Research on Computer Network Addressing Based on IP Framework

Hao Chang[1, a *]

[1]Xi'an Technological University, Xi'an, Shaanxi, China

[a]2856376405@qq.com

Abstract. IP address, namely Internet protocol address, is a very important concept in computer network. It provides a unique address for every computer and other devices on the Internet. IPv4 and IPv6 are currently the two most commonly used address protocols. This paper elaborates on the structure, classification, allocation and management mechanisms, address subnetting and aggregation of IPv4 and IPv6 addresses, as well as three transition technologies from IPv4 to IPv6. In addition, this paper also introduces the structure and allocation algorithm of decimal future network IPV9 address. The decimal network has the characteristics of completely autonomos and controllable, infinite address space, secure high-speed bitstream transmission, distributed analysis with low latency, and compatibility with existing networks. The huge address space can meet various needs of the future world for 750 years without the problem of address depletion.

Keywords: IPv4 address; IPv6 address; Address subnetting; Address aggregation; Transition technology; IPV9

1. Introduction

With the rapid development of the Internet, IP address, as the basic resource of network communication, becomes more and more important. IP address is a unified address format provided by IP protocol. It assigns a logical address to every network and every host on the Internet. It is a unique identifier used to identify equipment in the computer network. IPv6 is the next generation IP protocol designed by the Internet Engineering Task Force (IETF) to replace IPv4. It is proposed to solve some problems and shortcomings of IPv4. However, with the continuous development of the Internet of Things, big data, and cloud storage applications, IPv6 has gradually exposed some drawbacks in address structure design, security, and compatibility. Therefore, proposing a secure, reliable, compatible, and controllable future network is particularly important. This paper introduces the structural classification, allocation mechanism, subnetting and aggregation of IPv4 and IPv6 addresses, as well as three technologies for transitioning from IPv4 to IPv6. In addition, the composition and structure of IPV9 addresses, as well as the allocation algorithm are introduced.

2. IPv4 Address

IPv4 is the fourth version of Internet communication protocol and the first widely deployed version of Internet protocol. IPv4 was proposed in RFC 791 released by IETF in September 1981. In 1991, it was proposed to alleviate the problem of IPv4 address tension by dividing subnets to form a three-layer structure of addresses[1]. In 1993, Classless Inter-Domain Routing (CIDR) officially replaced classification networks, achieving more flexible IP address allocation and routing table aggregation. In 2019, all 4.3 billion IPv4 addresses worldwide have been allocated, making it impossible to assign IPv4 addresses to Internet Service Providers (ISPs) and other network infrastructure providers.

2.1 IPv4 Address Structure. An IP address is a 32-bit binary number, usually divided into four "8-bit binary numbers", which are four bytes. IPv4 addresses are usually represented in "dotted decimal" format, such as "a.b.c.d", where a,b,c,d are all decimal integers between 0 and 255. For example, a dotted decimal IPv4 address "192.168.1.1" is actually a 32-bit binary number "11000000.10101000.00000001.00000001".

The IPv4 address consists of the network ID (network number) and the host ID (host number). The network ID identifies the network where the IPv4 address is located, and the host ID identifies the

specific interface or adapter where the IPv4 address is located in that network, all hosts on the same physical network use the same network number. When the network number is determined, the host number takes all 0 to represent the network address of the network.

2.2 IPv4 Address Classification. Before the adoption of CIDR, IPv4 addresses were addressed using a classification based addressing scheme, which divided them into three classes, A, B, and C based on the first few bits (high bit) of the address, as well as two special classes, D and E. Currently, the classification based addressing scheme has been replaced by the more flexible and efficient CIDR. The Class A, B, and C addresses account for 87.5% of the entire IPv4 address space and are uniformly allocated globally by InterNIC. Except for special purpose IPv4 addresses and private IPv4 addresses, most can be used to identify network interfaces on public networks. Private addresses belong to unregistered addresses and are specifically used for internal organizational purposes. It is mainly used for allocation in the local area network and cannot be recognized on the public network. Internal IP addresses must be converted into publicly available IP addresses through NAT to achieve communication between internal IP addresses and the public network.

Class A IP addresses consist of a 1-byte (first 8 bits) network bit and a 3-byte (last 24 bits) host bit. The highest bit of the network number is "0", and the address range is 1.0.0.1-127.255.255.254[2].

Class B IP addresses consist of a 2-byte (first 16 bits) network bit and a 2-byte (last 16 bits) host bit. The highest bit of the network number is "10", and the address range is 128.0.0.1-191.255.255.254[3].

Class C IP addresses consist of a 3-byte (first 24 bits) network bit and a 1-byte (last 8 bits) host bit. The highest bit of the network number is "110", and the address range is 192.0.0.1-223.255.255.254[3]. The details of Class A, B, and C IPv4 addresses are shown in Table 1.

Table 1. Class A, B, C IPv4 address details

Classification	Maximum number of networks	IP address range	Maximum number of hosts	Private IP address range
A	126(2^{7-2})	1.0.0.1-127.255.255.254	16777214	10.0.0.0-10.255.255.255
B	16384(2^{14})	128.0.0.1-191.255.255.254	65534	172.16.0.0-172.31.255.255
C	2097152(2^{21})	192.0.0.1-223.255.255.254	254	192.168.0.0-192.168.255.255

Class D IP addresses are multicast addresses that do not distinguish between network bits and host bits, and is a specially reserved address. A multicast address is used to address a group of computers at once, identifying a group of computers that share the same protocol. The highest bit of the multicast address is "1110", and the address range is 224.0.0.0-239.255.255.255.

Class E IP addresses are reserved addresses for future use and experimentation, and also do not distinguish between network and host bits. The highest bit of Class E address is "11110", and the address range is 240.0.0.0-255.255.255.254.

There are some special IPv4 addresses that cannot be assigned to network interfaces for use:

(1) 0.0.0.0 represents the local host and can only be used as the source address.

(2) 255.255.255.255 is the broadcast address of the current subnet, which is sent to all hosts in the local subnet, and the data packets will not be forwarded to other subnets through the router. It can only be used as the destination address.

(3) The addresses where the network number is a decimal number 127, and the host number is not all 0 and not all 1 are loopback addresses, used for network communication testing of the host itself, and the most commonly used is 127.0.0.1. The packets sent to these addresses do not leave the host, but are directly processed in a loop within the host. It can serve as both the source address and the destination address.

(4) When the network number is a specific value and the host number is all 0, it represents the network address and is used to identify the entire network, rather than a single host in the network. It is usually used for routing and network definition. It can neither be used as a source address nor as a destination address.

(5) When the network number is a specific value and the host number is all 1, it represents the broadcast address, which is used to broadcast to all hosts on a specific network. It can only be used as the destination address.

2.3 Allocation and Management of IPv4 Address. IPv4 addresses are allocated globally by the Internet Assigned Numbers Authority (IANA), which allocates IP address blocks to five Regional Internet Registrars (RIRs), including AFRINIC, APNIC, ARIN, LACNIC, and RIPE NCC. Responsible respectively for Africa, Asia Pacific, North America, Latin America and the Caribbean, as well as Europe, the Middle East, and Central Asia. The RIR's role is to allocate IP addresses to Internet Service Providers (ISPs), who allocate these addresses to organizations or end users, such as enterprises, institutions and individual users. Enterprises and organizations can also directly apply for IP addresses from RIR.

The TCP/IP protocol requires different settings for different networks, with each node generally requiring an "IP address", a "subnet mask", and a "default gateway". Dynamic Host Configuration Protocol (DHCP) is a network management protocol used to automatically allocate IP addresses and other network parameters, relying on a DHCP server. DHCP can assign temporary IP addresses to clients with a lease period. After the lease expires, the client needs to reapply for an IP address. DHCP dynamically allocates IP addresses in a network with dynamically changing device numbers, which can improve address utilization; It is also easier to expand and can adapt to the growth and expansion of network scale. But when the DHCP server malfunctions, network devices will be unable to obtain IP addresses, affecting network connectivity.

CIDR is a standard used for aggregating and allocating IP addresses, which introduces the concept of "network prefix" and represents IP addresses as "IP address/prefix length". For example, 192.168.1.0/24 indicates that the first 24 bits of the IP address are the network portion, and the remaining 8 bits are the host portion. The emergence of CIDR eliminates the concept of Class A, B, and C IPv4 addresses, allowing for the allocation of appropriately sized address blocks according to demand, achieving a more flexible and efficient address allocation method. The introduction of CIDR aims to solve the problem of insufficient IPv4 address space and inefficient allocation.

2.4 IPv4 Address Subnetting. The essence of subnetting is to divide a large network into several smaller subnets, each with its own subnet address [4]. Further divide the host number in the IP address into subnet number and host number, that is, change from two-level addressing to three-level addressing. As shown in Fig. 1.

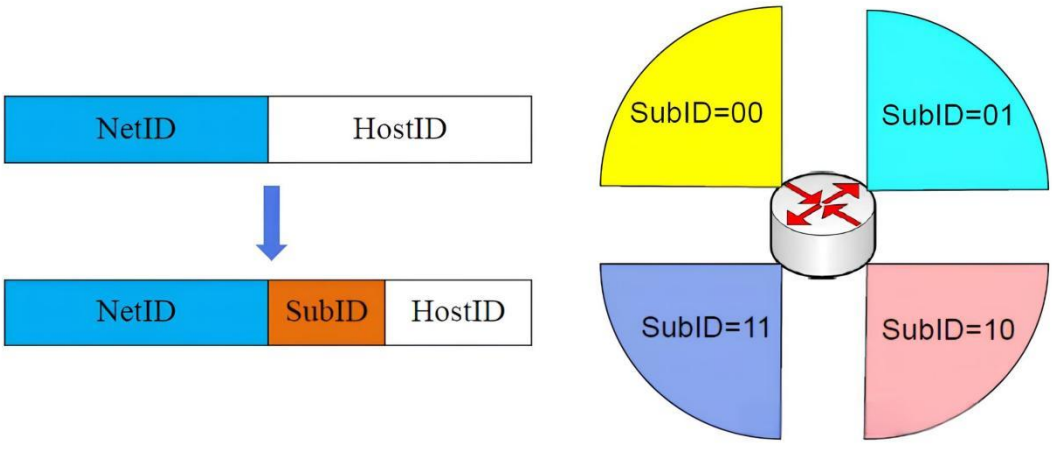

Figure 1. IP address changed from two-level addressing to three-level addressing

After subnetting, the entire network remains one network externally, while internally it is divided into many small subnets. Subnet masks provide a method of subnetting, which reduces communication on the network, saves IP addresses, and facilitates management. After using subnet masks to subnet, communication within the subnet is possible, but communication across subnets is not possible. The format of the subnet mask is the same as the IPv4 address, and it is also a 32-bit binary encoding. The encoding rule is to represent both the network number and subnet number in the IP address as 1, and the host number as 0.

For classified IPv4 addresses, the subnet mask for Class A networks is 255.0.0.0, the subnet mask for Class B networks is 255.255.0.0, and the subnet mask for Class C networks is 255.255.255.0. The method for calculating the new subnet mask is as follows: Determine the required number of subnets; Determine the required number of subnet bits (n), which must be "2^n-2 ⩾ the number of subnets"; Set all the bits before the host number to 1 to obtain the subnet mask for dividing the IP address into subnets.

CIDR eliminates the concept of dividing subnets. When using CIDR representation, the network prefix is a combination of network number and subnet number. For example, for address 128.14.32.0/20, the subnet mask is 255.255.240.0.

Variable Length Subnet Mask (VLSM) is used to use multiple subnet masks in the same network address space, which divides a network into multiple subnets of different sizes, each with a different subnet mask. When subnetting, it is necessary to ensure that there is no overlap between the subnets. VLSM can flexibly allocate IP addresses according to the needs of different subnets, avoiding the waste of IP address resources, and is particularly suitable for networks that need to be finely divided into subnets.

Taking VLSM as an example for subnetting: Divide 192.168.1.0/24 into two subnets, one subnet requires 50 hosts and the other subnet requires 20 hosts. For the first subnet, the host number must have at least 6 digits to meet this requirement. Therefore, the number of digits for the network number and subnet number is 26, and the subnet mask is /26 (255.255.255.192); For the second subnet, the host number must have at least 5 digits to meet this requirement. Therefore, the number of digits for the network number and subnet number is 27, and the subnet mask is /27 (255.255.255.224). When assigning IP addresses, the network address of the first subnet is 192.168.1.0/26, and the available IP address range is 192.168.1.1-192.168.1.62; The network address of the second subnet is 192.168.1.64/27, and the available IP address range is 192.168.1.65-192.168.1.94.

2.5 IPv4 Address Aggregation. The basic principle of IP address aggregation is to combine multiple IP addresses (whether consecutive or non-consecutive) into a single, larger range of IP addresses, known as aggregated addresses. As shown in Fig. 2. This aggregated address can represent multiple IP addresses, thereby reducing the number of entries in the routing table and improving the efficiency and stability of the router. For example, when aggregating IP addresses 215.167.159.224/27, 215.167.159.28/28, and 215.167.159.192/28, listing each IP address in binary form, finding the longest common prefix (11) in its fourth byte, and retaining all the digits of the same part is the number of digits of aggregated IP address network part. The aggregated subnet mask is /26 (255.255.255.192), so the aggregated IP address is 215.167.159.192/26.

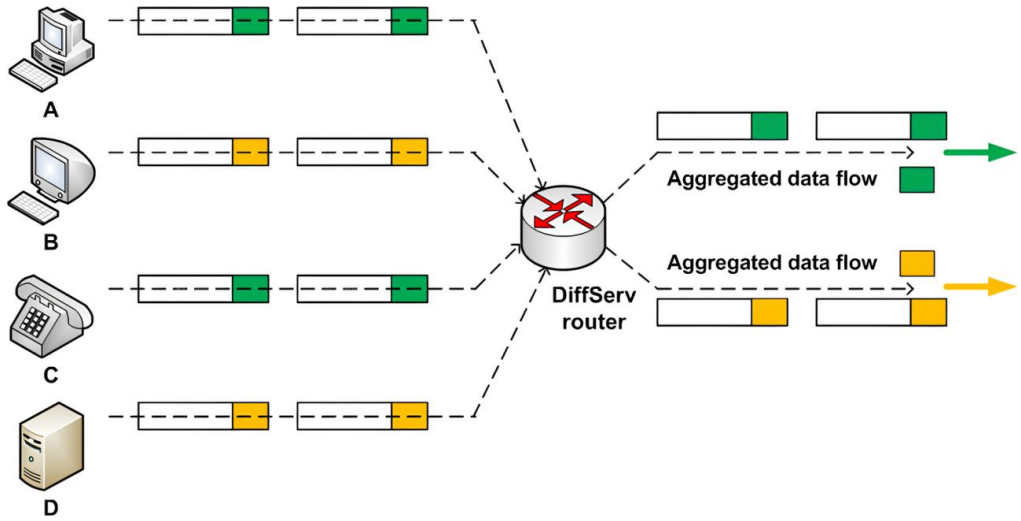

Figure 2. IP address aggregation

Supernetting is also a network address aggregation technology. It can aggregate multiple consecutive and similar subnets into a larger subnet in the routing table, known as forming a

supernetting or routing aggregation. CIDR is the primary way to achieve supernetting, which combines consecutive IP addresses with the same network prefix into a "CIDR address block". Supernetting provides a solution to the depletion of Class B network address space and fully utilizes Class C address space. For example, when aggregating IP addresses 172.16.0.1/24, 172.16.1.1/24, 172.16.2.1/24, and 172.16.3.1/24 using a subnet, the first 22 bits of the binary form of these four addresses are all the same. Therefore, the aggregated subnet mask is /22 (255.255.252.0), and the aggregated IP address is 172.16.0.0/22.

3. IPv6 Address

IPv6 is the sixth version of the Internet Protocol, which is used to solve the problem of the shortage of IPv4 network address resources, and also solves the obstacles for multiple devices to connect to the Internet. Compared to IPv4, IPv6 has a sufficient address space, with a maximum of 2^{128} addresses. Compared to IPv4, IPv6's address allocation follows the principle of clustering from the beginning, making the routing table smaller and thus improving the speed of forwarding datagrams; IPv6 adds enhanced multicast support and flow control, providing a better development platform for multimedia applications on the network; IPv6 adds support for auto configuration, and improves and expands the DHCP protocol, further enhancing the efficiency and convenience of network management.

3.1 IPv6 Address Structure. IPv6 addresses have a length of 128 bits and are typically divided into 8 groups, each consisting of 4 hexadecimal numbers separated by colons. There are two main ways to represent IPv6:

(1) Colon-hexadecimal notation. The format is X:X:X:X:X:X:X:X, where each X represents 16 bits in the address, represented in hexadecimal. The leading 0 of each X can be omitted, for example, "008A" can be written as "8A".

(2) Double colon notation. A string of all zeros can be represented by a double colon "::" and can only be used once in an address. For example, "0:0:0:0:0:0:1" can be represented as "::1", while "0:0:0:0:0:0:0:0" is represented as "::".

An IPv6 address can be divided into two parts: network prefix and interface identifier. The network prefix is used to identify a specific network or subnet, and the prefix length can be any value, usually 64 bits, usually indicated by the CIDR notation; Interface identifier is used to identify specific devices or interfaces in the network, usually 64 bit. This part of the address is usually generated by the device's MAC address through EUI-64 format conversion.

3.2 IPv6 Address Classification. The IPv6 protocol mainly defines three types of addresses: unicast address, multicast address, and anycast address. Compared to IPv4, broadcast addresses have been removed and replaced by multicast, while adding anycast address type.

Unicast addresses uniquely identify an interface, and messages sent to the unicast address will be delivered to the interface identified by this address. IPv6 defines various unicast addresses, such as unspecified address, loopback address, global unicast address, link-local address, and unique local address. An unspecified address only indicates that a certain address does not exist, and is usually used to attempt to verify the source address of a temporary address uniqueness packet; The loopback address is used to identify the loopback interface, allowing devices to send messages to themselves; Global unicast addresses are equivalent to public network addresses in IPv4 and can be globally routed and accessed on IPv6 networks; Link-local addresses can only communicate between sites connected to the same link and cannot be routed across different subnets; The unique local address can only be used within one site, and due to the abolition of the site local address, the unique local address is used instead of the site local address.

Multicast addresses are used to identify a group of interfaces that generally belong to different sites. Using an appropriate multicast routing topology, packets sent to multicast addresses will be sent to all interfaces belonging to that group.

Anycast addresses, like multicast addresses, are also used to identify a set of interfaces that typically belong to different sites. The data packet with the destination address being an anycast address will be sent to the nearest network interface in terms of routing. IPv6 does not specify a separate address space for anycast, and both anycast and unicast addresses use the same address space.

Anycast address can only be assigned to routing devices, cannot be assigned to IPv6 hosts, and cannot be used as the source address for an IPv6 packet message [5].

The correspondence between the main address types of IPv6 and address prefixes is shown in Table 2.

Table 2. Correspondence between the main address types of IPv6 and address prefixes

Address Type		Address Prefix (binary)	IPv6 Prefix Identification
Unicast Address	Unspecified Address	00…0(128bits)	::/128
	Loopback Address	00…1(128bits)	::1/128
	Link-Local Address	1111111010	FE80::/10
	Unique Local Address	1111110	FC00::/7
	Global Unicast Address	001	2000::/3
Multicast Address		11111111	FF00::/8
Anycast Address		Allocation from the unicast address space, using the unicast address format	

3.3 Allocation and Management of IPv6 Address. IPv6 address space management is allocated globally according to the specified hierarchy, that is, according to the hierarchy of IANA-RIR-National Internet Registration (NIR)-ISP/Local Internet Registration (LIR)-End User or ISP.

IPv6 address allocation mainly relies on two different mechanisms: Stateful Address Configuration (DHCPv6) and Stateless Address Autoconfiguration (SLAAC). DHCPv6 allocates IPv6 addresses and other network parameters through DHCPv6 servers. DHCPv6 provides rich configuration information such as subnet prefixes, gateway addresses, DNS server addresses, etc., ensuring that devices can fully participate in IPv6 networks. Meanwhile, DHCPv6 adopts centralized management, which can maintain status information between devices and servers. However, the centralized management mechanism of DHCPv6 may lead to its deployment and management being too complex. Therefore, in order to simplify the network configuration process and improve efficiency, SLAAC technology is proposed.

SLAAC is an automatic address configuration method in IPv6 networks that allows devices to automatically construct IPv6 addresses when connected to the network. The reason why it is called "stateless" is because SLAAC itself does not maintain any status information about IPv6 address allocation. Routers in the network inform devices of basic network information through periodic router advertisement messages. Devices automatically configure IPv6 addresses based on router advertisement and EUI-64 generated information, avoiding dependence on DHCPv6 servers.

3.4 IPv6 Address Subnetting. An IPv6 address consists of a network prefix and an interface identifier. For a global unicast address, the network portion consists of a global routing prefix and subnet ID. The global routing prefix is generally 48 bits, and the first 3 bits of the currently assigned global routing prefix are all 001; The subnet ID is usually at most 16 bits, and the last 64 bits are used as the interface identifier. The subnetting of IPv6 is mainly based on network prefixes, rather than interface identifier. IPv6 divides smaller subnets by increasing prefix length.

The process of subnetting mainly consists of two steps: determining the number of bits used for subnetting and enumerating the new subnet networks. In order to list all subnet networks, it is

necessary to determine the incremental value between every two subnet networks. If "s" represents the number of bits required for subnetting, "f" is the number of fixed bits in the subnet ID (f=prefix length-48), and "i" represents the incremental value, then $i = 2^{16-(f+s)}$.

Taking the IPv6 address 2001:0db8:0:000::/51 as an example, dividing it into 8 subnets will require 3 bits in the subnet division space. The new network prefix is 2001:0db8:0:C000::/54, and the hexadecimal incremental value is calculated to be 0x400, then all divided subnets can be obtained: 2001:0db8:0:C000::/54; 2001:0db8:0:C400::/54; 2001:0db8:0:C800::/54; 2001:0db8:0:CC00::/54; 2001:0db8:0:D000::/54; 2001:0db8:0:D400::/54; 2001:0db8:0:D800::/54; 2001:0db8:0DC00::/54.

3.5 IPv6 Address Aggregation. The principle of aggregation was considered at the beginning of the IPv6 design process. Global unicast address is also known as aggregatable global unicast address. By using the same global routing prefix, multiple subnets are aggregated into a larger IPv6 network, so that a single record can represent a subnet in the routing table, greatly reducing the number of routing entries and improving routing efficiency and network performance. In contrast to IPv6 subnetting, IPv6 achieves address aggregation by reducing prefix length.

If there are 4 subnets: 2001:0db8:abcd:0000::/52; 2001:0db8:abcd:1000::/52; 2001:0db8:abcd:2000::/52; 2001:0db8:abcd:3000::/52. The incremental value of every two subnets is 0X100, and among the 16 bits of the subnet division space, the first 2 bits are all the same. The aggregated IPv6 address is 2001:0db8:abcd:0000::/50, and the number of routing table entries is reduced from 4 to 1.

4. Transition Technology from IPv4 to IPv6

At present, the majority of network deployments are still based on IPv4, with a large number of IPv4 based network and terminal devices. The transition from IPv4 to IPv6 is a gradual process and cannot be achieved overnight [6]. To achieve the transition from IPv4 to IPv6 networks and interoperability between networks, three main technologies can be used to support it: dual stack technology, tunneling technology, and protocol conversion technology.

4.1 Dual Stack Technology. Dual stack technology is the earliest transition technology, which refers to running both IPv4 and IPv6 protocol stacks on the same network device. Dual stack nodes use the IPv4 protocol stack when communicating with IPv4 nodes and the IPv6 protocol stack when communicating with IPv6[7]. The dual stack protocol stack model is shown in Fig. 3.

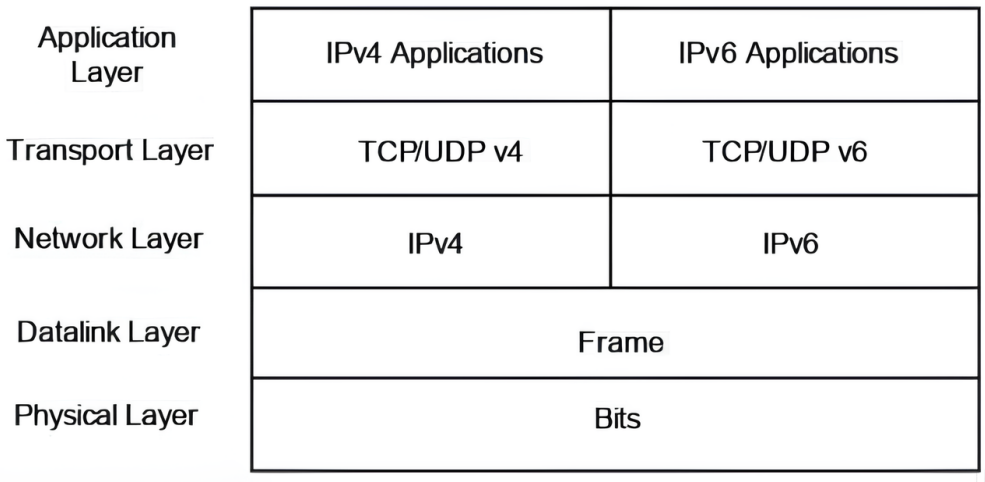

Figure 3. Dual stack protocol stack model

In network communication, network terminal devices select the appropriate IP protocol stack for data encapsulation based on the destination address provided by the upper layer application. If the destination address is an IPv4 device, use the IPv4 protocol stack; If it is an IPv6 device, use the IPv6 protocol stack. For the received packets, the device selects the corresponding IP protocol stack for parsing based on the first field (version number) in the IP data header. When a network supports dual stack, it requires all devices in the network to support both IPv4 and IPv6 protocol stacks, and the

device interfaces connecting to the dual stack network can be configured with both IPv4 and IPv6 addresses simultaneously.

4.2 Tunneling Technology. Tunneling is a technology that encapsulates data packets from one protocol into data packets from another protocol for transmission. Tunneling encapsulates IPv6 packets from the source into IPv4 packets at the tunnel entrance, uses a "6-to-4 tunnel" for transmission, and unpacks IPv6 packets from the IPv4 packets at the tunnel exit before sending them to the destination host [8], as shown in Fig. 4. Although tunneling technology has achieved good interoperability between IPv4 and IPv6 networks, it requires high requirements for IPv4 network edge routing and switching devices, requiring support for both dual stack protocols and tunneling technology [9].

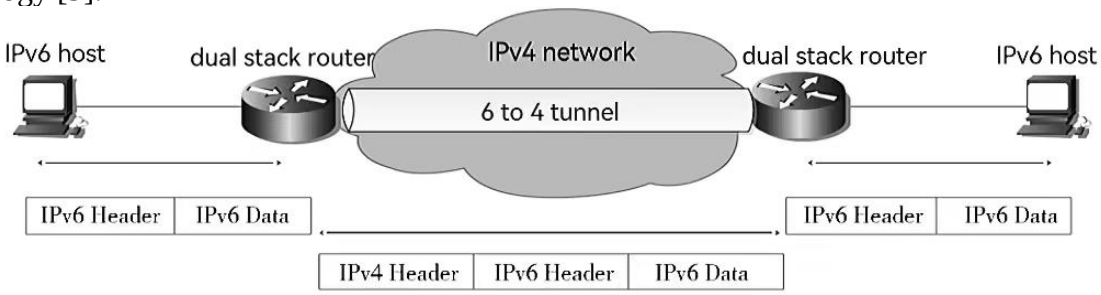

Figure 4. Tunneling technology schematic

4.3 Protocol Conversion Technology. Protocol conversion technology refers to the conversion of addresses and protocols between IPv4 and IPv6 to achieve network interoperability between the two protocols. There are three commonly used protocol conversion technologies: NAT64/DNS64 is used to convert IPv6 addresses to IPv4 addresses and achieve interoperability between IPv4 and IPv6 through DNS resolution; BIS implements the conversion between IPv4 and IPv6 in the protocol stack, suitable for dual stack devices; BIA implements protocol conversion at the application layer, suitable for applications that do not support IPv6.

The device that connects IPv6 and IPv4 networks is called a protocol converter, as shown in Fig. 5. During protocol conversion, network node devices incur significant processing costs for protocol and address conversion, and some application layer protocols cannot achieve conversion. Therefore, dual stack and tunneling technologies are preferred during the transition phase [10].

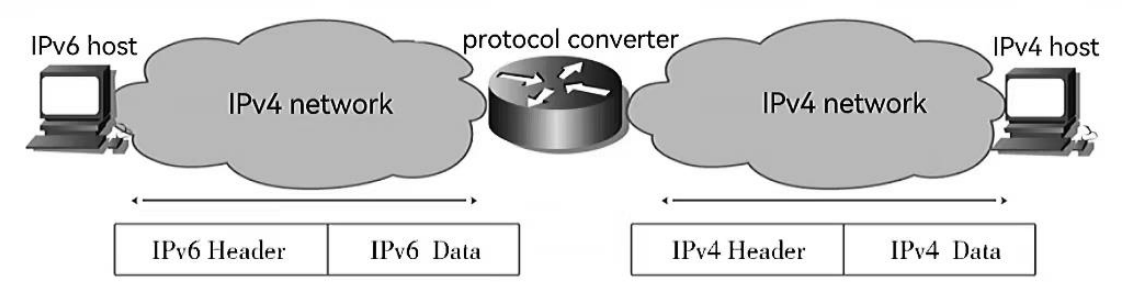

Figure 5. Protocol conversion technology schematic

5. Future Network IPV9

Future network is a technical term, a standardization project in the field of ISO/IEC international standards since 2007, which aims to develop a new network system independent of the existing Internet by using the method of "Clean Slate Design" and new architecture. IPV9 was proposed in 1998 by Shanghai Decimal Network Information Technology Co., Ltd. in China, also known as the Future Network. The full name of IPV9 is "the method of assigning addresses to computers using full digital encoding", which is completely independent intellectual property rights and a network space of 2^{256} addresses established based on full decimal digital codes. It has autonomous control, a huge

amount of addresses, distributed resolution, fast speed, security, and is compatible with IPv4, IPv6, geographic information, country numbers, region numbers, mobile phone numbers, etc.

5.1 IPV9 Network Address Composition. The default IP address for a decimal network is 256 bits, divided into 8 bits, with each segment consisting of 32 bits, separated by a single square bracket symbol "[" or "]", both of which can be used, but cannot be mixed.

For example, 0[1[2[3[4[5[6[7 and 0]1]2]3]4]5]6]7 are equivalent and legal, but 0[1[2[3[4]5]6]7 is not allowed, and the simultaneous use of left and right symbols has special meanings. Continuous 0 fields in an address can be replaced by a pair of "[]". For example, 0]0]0]0]0]0]0]1 can be abbreviated as []1 or [7]1. However, in address abbreviation, "[]" can only be used once to represent all 0 fields, as using "[]" multiple times will cause ambiguity in the address. In each address segment, multiple consecutive zeros on the left can be omitted, but all zeros in decimal are represented by at least one 0.

If there is a continuous and identical segment of Arabic numerals within an address, in order to further simplify the address, the segment of Arabic numerals can be replaced by a parenthesis, and the number to be omitted, separator, and number of omitted digits should be indicated from left to right within the parentheses. For example, 9800980000 can be abbreviated as 980098 (0/4).

In the address allocation process of networked computers and intelligent terminals, it is necessary to make the external address correspond to the internal binary address. Therefore, a fixed-length unfixed-position method is needed to make the two correspond to each other. For example, for external address [7]19, it will correspond to internal binary address [7] (0/251) 10011.

The address can be assigned to a network interface, and if it can be assigned to a single network interface, this identifier serves as a unicast address. Messages with the destination address of the unicast address will be sent to the unique network interface identified by it.

In order to achieve compatibility with IPv4 and IPv6 addresses, the complete 32-bit IPv4 and 128-bit IPv6 addresses are kept at the end of the IPv4 address segment, and the value of the first segment is used as an identifier to point to IPv4 or IPv6. The mapping relation between IPv4 and IPV9 addresses is shown in Table 3.

Table 3. The mapping relation between IPv4 and IPV9 addresses

Bit number	Legnth（bit）	Mapping relation
1-96	96	0[0[0
97-128	32	0
129-224	96	0
225-256	32	IPv4 address

The address mapping relation between IPv6 and IPV9 is shown in Table 4.

Table 4. The mapping relation between IPv6 and IPV9 addresses

Bit number	Legnth（bit）	Mapping relation
1-96	96	1[0[0
97-128	32	0
129-256	128	IPv6 address

For IPV9 nodes in tunneling technology, they should be assigned IPv4/IPv6 compatible addresses to communicate with other nodes in the corresponding network. The mapping table for this is shown in Table 5.

Table 5. The mapping relation of IPV9 compatible IPv4/IPv6 addresses

Bit number	Legnth（bit）	Content
1-10	10	Prefix
11-29	19	Reserve
30-32	3	Sign
33-96	64	0
97-128	32	Scope
129-224	96	IPv6 specific
225-256	32	IPv4 specific

5.2 IPV9 Address Allocation Algorithm. The method of using full digital codes to assign addresses to computers accessing the internet (IPV9) is as follows: the address of a computer is composed of an access number, a phone number, and a classification number. The access number is the numerical number of the website specified by the country and region, and the phone number includes the international direct dial phone number of the user's country, the domestic direct dial phone area code of the user's region, and a combination of the phone numbers of the user's unit or individual. The classification number is the numerical number assigned by the country or region to a unified business category.

The IPV9 technical solution is to input addresses into computers through input from computers and intelligent terminals, such as scanning input devices such as keyboards, barcodes, QR codes, visual input devices, voice input devices, etc. It combines various computer software and hardware, and uses various transmission media such as optical cables, microwaves, and coaxial cables to address the external addresses of networked computers and intelligent terminals stored in the database corresponding to the addresses of internal computer operations.

The address allocation steps for networked computers are as follows.

(1) Define various external addresses of all networked computers and intelligent terminals as decimal values, which represent decimal integers in the range of 10^0-10^{256}, and input the addresses into the computer through the input ports of the computer and intellligent terminals, such as keyboards, voice input devices, etc;

(2) Define the internal addresses of all networked computers and intelligent terminals as binary values, which represent binary numbers ranging from 2^0 to 2^{1024};

(3) The address allocation algorithm can correspond to a binary internal address using a fixed-length unfixed-position method or a fixed-position unfixed-length random length method;

(4) In addition to storing external addresses, the database also stores top-level domain names applied for in various languages such as numbers, English, and Chinese, as well as existing communication numbers such as phone numbers, region numbers, city numbers, mobile phone numbers, MAC addresses, and the latest numerical domain names based on decimal encoding;

(5) The addresses in the database are directly corresponding to the binary addresses inside the computer, and the data flow is directed to the host through transmission media such as optical cables, microwaves, and coaxial cables through the gateway. Character domain names can be parsed to find their decimal addresses and point to the address of their host. Telephone numbers, mobile phones, and

other communication numbers in the database are directly directed to the communication system to which the communication number belongs through the gateway.

6. Conclusions

This paper systematically explores the most commonly used IPv4 and IPv6 network addresses based on IP frameworks, and deeply analyzes the composition and structure, address types, address management and allocation mechanisms, address subnetting and aggregation, as well as the transition and interconnection technology from IPv4 to IPv6. With the advent of the Internet 4.0 era and the continuous emergence of emerging technologies, the traditional network is facing enormous challenges in scalability, security, reliability and other aspects. The development of the network in the future will become the next generation of national science and technology strategic innovation technology. This paper proposes a new type of network IPV9 based on decimal system, aiming to create an autonomous, secure, high-speed, and compatible future network. This paper provides a basic introduction to the composition of IPV9 network addresses, the compatibility of IPV9 addresses with IPv4 and IPv6 addresses, and address allocation algorithms.

References

[1] G. C. Wu, G.S. Jiang and N.R. Yang: Analysis and Research on IPv4/IPv6 Protocol [J], Network Security, Technology and Applications, (2014) No.09, p.9.

[2] Z. J. Lei: *Network Engineer Tutorial (Third Edition)* (Tsinghua University Press, Beijing 2011), p.177.

[3] X. R. Xie: *Computer Networks (Fifth Edition)* (Electronic Industry Press, 2008), p.113.

[4] L.Y. Zhang: Exploration and Research on the Regularity of IP Address Subnetting in Computer Networks [J], Network Security Technology and Applications, (2023) No.07, p.2.

[5] X. Chen and H. Zhao: Theory and Practice of Informatization Construction in Chinese Universities [M], Beijing: National School of Administration Press, (2013) p.432.

[6] X.F. Wang, J.P. Wu and Y. Cui: Overview of Internet IPv6 Transition Technology [J], Small Micro Computer Systems, Vol. 27 (2006) No.3, p.286.

[7] J. Chen and Z.P. Zhao: IPv6 Explanation Volume: Core Protocol Implementation [M], Beijing: People's Posts and Telecommunications Publishing House, (2009).

[8] K.T. Niu: Analysis of Transition Technology from IPv4 to IPv6 [J], Computer and Network, Vol. 41 (2015) No.08, p.35.

[9] Z. P. Zhu: Analysis of Transition Technology from IPv4 to IPv6 [J], Journal of Taiyuan University (Natural Science Edition), Vol. 36 (2018) No.02, p.41.

[10] Y. Fu: Research and Analysis of the Transition Technology from IPv4 to IPv6 [J], Computer Development and Applications, (2011) No.8, p.32.