The Shortcomings of Ipv6 and Upgrade of Ipv4

Wang Tao
Shanghai Lizard Craft Technologies Co., Ltd.,
The visiting professor of Minzu University of China
e-mail: unsnet@163.com

Gao Jiaqiong
Sichuan Vocational and Technical College
Suining, 629000, China
e-mail: 516719510@qq.com

***Abstract*—IPv6 is to solve the problem of IPv4 address exhaustion, with the development of the Internet of things, big data and cloud storage and other technologies, these technologies are gradually applied in recent years, the continuous development of new technologies application show that the IPv6 address structure design ideas have some fatal defects. This paper proposed a route to upgrade the original IPv4 by studying on the structure of IPv6 "spliced address", and point out the defects in the design of IPv6 interface ID and the potential problems such as security holes.**

Keywords-IPv6; Spliced Address; Interface ID; IPv4 Upgrading

IPv6 is a solution to the problem of running out of IPv4 addresses. In other words, it is to upgrade the IP address because the original number of IPv4 addresses is not enough to assign to more computers. The first version of IPv6 appeared in 1995, at that time the internet is in its infancy, with the development of Internet of things, big data and cloud storage technologies being gradually applied in the last decade, IPv6 has certain defects in the design of its address structure by the continuous development and application of new technologies.

Although at that time, it was believed that IPv6 adopted 128-bit address, which was large enough to meet people's large demands, so it integrated the information of the physical layer and the application layer, confused the network layer, and formed a peculiar "splicing address" structure, thus bringing potential problems such as unresolved security vulnerabilities.

I. IPV6 CONFIGURATION

IPv6is abbreviated of Internet Protocol Version 6, also known as the next generation Internet Protocol, it is a new IP Protocol designed by the Internet Engineering Task Force (IETF) to replace the current IPv4 Protocol.

A. The architecture of IPv4

IPV4 is represented in 32-bit binary. Which divide into 4 group data with symbol ". ", each group of numbers is 8 bits of binary, from 00000000~11111111, converted to decimal is 0~255, different computers on the Internet have different IP addresses; the address format for IPv4 is for example 192.168.10.1.

B. The architecture of IPV6

The difference between IPV6 and IPV4is their binary bits, IPv6 USES 128-bit binaries, which are represented in hexadecimal. Segments are separated bysymbol ":", and 128-bits are usually divided into eight groups of four hexadecimal digits.

C. Subnet prefix address

IPv6 addresses have been assigned a number of special to purpose USES, such as：

Unspecified address	::/128
Loopback address	::1/128
Multicast address	FF00::/8

DOI: 10.21307/ijanmc-2019-029

Address of local join FE80::/10

In addition, the body of an IPv6 address can be aggregation as "global unicast addresses" with prefixes ranging from 001 to 111.This unicast address adopts the basic mode of "subnet prefix" plus "interface ID", and "aggregation of whole network unicast address" adopts the mode that the subnet prefix and interface ID each occupy 64 bits for allocation.

In the case of IPv6 version RFC2373, the details of its allocation are as follows：

| 3| 13 | 8 | 24 | 16 | 64 bits |

+--+-----+---+--------+--------+-----------------------

------+

|FP| TLA |RES| NLA | SLA | Interface ID |

| | ID | | ID | ID | |

+--+-----+---+--------+--------+-----------------------

------+

Where

FP 001-111: Format Prefix (3 bit) for Aggregatable Global Unicast Addresses

TLA ID: Top-Level Aggregation Identifier

RES: Reserved for future use

NLA ID: Next-Level Aggregation Identifier

SLA ID: Site-Level Aggregation Identifier

INTERFACE ID: Interface Identifier

D. IPv4-IPv6 Each other

In order to achieve IPv4 and IPv6 connectivity, IPv4 addresses are embedded into IPv6 addresses, which are often expressed as: X:X:X:X:X:X:d.d.d.d, the first 96b USES a colon to separate the hexadecimal, while the last 32b address USES IPv4's dotted decimal, for example::192.168.0.1 and ::FFFF:192.168.0.1 are two typical examples.

E. The specific address

Special addresses include an unspecified address and a loopback address. An unspecified address (0:0:0:0:0:0:0:0 or ::) is used only to indicate that an address does not exist. This is equivalent to IPv4 not specifying the address 0.0.0.0.

An unspecified address is usually used as the source address of a packet trying to verify the temporary address is unique, and is never assigned to an interface or used as a destination address. The loopback address (0:0:0:0:0:0:0:0:0:0:0:1 or ::1) is used to identify the loopback interface and allow nodes to send packets to themselves. This is equivalent to the IPv4 loopback address of 127.0.0.1. Packets that sent to the loopback address are never sent to a link or forwarded via an IPv6 router.

II. IPV6 "SPLICE CODING" STRUCTURE

IPv6 addresses are 128 bits long, and the IPv6 address space is commonly referred to as 128 bits. But that's not true, because IPv6's address structure is designed in such a way that the address space is not 128-bit as one might expect. To understand the structure of IP addresses, it can be reference with E.164 phone Numbers, The phone number structure is "country code + area code + phone number", and three different codes represent different levels.

In IPv4 addresses, the structure is "network ID (different lengths addresses of A, B, C, D, E) + host ID".In unicast address IPv6is widely used, it also seems to be a similar to IPv4 "network ID +host ID" structure, and IPv6 network ID are changed into finer three layers, and is a fixed length subnet prefix: "top polymerization ID + secondary polymerizationID + site level polymerizationID, and the host ID of IPv4 becomes a fixed 64 bit length "interface ID".

On the surface, such a design is in line with the general address structure design law.The problem is that it is needed to"layering” in terms of the most general communication protocols and the most

common communication structure USES seven-layer protocols.Different levels of tasks should be assigned to different levels of the protocol to complete, and the different protocol layer should be transparent.

Since IPv6 designers thought the 128-bit address was too rich, and if IP addresses need to be upgraded, then it's better to take the opportunity to solve more problems. As a result, IPv6 addresses have been heavily adulterated with other protocol layers that should not be considered by the IP address layer, leading to a series of fatal consequences. In principle, IP addresses should belong to the network layer protocol, which should be transparent with the physical layer and the application layer, but IPv6's design of two large address segments mixes the physical layer address and the application layer. In fact the two addresses adopted different addressing and distribution system design, this is a very strange design, and makes the IPv6 is not a single address, it is a bit like the six post code with 13 personal ID number, the two separate coding directly spliced together to form " splice coding".

A. IPv6 Interface ID

The IPv6 interface takes RFC4291 as an example and is described below : ModifiedEUI-64 format-based interface identifiers may have universal scope when derivedfrom a universal token (e.g., IEEE 802 48-bit MACor IEEE EUI-64 identifiers [EUI64]) or may have local scope where a global token is not available (e.g., serial links, tunnel end-points) or whereglobal tokens are undesirable (e.g., temporary tokens for privacy [PRIV]).

The interface ID is resolved according to a network-wide unique identity other than the IPv6 protocol. Typically, a networkunique 48-bit (actual length is 47 bits) length MAC address is used to generate or 64-bit length IEEE eui-64 identifiers.It is also possible to obtain locally unique identifiers in the case that the globally unique identifiers are difficult to obtain. It can also get a private policy without having awhole network unique identity.

There are three ways to generate the interface ID in the case of no physical address: Manual configuration; Generate a random number; Use the node ordinal.

In this design, the name "interface ID" clearly indicates that its fundamental purpose is to use the terminal physical address to establish this part of the code. The most common design principle is that physical addresses need to be globally unique. Moreover, in the IPv6 environment, the network-wide uniqueness of the interface ID is also has great value.This is mainly reflected in the following two aspects:First, it can support mobile needs well. If the physical address is not unique, they will produce IPv6 addresses that are indistinguishable and conflict, when the two terminal devices with the same physical address arrive at the same portandthe whole system will collapse if there are too many conflicts; the second consideration is security. It is through the whole network unique physical address to determine the identity of the terminaluniquely.

According to the above analysis of IPv6 address, it can be seen that the protocol will have the following serious problems.

B. IPv6 address allocation

Let's imagine, if a telecom operator has applied for a batch of subnet prefixes, how will it use these subnet prefixes for network planning and distribution?

For example, a mobile operator M can use its top aggregation ID to plan provinces or municipalities, its secondary aggregation ID to plan cities and urban areas, and its site aggregation ID to plan each base station and sector.What does that mean?When a mobile phone user generates its IPv6 address, the address information clearly shows the province or municipality, the city and the urban areawhere the user is located, up to the subnet prefix number such as base station and carrier-cell.

If a user visits the web site GOOGLE, then GOOGLE can easily obtain the network topology on the path of mobile operator M and even accurately locate the base station and sector on the user's location.If it were just a message, it wouldn't mean much. However, after a large number of users visit GOOGLE network, the website can quickly restore all network topologies of the entire operator M, including the location of the base station, sector direction, carrier frequency number and even network performance through big data analysis.

Of course, it is not technically impossible to counter this problem. Operator Mcould allocate Subnet prefixes randomly or even dynamically. However, this dynamic adjustment cannot be carried out casually, especially when the business is relatively large, the adjustment will cause a large number of business interruption for a certain period of time.And IPv6 makes such a design for subnet prefixes is purpose to greatly improve routing efficiency at beginning.The more consistent the address planning is with the network topology, the simpler the routing table is, and the routing can be done based only on address information at the partial subnet address prefix.It is somewhat similar to MPLS (Multi-Protocol Label Switching) in the IPv4;the partial hierarchical address in the subnet prefix is a mark that can aggregate IPv6 packets within the subnet for exchange. This is really good for routing efficiency and QoS enhancement.

This is why the address of the subnet prefix is called “aggregation”. If the subnet prefixes are not assigned according to the network topology but randomly, the fundamental benefit of aggregationwill lost.If only from the view of IP routing itself, IPv6 can be aggregated subnet prefix design is indeed a very prominent advantage, to improve the routing efficiency and enhance QoS is indeed beneficial. However, in the era of big data and mobile phone positioning has been popularized, this advantage may face serious security problems at the same time.When the number of users in M network is large to a certain extent, the big data could analysis the M network topology in a very short time even if random or even dynamic subnet prefix allocation is adopted for websites, especially those with very concentrated visits like GOOGLE.

C. E.164 and IPv6

The different levels of the telephone number structure also contain network topology information in E.164,Why would IPv6 have such aeffect when E.164 Numbers don't?The reason is that E.164 serves the telephone of fixed-line network. When the number is fixed, even if the phone number is known through the caller, there is no location information and the corresponding network topology cannot be determined.

By talking to each other at point-to-point, onecanonly know the other's number, and it is rare for all users to make frequent calls to a service point.Moreover, most cases telephone network is voice service rather than data service, with little big data analysis ability.

Caller’s information is an active service provided by telecom operator. If the telecom operator does not want the other party to know the call information, it cannot provide. If the user does not move, it is difficult to accurately distinguish the boundary point between the station number and the user number.

However, IPv6 is completely different. The technologies of "user mobility, especially those with fixed interface ID", "big data", "mobile location", "cloud computing" together make the network topology of operators using IPv6 completely transparent.Because the mobile phone can be accessed through fixed networksuch as Wi-Fi, the network architecture of fixed-line telecoms operators can also be easily cracked, not only does GOOGLE have this capability, but any IPv6 Internet site with a slightly larger user can have it.

The first version of IPv6 was RFC1884, released in December 1995, before the concept of big data and the

advent of the World Wide Web, the first popular browser Mosaic1.0 was developed outin November 1993, before GOOGLE was even founded, today's technology was never expected. Although IPv6 protocol has changed many times, such as RFC2373 was releasedin July 1998, RFC3513 in April 2003 and RFC4291in February 2006, the latest standard for interface ID design is RFC8064, which was released in February 2017.

D. IPv4 and IPv6

IPv6 embeds the physical layer of information into the basic design idea of IP address, which cannot be changed once it is first formed, only the details.For example, interface ID can not only use MAC address as the global unique address tool, but also can use other more physical layer address.

Why IPv4 does not have this problem but IPv6 have?Since IPv4 is purely a network-layer address, the IPv4 addresses of the various network topologies of telecom operators are mainly used just within the network, and the communication host (the information receiving terminal) will not know these addresses.In the telecom operator network, each node of the topology has a corresponding physical layer address, including the base station and sector number. They are only used within the operator's network;this information will be stripped awayonce out of the operator's network, the other side of the communication terminal would not getthisinformation.

IPv6 conflates all physical addresses with IP layer addresses, and both sides of the communication generally know the other's entire IP address information, because a complete IP header contains both sides of the communication's IP address information. The physical layer information of the telecom operator is completely exposed in the IP address information, equivalent to streaking.

A telecom operator's network topology and network performance is one of its core trade secret, if the operators understand the consequences of IPv6, and are willing to accept it?

III. IPV6EXPOSES INFORMATION

A. Operator information transparent

In the IPv6 address application process, the entire IP address segment is not applied like IPv4.IPv6 operators can only apply for the first 64-bit subnet prefix address, the latter of 64-bit interface ID is completely another set of allocation rules, which is not subject to the management and control of operators. Address allocation rules of different structural segments are completely different. In fact, the mechanism of the allocation rules for different segments of telephone numbers in E.164 is also different. The ITU assigns a country or region code to each country and each country assigns its own area code and operator codes to each city. And then operator assigns its own numbers to users.

IPV6 is a bit of the other way around. The subnet prefix is applied in bulk, and the specific encoding is assigned by the operator itself, while the interface ID in the back is not managed and assigned by the operator.A bit like a telephone network where the area code is assigned by the operator and the user number is not managed and assigned by the operator. It's a little of confusing.

B. Users information naked

Interface technologies of IPv6 not only make telecom operators information transparent, but also have huge security risks for users. The interface ID corresponds to the terminal user address. In general, this address is a MAC address and other physical address according to certain rules generated.Once a user communicates in this way, the other party can easily restore the user's MAC address from the interface ID according to IPv6 rules.

MAC addresses are equivalent to a user's Internet ID. It's too bad that when a user visits a navigation site, the site is tracking them all the time.To make matters

worse, people who don't understand Internet technology in general, a design flaw will unwittingly use MAC addresses to generate their own interface ID, while IPv6 allows for other methods, even random and manual.What is the result of it? Hackers, professional users, and others can know how to use these methods to be anonymous, and forming "anonymous or invisible IPv6 users."Thus IPv6 classifies users into "citizens" and "incognito" by whether their interface ID has a unique physical address for the entire network.Websites such as GOOGLE, BAIDU, TENCENT, and ALIBAB, which are likely to be widely used by all Internet users, can be easily analyzing their MAC addresses in IPv6 addresses and developing corresponding software for big data analysis.This causes the real-time monitoring of user traces and behavior.

What happens once the problem is widely recognized, especially after a safety incident? Most users require their interface ID to be anonymous, invisible, or even constantly changing. This will result in the generation of interface ID from unique physical addresses across the networkeventually be discarded.In essence, the interface ID must be unique in the whole network, and the only way to ensure the uniqueness of the whole network is uniform allocation of the whole network and fixed address.Other methods, especially the interface ID randomly generated by hackers, cannot be distributed across the whole network.

Conflict detection is also only carried out within a site, at most within the site covered by the same sub-aggregation ID, and cannot be carried out across the network.Now IPv6 is not widely available, so there is no sense of the problem. However, as the number of IPv6 users on the Internet increases, the chance of interface ID conflicts will increase.This is equivalent to all users in the world are random or give their own 64 bit interface ID; then address conflict will be more and more likely.

C. Huge design safety hazard

Communication security is similar to the process of the battle between the offensive and defensive sides in the war. The security evaluation of the same technology is completely opposite to that of the two sides.The security of communication technology is also evaluated in the opposite way for different stakeholders.The stakeholders involved in the communication system include not only the two sides of the communication, but also the security supervision of the communication system by the sovereign and the detection of potential hackers.

If the communication process can be monitored, it is not secure for the communicator, but it is more secure for the monitoring party.If the communication process is encrypted and cannot be monitored by the third party, it will be more secure for both sides of the communication, but there will be information security problems for the sovereign country.Therefore, any communication security technology will not bring security benefits to everyone at the same time.In this way, it is inevitable that the security of communication should be solved in the application layer, rather than in the IP layer, that is to say, the IP layer should be neutral or in terms of security.Because the IP layer is the most fundamental protocol for network communication, security technology designed at this level will easily cause permanent damage to the security of some network stakeholders.

Anonymity was once an advantage of the Internet, but the utter inability to identify users led to a proliferation of hackers.IPv6 tries to provide a solution to communication security in the IP layer, which is mainly reflected in two aspects:First, IPv6 address design USES the interface ID setting, which provides to confirm the physical terminal of the other party.Second, IPv6 also adds authentication header AH and encapsulated security data header (ESP) to its extensions.

These security designs provide a variety of security services: (1) verify the data source identity.This is through the use of hash technology to digital signature; (2) keep the data transmission process secret.If tunnel mode is used, not only the transmitted data can be kept secret, but even the IP packet header can be.

To understand the problems with the above design, we can consider the case of INTEL's CPU security design.INTELCompany once wanted to add globally unique serial Numbers to its CPUs to increase so-called security.But the design was so strongly opposed that it locked down the world's PC users that it had to be scrapped.

IPv6 interface IDis designed to add even more serial Numbers than CPU.Because the serial numbers in the CPU also need special software to enable, not just anyone can use, and once added to the CPU serial Numbers, all CPUs will have, and we are all equal.But IPv6's interface ID allows "citizen users" to send their IP packets to each other in the process, giving them the MAC address of their terminal in the first place at the first time.This is equivalently to putting one’sID number on his forehead and revealing your identity in all correspondence.

As people living in society, they have to accept that their identity is disclosed in many cases, for example, showing one's identity card when travelling by plane or train.But if you just go to the supermarket to buy a bottle of water, to the restaurant to eat a meal, isitneeds to show ID? However, IPv6 actually requires all IPv6 users to perform any service online under all conditions before showing their ID. Is it socially acceptable?

If the people can't accept INTEL Companyadding a unique global serial number to the CPU, it's hard to understand why it can accept IPv6's interface ID design.Now that IPv6 is not widely used, people simply don't understand what IPv6's interface ID is and won't accept it once they understand and have problems with it.

In the IPv4-based Internet, if a hacker attacks a user, it is possible to find the location of the attack by using an IP address.But if the tunneling of a secure gateway in IPv6 is adopted by hackers, it is impossible to verify the data packets from the Internet.If the tunnel method is adopted by the spy agencies and criminals of hostile countries, it will be difficult for the security agencies to track their activities.Not only was it unclear what the other side was communicating with, it was unable to find out the address and how to tell the packets from each other.Can it be accepted as a sovereign country?

In fact, all the IP layer has to do is do a good job on the IP layer. The security problem to be solved by the IP layer should be limited to the correctness and reliability of the data itself, that is, how to accurately, reliably and efficiently transfer the data from the source to the terminal and the problem that should not be solved by it will not be considered. The problem of confusing the network level with IPv6 in terms of security is a permanent and insurmountable harm to the network operators, the vast of users, and national communications bodies, which is clearly unacceptable.

IV. ABOUT THE IPV4 ADDRESS SPACE

A. NAT and SDN

The IPv4 address space exhaustion problem does not exist. This may be a very shocking conclusion, but it is a real objective reality.The IPv4 address space is not commonly known as a 32-bit address space.Because of the use of NAT(Network Address Translation) addresses, IPv4 addresses are in fact vastly expanded. It's just like an extension number in a telephone network.How much can theIPv4 address spaceextend?

NAT addresses use three different types of network ID.

Class A addresses: 10.0.0.0 to 10.255.255.255,

Class B addresses: 172.16.0.0 to 172.31.255.255

Class C addresses: 192.168.0.0 to 192.168.255.255

Even in class C addresses, a public IPv4 address can extend to 65,535 NAT IPv4 addresses. In fact, the problem of insufficient IPv4 addresses is far less serious, even from purely IPv4 public addresses.As the number of Internet users approaches the total, the consumption of IP addresses will slow down.As long as there are two orders of magnitude more theoretical space than IPv4, the address space is sufficient.

Years ago we used to hear about phone Numbers going up, but we haven't heard about that for years. The reason is that on the one hand, due to the development of mobile technology, the number of fixed-line telephone users increases to a certain extent and then declines, no longer requiring more number resources.NAT addresses have the potential to extend by four orders of magnitude with minimal class C addresses. The potential is even greater if class B or even class A addresses are adopted.

To be more precise, NAPT is now commonly used, with the port number of the NAT gateway IP address used as a mapping for temporary TCP/IP links, which will have a port number limit of 2 bytes and 16 bits (65,535). There is a better way to solve this limitation.Wang Tao, the author of this article, has designed a patent technology of super IPv4, which can well solve this problem.

In addition, with the current SDN (Software Defined Network) technology, it is also easy to solve the NAPT port number limit problem.None of these technologies are complex and are truly IPv4 compatible;it is almost extending the IPv4 address space infinitely.

They all require a simple software upgrade of the edge router and the terminal TCP/IP section, no IPv6 required. So, from the address space alone, IPv6 is a lot of it, and a lot of nothing.

B. IPv4 smooth upgrade

IP address is the basic protocol of the Internet, and it is extremely difficult to solve the problem through complete and thorough replacement.The original designers of IPv6 didn't do much research on this, and decided that the 32 address space problem with IPv4 could not be solved by a smooth upgrade, so it was easy to redesign it entirely from scratch.We only have to look at one more technology case to know how important it is to upgrade smoothly in the web space, and how much effort it worth to do so.

Television technology was originally black and white, and in order to develop color TV, the difficulty to overcome was not how to realize the color TV itself, but how to make the past black and white TV network compatible and smooth upgrade. In other words, black and white TV transmission equipment can be compatible with color TV signals. The original black and white TV can receive and display color TV signals (although it is still black and white), and the new color TV can also receive the original black and white TV signals.

To solve this problem, the color signals of the three primary colors are separated into brightness signals (equivalent to black and white TV signals) and chromaticity signals, which are mixed together by a comb spectral arrangement and separated by a comb filter at the receiver end. It took more than 30 years for the industry to crack all the technical problems. It can be said that color TV system is the peak of technical complexity in analog circuit era. However, once the problem of smooth upgrades was solved, color television soon became widespread.

In the same way, compatibility and smooth upgrading of new communications technologies with existing technologies are important to their success.

C. From IPv4 to IPv6

Because IPv6 tried to bypass the problem of smooth upgrades, it took more than 20 years to extensive promotionwithno hope of real popularity. Till now still want to rely on executive order to make IPv6 forcibly popularize.Due to the large number of Internet users

around the world, if you want to achieve IPv4 to IPv6 conversion, it is impossible to complete all the users at the same time;it must be a very long transition period.In the conversion process, if only part of the users adopt IPv6, whether using tunneling mode or dual stack mode for compatibility, the users using IPv6 is actually equivalent to a private network in IPv4, and all its assumed technical advantages cannot play out.In that case, why not just use IPv4's NAT network instead? IPv6 has now become a political and technical issue in the world of communications, with all operators and users daring to oppose it, even seeming to support it, but not actively embracing it.

Some people think that the Internet of things is the most suitable for IPv6, it is all decided viewpoints, NB-IOT terminal communication in low frequency, low rate, almost no requirement of communication performance, the NAT technology is the most appropriate, use an IPv4 public address and class A private network address to expand the number of millions of Internet of things terminal.If it is not used on a large scale, the potential technical defects of IPv6 in network devices will not be discovered, and users who adopt IPv6 in the first place may encounter many problems with poor service. It won't really work until all users adopt IPv6.

V. CONCLUSION

The Internet based on IPv4 also has many security problems, but people have adapted to it, or made up for it with other technologies, which is a bit ofpessimistic to say.So, even if we don't consider IPv6 huge security problems, if it really can spread so we are also welcome, but because its span is too big to smooth upgrade, IPv4 is simple and effectively enough to solve all IPv6 want to solve the problem at the same time, and IPv6 itself poses far more security problems than it solves.All of the people in the world support it on the surface, and even agree that it is the most ideal technology, but after 100 years, it cannot be popularized. For this reason, the whole society will never end up wasting a lot of resources unnecessarily for a technology that cannot be popularized at all. Don't assume that all technology changes for the better. Who wants their zip code to keep changing?

ABOUT THE AUTHOR

Wang Tao, the CEO of Shanghai Lizard Craft Technologies Co., Ltd., an independent director of Yunnan Aluminum Co. Ltd. (000807), a Management consultant of Zhejiang Uniview Technologies Co., Ltd., and the visiting professor of Central University for Nationalities. Nanjing University of Posts and Telecommunications, graduate student of Beijing University of Posts and Telecommunications. Former Vice President of ZTE (000063) International Market, General Manager of Sumavision (300079) International Market, President of Global Investment. He has won five invention patents for network technology, published such academic monographs as "the Manifesto of Communicast Network", "Beyond War", "the Population Theory of Ecological Society", "The Upcoming World War for Food", "EV Rule All the Land", "Experiment, Measure and Science", "Principles of Scientific Economics". He was the chief editor of the training textbook "Marketing and Strategy" which has been used in ZTE's internal marketing leading cadres.

REFERENCES

[1] R. Hinden, S. IP Version 6 Addressing, IP Version 6 Addressing Architecture, Deering, Network Working Group.RFC2373.1998, 07.

[2] R. Hinden, S. Deering. IP Version 6 Addressing Architecture, Network Working Group.RFC-4291. 2006,02.

[3] R. Hinden, S. Deering. IP Version 6 Addressing Architecture, Network Working Group.RFC-3513. 1998.07.

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

[5] R. Hinden, S. Deering, IP Version 6 Addressing Architecture, Network Working Group. RFC-1884, 1995.12.

[6] F. Gont, A. Cooper, D. Thaler, W. Liu. Recommendation on Stable IPv6 Interface Identifiers, Internet Engineering Task Force (IETF), RFC-8064,2017, 02.