

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	III
引言	IV
1 范围	1
2 规范性引用文件	1
3 术语、定义和缩略语	1
4 第一级安全要求	1
4.1 安全功能要求	1
4.1.1 自主访问控制	1
4.1.2 身份鉴别	1
4.1.3 安全管理	2
4.1.4 划分虚拟局域网	2
4.2 安全保证要求	2
4.2.1 配置管理	2
4.2.2 交付和运行	2
4.2.3 开发	2
4.2.4 指导性文档	2
4.2.5 生命周期支持	2
4.2.6 测试	2
5 第二级安全要求	3
5.1 安全功能要求	3
5.1.1 自主访问控制	3
5.1.2 身份鉴别	3
5.1.3 安全管理	3
5.1.4 审计	3
5.1.5 划分虚拟局域网	4
5.2 安全保证要求	4
5.2.1 配置管理	4
5.2.2 交付和运行	4
5.2.3 开发	4
5.2.4 指导性文档	4
5.2.5 生命周期支持	5
5.2.6 测试	5
5.2.7 脆弱性评定	5
6 第三级安全要求	5
6.1 安全功能要求	5
6.1.1 自主访问控制	5
6.1.2 身份鉴别	5
6.1.3 安全管理	6

6.1.4	审计	6
6.1.5	划分虚拟局域网	7
6.2	安全保证要求	7
6.2.1	配置管理	7
6.2.2	交付和运行	7
6.2.3	开发	7
6.2.4	指导性文档	8
6.2.5	生命周期支持	8
6.2.6	测试	8
6.2.7	脆弱性评定	8
7	附加安全功能	8
7.1	网络访问控制功能	8
7.2	虚拟专网功能	8
7.3	防火墙防护功能	9
7.4	入侵检测功能	9
附录 A (资料性附录)	安全要求对照表	10
参考文献		11

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。

当进行鉴别时,交换机安全功能应仅将最少的反馈(如:打入的字符数,鉴别的成功或失败)提供给用户。

4.1.2.2 鉴别失败处理

在经过一定次数的鉴别失败以后,交换机应锁定该账号。最多失败次数仅由授权管理员设定。

4.1.3 安全管理

4.1.3.1 用户管理

应能够设置多个角色,具备划分管理员级别和规定相关权限(如监视、维护配置等)的能力,能够限定每个用户的管理范围和权限,防止非法用户和非法操作。

4.1.3.2 安全属性管理

应允许交换机管理员对安全功能行为进行控制管理,这些管理包括:

- a) 与对应的交换机自主访问控制、鉴别和安全保证技术相关的功能的管理。
- b) 与一般的安装和配置有关的功能的管理。交换机的安全配置参数要有初始值。交换机安装后,安全功能应能及时提醒管理员修改配置,并能周期性地提醒管理员维护配置。

4.1.4 划分虚拟局域网

交换机应具备划分虚拟局域网的功能,使得同一局域网内多台主机可以汇聚成一个用户组,从逻辑上可认为是在同一局域网内,而其他虚拟局域网与其在逻辑上分属在不同的局域网内。交换机应在帧结构中有对虚拟局域网的标识。

4.2 安全保证要求

4.2.1 配置管理

开发者应设计和实现交换机配置管理,为产品的不同版本提供唯一的标识,且产品的每个版本应当使用其唯一标识作为标签。

4.2.2 交付和运行

开发者应以文档形式对交换机安全交付以及安装和启动过程进行说明。文档中应包括:

- a) 对安全地将交换机交付给用户的说明;
- b) 对安全地安装和启动交换机的说明。

4.2.3 开发

开发者应提供交换机功能设计,要求按非形式化功能设计的要求进行功能设计,以非形式方法描述安全功能及其外部接口,并描述使用外部安全功能接口的目的与方法。

4.2.4 指导性文档

开发者应编制交换机的指导性文档,要求如下:

- a) 文档中应该提供关于交换机的安全功能与接口、交换机的管理和配置、交换机的启动和操作、安全属性、警告信息的描述。
- b) 文档中不应包含任何一旦泄漏将会危及系统安全的信息,文档可以为硬拷贝、电子文档或联机文档。如果是联机文档,应控制对文档的访问。

4.2.5 生命周期支持

开发者应建立开发和维护交换机的生命周期模型,包括用于开发和维护交换机的程序、工具和技术。开发者应按其定义的生命周期模型进行开发,并提供生命周期定义文档,在文档中描述用于开发和维护交换机安全功能的生命周期模型。

4.2.6 测试

开发者应对交换机进行测试,要求如下:

- a) 应进行一般功能测试,保证交换机能够满足所有安全功能的要求;
- b) 保留并提供测试文档,详细描述测试计划、测试过程以及预测结果和实际测试结果。

5 第二级安全要求

5.1 安全功能要求

5.1.1 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。

5.1.2 身份鉴别

5.1.2.1 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。

当进行鉴别时,交换机安全功能应仅将最少的反馈(如:打入的字符数,鉴别的成功或失败)提供给用户。

5.1.2.2 鉴别失败处理

在经过一定次数的鉴别失败以后,交换机应锁定该账号。最多失败次数仅由授权管理员设定。

5.1.2.3 超时锁定

应具有登录超时锁定功能。在设定的时间段内没有任何操作的情况下,终止会话,需要再次进行身份鉴别才能够重新操作。最大超时时间仅由授权管理员设定。

5.1.2.4 会话锁定

应允许管理员锁定自己的交互会话,锁定后需要再次进行身份鉴别才能够重新管理产品。

5.1.2.5 登录历史

应设计和实现交换机登录历史功能。为用户提供系统登录活动的有关信息,使用户识别入侵的企图。成功通过鉴别,登录系统后,交换机应向用户显示如下数据:

- 日期、时间、来源和上次成功登录系统的情况;
- 上次成功登录系统以来身份鉴别失败的情况;
- 口令距失效日期的天数。

5.1.3 安全管理

5.1.3.1 用户管理

应设置多个角色,具备划分管理员级别和规定相关权限(如监视、维护配置等)的能力,能够限定每个用户的管理范围和权限,防止非法用户和非法操作。

5.1.3.2 安全属性管理

应允许交换机管理员对安全功能行为进行控制管理,这些管理包括:

- a) 与对应的交换机自主访问控制、鉴别和安全保证技术相关的功能的管理。
- b) 与一般的安装和配置有关的功能的管理。交换机的安全配置参数要有初始值。交换机安装后,安全功能应能及时提醒管理员修改配置,并能周期性地提醒管理员维护配置。

5.1.4 审计

5.1.4.1 审计数据生成

交换机应具有审计功能,至少能够审计以下行为:

- 审计功能的启动和终止;
- 账户管理;
- 登录事件;
- 系统事件;
- 配置文件的修改。

应能为交换机的可审计行为生成审计记录,并在每一个审计记录中至少记录以下信息:

- 事件发生的日期和时间；
- 事件的类型；
- 管理员身份；
- 事件的结果(成功或失败)。

5.1.4.2 审计数据查阅

应提供给已授权的管理员从审计记录中读取审计信息的能力,为管理员提供的审计记录具有唯一、明确的定义和方便阅读的格式。

5.1.4.3 审计数据保护

应能保护已存储的审计记录,避免未经授权的删除,并能监测和防止对审计记录的修改。当审计存储耗尽、失败或受到攻击时,应确保最近的审计记录在一定的时间内不会被破坏。

5.1.5 划分虚拟局域网

交换机应具备划分虚拟局域网的功能,使得同一局域网内多台主机可以汇聚成一个用户组,从逻辑上可认为是在同一局域网内,而其他虚拟局域网与其在逻辑上分属在不同的局域网内。交换机应在帧结构中有对虚拟局域网的标识。

虚拟局域网可分为基于端口的划分,基于硬件 MAC 地址层,基于网络层(基于策略)。

5.2 安全保证要求

5.2.1 配置管理

开发者应设计和实现交换机配置管理,要求如下:

- a) 开发者应使用配置管理系统,并提供配置管理文档,为产品的不同版本提供唯一的标识,且产品的每个版本应当使用其唯一标识作为标签。
- b) 配置管理范围至少应包括交换机的产品实现表示、设计文档、测试文档、用户文档、配置管理,从而确保它们的修改是在一个正确授权的可控方式下进行的。配置管理文档至少应能跟踪上述内容,并描述配置管理系统是如何跟踪这些配置项的。

5.2.2 交付和运行

开发者应以文档形式对交换机安全交付以及安装和启动过程进行说明。文档中应包括:

- a) 对安全地将交换机交付给用户的说明;
- b) 对安全地安装和启动交换机的说明。

5.2.3 开发

开发者应提供交换机功能规范,要求如下:

- a) 按非形式化功能设计的要求进行功能设计,以非形式方法描述安全功能与其外部接口,并描述使用外部安全功能接口的目的与方法。
- b) 提供交换机安全功能的高层设计。高层设计应按子系统描述安全功能及其结构,并标识安全功能子系统的所有接口。高层设计还应标识实现安全功能所要求的基础性的硬件、固件和软件。
- c) 开发者应提供交换机安全功能的功能设计与高层设计之间的非形式化对应性分析,该分析应证明功能设计表示的所有相关安全功能都在高层设计中得到正确且完备的细化。

5.2.4 指导性文档

开发者应编制交换机的指导性文档,要求如下:

- a) 文档中应该提供关于交换机的安全功能与接口、交换机的管理和配置、交换机的启动和操作、安全属性、警告信息、审计工具的描述。
- b) 文档中不应包含任何一旦泄漏将会危及系统安全的信息,文档可以为硬拷贝、电子文档或联机文档。如果是联机文档,应控制对文档的访问。

5.2.5 生命周期支持

开发者应建立开发和维护交换机的生命周期模型,即用于开发和维护交换机的程序、工具和技术。要求如下:

- a) 开发者应按其定义的生命周期模型进行开发,并提供生命周期定义文档,在文档中描述用于开发和维护交换机安全功能的生命周期模型。
- b) 该模型对于交换机开发和维护应提供必要的控制,采用物理上、程序上、人员上以及其他方面的安全措施保护交换机开发环境的安全,包括场地的物理安全和对开发人员的选择,并采取适当的防护措施来消除或降低交换机开发所面临的安全威胁。

5.2.6 测试

开发者应对交换机进行测试,要求如下:

- a) 应进行一般功能测试,保证交换机能够满足所有安全功能的要求。
- b) 应提供测试深度的分析。在深度分析中,应论证测试文档中所标识的对安全功能的测试足以表明该安全功能的运行与高层设计是一致的。
- c) 应进行相符性独立测试,由专业第三方独立实验室或消费者组织实施测试,确认交换机能够满足所有安全功能的要求。
- d) 保留并提供测试文档,详细描述测试计划、测试过程以及预测结果和实际测试结果。

5.2.7 脆弱性评定

开发者应提供指导性文档和分析文档,在文档中确定对交换机的所有可能的操作方式(包括失败和操作失误后的操作)的后果以及对于保持安全操作的意义,并列出所有目标环境的假设和所有的外部安全措施(包括外部程序的、物理的或人员控制)要求。所述内容应是完备、清晰、一致和合理的。

开发者应对具有安全功能强度声明的安全机制(例如口令机制)进行安全功能强度分析。安全功能强度分析应证明安全机制达到了所声明的强度。

开发者应实施脆弱性分析,并提供脆弱性分布的文档。对所有已标识的脆弱性,文档应说明它们在所期望的交换机使用环境中不能被利用。文档还应说明如何确保用户能够得到最新的安全补丁。

6 第三级安全要求

6.1 安全功能要求

6.1.1 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。

6.1.2 身份鉴别

6.1.2.1 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。鉴别时除采用口令机制,还应有更加严格的身份鉴别,如采用智能 IC 卡、指纹等机制,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。

当进行鉴别时,交换机安全功能应仅将最少的反馈(如:打入的字符数,鉴别的成功或失败)提供给用户。

6.1.2.2 鉴别失败处理

在经过一定次数的鉴别失败以后,交换机应锁定该账号。最多失败次数仅由授权管理员设定。

6.1.2.3 超时锁定

应具有登录超时锁定功能。在设定的时间段内没有任何操作的情况下,终止会话,需要再次进行身份鉴别才能够重新操作。最大超时时间仅由授权管理员设定。

6.1.2.4 会话锁定

应允许管理员锁定自己的交互会话,锁定后需要再次进行身份鉴别才能够重新管理产品。

6.1.2.5 登录历史

应设计和实现交换机登录历史功能。为用户提供系统登录活动的有关信息,使用户识别入侵的企图。成功通过鉴别,登录系统后,交换机应向用户显示如下数据:

- 日期、时间、来源和上次成功登录系统的情况;
- 上次成功登录系统以来身份鉴别失败的情况;
- 口令距失效日期的天数。

6.1.3 安全管理

6.1.3.1 用户管理

应设置多个角色,具备划分管理员级别和规定相关权限(如监视、维护配置等)的能力,能够限定每个用户的管理范围和权限,防止非法用户和非法操作。

6.1.3.2 安全属性管理

应允许交换机管理员对安全功能行为进行控制管理,这些管理包括:

- a) 与对应的交换机自主访问控制、鉴别、数据完整性和安全保证技术相关的功能的管理。
- b) 与一般的安装和配置有关的功能的管理。交换机的安全配置参数要有初始值。交换机安装后,安全功能应能及时提醒管理员修改配置,并能周期性地提醒管理员维护配置。

6.1.4 审计

6.1.4.1 审计数据生成

交换机应具有审计功能,至少能够审计以下行为:

- 审计功能的启动和终止;
- 账户管理;
- 登录事件;
- 系统事件;
- 配置文件的修改。

应能为交换机的可审计行为生成审计记录,并在每一个审计记录中至少记录以下信息:

- 事件发生的日期和时间;
- 事件的类型;
- 管理员身份;
- 事件的结果(成功或失败)。

6.1.4.2 审计数据查阅

应提供给已授权的管理员从审计记录中读取审计信息的能力,为管理员提供的审计记录具有唯一、明确的定义和方便阅读的格式。

6.1.4.3 审计数据保护

应能保护已存储的审计记录,避免未经授权的删除,并能监测和防止对审计记录的修改。当审计存储耗尽、失败或受到攻击时,应确保最近的审计记录在一定的时间内不会被破坏。

当审计踪迹超过预定的限制值时,交换机安全功能应采取相应的行动,如:向授权管理员产生警告。

6.1.4.4 潜在侵害分析

交换机安全功能应能监控可审计行为,并指出潜在的侵害。

交换机安全功能在检测到可能有安全侵害发生时,应做出响应,如:通知管理员,向管理员提供一组遏制侵害的或采取矫正的行动。

6.1.5 划分虚拟局域网

交换机应具备划分虚拟局域网的功能,使得同一局域网内多台主机可以汇聚成一个用户组,从逻辑上可认为是在同一局域网内,而其他虚拟局域网与其在逻辑上分属在不同的局域网内。交换机应在帧结构中有对虚拟局域网的标识。

虚拟局域网可分为基于端口的划分,基于硬件 MAC 地址层,基于网络层(基于策略)。

虚拟局域网的应用应支持局域网内的局域网,支持共享访问(访问共同的接入点和服务器),支持虚拟局域网的交叠。

6.2 安全保证要求

6.2.1 配置管理

开发者应设计和实现交换机配置管理,要求如下:

- a) 开发者应使用配置管理系统,并提供配置管理文档,为产品的不同版本提供唯一的标识,且产品的每个版本应当使用其唯一标识作为标签;
- b) 配置管理范围至少应包括交换机的产品实现表示、设计文档、测试文档、用户文档、配置管理,从而确保它们的修改是在一个正确授权的可控方式下进行的。配置管理文档至少应能跟踪上述内容,并描述配置管理系统是如何跟踪这些配置项的;
- c) 部分的配置管理应实现自动化。

6.2.2 交付和运行

开发者应以文档形式提供对交换机安全地交付以及安装和启动的过程进行说明。文档中应包括:

- a) 对如何安全地将交换机交付给用户的说明;
- b) 对如何安全地安装和启动交换机的说明;
- c) 对如何检测交换机在分发过程中发生的未授权修改、如何检测攻击者伪装成开发者向用户交付交换机产品的说明。

以安全方式分发并交付产品后,仍应提供对交换机的长期维护和评估的支持,包括产品中的漏洞和现场问题的解决。

以安全方式分发并交付产品后,仍应不断向用户提供可能会影响到交换机安全的注意事项或警告信息。

6.2.3 开发

开发者应提供交换机功能规范,要求如下:

- a) 按非形式化功能设计的要求进行功能设计,以非形式方法描述安全功能与其外部接口,并描述使用外部安全功能接口的目的与方法。
- b) 提供交换机安全功能的高层设计。高层设计应按子系统描述安全功能及其结构,并标识安全功能子系统的所有接口。高层设计还应标识实现安全功能所要求的基础性的硬件、固件和软件。高层设计还应描述安全功能子系统所有接口及使用接口的目的和方法,并详细描述接口的返回结果、例外情况和错误信息等,以及如何将交换机中有助于增强安全策略的子系统分离出来。
- c) 开发者应提供交换机安全功能的低层设计。低层设计应以模块术语描述安全功能,并描述每一个模块的目的、接口和相互间的关系。低层设计还应描述如何将交换机中有助于增强安全策略的模块分离出来。
- d) 开发者应提供交换机安全功能的功能设计与高层设计之间的非形式化对应性分析,该分析应证明功能设计表示的所有相关安全功能都在高层设计中得到正确且完备的细化。
- e) 开发者应提供安全策略模型,并阐明该模型和交换机功能设计之间的对应性,这一对应性是一致和完备的。安全策略模型是非形式化的。该模型应描述所有可以模型化的安全策略的规则和特征,并阐明该模型对于所有可模型化的安全策略来说,是与其一致且完备的。

6.2.4 指导性文档

开发者应编制交换机的指导性文档,要求如下:

- a) 文档中应该提供关于交换机的安全功能与接口、交换机的管理和配置、交换机的启动和操作、安全属性、警告信息、审计工具的描述。
- b) 文档中不应包含任何一旦泄漏将会危及系统安全的信息,文档可以为硬拷贝、电子文档或联机文档。如果是联机文档,应控制对文档的访问。

6.2.5 生命周期支持

开发者应建立开发和维护交换机的生命周期模型,即用于开发和维护交换机的程序、工具和技术。要求如下:

- a) 开发者应按其定义的生命周期模型进行开发,并提供生命周期定义文档,在文档中描述用于开发和维护交换机安全功能的生命周期模型。
- b) 该模型对于交换机开发和维护应提供必要的控制,采用物理上、程序上、人员上以及其他方面的安全措施保护交换机开发环境的安全,包括场地的物理安全和对开发人员的选择,并采取适当的防护措施来消除或降低交换机开发所面临的安全威胁。
- c) 开发者应描述用于开发交换机的工具和参照标准,并提供关于已选择的开发工具选项的描述文档。开发工具文档应明确说明所有开发工具选项的含义。

6.2.6 测试

开发者应对交换机进行测试,要求如下:

- a) 应进行一般功能测试,保证交换机能够满足所有安全功能的要求。
- b) 应提供测试深度的分析。在深度分析中,应论证测试文档中所标识的对安全功能的测试足以表明该安全功能的运行与高层设计以及低层设计是一致的。
- c) 应进行相符性独立测试,由专业第三方独立实验室或消费者组织实施测试,确认交换机能够满足所有安全功能的要求。
- d) 应由专业第三方独立实验室或消费者组织抽样独立性测试。开发者应提供能有效重现开发者测试的必需资料,包括可由机器阅读的测试文档、测试程序等。
- e) 保留并提供测试文档,详细描述测试计划、测试过程以及预测结果和实际测试结果。

6.2.7 脆弱性评定

开发者应提供指导性文档和分析文档,在文档中确定对交换机的所有可能的操作方式(包括失败和操作失误后的操作)的后果以及对于保持安全操作的意义,并列出现所有目标环境的假设和所有的外部安全措施(包括外部程序的、物理的或人员控制)要求。所述内容应是完备、清晰、一致和合理的。

开发者应对具有安全功能强度声明的安全机制(例如口令机制)进行安全功能强度分析。安全功能强度分析应证明安全机制达到了所声明的强度。

开发者应实施脆弱性分析,并提供脆弱性分布的文档。对所有已标识的脆弱性,文档应说明它们在所期望的交换机使用环境中不能被利用。文档还应说明如何确保用户能够得到最新的安全补丁。

开发者应避免使用路由信息协议(RIP)等不安全的协议,脆弱性分析文档中应包含对所使用协议的脆弱性分析。

7 附加安全功能

7.1 网络访问控制功能

交换机上可采用多种用户接入的控制手段,如 PPP、Web 登录认证、ACL、802.1x 协议等,保护接入用户不受网络攻击,同时能够阻止接入用户攻击其他用户和网络。

7.2 虚拟专网功能

具有三层功能的交换机可实现 IPSec 和多协议标记交换协议(MPLS)两种虚拟专用网架构。

IPSec VPN 支持隧道和传输模式,确保数据通信的保密性和完整性。

MPLS VPN 使用标签交换,提供 QoS 机制和流量工程能力。MPLS 支持全网状 VPN 的建立,不同的 VPN 具有地址空间和路由独立性。

交换机支持 MPLS 和 IPSec 的结合,在进行数据加密和头部鉴权的同时能够提供良好的可管理性。

交换机使用的加密算法应通过国家密码管理部门的审批。

7.3 防火墙防护功能

交换机可加入防火墙功能模块,实现报文过滤功能,对所有接收和转发的报文进行过滤和检查。交换机还可提供基于报文内容的防护,当报文通过交换机时,防火墙功能模块可以对报文与指定的访问规则进行比较,决定是否直接丢弃报文。

7.4 入侵检测功能

交换机可内置 IDS 功能模块。具备完善的端口镜像和报文统计支持功能,能够检测并阻断非法攻击。



附 录 A
(资料性附录)
安全要求对照表

A.1 表 A.1 和表 A.2 分别给出了条款中安全功能要求和安全保证要求的对照表。

表 A.1 安全功能要求对照表

功能类别		第一级	第二级	第三级
自主访问控制		+	+	+
身份鉴别	管理员鉴别	+	+	++
	鉴别失败处理	+	+	+
	超时锁定		+	+
	会话锁定		+	+
	登录历史		+	+
数据保护				+
安全管理	权限管理	+	+	+
	安全属性管理	+	+	+
审计	审计数据生成		+	+
	审计数据查阅		+	+
	审计数据保护		+	+
	潜在侵害分析			+
划分虚拟局域网		+	++	+++

表 A.2 安全保证要求对照表(来自本标准安全保证部分)

功能类别	第一级	第二级	第三级
配置管理	+	++	+++
交付和运行	+	+	++
开发	+	++	+++
指导性文档	+	++	++
生命周期支持	+	++	+++
测试	+	++	+++
脆弱性评定		+	+

参 考 文 献

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

中华人民共和国公共安全
行业标准
信息安全技术 交换机安全技术要求
GA/T 684—2007

*

中国标准出版社出版发行
北京复兴门外三里河北街16号
邮政编码:100045

网址 www.spc.net.cn

电话:68523946 68517548

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230 1/16 印张 1.25 字数 26 千字
2007年7月第一版 2007年7月第一次印刷

*

书号: 155066·2-17904 定价 18.00 元

如有印装差错 由本社发行中心调换
版权专有 侵权必究
举报电话:(010)68533533



GA/T 684-2007