Summary of Stateless Address Auto-Configuration for Ipv6

Zi-Wen Wang, Geng-Yu Wei
School of Computer Science, Beijing University of Posts and Telecommunications, Beijing, China
E-mail: 471666331@qq.com, weigengyu@bupt.com

***Abstract*-IPv6 stateless address auto-configuration is a brand new method to generate IPv6 address. Similar to IPv4, IPv6 has also defined stateful address auto-configuration rules based on DHCPv6, while SLAAC can either work without DHCPv6 or rely on some functions of it. This research has summarized and analyzed four SLAAC IID generation methods, namely EUI-64 encoding method, random generation method, encrypted generation method, and steady generation method.**

Keywords-IPv6 address; stateful address auto-configuration; stateless address auto-configuration

I. INTRODUCTION

In the IPv4 technology, distribution modes of address are manual configuration and dynamic host automatic assignment(DHCP) [1,2]. However. the 128-bit IPv6 address is too relatively long to use manual configuration, therefore, a host get a IPv6 address by auto-configuration. Address automatically assigned in IPv6 is different in IPv4, it is divided into stateless address auto configuration (SLAAC) and dynamic host configuration protocol for IPv6(DHCPv6). Because the DHCPv6 is similar to DHCP in IPv4, all of the addresses are managed centrally by DHCP server, this paper will not repeat it. Since DHCPv6 is similar to DHCPv4, addresses are managed centrally by the DHCP Server, this will not repeat, this article will mainly introduce a new set of fully distributed IPv6 stateless address auto-configuration, and address assignment technology compared with other technology of IPv6 is very important and basic.

State address automatically assigned to the IPv6 address is divided into two parts, the first 64 are network prefix, after the 64 is the interface Id. Network prefix is always provided by the router, so SLAAC is to determine how the interface Id is generated. At present, there are 4 ways to generate the interface: EUI-64 mode, random mode, encryption mode and stable mode. In this paper, it will analyze and introduce the interface Id generation from the above 4 modes and their security and application scenarios.

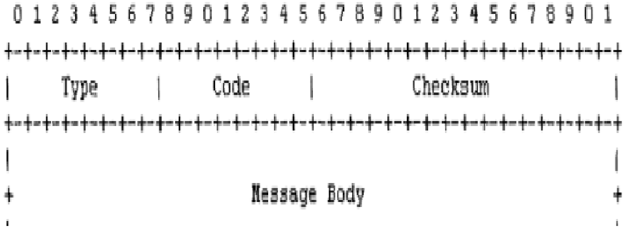
The first chapter of this paper mainly introduces the specific process of SLAAC, as well as the difference and connection between SLAAC and DHCPv6. In the second chapter, the paper mainly introduces the 4 interface Id generation methods in SLAAC. The third chapter makes a comparative analysis of their security and application scenarios. The fourth chapter is the conclusion.

II. IPV6 ADDRESS CONFIGURATION

A. *Neighbor Discovery Protocol*

For the length of the 128 bit IPv6 address, the use of manual distribution of the type of address error prone, so IETF does not recommend to manually assign an IPv6 address assigned to the host. It can be seen, SLAAC and DHCPv6 will be the main way to get IPv6 address in the future. But how to choose SLAAC or DHCPv6 and host how to validate the uniqueness of the IPv6 address? In order to solve the above problems, this first has to introduce the neighbor discovery protocol[10] (NDP), NDP is the basis of SLAAC and DHCPv6.

Noted in RFC 4862, Neighbor Discovery Protocol combines the IPv4's address Resolution Protocol(ARP), ICMP routing protocols, and ICMP redirection protocol, and IPv6 also provides prefix discovery, neighbor unreachable detection, duplicate address detection (DAD) and address auto-configuration functions. NDP message body shown in figure 1.



```
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|     Type      |     Code      |          Checksum             |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                         Message Body                          +
'                                                               '
```

Figure 1. NDP message body.

In the NDP defines five packets. 1. Router advertisement(RA) message. 2. Router solicitation(RS) message. 3. Neighbor Advertisement(NA) message. 4. Neighbor Solicitation(NS) message. 5. Redirect message. Which contains a marker M (managed address configuration flag) and O flags (other configuration flag) in the RA message.When the M is 1, the address can be obtained by DHCPv6, and the O tag can be ignored. M is 0 when the address can be obtained by SLAAC. When O is 1, the other configuration information can be obtained by DHCPv6. Through these five kinds of messages, NDP allows the host to get a unique IPv6 address.

B. *Slaac*

When the network only exists in the router, but no DHCP Server, hosts on the network can only be obtained IPv6 address by SLAAC. Since the router unlike the DHCP Server to manage each address allocated out of the state and the interface Id IPv6 addresses by the host itself, by SLAAC assigned address can reduce the router's resource consumption, but also because of this, the resulting IPv6 host no such domain name[11] (DNS) and other configuration information.

The process of SLAAC is as follows. The first step: using the host interface to generate the link local address. The second step: duplicate address detection for the link local address. The third step: to send the RS message, the request of the local router RA message. The fourth step: access to the router's RA message, and view the RA message in the M and O flags, when the M is 0 and use the stateless address auto configuration. Host according to the specific interface of the Id generation mode to generate the 64-bit interface Id, and plus the 64 network prefix in RA, then the 128-bit IPv6 address is generated. The fifth step: duplicate address detection for the newly generated address. Its process as shown in figure 2.

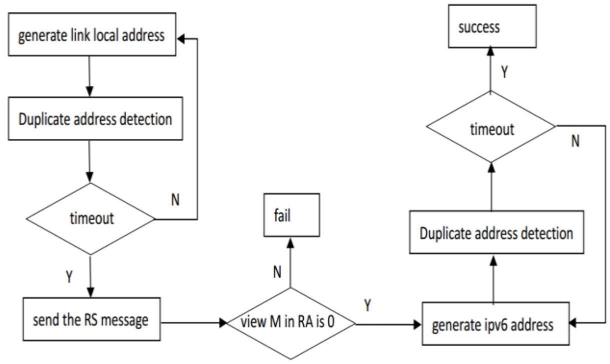


Figure 2. Address allocation process with SLAAC.

C. Relationship Between SLAAC And Dhcpv6

In IPv6 network and there are only routers in it, each host can only get the address by SLAAC, but the host get the IPv6 address without such as DNS and other configuration. However, with the help of DHCPv6 Server in the network, it can provide hosts addresses by SLAAC or DHCPv6. SLAAC and DHCPv6 can be used simultaneously, host use SLAAC to obtain IPv6 address and through DHCPv6 to obtain configuration information such as DNS, depending RA packets of M and O flags.

If the host's IPv6 address is assigned by DHCPv6, the whole IPv6 addresses are assigned by the DHCP Server address pool. If the host's IPv6 address is assigned by the SLAAC, its network prefix is given by the router, and the interface Id is generated by SLAAC using specific Id generation method, then by the two parts to form IPv6 address. Because the interface Id generation mode is different, so the security of the address generated by SLAAC is also different. At present, the main interface Id generation methods are: EUI-64 mode, random mode, encryption mode and stable mode. The next chapter describes in detail the 4 types of interface Id generation and their security and application of the scene to make a corresponding comparative analysis.

III. INTERFACE ID GENERATION MODE

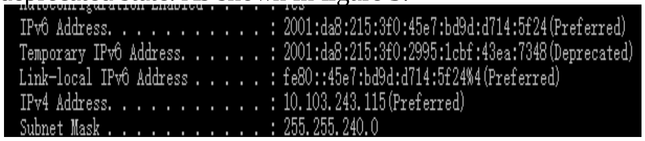
A. EUI-64 Mode

EUI-64 is a method based on MAC[12] address to generate the interface ID. Using the MAC address of the first byte seventh bit 0/1 to indicate that the IPv6 address is local / global management, with first byte of eighth bit 0/1 to represent the address is unicast / multicast address. IETF use 16-bit 0xfffe insert between the organizationally unique identifier and the extension identifier for the interface Id.

This EUI-64 encoding method to generate the interface Id is simple, it does not need to consume a large number of computing resources for a node. But this approach will be exposed to their MAC address in the IPv6 address.

B. Random Mode

RFC 4941 think that EUI-64 mode is lack of security, and it is proposed to use temporary addresses[13] to improve security. The 64-bit interface Id of a temporary address generated by random values and it has a certain lifetime, when the temporary address becomes deprecated, a new one must be generated. Standard recommends temporary address's preferred lifetime and valid lifetime for one day and one week. At present, the windows system use this mode generate interface Id. Use the ipconfig command to view more than a temporary IPv6 addresses, these temporary IPv6 addresses only one is in the preferred state, the rest are deprecated state. As shown in figure 3.



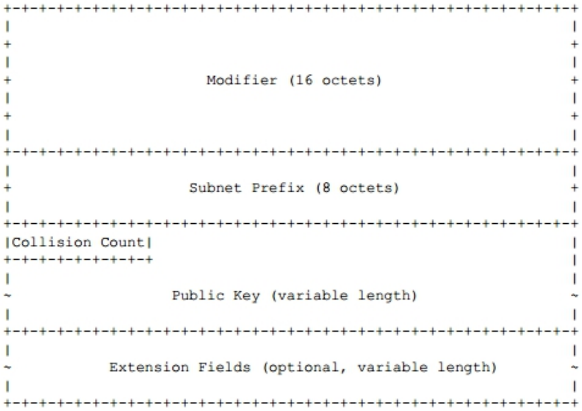
```
   Autoconfiguration Enabled . . . . : Yes
   IPv6 Address. . . . . . . . . . . : 2001:da8:215:3f0:45e7:bd9d:d714:5f24(Preferred)
   Temporary IPv6 Address. . . . . . : 2001:da8:215:3f0:2995:1cbf:43ea:7348(Deprecated)
   Link-local IPv6 Address . . . . . : fe80::45e7:bd9d:d714:5f24%4(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.103.243.115(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
```

Figure 3. Address allocation process with SLAAC.

From the picture above we can see that the host generates a global IPv6 address and a local link IPv6 address. The interface ids of above two IPv6 addresses are also randomly generated, and there are no relationship with MAC address, and they are fixed. One of the global IPv6 address is typically used as a Server-side address for other hosts to communicate with it. There may be more than one temporary IPv6 addresses, of which only one is in the preferred state, the rest are deprecated state. This is due to the temporary IPv6 address in deprecated state maintained previously connection, and did not enter invalid state, so often in this case there will be more than one temporary IPv6 address in deprecated state. The only temporary IPv6 address that is in the preferred state is to be selected by the host to create a new connection, and to communicate with the other hosts. But for a host of the existence of a number of temporary address of the situation, the other host how to know different temporary IPv6 address is corresponding to the same host? RFC 4941 did not give a clear solution, so in order to solve this problem, it is bound to spend a greater price to solve it. But this temporary address can greatly improve the security of the address.

C. Encryption Mode

Also for the address security considerations, in RFC 3972, it is proposed to cryptographically generate address(CGA). Each has address its CGA parameters data structure of the following format in figure 4.



```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                      Modifier (16 octets)                     +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                    Subnet Prefix (8 octets)                   +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Collision Count|                                               |
+-+-+-+-+-+-+-+-+                                               |
|                                                               |
~                  Public Key (variable length)                 ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
~           Extension Fields (optional, variable length)        ~
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Figure 4. CGA parameter format.

Among them, Modifier is 128-bit data which randomly generated, Subnet Prefix is the network subnet prefix, Collision Count is the number of duplicate address detection, only for 0,1,2. Public Key is based on RFC 3280[14] defined public key, Extension Fields is an extension option. Its IPv6 address generation process:

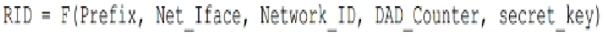
- Set the modifier to a random or pseudo-random 128-bit value.
- Concatenate from left to right the modifier, 9 zero octets, the encoded public key, and any optional extension fields. Execute the SHA-1 algorithm on the concatenation. Take the 112 leftmost bits of the SHA-1 hash value. The result is Hash2.
- Compare the 16*Sec leftmost bits of Hash2 with zero. If they are all zero (or if Sec=0), continue with step 4. Otherwise, increment the modifier by one and go back to step 2.
- Set the 8-bit collision count to zero.
- Concatenate from left to right the final modifier value, the subnet prefix, the collision count, the encoded public key, and any optional extension fields. Execute the SHA-1 algorithm on the concatenation. Take the 64 leftmost bits of the SHA-1 hash value. The result is Hash1.
- Form an interface identifier from Hash1 by writing the value of Sec into the three leftmost bits and by setting bits 6 and 7 to zero.
- Concatenate the 64-bit subnet prefix and the 64-bit interface identifier to form a 128-bit IPv6 address with the subnet prefix to the left and interface identifier to the right, as in a standard IPv6 address.
- Perform duplicate address detection if required, as per. If an address collision is detected, increment the collision count by one and go back to step 5. However, after three collisions, stop and report the error.
- Form the CGA Parameters date structure by concatenating from left to right the final modifier value, the subnet prefix, the final collision count value, the encoded public key, and any optional extension fields.

As can be seen from the above, get the interface Id by means of encryption, the host needs certain computational overhead and storage overhead, but this overhead for limited networking nodes may be a burden. But it does improve the security of the address with a certain overhead.

Due to the different subnet, the IPv6 address will change accordingly, and the modifier is randomly generated, even in the same subnet will generate different IPv6 address, which is the same as the temporary IPv6, so this kind of IPv6 address is also called "unstable" address. The meaning of "stability" of IPv6 addresses in IPv6 address, although that is different subnets formed different, but once in the same subnet, IPv6 address with an interface formed is fixed. Following a stable manner generated interface Id is fixed.

D. Stable Mode

Although the temporary address in RFC 4941 can improve the safety of the address, but if you use the method of RFC 4941 to form IPv6 address, there will be a stable IPv6 address in a computer (as in Figure 5 to see the IPv6 address). For this consideration, RFC 7217 presents an algorithm to generate stable IPv6 addresses which are fixed to the interface RId (Random Id) generated by this algorithm. The formula of the algorithm is shown in figure 5.



```
RID = F(Prefix, Net_Iface, Network_ID, DAD_Counter, secret_key)
```

Figure 5. Stable Id algorithm formula.

RFC 7217 does not require the use of any specific pseudorandom function for the function F() above, and the best choice for F() might be different for different types of devices. SHA-1 and SHA-256 are two possible options for F(). For this particular F(), once the given parameter is fixed, the results of its generation is also stable Prefix is representative of the network prefix. Net_Iface is used to represent IPv6 address is generated which is part of a network interface. Network_ID is used to show that witch interface belongs to witch sub network. This means that a host would employ a different interface Id as it moves from one network to another even for IPv6 link-local addresses. DAD_Counter is used to count the number of DAD. For each {Prefix, Net_Iface, Network_ID} triples, there will be a DAD_Counter. Secret_key should be of at least 128 bits and it must be initialized to a pseudo-random number when the operating system is installed or when the IPv6 protocol stack is "bootstrapped" for the first time. Therefore, according to the parameters given can be found when entering different subnets will form a different IPv6 address, but whenever you enter the same subnet, the IPv6 address is stable.

But the author thinks that in this way the address generation interface Id is not as written in the formula is RId, if it is RId, and it should be like a temporary IPv6 address as often changed randomly, rather than fixed. So for the definition of the RId there is a certain problem.

IV. COMPARISON OF FOUR KINDS OF MODES TO GENERATE INTERFACE ID

A. Security Comparison

In summary, because EUI-64 mode will be exposed to the host's MAC address in IPv6 address, such an approach will make criminals through IPv6 address to track a particular host and attack it, so this security has been very low. In the future, focusing on privacy and security of the network environment, it is not suitable for this kind of interface Id generation. For the interface Id generated in a stable manner, although the security are greatly improved, but once criminals cracked F(), he can track any host which is built by the same manufacturers, because each vendor implemented F() method is relatively fixed. For encryption and random manner, the security is relatively the highest, and the interface Id will change over time, so the IPv6 address generated by the tracking of these two methods is very difficult.

B. *Application Scenario Comparison*

In the future, the network can be divided into restricted network[15] (Internet of things) and non-restricted network (Internet). In the restricted network, low bandwidth network, low processing power and low storage capacity of nodes often can't send such large amounts of data. The mode of interface Id generation should be simple and node can't manage a lot of IPv6 addresses. Therefore, EUI-64 mode is more suited to the restricted network (the premise is not to consider security). For random mode, the algorithm to generate random interface Id is not complicated, but it is bound to manage multiple IPv6 addresses for a node who use random mode (at least three IPv6 addresses: a globally unique IPv6 address, a link-local IPv6 address and a temporary address in preferred state). So on the restricted network, irrespective of node storage capacity, it is applied in this way, but once the node storage capacity is limited, this approach also does not apply in the restricted network. For encryption, because a relatively complicated algorithm, is not recommended for use in the restricted network. IPv6 address obtained by encryption is not fixed, and hosts often change the address for the node in the network is not a small overhead. For a stable manner, nodes do not need to store multiple IPv6 addresses, if F() algorithm is less complex, the authors believe that is most appropriate than other modes, and subject to nodes in the restricted network which does not often change the subnet, so the address is relatively fixed. For non-restricted networks in addition to EUI-64 mode, the other three methods are applicable to non-restricted network environment.

V. CONCLUSION

Address assignment either in IPv4 or in IPv6 technology is based on the relative technology, hosts in the network only get the correct address to interoperability, so the research of address allocation method in IPv6 is very important and needs more people to care. How to allocate address in IPv4 is relatively mature, and how to allocate address in IPv6, and which mode of interface Id generation is best, all of there are still in the discussion and research. And if the interface Id is generated by random mode, it would generate many temporary IPv6 addresses, but how to inform other nodes, the number of IPv6 nodes is corresponding to the same node, which is the problem we need to solve. As IPv6 provides a new set of fully distributed stateless address auto-configuration technology, there are many aspects that we need to research and study, this article describes SLAAC and four interfaces Id generation modes, and under the conditions of security and application scenarios are compared. This author hope that this paper will be helpful for other people.

REFERENCES

[1] Wang da, Depth understanding of computer networks, Machinery Industry Press, Bei Jing, 2013, pp.599-611.

[2] R.Droms, Dynamic host configuration protocol, RFC 2131, IETF, 1997.

[3] R.Droms, Internet protocal, version 6(ipv6) specification, RFC 2460, IETF, 1998.

[4] S.Thomson, T.Narten, T.Jinmei, Ipv6 stateless address autoconfiguration, RFC 4862, 2007.

[5] R.Droms, J.Bound, B.Bvlz, Dynamic host configuration protocol for ipv6, RFC 3315, IETF, 2003.

[6] Jeremy Stretch. Eui-64 in ipv6, 2008, http://packetlife.net/blog/2008/aug/4/eui-64-ipv6.

[7] T.Narten, R.Draves, S.Krishnan, Privacy extensions for stateless address autoconfiguration in ipv6, RFC 4941, IETF, 2007.

[8] T.Aura, Cryptographically generated address(cga), RFC 3972, IETF, 2005.

[9] F.Gont, A method for generating semantically opaque interface identifiers with ipv6 stateless address autoconfiguration(slaac), RFC 7217, IETF, 2014.

[10] T.Narten, E.Nordmark, W.Simpson, Neighbor discovery for ip version6, RFC 4861, IETF, 2007.

[11] Wang Yao, Hu Minzeng, Li Bin, Survey on domain name system security, Journal on Communications, 2007, 28(9) 92-101.

[12] [12] Zhou Zongping, Fan Chen, Study of ip address and mac address binding method, Journal of Shandong University of Science and Technology, 2002, 21(4) 51-54.

[13] T.Narten, R.Draves, Privacy extensions for stateless address autoconfiguration in ipv6,RFC 3041, IETF, 2001.

[14] R.Housley, W.Polk, W.Ford. Internet X.509 public key infrastructure certificate and certificate revocation list(crl) profile, RFC 3280, IETF, 2008.

[15] Song Yan, Fu Qian. Network proxy research and implementation for internet of things applications based on constrained application protocal. Journal of Computer Applications, 2013, 33(11) 3010-3015.