ICS 33 040 40
M 32

YD

中华人民共和国通信行业标准

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

Technical Requirements for Ethernet Switching Derices Security with Routing Capability

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。本系列标准预计的结构和名称如下：

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规范）
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 1255-2003　具有路由功能的以太网交换机技术要求
4. YD/T 1287-2003　具有路由功能的以太网交换机测试方法
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，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》是本标准的配套标准，本标准同时也是 YD/T 1255-2003《具有路由功能的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

具有路由功能的以太网交换机设备安全技术要求

1 范围

本标准规定了支持 IPv4 协议的具有路由功能的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具有路由功能的以太网交换机应该具备的安全功能做了详细规定。

本标准适用于支持 IPv4 协议的具有路由功能的以太网交换机。

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 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（damage））

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。

3DES	triple Data Encryption Standard	三重数据加密标准
ACL	Access Control List	访问控制列表
AES	Advanced Encryption Standard	先进加密标准
ARP	Address Resolution Protocol	地址解析协议
BGP	Border Gateway Protocol	边界网关协议
BGP-4	Border Gateway Protocol version 4	边界网关协议版本 4
CAR	Committed Access Rate	承诺接入速率
CBC	Cipher Block Chaining	密码块链
CHAP	Challenge-Handshake Authentication Protocol	质询握手认证协议
CoS	Class of Service	业务类别
CR-LDP	Constraint-based Routing Label Ditribution Protocol	基于约束路由的标记分发协议
DNS	Domain Name Service	域名服务
DoS	Denial of Service	拒绝服务
DSS	Digital Signature Stardard	数字签名标准
EGP	Exterior Gateway Protocol	外部网关协议
FTP	File Transfer Protocol	文件传输协议
HMAC	Hashed Message Authentication Code	散列消息认证码
HTTP	HyperText Transport Protocol	超文本传输协议

ICMP	Internet Control Messages Protocol	因特网报文控制协议
IDEA	International Data Encryption Algorithm	国际数据加密算法
IGP	Interior Gateway Protocol	内部网关协议
IKE	Internet Key Exchange	因特网密钥交换
IP	Internet Protocol	因特网协议
IPFIX	IP Flow Information Export	IP 流信息输出
IPSec	Internet Protocol Security	因特网协议安全
IS-IS	Intermediate System to Intermediate System	中间系统到中间系统协议
L2TP	Layer 2 Tunneling Protocol	二层隧道协议
LAC	L2TP Access Concentrator	L2TP 接入集中器
LDP	Label Distribution Protocol	标记分发协议
LNS	L2TP Network Server L2TP	网络服务器
LSP	Label Switched Path	标记交换路径
LSR	Label Switch Router	标记交换路由器
MAC	Media Access Control	媒介访问控制
MD5	Message Digest version 5	消息摘要版本 5
MODP	Modular exPonentiation group	模求幂组
MPLS	Multi-Protocol Label Switching	多协议标记交换
NAT	Network Address Translation	网络地址转换
NAPT	Network Address Port Translation	网络地址端口转换
NTP	Network Time Protocol	网络时间协议
OSPF	Open Shortest Path First	开放最短路径优先协议
PAP	Password Authentication Protocol	口令认证协议
PFS	Perfect Forward Secrecy	完美前向保密
RIP	Routing Information Protocol	路由信息协议
RIPv2	Routing Information Protocol version 2	路由信息协议版本 2
RSVP	Resource Reservation Protocol	资源预留协议
RSVP-TE	RSVP Traffic Engineering	RSVP 流量工程
RSA	Rivest，Shamir and Adleman Algorithm	RSA 算法
SHA	Secure Hash Algorithm	安全散列算法
SHA-1	Secure Hash Algorithm 1	安全散列算法版本 1
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
SSL	Secure Socket Layer	安全套接层
TCP	Transmission Control Protocol	传输控制协议
TFTP	Trivial File Transfer Protocol	简单文件传输协议
TLS	Transport Layer Security	传输层安全
ToS	Type of Service	服务类型
UDP	User Datagram Protocol	用户数据报协议
URPF	Unicase Reverse Path Forwarding	单播反向路径转发
VLAN	Virtual Local Area Network	虚拟局域网
VPN	Virtual Private Network	虚拟专用网
VRF	VPN Routing and Forwarding	VPN 路由和转发

5 概述

具有路由功能的以太网交换机可放置在网络的各个层次，可作为接入用户的网络设备，作为汇聚业务的网络设备或作为网络的核心交换设备。

具有路由功能的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，主要包括路由协议、ICMP 协议等与建立会话连接、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，具有路由功能的以太网交换机应提供一定的安全功能，如图 1 所示。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具有路由功能的以太网交换机中，这些安全功能包括：

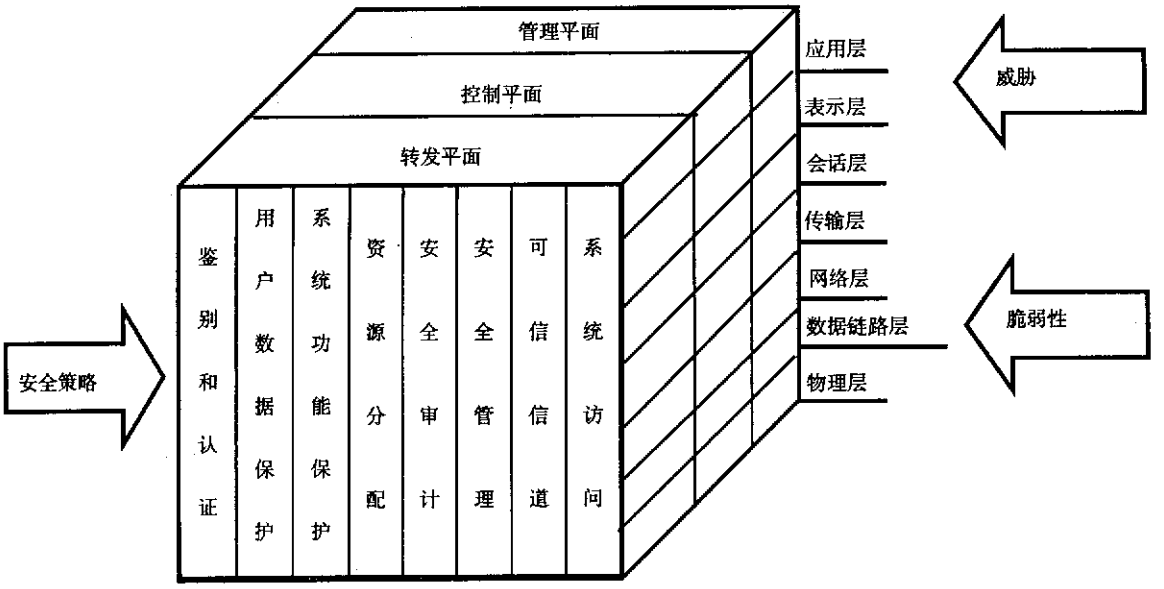

图 1 具有路由功能的以太网交换机设备安全框架

—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造成的拒绝服务；

—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，具有路由功能的以太网交换机之间以及具有路由功能的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；

—系统访问，本安全功能要求控制用户会话的建立。

硬件系统和操作系统是具有路由功能的以太网交换机本身的安全的重要因素，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

对数据平面的安全威胁主要有以下方面，但并不局限于这些方面：

- 对数据流的流量分析，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

具有路由功能的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 IP、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

6.2.2.1 IPSec 功能

IPSec 在 IP 层上提供数据保密性、数据源认证、数据完整性和抗重放等安全服务，由 AH、ESP 和 IKE 等协议组成。

具有路由功能的以太网交换机，可选支持 IPSec 协议，对 IPSec 的特性要求如下：

- 应支持手工密钥管理和 IKE 自动密钥管理；
- 应支持 AH 和 ESP 协议，对于这两种协议，应支持隧道和传送两种封装模式，宜支持 AH 和 ESP 协议的嵌套封装；
- AH 和 ESP 协议应支持 HMAC-MD5-96 和 HMAC-SHA1-96 认证算法，ESP 协议应支持国家相关部门规定的加密算法以及 DES-CBC、3DES-CBC 和 AES 等加密算法，应支持空加密算法和空认证算法，但二者不应同时使用。

对 IKE 的特性要求如下：

- 第一阶段应支持主模式和野蛮模式；
- 第二阶段应支持快速模式；
- 应支持情报模式（New Group Mode）；
- 应支持预共享密钥认证方式，宜实现 RSA 加密 nonce 验证和数字证书认证方式；

- 应支持 HMAC-MD5-96 和 HMAC-SHA1-96 认证算法，支持 MD5 和 SHA1 散列算法，应支持国家相关部门规定的加密算法以及 DES-CBC、3DES-CBC 和 AES 等加密算法；
- 密钥交换应支持 MODP-Group1、MODP-Group2 等 Diffie-Hellman 组；
- 对于快速模式，支持 PFS。

6.2.2.2 802.3ad 链路聚合功能

具有路由功能的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，可以将多个百兆或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，具有路由功能的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。

具有路由功能的以太网交换机宜支持数据包标记功能（RFC 2697，RFC 2698），具有路由功能的以太网交换机可以完成对 TOS/DSCP/COS 的重新标记。

具有路由功能的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，避免单端口失效引起设备整体功能。

6.2.5 安全审计

对于用户流量，具有路由功能的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 8.2.4 节的有关规定。

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

具有路由功能的以太网交换机间以及具有路由功能的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。

VPN 能够将 VPN 内的用户数据同 VPN 外部或其他 VPN 的数据隔离开，能够提供可信的通信信道/路径，对 VPN 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

具有路由功能的以太网交换机可选支持 RFC 1858 和 RFC 3128 规定的 IP 分片包过滤以及 RFC 2827 和 RFC 3704 规定的 Ingress 包过滤器。

具有路由功能的以太网交换机应支持广播风暴的抑止功能。

具有路由功能的以太网交换机宜支持对未知组播和未知单播报文的抑止功能。

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、IP 地址、协议和端口等，指定的安全规则表，具

有路由功能的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。

应支持基于源地址、目的地址、协议类型、源端口号、目的端口号的访问控制列表，宜支持基于 IP 头部的 ToS 域的访问控制列表以及在指定时间有效的访问控制列表，可根据配置对指定的报文匹配情况进行统计和产生日志等。具有路由功能的以太网交换机宜支持不低于 1000 访问规则，性能不受 ACL 规则数影响。

6.2.8.3 VPN 功能

VPN 利用公共网络的资源，建立虚拟的专用网络，利用 VPN 可以实现不同专用网络用户流量的隔离。具有路由功能的以太网交换机支持利用以下技术实现 VPN：

- VLAN

应支持通过 VLAN 技术实现 VPN，应支持基于端口，宜支持基于 MAC 地址或基于协议的 VLAN 或基于子网的 VLAN。

应支持同一 VLAN 内不同端口间的隔离功能。

宜支持 VLAN 堆栈功能。

缺省情况下将所有端口都配置在系统缺省的 VLAN 中。

- L2TP 隧道（可选支持）

应支持通过 L2TP 隧道技术实现 VPN，应支持 LAC 和 LNS 功能，支持 CHAP 鉴别协议。

- IPSec 隧道（可选支持）

可选支持通过 IPSec 隧道技术实现 VPN，对 IPSec 的要求见 6.2.2.1 节。

- MPLS LSP（可选支持）

可选支持基于 MPLS LSP 实现的 MPLS VPN，对 MPLS VPN 的要求如下：

1）不管是 L2 VPN 还是 L3 VPN，数据应严格基于标签沿着 LSP 转发，除非需要，一个 VPN 的数据不应被发送到该 VPN 之外，一个 VPN 的数据不应进入到另一个 VPN；

2）当同时支持 VPN 服务和因特网服务时，特别是在同一个物理接口上通过不同的逻辑接口支持 VPN 服务和因特网服务时，可基于逻辑接口对接入速率进行限制。

6.2.8.4 NAT

NAT 的初衷是为了解决 IP 地址资源匮乏的问题，但 NAT 可以实现内网和外网的隔离，内网可以正常地访问外网，同时可以隐藏内网的编址方案和网络结构，保证了内网的安全。

对 NAT 功能的特性的要求如下：

- 宜支持 NAPT；
- 宜支持 HTTP、FTP、DNS、H.323 等应用协议；
- 宜支持输出 NAT 日志记录。

6.2.8.5 防火墙功能

具有路由功能的以太网交换机宜支持防火墙功能，除包过滤、访问控制列表、NAT 外，可选支持应用代理功能，只允许被保护的网络访问允许的网络应用。

状态检测不仅检查网络层和传输层信息，还检查应用层协议的信息，实时维护这些 TCP 或 UDP 的状态信息，使用这些状态信息，确定访问控制，具有路由功能的以太网交换机可选支持基于状态检测的包

过滤功能。

6.2.8.6 端口镜像功能

具有路由功能的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。

6.2.8.7 基于 802.1x 的访问控制

具有路由功能的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。

具有路由功能的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，真正提高 MAC 地址效率，极大减少网管工作量，极大强化端点准入安全。

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

具有路由功能的以太网交换机可选支持 TACACS+协议。

6.2.8.8 MAC 地址绑定功能

具有路由功能的以太网交换机应支持 MAC 地址绑定功能，可以对端口、VLAN、IP 地址、MAC 地址进行静态绑定。具有路由功能的以太网交换机宜通过 DHCP SNOOPING 等手段提供自动绑定动态 ARP 条目的功能，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有以下几个方面，但并不局限于这些方面：

- 对协议流进行探测或者进行流量分析，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；
- 利用协议流实施的拒绝服务攻击，如利用 ICMP 协议的 Smurf 攻击，利用路由协议的拒绝服务攻击，利用面向连接协议的半连接攻击等；
- 非法设备进行身份哄骗，建立路由协议的信任关系，非法获得转发路径信息；
- 针对路由协议转发路径信息的欺骗。

7.2 安全功能

7.2.1 鉴别和认证

路由的安全是交换机执行正常功能的重要基础。动态路由协议可以分为 IGP 和 EGP 两类，对于具有路由功能的以太网交换机，目前广泛采用的 IGP 有 RIP、OSPF 和 IS-IS 协议，EGP 主要是 BGP 协议，具有路由功能的以太网交换机可选支持一种 IGP，可选支持 BGP 协议。其中：

- RIPv2、OSPFv2 应支持明文认证和 MD5 认证；
- IS-IS 应支持明文认证和 MD5 认证；
- BGP-4 应支持 MD5 认证。

对于 MPLS（可选支持），用于建立 LSP 的标记分配协议主要有 LDP/CR-LDP 和 RSVP-TE 两种：

- LDP/CR-LDP

发现交换过程使用的消息由 UDP 协议承载，对于基本 Hello 消息，具有路由功能的以太网交换机应只接受与可信 LSR 直接相连的接口上的基本 Hello 消息，忽略地址不是到该子网组播组的所有交换机的基本 Hello 消息；对于扩展 Hello 消息，可利用访问列表控制只接受允许的源发送来的扩展 Hello 消息。LDP 会话过程使用的消息由 TCP 协议承载，应通过 TCP MD5 签名选项对会话消息进行真实性和完整性认证。

- RSVP-TE（可选支持）

应通过加密的散列算法支持实体的认证，从而实现逐跳的认证机制，应支持 HMAC-MD5 算法和 HMAC-SHA1 算法。

7.2.2 用户数据保护

7.2.2.1 采用最长前缀匹配路由查找方式

具有路由功能的以太网交换机应采用最长前缀匹配路由查找方式。

7.2.2.2 路由认证

路由认证往往使用加密散列算法，在提供数据源认证的同时，也提供了数据完整性认证，路由认证功能参见 7.2.1 节。

7.2.3 资源分配

7.2.3.1 抗常见网络攻击

7.2.3.1.1 URPF

URPF 是通过在转发表中查找收到分组的源 IP 地址和接口，只转发源 IP 地址在 IP 路由表中存在的分组的一种技术，这种技术可以缓解基于 IP 地址哄骗的网络攻击，具有路由功能的以太网交换机宜支持 URPF 功能。

7.2.3.1.2 禁止定向广播报文转发

Smurf 攻击是一种利用定向广播报文实施的 DoS 攻击，具有路由功能的以太网交换机宜在端口上禁止定向广播报文转发。

7.2.3.2 可关闭一些 IP 服务

7.2.3.2.1 ICMP 协议（可选）

ICMP用于网络操作和排障，具有路由功能的以太网交换机需要实现ICMP协议的一些功能，但设备应具有关闭这些功能的能力。这些ICMP消息类型包括：

- Type = 0　回显应答
- Type = 3　目的地不可达
- Type = 5　重定向
- Type = 8　回显请求
- Type = 11　超时

7.2.3.2.2 代理 ARP

代理 ARP 是一台主机（常常是交换机）代替另一台主机应答 ARP 请求，该主机负责将分组转发到最终目的地的一种技术，代理 ARP 能够帮助一个子网的主机不用配置路由或默认网关到达远端子网。具

有路由功能的以太网交换机如果支持该功能，应具有关闭代理 ARP 的能力。

对于 ARP 代理应支持安全代理功能，可选配置只对某些地址响应 ARP 请求。

7.2.3.2.3 IP 源路由选项（可选）

IP 源路由选项取消了报文传输路径中的各个设备的中间转发过程，而不管转发接口的工作状态，可能被恶意攻击者利用，刺探网络结构。具有路由功能的以太网交换机如果支持该功能，应提供关闭 IP 源路由选项功能能力。

7.2.3.2.4 其他服务

对于下列 TCP 和 UDP 小端口服务，应缺省关闭这些服务或者不提供这些服务：

- Echo
- Chargen
- Finger
- NTP

7.2.3.3 MPLS VPN

可选实现 MPLS VPN 使用的交换机资源（如 CPU、内存等）的相互隔离，防止因一个 VPN 独占资源而造成的对于其他 VPN 的 DoS 攻击。

7.2.4 安全审计

对控制平面的信息要提供日志记录功能，特别是对设备的路由表等重要数据有影响的控制数据，关于日志可以参见 8.2.4 节。

7.2.5 安全管理

具有路由功能的以太网交换机涉及的口令长度宜不少于 8 个字符，并且应由数字、字符或特殊符号组成，具有路由功能的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。具有路由功能的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。

7.2.6 可信信道/路径

具有路由功能的以太网交换机之间以及具有路由功能的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。

7.2.7 系统访问

7.2.7.1 STP 攻击防护

具有路由功能的以太网交换机应支持对 STP 攻击的防护功能。

具有路由功能的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。

具有路由功能的以太网交换机应支持对生成树协议的关闭功能。

具有路由功能的以太网交换机应支持 BPDU Guard 功能。

具有路由功能的以太网交换机应支持 Root Guard 功能。

7.2.7.2 路由过滤

路由过滤可以控制路由协议对路由信息的发布和接受，可以只发布某些指定的路由，也可以只接收符合某些条件的路由，这样可以在满足需要的前提下减少交换机的资源消耗，达到更好的性能，避免路由攻击。在接收和发布路由信息时，所有路由协议应支持按 IP 地址前缀信息进行过滤，针对 BGP 路由应

支持根据自治系统路径、团体属性进行过滤。

7.2.7.3 可选支持 MPLS VPN

7.2.7.3.1 L2 VPN

- VPN 之间 MAC 地址和 VLAN 信息应相互隔离，VPN 之间或 VPN 和 MPLS 骨干之间应可以复用 MAC 地址空间和 VLAN 空间。
- 当没有 VPN 互通的要求时，VPN 之间或 VPN 和 MPLS 骨干之间的数据流应相互隔离。

7.2.7.3.2 L3 VPN

常用的 L3 VPN 技术是 BGP/MPLS VPN，BGP/MPLS VPN 实质上是通过 BGP 协议约束路由信息分配的 MPLS，对 L3 VPN 要求如下：

- 应支持静态路由算法和动态路由算法。对于动态路由算法，宜具有在接口上过滤路由更新的能力，IGP 和 EGP 路由协议都应支持 MD5 认证，并可基于 VRF 实例限制路由更新的速度。
- VPN 之间的拓扑和编址信息应相互隔离，一个 VPN 应可以使用所有因特网地址范围，包括 RFC 1918 定义的私有地址范围，VPN 之间或 VPN 和 MPLS 骨干之间应可以复用 IP 地址空间。
- 应为每个 VPN 维持一个独立的 VRF 实例，除非需要，VPN 之间或 VPN 和 MPLS 骨干之间的路由信息及其分发和处理应相互独立，互不干扰。

7.2.7.4 防火墙功能

宜支持对 TCP 连接的攻击防护功能。

宜支持 RFC 3882 描述的 BGP 抵御 DDoS 攻击的能力。

7.2.8 IGMP Snooping

具有路由功能的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。

具有路由功能的以太网交换机宜支持对每端口组播组的数目限制。

具有路由功能的以太网交换机宜支持 IGMP 响应报文的过滤、抑止功能。

具有路由功能的以太网交换机宜支持对 IGMP 加入组范围进行限制。

7.2.9 DHCP Snooping

具有路由功能的以太网交换机宜支持DHCP监听功能，记录DHCP服务器的地址。

7.2.10 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，对CPU的运行状态监控。

8 管理平面安全

8.1 安全威胁

对管理平面的安全威胁主要有以下方面，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。

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 8.2.7 节。

8.2.2 用户数据保护

对于具有路由功能的以太网交换机，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。具有路由功能的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 8.2.7.1、8.2.7.2 和 8.2.7.5 等节。

8.2.3 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。

8.2.4 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作进一步处理；
- 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。

8.2.5 安全管理

8.2.5.1 分级网管

具有路由功能的以太网交换机应支持分级网管功能。

8.2.5.2 口令管理

有关口令管理的要求参见 7.2.5 节。

8.2.6 可信信道/路径

由于带内管理面临的潜在的安全问题，具有路由功能的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。具有路由功能的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。

8.2.7 系统访问

8.2.7.1 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。具有路由功能的以太网交换机应支持安全性较好的 SNMPv3 作为网管协议。

此外，宜具有路由功能的以太网交换机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。

8.2.7.2 Telnet 访问

Telnet 协议用于通过网络对设备进行远程登录。在具有路由功能的以太网交换机中，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。

8.2.7.3 串口访问

具有路由功能的以太网交换机如果支持串口访问功能，应提供同 8.2.7.2 节相同的安全保护能力。

8.2.7.4 SSH 访问

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：

- 应支持 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，具有路由功能的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的 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。

8.2.7.5 Web 管理

Web 管理基于 HTTP 协议，具有路由功能的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。

8.2.7.6 软件升级

具有路由功能的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。

8.2.8 流量监控功能

具有路由功能的以太网交换机应支持流量统计监控功能，宜实现 IPFIX 功能。

参考文献

GB 4943-1995	信息技术设备（包括电气事务设备）的安全
GB 9254-1998	信息技术设备的无线电骚扰限值和测量方法
GB 9361-88	计算机场地安全要求
GB/T 17618-1998	信息技术设备抗扰度限值和测量方法
GB/T 18018-1999	路由器安全技术要求
GB/T 18336-2001	信息技术 安全技术 信息技术安全性评估准则
YD/T 849-1996	开放系统互联安全体系结构
YD/T 968-1998	电信终端设备电磁兼容性限值及测量方法
YD/T 1163-2001	IP 网络安全技术要求 安全框架
ISO 7498-2：1989	信息处理系统——开放系统互连 基本参考模型第 2 部分：安全体系结构
ISO/IEC 10164-7：1992	信息技术 开放系统互连 系统管理 第 7 部分：安全报警报告功能
ISO/IEC 10164-8：1993	信息技术 开放系统互连 系统管理 第 8 部分：安全审计跟踪功能
ISO/IEC 10745：1995	信息技术 开放系统互连 上层安全模型
ISO/IEC 11577：1995	信息技术 开放系统互连 网络层安全协议
ISO/IEC 11770-1	信息技术 安全技术 密钥管理 第 1 部分：框架
ISO/IEC 11770-2	信息技术 安全技术 密钥管理 第 2 部分：使用对称技术的机制
ISO/IEC TR 13335-1	信息技术安全管理的指导 第 1 部分：IT 安全概念和模型
ISO/IEC 15408-1	信息技术安全的评估准则 第 1 部分：引言和一般模型
ISO/IEC 15408-2	信息技术安全的评估准则 第 2 部分：安全功能要求
ISO/IEC 15408-3	信息技术安全的评估准则 第 3 部分：安全保证要求
ITU-T X.805（10/2003）	数据网络和开放系统通信 安全：提供端到端通信系统的安全体系结构
IETF RFC 0793	传输控制协议
IETF RFC 1321	MD5 消息摘要算法
IETF RFC 1352	SNMP 安全协议
IETF RFC 1446	SNMPv2 的安全协议
IETF RFC 1700	分配号码
IETF RFC 1704	关于因特网的认证
IETF RFC 1858	IP 分片过滤的安全考虑
IETF RFC 1918	私有因特网的地址分配
IETF RFC 2082	RIP-2 MD5 认证
IETF RFC 2154	使用数字签名的 OSPF
IETF RFC 2196	站点安全手册
IETF RFC 2385	通过 TCP MD5 签名选项的保护 BGP 会话
IETF RFC 2401	因特网协议的安全体系结构
IETF RFC 2408	因特网安全关联和密钥管理协议

IETF RFC 2510	因特网 X.509 公开密钥基础设施证书管理协议
IETF RFC 2573	SNMPv3 应用
IETF RFC 2644	改变路由器的默认的定向广播
IETF RFC 2827	网络入口过滤：防止使用 IP 源地址哄骗的拒绝服务
IETF RFC 2828	因特网安全术语表
IETF RFC 3013	建议的因特网服务提供商安全服务和程序
IETF RFC 3128	保护免受一种残片攻击的变种
IETF RFC 3567	IS-IS 加密认证
IETF RFC 3704	多宿主（multihomed）网络的入口过滤