Research on IPv4, IPv6 and IPV9 Address Representation

YURY Halavachou
Department of the International Relations
Belarusian State University of Transport
Republic of Belarus
34, Kirova street, Gomel, 246653
Republic of Belarus
e-mail: oms@bsut.by

Wang Yubian
Department of Railway Transportation Control
Belarusian State University of Transport
34, Kirova street, Gomel, 246653
Republic of Belarus
e-mail: alika_wang@mail.ru

***Abstract*—The new generation network architecture (IPV9) is designed to solve a series of problems such as the shortage of address space and the danger of information security. IPv4 addresses have a length of 32 bits and a theoretically expressible address space of 232, while IPv6 addresses extend to 128 bits and theoretically an address space of 2128. In this paper, by studying IPv4, IPv6 address structure focuses on the new generation of network IPV9 address representation method. This method adopts the address coding method of the variable-length and variable-position, ranging from 16 bits to 2048 bits. Moreover, it adopts the mechanism of verification before communication, and relies on the method of assigning addresses to the computers on the Internet with full character codes. It redefines the address structure of the future Internet and provides new solutions for the Internet of things and the Internet of everything.**

Keywords-IPv4; IPv6; IPV9; Address Structure

I. NETWORK ADDRESS

An interconnected network is made up of LAN with interconnected nodes, also known as hosts or routers. Each device has a physical address connected to a network with a MAC layer address and a logical Internet address. Because a network address can be logically assigned to any network device, it is also called a logical address.

Internet addresses are assigned by the Internet Corporation for Assigned Names and Numbers. The association appoints three local organizations - INTERNIC, RIPENCC and APNIC - to carry out location assignments in North America, Europe and the Asia Pacific region. The purpose of this uniform allocation is to ensure that network addresses are globally unique.

II. ADDRESS SPACE FOR IPV4

The entire Internet is a single and abstract network. An IP address is a worldwide unique 32-bit identifier assigned to each interface of every host (or router) on the Internet. The structure of IP addresses makes it easy to address them on the Internet.

A. The base header of IPv4

The base first format design of IPv4 is shown in Figure 1.

DOI: 10.21307/ijanmc-2019-047

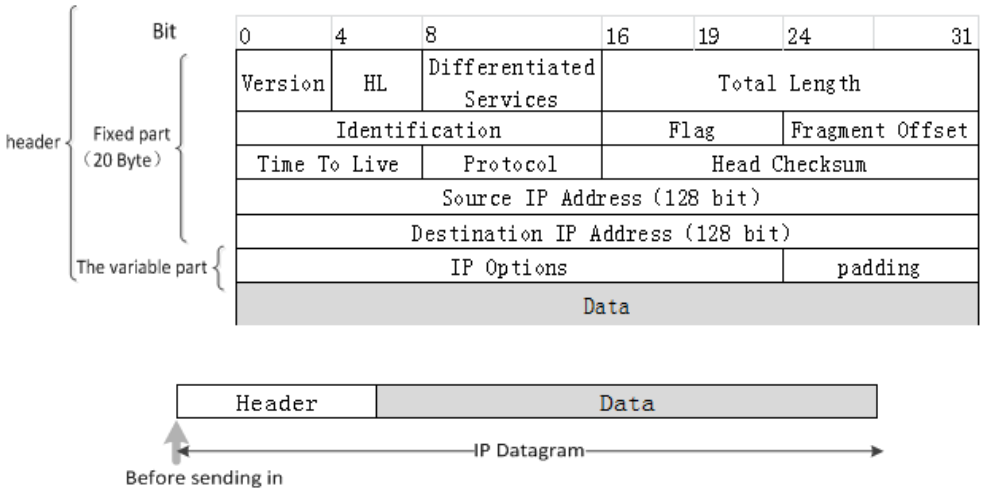


Figure 1. IP datagram format

Figure 1 shows. The first line of the above section indicates the bits occupied by each field in the header format. The whole header format is divided into fixed part (20 bytes in total) and variable part. The variable part is to increase the function of IP datagram, but the variable header length of IP datagram also increases the overhead of each router to process datagram.

The following explains the role of the fields in the base IPv4 header.

1) Version. IP Version.

2) Header Length (HL). It can represent a maximum decimal value of 15 and the most commonly used header length of 20 bytes (header length of 0101).

3) Differentiated services. It is used to get better service.

4) Total Length. It refers to the length of the sum of the radical and the data.

5) Identification. It holds the value of the counter that accumulates the number of datagram.

6) Flag. It is a total of 3 bits, the lowest bit (More Fragment) means if there is still fragmentation, the middle bit (Don't Fragment) means if there is still fragmentation.

7) Fragment Offset. It represents the relative position of a slice in the original grouping after the longer grouping is fragmented.

8) Time To Live. It represents the lifetime of the datagram in the network.

9) Protocol. It indicates which protocol is used for the data carried by the datagram.

10) Head *Checksum*. As the datagram passes through each router, the router calculates the sum again.

B. Classified IP addresses

Classification of IP address is the most base addressing method, the core of which is to divide the IP address into several fixed classes, each of which is composed of two fixed-length fields: network-id and host-id. The first field indicates the network to which the host or router is connected, and the network number must be unique. The second field identifies the host or router, and a host number must be unique within the range indicated by the network number it is on. Thus, the uniqueness of an IP address is ensured.

This two-level IP address can be recorded as: IP address: : ={< network number >, < host number >}, where ": : =" means "defined as".

Figure 2 below shows the network number field and host number field of various IP addresses:

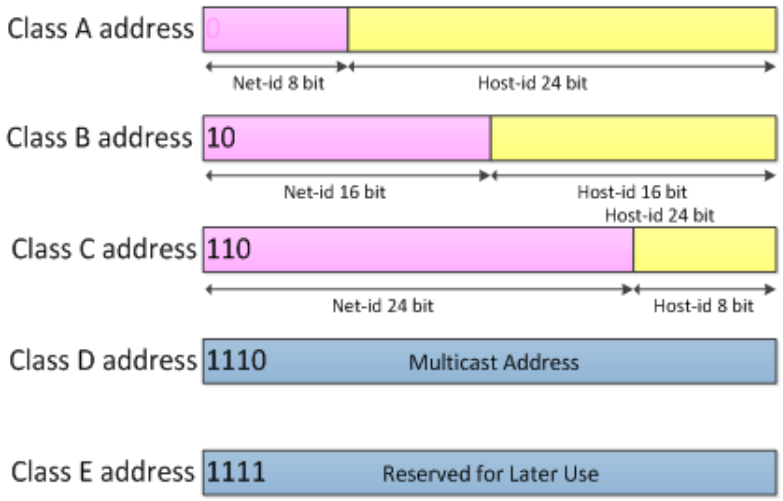


Figure 2. Network number field and host number field in IP address

Figure 2 shows:

The network number field of address of class A, B and C (the field is pink in the figure) is 1, 2 and 3 word length respectively, while the category bit of 1-3 bits in the front of the network number field is specified as 0, 10 and 110 respectively.

The host number fields of class A, B, and C addresses are 3, 2, and 1 word long, respectively.

Class D addresses (the first four bits are 1110) are used for multicast (one-to-many communication).

Class E addresses (the first four bits are 1111) are reserved for later use.

A dotted decimal notation is presented to improve the readability of IP addresses when it is 32-bit binary code. In IP addresses, every eight bits is represented in decimal, with a dot inserted between the digits. Figure 3 illustrates the convenience of this method.

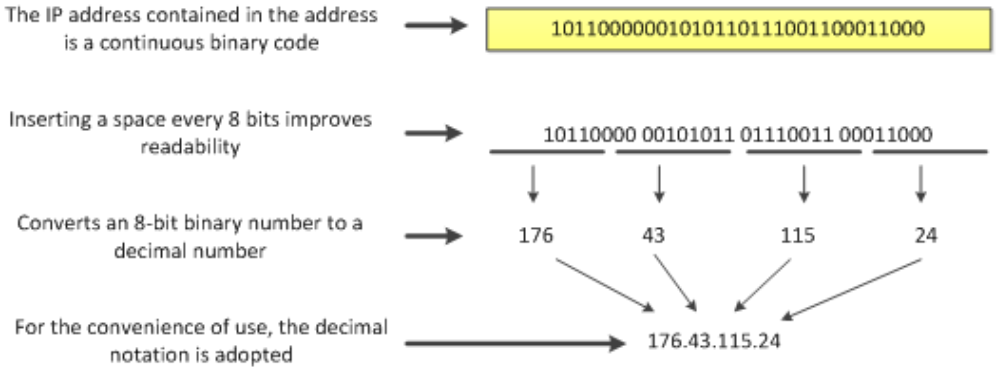


Figure 3. Illustrates the decimal system

C. Improvement of base addressing method

Because the classified IP address has defects, the IP address addressing method also goes through the following two historical stages.

1) Subnet partitioning

Subnet division mainly includes two contents, one is to make the IP address from two to three levels, improve the utilization of IP address space, improve

network performance and enhance the flexibility of IP address; The second is the use of subnet mask, subnet mask AND IP address bitwise "AND" operation (AND) to get the network address, so as to facilitate the datagram sent to the destination network.

a) Subnet idea

- The subnet is still represented as a network.
- Borrow some bits from the host number of the network as the subnet number, and the two-level IP address becomes the three-level IP address within a certain range, which can be expressed as:

IP address: : ={< network number >,< subnet number >,< host number >}

- The IP datagram can be sent to the router according to the destination network number, and then the router can find the destination subnet according to the network number and subnet number, and deliver the IP datagram to the destination host.

b) Subnet mask

A subnet mask, also known as a network mask or address mask, is a 32-bit address that consists of a string of one's followed by a string of zeros. It is used to indicate which bits are the subnet and host that identify an IP address.

The following example illustrates the role of subnet masks:

[Example] the known IP address is 132.32.63.23, and the subnet mask is 255.255.224.0.Try to find the network address.

[Answer]The subnet mask is 11111111 11111111 11100000 00000000, because the first two bytes of the mask are all 1, so the first two bytes of the network address can be written as 132.32.The fourth byte of the subnet mask is all 0, so the fourth byte of the network address is 0.It can be seen that this question only needs to calculate the third byte in the address, and we can easily obtain the network address by using binary representation of the third byte of IP address and subnet mask, as shown in figure 4 below:

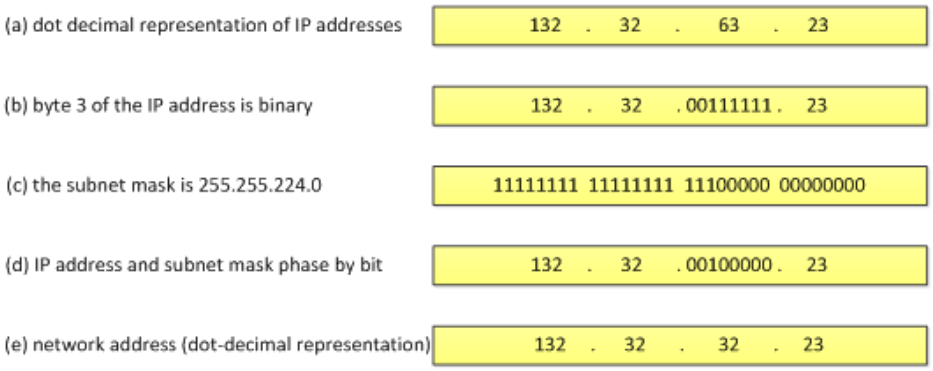


Figure 4. Solving process of network address

2) Classless Inter-Domain Routing (constitute super-netting)

The main characteristics of Classless Inter-Domain Routing (CIDR) are as follows:

a) CIDR eliminates the traditional concept of classified address and subnet division.

CIDR divides the IP address into a network-prefix and a host number, denoted by:

IP address: : ={< network prefix >, < host number >}

CIDR also uses slash notation. It is to add "/" after the IP address, and write the number of network prefix after the slash, for example:

128.85.36.17/19 = 10000000, 01010101, 00100100, 00010001

b) CIDR address block

CIDR combines the same network prefix with consecutive IP addresses to form a "CIDR address block", which can be specified by the smallest address in the address block and the number of digits in the network prefix. For example: 128.85.36.17/19 in the address block:

The minimum address is 128.85.32.0/19=10000000 01010101 00100000 00000000

The maximum address is 128.85.63.255/19=10000000 01010101 00111111

So the above address can be recorded as 128.85.32.0/20, referred to as "/20 address block" for short.

The routing table can use a CIDR address block containing multiple addresses to query the destination network. This aggregation of addresses is known as routing aggregation and is also known as composition supernettingting.

III. IPV6 ADDRESS SPACE

IPv6 is the sixth version of the Internet protocol. IPv6 USES 128-bit addresses (2128 bits), which is about 3.4 x 1038 addresses, but IPv6 addresses up to 128 bits in length does not say how many addresses there are per square meter of the earth. Rather, IPv6 addresses were designed to be large in size, with the aim of further subdividing them into layered routing domains that reflect the topology of the modern Internet. Using a 128-bit address space provides multiple levels of hierarchy and flexibility in designing hierarchical addressing and routing, which is lacking in the current ipv4-based Internet.

IPv6 addresses consist of global routing prefixes, subnet ids, and interface ids. Where the global routing prefix is used to specify a site, the subnet ID is used to specify a link within the site, and the interface ID is used to specify an interface on the link.

A. Base IPv6 headers

IPv6 datagram with multiple optional extension headers is shown in figure 5, and IPv6 base headers are shown in figure 6.

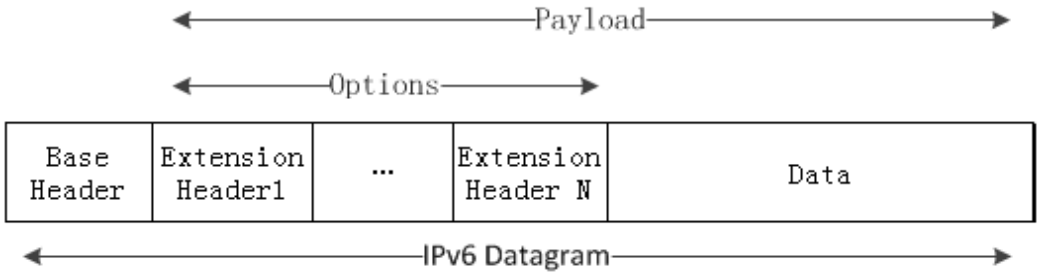


Figure 5. IPv6 datagram with multiple optional extension headers

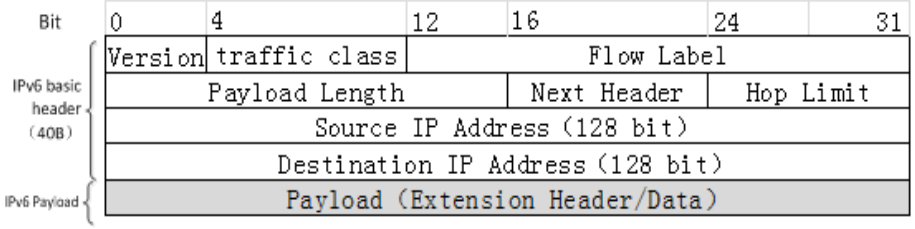


Figure 6. Basic IPv6 header with a length of 40 bytes

As shown in figure 6, the first line of the figure indicates the bit occupied by each field in the header format. Compared to IPv4, IPv6 fixed the base header with 40 bytes, eliminated many unnecessary fields, and reduced the number of private segments in the header to 8 (although the header length was doubled).

The following explains the function of each field in the IPv6 basic header:

1) Version. It specifies the version of the protocol.

2) Traffic Class. It distinguishes between different IPv6 datagram categories or priorities.

3) Flow Label. It is a new mechanism for IPv6 to support pre-allocation of resources.

4) Payload Length. It specifies the number of bytes in an IPv6 datagram other than the base header.

5) Next Head. It is equivalent to the IPv4 protocol field or optional field.

6) Hop Limit. It is used to prevent datagram from being in the network indefinitely.

B. IPv6 address representation method

1) Colon hexadecimal form

Preferred form "n:n:n:n:n:n:n:n".Each n represents a 16-bit value and is hexadecimal, separated by a colon. For example: "3FFE:FFFF:7654:FEDA:1245:BA98:3210:4562".

2) Compressed form

Writing a long string of zeros can be simplified using a compressed form, where a single contiguous sequence of zeros is represented by a double colon, ": : ".This symbol can only appear once in an address. For example, the local link unicast address FE80:0:0:0:0:0:0:10 is shortened as"FE80::/10", and the multicast address FFDE:0:0:0:0:0:0:101 is shortened as "FFED::101".Loop address 0:0:0:0:0:0:0:1compression form "::1". An unspecified address 0:0:0:0:0:0:0:0 is shortened as "::".

3) Mixed form

This form combines IPv4 and IPv6 addresses. In this case, the address format is "n:n:n:n:n:n:d.d.d.d". Where each "n" represents the 16-bit value of the IPv6 address and is represented in hexadecimal, and each "d" represents the 8-bit value of the IPv4 address and is represented in decimal.

C. Transition from IPv4 to IPv6

The transition from IPv4 to IPv6 can only be done incrementally, because the number of routers using IPv4 across the Internet is so large that it is impractical to set a cut-off point to upgrade the system. There is also backward compatibility when installing a new IPv6 system.IPv6 system must be able to complete the IPv4 system to receive, forward IP datagram and routing selection.

Here are three strategies for transitioning to IPV6:

1) Dual stack

Prior to the full transition to IPv6, there were stacks of IPv4 and IPv6 on some hosts or routers. Dual stack hosts or routers can communicate with both IPv4 and IPv6 systems.

2) Tunneling

The point of this technique is that the IPv6 datagram is disguised as an IPv4 datagram, and the entire IPv6 datagram becomes the data portion of the IPv4 datagram. This allows unimpeded access to the IPv4 network and, upon leaving the IPv4 network, transfers the data portion of the IPv4 datagram to the host's IPv6 protocol stack.IPv6 datagram is submitted to the IPv6 protocol stack to complete the communication.

3) Network address conversion/protocol conversion technology

Network Address Translation/Protocol Translation technology NAT-PT (Network Address Translation - Protocol Translation) is combined with SIIT Protocol Translation, dynamic Address Translation (NAT) under traditional IPv4 and appropriate application layer gateway (ALG).It enables communication between

hosts with only IPv6 installed and most applications with only IPv4 machines installed.

IV. THE RESEARCH STATUS OF IPV4 AND IPV6

A. *Current status of IPv4*

Due to the allocation of IPv4 addresses adopts the principle of "first come, first served, distributed according to needs", the uneven distribution makes the address allocation has a huge loophole, which makes many countries and regions have insufficient IP address resources. With the development of Internet, especially the explosive growth of scale, some inherent defects of IPv4 are gradually exposed, mainly focusing on address exhaustion, rapid expansion of routing table to the bottleneck, security and service quality is difficult to guarantee, and serious waste of IPv4 address structure. The design of IPv4 protocol does not consider the real-time transmission of audio stream and video stream.IPv4 does not provide encryption and authentication mechanisms, so the secure transmission of confidential data resources cannot be guaranteed.

B. *Current status of IPv6*

Due to the limitations of the technology era, there are many defects in the design idea of the address structure of IPv6.The richness of the IPv6128 bit address length makes it more than just a matter of extending the address. Instead of following the principle of transparency between different protocol layers, IP addresses, which should belong to the protocol of the network layer, are mixed with physical layer addresses and application layer, resulting in a series of fatal consequences.

V. IPV9 ADDRESS CODE

IPV9 not only expands the length of IP address, but also makes the network support more address levels. In addition, the method of address coding method of the variable-length and variable-position is adopted, and the parsing link is cancelled. The formal text representation method used by human is directly converted into machine language, which actually reduces the overhead of network.

A. *IPV9 header format*

IPV9 header format design is shown in figure 7.

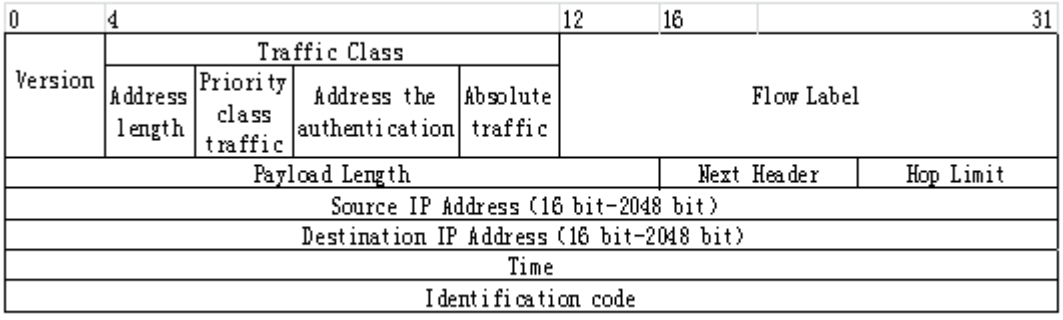


Figure 7. Header format of IPV9

Figure 7 design explanation is as follows:

1) Version. It has a length of four bits. Internet protocol version number, for IPV9, this field must be 9.

2) Traffic Class. It has a length of 8 bits. The three bits high are used to specify the length of the address, and the value is 0 to 7, which is the power of 2.The address length is 1Byte ~ 128Byte.The default value is 256 bits, where 0 is 16 bits, 1 is 32 bits, 2 is 64 bits, 3 is 128 bits, 4 is 256 bits, 5 is 512 bits, 6 is 1024 bits,

and 7 is 2048 bits. The last five bits specify the communication class and authentication for the source and destination addresses.0 through 15 are the priority values, where 0 through 5 are used to specify the priority class for the traffic.6 through 7 are used to specify a communication method for authentication before communication, which is used by the packet sender for traffic control and whether authentication of source and destination addresses is required.8 through 14 are used to specify absolute traffic that will not fall back when congestion is encountered.15 for virtual circuits.16 and 17 respectively assign audio and video, called absolute value, to ensure the uninterrupted transmission of audio and video. The other values are reserved for future use.

3) Flow Label. It is 20 bits long and is used to identify packages that belong to the same business flow.

4) Payload Length. It has a length of 16 bits, including the net payload of bytes, which is the number of bytes contained in the packet behind the IPV9 header.

5) Next Header. Its length is 8 bits, and this field indicates the protocol type in the field following the IPV9 header.

6) Hop Limit. Its length is 8 bits, and this field is subtracted by one each time a node forwards a packet.

7) Source address. Its length is 8 bit ~ 2048 bit; specify IPV9 packet sender address, using variable length and location method.

8) Destination address. Its length is 8 bit ~ 2048 bit, and the destination address of IPV9 packet is specified.

9) Time. It is used to control the lifetime of the address in the header.

10) Identification code. It identifies the authenticity of the address in the header.

B. Text representation of IPV9 addresses

This paper has developed a unified method to represent IPV9 address, including "bracket decimal", "curly braces decimal" and "parentheses bracket".

1) Bracket decimal

The bracket decimal can be expressed in the following two ways:

Method 1: use "[]" when the length is 2048 bits. Where, the parentheses are expressed in decimal notation, and the length can be written in indefinite length.

Method 2: length 256 able address in the form of representation is "y[y] [y] [y] [y] [y] [y]", where each y represents the address as a 32 bit part, and used the decimal representation. Because 232 = 4294967296. Each "y" represents a 32 bits portion of the address and is represented in decimal. The difference in decimal number of each of the range is 0 to 9, such as the first digit from left the range is 0 ~ 4, so you don't have the phenomenon of overflow.

2) Curly braces decimal

This method divides the 256-bit address into four 64-bit decimal Numbers represented by curly braces separating them. The representation is "Z}Z}Z}Z", where each Z represents a 64-bit portion of the address and is represented in decimal. It's exactly the same as Y, but it's also compatible with Y, so you can mix the two. This approach makes it very convenient for IPv4 addresses to be compatible in IPV9.Such as:

z}z}z}z;

z}z}y]y]y]y;

z}z}y]y]y]d.d.d.d;

z}z}z}y]d.d.d.d;

z}z}z}y]J.J.J.J;

3) Bracketed notation

Since IPV9 has an address length of 256 bits, whether you use four or eight segments, there are still many bits in each segment. For example:

...]00000000000000000000000000110100]...

...]01011111111111111111111111111111]...

The above situation input cumbersome, prone to errors. For convenience, the parenthesis notation --(K/L) is introduced. Where "K" means 0 or 1 and "L" means the number of 0 or 1.In this way, the above two examples can be abbreviated as:

...](0/26) of 110100]...

...]010 (1/29)]...

4) Text representation of address prefixes

The IPV9 address scheme is similar to the CIDR (unclassified addressing) scheme of IPv4 in that the address prefix is used to represent the network hierarchy. On the representation of IPV9 address prefix, a representation similar to CIDR is adopted, whose form is as follows:

IPV9 address/address prefixes length

For example, Address prefix 1706[0[0[0[210[22[0 of 200 bits can be expressed as:

1706[0[0[0[210[22[0[0/200

5) IPV9 address type

c) Pure IPV9 address

The form is Y[Y[Y[Y[Y[Y[Y[Y

Each "Y" represents a decimal integer from 0 to 232 =4294967296.

d) IPV9 addresses compatible with IPv4

The form is: Y[Y[Y[Y[Y[Y[Y[D.D.D.D

Each "Y" represents a decimal integer from 0 to 232 =4294967296. "D" represents a decimal integer between 0 and 255 from the original IPv4.

e) IPV9 addresses compatible with Ipv6

The form is: Y[Y[Y[Y[X:X:X:X:X:X:X:X

Each "Y" represents a decimal integer from 0 to 232 =4294967296.The "X" represents a hexadecimal number that originally Ipv6 ranged from 0000 to FFFF.

f) Special compatibility address

In order to guarantee the research results of IPv4 and Ipv6, IPV9 has designed some compatible addresses. The new compatibility address design idea is in this part of the address with the appropriate prefix form. In order to make their representation more convenient and ensure accuracy, the following abbreviations were introduced:

y[y[y[y[x:x:x:x:x:x:d.d.d.d

Where, each y represents the address as 32 bits, represented by decimal; Each "x" represents the original Ipv6 address of 16 bits, in hexadecimal; Each "d" represents the original IPv4 address of 8 bits, in decimal notation.

g) [] full decimal address

In order to facilitate the application of logistics code and full decimal address. Category number 5 is recommended. In the power of 10 to the power of 512, fixed length positioning method is adopted according to application needs.

h) IPV9 address for transitional period

IPV9 is compatible with IPv4 and IPv6 technical protocols for the Internet, but IPv4 and IPv6 technical protocols are not compatible with IPV9 in reverse.

C. IPv4 and IPv6 transition to IPV9

In order to solve the IPv4 flat to IPV9 transition, special design IPV9 transition address. Transitioning IPv4 to a 232 address in the IPV9 address allows a small change to the current system to complete the transition. In IPV9, there is a section of J.J.J.J address, where each "J" represents a decimal number from 0 to 28 (0~255), where the preceding [7] can be omitted in the middle of the local address, that is, local users (or designated users) can use J.J.J.J directly, which is different from the original IPv4 D.D.D.D. At the same time, this part of the user in order to smooth the

transition to full decimal can be allocated at the same time decimal. In order to improve the software and hardware in the future, there is no need to re-address, such as [7]741852963 can be written into [7]44.55.199.35 can be directly used in a local IP network to write 44.55.199.35, so that the original terminal can be used. Interim IPV9 address system can be modified to the original IPv4 system. The IPv4 header is also used, but the version number is 9 to distinguish the original IPv4.However, users may use the original terminal equipment within the territory.

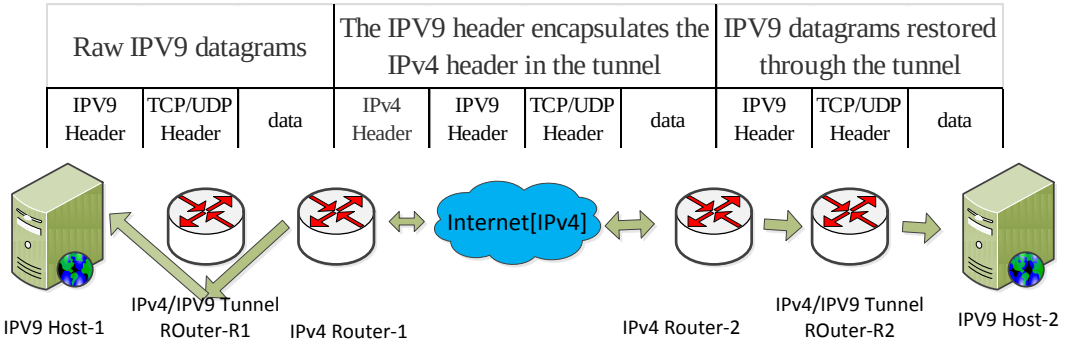
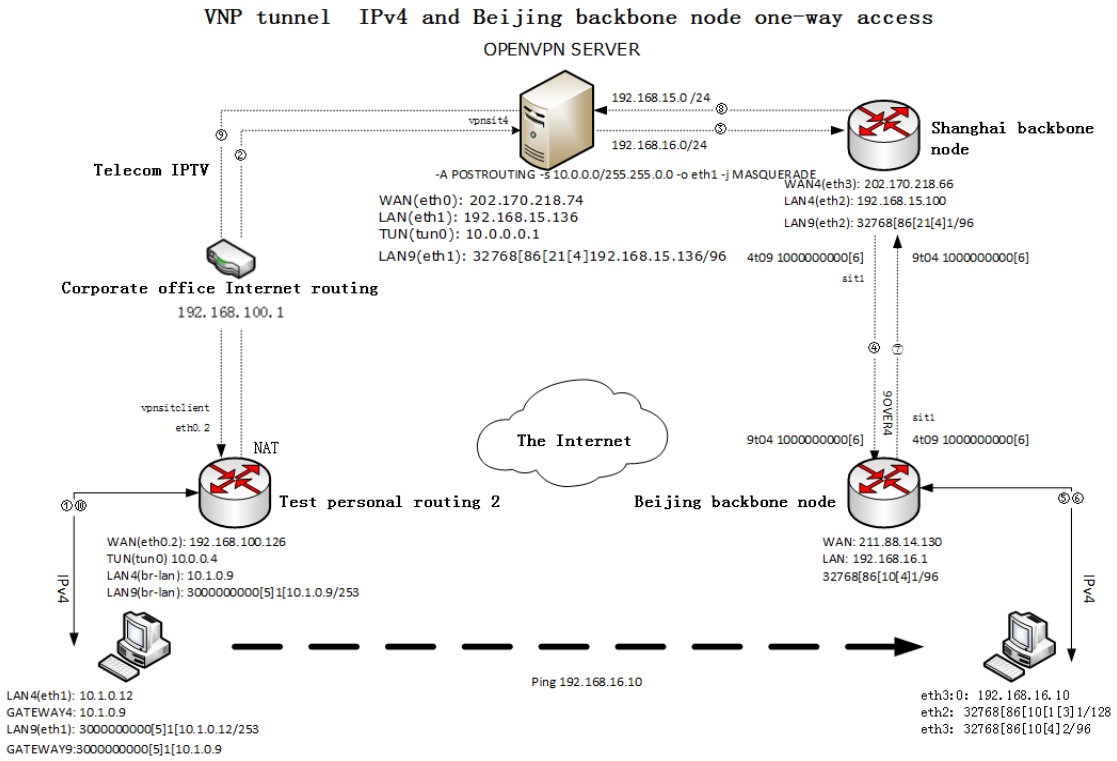


Figure 8. IPV9 is IPv4 compatible

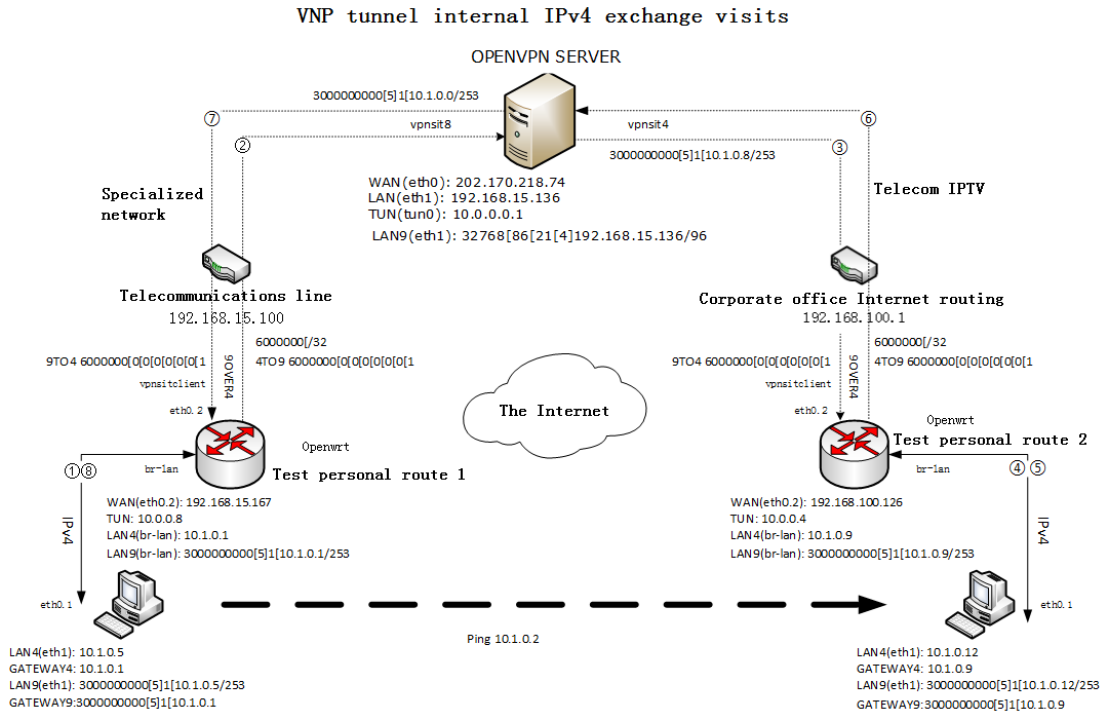
Figure 8 above means that it is possible to build the IPV9 backbone, provide application services and gradually upgrade the backbone network to IPV9 without affecting or modifying the existing terminal IPv4 applications.IPV9 inherited and transplanted most of the application functions on the existing IPv4 Internet, and successfully solved the development problem of IPV9 online application functions. Most of the existing Internet application functions can be copied to the IPV9 network, and began to enter the practical stage. At the same time, the application of IPV9 will continue to innovate and develop.

D. Support IPV9 device working mode

In the decimal network working group of scientific research, the current IPV9 support devices are ipv9-100m WIFI router, ipv9-1000m WI-FI router, ipv9-10000m router, ipv9-100g router, ipv9-linux client and ipv9-windows client. The IPV9 router network interface types include ordinary Ethernet interface, 4to9 interface (convert IPv4 packets into IPV9 packets according to custom mapping rules), 9to4 interface (convert IPV9 packets into IPv4 packets according to custom mapping rules) and sit interface (realize IPV9 data packets to be transmitted in the current IPv4 network. Implement 9over4, where IPV9 data over is the data portion of the IPv4 packet. The following takes IPV9 100/1000m WIFI router as an example to explain its working mode VPN. Under the VPN mode, most configuration of the router is completed by the background server, which is divided into IPv4 mode and IPV9 mode. In IPv4 mode, the router runs the NAT module, and the client (IPv4) accesses the Internet network in the same way as other IPv4 routers. When the client accesses the server in IPV9 backbone network, the VPN server will communicate with it. Although the pure IPV9 client is not supported in this mode, the communication between the client of WIFI router A and the client of WIF router B is supported. The data flow diagram is shown in figure 9 below:



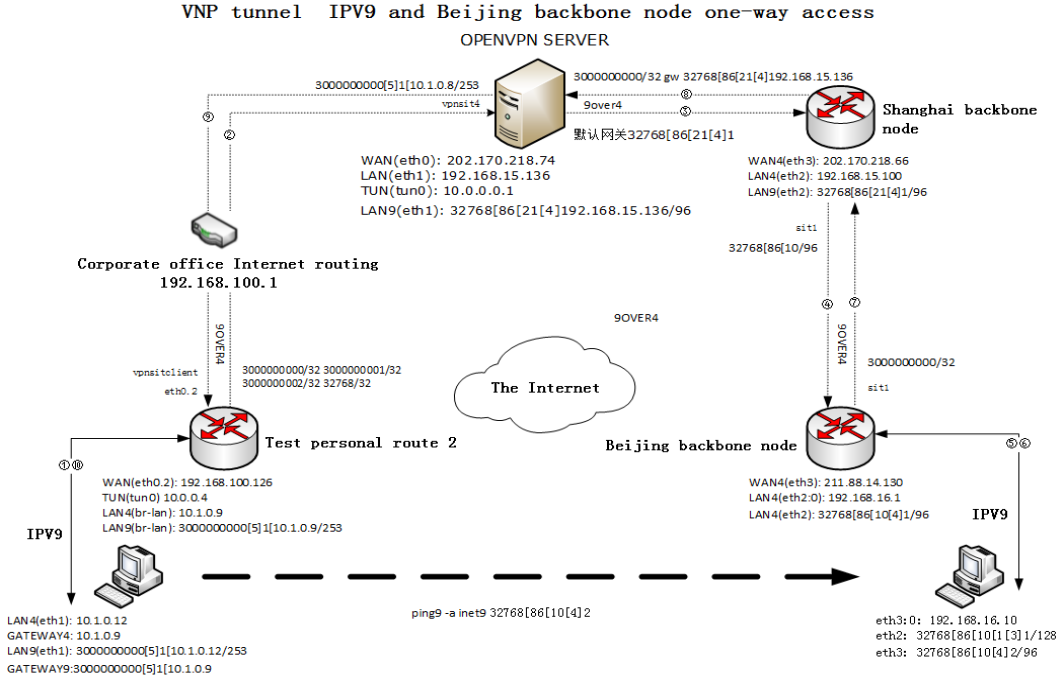
(a) one-way access between IPv4 of VPN tunnel and Beijing backbone node



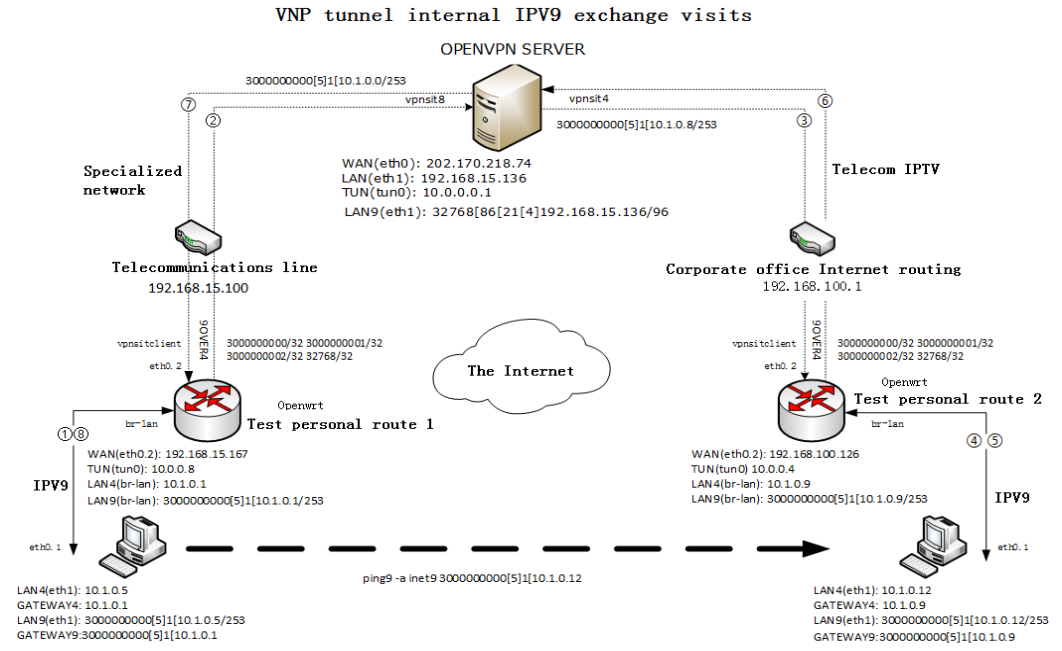
(b) IPv4 reciprocal visits within the VPN tunnel

Figure 9. (a) one-way access between IPv4 of VPN tunnel and Beijing backbone node; (b) IPv4 reciprocal visits within the VPN tunnel

In IPV9 mode, clients (IPv4) access the Internet network in the same way as other IPv4 routers. This mode supports the pure IPV9 client, but does not support the communication between the client of WIFI router A and the client of WIF router B, as shown in data flow figure 10.



(a) IPV9 exchange visits between VPN tunnel and Beijing backbone node



(b) IPV9 mutual visits within the VPN tunnel

Figure 10. (a) IPV9 exchange visits between VPN tunnel and Beijing backbone node; (b) IPV9 mutual visits within the VPN tunnel

To sum up, IPV9 inherits most functions on the existing Internet. In the protection of IPv4 and IPv6 research results, address expansion, security verification and other operations. This makes IPV9 more competitive in the development of the Internet, and its functions will continue to develop with the development of technology.

VI. SUMMARIZES

Although the use of NAT (" network address translation "), CIDR (" classless inter-domain routing ") and other technologies can alleviate the IPv4 crisis to some extent. However, this does not fundamentally solve the problem, and at the same time, it will bring about new problems in cost, service quality, safety and other aspects, but create greater challenges. But the new generation network layer protocol IPv6 itself also has the corresponding question, causes it not to have the Omni-directional. In this situation, a new network will come into being, which not only represents the progress of people's technology, but also symbolizes people's dedication to new technology. This paper mainly designs and researches the new network address coding, compares the IPv4 and IPv6 address coding, and proposes a new address coding. This method solves the problem of address exhaustion thoroughly, and puts forward the theory of verification before communication, which solves the problems of current network address exhaustion and information security. It also describes the ipv9-compatible IPv4 working mode, which guarantees the existing research results, provides some new design ideas for new network addresses, and promotes the development of new network addresses.

REFERENCES

[1] RFC - Internet Standard. Internet Protocol, DARPA INTERNET PROGRAM PROTOCOL SPECIFICATION, RFC 791, 1981.09.

[2] S. Deering, R. Hinden, Network Working Group.Internet Protocol, Version 6 (IPv6)-Specification, RFC-1883, 1995.12.

[3] M. Crawford. Network Working Group.Transmission of IPv6 Packets over Ethernet Networks.RFC-2464, 1998.12.

[4] J. Onions, Network Working Group.A Historical Perspective on the usage of IP version 9. RFC1606. 1994.04.

[5] V. Cerf, Network Working Group. A VIEW FROM THE 21ST CENTURY, RFC1607. 1994.04.

[6] Information technology-FutureNetwork-Problem statement and requirement-Part 5: Security, ISO/IEC DTR 29181-5,2014,12.

[7] Wang Wenfeng, Xie Jianping,etc.Product and servicedigital identification format for information procession.SJ/T11603-2016, 2016.06.

[8] S. Deering, R. Hinden, Internet Protocol, Version 6 (IPv6)-Specification, Network Working Group. RFC-1883, 1995.12.