Research on IPv6 Address Space and Super IP Upgrade

Wang Tao

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

Wang Xiaodong

Xi'an North Opto-Electronic Science & Technology
Defense CO.,Ltd.
Xi'an, Shaanxi, China
e-mail: 506135693@qq.com

Abstract—**The IPv6 address space design is not a 128-bit address space that people think.Its special address structure leads IPv6 to go through three significantly different transitional versions if it is really implement 128bits address space.The transition between the three versions is the same as going through three different IP protocols from IPv4 to IPv6.It is often unscientific to say that IPv6 can assign an IP address to every grain of sand on the planet.This paper studies the IPv6 address space structure, MAC address and upgrade, and proposes a super IP upgrade method, and strives to achieve Internet address upgrade at the lowest cost to meet the needs of human production and life.**

Keywords-Ipv6; Address Space; Address Splicing; Address Upgrade

I.   IPV6 ADDRESS SPATIAL STRUCTURE

The IPv6 address space design is not a 128-bit address space that people think. Its special address structure leads IPv6 to go through three significantly different transitional versions if it is really implement 128 bits address space. The transition between the three versions is the same as going through three different IP protocols from IPv4 to IPv6. It is often unscientific to say that IPv6 can assign an IP address to every grain of sand on the planet.

In addition to the need fully update devices and terminals, IPv6 is extremely costly and violates the theory of smooth network upgrade. There are also major flaws in the design of address space: IPv6 addresses have a length of 128 bits. It is widely believed that the address space of IPv6 is 128 bits. It can reach 2128, but in fact, due to the specific way of designing the IPv6 address structure, its address space is not as expected.

The address design of IPv6 is very special, and many IPv6 addresses assigned to some special purposes, such as:

Unspecified address:::

Loopback address: ::1

Reserved address assigned to NSAP: prefix 0000 001

Reserved for IPX assigned address: prefix 0000 010

Embed IPv4 addresses: ::x.x.x.x and ::FFFF:x.x.x.x

Locally connected address: prefix 1111 1110 10

Local site address: prefix 1111 1110 11

Multicast address: prefix 1111 1111

In addition, the subject of the IPv6 address called "the aggregatable global unicast address", and the prefixes of these addresses are from 001 to 111. The unicast address adopts the basic mode of "subnet prefix" plus "interface ID", and the "the aggregatable whole network unicast address" is allocated in a mode in which the subnet prefix and the interface ID each occupy 64 bits.

Detailed allocation details in the latest standard RFC2373 for the IPv6 version. The biggest problem

here is the interface ID of the next 64 bits. According to the description of how to obtain the interface ID in Appendix A of RFC2373, it is obvious that the IPv6 design is that the interface ID is unique to the entire network.

Its most preferred way is to use the 48-bit MAC address of the most popular IEEE 802. The MAC address is unique to the entire network, and each NIC produced by the manufacturer assigned a unique MAC address. The IPv6 interface ID converts the MAC addresses into a 64-bit interface ID in a one-to-one correspondence by adding two fixed bytes "1111 1111 1111 1110" in the middle and setting the "u" bit to 1.

Appendix A also provides a method for generating an interface ID if there is only a physical interface address that is not unique to the entire network. . In the case of having only a non-full network unique physical address, by filling in the preceding 0 to the 64-bit interface address, in which case the u bit is set to 0 to indicate that it is local rather than full-network;

In the case of no physical address, three methods can used to generate the interface ID: manual configuration; to generate a random number; and to use the serial number of the node. We strongly recommend the use of conflict detection algorithm.

In this design, using the name of the "Interface ID", it is clear that its fundamental purpose is to use the physical address of the terminal to establish this partial address. From the most common design principles, physical addresses need to be unique across the network. The uniqueness of the whole network interface ID of great value in the use environment set by the IPv6. This mainly reflected in two aspects:

A. *Good support for mobile.*

It assumed the physical address is not unique, when two terminals with the same physical address move to the same site, there will be no difference in the IPv6 address they produce. If there are too many conflicts, the whole system will crash. Therefore, although

Appendix A recommends how to obtain interface ID without a unique physical address for the entire network, or even if it does not have a physical address, and even suggests ways to generate a random number at will. This approach cannot become mainstream, because if it becomes mainstream, the so-called "interface ID" will be completely meaningless.

B. *Consideration of its security*

The security consideration is uniquely determining the identity of the terminal through the unique physical address of the whole network. Let us assume that the interface ID must be unique to the whole network. In this way, the address space will no longer be 128 bits, but completely determined by the 64-bit interface ID.

If the interface ID is not unique to the whole network, it is inevitable that the IPv6 address assigned by two terminals with the same interface ID will conflict when they move to the same site. Although a certain algorithm can used for conflict detection, and assignanew interface ID after the conflict is found. However, if the total number of end-users exceeds 64 bits, the conflict will increase a lot. The more the conflict exceeded, the faster the probability of conflict will rise, and the conflict will soon make the conflict too large for the whole system to run.

To understand this problem more clearly, let's simplify the whole model. Let's assume that this address system is simulated with four decimal digits. Assume that the first two digits represent the site prefix and the last two digits represent the interface ID. This has 100 site spaces and 100 interface ID spaces.

Let's assume that the interface ID is unique to the whole network and that repetition is not allowed. In this way, the theoretical space of four-digit number is 10, 000, but the maximum allocated number space is 100 under the requirement of this unique interface ID, because if there are more, there will inevitably be the problem that two interfaces ID are duplicated. In the case of unique interface ID, no matter how the terminal

moves, the assigned number not repeated. Even when all terminals moved to a site, the number of each terminal is unique.

Let us assume that the allowable interface ID repeated fully use the four-digit number space. Each interface ID can have 100 repetitions under the maximum possible condition, so that there can be 10,000 terminals on the network.

However, we only need to look at one situation to know that the system is almost inoperable under such conditions: when more than 100 terminals moved to a site, each terminal cannot have a unique number anyway.At this time, only when each site has exactly 100 terminals, and they are extreme special cases such as ID, a different interface, a unique number assigned to each terminal, and no cross-site movement allowed.

Because each interface ID has 100 repeats, when a terminal accesses to any site, there is a close to 100% chance of conflict. Because the specific conflict probability model is very complex, its specific quantitative analysis is also quite difficult. To be sure: the more space there is beyond the interface ID, the more likely it is to conflict. This makes it almost impossible to determine how much the real space is when the interface ID is not unique to the whole network. At least for now, IPv6 supporters have not given a mathematical model to solve the problem.

If the interface ID is strictly required to be unique to the whole network, the IPv6 address space is only 64 bits, not 128 bits. Let's not discuss whether 64-bit address space is enough, but the difference between 128-bit and 64-bit is too big. The relationship between the two is not half, but $2^{64}=18446744073709551616$ times, about 184.5 billion times.

Proponents of IPv6 can argue that unicast addresses now only allocated 1/8 of the space portion with a format prefix of 001. If the prefix of 010-111 enabled after the address is insufficient, the address structure of "prefix" + "interface ID" changed, so that the latter 64

bits do not need to have the uniqueness requirement of the whole network. We admit that this does solve the problem of the above interface ID determining the overall address space, but what does this mean? This means that the most basic structure of the address has undergone a major change, and the entire network routing protocol will need to be fully upgrade to support it.

Is this finished? Not yet. Because the physical address of the most commonly used physical address IEEE 802 is now 48 bits, and the u bit is required to be set to 1 in IPv6 to indicate that it is a unique address of the entire network. Theseaddressesin IPv6 by insert two fixe bytes in the middle to get the 64-bit interface ID. Therefore, under the actual physical ID technology conditions, the real interface ID space is only 47 bits.

How much address space is there for 47 bits? It is only 15 digits more than IPv4, and the difference is $2^{15}=32768$ times. If we assume that the current IPv6 used up after the IPv4 address used up, the annual address consumption is calculate at an annual increase of 30 per cent, and the expanded address space used up in only 40 years. People are happy to think that as long as IPv6 is used, the address space is infinitely wide.If we know that the address space limited by MAC address space because of its special address structure, will there be infinite regret?

If operators know that because IPv6 adopts this special address design, the IPv6 address they apply for actually not directly related to the available address space in theory, will it feel that it is too inexplicable?

II. MAC ADDRESS AND IPV6 ADDRESS

Since the address requested by the user only determines the prefix address, and the prefix address is only the identity of the network node, the following interface ID not managed by the network operator, which is just as the operator only allocates the area code in the telephone network. The subscriber number

is notmanaged by the operator at all. This will have serious consequences.

If the 47-bit MAC space consumed, it is possible to solve the problem from the IPv6 address structure. This requires a new physical ID technology to upgrade the MAC address from 48 bits to 64 bits.This means that all network interfaces in the world must upgrade to achieve this.

From the above analysis, the 128-bit IPv6 address protocol is not a single protocol. If you want to achieve the true 128-bit space, there are actually three major differences between the versions: one currently developed with 47 valid IPv06 of address space.The other is IPv6 with full 64-bit interface ID space, 64-bit effective address.Finally, the basic address design structure of "prefix + interface ID" is completely changed, and IPv26 with 128-bit effective address space is available. The transition between these three different 128bits IP addresses is almost equivalent to the transition between three completely different IP address protocols, and its economic cost and technical difficulty are huge.

Another serious threat is that if IPv6 uses a random algorithm to allocate interface IDs, there must be a certain probability of an address conflict in theory. The more terminals use the random allocation method, the greater the chance of address conflicts.

If the interface ID generated again after the conflict still conflicts, the valid method at this time is manually configure the interface ID. After adopting the DHCP protocol, IPv4 can at least complete eliminate the manual configuration of IP addresses. The new IPv6 in

the protocol design must have the problem of manually configuring the IP address that not be absolutely eliminated theoretically. This is undoubtedly very annoying.

There are very few users of IPv6 and this problem not seen at all. If a huge number of IPv6 terminals appear on the Internet and the problem of using the MAC generation interface ID discovered by the user and all turned to the randomly generated interface ID, the address conflict problem becomes more and more obvious.

III. RESEARCH ON THE NUMBER OF IPV6 ADDRESSES

The fundamental purpose of developing IPv6 is to solve the problem of insufficient IPv4 address space, and when faced with the problem of insufficient IPv4 address space, people have repeatedly claimed that "no one thought of (IPv4) space is not enough 20 years ago." Whenever people talk about IPv6's address space, they say triumphantly that IPv6 can assign an IP address to every grain of sand on Earth.

We not say whether it is necessary to assign an IP address to every grain of sand on the earth, or how much IP address space supported by the IPv6 developed now. What we have to ask is whether anyone really calculated the earth on the earth. How much grain of sand?

Let us now roughly calculate the surface area of the Earth (excluding the ocean area) as:

$$1.49 \times 108 km^2 = 1.49 \times 1014 m^2 = 1.49 \times 1020 mm^2 = 1.49 \times 1026 \mu m^2 \tag{1}$$

Taking the thickness of the earth's surface for 10 kilometers, and assuming that the surface area change caused by the spherical thermal expansion and

contraction not considered, its volume roughly estimated as:

$$1.49 \times 109 km^3 = 1.49 \times 1018 m^3 = 1.49 \times 1030 mm^3 = 1.49 \times 1036 \mu m^3$$

(2)

If we assume that the smallest sand size calculated at 0.1 microns and that all the land surfaces 10 kilometers thick on Earth become sand of this size, the number is 1.49*1039.

Then calculate the IPv6 protocol address space. The 128-bit address space is:

$2^{128} = 3.4 \times 10^{38}$ An average of 0.1 micron-sized sand has only about 0.2 addresses, which is not enough. The 64-bit address space is 264=1.845*1019.

About 100 billion grains of sand assigned an IP address per 100 billion grains of sand. If you want to assign 1 IP address to each grain of sand, the sand size is as large as 0.1 cubic meters, and the 47-bit address space is: $2^{47} = 1.41 \times 10^{14}$. This quantity requires 100000 huge sand the size of 1 cubic meter to get a IP address.

Then, IPv6 has cost so much, even if its address space shrinks by 81 bits, from 128 to 47, its new design, such as security, should always have merit. Unfortunately, it is the security design of IPv6 with great security vulnerabilities.

IV.   SUPER IP UPGRADE

For IPv6 to succeed, no other competitive technology will emerge in the next 15 to 20 years, and people around the world will patiently wait for IPv6 technology slowly replaced existing network devices. This is impossible. If there is a very simple and effective competitive technology during the period, and quickly popularized in the short term, then all the investment in IPv6 wiped out. This is by no means an unfounded alarmist. The process of replacing ISDN and ATM with IP is such a case.

At present, we have successfully developed super IP technology. The greatest value of this success is that we have proved that competitive technology can quickly replace IPv6.

It is proved theoretically that as long as the IP address upgrade design is carried out by using N × IPv4 (positive integer N > 1), it is possible to break through the limitation of IPv4 address space under the premise of 100% compatibility with IPv4. This rapidly increases the risk of IPv6 eliminated to nearly 100 per cent.

Network technology is different from general technology; the upgrade of its technology is a one-stop move. This unified requirement of the whole network standard of network technology puts forward a special requirement for its technology upgrade-the smoothness of upgrade. The smoothness of network technology upgrade and evolution is not an ordinary technical requirement; it is almost a heavenly rule and not violated.

If this law is violate, even if this new technology supported by all international standards organizations, all governments, all operators, and all equipment manufacturers in the world, it is equally difficult to succeed.

The design of IPv6 adopts a completely different protocol from IPv4. IPv6 adopts the behavior of completely pushing IPv4 upside down, and its upgrade cost is very huge and the time is very long. According to the difficulty of technology upgrade, the objects that IPv6 needs to upgrade be divided into four parts: a. the core routing node device; b. various devices on the edge (routers for enterprise and individual users, switches, etc.); c. terminal or server operating system. d. Terminal or server application software.

Relatively speaking, since the core node devices and computer operating systems supported by large manufacturers, the core network is generally operated by large operators, so the technology upgrade is relatively easy, and the steps can be relatively easy to unify. In fact, computer operating systems have long supported IPv6.

However, all kinds of IP devices and applications on the edge are the difficult problem of technology upgrade. First, their number is extremely large, a wide variety, is the real difficulty in the upgrade work; second, they provide technical support to a very large number of manufacturers, and a considerable number of small manufacturers, weak. Third, they have a large number of owners and guided by a unified ideology. A large number of enterprise-class IP devices owned by various enterprises, and their technological upgrades dominated by their own will. On the issue of IPv4 address space; although the industry has been shouting that the address will run out, no one can give exact point in time when the IP address will run out.

According to statistics, in 2017, the funds for purchasing IP equipment by China Enterprise Network alone are about 16 billion, all of which are pure IPv4 equipment. Routers and switches each account for about 80 billion. IPv4 and IPv4 dual protocol stack equipment mainly used in the experimental network of education network. The financial depreciation of IP equipment in an enterprise calculated on a 5-year basis, but the actual service life is generally 8 to 10 years. In this way, if you want to transition from IPv4 to IPv6, it will take up to 15 to 20 years from now.

The greatest value of the success of Super IP development is that we have proven that IPv6's competitive technology completely can be present. Super IP is 100% compatible with existing network protocols. Not only the deployment cost almost negligible compared to IPv6, but also global network upgraded in just one year.

We prove theoretically that as long as $N \times$ IPv4 (positive integer $N > 1$) is used for upgradeIP address. It is possible to break through the limitation of IPv4 address space on the premise of 100% compatibility with IPv4. Therefore, the way to extend IP address space based on 100% compatible IPv4 protocol is not unique. Super IP is the best $N \times$ IPv4 mode protocol found in our research at present.

Even if China does not promote the self-developed super IP protocol in order to protect the IPv6 process, how can we guarantee that no other country will develop similar technologies in the next 15-20 years?In particular, the United States is very non-standard and fair open in its technical system. They especially advocate free competition from different technologies. In the United States, whether it is CPU or operating system, whether it is wireless technology or wired technology, products of various technical standards can be popular. Although IPv6 is a standard under the US-led IETF, no one in the United States can guarantee that alternative technologies other than IPv6 will not develop.

There is no way for us to lose on ISDN and ATM, because we used to be technically behind others. Nowwe are in front of the world on super IP, and we have the most realistic and urgent requirements on the lack of IPv4 address. Countries with rich IP addresses, such as the United States, can completely wait for others to try before switching to the Internet after fully confirming the direction of the technology. Because the per capita IPv4 address in the United States is about 10, ordinary operators, enterprises and other users will not have an urgent need to turn to IPv6. If there is a major change in the direction of technological development, they can easily stop the IPv6 process, but those countries that first turn to IPv6 will suffer the greatest loss. If we replace our network with a large number of IPv6 promoted by the United States, the process of IPv6 will stop all over the world, especially in the US, because of the rapid popularity of

super IP or similar super IP technology. The consequences will be heavier than China's losses on ISDN and ATM.

Moreover, IPv6 has great contradictions in the industrial interest relationship, which is also a very critical issue. If Computer Millennium Bug problem not solved, all machines and equipment may have problems, which will affect the interests of all users who need to upgrade. However, the nature of the problem of insufficient IP addresses is completely different. Even if the addresses are exhausted, they will not directly affect the existing network users. The technology upgrade will not bring them direct benefits. This affects that the basic network operation users can no longer increase, and the latecomers of the network users can no longer access the network, and have no impact on the existing network users. Therefore, users who need to upgrade their devices will not be anxious about the problem of insufficient IPv4 addresses.

Therefore, the upgrade of IP address space is far from the fact that the computer Millennium Bug problem can use the pressure of objective unified time points, as well as the inherent demand of interests, to force huge enterprises and individual users to take unified action. Existing online end-users upgrade to IPv6 purely to make wedding clothes for others. If the technology upgrade does not bring obvious benefits to the adopters of the original technology, they will not have the inherent incentive to do so.

However, the technical design of IPv6 itself not only does not solve these problems, but also makes these problems more difficult:

a. IPv6 requires all nodes of the entire network to support the new IP protocol, and the terminal operating system and application software must all support upgrade.

b. In addition, all IPv6 upgrades of all IP devices involve hardware upgrade, which makes the problem

very difficult. The investment in equipment investment and upgrade is huge, and the upgrade time is long.

c. IPv6 can only function effectively after all the parts of the whole network support the new protocol. This makes the users who upgrade the technology, especially the users who have upgraded in the initial stage, have no internal motivation to do this.

d. A large number of application software cannot to be upgrade to a new protocol at one time, so there will be a long period of coexistence of new and old technologies. Application software supporting new technologies needs to support the original IPv4 technology at the same time, which makes the development of application software very complicated in a long coexistence cycle.

There are also the following factors that hinder the IPv6 process that need carefully considered. First, only China, Japan and South Korea, which are short of IP addresses, are relatively keen on Ipv6, while the IPv4 addresses in developed countries such as the United States are very abundant, and not much pressure to upgrade IP address space in the near future. Second, there is NAT technology that can expand IP address through private network address, so even in China, operators, especially enterprise networks, do not have a strong demand for IPv6. Third, IPv6 has not improved the existing network technology. In the process of transition, the problem of NAT address traversing still exists. This kind of end-to-end communication problem not really solved until the whole network adopts IPv6. In contrast, super IP protocol can solve all existing network NAT problems in short period of time.

If the existing network technology pushed back, it will inevitably lead to a huge cost of network upgrade, which is actually easy to understand. What is more important is that since all the technologies pushed back, there are almost no realistic constraints in their technical design. This makes it easy for designers to take it for granted that they continue to add endless

"ideal functions" to new technologies from a variety of ideal angles and different interests. In the end, the new technology, which has no real technical constraints, becomes the perfect stupid duck, which increases the cost of development and deployment making the new function become flashy decoration.

The IPv6 protocol originally designed to solve the problem of insufficient IPv4 addresses, but now IPv6 seems completely throw away this most fundamental problem. All the thoughts spent on things that are completely irrelevant to the address space, so that people now have Unclear. Due to the complexity of technical design, the address space in the IPv6 technology solution has shrunk to the point where it is

likely to be unable to meet the needs. This may be something that is surprisingly unexpected.

REFERENCE

[1] RFC2373 IP Version 6 Addressing Architecture

[2] Wang Tao. An method of IP address system and create a connection between users for communication , [P]. CN: 200710073741.2, 2007.10

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

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

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

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

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

[8] Information technology-Future Network- Problem statement and requirement-Part