# Comparative Research on Key Technologies from IPv4, IPv6 to IPV9

Sun Huai
School of Computer Science and Engineering
Xi'an Technological University
Xi'an, 710021, China
e-mail: sh1227467868@163.com

Liu Zhang
School of Computer Science and Engineering
Xi'an Technological University
Xi'an, 710021, China
e-mail: 604463203@qq.com

***Abstract*—Since the United States developed the IPv4 protocol based on TCP/IP in the 1970s, it has been more than 30 years old. IPv4 is the "fourth edition of the Internet Protocol." From a technical point of view, although IPv4 has a brilliant performance in the past, it seems to have revealed many drawbacks. With the addition of multimedia data streams and security considerations, IPv4's address space is running out of crisis, and IPv4 is no longer sufficient. Under such circumstances, IPv6 was born as needed. When designing IPv6, not only the IPv4 address space was expanded, but also the parties to the original IPv4 protocol were reconsidered and a lot of improvements were made. In addition to the large number of addresses, there is higher security, better manageability, and better support for QoS and multicast technologies. It is an abbreviation for "6th Edition of Internet Protocol." IPV9 was proposed in 1992 to replace the IPv4 with the ISO/OSI CLNP protocol, using the 20B NSAP address and the platform for the available OSI transport protocol. Later, DDNS was introduced and gradually developed into an IPV9 decimal network with a 256-bit address. IPV9 masters "the right to control the use of the Internet, the allocation of IP addresses, the initiative of information monitoring, the right to use routing protocols, and the ownership of technology patents." Therefore, the research and application of a new generation of Internet Protocol Next Generation has become a worldwide hotspot.**

***Keywords-IPv4; IPv6; IPV9***

## I. INTRODUCTION

Internet Protocol (IP) is a communication protocol designed for computers to communicate with each other in the network. IP provides a common rule for computers to access the Internet. The Internet has become the largest open network in the world. With the rapid development of the global economy, the advancement of communication technology and network technology, the penetration rate of computers and mobile terminals is getting higher and higher. The problems with IPv4 are also exposed [1]. For example, in the address space, performance, network security and routing bottlenecks, IPv4 makes it difficult to meet the needs of the Internet in the future. To solve the IPv4 many problems, IPv6, IPV9 and other Internet protocols have been born.

## II. THE STATUS OF IPV4

IPv4 plays a key role in the development of the network. However, with the continuous expansion of the network scale, it can no longer meet the network development needs. Firstly, the address resources are exhausted, which directly leads to the address crisis, although the CIDR technology is not classified. The network address translation NAT technology alleviated the address crisis, but still cannot solve the problem. Secondly, the routing table expansion problem, the topology structure of the address space directly causes

DOI: 10.21307/ijanmc-2019-062

the address allocation form to be independent of the network topology. As the number of networks and routers increases, the excessively expanded routing table increases the lookup and storage overhead and becomes the bottleneck of the Internet. At the same time, the length of the packet header is not fixed, and it is very inconvenient to use hardware to implement path extraction, analysis and selection, so it is difficult to improve the routing data throughput rate. There is also an uneven distribution of IP addresses. Since most of the addresses are from the United States, most of the addresses are in the United States, resulting in a serious imbalance in IP address allocation.

There is also a lack of QoS (Quality of Service) support. The design does not introduce the QoS concept. The original intention is for the military. It does not want to be open to the outside world. Therefore, it is lacking in quality of service QoS and security. It is difficult to be real-time. Commercial services such as multimedia and mobile IP provide rich QoS functions. Although protocols such as RSVP have been developed to provide QoS support, the cost of planning and constructing IP networks is relatively high.

## III. THE CHARACTERISTICS OF IPV6

The IPv4 protocol is currently widely deployed Internet protocols. The IPv4 protocol is simple, easy to implement, and interoperable. However, with the rapid development of the Internet, the shortage of IPv4 design is becoming more and more obvious. The number of IPv4 address spaces is insufficient and the number of routing table entries to be maintained is too large[2]. Compared with IPv4, IPv6 has the following characteristics.

*1) IPv6 has a larger address space. IPv4 specified IP address length is 32 bits, there are 2^32-1 addresses, and IPv6 the IP address length is 128 bits, there are 2^ 128-1 addresses. Compared to the 32 -bit address space, its address space is greatly increased.*

*2) IPv6 uses a smaller routing table. The IPv6 address allocation follows the principle of aggregation (Aggregation) at the beginning, which enables the router to use a record (Entry) to represent a subnet in the routing table, which greatly reduces the length of the routing table in the router and improves router forwarding. The speed of the packet.*

*3) IPv6 adds enhanced multicast (Multicast) support and the support of convection(Flow Control), which makes multimedia applications on the network has made great development opportunity for quality of service(QoS , at Quality of Service) provides control Good network platform.*

*4) IPv6 has added support for Auto Configuration. This is an improvement and extension of the DHCP protocol, making network management more convenient and faster.*

*5) Better header format. IPV6 uses a new header format with options that are separate from the base header and can be inserted between the base header and the upper layer data if needed. This simplifies and speeds up the routing process because most of the options do not need to be routed.*

Although IPv6 has obvious advantages, the number of IPv4 routers is huge. The transition from IPv4 to IPv6 is a gradual process, and IPv6 must have backward compatibility. Therefore, the coexistence of IPv6 and IPv4 will coexist for a long time. Moreover, IPv6 has great drawbacks in the design of its address structure. IPv6 confuses the network hierarchy in design. The interface ID embeds the address of the physical layer into the logical address layer. In this respect, the space of the physical address forms a restriction on the IP address space, and the security does not belong to the IP layer. Designing security technologies at the IP layer should not be. Because with the development of security technology, the security method and key length will continue to change, so the development of security technology will eventually lead to the redesign of IP addresses. Due to the chaos of network-level logical relationships, IPv6 creates far more new problems than it solves.

## IV. Definition of IPV9

The new IPV9 network covers three new technologies: address coding design, new addressing mechanism and new address architecture design. It aims to build a core technology system based on the underlying IP network. On this basis, a new framework can be formed. Connected and compatible with a network system that covers existing networks (Internet with IPv4 and IPv6 technologies). 2011 US government agency has the authority of the professional and technical confirmation from the law, my country has IP framework with the United States Internet network to the prior art, proprietary technology core network sovereignty[3]. This is the patented technology of IPV9 (Method of using whole digital code to assign address for computer). The official patent name is “the method of allocating addresses to computers using full digital coding”.

The IPV9 protocol refers to the 0-9 Arabic digital network as the virtual IP address, and uses decimal as the text representation method, which is a convenient way to find online users. In order to improve efficiency and facilitate end users, some of the addresses can be directly used for domain name. At the same time, it is also called “new generation security and reliable information integrated network protocol”. It uses the classification and coding of the original computer network, cable radio and television network and telecommunication network.

## V. The architecture of IPV9

By using IPV9 routers, clients, protocol conversion routers and other devices to build a pure IPV9 network, IPV9/IPv4 hybrid network to achieve a new generation of Internet systems with independent and secure intellectual property rights. Including the domestically controllable IPV9 future network root domain name system, promote technology convergence, service integration, data convergence, and achieve cross-level, cross-regional, cross-system, cross-department, cross-business collaborative management and services. With the data concentration and sharing as the way, we will build a national integrated national big data center, accelerate the promotion of domestically-controlled independent control alternative plans, and build a safe and controllable information technology system. Separate from the control of the US domain name system and realize the independent domain name system. In order to speed up the promotion of China's international discourse rights and rules-making rights to cyberspace, we will make unremitting efforts towards building a network-strengthening country.

In the existing TCP/IP protocol, conventional packet switching cannot support true real-time applications and circuit switching, and supports applications such as transmitting sound or images in circuits in a four-layer protocol. With the demand for voice, image and data triple play, the incompatibility of human-machine interface and the environmental protection requirements for redundant links, especially the original security mechanism is unreasonable, it is imperative to establish a new network theory foundation. So in 2001, China established the Decimal Network Standard Working Group (also known as IPV9 Working Group) to study and implement security-based first-come-authentication communication rules, address encryption, as short as 16 bits up to 2048 bits of address space, resource reservation, virtual real circuit The communication network transmission mode, such as character direct addressing and three-layer four-layer hybrid network architecture, was first proposed by China and has formed a demonstration project.

The existing TCP/IP protocol is a connectionless, unreliable packet protocol with a maximum packet length of 1514 bytes. The TCP/IP/M protocol of IPV9, which is led by China, not only inherits the connectionless and unreliable packet protocol of the existing TCP/IP protocol, but also develops absolute code stream and long stream code. The data packet can reach tens of megabytes or more. After three can be transmitted directly by telephone and cable television data link is established without affecting the existing transmission network until four transmission new transmission theory until they have finished the removal of three of four transport protocol.

And continue to develop and develop and manufacture the ISO-based future network "naming and addressing" and "safety" led by China. Such as:

1) *Based on three / new four-core network architecture of PC desktops and mobile phone network Operating system kernel.*

2) *An instruction set of a new kernel based on a three-layer / four-layer network architecture network operating system.*

3) *A chip based on a new core of a three-layer / four-layer network operating system architecture.*

4) *The IPV9 block domain of the new kernel based on the three-layer / four-layer network operating system architecture.*

5) *New operating network for optical switching and router based on network operating system.*

6) *Research and development based on the header encryption system for communication after verification and IPV9 based mobile phone and industrial control.*

## VI. THE ADVANTAGE OF IPV9

Compared with the traditional IPv4 and IPv6, the changes of IPV9 mainly include the following aspects. IPV9 has a larger address space than IPv4 and IPv6. The address length of IPv4 is 32 bits, that is, there are 2^32-1 addresses. The address length of IPv6 is 128 bits, that is, there are 2^128-1 addresses. But IPV9 increases the address capacity to 256 bits, that is, there are 2^ 256-1 addresses. In mobile communications, the biggest drawback of IPv4 is that there are not enough addresses available for mobile devices that people use. If IPv6 is widely used, the problem of IP shortages around the world will be solved.

### B. Digital Domain Name System

In the digital domain name system, IPv4 and IPv6 are domain name resolutions through the United States, while IPV9 is set by countries, which avoids the limitation of IP addresses and reduces the use of domain names by the state. IPV9 is a "decimal network" with independent intellectual property rights developed according to the invention patent "Method of Allocating Addresses for Computers Using All Digital Encoding". Its decimal network introduces a digital domain name system, which can be used to convert the original binary through a decimal network. The address is converted into decimal text, allowing the computers on the network to connect to each other, to communicate and transmit data to each other, and to be compatible with Chinese and English domain names.

The digital domain name technology used by the IPV9 decimal network reduces the difficulty of network management, the vast address space and the newly added security mechanism, and solves many problems faced by the existing IPv4 [4]. The advantages of other aspects can also meet the different levels of demand for various devices in the future.

### C. Routing

In terms of routing, the increase in the size of the Internet has caused the IPv4 routing table to swell, making the efficiency of network routing declining. The emergence of IPV9 solves this problem, and the optimization of routing improves the efficiency of the network. IPV9 establishes an IPV9 tunnel between the mobile unit and the proxy , and then relays the data packet sent to the mobile unit's home address received by the “proxy” used as the mobile unit to the current location of the mobile unit through the tunnel, thereby implementing Network terminal mobility support.

The IPv6 routing table is smaller than IPv4. IPv6 address allocation follows the principle of aggregation, which enables the router to use a record to represent a subnet in the table, which greatly reduces the length of the routing table in the router and improves the routing table forwarding[5]. IPV9's routing table is very small. IPV9's address allocation follows the principle of geospatial clustering. This allows a record in the IPV9 router to represent a country subnet and an application subnet, greatly reducing the routing in the router. The length and cleanliness of the table increases the speed at which the routing table forwards packets. At the same time, this subnet can express a specific geographical location. According to this logic, only one route is needed between the country and the country. For example, the route to China is 86/64. The IPv4 routing table is extremely large and irregular. The IPv6 routing table is smaller than IPv4, but the IPv6 routing table does not contain geographic information and the routing is cluttered.

### *D. Security*

IPV9 encryption technology and authentication technology have significantly improved than IPv4, and the encryption technology proposed by IPV9 is difficult to decipher at the physical level, and the confidential performance has been significantly improved. However, at the level of network information security, there are still many factors that cause insecure network information in China. The fundamental reason is that the root servers of IPv4 and IPv6 are in the United States. Many patents related to the network are in the hands of the United States. At the same time, the risk of information exposure may also be introduced. The IPV9 is to have independent intellectual property rights of Internet Protocol, can bring a lot of protection to the information security of the country. IPV9's address space enables end-to-end secure transmission, making it possible for people to use devices to directly assign addresses[6]. Both IPv4 and IPv6 do not have the concept of national geographic location. Most of their domain name resolution servers are in the United States, and IPV9 proposes the concept of "sovereign equality", which enables each country to have its own root domain name system, which guarantees that all countries are on the Internet.

## VII. APPLICATION RESEARCH OF IPV9 SYSTEM

We designed the following 10 test scenarios to fully reflect the features and advantages of the IPV9 network system. Covers some functions of the IPV9 network system, and the test case selects several typical scenarios for testing.

### *A. Application 1—Pure the IPV9 Network Architecture*

This application implements a pure IPV9 network architecture. The simplest system includes IPV9 client / server A, IPV9 client / server B, 10G IPV9 Routers C, D. The network topology is shown in Figure 1.

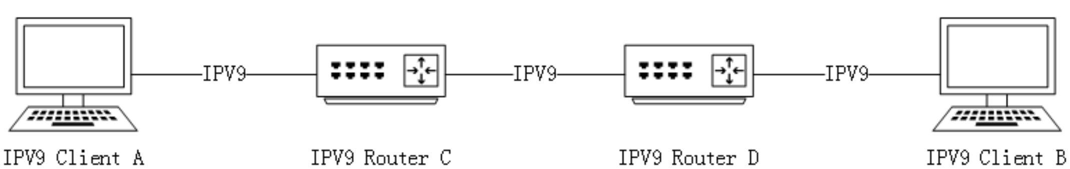


Figure 1. Pure IPV9 client - server test topology

The pure IPV9 client - server scenario is suitable for building a pure IPV9 network in an area, which is suitable for establishing an independent IPV9 network system.

### *B. Application 2—IPv4 network by purely the IPV9 connected to the network*

This application implements IPv4 network applications through pure IPV9 network communication. The simplest system includes IPv4 client / server A, IPv4 client / server B, IPV9 10G router C, D. The network topology is shown in Figure 2.

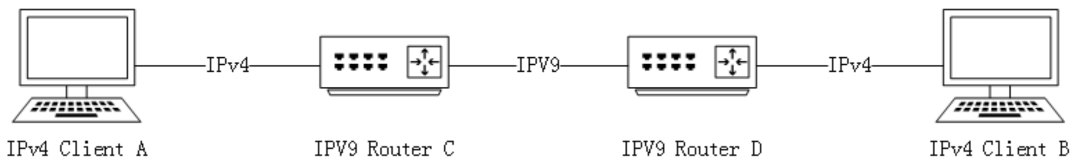


Figure 2. The IPv4 network by purely the IPV9 connected to the test network topology

This scenario is applicable to IPv4 networks in several different areas connected through the IPV9 core network to implement penetration access between different IPv4 networks. One of the main features is that in addition to the existing IPv4 network, other areas use IPV9 protocol transmission, which requires special network connections (such as fiber, DDN line, etc.) between different IPv4 networks.

### *C. Application 3—IPv4 network through 9over4 connection tunnel*

This application implements IPv4 network through 9over4 tunnel communication, the simplest system comprising an IPv4 client / server A, IPv4 client / server B, the IPV9 1OG routers C, D. The biggest difference between scenario 3 and scenario 2 is that the IPv4 public network address between routers C and D is based on 9over4 tunnel communication. This scenario simulates the IPV9 network using the existing IPv4 public network to achieve IPV9 network connectivity in different geographic regions under the current conditions, and has the ability to build a national network. The network topology is shown in Figure 3.

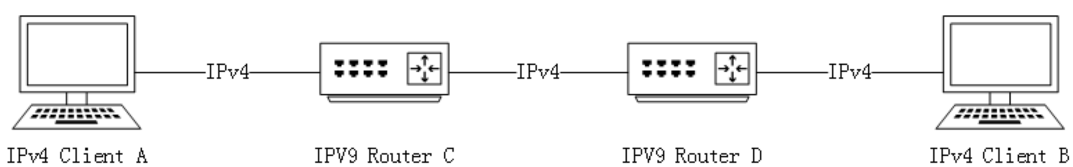


Figure 3. The IPv4 network through 9over4 connection topology tunnel test

IPv4 networks in different areas are connected through the IPV9 over IPv4 core network to achieve transparent access between different IPv4 networks. A major feature is the use of existing IPv4 networks between core networks, communicating via 9over4 tunnel mode. You can use the existing IPv4 public network to quickly establish connections between different regional IPv4 networks and implement penetration access.

### *D. Application 4—The IPV9 network via 9over4 tunnel connection*

This application implements the IPV9 network applications by 9over4 tunnel communication, the simplest system comprising the IPV9 client / server A, the IPV9 client / server B, the IPV9 1OG routers C, D. The biggest difference between this scenario 4 and scenario 1 is that the IPv4 public network address between routers C and D is based on 9over4 tunnel communication. This scenario simulates the IPV9 network using the existing IPv4 public network to achieve IPV9 network connectivity in different geographic regions under the current conditions, and has the ability to build a national network. The network topology is shown in Figure 4.

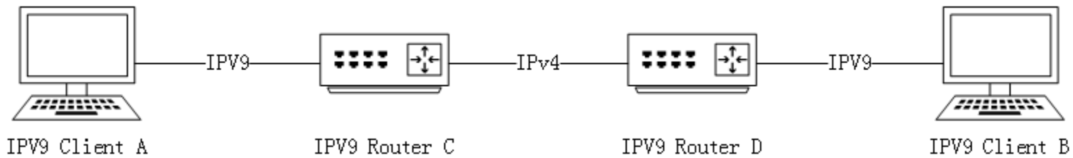


Figure 4. The IPv4 network through 9over4 connection topology tunnel test

The application implements the IPV9 network islands of N scenarios 1 to be connected through the IPV9 over IPv4 core network to implement penetration access between different IPV9 networks. A major feature is the use of existing IPv4 networks between core networks, communicating via 9over4 tunnel mode. Can use existing IPv4 quick connect different regions of the public network the IPV9 network, and access to achieve penetration.

### *E. Application 5—hybrid network architecture*

In this application, the client side of the IPV9 access router accesses the IPv4 network at the same time, the IPV9 network, and the network side of multiple IPV9 access routers access the user side of the same core router, and the network side of the core router Simultaneous access to IPV9 networks and IPv4 networks (including public networks). Can be achieved (1) IPv4 clients penetrate the network access to other subnets IPv4 clients. (2) IPv4 client normal access to the Internet. (3) IPV9 clients to access other autonomous domain of IPV9 clients. (4) Between the access routers using the OSPFV9 dynamic router protocol networking. (5) The IPV9 core routers can choose to use the 9over4 network to access the Shanghai node IPV9 network, or use the pure IPV9 protocol to access the Beijing node IPV9 network. The network topology is shown in Figure5.

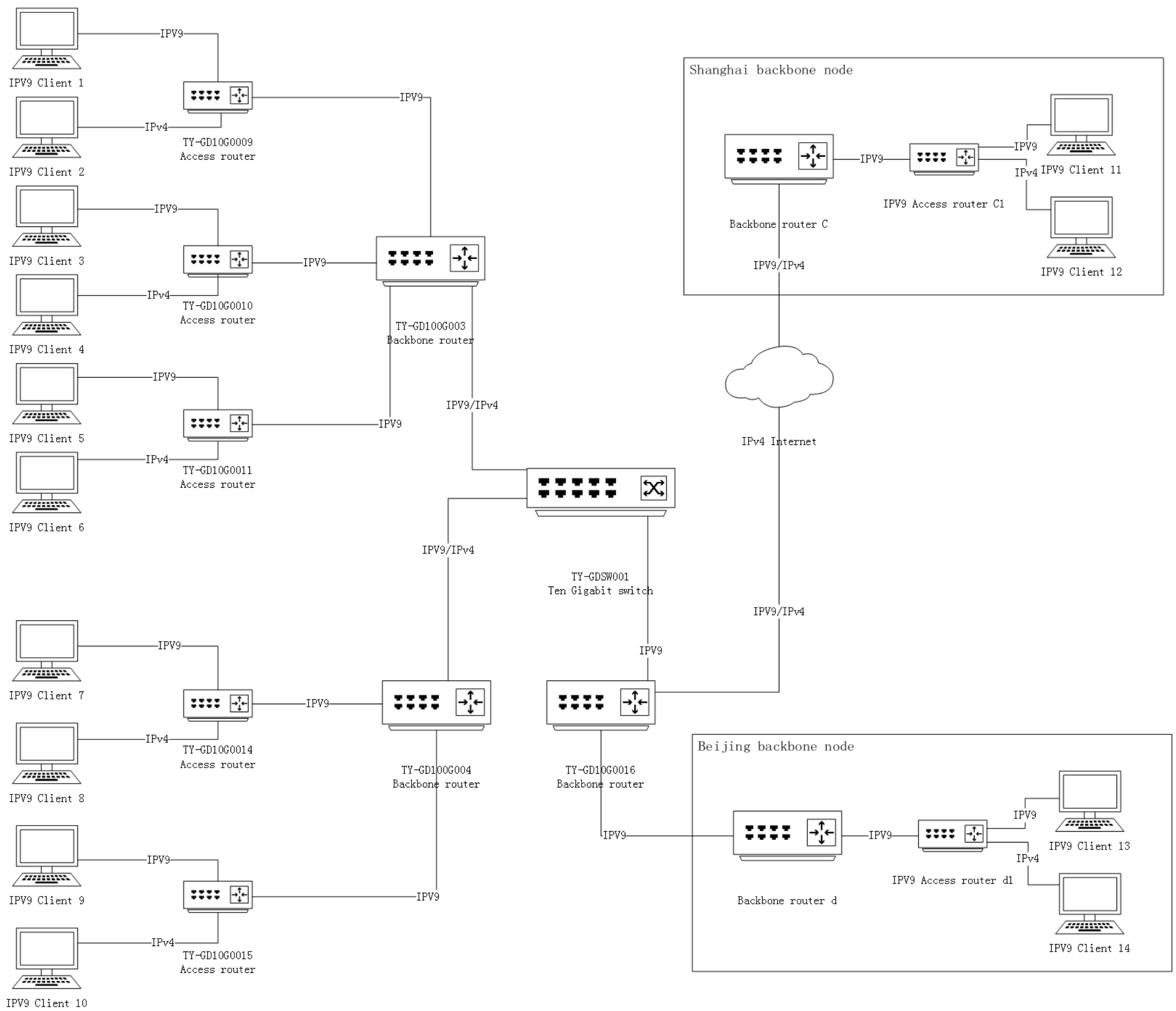


Figure 5. The IPV9 hybrid network topology architecture test

This application scenario is mainly used to build an IPV9 network environment, seamlessly integrate IPv4 networks, and IPV9 networks. All IPv4, IPV9 network islands are connected using the IPV9 protocol or the existing IPv4 public network. It is convenient and quick to connect independent networks in different regions to form a national unified network by using the IPV9 network system.

## VIII. DEVELOPMENT AND OBSTACLES

Whether transitioning from IPv4 to IPv6 or evolving to IPV9 is a gradual process, it is necessary to maintain mature services based on IPv4 and support interoperability between new and old protocols.

Net network only charge network access fees, mainstream technology not well supported by successful business models, which is IPV9 of fatal weakness. IPv6 is supported by governments and vendors around the world. IPV9 supporter limited, difficult to scale and provide good service in the short term, relying on China's own development, it is difficult to fight IPv6 research network externalities and spend a huge human and financial resources have formed the results. It is difficult through the inlet into commercial use the network market to form economies of scale and reduce costs.

## IX. CONCLUSION

With the development of the Internet, the number of Internet users is increasing, and the lack of IPv4 address resources has become a bottleneck restricting its development. Regardless of the evolution from IPv4 to IPv6 or to IPV9, IPv4-based mature services are required to support protocol compatibility. IPV9 absorbs a large number of advanced design concepts and technologies at home and abroad in the design and development process. It is a secure and controllable network information platform that can be compatible with the current IPv4 and IPv6 Internet, and can operate independently. It is suitable for establishment. National government, banks and other private networks. The IPV9 network has established a digital domain name resolution center in Shanghai, and has established sub-centers in Beijing, Changsha, and Macao, and is operating normally. In military networks and some government networks, IPV9 may gain a place from the perspective of national security. Regardless of future trends, providing a safe, efficient, stable and reliable network environment is our common goal.

## REFERENCE

[1] Xie Jianping etc. Method of using whole digital code to assign address for computer [P]. US: 8082365, 2011.12.

[2] Zang Qianli etc. A Survey on IPv6 Address Structure Standardization Researches [J]. Chinese Journal of Computers. 2019: 1-23 [2019-03-04].

[3] Xie Jianping etc. A method of assigning addresses to network computers using the full decimal algorithm [P]. CN: ZL00135182.6, 2004.2.6.

[4] V. Fuller, T. Li,Network Working Group. Classless Inter-Domain Routing (CIDR): an Address Assignment and Aggregation Strategy, RFC-1519, 1993.9.

[5] Kohler E, Li J, Paxson V, et al. Observed Structure of Addresses in IP Traffic [J]. IEEE/ACM Transactions on Networking, 2006, 14(6):1207-1218.

[6] Information technology-Future Network- Problem statement and requirement-Part 2: Naming and addressing, ISO/IEC DTR 29181-2, 2014, 12.