ICS 35.030
CCS L 80

# 中华人民共和国国家标准

GB/T XXXXX—XXXX

# IPv6 地址分配和编码规则 接口标识符

IPv6 address assignment and coding rules Interface identifier

(点击此处添加与国际标准一致性程度的标识)

（征求意见稿）

（本草案完成时间：2023 年 5 月 19 日）

**在提交反馈意见时，请将您知道的相关专利连同支持性文件一并附上。**

XXXX-XX-XX 发布 XXXX-XX-XX 实施

国家市场监督管理总局
国家标准化管理委员会 发布

# 目　　次

前言 ..... III
1 范围 ..... 1
2 规范性引用文件 ..... 1
3 术语和定义 ..... 1
4 缩略语 ..... 2
5 接口标识符编码方法 ..... 2
5.1 EUI-64 编码方法 ..... 2
5.2 加密变换编码方法 ..... 3
6 实施要求 ..... 3
参考文献 ..... 4

# 前　言

本文件按照GB/T 1.1—2020《标准化工作导则　第1部分：标准化文件的结构和起草规则》的规定起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别专利的责任。

本文件由全国信息安全标准化技术委员会（SAC/TC260）提出，全国信息安全标准化技术委员会（SAC/TC260）和全国通信标准化技术委员会（SAC/TC485）归口。

本文件起草单位：国家计算机网络应急技术处理协调中心、中国电子技术标准化研究院、中国信息通信研究院、中国互联网络信息中心、清华大学、四川大学、中国移动通信集团有限公司、中国联合通信集团有限公司、中国电信集团有限公司、华为技术有限公司、中兴通讯股份有限公司、中国信息通信科技集团有限公司、华东师范大学、北京百度网讯科技有限公司、维沃移动通信有限公司等。

本文件主要起草人：

# IPv6 地址分配和编码规则　接口标识符

## 1　范围

本文件规定了IPv6地址接口标识符的编码方法和实施要求。

本文件适用于通过IPv6网络动态分配IPv6地址接口标识符的相关实体以及实现IPv6地址分配的相关实体，包括互联网接入服务商、应用基础设施服务商、自用网络运营者、联网终端厂商、网络设备厂商等。

## 2　规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中，注日期的引用文件，仅该日期对应的版本适用于本文件；不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB/T 25069—2022　信息安全技术　术语

GB/T AAAAA—202X　IPv6地址规划和编码规则　总体要求

## 3　术语和定义

GB/T 25069—2022和GB/T AAAAA—202X界定的以及下列术语和定义适用于本文件。

3.1

**接口标识符　interface identifier；IID**

IPv6地址的低64位，用于标识网络内特定接口。

3.2

**互联网接入服务商　Internet access service provider**

专门从事互联网接入服务的提供商，为终端用户提供接入互联网的服务及有限的信息服务，公益性网络也包含在内。互联网接入服务商的基本条件是拥有全国性或区域性用户接入网络，能够向用户提供专线、拨号上网或其他接入服务，根据服务范围分为全国性互联网接入服务商和区域性互联网接入服务商。

[来源：GB/T AAAAA—202X]

3.3

**应用基础设施服务商　Application infrastructure provider**

全国性和区域性互联网数据中心服务商、云计算服务商、内容分发网络服务商、域名注册和解析服务商。

[来源：GB/T AAAAA—202X]

3.4

**自用网络　self-operating network**

除互联网接入服务商和应用基础设施服务商之外，从境内地址分配机构获得地址或从亚太互联网信息中心等具有IP地址管理权的国际机构获得地址的网络。

[来源：GB/T AAAAA—202X]

3.5

**IPv6动态主机配置协议 Dynamic Host Configuration Protocol for IPv6; DHCPv6**

一种动态配置协议，用于配置IPv6节点的网络配置参数、IPv6地址以及IPv6地址前缀的可扩展机制，分为无状态（Stateless DHCPv6）和有状态(Stateful DHCPv6)两种模式。

[来源：IETF RFC 8415]

3.6

**无状态地址自动配置 Stateless Address Autoconfiguration; SLAAC**

一种动态配置协议，由节点通过监听路由通告获得全局地址前缀，与节点生成的接口标识符结合得到全局IPv6地址。

3.7

**盐值 salt**

随机字符串，附加在消息后或消息前进行杂凑运算，用以产生不同的杂凑值。

## 4 缩略语

下列缩略语适用于本文件。

EUI-64：64位扩展唯一标识符(64-bit Extended Unique Identifier)

MAC：媒体访问控制（Media Access Control）

RA：路由器通告（Router Advertisement）

## 5 接口标识符编码方法

### 5.1 EUI-64编码方法

该编码方法参考IETF RFC 4291，适用于通过DHCPv6向联网终端分配IPv6地址时的接口标识符编码，也适用于通过SLAAC由联网终端生成的接口标识符编码。编码方法如下（见图1）：

a) 在MAC地址的制造商标识符和网络适配器标识符之间插入“0xff”和“0xfe”作为中间16位；

b) 对a）形成的64位比特串的第7位进行取反操作，生成的64位比特串即为接口标识符。

注1：MAC地址共48位，前24位为制造商标识符,后24位为网络适配器标识符。

注2：生成的接口标识符第7位标识该接口标识符是全局唯一或本地唯一。0表示该接口标识符本地唯一，1表示该接口标识符全局唯一。

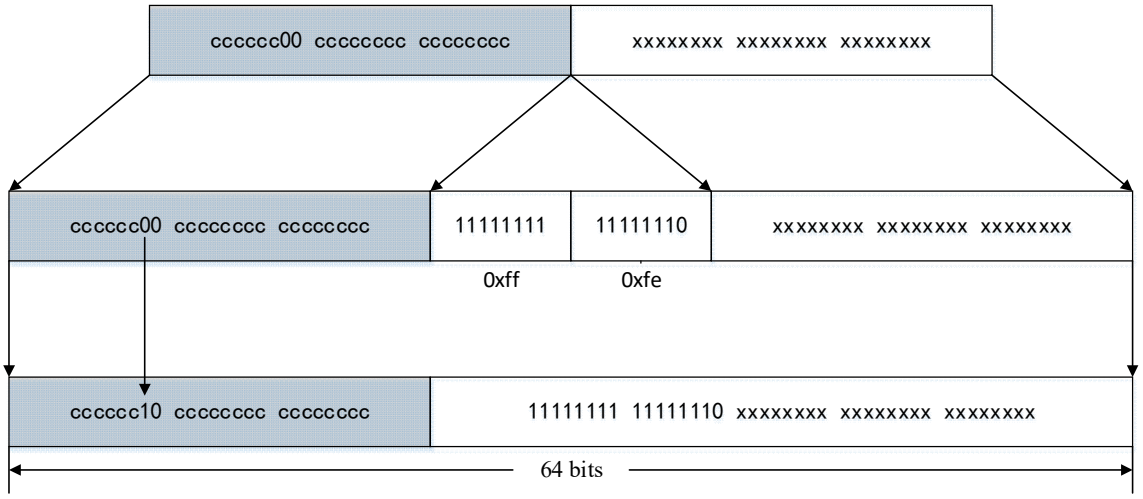


图 1　EUI-64 接口标识符编码方法

## 5.2　加密变换编码方法

该编码方法仅适用于通过DHCPv6向联网终端分配IPv6地址时的接口标识符编码。通过对联网终端标识进行加密变换处理后形成接口标识符，计算方法为：

*IID=E(联网终端标识，前缀，随机数，保留项，鉴别码，KEY)*

参数描述如下：

——E（）：加密变换函数，可为加密、杂凑等算法，输出为64位，应可根据E（）算法、KEY等参数以及生成的IID计算出联网终端标识；

——联网终端标识：必选参数，用于标识联网终端，可为MAC地址、IMEI等；

——前缀：可选参数，分配给联网终端的IPv6地址前缀，长度为64位；

——随机数：可选参数，随机生成的序列，用于随机化IPv6地址，解决多地址冲突问题；

——保留项：可选参数，用于标识其他信息；

——鉴别码：可选参数，用于编码方法鉴别；

——KEY：可选参数，加密算法所需的密钥或杂凑算法所需的盐值。

# 6　实施要求

IPv6地址接口标识符编码方法的实施要求如下：

a)　互联网接入服务商、应用基础设施服务商、自用网络运营者等运营者通过 DHCPv6 向联网终端分配包括接口标识符的 IPv6 地址时，其接口标识符编码应采用 5.1 或 5.2 的编码方法；

b)　IPv6 地址分配软硬件宜支持本文件第 5 章的编码方法；

c)　联网终端宜支持 DHCPv6 协议及采用 5.1 的编码方法无状态生成接口标识符。

# 参 考 文 献

[1] IETF RFC 4291 IP Version 6 Addressing Architecture
[2] IETF RFC 8415 Dynamic Host Configuration Protocol for IPv6(DHCPv6)
[3] IETF RFC 7039 Source Address Validation Improvement(SAVI) Framework