Research on the System Structure of IPV9 Based on TCP/IP/M

Wang Jianguo
[1.] State and Provincial Joint Engineering Lab. of Advanced Network, Monitoring and Control
Xi'an, China
[2.] School of Computer Science and Engineering
Xi'an Technological University
Xi'an, China
e-mail: wjg_xit@126.com

Xie Jianping
[1.] Chinese Decimal Network Working Group
Shanghai, China
[2.] Shanghai Decimal System Network Information Technology Ltd.
e-mail: 13386036170@189.cn

Wang Zhongsheng
[1.] School of Computer Science and Engineering
Xi'an Technological University
Xi'an, China
[2.] State and Provincial Joint Engineering Lab. of Advanced Network, Monitoring and Control
Xi'an, China
e-mail: wzhsh1681@163.com

Zhong Wei
[1.] Chinese Decimal Network Working Group
Shanghai, China
[2.] Shanghai Decimal System Network Information Technology Ltd.
e-mail: 13331860961@189.cn

***Abstract*—Network system structure is the basis of network communication. The design of network model can change the network structure from the root, solve the deficiency of the original network system, and meet the new demand of the future network. TCP/IP as the core network technology is successful, it has shortcomings but is a reasonable existence, will continue to play a role. Considering the compatibility with the original network, the new network model needs to be compatible with the existing TCP/IP four-layer model, at the same time; it can provide a better technical system to implement the future network. Based on the Internet three-layer/four-layer hybrid architecture TCP/IP/M and ISO/IEC next-generation Internet standard solutions, this paper proposes the IPV9 system architecture, which can directly transmit audio and video data with three layers on the premise of not affecting the existing four-layer network transmission. The hybrid structure is a new transmission theory, which requires the establishment of a link before data transmission and the withdrawal of the link after the transmission is completed. It solves the problem of high-quality real-time media communication caused by the integration of three networks (communication network, broadcasting network and Internet) from the underlying structure of the network, realizes the long-distance and large-traffic data transmission of the future network, and lays a solid foundation for the digital currency and virtual currency of the Internet. The system framework is verified by practical application. It have been deployed to verify the compatibility and reliable transmission between IPV9 network and the existing network, under the independent, reliable, secure and controllable network architecture, a new generation of master root server and 13 root domain name servers.**

DOI: 10.21307/ijanmc-2019-054

Keywords-TCP/IP/M; Next Generation Internet; IPV9; Big Data Stream

I. NEW GENERATION NETWORK SYSTEM IPV9

IPv9 protocol as one of the future network concepts, IETF proposed some basic dreams of IPv9 in 1994, and looked forward to the idea of network in the 21st century. Such as: 1024-bit length address, direct routing and the 42 layer routing addressing method. However, due to the lack of research results of basic theories, address stratification technology, high research and development costs, intellectual property rights and other factors, the research publicly failed. In 1997, the IPv9 working group was disbanded and intellectual property and patent results were not obtained.

Inspired by IPv9, Chinese scholars have established a new generation of network work expert teams. Based on the patent "Method of Using Whole Digital Code to Assign Addresses for Computer", they have completed the development of a new generation of network system after more than 20 years of research and development. The development of the system, its theory and practice has reflected the novelty and originality. The decimal network has experienced the stages of assumption, theory, model, prototype, small-scale trial and demonstration project implementation. Since September 2001, the Ministry of Information Industry of China has decided to establish "Decimal Network Standard Working Group (also known as IPV9 Working Group)", "New-generation Security and Controllable Network Expert Working Group", and "Electronic Label Working Group Data", united domestic and foreign enterprises, research institutions and universities to develop the IPV9 protocol with independent intellectual property of the digital domain name and other technical standards. By June 2016, the Ministry of Industry and Information Technology announced the approval of the four standards of the IPV9 system. Through unremitting efforts in various aspects, the IPV9 system mother root server, the main root server, and 13 root name servers named after N-Z letter have been developed.

II. THE DESIGN OF IPV9 ARCHITECTURE

The conventional packet switching of TCP/IP protocol does not support real time application and circuit switching application, that is, the transmission of sound or image by circuit in the four-layer protocol. TCP/IP is a connectionless unreliable packet protocol with a maximum packet size of 1514 bytes. The main idea of IPV9 design is to combine the IP protocol of TCP/IP with circuit switching, and make use of routers compatible with both protocols and a series of protocols, so that the addresses of IPv4, IPv6 and IPV9 can be used simultaneously on the Internet.

A. The hierarchy of IPV9

IPV9 system adopts the mixed network architecture of three-layer circuit/four-layer grouping, adopts the rules of verify first and then communication, address encryption, the address length could alter from 16-bie to 2048-bit, resource reservation, and adopts character direct route transmission mode, which apply virtual and real circuit to ensure the transmission security. The architecture diagram is shown in Figure 1.

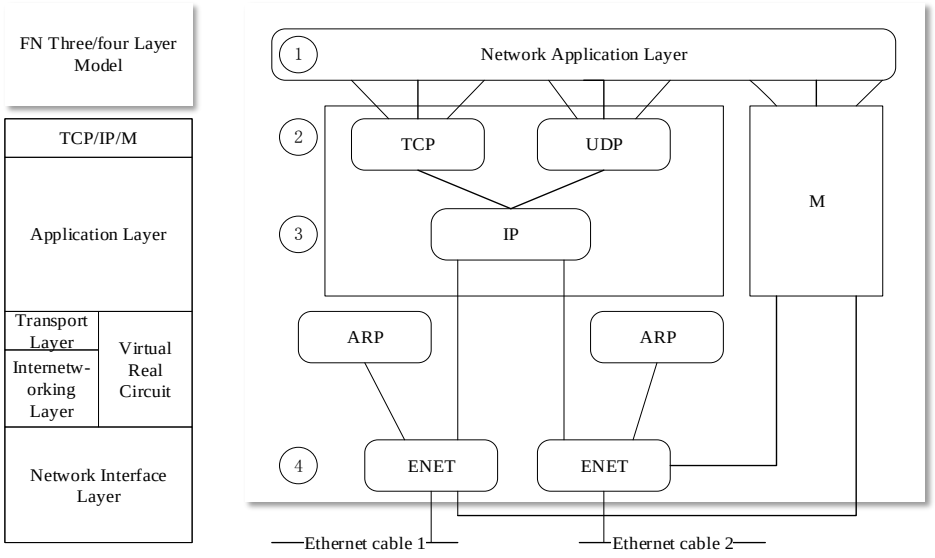

Figure 1. The Architecture Diagram

B. IPV9 connection method

TCP/IP/M protocol has developed absolute code stream and long stream code classes, a long packet can reach more than tens of megabytes. It can transmit telephone and cable TV data directly in three layers without affecting existing four-layer networks.

A four/three-layer transport protocol with a new transmit theory that is not removed connect link until finished the transmission.

The connection mode is shown in Figure 2.

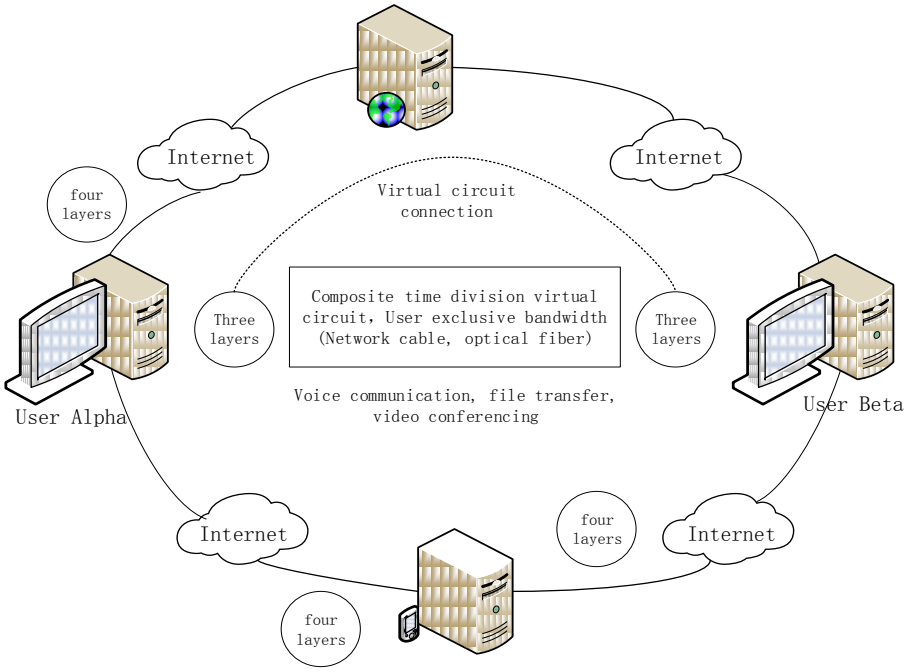

Figure 2. The connection mode

IPV9 automatic allocation access system, the system uses OpenVpn to set up virtual private network, uses IP TUNNEL for 9over4 data transmission, TR069 as the control protocol to push data to the terminal, to achieve the IPv4 subnet to subnet or IPV9 transmission. It can be a transmission between different individual routes or between the same enterprise routes, or between enterprise or individual routes to backbone routes. OpenVpn was adopted to penetrate the subnet to form the proprietary virtual network, and on the basis of the virtual network, IP TUNNEL was implemented to complete the data transmission of 9over4.In the virtual private network, the TR069 protocol is used to push the automatically assigned personal address or manually assigned business address, and at the same time, the 4to9 of the individual or business is automatically pushed to the device router.IPV9 network management system is a set of comprehensive network management system based on web interface that provides network monitoring and other functions. It can monitor various network parameters and server parameters to ensure the safe operation of server system. Both IPV4 and IPV9 protocols are supported and flexible notification mechanisms are provided for system administrators to quickly locate and resolve problems. IPV9 network and IPV9 /IPv4 hybrid network is constructed by using IPV9 design router, client, protocol conversion router and other devices. It includes IPV9 future network root domain name system, promoting technology integration, business integration and data integration, and realizing cross-level, cross-region, cross-system, cross-department and cross-business collaborative management and services. We will build an integrated national big data center and gateway bureau through data centralization and sharing, and build a secure and controllable information technology system.

C. Root domain name server

IPV9 root DNS server is mainly used to manage the Internet and decimal network home directory. IPV9 root name server system consists of a parent root server, primary root server, 13 root name servers named by N-Z, Top-level domain server named by • CHN, • USA, • HKG, • MAC and other three characters 239 countries and regions, routing management system, application server and 10 Gigabit backbone routers. The China Decimal Network Standards Working Group is responsible for management of the decimal network root name server, domain name system, and IP address.

The principle of root domain name server is that 13 root domain servers first read the primary root server, and then read the parent root server to obtain the data, and then spread to the whole network. The 13 root DNS servers are all equal. The system includes the parent root server and the primary root server. This hidden publishing host is accessed by only 13 root domain-name servers, which are read by mirror servers. The IPV9 root name server system is shown in Figure 3.

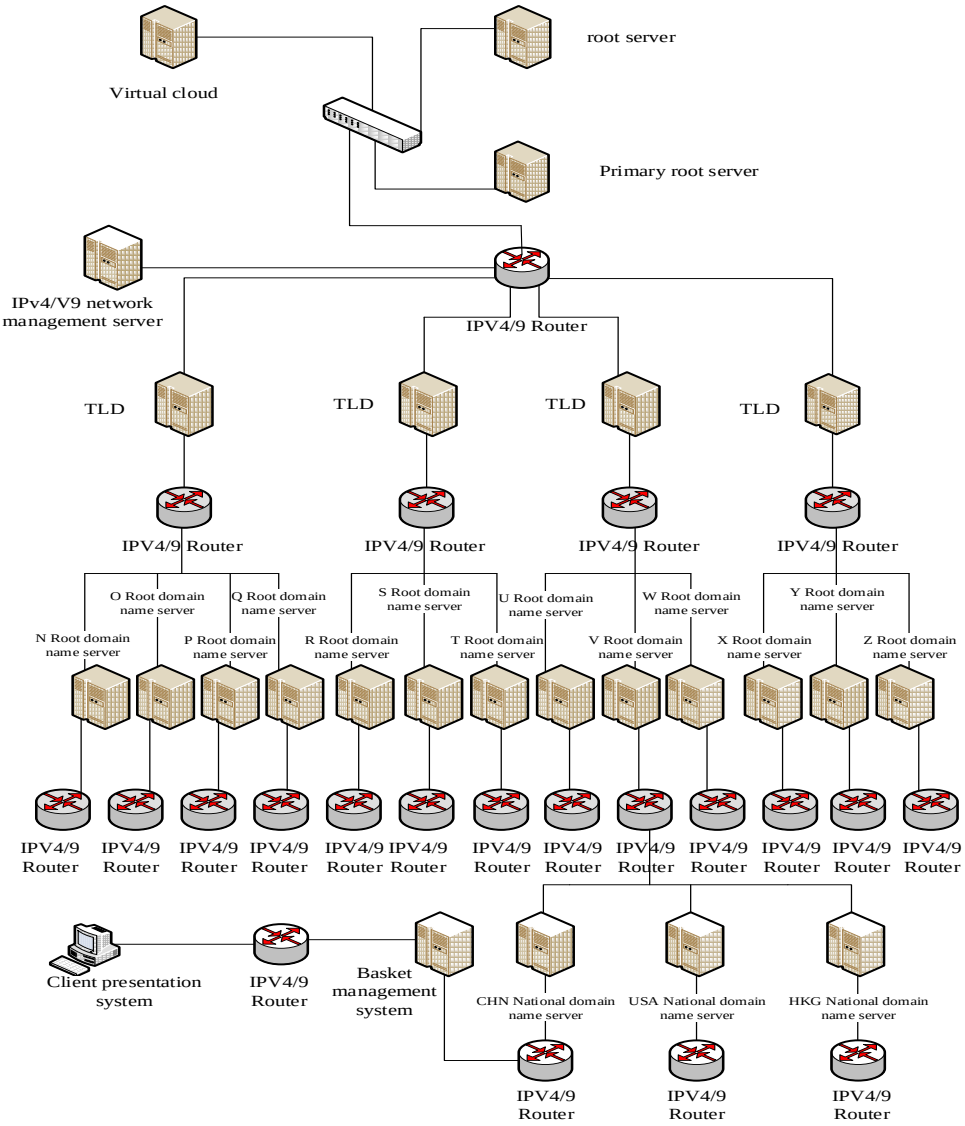

Figure 3. The IPV9 root name server system

The root name server is the highest level domain name server in DNS (Domain Name System) and is responsible for providing the authorized domain name server address for resolving the TLD (Top Level Domain). At present, the root DNS server and the gTLD (general top-level domain) and the ccTLD (country/region top-level domain) are managed and controlled by ICANN (Internet Corporation for Assigned Names and Numbers). The domain name system is the basic service of the Internet, and the root server is the foundation of the whole domain name system.

The IPV9-based root domain name resolution system can adapt to the IPv4 network, IPv6 network, IPV9 network. IPv9 resolution system can resolve the Internet user's domain name through the domain name server to obtain the corresponding access object IP address, and can send the request of non-digital domain name to the corresponding English domain name server or Chinese domain name server and domain name server in various languages, compatible with the current various domain name services.

III. THE TEXT REPRESENTATION OF IPV9 ADDRESS

The text representation of IPV9 address include "square brackets decimal" notation, "curly brackets decimal" notation, and " round brackets decimal" notation.

A. Square brackets decimal

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

1) 2048 bits are represented by "[]". The 2048 bits in the "[]" symbol are expressed in decimal notation and can be written in indefinite length.

2) IPV9 address representation with a length of 256 bits is in the form of " y[y[y[y[y[y[y[y", where each y represents a 32-bit part of the address and is expressed in decimal. 232 =4294967296, so y is a decimal number of ten digits. For example: 0003625410[0000030201]0000000000[0000000000]0000000000[00008701]0000000562.

In address representation, multiple consecutive zeros to the left of each decimal number can be omitted, but a decimal number that is completely zero needs to be represented by a zero. The contiguous all-0 field in the address is replaced by a pair of square brackets "[X]" (X is the number of segments in the all-0 field).The above address may be written as 3625410[30201[4] [508701[562.

B. Curly brackets decimal

This method divides the 256-bit address into four 64-bit decimal numbers represented by curly braces separating them. The representation method is in the form of "Z}Z}Z}Z", where each Z represents a 64-bit portion and is represented in decimal notation. It usage is exactly the same as Y, and it is compatible with Y. This greatly facilitates the current compatibility of these IPv4 addresses in IPV9.

C. Round brackets decimal

Since the address length of IPV9 defaults to 256 bits, there will still be many bits in each segment regardless of whether 4 or 8 segments are used. For example, each segment still has 32 bits with an 8-segment representation. In this way, the following situation will appear in the paragraph: ...] 00000000000000000000000000101101 0]...Such a situation is not only cumbersome to input, but also easy to make mistakes. For convenience, the parenthesis notation -- (K/L) is introduced, where "K" means 0 or 1 and "L" means the number of 0 or 1. The above example can be abbreviated as :...](0/25) of 1011010]....

D. A text representation of the address prefix

The IPV9 address scheme is similar to the supernetting and CIDR (Classless Inter-Domain Routing) schemes of IPv4, which all use the address prefix to represent the network hierarchy. The IPV9 address prefix is represented by a CIDR like representation in the form IPV9 address/address prefix length.

IPV9 addresses are written in IPV9 address notation, and the length of the address prefix is the length of the contiguous bits that form the address prefix from the leftmost part of the address. For example, the address prefix 1502[0] [0[0]390820[4027] for 210 bits can be expressed as: 1502[0] [0] [0]390820[4027] [0] [0] [0]390820[0] [0] [0]/210, short for: 1502[3]390820[4027]/210.

The ping implementation of the decimal network IPV9 address is shown in Figure 4.

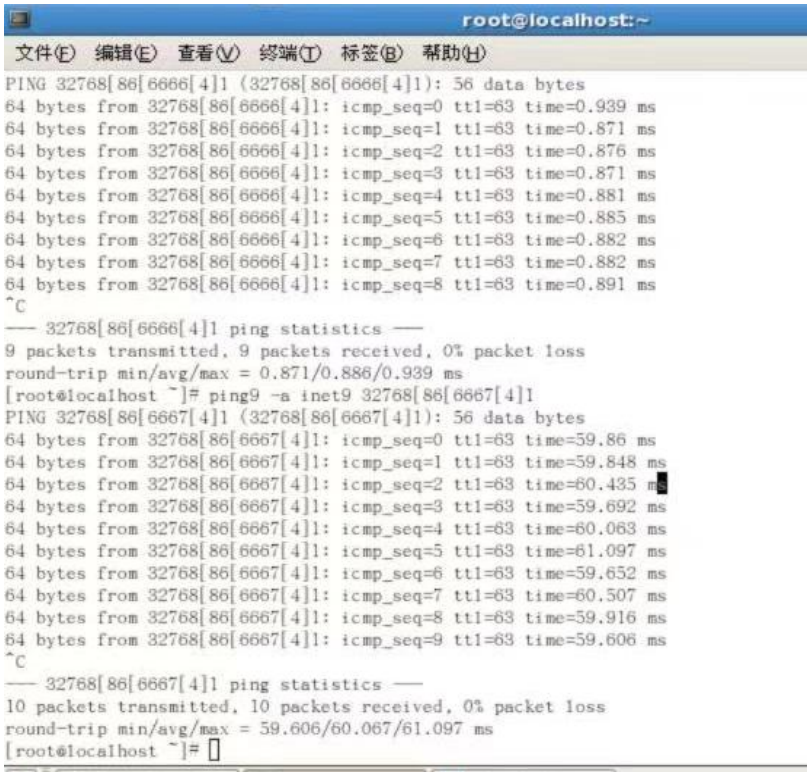

Figure 4. The ping implementation of the decimal network IPV9 address

IV. IMPLEMENTATION OF IPV9 SYSTEM

The IPV9 protocol implements the assumption that the address length is extended by the current 32-bit 1024-bit address and direct routing, and the original router class address addressing method is extended to the 42-layer route addressing method. According to the deficiency of the real network and the actual demand of future network, the new address, domain name system and routing addressing theory are studied to solve the problem of network resources and engineering implementation technology.

In order to be compatible with the existing Internet, dual stack technology is adopted. Dual stack technology refers to enabling both IPv4 stack and IPV9 stack on a single device. In this way, the device can communicate with both the IPv4 and IPV9 networks. If the device is a router, the interfaces of router are configured with IPv4 addresses and IPV9 addresses, and can connect to the IPv4 and IPV9 networks. If the device is a computer, it would have both an IPv4 address and an IPV9 address, and the ability to handle both. The IPV9 dual protocol stack is shown in Figure 5.

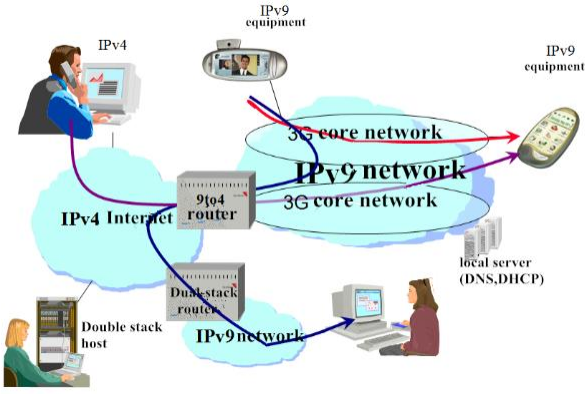

Figure 5. The IPV9 dual protocol stack

A. *Hardware component*

IPV9 system hardware devices are composed as follows:

1) Core router

Core routers, also known as "backbone routers", are routers located in the center of the network. Routers located on the edge of the network are called access routers. Core routers and edge routers are relative concepts. They all belong to the router, but they come in different sizes and capacities. The core router of one layer is the edge router of the other layer. It is used for IPv9 core network environment to realize large capacity data exchange.

2) Edge router

Edge routers, also known as "access routers", are routers located on the periphery of a network. Edge routers and core routers both belong to routers, but they have different sizes and capacities. The core router of one layer is the edge router of another layer.

3) IPV9-IPv4 protocol conversion router

IPV9-IPv4 protocol conversion router is used for mutual conversion between IPV9 and IPv4 protocols. IPv4 protocol data is converted to IPV9 protocol data by using preset mapping rules through 4to9 network interface devices.IPV9 protocol data is converted to IPv4 protocol data using preset mapping rules through the 9to4 network interface device.

4) Embedded router

Embedded router is low-cost user side access router. It can be easily deployed in the case of access to IPV9 network and the Internet.

5) Client

System support Centos5.5 32bit, Centos7 64bit client, and support mainstream Linux release later. IPv9 virtual machine that supports VMware allows customers to quickly deploy with existing hardware devices. Windows7, 9, 10 based on Windows IPv9 protocol stack client.

6) Beidou /GPS timing server

System Support Beidou, GPS satellite signal, and provide IPv4, IPV9 protocol NTP Server. User devices can be timed over IPv4 or IPV9 protocols.

B. Software system

1) IPv9 network management system

IPV9 network management system is a set of comprehensive network management system based on web interface that provides network monitoring and other functions. It can monitor various network parameters and server parameters to ensure the secure operation of server system. Both IPv4 and IPV9 protocols are supported and flexible notification mechanisms are provided for system administrators to quickly locate and resolve problems.

2) IPv9 automatic allocation access system

The system set up a virtual private network with OpenVpn, IP TUNNEL for 9over4 data transmission, and TR069 as the control protocol to push data to the terminal, and finally the IPv4 subnet to subnet or IPv9 transmission was realized. IPv4 subnet to subnet or IPv9 transmission can be implemented in different personal routing, the same enterprise routing, or between enterprise and personal routers to backbone routes.

OpenVpn is adopted to penetrate the subnet to form the proprietary virtual network; IP TUNNEL is implemented to complete the data transmission of 9over4 on the basis of the virtual network. In the virtual private network, the TR069 protocol is used to push the automatically assigned personal address and manually assigned enterprise address, and at the same time, the 4to9 of the individual or enterprise is automatically pushed to the device router.

3) IPv9 Windows protocol stack

Based on the original IPv4 and IPv6 protocols of the Windows operating system, the IPV9 protocol is added to realize the dual stack working access.

V. APPLICATION OF IPV9 SYSTEM

We designed the following scenarios to more fully reflect the features and advantages of the IPV9 network system.

A. Application 1—Pure 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 6.

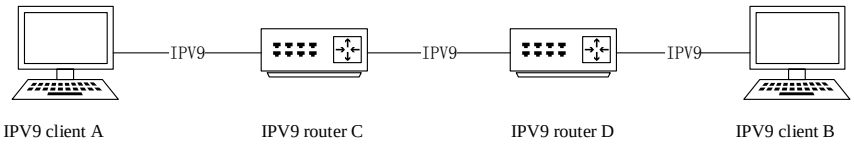

Figure 6. Pure IPV9 client-server test topology

The pure IPV9 network architecture is suitable for building a pure IPV9 network in one area and establishing an independent IPV9 network system.

B. Application 2—IPv4 network applications are connected via pure IPV9 network.

This application implements IPv4 network application to communicate through pure IPV9 network. The simplest system includes IPv4 client/server A, IPv4 client/server B, IPV9 10G routers C and D. The network topology is shown in figure 7.

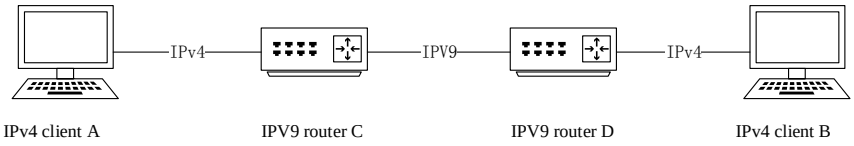

Figure 7. IPv4 network application test topology through pure IPV9 network connection

This scenario is suitable for several IPv4 networks in different regions connected through the IPV9 core network to achieve penetration access between different IPv4 networks. A main feature is that other areas are using the IPV9 protocol transmission in addition to the existing IPv4 network, which requires the different IPv4 network between the need for a private network connection (such as optical fiber, DDN line, etc.).

C. Application 3—IPv4 network is connected through 9over4 tunnel

This application implements IPv4 network application communication through 9over4 tunnel. The simplest system includes IPv4 client/server A, IPv4 client/server B, IPV9 10G router 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 that IPV9 uses the existing IPv4 public network to achieve IPV9 network connectivity in different geographic regions, and has the ability to build a national network. The network topology is shown in Figure 8.

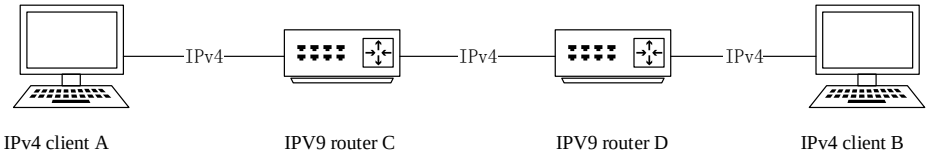

Figure 8. IPv4 network test topology through 9over4 tunnel connection

IPv4 networks in different areas are connected through the IPV9 over IPv4 core network to achieve transparent access between different IPv9 networks. A major feature is that system uses existing IPv4 networks between core networks, communicates via 9over4 tunnel mode. It uses the existing IPv4 public network to quickly establish connections between different regional IPv4 networks and achieve penetration access.

D. Application 4—IPV9 network connected through 9over4 tunnel

This application implements IPV9 network application communication through 9over4 tunnel. The simplest system includes IPV9 client/server A, IPV9 client/server B, IPV9 10G router C, D. The network topology is shown in Figure 9.

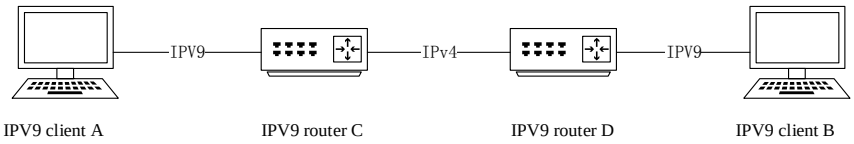

Figure 9. IPv9 network test topology through 9over4 tunnel connection

The application implements the IPV9 network to connect through the IPV9 over IPv4 core network to achieve transparent access between different IPV9 networks. A major feature is the use of existing IPv4 networks between core networks, communicating via 9over4 tunnel mode.

E. Application 5—Hybrid Network Architecture

In this application, the client side of the IPV9 access router accesses the IPv4 network and the IPV9 network. The network side of multiple IPV9 access routers accesses the user side of the same core router, and the network side of the core router accesses the IPV9 network and IPv4 network (including public network). The application can achieve the following functions: (1) IPv4 client penetrates private network to access the IPv4 client of other subnets; (2) IPv4 client accesses the Internet normally; (3) IPV9 client accesses the IPV9 client of other autonomous domains; (4) OSPFv9 dynamic router protocol is used between access routers to establish network; (5) IPV9 core routers can choose to use 9over4 network to access Shanghai node IPV9 network, or use pure IPV9 protocol to access Beijing node IPV9 network. The network topology is shown in Figure 10.

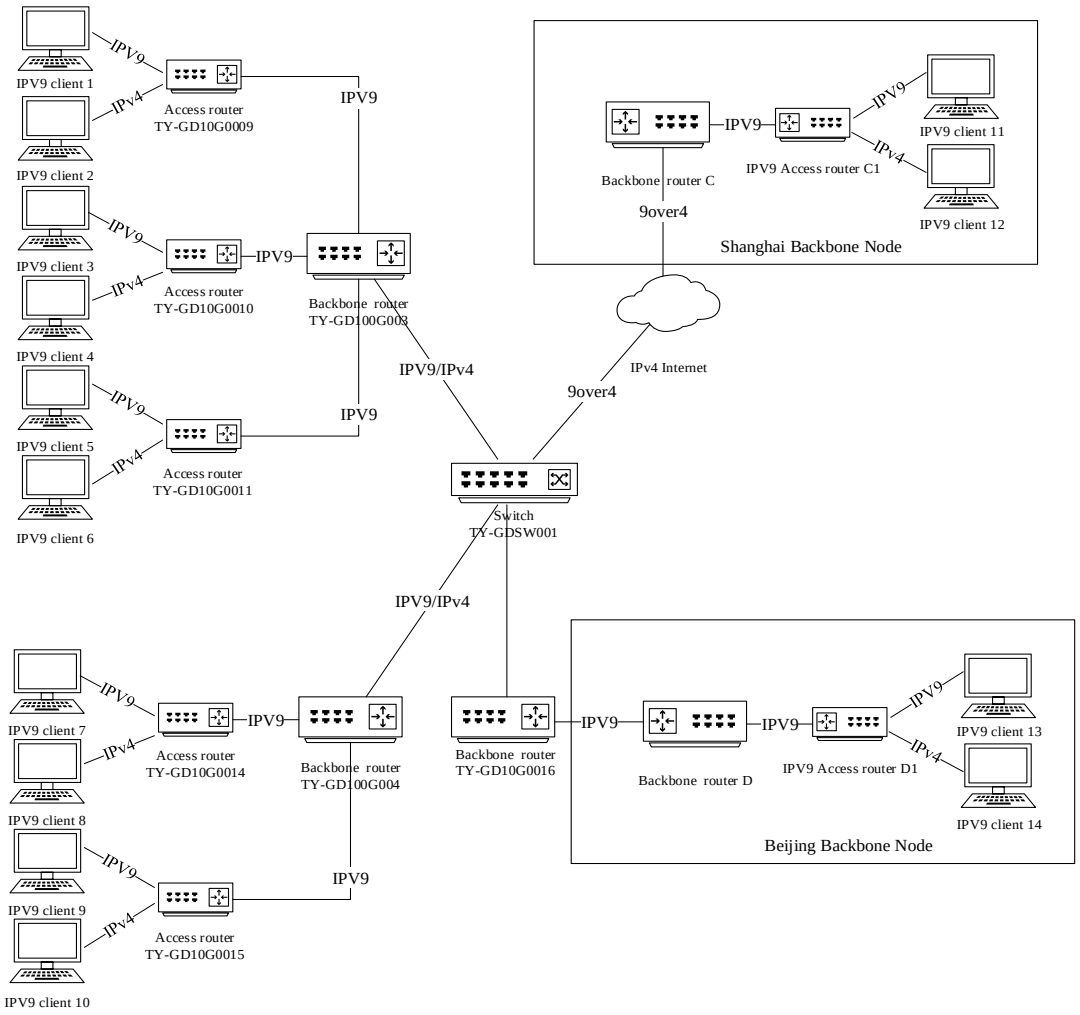

Figure 10. IPV9 hybrid network architecture test topology

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

F. Application 6--IPV9 Root Domain Name Agent System

IPV9 root domain name system provides the system expansion support capability compatible with the RFC1035 protocol under the support of a powerful database, and forms a symbiotic relationship with the existing IPv4 domain name system. At the same time, it provides an independent and controllable application guarantee for the IPV9 domain name.

The system network includes three parts: IPV9 domain name back-end support system, routing and network add service system, and application system. IPV9 domain name back-end support system can be deployed in a grid, deployed in Shanghai and Beijing to establish a root domain extension support environment that is both organic and relatively independent. The routing and network service system can choose IPv4, IPv6 networks or IPV9 network. The application system includes mobile terminal and

desktop platform support system. The network topology is shown in Figure 11.

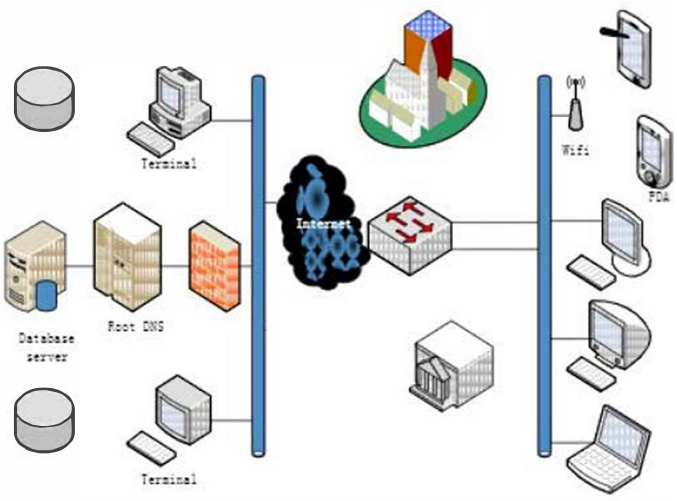

Figure 11. IPV9 root domain name proxy system topology

```
xtiger@ubuntu:~$ dig9 +trace -x 202.170.218.91 +noedns +nodnssec

; <<>> DiG 9.12.0b2 <<>> +trace -x 202.170.218.91 +noedns +nodnssec
;; global options: +cmd
.                       84400   IN      NS      n.root-servers.chn.
.                       84400   IN      NS      o.root-servers.chn.
.                       84400   IN      NS      p.root-servers.chn.
.                       84400   IN      NS      q.root-servers.chn.
.                       84400   IN      NS      r.root-servers.chn.
.                       84400   IN      NS      s.root-servers.chn.
.                       84400   IN      NS      t.root-servers.chn.
.                       84400   IN      NS      u.root-servers.chn.
.                       84400   IN      NS      v.root-servers.chn.
.                       84400   IN      NS      w.root-servers.chn.
.                       84400   IN      NS      x.root-servers.chn.
.                       84400   IN      NS      y.root-servers.chn.
.                       84400   IN      NS      z.root-servers.chn.
;; Received 506 bytes from 32768[86[21[4]3232239457#53(32768[86[21[4]3232239457)
 in 471 ms

202.in-addr.arpa.       86400   IN      NS      a.arpa-servers.chn.
;; Received 109 bytes from 32768[86[10[3[3]2#53(q.root-servers.chn) in 29 ms

91.218.170.202.in-addr.arpa. 120 IN     PTR     em777.chn.
218.170.202.in-addr.arpa. 86400 IN      NS      a.arpa-servers.chn.
218.170.202.in-addr.arpa. 86400 IN      NS      a.gtld-servers.chn.
218.170.202.in-addr.arpa. 86400 IN      NS      b.gtld-servers.chn.
;; Received 182 bytes from 172.16.3.2#53(a.arpa-servers.chn) in 187 ms

xtiger@ubuntu:~$
```

Figure 12. IPV9 root domain name proxy system analysis results

VI. SUMMARY

The main technical features and innovations of IPV9 system are as follows.

1) Independent address text format

Decimal network technology can be independent of the original IPv4 and IPv6 network networking. The IPV9 address text representation of decimal network uses the Arabic numerals of 0-9 and "[" as a separator, which is compatible with IPv4 and IPv6.

2) Infinite IP address space

The length of IPV9 address is 2256, can be up to 21024. It conforms to assumptions of ISO future networks 66N13376, 66N13488, 6N13947 and RFC1606, RFC1607. The address resources are very rich. End-to-end transmission can be achieved according to the requirements, which have high efficiency and economy. The IPV9 address uses a technique of two-sided compression and a number of brackets in the compression section, which is simple and convenient to use.

3) Safe and controllable

IPV9 USES a specific encryption mechanism for the address to achieve point-to-point transmission to enhance the privacy of users. In order to ensure the healthy and orderly development of information services, the means of verification before communication can be temporarily closed to businesses with incomplete or unqualified security measures.

IPV9 is independent of IPv4 and IPv6 Internet networking. It can effectively manage and control network security and information security. According to the actual needs, users can choose valuable information download, methods to avoid intrusion of bad information and unexpected attacks.

4) Unified coding

The domain name and the IP address synthesize, may cause the telephone, the handset, the domain name and the IP address, IPTV, the IP telephone and so on to combine into one number. This method saves the translation time between the domain name and the IP address, makes the network communication fast and convenient, and improves the communication capability of the existing network switching equipment.

At present, electronic labels and bar codes are used and managed separately. IPV9 has developed more superior and more viable RFID electronic tags, barcode unified data format and application standard

system. It can make the electronic label and barcode unified into a code, so that a commodity code has three ways of identification: one-dimensional barcode, two-dimensional code and electronic label, the three represents are global unique code, and also are the IP address of the IPV9 domain name. This feature enables barcodes and electronic tags have the same Internet access capabilities, which will greatly reduce the management costs of the global manufacturing and logistics industries.

ACKNOWLEDGMENT

This paper is sponsored by the Xi'an Decimal Network Technology Co., Ltd..

REFERENCE

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

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

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

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

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

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

[7] Xie Jianping, Xu Dongmei, etc.Digital domain name specification. SJ/T11271-2002, 2002.07.

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

[9] Wenfeng, Xie Jianping, etc. Product and service digital identification format for information procession. SJ/T11603-2016, 2016. 06.

[10] Radio frequency identification tag information query service network architecture technical specification. SJ/T11606-2016, 2016. 06.