ICS 35.040
L 80

中华人民共和国国家标准

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）

Information security techniques—Security requirements for network switch（EAL3）

2007-08-24 发布　　2008-01-01 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　　次

前　言

本标准依据GB/T 18336—2001《信息技术　安全技术　信息技术安全性评估准则》的要求，规定了网络交换机的安全技术要求。附录A和附录B是资料性附录，附录A对本标准的内在合理性进行了阐述，附录B是安全功能要求的应用注释。

本标准由全国信息安全标准化技术委员会提出并归口。

本标准起草单位：中国信息安全产品测评认证中心。

本标准主要起草人：李守鹏、徐长醒、付敏、王书毅、郭颖、刘楠、毕强、王迪、裘晓峰、闫石、王眉林、刘威鹏、李云雪、张展、苏智睿、王伟雄、王怡、万晓兰。

引　言

本标准定义了网络交换机应在生产商安全目标文档中包括的安全要求的最小集合。系统集成商和信息系统安全工程师可以利用本标准确认现有交换机的应用领域，以提供更为全面的安全方案。本标准规定了交换机应满足的用于信息保护的安全要求。

满足本标准的交换机，可以为组织提供自行处理的额外安全机制，以加强其对自身信息的保障。额外的安全机制包括但不限于以下几种：防火墙、网关、加密。另外，本标准适用于以下三种可能出现的管理情形，概括总结如下：

a) 购买者本人管理自己的设备。

b) 设备不是由购买者而是由网络供应商或商业组织管理。设备被安放在网络供应商或商业组织的场所。

c) 仅仅从提供商那里购买服务。

为正确执行交换机的管理功能，需要网络管理系统的支持。网络管理系统的连接参数是预先设置的，它是执行操作功能应有的一部分，但在本标准中不作为交换机的一部分。

本标准定义的要求适用于保护日常的私有敏感信息，此信息是与管理和控制相关的信息，不包括对通过交换机的用户数据的保护。本标准列出了交换机所需处理的假设、威胁和组织安全策略，并定义了交换机及其环境的独立的安全目的。最后，本标准提供了安全环境、安全目的和安全要求的对应关系。附录 A 描述了这些对应关系。

信息安全技术
网络交换机安全技术要求
（评估保证级 3）

1 范围

本标准规定了网络交换机 EAL3 级的安全技术要求，主要包括网络交换机的安全假设、威胁和组织策略等安全环境，以及网络交换机 EAL3 级的安全目的、安全功能要求和安全保证要求。

本标准适用于网络交换机的研制、开发、测试、评估和采购。

本标准主要适用于信息系统安全工程师、产品生产商、安全产品评估者。

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/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（idt ISO/IEC 15408-1：1999）

GB/T 18336.2—2001 信息技术 安全技术 信息技术安全性评估准则 第 2 部分：安全功能要求（idt ISO/IEC 15408-2：1999）

GB/T 18336.3—2001 信息技术 安全技术 信息技术安全性评估准则 第 3 部分：安全保证要求（idt ISO/IEC 15408-3：1999）

3 术语、定义、缩略语和约定

3.1 术语和定义

GB/T 18336—2001 确立的以及下列术语和定义适用于本标准。

3.1.1

客户端 client

发起或接受数据传送的源。通过网络交换机的数据的源发者。

3.1.2

网络审计管理员 network audit management operator

仅具有查看权限，负责收集、分析和查看网络行为数据的网络管理角色。如：查看网络交换机配置和信息流策略等。

3.1.3

网络配置管理员 network management administrator

受到严格限制的具有部分网络管理能力的管理角色，可以执行网络交换机管理功能的子集，如：配置管理网络系统，利用权限解决网络故障等。该管理员同时具备网络审计管理员的能力。

3.1.4

网络安全管理员 network security administrator

具有所有管理级别的访问权限，可以访问网络交换机的各个区域，同时具备网络配置管理员和网络审计管理员的能力，如：创建、修改和存取访问控制列表、加载密钥、限制应用程序执行以及维护网络管