Research of New Network Address Structure

Chong Jiao
[1.]State and Provincial Joint Engineering Lab. of Advanced Network, Monitoring and Control, China
[2.]School of Computer Science and Engineering
Xi'an Technological University
Xi'an, 710021, China
e-mail: 1342748406@qq.com

Xu Yinqiu
[1.]Chinese Decimal Network Working Group
[2.]Shanghai Decimal System Network Information Technology Ltd.
e-mail: 8918616209@126.com,

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

Zhao Hongwen
Shandong Radio, Television and Network Co., LTD.
Tai 'an Branch.
e-mail: tagdglcs@qq.com

***Abstract*—With the wide application of Internet technology, the number of hosts accessing the Internet has grown rapidly, and addresses will be more and more widely used in other intelligent terminals such as e-commerce logistics codes, space codes, identity codes, and 3D geocodes. The number of existing addresses is no longer sufficient for this development demand. The emergence of IPv6 temporarily alleviated the problem of IP address shortage, and IPv6 did not fully consider the security of data transmission at the beginning of design. Chinese researchers have proposed a new Internet address architecture, that is, method of using whole digital code to assign address for computer, referred to as IPV9. IPV9 extends address capacity; supports more address hierarchies, more addressable nodes, and simpler automatic address configuration. Based on the study of IPv4 and IPv6 address structure, this paper designs the standards of the new generation network address structure, including IPV9 unicast address structure, cluster address structure and multicast address structure, which provides a solid foundation for new generation of Internet research.**

Keywords-Addressing; Address Structure; IPV9; Decimal Network

I. INTRODUCTION

At the beginning of the Internet development, IPv4 addresses were sufficient and successful, but in the last 20 years of the 20th century, the global Internet was growing rapidly, and the number of hosts connected to the Internet was growing exponentially every year. Therefore, the number of existing addresses is no longer sufficient for this development demand. IPv6 solves the problem of address shortage in IPv4, but it does not fully consider the network security problem in design. There are many security risks, and IPv6 is not compatible with the original IPv4. In order to adapt to the network development, Chinese researchers proposed a new network address architecture. This structure adopts a method of using whole digital code to assign address for computer and intelligent terminal. It is input to a computer through various input devices of a computer and a smart terminal, and combines software and hardware of various computers. The external addresses of the networked computers and

DOI: 10.21307/ijanmc-2019-032

intelligent terminals are compiled corresponding to the addresses of the internal operations of the computer through various transmission media.

This new address allocation method can provide sufficient address space for the future development of the Internet, and this new one also provides sufficient information for various personal information appliances and e-commerce logistics and personal communication terminal applications. This also ensures that the address hierarchies can have more layers. The IP address length from 32 bits to 128 bits to 2048, to support more address hierarchies, more addressable nodes and simpler automatic address configuration. At the same time, the 32 -bit address length of IPv4 has been reduced to 16 bits to solve the quick use of cellular communication in mobile communication.

II. ADDRESS TEXT REPRESENTATION

The decimal network address is expressed in "brackets in decimal", that is, y[y[y[y[y[y[y[y[y, where each y represents a 32- bit long integer in decimal. Such as: 0000030620[0000000000[0000000000[0000000000[0000000000[0009635485[0000000000[000005953246. In the address representation, multiple consecutive zeros on the left of each decimal number can be omitted, but all zero decimal numbers need to be represented by a zero. For example, the above address can be written as: 30620[0[0[0[0[9635485[0[5953246]. In order to further simplify the representation of address, we can address the entire continuous field zero can be represented by "[X]" (X is the number of stages of the all-zero field). For example, the above address can be abbreviated as 30620 [4] 9635485 [0 [5953246].

The decimal network address prefix uses a CIDR (Classless Inter-Domain Routing) like representation, which has the following form: IPV9 address/address prefix length. The IPV9 address is an address written by the IPV9 address representation, and the address prefix length is the number of consecutive digits from the leftmost part of the address to indicate the address prefix. The decimal number is used in the IPV9 address, but the prefix length refers to the binary. For example: 200-bit address prefix 3659[0[0[0[31548[150[0 can be expressed as: 3659[0[0[0[31548[150[0[0/200 or 1212[3]343[150[2]/200. In the representation of the address prefix, the IPV9 address to the left of the slash "/" must be restored to the correct address.

IPV9 addresses are assigned to interfaces, not nodes. The IPV9 address specifies a 256-bit identifier for the interface and interface group. There are three types of addresses: a single interface with a single unicast address, anycast address, and a multicast address.

III. UNICAST ADDRESS STRUCTURE

The unicast address is the identifier of a single network interface, and the packet with the unicast address as the destination address is sent to the unique network interface identified by it. The address hierarchy of the unicast address is very similar in form to the CIDR address structure of IPv4, and they all have consecutive address prefixes and address codes of arbitrary length. IPV9's unicast address has the following forms: aggregate global unicast address, decimal internet address and domain name decision and assignment organization address, IPX address, local IPV9 unicast address, and IPv4 compatible address.

The aggregatable global unicast address and cluster address belong to the unicast address. They are not different in form, but differ in the propagation mode of the message. Therefore, the aggregatable unicast address and cluster address are assigned the same format prefix 0100. Both the local link unicast address and the in-station unicast address are used in the local range. To facilitate the router to speed up the identification of these two types of addresses, 111111111010 and 111111111011 address format prefix are assigned to them respectively.

A. Aggregate Global Unicast Address

The Internet has a tree topology hierarchy. In order to better express this hierarchy, IPV9 introduces a multi-hierarchical addressable address. Organizations at all levels of the Internet are assigned their own identity (address prefix) in the address, and each organization identity is assigned based on the higher-level agency identity to which it is directly affiliated. Different levels of the Internet routing systems can only distinguish subnet identifiers in the address above its level, that is, low-level network structures are transparent in high-level nodes. In this way, the low-level subnets are aggregated at a high level, sharing a high-level subnet number, which are represented by an item in the high-level router routing table.

The aggregatable global unicast address is the most widely used unicast address when a node is connected to the Internet. This kind of address is used primarily to support network vendor-based address aggregation and network intermediary based address aggregation. The use of aggregatable global unicast addresses can effectively aggregate subnets in all levels of routing systems, thereby reducing the size of the routing table.

1) Introduction of Aggregatable Global Unicast Address

The multi-level network structure has good scalability, which is beneficial to solve the problem of routing addressing. Like the telephone network, IPV9 has a good hierarchical structure for aggregatable global unicast addresses, which can have the following three levels:

a) Public topology layer: The public topology layer is a collection of network providers and network intermediaries that provide public Internet transit services.

b) Site topology layer: The site topology layer is limited to specific sites or organizations that do not provide public Internet transit services to off-site nodes.

c) Network interface identification: The network interface identifier is used to identify the network interface on the link.

2) Structure of Aggregatable Global Unicast Address

The IPV9 aggregatable global unicast address consists of six domains: address format prefix (FP), top-level aggregation identifier (TLA), reserved domain (RES), secondary aggregation identifier (NAA), and site-level aggregation identifier (SLA), and network interface identification. In order to reduce the difficulty of readdressing when changing network access, the lengths of these six domains are fixed, the structure of aggregatable unicast addresses is shown in table 1:

TABLE I. AGGREGATE UNICAST ADDRESS STRUCTURE

4	26	18	48 bits	32 bits	128 bits
FP	TLA logo	RES	NLA identifier	SLA identifier	Network interface identifier
←Public topological layer→				Site topology layer	Network interface identifier

a) Format prefix: The format prefix of the aggregatable global unicast address is defined as a "0100" four-bit binary string. With this address format prefix, the routing system can quickly distinguish whether an address is an aggregatable global unicast address or other type of address.

b) Top level aggregation identifier: The top-level aggregate identifier is the highest level in the routing hierarchy. Default router must be given each

active polymerization top of an identifier correspondence, and provide the top aggregation in the identifier represents the address of the region of the routing information. Currently, the top-level aggregation identifier is 26 bits and can support 67108864 network switcher nodes, remote network providers, or backbone network service provider nodes.

c) Secondary aggregation identifier: The organization using two polymerization identification to establish internal addressing hierarchy and identifier within the site which have top level aggregation identifier. The organization with top-level aggregation identifier has 48-bits secondary aggregation identifier space, that is, if the organization directly allocates these secondary aggregation identifiers, it can allocate 248. The 48- bit long secondary aggregation identifier divides the first-level NLA1 of n bits, and the remaining (48-n) bits serve as site IDs.

The allocation scheme of the secondary aggregation identifier is a compromise between route aggregation efficiency and flexibility. When an organization allocates its internal secondary aggregation identifier, it can select an allocation scheme according to its own needs. Establishing a hierarchy allows the network to aggregate to a greater degree at all levels of the router, and to make the routing table smaller. Directly assigning a secondary aggregated identifier simplifies the allocation process, but results in excessive routing table size.

d) Site-level aggregation identifier: Site-level aggregation identifier is used for individual organizations (sites) to establish their internal addressing hierarchy and identity subnets. The site-level aggregate identifier is similar to the IPv4 subnet number, except that the IPV9 site can accommodate a larger number of subnets. The 32-bit site-level aggregation identifier domain can support 4,294,967,296 subnets, which is sufficient to support the subnet size within most organizations.

An organization can directly assign its site-level aggregation identifiers. There is no logical relationship between the site-level aggregation identifiers, and the routing table size of the router is large. It is also possible to divide two or more layers of structures within a site-level aggregation identifier domain.

e) Network interface identifier: The network interface identifier is used to identify the network interface on a link. On the same link, each network interface identifier must be unique. The aggregatable global unicast address ultimately identifies a network interface (or node) at the network interface level. In many cases, the network interface identifier is the same as the link layer address of the network interface, or based on the link layer address of the network interface. The same network interface identifier can be used on multiple interfaces of the same node, which are only treated as one network interface on the network.

B. Local Link Unicast Address

The local link unicast address is used for communication between nodes on the same link. This type of address has a separate address format prefix "1111 1111 1010" for efficient addressing on this link. This type of address is used for automatic configuration of addresses, neighbor detection, and there are no routers on the link. If there are routers on the link, these routers do not forward IPV9 packets to other links which have the local link unicast address as the destination address the source address.

The structure of the local link unicast address is very simple. It consists directly of the address format prefix and the 128- bit network interface identifier, and is filled with 54 bits of 0, as shown in the table 2.

TABLE II. LOCAL LINK UNICAST ADDRESS STRUCTURE

12 bits	116 bits	128 bits
1111 1111 1010	0	Network interface identifier

An in-site unicast address can be used when it is desired to address the network interface of the communication within the site and does not wish to use the global address format prefix. At the same time, the station's unicast address is also used for the addressing of isolated sites that are independent of the Internet, such as addressing in a campus network that is not connected to the Internet.

Because the scope of the unicast address in the station is much larger than the range of the local link unicast address, and a site often contains multiple subnets, the structure of the unicast address in the station is more than that of the local link. The format prefix assigned to the unicast address in the station is "1111 1111 1011". The specific structure of the address is shown in the table 3.

TABLE III. STRUCTURE OF THE UNICAST ADDRESS IN THE STATION

12 bits	84 bits	32 bits	128 bits
1111 1111 1011	0	Subnet identifier	Network interface representation

Similar to the use of the local link unicast address, IPV9 packets with the source address or destination address in the station can only be propagated within the site. The router cannot forward these packets out of the site.

C. Compatible Address

In IPV9, some mechanisms for smoothing the transition from IPv4 /IPv6 to IPV9 have been developed, including the use of existing IPv4 and IPv6 routing systems as tunnel forwarding IPV9 packet technologies. For IPV9 nodes using this technology, it is required to assign several special IPV9 addresses of "IPv4 compatible address", "IPv6 compatible address" and "special compatible address". The specific structure of these addresses is shown in the table 4-7:

TABLE IV. COMPATIBLE ADDRESS FORMAT

10 bits	19 bits	3 bits	64 bits	32 bits	96 bits	32 bits
Prefix	Reserved	Sign	0	Scope	DedicatedIPv6	IPv4address

TABLE V. IPV4 MAPPED ADDRESS FORMAT

96 bits	32 bits	96 bits	32 bits
0[0[0	0	0	IPv4address

TABLE VI. MAPPED ADDRESS FORMAT

96 bits	32 bits	128 bits
1[0[0	0	IPv6 address

TABLE VII. MAPPING ADDRESS FORMAT FOR SPECIAL COMPATIBLE ADDRESSES

96 bits	32 bits	96 bits	32 bits
2[0[0	0	0	IPv4address

IV. CLUSTER ADDRESS STRUCTURE

In many cases, there may be multiple servers on the network that provide the same service at the same time (for example, a mirror server). A host, an application or a user often only wants to get a service without paying attention to which server the service is provided, that is, only one of all these servers is required to serve the user. Anycast transmission mechanism is proposed to meet such needs on the network. The mechanism uses the cluster address to identify the set of servers that provide the same service. When a user sends a message to the cluster address, the network sends the message to at least one server that owns the cluster address.

A cluster address is a type of IPV9 address that is simultaneously assigned to multiple network interfaces. The IPV9 message destined for the destination address of the cluster address will be sent to the interface that owns the cluster address. The routing protocol considers the nearest one, that is, only one interface can receive the packet. The cluster address of IPV9 is allocated from the unicast address and is defined in the same format as the unicast address, that is, the cluster address is formally indistinguishable from the unicast address. When a unicast address is assigned to multiple network interfaces, it is functionally translated into a cluster address. The node that gets the cluster address must perform the appropriate configuration process to recognize that the address is a cluster address.

For each assigned cluster address, it always has a longest prefix P to identify the minimum containment level of all network interfaces that have the cluster address in the network topology. For example, each school in a school has an image of an FTP server, and the minimum inclusion of all of these servers may be the highest level in the school's network structure. The corresponding prefix P is used to identify the highest network level. Within the network hierarchy identified by the prefix P of a cluster address, each member that owns the address must be published as a separate item in the routing system (often referred to as host routing); outside the hierarchy identified by the prefix P All member network interfaces identified by the cluster address can be aggregated into one item to be published in the routing system.

It is worth noting that in the worst case, the prefix P of a cluster address may be 0 in length, that is, the distribution of the network interface that owns the cluster address in the Internet cannot form a topology, so all of these networks are included. The smallest hierarchy of interfaces is the entire Internet. In this case, each node corresponding to the cluster address must be published on the Internet as a separate item. This severely limits the number of such global cluster address sets that the routing system can support. Therefore, the Internet may not support a global set of cluster addresses, or only provide extremely restrictive support.

At present, the use and implementation mechanism of IPV9 for cluster addresses are still being researched and tried. There are three types of cluster addresses that have been identified so far:

- Identify a collection of routers in an organization that provides Internet services. At this time, the cluster address can be used as the intermediate router address in the extension header of the packet source path, so that the packet is converted by any router of the designated network service access organization.

- Identify the set of routers that connect to a particular subnet.
- Identify a set of routers that provide routing information to a certain network area.

Because the experience of using cluster addresses in a wide range is rare, and there are some known problems and dangers in the use of cluster addresses, before accumulating a lot of experience with cluster addresses and finding solutions to cluster address ills, The following restrictions must be adhered to when implementing an IPV9 cluster address:

- The cluster address cannot be used as the source address in the IPV9 message;
- The cluster address can only be assigned to the router at present, but not to the normal IPV9 host node.

Currently, the IPV9 protocol only predefines a cluster address – the subnet router cluster address. This kind of address must be owned and must be identifiable by each subnet router. The specific format is shown in the table 8:

TABLE VIII. SUBNET ROUTER CLUSTER ADDRESS

n bits	256-n bit
Subnet prefix	Host number (all 0)

The entire subnet router cluster address, as its name implies, is the cluster ID of all routers connected to the link subnet. Its purpose is to allow applications on one node to communicate with one of all router collections on the remote subnet.

V. MULTICAST STRUCTURES

Multicast is used when implementing the network multicast mechanism. The IPV9 protocol also adopts a multicast mechanism and specifically designed a multi-purpose address for multicast use. The address space prefixed with the 1111 1111 11 address format in the address space of IPV9 is reserved for multicast. The multicast address is assigned to multiple network interfaces in the same way as the cluster address. The difference between the two is that IPV9 packets with the destination address of the multicast address will be received by all network interfaces that have the multicast address at the same time. This sending process is called multicast. A collection of network interfaces that have the same multi-cast address is called a multicast group.

The multicast address of IPV9 consists of four parts, with "1111 1111 11" as the address format prefix. The specific structure is shown in the table 9.

TABLE IX. IPV9 MULTICAST ADDRESS FORMAT

10 bits	8 bits	4 bits	234 bits
1111 1111 11	Sign	Range of action	Group identification

The remaining three parts of the format followed by the address format prefix are the flag bit field, the address scope field, and the group identification field. The flag bit field consists of 8 bits, the flag bit field uses only the lowest bit of the 8 bits (T bit), and the remaining upper seven bits are reserved. The T bit is called the "temporary address bit" and it indicates that the assigned multicast address is temporarily valid or permanent. The address range is an integer consisting of 4 bits. It is used to limit the distribution range of multicast group members, thus limiting the effective range of the multicast address relative to the sender of

the message during multicast. Group identification field for a multicast group, it is in the low 234 among the entire address format. A multicast group identified by a group identity field may be a temporary or permanent multicast group within a given range.

A. Universal multicast address

In the design of IPV9, some common multicast addresses are predefined, such as reserved multicast address, all-node multicast address, all router multicast address, and the requested node multicast address. These addresses are typically used when neighboring nodes are probed and the address is automatically configured.

1) Reserved multicast address: multicast address with group identifier of 0 can only be reserved but cannot be assigned to any multicast group, that is, the flag bit is 0, the address range is arbitrary, and the group ID is all 0. The addresses at the time are all reserved multicast address addresses.

2) All node multicast address addresses: general multicast addresses 4230774016 [7]1 and 4230775040[7]1 are all node multicast addresses, which identify all nodes within the scope of the node and within the scope of the link. These two addresses function similarly to the broadcast address in IPv4 and are used to send broadcast messages within their corresponding scope.

3) All routers multicast address: It contains the following three general multicast address addresses, which identify all routers in range 1 (scop=1, on the same node), in range 2 (scop=2, on the same link). All routers and all routers in range 5 (scop=5, same site):

4290774016[7]2
4290775040[7]2
4290778112[7]2

4) The requested node multicast address: the requested node multicast address ranges from 4290775040[4]1[4294901760[0 to 4290775040[4]1[4294967295[42949 67295. The requesting node is a node for detection probe target node is the neighbor (there may be multiple simultaneous). In the process of neighbor discovery, the requested node multicast address is used as the address identifier of the requested target node, and its scope is on the local link.

B. Distribution of multicast addresses

The assignment process of the multicast address is the assignment of the multicast address group identification. In the format structure of the multicast address, the group representation is allocated 234 bits of space. In theory, these 234 bits can allocate 2 234 different group identifiers. However, because the current multicast Ethernet embodiment only the lower 64 bits of the IPV9 multicast address mapped to the MAC address of IEEE802, and the processing of the token ring network multicast address will also be different, in order to ensure IPV9 can be generated on the basis of the multicast address of the MAC address is unique, is currently only available in the 234 bit group identification assigned to the lower 64 bits of the group identifier, the remaining 170 bits are reserved (set to all zeros), The multicast address format is shown in table 10.

TABLE X. MULTICAST ADDRESS FORMAT WITH 64- BIT GROUP IDENTIFICATION

10 bits	8 bits	4 bits	170 bits	64 bits
1111 1111 11	Sign	Range of action	0	Group identification

The above scheme limits the permanent group identification of the IPV9 multicast address to 264, which has been able to meet the currently foreseeable needs. If the need for group identification exceeds this

limit in the future, multicast will still work but the processing speed will be slightly reduced; with the development of network equipment in the future, the 234-bit group identification space can be fully utilized.

VI. SUMMARY

IPV9 has a huge address capacity, can be compatible with IPv4 and IPv6, and USES a special encryption mechanism to make the network environment more secure. The application of IPV9 is being promoted in China, especially in the government, banking and other departments. This paper summarizes the current IPV9 address structure, including IPV9 unicast address structure, cluster address structure and multicast address structure, etc., and introduces the compatible address format of IPv4, IPv6 to IPV9 transition, and the aggregatable global unicast address. The aggregation logo provides a corresponding basis for future application development based on IPV9.

REFERENCE

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

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

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

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

[5] Xie Xiren. The concise tutorial on computer network [M]. Publishing House of Electronics Industry, 2011.

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