ICS 35.040
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1484—2018
代替 GA/T 684—2007 和 GA/T 685—2007

信息安全技术　交换机安全技术要求和测试评价方法

Information security technology—Security technical requirements and testing and evaluation methods for switch

2018-05-07 发布　　2018-05-07 实施

中华人民共和国公安部　　发 布

目　　次

前　言

本标准按照GB/T 1.1—2009给出的规则起草。

本标准代替GA/T 684—2007《信息安全技术　交换机安全技术要求》和GA/T 685—2007《信息安全技术　交换机安全评估准则》，与GA/T 684—2007和GA/T 685—2007相比主要技术变化如下：

——修改了等级划分要求，将等级划分为基本级和增强级（见第8章，GA/T 684—2007的第4章～第6章和A.1，GA/T 685—2007的第4章～第6章）；

——删除了“IDS”“IPSec”“MPLS”“VPN”等缩略语，增加了“TOS”缩略语（见第4章，GA/T 684—2007的第3章）；

——增加了“交换机描述”（见第5章）；

——增加了“总体说明”（见6.1）；

——修改了“自主访问控制”功能和测试评价方法（见6.2.1、7.1.1，GA/T 684—2007的6.1.1，GA/T 685—2007的6.1.1）；

——修改了“划分虚拟局域网”功能和测试评价方法（见6.2.2、7.1.2，GA/T 684—2007的6.1.5，GA/T 685—2007的6.1.5）；

——修改了“身份鉴别”功能和测试评价方法（见6.2.3、7.1.3，GA/T 684—2007的6.1.2，GA/T 685—2007的6.1.2）；

——修改了“安全审计”功能和测试评价方法（见6.2.4、7.1.4，GA/T 684—2007的6.1.4，GA/T 685—2007的6.1.4）；

——修改了“安全管理”功能和测试评价方法（见6.2.5、7.1.5，GA/T 684—2007的6.1.3，GA/T 685—2007的6.1.3）；

——修改了安全保障要求和测试评价方法（见6.3、7.2，GA/T 684—2007的4.2、5.2、6.2，GA/T 685—2007的4.2、5.2、6.2）；

——删除了附加安全功能和评估准则（见GA/T 684—2007的第7章、GA/T 685—2007的第7章）。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：公安部计算机信息系统安全产品质量监督检验中心、公安部第三研究所。

本标准主要起草人：杨元原、俞优、陈玉成、张笑笑、邹春明、顾玮。

本标准的历次版本发布情况为：

——GA/T 684—2007、GA/T 685—2007。

信息安全技术　交换机安全技术要求和测试评价方法

1　范围

本标准规定了交换机的安全技术要求、测试评价方法及安全等级划分。

本标准适用于交换机的设计、开发与测试。

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 18336.3—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

GB/T 18336.3—2015 和 GB/T 25069—2010 界定的以及下列术语和定义适用于本文件。

3.1

交换机　switch

工作于开放式系统互联模型第二层，可基于数据链路层信息转发数据包，并提供信息流控制、划分虚拟局域网、身份鉴别、安全审计等安全功能的网络设备。

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)

MAC：介质访问控制(Media Access Control)

VLAN：虚拟局域网(Virtual Local Area Network)

TOS：服务类型(Type of Service)

5　交换机描述

交换机除具备联通多个小型网络或子网、提供数据交换平台的功能外，为抵御网络安全威胁，还具备访问控制、划分虚拟局域网、身份鉴别、安全审计和安全管理等能力。

交换机通过对不同子网发送的数据包进行过滤转发来防止广播风暴和网络拥塞等安全威胁。交换机保护的资产是其连接的不同的子网数据，此外，交换机本身及其内部的重要数据也是受保护的资产。