needed for outbound and inbound session.

b) **Bi-directinal NAT or Two-way NAT**

With a Bi-directional NAT, session can be initiated from any host in public network as well as private network. Private network addresses are bound to globally unique addresses, statically or dynamically as connections are established in either direction. Hosts in external network access private host by using DNS for address resolution. In Bi-directional NAT, DNS-ALG [13] are deployed to cooperate and to facilitate name to address mapping. The name space between hosts in private and external networks is assumed to be end-to-end unique.

For instance, an overview of NAT operations is presented in Figure 2.3. Inside network A and B, every host has a unique address from class C blocks 172.30.21.0/24 and 172.30.22.0/24 respectively. Networks A and B are assigned the class C blocks 198.10.8.0/24 and 198.10.9.0/24 respectively as address pools of the NAT routers in each network. These addresses are globally unique and the other NAT boxes cannot use them.

When host A1 172.30.21.10 connects to host B2 in network B, it uses globally unique address 198.10.9.20 as destination number and sends the packet to its gateway router. NAT translates source address 172.30.21.10 of the IP header to globally unique address 198.10.8.10 before the packet is forwarded. The modified packet is sent to network B 198.10.9.0/24 following the routing table.

When the packet arrives at network B, NAT looks for address in the mapping table and processes address translation. The host 172.30.22.20 has already mapped to globally unique address

198.10.9.20 in the translation table. Likewise, IP packets on the return path go through similar address translations.

Notice that it does not require the changing at hosts or routers. As long as the host A1 is translated to 198.10.8.10 and connects to host B1 with the global address 198.10.9.20, the translation is still the same address for all sessions between these hosts. The address translations are transparent to end hosts.

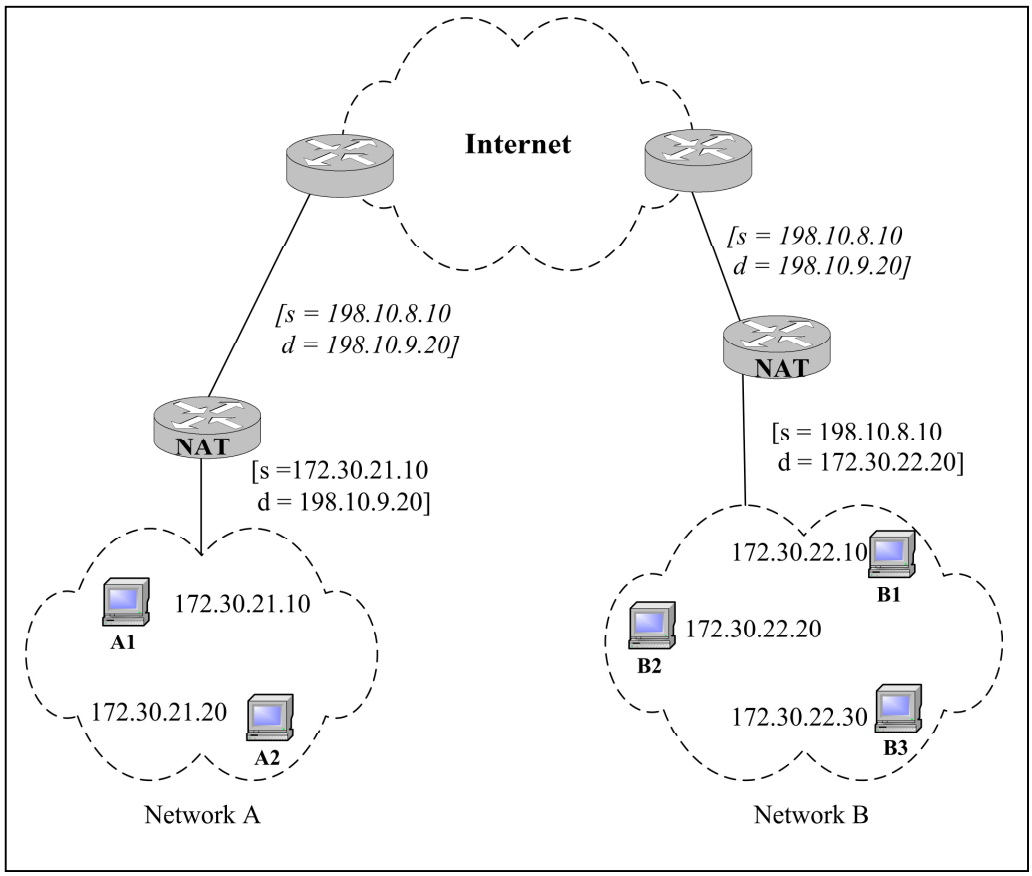

Figure 2.1 Bi-directional NAT operation

Advantages

1. NAT can be installed without change to either hosts or routers. A few applications that are unusual may require changes.
2. It is applied at the border network where is a single point to control and manage whole network. So it is convenient to maintain and widely used.
3. NAT is a short-term solution which can help conserve IPv4 address.

4. Sometime NAT acts as a firewall to protect its own network from outside. It has an IP table which can be configured to allow or denied a host in external network.

Limitations

1. NAT may need to co-exist with an ALG to provide address translation for some applications because they have IP address embedded in the payload which NAT cannot translate.
2. DNS-ALG is required to provide address mapping for address resolution.
3. NAT changes IP address and header of packet. It does not support a service which needs IP address as part of the subject name for authentication purposes, for example IPsec.
4. This way is not end-to-end connection then it is difficult to find the missing host because the original IP of each host in the private network is unseen externally.
5. NAT is located at the border network. It is a single place to process address translation. It is a single point of failure when the NAT box is broken.
6. NAT breaks the flexible end-to-end model of the Internet.
7. Private addresses are applied inside a network of NATs. These addresses might be subject to collision when organizations want to directly interconnect using VPNs.

Using private and global addresses and relying upon NAT is a way to extend the lifetime of the dwindling IPv4 address space. It allows the Internet to continue growing. However, IPv4 address space is evaluated that whether it covers the cost of investment to use IPv4 address and adjust the existing applications to work with NAT. Several limitations of NAT have been found from the review and its operations. NAT functionalities might be a crucial factor to deploy IPv6.

The Internet cannot be completely changed in a short time because of the huge number of network devices and computers. Some of these networks are connected to the Internet and some networks are isolated private IPv4 worlds. There will be a long period to cooperate between IPv4 and IPv6 which are being used in the Internet and private networks. The original plan and requirement to transit to IPv6 will be presented in chapter 3.

An altered method would be enabling NAT to translate between IPv4 and IPv6 and locate at the border between v4 and v6 network. The improved NAT has similar functions and relied on the same fundamental as the original NAT. It encounters all the problems that NAT has in pure

IPv4. The detail of NAT in IPv4 and IPv6 address translation will be presented in chapter 3.

2.4 Overview of IPv6: the next generation IP

The IETF invented the new Internet Protocol, IPv6 [5], to replace the exhausted IPv4. The basic features of IPv6 are the same as IPv4. They are still used to perform the same tasks to provide communication in the Internet. However, several functions were improved in order to enhance the performance of IP or to respond to the requirements and communications in the Internet. They also eradicate some limitations of the old IP. These properties are different from IPv4 and they have several advantages over the old one. The new features for IPv6 have following [12]:

1. IPv6 has 128 bit address fields that can provide a huge number of addresses.
2. IPv6 address can be structured hierarchically to simplify address delegation and routing.
3. Simplifies the main IP header but defines many optional extension headers. This will enable new networking functions to be as needed.
4. Supports authentication, data integrity, and confidentiality at the IP level.
5. Introduces flows, which can be used to support many new kinds of transmission requirements such as real time video.
6. Makes easy to encapsulate other protocols and provides the methods of congestion control when carrying “foreign” protocols.
7. Provides new automatic address self configuration methods and builds in a test for IP address uniqueness.
8. Improves router discovery and detection of dead routers or unreachable neighbors in the link.

The following sections present the overview of IPv6 address, header and the benefits of IPv6. It also describes the difference and the changes between IPv4 and IPv6. The headers and features of IPv4 and IPv6 are compared in the last part.

2.4.1 IPv6 address

IPv6 address has 128 bits so the maximum number of addresses is 3.40×10^{38}. These addresses can be classified into three types [5],[12]:

1. **unicast address:** identifies a single interface; here the packet from a single source can be used by only one destination whose address is specified.
2. **anycast address:** identifies a set of interfaces; but here the packet that is delivered to any address can be used by only one interface, which is the nearest one.
3. **multicast address:** identifies a set of interfaces; here the packet sent to a multicast address is delivered to all interfaces that have joined the multicast group for this address.

Unlike IPv4, IPv6 does not have address classes. It uses prefix numbers of various sizes to identify different types of addresses. These prefixes are assigned following the RFC2373. There are many kinds of IPv6 prefix addresses such as:

Prefix local address: identifies a single interface but here a connection is inside a particular network. There are two types of local address: **prefix link local** identifies an address for a node itself without configuration global address. The prefix number is FE80::/10. It is automatically generated from MAC address as a suffix of IPv6 link local prefix. This address type can be used on the same link. A packet with this address is not forwarded to outside that link or the other routers. An advantage of this address type is to discover neighbor router. And **prefix site local:** identifies an address for using within the same site. The prefix address is FEC0::/10. It was created to provide communication inside office or organization that does not connect to the Internet. So a packet with IPv6 site local address is not forwarded to outside its own network.

Prefix global address: identifies a single interface to connect to the Internet. The prefix address for global unicast is 2000::/3. This kind of address provides the same task as unicast IPv4 address in class A, B, C.

Prefix multicast address: it is used to identify a group address for IPv6. The multicast prefix is FF00::/8. The address with this prefix has similar function to IPv4 address in class D, multicast address.

IPv6 has the other specific address types which are used in different tasks such as:

Loop back address: identifies its own interface. It is used to send datagram back to itself. The address is presented by hexadecimal number 0:0:0:0:0:0:0:1 or ::1.

Unspecified address: the address is represented by the number 0:0:0:0:0:0:0:0 or :: . It is

not used to identify any host. However, it is used as source address of a host that is not configured any IPv6 address in order to request global unicast address from a router or a host configuration server.

Address IPv4 in IPv6: it is a special kind of IPv6 address. IPv4 address is allowed to be embedded as suffix number of an IPv6 prefix. This address is utilized in the similar way to the other address following the type of prefix number.

2.4.2 IPv6 header

Several features of IPv6 were improved to perform and provide the benefit over IPv4 include the size of address number. Although IPv6 can be allocated to have a huge number of addresses, the IPv6 header is simpler than IPv4 and its features can reduce many tasks for network checking. The components in the header fields of IPv6 were improved and modified from IPv4 to be the appropriate things. IPv6 address was created to be 16 bytes long. IPv6 has a fix header size, 40 bytes. The header contains 8 bytes of worked fields and 32 bytes of source and destination address. The structure of an IPv6 header is presented in Figure 2.1.

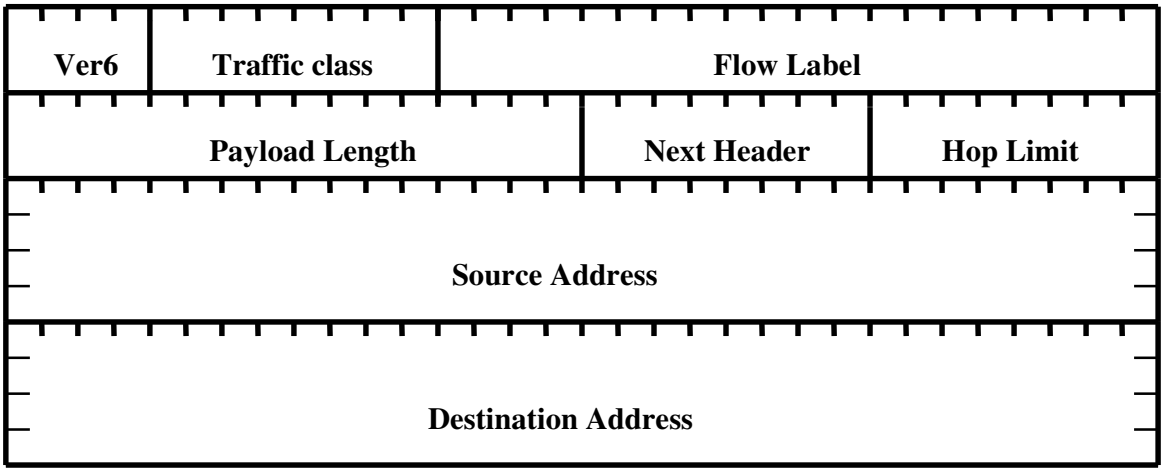

Figure 2.1 Structure of IPv6 header

The IPv6 header consists of the following fields:

Version: (4 bits) it is used to identify version of IP packet. Its value is 6 for IPv6.

Traffic class: (8 bits) it is used to identify the classes or priorities that effect the handling

of the packet.

Flow label: (20 bits) it is used for specification special router handling from source to destination(s) for a sequence of packets.

Payload length: (16 bits) it indicates the length of data in a packet.

Next header: (8 bits) it specifies the next encapsulated protocol.

Hop limit: (8 bits) it is used to count hop that a packet is passed through each router.

Source address: (128 bits) it is network address of sender of a packet.

Destination address: (128 bits) it is network address of receiver of a packet.

Extension header: IPv6 options are placed in separate extension headers to provide a task (s) following the means to implement additional options for example routing header provides explicit routing. The extension headers are placed between the transport layer header and the IPv6 header. A value in the next header field identifies the type of extension header which follows. There are several types of extension headers which defined for IPv6. Each header contains its own next header field to identify the later headers.

In practice, for IPv4, the options field is almost never included in IPv4 packets. For IPv6, the extension headers are placed in order so that a router can stop reading the next header field once it reaches to the extension header that may belong to it. In this case, all of the extension options do not have to be processed by each router that a packet passes along the path to a destination. Many IPv6 extension headers are not processed until they arrive at the destination.

The main benefits of IPv6

1. Providing very large number of IP address.
2. Simplified header and flexible extension.
3. IP layer authentication and the security of end-to-end connection.
4. Quality of Service and real time application are supported by flow label.
5. Plug and play (e.g. link-local address, stateless and statefull, autoconfiguration)
6. Reducing the cost of header processing by removing unnecessary fields.
7. The path MTU is provided to IPv6. It is used to find an appropriate path for an appropriate size of packet. The advantage is this way may reduce packet loss from the fragmentation.

2.4.3 Comparison of IPv4 with IPv6

This section points out the difference and the changing of IPv4 to IPv6. Both protocols have different the size of address but also structures of their headers. For IPv4, the structure of header and components are presented in Figure 2.1.

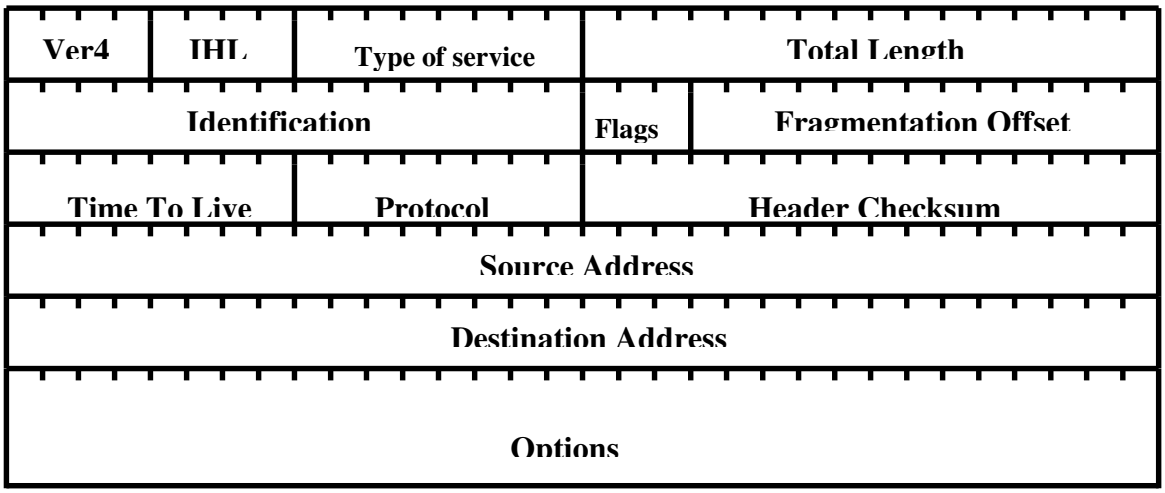

Figure 2.1 Structure of IPv4 header

The IPv4 header consists of the following fields:

Version: this field is used to identify version of IP protocol. Its value is 4.

The header length (IHL): it is header length. It is 20 bytes without options.

Type of Service: this field is used to specify the treatment of a packet when it is delivered through the component network.

Identification, Flags, Fragment Offset: these three fields are used to enable datagram to be fragmented and reassembled.

Time to live (TTL): it is a hop counter which is set when a datagram is launched and counts down at each router. If the counter reaches 0 then the datagram is thrown away.

Protocol: it identifies the encapsulated protocol.

Header Checksum: it is used for the error checking of the header.

Source address: network address of sender.

Destination address: network address of receiver.

Options: it is the options which are requested by IP users.

An obvious difference between IPv4 and IPv6 protocols is number of fields in their headers. The new IP as in Figure 2.1 seems simpler than the old one. It has six fields with source and destination addresses while the old has ten fields with source and destination addresses, and, some options. Both IP protocols have the only one field that is identical. It is IP version.

In IPv6, six fields were removed from IPv4: the header length, the identification, the flags, the fragmentation offset, the header checksum, the type of service. IPv6 has fix header length 40 bytes but IPv4 has 20 bytes without options. Then it has Payload length to indicate the length of data in payload only and no need to specify header length. The IPv6 packet is not allowed to be fragmented. Then Identification, Flags and Fragment Offset are removed. The header checksum is eradicated. It can reduce some procedures to process checksum of IP packet. It might be a risk to avoid this checking. However, the lower layer performs this task. Data link layer must encapsulate IP packet and it must perform the header checksum.

Normally, Type of Service is not used and enabled on an IP packet. Then this field is removed. For IPv6, two new fields are replaced, Traffic class and Flow label. Traffic class is used to provide real time services. While Flow label is used to identify a way that a session must be treated by routers.

Two fields, Protocol and Time to Live in IPv4, are renamed to be Next header and Hop limit respectively. Although their names are changed, they still perform the similar tasks for each IP version. While network address in each source and destination fields for IPv4 has 32 bits, for IPv6, they are changed to be 128 bits. IPv6 address can provide more than 3.40×10^{38} addresses to allow a very large number of nodes to be attached to the Internet. Address notation is presented by hexadecimal number. The comparison of IPv4 with IPv6 is concluded in Table 2.1.

Table 2.1Comparison IPv4 with IPv6

Feature	IPv4	IPv6
Address	32 bits	128 bits
Address space	10^9 possible address	10^{38} possible address
Address assignment	Classify by using class	Classify by prefix address
Packet header	Variable size	Fixed size
Special field in header	Several types but not sported by the venders as it effects the performance	Eliminated and it might be extended in the separated header
Address notation (numeric)	Dotted decimal notation	Hexadecimal with colon and abbreviations; IPv4 address in IPv6 for special case
Fragmentation	Possible multiple steps Fragmentation, done by routers, Impacting routing performance	Done once at most, by host (not router), after MTU discovery over the path improving router performance
Quality of service	Defined but not generally used	Flow labeling, priority, support for real-time data and multimedia distribution
Security	Limited; no authentication or encryption at IP level	Authentication (validation of packet origin), encryption (privacy of contents), requires administration of "security associations" to handle key distribution

Configuration management	Manual compilation of tables; even simple networks require investment of time to configure	Plug and Play; Automatic configuration of link-local addresses based on physical addresses (e.g. Ethernet)

2.5 Summary

This chapter points out the problem of IPv4 address depletion in the Internet. This problem leads to have the solution CIDR, NAT and IPv6 address to allow more available of IP address for use. CIDR and NAT can slow down the IPv4 address consumption but the site effects of deployment of NAT impact to network management, application and maintenance cost. These problems have been relieved by the deployment of IPv6 to the Internet.

However, it is the hard work to migrate the Internet to IPv6 in a short time. IPv6 nodes can be attached into private networks and the Internet but several of the existing applications in these realms are provided by using IPv4. There is the requirement to coordinate between IPv4 and IPv6. NAT which translates pure IPv4 was improved to translate between IPv4 and IPv6. It has been a solution to provide application and communication between IPv4 and IPv6 worlds.