ICS 33 040 40
M 32

YD

中华人民共和国通信行业标准

YD/T 1627-2007

以太网交换机设备安全技术要求

Security requirements of ethernet switch eqiupment

2007-04-16 发布　　2007-10-01 实施

中华人民共和国信息产业部　发布

目　次

前　言

本标准是“以太网交换机设备”系列标准之一，本系列标准的结构和名称预计如下：

1. YD/T 1099-2005　以太网交换机技术要求（修订 YD/T 1099-2001 千兆比以太网交换机设备技术要求）
2. YD/T 1141-2005　以太网交换机测试方法（修订 YD/T 1141-2001 千兆比以太网交换机测试方法）
3. YD/T 1287-2003　具有路由功能的以太网交换机测试方法
4. YD/T 1255-2003　具有路由功能的以太网交换机技术要求
5. YD/T 1627-2007　以太网交换机设备安全技术要求
6. YD/T 1628-2007　以太网交换机设备安全测试方法
7. YD/T 1629-2007　具有路由功能的以太网交换机设备安全技术要求
8. YD/T 1630-2007　具有路由功能的以太网交换机设备安全测试方法

其中《以太网交换机设备安全测试方法》是本标准的配套标准，本标准同时也是 YD/T 1099-2005《以太网交换机技术要求》的配套标准。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：中兴通讯股份有限公司
华为技术有限公司
武汉邮电科学研究院
国家计算机网络应急技术处理协调中心
信息产业部电信研究院

本标准主要起草人：陈建业　罗　鉴　梁　冰　周开波

以太网交换机设备安全技术要求

1 范围

本标准规定了二层以太网交换机的安全技术要求。本标准主要从数据平面、控制平面和管理平面这三个平面对二层以太网交换机应该具备的安全功能做了详细规定。

本标准适于二层以太网交换机。

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 18336.2-2001　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

YD/T 1358-2005　路由器设备安全技术要求——中低端路由器（基于IPv4）

3 术语和定义

下列定义适用于本标准。

· **访问控制**（Access Control）

防止未经授权使用资源。

· **授权**（Authorization）

授予权限，包括根据访问权进行访问的权限。

· **密钥管理**（Key Management）

根据安全策略产生、分发、存储、使用、更换、销毁和恢复密钥。

· **安全审计**（Security Audit）

对系统的记录及活动独立的复查与检查，以便检测系统控制是否充分，确保系统控制与现行策略和操作程序保持一致、探测违背安全性的行为，并介绍控制、策略和程序中所显示的任何变化。

· **数字签名**（Digital Signature）

附在数据单元后面的数据或对数据单元进行密码变换得到的数据。允许数据的接收者证明数据的来源和完整性，保护数据不被伪造，并保证数据的不可否认性。

· **否认**（Repudiation）

参与通信的实体否认参加了全部或部分的通信过程。

· **可用性**（Availability）

根据需要，信息允许有权实体访问和使用的特性。

· **保密性**（Confidentiality）

信息对非授权个人、实体或进程是不可知、不可用的特性。

· **数据完整性**（Data Integrity）

数据免遭非法更改或破坏的特性。

- **安全服务**（Security Service）

由通信的系统提供的、对系统或数据传递提供充分的安全保障的一种服务。

- **安全策略**（Security Policy）

提供安全服务的一套规则。

- **安全机制**（Security Mechanism）

实现安全服务的过程。

- **拒绝服务**（Denial of Service）

阻止授权访问资源或延迟时间敏感操作。

- **防重放**（Anti-Replay）

防止对数据的重放攻击。

- **信息泄露**（Information Disclosure）

指信息被泄露或透漏给非授权的个人或实体。

- **完整性破坏**（Integrity Compromise）

数据的一致性通过对数据进行非授权的增加、修改、重排序或伪造而受到损害。

- **非法使用**（Illegal Use）

资源被非授权的实体或者授权的实体以非授权的方式或错误的方式使用。

4 缩略语

下列缩略语适用于本标准。

ACL	Access Control List	访问控制列表
ARP	Address Resolution Protocol	地址解析协议
CAR	Committed Access Rate	承诺接入速率
CHAP	Challenge-Handshake Authentication Protocol	质询握手认证协议
CoS	Class of Service	业务类别
DoS	Denial of Service	拒绝服务
FTP	File Transfer Protocol	文件传输协议
HTTP	HyperText Transport Protocol	超文本传输协议
ICMP	Internet Control Messages Protocol	因特网控制报文协议
IP	Internet Protocol	因特网协议
MAC	Media Access Control	媒介访问控制
NTP	Network Time Protocol	网络时间协议
PAP	Password Authentication Protocol	口令认证协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SNMPv1	SNMP version 1	SNMP 版本 1
SNMPv2c	SNMP version 2c	SNMP 版本 2c
SNMPv3	SNMP version 3	SNMP 版本 3
SSH	Secure Shell	安全外壳
SSHv1	Secure Shell version 1	SSH 版本 1

SSHv2	Secure Shell version 2	SSH 版本 2
TCP	Transmission Control Protocol	传输控制协议
TFTP	Trivial File Transfer Protocol	简单文件传输协议
ToS	Type of Service	服务类型
VLAN	Virtual Local Area Network	虚拟局域网

5 概述

以太网交换机可放置在网络的边缘层，作为用户接入网络的设备。

以太网交换机在逻辑上可以划分为三个功能平面：

- 数据平面。主要指为用户访问和利用网络而提供的功能，如数据转发等。
- 控制平面。也可以称为信令平面，主要包括控制转发路径等有关的功能。
- 管理平面。主要指与 OAM&P 有关的功能，如 SNMP、管理用户 Telnet 登录、日志等，支持 FCAPS（Fault、Capacity、Administration、Provisioning and Security）功能。管理平面消息的传送方式有带内和带外两种。

为了抵御网络攻击，以太网交换机应提供一定的安全功能。本标准参考 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》中定义的安全功能并应用到以太网交换机中，这些安全功能包括：

- 鉴别和认证。确认用户的身份及其真实性。
- 用户数据保护。与保护用户数据相关的安全功能和安全策略。
- 系统功能保护。安全数据（完成安全功能所需要的数据，如用户身份和口令）的保护能力。
- 资源分配。对用户对资源的使用进行控制，不允许用户过量占用资源以免造成拒绝服务。
- 安全审计。能够提供日志等审计记录，这些记录可以用来分析安全威胁活动和对策。
- 安全管理。安全功能、数据和安全属性的管理能力。
- 可信信道/路径。以太网交换机之间以及以太网交换机同其他设备之间通信的信道/路径要求可信，对于传送敏感数据的通信要同传送其他数据的通信隔离开来。
- 系统访问。本安全功能要求控制用户会话的建立。

以太网交换机设备安全框架如图 1 所示。

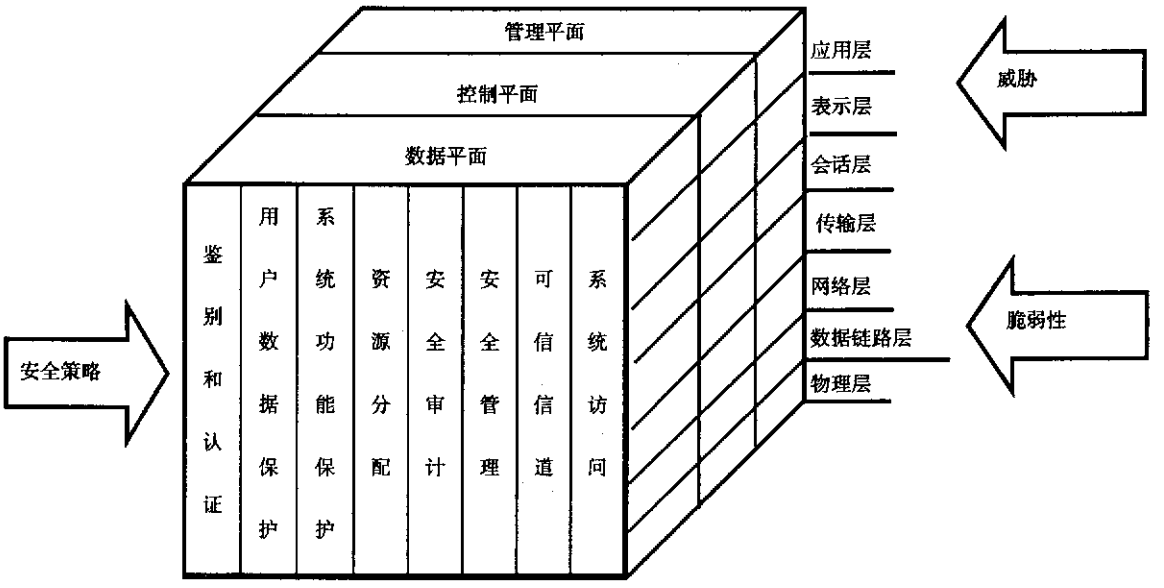

图 1 以太网交换机设备安全框架

硬件系统和操作系统是以太网交换机本身安全的重要因素，对硬件系统和操作系统的要求参见 YD/T 1358-2005《路由器设备安全技术要求——中低端路由器（基于 IPv4）》附录 A。

6 数据平面安全

6.1 安全威胁

数据平面的安全威胁主要来自以下方面，但并不局限于这些方面：

- 对数据流进行流量分析，从而获得敏感信息。
- 未授权观察、修改、插入、删除数据流。
- 拒绝服务攻击，降低设备的转发性能。

6.2 安全功能

6.2.1 鉴别和认证

以太网交换机需要对接入网络的数据源进行检查和确认（包括源 MAC、源端口），保证报文来自可信/合法的用户或设备。

6.2.2 用户数据保护

以太网交换机应支持 802.3ad 链路聚合功能的提供网络冗余以及高带宽的要求。IEEE 802.3ad 的链路聚合技术，可以将多个百兆位、千兆位或万兆位以太网端口结合成一条干线，在多个端口之间进行负载平衡，同时完成链路失效保护。

6.2.3 系统功能保护

对于用户的安全数据，系统要提供妥善的保护手段，包括对访问安全数据的用户进行标识和鉴别。

6.2.4 资源分配

常见的流量攻击是通过大量的某种流量实施的，对该种流量进行控制，限制其进入网络的容量，可以缓解这种攻击，以太网交换机应在其端口上全双工支持 802.3x，半双工可选支持背压流控、CAR、ACL 和 COS。以太网交换机宜支持数据包标记功能，可以完成对 802.1p 的重标记。

以太网交换机应支持每端口或每 VLAN 对 MAC 地址学习数目可限定的功能，避免单端口失效影响设备整体功能。以太网交换机可根据实际情况选择静态配置或采用动态调整的方式实现。

6.2.5 安全审计

对于用户流量，以太网交换机宜提供流量日志能力，提供对异常用户流量的安全审计，相关的日志与告警要求参见 8.2.5 节有关规定。

6.2.6 安全管理

要能够提供对本章提供的安全功能和数据的管理能力，管理方式包括但不限于控制台、远程连接或网络管理接口/系统等方式。

6.2.7 可信信道/路径

以太网交换机间以及以太网交换机同其他设备间通信的信道/路径要求可信，对于传送敏感数据的通信要同传送其他数据的通信隔离开来。

VLAN 能够将 VLAN 内的用户数据同 VLAN 外部或其他 VLAN 的数据隔离开来，能够提供可信的通信信道/路径，对 VLAN 功能的要求参见 6.2.8.3 节。

6.2.8 系统访问

6.2.8.1 过滤功能

以太网交换机应支持广播风暴的抑制功能。

以太网交换机宜支持对未知组播和未知单播报文的抑制功能。

6.2.8.2 访问控制列表

访问控制列表是基于报文的内容，如 MAC 地址、端口等，指定的安全规则表，以太网交换机通过对每个进出交换机的报文进行规则匹配，确定对报文的处理动作。

宜实现基于源 MAC 地址的访问控制列表。可选支持基于源 IP、源端口、目的 IP、目的端口的访问控制列表。

6.2.8.3 二层隔离功能

VLAN 利用公共网络的资源，建立虚拟的专用网络，利用 VLAN 可以实现不同专用网络用户流量的隔离。

VLAN 的功能要求如下：

- 应支持通过 VLAN 技术实现 VPN，应支持基于端口或 MAC 地址的 VLAN。
- 应支持同一 VLAN 内不同端口间的隔离功能。
- 缺省情况下将所有端口都配置在系统缺省的 VLAN 中。
- 宜支持 VLAN 堆栈功能。

6.2.8.4 端口镜像功能

以太网交换机应支持报文镜像功能，包括一对一、多对一镜像。使用该功能，可以将交换机的流量拷贝以用于进行详细的分析。

6.2.8.5 基于 802.1x 的访问控制

以太网交换机应支持基于 802.1x 的访问控制。802.1x 是一种基于端口的认证协议，是一种对用户进行认证的方法和策略。IEEE 802.1x 可以实现动态的、基于端口的安全，提供用户身份验证功能。

以太网交换机应支持基于用户 MAC 地址 802.1x 的认证，从而满足一个端口下多用户认证需求。可选支持交换机作为认证 Server，提供对远端认证的备份。应支持交换机与 RADIUS 下发安全策略，802.1x 认证条件下用户账号绑定 IP、MAC、交换机端口等，可以真正提高 MAC 地址效率、极大减少网管工作量和强化端点准入安全。

802.1x 应支持 CHAP，可选支持 EAP MD5、EAP-TLS、PEAP、PAP。

以太网交换机可选支持 TACACS+协议。

6.2.8.6 MAC 地址绑定功能

以太网交换机应支持 MAC 地址绑定功能，可以对端口、VLAN、MAC 地址进行静态绑定。以太网交换机宜支持通过 802.1x 认证等手段自动绑定 MAC 地址的功能，提高 MAC 地址的绑定效率，减少网管的工作量。

7 控制平面安全

7.1 安全威胁

对控制平面的安全威胁主要来自以下几个方面，但并不局限于这些方面：

- 对协议流进行探测或者流量分析，从而获得转发路径信息。
- 获得设备服务的控制权，暴露转发路径信息，包括将转发路径信息暴露给非授权设备，一个 VPN 转发路径信息暴露给另一个 VPN 等。

- 非法设备进行身份哄骗。

7.2 安全功能

7.2.1 系统功能保护

安全数据应要得到妥善的保护。

7.2.2 安全审计

对控制平面的信息要提供日志记录功能，特别是对设备的 MAC 表等重要数据有影响的控制数据，关于日志可以参见 8.2.5 节。

7.2.3 安全管理

以太网交换机涉及的口令长度不宜少于 8 个字符，并且应由数字、字符或特殊符号组成，以太网交换机宜提供检查机制，保证每个口令至少是由前述的三类符号中的两类组成。以太网交换机宜支持历史口令检查、口令最长使用时间设置、提醒用户定期更改口令。

7.2.4 可信信道/路径

以太网交换机之间以及以太网交换机同其他设备之间的控制信息通信的信道/路径要求可信，对于传送敏感数据的通信要同传送其他数据的通信隔离开来。

7.2.5 系统访问

7.2.5.1 STP 攻击防护

以太网交换机应支持对 STP 攻击的防护功能。

以太网交换机应支持快速生成树协议，在网络故障时能够快速收敛。

以太网交换机应支持对生成树协议的关闭功能。

以太网交换机应支持 BPDU Guard 功能。

以太网交换机应支持 Root Guard 功能。

7.2.5.2 IGMP Snooping

以太网交换机宜支持 IGMP 监听功能。监听主机发出的 IGMP 成员报告消息，并记录下来形成组成员和接口的对应关系，以防止组播报文的扩散。

以太网交换机宜支持 IGMP 响应报文的过滤、抑制功能。

以太网交换机宜支持对 IGMP 加入组范围进行限制。

7.2.5.3 DHCP Snooping

以太网交换机宜支持 DHCP 监听功能，记录 DHCP 服务器的地址。

7.2.5.4 CPU 保护

以太网交换机宜支持对CPU的保护功能，包括对到达CPU的流量进行控制和对CPU的运行状态进行监控。

8 管理平面安全

8.1 安全威胁

管理平面的安全威胁主要来自以下方面，但并不局限于这些方面：

- 对数据流进行流量分析，从而获得设备有关的系统配置信息；
- 未授权观察、修改、插入、删除数据流；
- 未授权地访问管理接口，控制整个设备；

- 利用管理信息流实施拒绝服务攻击；
- 利用协议流实施的拒绝服务攻击，如利用 ICMP 协议的 Smurf 攻击、利用面向连接协议的半连接攻击等。

8.2 安全功能

8.2.1 鉴别和认证

对设备的管理用户都需要鉴别和认证，鉴别和认证是系统访问的基础，对有关 SNMP 管理、Web 管理、远程登录管理中用户认证的要求参见 8.2.8 节。

8.2.2 用户数据保护

对于以太网交换机，一般使用以下远程管理方式：

- SNMP。SNMP 是一种应用非常广泛的网络管理协议，主要用于设备的监控和配置的更改等，目前使用的 SNMP 协议有三个版本，分别是 SNMPv1、SNMPv2c 和 SNMPv3。以太网交换机应支持安全性较好的 SNMPv3 作为网管协议。此外，具有路由功能的以太网交换机宜实现对设备的访问控制，可通过指定 IP 地址的方式，限定可对设备进行访问的用户范围。
- 远程登录。宜支持 SSHv1 或 SSHv2，通过认证算法和加密算法实现对管理用户数据的保密性和完整性保护。
- Web 管理。可通过支持 SSL/TLS 安全协议，实现对管理用户数据的完整性保护。

有关这三种远程管理方式的详细要求参见 8.2.8.1、8.2.8.4、8.2.8.5 等节。

8.2.3 系统功能保护

与管理相关的安全数据应得到妥善的保护。

8.2.4 资源分配

管理数据是系统运行的重要数据，系统要保证管理系统获得足够的运行资源，但是不能因此显著影响控制平面和数据平面的正常工作。此外，通过管理平面提供的设备补丁下载功能应该得到严格的管理，不应该被用来对设备资源实施恶意占用。

8.2.5 安全审计

日志应记录配置修改等安全相关事件、告警记录发生的安全违章事件，并可以一定的方式提示管理员；审计可对记录的安全事件进行回顾和检查，分析和报告安全信息；管理员基于该信息了解安全策略的执行情况，并据此进行修改。安全日志、安全告警等安全记录往往是安全审计的素材。

对日志的要求：

- 每个安全日志条目应包含事件的主体、发生时间和事件描述等；
- 应可以保存在本地系统的缓存区内，也可以发送到专用的日志主机上做进一步处理；
- 应定义日志的严重程度级别，并能够根据严重程度级别过滤输出；
- 应支持和日志主机之间的接口。

对告警的要求：

- 应支持告警输出到打印机或显示终端，可根据严重程度级别输出到不同的显示终端；
- 告警应保存在本地或通过网络存储到其他主机；
- 在设备出现异常时宜使用 SNMP TRAP 方式发出必要的告警。

8.2.6 安全管理

8.2.6.1 分级网管

以太网交换机应支持分级网管功能。

8.2.6.2 口令管理

有关口令管理的要求参见 7.2.3 节。

8.2.7 可信信道/路径

对于带内管理面临的潜在的安全问题，以太网交换机可通过如独立的管理端口、VPN 虚接口等方式支持专用的管理网络，将管理通信流和其他通信流量隔离。以太网交换机可提供关闭带内接口的能力，以实现只通过专用管理网络管理设备。

8.2.8 系统访问

8.2.8.1 SNMP 的安全性

SNMP 是一种应用非常广泛的网络管理协议，主要用于设备的监控和配置的更改等，目前使用的 SNMP 协议有三个版本，分别是 SNMPv1、SNMPv2c 和 SNMPv3。以太网交换机应支持安全性较好的 SNMPv3 作为网管协议。

此外，以太网交换机宜实现对网管站的访问控制，限定用户通过指定 IP 地址使用 SNMP 对设备进行访问。

8.2.8.2 Telnet 访问

Telnet 协议用于通过网络对设备进行远程登录。在以太网交换机中，如果对用户提供 Telnet 服务，则宜满足下列约定：

- 用户应提供用户名/口令才能进行后续的操作，用户地址和操作应记入日志；
- 应限制同时访问的用户数目；
- 在设定的时间内不进行交互，用户应自动被注销；
- 可限定用户通过指定 IP 地址使用 Telnet 服务对设备进行访问；
- 必要时可关闭 Telnet 服务。

8.2.8.3 串口访问

以太网交换机如果支持串口访问功能，应提供同 8.2.8.2 节相同的安全保护能力。

8.2.8.4 SSH 访问（可选支持）

SSH 是在不安全的网络上为远程登录会话和其他网络服务提供安全性的一种协议，对 SSH 服务的要求如下：

- 宜支持 SSHv1 或 SSHv2 两种版本。
- 用户应通过身份认证才能进行后续的操作，用户地址和操作记入日志。以太网交换机应支持口令认证，宜支持公钥认证，宜实现基于主机认证。
- SSH 服务器宜采用认证超时机制，在超时范围内没有通过认证应断开连接，宜限制客户端在一个会话上认证尝试的次数。
- SSHv2 应支持用于会话的加密密钥和认证密钥的动态管理，宜支持基于 diffie-hellman-group1-sha1 的 Diffie-Hellman，其中宜支持 Oakley 组 2（1024bit MODP Group，RFC2409）、Oakley 组 14（2048bit MODP Group，RFC3526）、组协商的密钥交换，在密钥交换过程中协商密钥交换算法、对称加密算法和认证算

法等，并对服务器端进行主机认证。

- 应支持HMAC-SHA1认证算法，宜支持HMAC-SHA1-96认证算法，可实现HMAC-MD5、HMAC-MD5-96等认证算法。
- 应支持3DES-CBC对称加密算法，可实现Blowfish-CBC、IDEA-CBC、CAST128-CBC、AES256-CBC、AES128-CBC等对称加密算法。
- 对于非对称加密算法，可选支持SSH-DSS或实现SSH-RSA。
- 可限定用户通过指定IP地址使用SSH服务对设备进行访问。
- 应支持必要时关闭SSH服务。

8.2.8.5 Web管理

Web管理基于HTTP协议，以太网交换机宜支持Web管理，宜满足下列约定：

- 用户应提供用户名/口令才能进行后续的操作，用户地址和操作应记入日志；
- 可限定用户通过指定IP地址使用HTTP对设备进行访问；
- 必要时可关闭HTTP服务；
- 应支持SSL/TLS。

8.2.8.6 软件升级

以太网交换机一般使用FTP/TFTP协议实现设备的软件升级，软件升级包括软件版本、设备配置等，有本地和远程两种途径。软件升级通过建立FTP服务器和客户端的连接来实现，FTP协议应支持口令认证功能。

对于远程软件升级，宜支持SSH，实现文件的安全传送。升级方式也可选采用HTTPS协议实现。