ICS 33.040.40

CSS M32

团体标准

体

标

准

民共和国国家标准

T/GXXXZX XXXXX—2025

|  |
| --- |
|  |

IPv6域名规划技术要求

Technical requirements for IPv6 domain name planning

|  |
| --- |
| （征求意见稿） |
|  |

2025 - 05 - 01发布

2025 - 12 - 01实施

发布

目  次

目录

[目  次 I](#_Toc511032051)

[前  言 III](#_Toc1128576804)

[引  言 IV](#_Toc1414774524)

[1 范围 1](#_Toc1176485284)

[2 规范性引用文件 1](#_Toc1306230259)

[3 术语和定义 1](#_Toc86639732)

[4 域名结构 2](#_Toc160063058)

[4.1 域名层次结构 2](#_Toc1530289762)

[4.2 顶级域名 2](#_Toc1315873462)

[4.3 二级域名 2](#_Toc1098679028)

[4.4 子域名 2](#_Toc1434026690)

[5 命名规则 2](#_Toc477608549)

[5.1 字符集 2](#_Toc2020494204)

[5.2 长度限制 2](#_Toc287176617)

[5.3 命名规范 2](#_Toc1181647110)

[5.4 特殊字符处理 2](#_Toc14210314)

[6 解析机制 2](#_Toc462062581)

[6.1 递归解析 2](#_Toc584931315)

[6.2 权威解析 3](#_Toc1907958886)

[6.3 缓存机制 3](#_Toc839179998)

[6.4 负载均衡 3](#_Toc1573116537)

[6.5 解析性能要求 3](#_Toc1698459142)

[7 安全性要求 3](#_Toc1650163670)

[7.1 DNSSEC 3](#_Toc1696984332)

[7.2 DoH 3](#_Toc485352117)

[7.3 防DDoS攻击 3](#_Toc1170139113)

[7.4 日志记录与审计 3](#_Toc2020316612)

[7.5 访问控制 3](#_Toc1597355167)

[8 生命周期管理 3](#_Toc1055220622)

[8.1 域名注册 3](#_Toc1173037028)

[8.2 域名续费 4](#_Toc1333450136)

[8.3 域名转移 4](#_Toc157095660)

[8.4 域名注销 4](#_Toc1049355457)

[9 管理规范 4](#_Toc1381456635)

[9.1 实施流程 4](#_Toc1695956728)

[9.2 维护管理 5](#_Toc394280865)

[9.3 培训与支持 6](#_Toc1691447060)

[9.4 持续改进 6](#_Toc1909702081)

[9.5 文档管理 7](#_Toc72287305)

[9.6 审计与评估 7](#_Toc1604474580)

[附录 A （资料性） 域名命名示例 8](#_Toc452110681)

[附录 B （资料性） 域名解析流程图 9](#_Toc827072481)

[附录 C （资料性） 域名安全配置指南 10](#_Toc2093024783)

[C.1 DNSSEC配置 10](#_Toc1685390021)

[C.2 DoH配置 10](#_Toc1040779017)

[C.3 防DDoS攻击配置 10](#_Toc1118633904)

[C.4 访问控制配置 10](#_Toc1808178690)

[C.5 日志记录与审计 10](#_Toc1018154133)

[C.6 密钥与证书管理 10](#_Toc966814035)

[C.7 应急响应 10](#_Toc1382213043)

[参 考 文 献 11](#_Toc1524004102)

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设计专利，本文件的发布机构不承担识别这些专利的责任。

本文件由广西电子学会提出、归口并宣贯。

本文件起草单位：。

本文件主要起草人： 。

引  言

在互联网发展的当下，IPv6 的广泛应用解决了 IPv4 地址不足问题，推动了新一代互联网基础设施建设。域名系统作为互联网关键部分，在 IPv6 环境下需进行适配变革，以实现高效解析与精准映射，满足不同主体的多样化需求并保障安全。

团体标准《IPv6 域名规划技术要求》应运而生，为 IPv6 网络环境下域名规划的各个环节提供技术指导与规范遵循。该标准涵盖域名结构、命名规则、解析机制、安全性要求、管理规范以及实施与维护等技术要求，适用于网络运营商、域名管理机构、企业及组织等，助力 IPv6 网络的健康、有序发展。

IPv6域名规划技术要求

1. 范围

本文件规定了IPv6环境下域名规划的技术要求，涵盖域名结构、命名规则、解析机制、安全性要求、管理规范以及实施与维护等内容。

本文件适用于IPv6网络环境下的域名规划、设计、实施和管理，适用于网络运营商、域名管理机构、企业及组织等。

1. 规范性引用文件

下列文件对于本标准的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本标准。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本标准。

GB/T 20001.1-2024 标准编写规则 第1部分：标准的结构和编写

RFC 8200 Internet Protocol, Version 6 (IPv6) Specification

RFC 8484 DNS Queries over HTTPS (DoH)

RFC 4033 DNS Security Introduction and Requirements

RFC 1034 Domain Names - Concepts and Facilities

RFC 1035 Domain Names - Implementation and Specification

1. 术语和定义

下列术语和定义适用于本文件。

3.1

IPv6域名　IPv6 domain name

基于IPv6协议的域名系统，用于将人类可读的域名转换为IPv6地址，支持IPv6网络的资源定位和访问。

3.2

域名解析　Domain name resolution

将域名转换为IP地址的过程，包括递归解析和权威解析。

3.3

递归解析　Recursive parsing

域名服务器向其他域名服务器查询，直到获得最终IP地址的过程，通常由递归域名服务器完成。

3.4

权威解析　Authoritative analysis

域名服务器直接返回域名对应的IP地址的过程，通常由权威域名服务器完成。

3.5

DNSSEC　DNS安全扩展

域名系统安全扩展（DNS Security Extensions），用于验证域名解析结果的真实性和完整性。

3.6

DoH　DNS over HTTPS

通过HTTPS协议加密传输DNS查询，保护用户隐私。

1. 域名结构
   1. 域名层次结构

IPv6域名应采用层次化结构，包括顶级域名（TLD）、二级域名（SLD）和子域名（Subdomain）。

* 1. 顶级域名
  2. 二级域名
  3. 子域名

1. 命名规则
   1. 字符集
   2. 长度限制
   3. 命名规范
   4. 特殊字符处理
2. 解析机制
   1. 递归解析
   2. 权威解析
   3. 缓存机制
   4. 负载均衡
   5. 解析性能要求
3. 安全性要求
   1. DNSSEC
   2. DoH
   3. 防DDoS攻击
   4. 日志记录与审计
   5. 访问控制
4. 生命周期管理
   1. 域名注册
   2. 域名续费
   3. 域名转移
   4. 域名注销
5. 管理规范
   1. 实施流程
   2. 维护管理

日常维护

安全管理

故障处理

* 1. 培训与支持

技术支持

* 1. 持续改进
  2. 文档管理
  3. 审计与评估

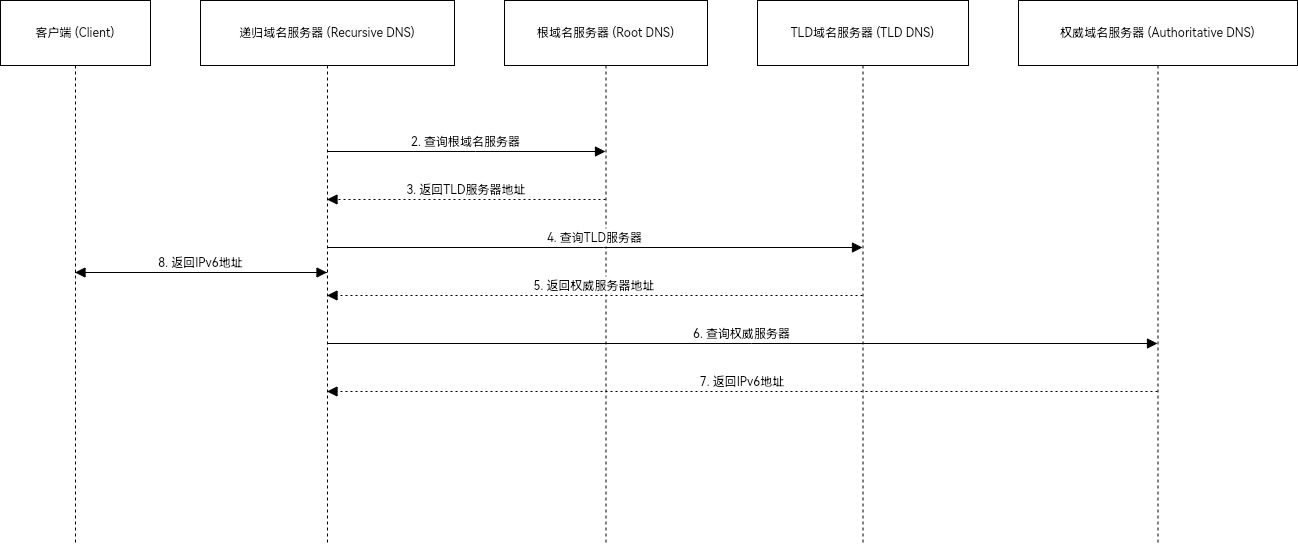
# 附录 A （资料性） 域名命名示例

示例1：www.example.com

示例2：mail.example.com

示例3：ftp.example.com

# 附录 B （资料性） 域名解析流程图



# 附录 C （资料性） 域名安全配置指南

* 1. DNSSEC配置

1. 密钥生成：使用工具生成ZSK（Zone Signing Key）和KSK（Key Signing Key）。

2. 签名区域文件：使用dnssec-signzone工具对区域文件进行签名。

3. 发布DS记录：从KSK中提取DS记录并提交至上级域名服务器。

* 1. DoH配置

1. 服务器端配置：配置支持DoH的DNS服务器软件，启用HTTPS证书。

2. 客户端配置：在客户端配置DoH服务器地址，使用支持DoH的客户端软件。

* 1. 防DDoS攻击配置

1. 流量清洗：使用CDN或云服务提供商的流量清洗服务。

2. 速率限制：在域名服务器上配置查询速率限制。

3. IP黑名单：使用工具动态屏蔽恶意IP地址。

* 1. 访问控制配置

1. 限制查询来源：在域名服务器上配置ACL，仅允许可信IP地址查询。

2. 管理接口保护：使用强密码和双因素认证保护管理接口。

* 1. 日志记录与审计

1. 日志配置：在域名服务器上启用查询日志记录。

2. 日志分析：使用日志分析工具监控域名解析行为，识别异常查询。

* 1. 密钥与证书管理

1. 密钥轮换：定期轮换DNSSEC密钥，更新签名区域文件。

2. 证书更新：定期更新HTTPS证书，配置自动更新工具。

* 1. 应急响应

1. 故障处理：制定域名解析故障应急预案，定期进行故障演练。

2. 安全事件处理：

- 监控域名解析日志，及时发现和处置安全事件。

- 与上级域名管理机构或安全服务提供商协作，快速恢复服务。

- 制定安全事件应急预案，明确处理流程和责任人。

参 考 文 献

[1]　RFC 1034 Domain Names - Concepts and Facilities

[2]　RFC 1035 Domain Names - Implementation and Specification

[3]　RFC 4033 DNS Security Introduction and Requirements

[4]　RFC 8200 Internet Protocol, Version 6 (IPv6) Specification

[5] RFC 8484 DNS Queries over HTTPS (DoH)

[6] GB/T 7714 信息与文献 参考文献著录规则

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_