



# 中华人民共和国国家标准

GB/T 21050—2019  
代替 GB/T 21050—2007

---

## 信息安全技术 网络交换机安全技术要求

Information security technology—  
Security requirements for network switch

2019-08-30 发布

2020-03-01 实施

---

国家市场监督管理总局  
中国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、缩略语 .....	1
3.1 术语和定义 .....	1
3.2 缩略语 .....	2
4 网络交换机描述 .....	2
5 安全问题定义 .....	3
5.1 资产 .....	3
5.2 威胁 .....	4
5.3 组织安全策略 .....	5
5.4 假设 .....	6
6 安全目的 .....	7
6.1 TOE 安全目的 .....	7
6.2 环境安全目的 .....	9
7 安全要求 .....	9
7.1 扩展组件定义 .....	9
7.2 安全功能要求 .....	10
7.3 安全保障要求 .....	19
8 基本原理 .....	30
8.1 安全目的基本原理 .....	30
8.2 安全要求基本原理 .....	42
8.3 组件依赖关系 .....	49
参考文献 .....	52

## 前 言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准代替 GB/T 21050—2007《信息安全技术 网络交换机安全技术要求(评估保证级 3)》。与 GB/T 21050—2007 相比,除编辑性修改外主要技术变化如下:

- 对使用范围进行了修改,并增加了关于密码算法的约定(见第 1 章,2007 年版的第 1 章);
- 增加了对术语标准的引用(见第 2 章,2007 年版第 2 章);
- 增加了“可信 IT 产品”术语,删掉了“网络交换机”术语(见第 3 章,2007 年版的第 3 章);
- 修改了网络交换机的描述(见第 4 章,2007 年版的第 4 章);
- 将安全环境修改为安全问题定义,且归并和修改了假设、威胁、组织安全策略(见第 5 章,2007 年版的第 5 章);
- 修改和删减了安全目的(见第 6 章,2007 年版的第 6 章);
- 增加了扩展组件,根据 GB/T 18336—2015 增删了安全要求(见第 7 章);
- 增加了基本原理一章(见第 8 章)。

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这些专利的责任。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:中国信息安全测评中心、吉林信息安全测评中心、华为技术有限公司、清华大学、锐捷网络股份有限公司、网神信息技术(北京)股份有限公司。

本标准主要起草人:李凤娟、张宝峰、刘晖、张翀斌、贾炜、张骁、庞博、刘昱函、唐喜庆、蒋显岚、刘玘娉、钟建伟、刘海利、叶晓俊、李玲、徐涛。

本标准所代替标准的历次版本发布情况为:

- GB/T 21050—2007。

# 信息安全技术

## 网络交换机安全技术要求

### 1 范围

本标准规定了网络交换机达到 EAL2 和 EAL3 的安全功能要求及安全保障要求,涵盖了安全问题定义、安全目的、安全要求等内容。

本标准适用于网络交换机的测试、评估和采购,也可用于指导该类产品的研制和开发。

### 2 规范性引用文件

下列文件对于本文件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文件。凡是不注日期的引用文件,其最新版本(包括所有的修改单)适用于本文件。

GB/T 18336.1—2015 信息技术 安全技术 信息技术安全评估准则 第 1 部分:简介和一般模型

GB/T 18336.2—2015 信息技术 安全技术 信息技术安全评估准则 第 2 部分:安全功能组件

GB/T 18336.3—2015 信息技术 安全技术 信息技术安全评估准则 第 3 部分:安全保障组件

GB/T 25069—2010 信息安全技术 术语

### 3 术语和定义、缩略语

#### 3.1 术语和定义

GB/T 25069—2010 和 GB/T 18336.1—2015 界定的以及下列术语和定义适用于本文件。

##### 3.1.1

**可信 IT 产品** **trusted IT product**

有与 TOE 协调管理的安全功能要求,但不属于 TOE 的其他 IT 产品,且假定可正确执行自身的安全功能要求。

##### 3.1.2

**可信信道** **trusted channel**

TSF 和远程可信 IT 产品间在必要的信任基础上进行通信的一种通信手段。

##### 3.1.3

**可信路径** **trusted path**

用户与 TSF 间在必要的信任基础上进行通信的一种通信手段。

##### 3.1.4

**可信源** **trusted source**

能够被标识和鉴别的源或节点,从该源或节点发出信息的完整性能被核实和确认。

##### 3.1.5

**客户** **client**

向另一方请求服务的一方。