ICS 33.040.30
M 32

YD

中华人民共和国通信行业标准

YD/T 2042-2009

IPv6网络设备安全技术要求
——具有路由功能的以太网交换机

IPv6 network equipment security requirements
——Ethernet switch with routing capability

2009-12-11 发布　　2010-01-01 实施

中华人民共和国工业和信息化部　发布

目　次

前　言……II
1　范围……1
2　规范性引用文件……1
3　术语、定义和缩略语……2
3.1　术语和定义……2
3.2　缩略语……3
4　概述……4
5　数据平面安全……5
5.1　安全威胁……5
5.2　安全功能……6
6　控制平面安全……8
6.1　安全威胁……8
6.2　安全功能……8
7　管理平面安全……11
7.1　安全威胁……11
7.2　安全功能……11

前　言

本标准是“IPv6网络设备安全”系列标准之一，该系列标准预计的结构及名称如下：

1．YD/T 1905-2009　IPv6网络设备安全技术要求——宽带网络接入服务器

2．YD/T 2041-2009　IPv6网络设备安全测试方法——宽带网络接入服务器

3．YD/T 2042-2009　IPv6网络设备安全技术要求——具有路由功能的以太网交换机

4．YD/T 2043-2009　IPv6网络设备安全测试方法——具有路由功能的以太网交换机

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：工业和信息化部电信研究院。

本标准主要起草人：马军锋、赵世卓。

IPv6网络设备安全技术要求
——具有路由功能的以太网交换机

1 范围

本标准规定了具有IPv6路由功能的以太网交换机安全技术的基本要求，包括数据转发平面、控制平面和管理平面的安全威胁和安全服务要求，以及鉴别验证、数据保护、系统功能保护、资源分配、安全审计、安全管理、可信信道/路径和系统访问等8个安全功能需求。

本标准适用于支持IPv6协议并具有路由功能的以太网交换机设备。

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	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）
IETF RFC1195（1990）	在TCP/IP和双栈环境下使用OSI ISIS路由协议
IETF RFC1352（1992）	SNMP安全协议
IETF RFC2385（1998）	通过TCP MD5签名选项保护BGP会话
IETF RFC2407（1998）	基于ISAKMP的INTERNET IP 安全域
IETF RFC2408（1998）	INTERNET安全协商和关键管理协议
IETF RFC2409（1998）	互联网密钥交换协议(IKEv1)
IETF RFC2740（1999）	IPv6下的OSPF协议
IETF RFC2827（2000）	网络入口过滤：抵御利用IP源地址欺骗的拒绝服务攻击
IETF RFC3567（2003）	ISIS协议加密认证
IETF RFC3682（2004）	通用TTL安全机制
IETF RFC3882（2004）	配置BGP阻止拒绝服务攻击
IETF RFC3971（2005）	安全邻居发现
IETF RFC4291（2006）	IP地址框架
IETF RFC4301（2005）	互联网协议安全框架
IETF RFC4302（2005）	IP认证头协议
IETF RFC4303（2005）	IP安全载荷封装
IETF RFC4306（2005）	互联网密钥交换协议
IETF RFC4552（2006）	OSPFv3认证/机密性

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本标准。

3.1.1

具有 IPv6 路由功能的以太网交换机 ethernet LAN switch with IPv6 routing capability

具有第三层路由功能的 IPv6 数据包交换机。除实现数据帧转发功能外，能根据接收数据包中的网络层地址以及交换机内部维护的路由表决定输出端口以及下一跳交换机地址或主机地址并且重写链路层数据包头。

路由表可以通过静态配置方式维护，也可以动态维护来反映当前的网络拓扑。具有路由功能的以太网交换机通常通过与其他类似设备（如路由器）交换路由信息来完成路由表的动态维护。如果文中没有特别说明，那么交换机就特指此类具有路由功能的以太网交换机。

3.1.2

访问控制 access control

防止对资源的未授权使用。

3.1.3

可确认性 accountability

确保一个实体的行为能够被独一无二地跟踪。

3.1.4

授权 authorization

授予权限，包括允许基于访问权的访问。

3.1.5

可用性 availability

根据授权实体的请求可被访问与使用。

3.1.6

保密性 confidentiality

这一性质使信息不泄露给非授权的个人、实体或进程，不为其所用。

3.1.7

数据完整性 data integrity

这一性质表明数据没有遭受以非授权方式所作的篡改或破坏。

3.1.8

服务拒绝 denial of service

阻止对资源的授权访问或拖延时限操作。

3.1.9

数字签名 digital signature

附加在数据单元上的一些数据，或是对数据单元所作的密码变换，这种数据或变换允许数据单元的接收者用以确认数据单元来源和数据单元的完整性，并保护数据，防止被人(例如接收者)进行伪造。

3.1.10

加密 encryption

对数据进行密码变换以产生密文。

3.1.11

基于身份的安全策略 identity-based security policy

这种安全策略的基础是用户或用户群的身份或属性,或者是代表用户进行活动的实体以及被访问的资源或客体的身份或属性。

3.1.12

密钥 key

控制加密与解密操作的一序列符号。

3.1.13

基于规则的安全策略 rule-based security policy

这种安全策略的基础是强加于全体用户的总体规则。这些规则往往依赖于把被访问资源的敏感性与用户、用户群或代表用户活动的实体的相应属性进行比较。

3.1.14

安全审计 security audit

为了测试出系统的控制是否足够，保证与已建立的策略和操作堆积相符合，或者是发现安全中的漏洞，以及为了建议在控制、策略和堆积中作任何指定的改变，而对系统记录与活动进行的独立观察和考核。

3.1.15

安全策略 security policy

提供安全服务的一套准则。(见“基于身份的安全策略”与“基于规则的安全策略”)

3.1.16

安全服务 security service

由参与通信的开放系统层所提供的服务，它确保该系统或数据传送具有足够的安全性。

3.2 缩略语

下列缩略语适用于本标准。

3DES	Triple DES	三重数据加密标准
AES	Advanced Encryption Standard	高级加密标准
AH	Authentication Header	认证头
BGP	Border Gateway Protocol	边界网关协议
DAD	Duplicate Address Detection	重复地址探测
DoS	Denial of Service	拒绝服务
ESP	Encapsulation Secure Payload	封装安全载荷
FCAPS	Fault，Capacity，Administration，Provisioning and Security	故障，配置，计费，性能，安全
HMAC	Hashed Message Authentication Code	散列消息验证码
ICMP	Internet Control Management Protocol	互联网控制管理协议

IKE	Internet Key Exchange	互联网密钥交换协议
IP	Internet Protocol	网际互连协议
IPSec	IP Security	IP 安全机制
IPv6	Internet Protocol version 6	网际互连协议版本 6
IS-IS	Intermediate System to Intermediate System	中间系统一中间系统
MAC	Media Access Control	媒质访问控制
MD5	Message Digest 5	报文摘要 5
RFC	Request for Comments	注释请求
OAM&P	Operation，Administration，Maintenance and Provisioning	操作，管理，维护和配置
OSPFv3	Open Shortest Path First version 3	最短路径优先版本 3
Ripng	Routing Information Protocol Next Generation	下一代路由信息协议
SHA-1	Secure Hash Algorithm 1	安全散列算法 1
SNMP	Simple Network Management protocol	简单网络管理协议
SSH	Secure Shell	安全外壳程序协议
TCP	Transmission Control Protocol	传输控制协议
UDP	User Datagram Protocol	用户数据报协议
USM	User-based Security Model	基于用户的安全模型
uRPF	Unicast Reverse Path Filter	单播反向路径检查
VLAN	Virtual Local Area Network	虚拟局域网
VPN	Virtual Private Network	虚拟专用网

4 概述

具有IPv6路由功能的以太网交换机可以应用在网络的各个层次，例如作为边缘汇聚设备，终结二层网络，实现三层业务的汇聚，或者是作为网络的核心交换设备。在网络中此类设备容易遭受到来自网络和其他方面的威胁，这些安全威胁可以利用设备自身的脆弱性或者是配置上的策略漏洞，给设备造成一定的危害，而且设备一旦被攻击，性能和正常运行都将会受到很大的影响，甚至造成拒绝对正常用户的访问服务。

本标准将具有IPv6路由功能的以太网交换机的功能划分为3个平面，如图1所示。

—— 数据平面：主要是根据交换机维护的转发表信息提供用户数据的转发。

—— 控制平面：主要是通过静态或者是动态路由协议学习网络拓扑信息，产生和维护用于数据转发的路由信息；使用网络控制管理协议探测网络可达性，无状态的自动地址配置协议完成主机 IP 地址的配置，邻居发现协议实现相同网段内相关设备的主动发现等。

—— 管理平面：主要是指与 OAM&P 相关的功能，如 SNMP、管理用户 Telnet 登录、日志等，支持 FCAPS（Fault，Capacity，Administration，Provisioning and Security）功能。管理平面的消息传送可以采用带内和带外两种形式。

为了抵御来自网络和用户的攻击，具有IPv6路由功能的以太网交换机必须提供一定的安全功能。本标准采用GB/T 18336.2中定义的安全功能并应用到交换机中（如图1所示），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，保护用户数据的完整性、可用性和保密性；

—— 系统功能保护，对实现系统关键功能包括安全功能所需要的数据（如用户身份和口令）的保护，确保相关数据的完整性、可用性和保密性；

—— 资源分配，控制用户对资源的访问，不允许用户过量占用资源，避免因为非法占用资源造成系统对合法业务拒绝服务；

—— 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指定安全对策，探测违背安全性的行为；

—— 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 IPv6 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，对于安全数据的通信要同其他通信隔离开来；

—— 系统访问，管理和控制用户会话的建立。

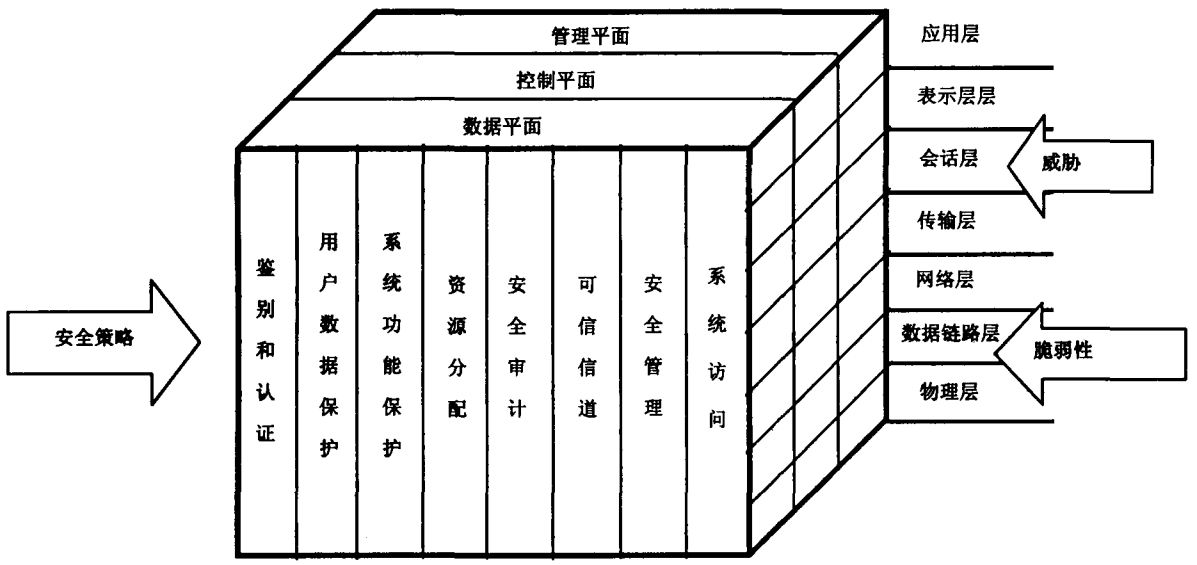

图 1　具有 IPv6 路由功能的以太网交换机安全框架

硬件系统和操作系统是具有路由功能的以太网交换机自身安全的重要因素，对硬件系统和操作系统的要求见 YD/T 1358-2005 的附录 A。

5　数据平面安全

5.1　安全威胁

基于流量的攻击会对交换机的性能造成很大影响，如大流量攻击（如Ping Flooding、TCP SYN Flooding等）可能会影响设备对正常用户数据进行处理，处理畸形报文可能会占用大量的CPU和内存资源，所以需要提供安全机制来限定用户流量行为，抵御来自网络攻击者对数据平面的恶意攻击。

此外，对数据流未经授权的观察、修改、插入和删除操作，会破坏数据流的完整性、可用性和保密性。具有IPv6路由功能的以太网交换机数据平面的安全威胁主要有以下方面，但不局限在这些方面：

—— 对数据流进行流量分析，从而获得用户数据的敏感信息；

—— 未经授权的观察、修改、插入和删除用户数据；

—— 利用用户数据流进行分布式的 DoS 攻击。

5.2 安全功能

5.2.1 鉴别和认证

具有IPv6路由功能的以太网交换机可以使用VLAN_ID、MAC地址、物理端口号、IP地址、账号等组合绑定的形式来标识一个用户；通过实现802.1x认证协议来验证用户的合法性。

5.2.2 数据保护

具有IPv6路由功能的以太网交换机可选为用户提供IP安全服务(具体实现应符合IETF RFC4301)，通过建立IPSec隧道，为用户数据提供完整性、数据源身份认证、保密性以及防重放攻击的保护。应支持AH和ESP协议，支持传输模式和隧道模式，支持安全联盟手工建立和IKE协议自动协商建立两种方式。在手工管理安全联盟时，可支持以十六进制配置算法所需密钥，应支持任意长度字符串形式配置密钥。

AH协议实现应符合IETF RFC4302，应支持HMAC-SHA1-96验证算法，可支持HMAC-MD5-96验证算法。

ESP协议实现应符合IETF RFC4303，应支持HMAC-SHA1-96验证算法，可支持HMAC-MD5-96验证算法。

加密算法应支持空加密算法、3DES-CBC加密算法，可选支持AES-CBC和国家规定的标准分组加密算法。

如果交换机支持动态密钥管理IKE协议，应支持IKEv1版本，符合IETF RFC2407、IETF RFC2408、IETF RFC2409，可选支持IKEv2版本，符合IETF RFC4306，并支持IKE的下列特性：

—— 支持预共享密钥验证，可支持数字证书验证和 RSA 加密 Nonce 验证；

—— 应支持 3DES 加密算法，支持 SHA1 完整性验证算法，可支持 MD5 完整性验证算法，同时还可支持 DES、AES 加密算法和国内的分组加密算法；

—— 在 IKE 的 Diffie-Hellman 交换中，应支持 MODP-Group1、MODP-Group2。

如果交换机支持 IKEv1 版本，应支持下列特性：

—— 阶段 2 交换中应支持完美前向保护特性；

—— 阶段 1 应支持主模式和野蛮模式，阶段 2 应支持快速模式，还应支持信息交换；

—— 在 IKE 阶段 1 中应该能指定发起模式。

5.2.3 系统功能保护

对于用户数据，系统要提供妥善的保护手段，通过基于角色的分级访问控制机制来实现对此类数据的访问控制（包括用户、系统进程等）。

5.2.4 资源分配

具有IPv6路由功能的以太网交换机应能够提供有效的过滤控制机制，保障网络带宽的合理利用，特别是要能够抵御来自网络的各种侵占网络资源类的攻击，要确保网络在遭受攻击的情况下仍旧能够正常转发用户数据。

具有IPv6路由功能的以太网交换机应能够抵御以下的常见攻击类型，但并不局限于这些方面。

—— 大流量攻击：大流量可以分成两种类型，一种是流经流量，即需要交换机转发的流量，对于这类攻击，交换机宜具有端口线速转发的能力，对于超过端口处理能力的流量可以采用按比例丢弃的策略。另一种流量的目的地就是交换机本身，这类攻击可能会占用被攻击设备的大量 CPU 处理时间和内存，严重的甚至会造成设备崩溃，导致中断无法为用户提供正常服务。对这类攻击流量，交换机宜采取过滤和

丢弃策略，同时应将必要的信息（如报文类型、源地址以及攻击时间等）记录到安全日志中。

（注：记录安全日志信息要求应用于汇聚层及以上的设备必须支持，对于应用于接入层的设备可选）。

交换机应支持基于 VLAN ID、 MAC 地址、IP 五元组等字段对转发流量进行过滤整形。

—— 畸形包处理：交换机应能够处理目的地址为其自身的各种类型畸形包，如：

1） 超长包，例如包长大于 65535；

2） 超短包；

3） 链路层错误包；

4） 网络层错误包；

5） 上层协议错误包；

6） 不可识别的扩展头字段等。

对于这些报文应采取丢弃策略，不能影响设备的正常功能。此外，也要保证交换机自身不会产生上述类型的畸形包。

—— 定向广播报文攻击：SMURF 攻击是一种利用定向广播报文的分布式 DoS 攻击方法。对于此类攻击交换机应能够提供控制策略，禁止该类报文转发或者以广播形式转发；对于分布式 DoS 攻击，应能够提供简单策略阻止这种分布式 DoS 攻击向其他设备扩散。

—— IP 地址哄骗：针对网络中源地址哄骗报文，交换机宜可选实现单播逆向路径转发（uRPF）技术来过滤这类报文，禁止其在网络中传播，可选实现稀疏和密集两种模式，具体实现应符合 IETF RFC2827 的规定。交换机需要考虑对特定业务报文要能够正确的处理，例如在入口避免过滤中继 DHCPv6 的请求报文。

—— 组播报文处理，交换机应当丢弃源地址是组播地址的报文，对于接收的组播报文根据 IETF RFC4291 规定的组播地址作用域转发组播数据报文。

建议交换机支持基于IPv6报头流标签的数据包过滤，当网络发生拥塞时，根据报文的流标签对用户数据进行限速、丢弃、整形等操作。

5.2.5 安全审计

对于用户流量，具有IPv6路由功能的以太网交换机应能够提供流量日志能力，相关的要求见7.2.5节有关安全日志方面的规定。

5.2.6 安全管理

要能够提供对本节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。

5.2.7 可信信道/路径

具有IPv6路由功能的以太网交换机同其他设备通信的信道/路径要求可信，对于传送敏感数据的通信同传送其他数据的通信隔离开来，可以采用物理隔离或者是VPN（可选实现L2VPN、L3VPN）逻辑隔离。

5.2.8 系统访问

访问控制是一种安全手段，它控制用户和系统与其他的系统和资源进行通信和交互。它能够保护系统和资源免受未经授权的访问，并且在认证过程成功结束后授权访问的等级。访问控制能够提供控制、限制、监控以及保护资源的可用性、完整性和机密性等能力。

具有IPv6路由功能的以太网交换机应能够提供基于VLAN ID、源MAC地址的过滤，基于源/目的IP地址、源/目的端口和协议类型等元素的过滤，支持对ICMP报文进行过滤，支持对报文优先级进行过滤，支持对报文匹配情况进行统计计数和记入日志，该项功能要求汇聚层及以上设备必须支持，接入层设备作为可选功能。

6 控制平面安全

6.1 安全威胁

具有IPv6路由功能的以太网交换机控制平面主要负责MAC地址与IP地址的绑定、路由信息的学习、主机地址的自动配置等。

控制平面的安全威胁主要有以下几个方面，但不局限在这些方面：

—— 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，将转发路径信息暴露给非授权设备；

—— 利用协议的拒绝服务攻击，如利用路由协议、ICMPv6 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，建立路由协议的实体信任关系，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。

6.2 安全功能

6.2.1 鉴别和认证

6.2.1.1 路由认证

具有IPv6路由功能的以太网交换机通过路由协议来传递路由信息，计算到达目的网络的最佳路径，因此必须确保路由信息的完整性和可用性，并且对路由信息通告者的真实身份进行认证，以免造成由于恶意的攻击者冒充路由对等体通告不正确或者是不一致的路由信息导致网络服务的不可达。

具有IPv6路由功能的以太网交换机应可选支持路由协议认证，具体要求如下：

—— Ripng：实现 IP 认证头和 IP 安全载荷封装来保证路由信息交互的完整性、机密性和对交互实体的认证。

注：RIPng 协议去除了在 Ripv2 中定义的认证域。

—— OSPFv3：在 OSPFv3 的协议报头中已经去除了认证和认证类别域，依赖 IP 认证头和 IP 安全载荷封装来提供交互实体的鉴别和路由交互信息的完整性和保密性，在实现上必须符合 IETF RFC2740 和 IETF RFC4552 规定。

—— IS-IS：应实现基于链路、Level1 和 level2 域的认证，符合 IETF RFC1195 的规定；建议按照 IETF RFC3567 规范，使用 HMAC-MD5 算法实现对 ISIS 协议数据报文的认证。

—— BGP4+：通过使用 TCP MD5 签名选项来保护 BGP 会话，其实现应符合 IETF RFC2385 规定。

建议交换机实现 IETF RFC3682 中描述的通用 TTL（在 IPv6 中使用 Hop Limit 字段）安全机制来保护 EBGP 会话。

建议交换机支持 BGP-Triggered Black holing 技术，实现 IETF RFC3882 中描述的机制，通过利用 BGP 协议中的 Community 属性来阻挡 DoS 攻击流量。

6.2.1.2 NDP（邻居发现）协议认证

IPv6 定义了邻居发现协议，它使用一系列 IPv6 控制信息报文（ICMPv6）来实现相邻节点（同一链路上的节点）的交互管理，并在一个子网中保持网络层地址和链路层地址之间的映射。邻居发现协议中定义了 5 种类型的消息：路由器宣告、路由器请求、路由重定向、邻居请求和邻居宣告。通过这些消息，实现了对以下功能的支持：路由器发现、前缀发现、参数发现、地址自动配置、地址解析、下一跳确定、邻居不可达检测、重复地址检测、重定向等。

交换机可选实现相应的保护机制来抑制攻击者对网络发起的 DoS 攻击，截取并修改数据包的攻击，例如：攻击者可以通过发送路由器通告报文向同网段内的主机声称将其作为缺省网关，然后再将接收的报文转发到真正的网关，通过这种方式，可以截获用户的数据，并根据需要对其修改或者丢弃，而数据源却无法获知。即使使用邻居不可达检测机制也无法发现此类攻击，因为只要攻击者能够响应 NUD 检测报文。

交换机应当丢弃从相邻节点收到的所有 Hop Limit 域值小于 255 的 NDP 协议报文。

此外，交换机可选实现 IETF RFC3971 中建议的 NDP 安全机制，支持授权委托发现过程，地址验证机制以及相应的协议扩展（如密码地址生成选项、签名选项、时间戳和随机数选项等）。

6.2.1.3 有状态/无状态地址配置认证

具有 IPv6 路由功能的以太网交换机应支持无状态的地址配置，可选支持有状态的地址配置。对于无状态的地址配置方案，交换机宜提供安全机制保护路由器通告消息的完整性，确保 DAD 探测过程的可靠性，避免攻击者针对地址分配的 DoS 攻击（攻击者通过响应 DAD 探测过程中的邻居请求报文，声称该报文中目标地址已经被分配使用，从而导致申请者无法获得有效的 global-scope 地址）。对于有状态的地址分配方案，交换机宜支持 DHCP 监听功能，记录 DHCP 服务器的地址，防止 DHCP 服务器假冒攻击。

6.2.2 数据保护

具有IPv6路由功能的以太网交换机应当对控制平面的信息（主要是路由信息、地址配置信息）提供完整性、保密性和可用性保护，可以采用数据加密技术实现。

6.2.3 系统功能保护

用于系统控制平面的安全数据（如路由协议的认证密钥）应得到妥善的保护。

6.2.4 资源分配

6.2.4.1 路由控制策略和路由过滤

由于控制信息的运算和存储需要消耗大量的CPU运算资源和内存存储资源，因此交换机在控制平面应支持路由控制策略和路由过滤，抑制攻击者利用路由协议的安全缺陷进行资源耗尽型的攻击。

6.2.4.2 MAC 地址学习

建议交换机能够提供IP-MAC地址静态绑定机制（可选），避免在IP-MAC地址动态学习过程中遭受攻击者的欺骗，导致将攻击者的IP地址作为缺省网关，从而使得流量经由攻击者转发遭受中间人攻击。

建议交换机实现基于物理端口的MAC地址学习控制机制，能够限定通过每个物理端口学习MAC地址的数量，以避免在同一个网段内接收到攻击者发送的大量源MAC地址不同的ARP消息，导致交换机MAC地址表溢出。

6.2.4.3 可关闭一些 IP 服务

6.2.4.3.1 ICMPv6 协议

ICMPv6作为IPv6协议栈的基本协议之一，主要用于网络操作和故障排除，由于协议自身存在安全漏洞，从而导致被利用于攻击网络，因此要求具有关闭相关ICMPv6功能的能力，包括如下：

—— Type 1:目的地不可达；

—— Type 2:分组过大；

—— Type 3:超时；

—— Type 4:参数错误；

—— Type 129:回显应答消息；

—— Type 130－132：组播监听者消息；

—— Type 133/134：路由器请求/通告消息；

—— Type 135/136：邻居请求/通告消息；

—— Type 137：重定向消息。

交换机应当能够按照ICMPv6消息的类型，源、目的地址类型和范围（单播、组播， 本地链路、全局）或者是错误消息的错误码对ICMPv6消息进行过滤。

6.2.4.3.2 重定向功能

交换机应当能够关闭路由重定向功能，避免攻击者通过路由重定向截取用户数据。

6.2.4.3.3 Hop-by-Hop 选项功能

交换机应当能够关闭Hop-by-Hop选项功能（可选）。

6.2.5 安全审计

对控制平面的控制信息要提供日志记录功能，特别是记录路由邻居状态变化、IP-MAC地址绑定等重要的有影响的控制数据。

具有IPv6路由功能的以太网交换机可以支持端口镜像功能，通过配置，将系统中某个端口的部分或者全部流量镜像到其他的端口，出方向的报文和入方向的报文可以分别镜像到不同的端口。此外可选支持向远端安全中心进行数据镜像的功能。

端口镜像时，对帧不进行修改，有如下两种镜像类型：

—— 一对一端口镜像，把一个端口的流量，全部原封不动地拷贝到指定的镜像端口；

—— 多对一端口镜像。

6.2.6 安全管理

具有IPv6路由功能的以太网交换机应当能够提供控制平面的安全功能和安全数据管理能力，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IPv6路由功能的以太网交换机与其他设备之间交互的控制信息应保证其完整性、保密性和可用性，因此必须要确保通信信道是可信的，可以通过物理隔离或者是建立安全的逻辑隧道来实现。

6.2.8 系统访问

具有IPv6路由功能的以太网交换机在控制平面应对通告路由信息的对等体进行认证，如果认证不通过，则应丢弃该对等体通告的路由信息，并将相关信息记录到日志文件中。

6.2.8.1 路由策略和路由过滤

具有IPv6路由功能的以太网交换机应支持路由控制策略和路由过滤，防止攻击者利用路由协议安全漏洞通告错误路由或者是倾泄大量路由信息导致内存溢出，设备瘫痪。

交换机应支持如下的路由策略和过滤机制：

—— 按照目的网段、自治系统路径、团体属性等特性进行过滤；

—— 能够配置成 Passive(被动)模式，只接收处理路由信息，而不向邻居对等体通告路由信息；

—— 在路由协议重分布过程中能够按照目的网段、自治系统号等信息过滤。

7 管理平面安全

7.1 安全威胁

具有IPv6路由功能的以太网交换机网络管理平面的主要功能是实现对设备系统参数配置以及设备状态信息的统计，其可能面临的主要安全威胁包括以下几个方面，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；

—— 未经授权地观察、修改、删除系统的配置信息；

—— 未经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。

7.2 安全功能

7.2.1 鉴别和认证

管理接口应提供必要的用户身份鉴别和认证功能，只授权合法用户的访问。为了审计的需要，要确保用户标识的惟一性，不建议一个用户使用多个标识或者是多个用户使用同一个标识。

7.2.1.1 串口访问

具有IPv6路由功能的以太网交换机应当支持串口访问功能，能够设置密码保护，设定登录的有效时间（可选），或者设置二次登录来获得更高的访问权限(可选)。

7.2.1.2 Telnet 访问

具有 IPv6 路由功能的以太网交换机应当提供远程登录 Telnet 访问模式，对登录用户的访问应符合下述要求：

—— 提供对用户身份的验证，在日志文件中记录用户的访问活动；

—— 提供对用户账号的分级管理，不同的用户分配不同的访问权限；

—— 提供对 Telnet 用户密码试探攻击的保护，可对同一个 IP 地址使用延时响应机制，也可以限定来自同一个 IP 地址的登录尝试次数；当用户连续登录系统失败次数超过系统设定值时，系统管理员可以考虑将该用户账号锁定；

—— 能够限制同时登录的 Telnet 用户数量；

—— 在设定的时间周期内不进行交互应注销该用户；

—— 应支持必要时关闭 Telnet 远程服务。

7.2.1.3 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 和 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 IPv6 路由功能的以

太网交换机应支持口令认证；

—— 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切断连接，建议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，支持 Diffie-Hellman 组 14 或组 1 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，建议支持 HMAC-SHA1-96 认证算法，可选实现 HMAC-MD5、HMAC-MD5-96 等认证算法；

—— 应支持 3DES-CBC 对称加密算法，可选实现 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，应支持 SSH-DSS，建议可选实现 SSH-RSA；

—— 可限定用户通过哪些 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。

7.2.1.4 Web 管理 (可选)

具有IPv6路由功能的以太网交换机应可选提供基于Web的管理模式，系统管理员能够通过Web方式配置系统参数，查看统计信息等，建议满足下列要求：

—— 用户应提供用户名/口令才能进行后续的操作，用户地址、用户标识和操作应记入日志文件；

—— 可限定用户通过哪些 IP 地址使用 HTTP 对设备进行访问；

—— 应能够支持 SSL/TLS 协议，确保数据的完整性和机密性；

—— 应支持必要时可关闭 HTTP 服务。

7.2.1.5 SNMP 安全

具有IPv6路由功能的以太网交换机应支持通过实现安全协议来保护网络管理操作的功能，提供数据完整性、数据源认证和数据保密性服务。

SNMP是最常用的网络管理协议，它提供了网管工作站和位于被管设备上的代理之间的通信接口。通过该接口，网络管理员能够将配置参数下载到被管设备，查看被管设备的运行状况和运行参数，因此确保网络管理接口的安全是非常重要的。

SNMP协议应当支持IETF RFC1352规定的摘要认证协议和对称私有协议，实现消息摘要算法和对称加密算法。通过摘要认证协议来保证网管消息发送者/接收者之间网管信息的完整性，同时可以验证消息源；对称私有协议来保护网管信息防止泄密。

SNMPv1本身只能提供非常弱的安全保护能力，在SNMPv1中代理和管理站之间的通信除依靠团体串验证外不作任何安全设置，一旦团体串被泄漏，则会给网络设备带来很大的安全风险。

SNMPv2提供了一定的安全机制，但是没有得到广泛的实施，不支持SNMPv2安全机制的实现称为SNMPv2c。

SNMPv3是一个安全的网络管理协议，能够提供支持基于视图的访问控制（VACM）和基于用户的安全模型（USM）等安全机制，能够提供完善的安全保护。

具有IPv6路由功能的以太网交换机可支持SNMPv1和SNMPv2c，但应提供禁用功能，并且缺省应该是禁用的；应支持SNMPv3的网络管理接口。提供SNMPv1和SNMPv2c应可以和访问控制列表相结合，控制

非法网管接入设备，同时不使用public/private作为缺省团体名，缺省只读团体名和读写团体名称不能够相同，并且在适当的时机提示管理员修改团体名。此外交换机应可结合IP地址和传输端口、服务类型进行过滤，SNMP服务常使用UDP端口161、162，可能用到的其他端口还有TCP端口161、162、199、1993，UDP端口199、1993等。另外，还应该注意过滤来自广播地址、子网广播地址的SNMP流。

7.2.2 数据保护

管理平面的用户数据主要是一些用户配置数据，需要保证数据的完整性和可用性，以防止配置数据出错而导致整个设备工作不正常，同时也要防止敏感数据被窃取，导致网络遭受攻击。管理平面的用户数据可以采用带内和带外两种传送模式，带外模式通过物理隔离实现数据保护，带内模式则可以通过采用SSHv2或者是SNMP协议的安全扩展来实现。

7.2.3 系统功能保护

用于管理平面管理的相关安全数据（如配置信息）应得到妥善的保护。

7.2.4 资源分配

管理信息的处理需要占用系统的CPU、内存等资源，对这部分信息的处理一定要确保不能影响控制平面对路由信息和数据平面对用户数据转发的影响。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。

7.2.5 安全审计

具有IPv6路由功能的以太网交换机应当提供基本的日志功能，记录用户访问活动，以便于网络安全管理员根据日志信息监控网络运行情况和诊断网络故障。

日志应记录过滤规则、拒绝访问、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。

对日志的要求如下：

—— 安全日志条目应包含用户 IP 地址、用户名、操作类型、访问时间、操作结果等基本访问信息；

—— 应可以保存在本地系统（如磁盘介质），也可以发送到专用的日志主机上做进一步的处理；

—— 应可以实时打印在专用打印机或连接交换机的显示终端上；

—— 应定义日志的严重程度等级，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通信接口。

对告警的要求如下：

—— 应定义告警的严重程度级别，并根据严重程度级别确定是否以一定的方式（如声光显示）提示管理员；

—— 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。

7.2.6 安全管理

7.2.6.1 口令管理

具有IPv6路由功能的以太网交换机应能够支持一定长度的口令字（不短于8个），并且由数字、字符或特殊符号组成，支持对简单口令的检查功能；支持以密文的形式在系统配置文件中存储用户口令，此外，登录用户在查看系统配置时用户口令也应当以密文形式回显。

7.2.7 可信信道/路径

具有IPv6路由功能的以太网交换机应可选预留独立的以太网管理接口支持带外管理方式，在配置中要确保仅有内网管理用户可以访问，如果不使用该接口则应当关闭。此外，也可以通过专用的逻辑信道或者是加密信道（IPsec隧道）来提供网管数据的传送安全。

7.2.8 系统访问

7.2.8.1 设备的访问控制

具有IPv6路由功能的以太网交换机提供管理功能来配置设备，系统管理员能够远程登录到设备上进行维护和管理；对系统管理员用户的访问实现控制：

—— 验证登录用户的身份，核实用户的操作权限；

—— 不允许使用不安全的口令登交换机；

—— 用户所有的写操作、执行操作都应记录到日志文件中。

7.2.8.2 版本管理的控制

具有IPv6路由功能的以太网交换机宜提供完善的补丁或版本权限的管理功能，实现设备的软件升级，包括软件版本和设备的配置，可以通过本地和远程两种方式。