ICS 35.040
A 90

GA

中华人民共和国公共安全行业标准

GA/T 684—2007

信息安全技术　交换机安全技术要求

Information security technology—
Technical requirements for switch security

2007-03-20 发布　　2007-05-01 实施

中华人民共和国公安部　　发 布

目　　次

前　言

本标准是从信息技术方面详细规定了各安全保护级别的交换机所应具有的安全功能要求和安全保证要求。

本标准中的附录 A 是资料性附录。

本标准由公安部公共信息网络安全监察局提出。

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：中国科学院研究生院信息安全国家重点实验室。

本标准主要起草人：戴英侠、左晓栋、何申。

引　言

交换机是重要的网络互连设备，制定交换机安全技术要求对于评估交换机产品安全等级，保障网络安全具有重要的意义。

本标准仅对一到三级安全保护等级做了技术要求，与 GB 17859—1999 的对应关系是，第一级对应用户自主保护级，第二级对应系统审计保护级，第三级对应安全标记保护级。

本标准文本中，加粗字体表示较低等级中没有出现或增强的技术要求。

信息安全技术　交换机安全技术要求

1　范围

本标准分等级规定了交换机的安全功能要求和安全保证要求。

本标准适用于公共安全行业对交换机产品的研发、生产；同时也可适用于对交换机产品的采购和部署。

2　规范性引用文件

下列文件中的条款通过本标准的引用而成为本标准的条款。凡是注日期的引用文件，其随后所有的修改单（不包括勘误的内容）或修订版均不适用于本标准，然而，鼓励根据本标准达成协议的各方研究是否可使用这些文件的最新版本。凡是不注日期的引用文件，其最新版本适用于本标准。

GB 17859—1999　计算机信息系统　安全保护等级划分准则

GB/T 18336.1—2001　信息技术　安全技术　信息技术安全性评估准则　第1部分：简介和一般模型

3　术语、定义和缩略语

3.1　术语和定义

GB 17859—1999 和 GB/T 18336.1—2001 确立的以及下列术语和定义适用于本标准。

3.1.1

交换机　switch

一种基于硬件网卡地址，能完成封装转发数据包功能的网络设备。

3.2　缩略语

下列缩略语适用于本标准。

ACL	Access ControlList　访问控制列表
IDS	Instrusion Detection System　入侵检测系统
IPSec	Internet Protocol Security　互联网协议安全协议
MAC	Media Access Control　介质访问控制
MPLS	Multi-Protocol Label Switching　多协议标记交换
VLAN	Virtual Local Area Network　虚拟局域网
VPN	Virtual Private Network　虚拟专用网

4　第一级安全要求

4.1　安全功能要求

4.1.1　自主访问控制

交换机应执行自主访问控制策略，通过管理员属性表，控制不同管理员对交换机的配置数据和其他数据的查看、修改，以及对交换机上程序的执行，阻止非授权人员进行上述活动。

4.1.2　身份鉴别

4.1.2.1　管理员鉴别

在管理员进入系统会话之前，安全功能应鉴别管理员身份。鉴别时采用口令机制，并在每次登录系统时进行。口令应是不可见的，并在存储和传输时加密保护。