



中华人民共和国国家标准

GB/T 46240.2—2025

IPv6 网络设备安全技术要求和测试方法 第 2 部分：交换机

Security requirements and testing methods of IPv6 network equipment—
Part 2: Switch

2025-08-29 发布

2025-12-01 实施

国家市场监督管理总局 发布
国家标准化管理委员会

目 次

前言 V

引言 VI

1 范围 1

2 规范性引用文件 1

3 术语和定义 1

4 缩略语 1

5 通则 2

6 安全技术要求 3

6.1 数据平面安全 3

6.1.1 标识和鉴别 3

6.1.2 可信信道 3

6.1.3 系统访问 3

6.1.4 资源分配 3

6.1.4.1 抗大流量攻击能力 3

6.1.4.2 抗畸形包能力 4

6.1.4.3 ND 非法报文攻击防护 4

6.1.4.4 IPv6 地址欺骗防护 4

6.1.4.5 组播报文抑制 4

6.1.5 安全审计 4

6.1.5.1 攻击溯源功能 4

6.1.5.2 采样功能 4

6.1.6 系统功能保护 5

6.1.7 安全管理 5

6.2 控制平面安全 5

6.2.1 标识和鉴别 5

6.2.1.1 路由认证 5

6.2.1.2 ND 报文鉴别功能 5

6.2.1.3 智能无损存储网络认证 5

6.2.1.4 跨设备链路聚合认证 5

6.2.1.5 OpenFlow 认证 5

6.2.2 可信信道 5

6.2.3 系统访问 6

6.2.4 资源分配 6

6.2.4.1	MAC 地址学习限制	6
6.2.4.2	关闭 ICMPv6 功能	6
6.2.4.3	关闭 Hop-by-Hop 选项功能	6
6.2.5	安全审计	6
6.2.6	系统功能保护	6
6.2.7	安全管理	6
6.3	管理平面安全	6
6.3.1	标识和鉴别	6
6.3.2	可信信道	6
6.3.3	系统访问	7
6.3.3.1	访问控制安全	7
6.3.3.2	串口访问	7
6.3.3.3	SSH 访问	7
6.3.3.4	SNMP 访问	7
6.3.3.5	Web 访问	7
6.3.4	资源分配	7
6.3.5	安全审计	8
6.3.6	系统功能保护	8
6.3.7	安全管理	8
6.3.7.1	分级分权管理	8
6.3.7.2	不安全配置检查	8
6.3.7.3	数字证书管理	8
6.3.7.4	密码要求	8
7	测试方法	8
7.1	测试环境	8
7.2	数据平面安全测试	10
7.2.1	标识和鉴别	10
7.2.1.1	802.1X 接入认证功能	10
7.2.1.2	MAC 接入认证功能	11
7.2.1.3	MAC 地址漂移检测功能	11
7.2.2	可信信道	11
7.2.3	系统访问	11
7.2.4	资源分配	12
7.2.4.1	抗大流量攻击能力	12
7.2.4.2	抗畸形包能力	13
7.2.4.3	ND 非法报文攻击防护	15
7.2.4.4	IPv6 地址欺骗防护	15

7.2.4.5 组播报文抑制	16
7.2.5 安全审计	16
7.2.5.1 攻击溯源功能	16
7.2.5.2 采样功能	16
7.2.6 系统功能保护	16
7.2.7 安全管理	17
7.3 控制平面安全测试	17
7.3.1 标识和鉴别	17
7.3.1.1 路由认证	17
7.3.1.2 ND 报文鉴别功能	18
7.3.1.3 智能无损存储网络认证	19
7.3.1.4 跨设备链路聚合认证	20
7.3.1.5 OpenFlow 认证	20
7.3.2 可信信道	20
7.3.2.1 RIPng 支持 IPsec 功能	20
7.3.2.2 OSPFv3 支持 IPsec 功能	21
7.3.2.3 BGP4+ 支持 TLS 功能	21
7.3.3 系统访问	21
7.3.3.1 BGP4+ 入向路由过滤功能	21
7.3.3.2 BGP4+ 出向路由过滤功能	21
7.3.3.3 基于 BGP4+ 属性的路由过滤功能	22
7.3.3.4 路由重分布中的路由过滤功能	22
7.3.4 资源分配	22
7.3.4.1 MAC 地址学习限制	22
7.3.4.2 关闭 ICMPv6 功能	23
7.3.4.3 关闭 Hop-by-Hop 选项功能	23
7.3.5 安全审计	23
7.3.6 系统功能保护	23
7.3.7 安全管理	24
7.4 管理平面安全测试	24
7.4.1 标识和鉴别	24
7.4.2 可信信道	24
7.4.2.1 SSH	24
7.4.2.2 TLS	24
7.4.3 系统访问	25
7.4.3.1 访问控制安全	25
7.4.3.2 串口访问	25

7.4.3.3	SSH 访问	25
7.4.3.4	SNMP 访问	26
7.4.3.5	Web 访问	26
7.4.4	资源分配	26
7.4.4.1	管理平面协议防范异常报文攻击	26
7.4.4.2	管理平面协议防范拒绝服务攻击	27
7.4.5	安全审计	27
7.4.6	系统功能保护	27
7.4.6.1	敏感数据加密保存	27
7.4.6.2	安全启动功能	27
7.4.6.3	预装软件启动及更新安全	28
7.4.7	安全管理	28
7.4.7.1	分级分权管理	28
7.4.7.2	不安全配置检查	28
7.4.7.3	数字证书管理	28
参考文献	29

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。

本文件是 GB/T 46240《IPv6 网络设备安全技术要求和测试方法》的第 2 部分。GB/T 46240 已经发布了以下部分：

- 第 1 部分：路由器；
- 第 2 部分：交换机。

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。

本文件由中华人民共和国工业和信息化部提出。

本文件由全国通信标准化技术委员会(SAC/TC 485)归口。

本文件起草单位：中国信息通信研究院、华为技术有限公司、国家计算机网络应急技术处理协调中心、国家石油天然气管网集团有限公司、中讯邮电咨询设计院有限公司、中兴通讯股份有限公司、国家工业信息安全发展研究中心、中国福利会国际和平妇幼保健院、山石网科通信技术股份有限公司、哈尔滨华德学院。

本文件主要起草人：葛裴、夏立强、刘述、胡俊理、王文磊、瞿洁武、王力、李长连、王东博、周继华、刘子贺、陈昌杰、徐俊、吴迪。

引 言

根据《关于加快推进互联网协议第六版（IPv6）规模部署和应用工作的通知》，为加快解决网络设备 IPv6 安全方面的缺失，推动 IPv6 规模部署和应用创新成果标准化，我国制定了一系列 IPv6 应用标准。其中，GB/T 46240《IPv6 网络设备安全技术要求和测试方法》是为规范和指导我国 IPv6 规模部署的顺利推进而制定的标准，拟由两个部分构成。

- 第 1 部分：路由器。目的在于提出并规范路由器 IPv6 安全开发和应用。
- 第 2 部分：交换机。目的在于提出并规范交换机 IPv6 安全开发和应用。

IPv6 网络设备安全技术要求和测试方法

第 2 部分：交换机

1 范围

本文件规定了支持 IPv6 能力的交换机的安全架构,以及数据平面、控制平面、管理平面的安全技术要求,描述了相应的测试方法。

本文件适用于支持 IPv6 能力的交换机设备的设计、开发和测试。

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 信息安全技术 术语

GB/T 41267—2022 网络关键设备安全技术要求 交换机设备

3 术语和定义

GB/T 25069 界定的以及下列术语和定义适用于本文件。

3.1

交换机 switch

利用内部交换机制来提供联网设备之间连通性的设备。

注:交换机中的交换机制通常在开放系统互联(OSI)参考模型的第 2 层或第 3 层实现。

[来源:GB/T 41267—2022,3.1]

4 缩略语

下列缩略语适用于本文件。

ACL:访问控制列表(Access Control List)

BGP4+:IPv6 边界网关协议(Border Gateway Protocol for IPv6)

CGA:加密生成地址(Cryptographically Generated Address)

CLI:命令行接口(Command-Line Interface)

CPU:中央处理器(Central Processing Unit)

DAD:重复地址探测(Duplicate Address Detection)

DUT:被测设备(Device Under Test)

HMAC:散列消息验证码(Hashed Message Authentication Code)

HTTPS:超文本传输安全协议(Hypertext Transfer Protocol Secure)

ICMPv6:互联网控制管理协议版本 6(Internet Control Management Protocol version 6)

IPsec:互联网协议安全(Internet Protocol security)