TC260-PG-20232A

网络安全标准实践指南

—IPv6 地址分配和编码规则 接口标识符

（v1.0-202306）

全国信息安全标准化技术委员会秘书处

2023 年 6 月

本文档可从以下网址获得：
www.tc260.org.cn/

全国信息安全标准化技术委员会
NATIONAL INFORMATION SECURITY STANDARDIZATION TECHNICAL COMMITTEE

前　言

《网络安全标准实践指南》（以下简称《实践指南》）是全国信息安全标准化技术委员会（以下简称“信安标委”）秘书处组织制定和发布的标准相关技术文件，旨在围绕网络安全法律法规政策、标准、网络安全热点和事件等主题，宣传网络安全相关标准及知识，提供标准化实践指引。

声　明

技术支持单位

本《实践指南》得到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、清华大学等单位的技术支持。

目　录

1 范围

本指南规定了IPv6地址接口标识符的编码方法和实施要求。

本指南适用于通过IPv6网络动态分配IPv6地址接口标识符所涉及的相关实体，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 术语定义

2.1 接口标识符（interface identifier; IID）

位于IPv6地址的低64位，用于标识网络内特定接口的标识符。

2.2 互联网接入服务商

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。

注：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。

2.3 应用基础设施服务商

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。

2.4 自用网络

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。

2.5 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。

[来源：IETF RFC 8415]

2.6 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。

2.7 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。

3 接口标识符编码方法

3.1 EUI-64 编码方法

该编码方法采用 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。

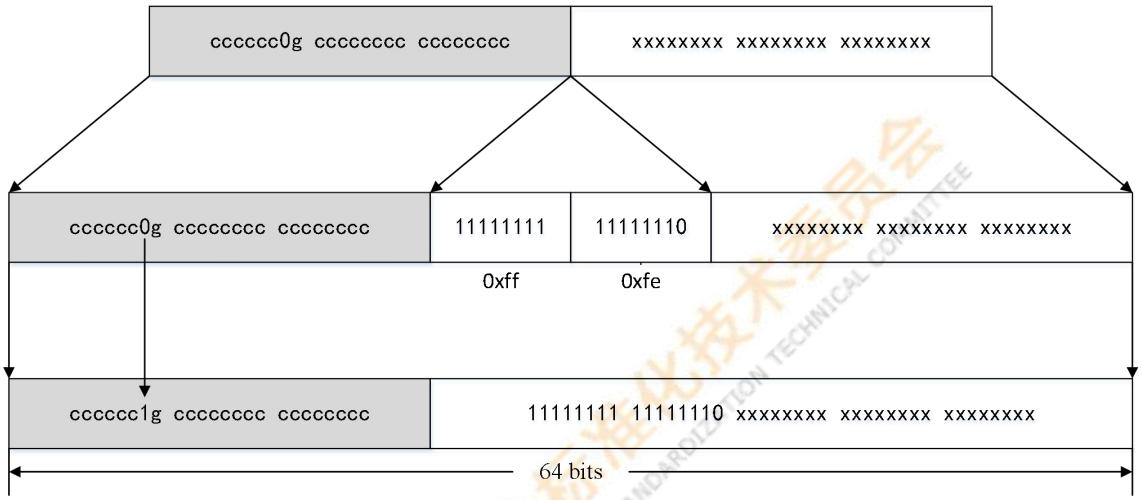

图 1 EUI-64 接口标识符编码方法

3.2 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；E()示例参见附录 A；

——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。

注 1：采用不同的 E()，会产生不同的性能开销。

注 2：使用加密算法时，运营者应采取措施保护密钥安全。

4 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 3.1 或 3.2 的编码方法;

b) 用于 IPv6 地址分配的软硬件宜支持本指南第 3 章的编码方法;

c) 联网终端宜支持 DHCPv6 协议及 3.1 的编码方法。

附录 A　E()示例

A.1　E()示例一

使用对称加密算法，E()可为输入输出长度为 64bit 的块密码算法（如 IDEA、Blowfish 等）。

A.2　E()示例二

使用异或变换方法，E()可为以下运算过程：对“前缀||盐值”进行散列运算取前 64 位，与 64 位二进制序列“联网终端标识||填充位”按位异或运算。

注：||为连接运算符，功能为将两个或多个二进制序列以连接方式合并成一个二进制序列。

参 考 文 献

[1] IETF RFC 4291 IP Version 6 Addressing Architecture

[2] IETF RFC 8415 Dynamic Host Configuration Protocol for IPv6(DHCPv6)