ICS 33 040 40
M 32

YD

中华人民共和国通信行业标准

YD/T 1628-2007

以太网交换机设备安全测试方法

Security test mothods for ethernet switching 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……Ⅱ
1　范围……1
2　规范性引用文件……1
3　术语和定义……1
4　缩略语……1
5　测试环境……3
6　数据平面安全测试……5
6.1　DoS攻击……5
6.2　ACL……7
6.3　流量控制……10
6.4　802.3ad 链路聚合……12
6.5　802.1x……12
6.6　MAC地址数目限制……14
6.7　MAC地址绑定功能……15
6.8　端口镜像……15
6.9　广播风暴抑制……16
7　控制平面安全测试……16
7.1　VLAN安全测试……16
7.2　STP/RSTP功能测试……17
7.3　IGMP Snooping 功能测试……20
7.4　DHCP Snooping功能测试……20
8　管理平面安全测试……21
8.1　用户访问控制……21
8.2　Telnet……22
8.3　Web管理功能测试……22
8.4　SSH……23
8.5　SNMPv3……27
8.6　安全审计……30

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技术要求》是本标准的技术依据，同时本标准也是 YD/T 1141-2005《以太网交换机测试方法》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：信息产业部电信研究院

本标准参加单位：中兴通讯股份有限公司

华为技术有限公司

国家计算机网络应急技术处理协调中心

武汉邮电科学研究院

北京通和实益电信科学技术研究所有限公司

本标准主要起草人：梁　冰　周开波　韩　韧　肖　雳　董　萌　罗　鉴　陈建业

以太网交换机设备安全测试方法

1 范围

本标准规定了二层以太网交换机的安全测试内容及测试方法。

本标准适用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。

YD/T 1627-2007　　以太网交换机设备安全技术要求

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。

·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。

·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。

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
CAR	Committed Access Rate	承诺接入速率
CBC	Cipher Block Chaining	密码块链

DoS	Denial of Service	拒绝服务
DSS	Digital Signature Standard	数字签名标准
DUT	Device Under Test	被测设备
HMAC	Hashed Message Authentication Code	散列消息认证码
ICMP	Internet Control Messages Protocol	因特网控制报文协议
IKE	Internet Key Exchange	因特网密钥交换
IP	Internet Protocol	因特网协议
IPSec	IP Security	IP安全机制
IS-IS	Intermediate System to Intermediate System	中间系统到中间系统
MAC	Media Access Control	媒介访问控制
MD5	Message Digest version 5	消息摘要版本5
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
PPP	Point-to-Point Protocol	点到点协议
RSA	Rivest, Shamir and Adleman Algorithm	RSA 算法
SHA	Security 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 version1	SNMP 版本1
SNMPv2c	SNMP version2c	SNMP 版本2c
SNMPv3	SNMP version3	SNMP 版本
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
UDP	User Datagram Protocol	用户数据报协议
URPF	Unicase Reverse Path Forwarding	单播反向路径转发
VPN	Virtual Private Network	虚拟专用网

5 测试环境

测试环境如图1~图8所示。

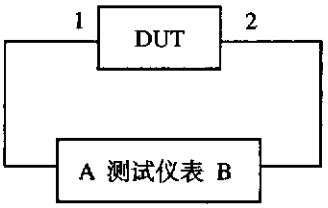

图1 测试环境1

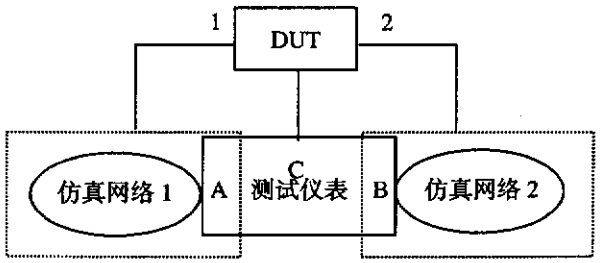

图2 测试环境2

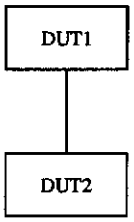

图3 测试环境3

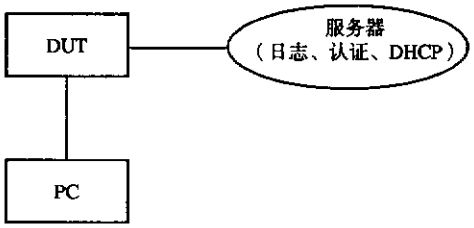

图4 测试环境4

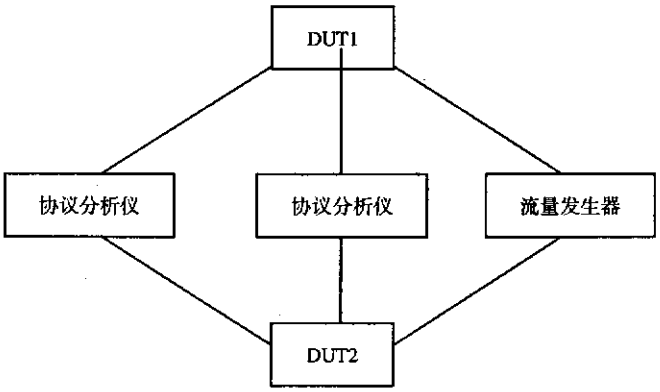

图5 测试环境5

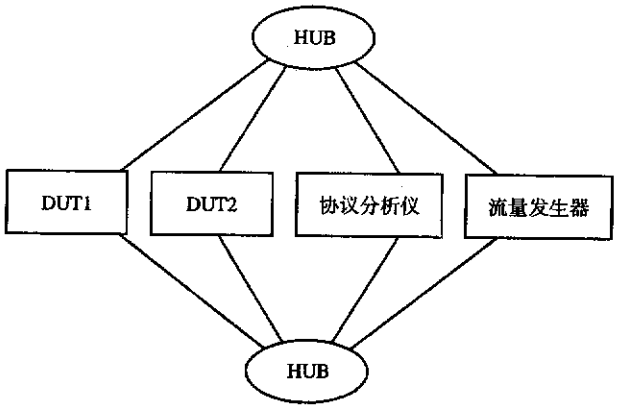

图6 测试环境6

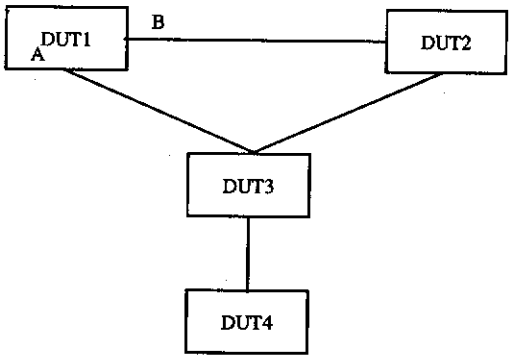

图7 测试环境7

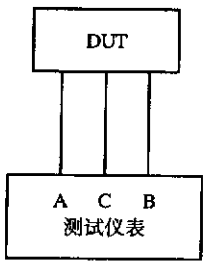

图8 测试环境8

6 数据平面安全测试

6.1 DoS 攻击

测试编号：1
测试项目：抗大流量攻击能力测试
测试目的：检验 DUT 处理大流量数据的能力
测试配置：测试环境 8
测试过程： 1. 按测试环境连接设备； 2. 从测试仪表端口 A 向测试仪表端口 B 以线速率发送数据包； 3. 从测试仪表端口 C 向 DUT 的管理地址以线速率发送数据包
预期结果： 在步骤 3 中，DUT 应能正常转发数据包，不受端口 C 上流量的影响
判定原则： 应符合预期结果要求，否则为不合格

测试编号：2
测试项目：畸形包处理能力测试
测试目的：检验 DUT 处理畸形数据包的能力
测试配置：测试环境 8
测试过程： 1. 按测试环境连接设备； 2. 从测试仪表端口 A 向测试仪表端口 B 发送小于端口速率的背景流量； 3. 由测试仪表端口 C 以端口速率向 DUT 管理地址发送报文长度(包括 IP 包头)大于 65535 字节的 ICMP Echo Request 报文（Ping of Death 攻击仿真报文）； 4. 停止步骤 3 中报文的发送，由测试仪表端口 C 向 DUT 管理地址发送多个 Offset 字段重叠的 IP 报文（Teardrop 攻击仿真报文）； 5. 停止步骤 4 中报文的发送，由测试仪表端口 A 向仪表端口 B 发送链路层错误（如以太网的 FCS 错误帧）报文； 6. 停止步骤 5 中报文的发送，由测试仪表端口 A 向仪表端口 B 发送长度小于 64 字节（以太网链路）的超短帧（Runt）； 7. 停止步骤 6 中报文的发送，由测试仪表端口 A 向测试仪表端口 B 发送长度大于链路 MTU 的超长帧（Giant）
预期结果： 1. 在步骤 3 中，攻击报文应被丢弃，记录攻击对背景流量的影响； 2. 在步骤 4 中，攻击报文应被丢弃，记录攻击对背景流量的影响； 3. 在步骤 5 中，错误帧应被丢弃，记录攻击对背景流量的影响； 4. 在步骤 6 中，超短帧应被丢弃，并提供统计数据，记录攻击对背景流量的影响； 5. 在步骤 7 中，超长帧应被丢弃，并提供统计数据，记录攻击对背景流量的影响
判定原则： 应符合预期结果要求，否则为不合格

测试编号：3
测试项目：Ping Flood 攻击处理能力测试
测试目的：检验 DUT 处理 Ping Flood 攻击的能力
测试配置：测试环境 8
测试过程： 1. 按测试环境连接设备； 2. 从测试仪表端口 A 向端口 B 以端口速率发送流量，并验证测试仪表端口 B 上流量能够正常接收； 3. 从测试仪表端口 C 向 DUT 管理地址以端口线速率发送 ICMP Echo Request 数据包
预期结果： 在步骤 3 中，DUT 应对超量 ICMP 报文进行丢弃或限速，记录攻击对其他端口流量的影响
判定原则： 应符合预期结果要求，否则为不合格

测试编号：4
测试项目：SYN Flood 攻击处理能力测试
测试目的：检验 DUT 处理 SYN Flood 攻击的能力
测试配置：测试环境 2
测试过程： 1. 按测试环境连接设备； 2. 从测试仪表端口 A 向端口 B 以端口速率的发送流量，并验证测试仪表端口 B 上流量能够正常接收； 3. 从测试仪表端口 C 向 DUT 管理地址发送 TCP SYN 数据包
预期结果： 在步骤 3 中，DUT 应对过量 TCP SYN 报文进行丢弃或降低优先级的排队处理，记录攻击对其他端口流量的影响
判定原则： DUT 可以对过量 TCP SYN 报文进行丢弃或降低优先级的排队处理，其他端口流量和时延应不会受到严重影响

测试编号：5
测试项目：Smurf 攻击处理能力测试
测试目的：检验 DUT 处理 Smurf 攻击的能力
测试配置：测试环境 2
测试过程： 1. 按测试环境连接设备； 2. 从测试仪表端口 A 向端口 B 以端口速率发送流量，端口 B 上流量能够正常接收； 3. 从测试仪表端口 C 向 DUT 管理地址以端口线速率发送 ICMP Echo Request 数据包
预期结果： 在步骤 3 中，DUT 应对 ICMP 报文进行丢弃，记录攻击对其他端口流量的影响
判定原则： 应符合预期结果要求，否则为不合格

6.2 ACL

测试编号：6
测试项目：基于源 MAC 地址的 ACL 测试
测试目的：检验 DUT 是否实现基于源 MAC 地址的 ACL
测试配置：测试环境 1
测试过程： 1. 按测试环境连接设备（互联接口采用以太网接口）； 2. 在 DUT 上配置基于源 MAC 地址的 ACL 条目，拒绝源 MAC 地址非特定地址的数据包； 3. 从测试仪表端口 A 向仪表端口 B 发送数据包，源 MAC 地址不是 DUT 配置的特定 MAC 地址； 4. 从测试仪表端口 A 向仪表端口 B 发送数据包，源 MAC 地址是 DUT 配置的特定 MAC 地址
预期结果： 1. 在步骤 3 中，测试仪表端口 B 没有收到数据包； 2. 在步骤 4 中，测试仪表端口 B 可以收到数据包
判定原则： 应符合预期结果要求，否则为不合格

测试编号：7
测试项目：基于目的 MAC 地址的 ACL 测试
测试目的：检验 DUT 是否实现基于目的 MAC 地址的 ACL
测试配置：测试环境 1
测试过程： 1. 按测试环境连接设备（互联接口采用以太网接口）； 2. 在 DUT 上配置基于目的 MAC 地址的 ACL 条目，拒绝目的 MAC 地址非特定地址的数据包； 3. 从测试仪表端口 A 向仪表端口 B 发送数据包，目的 MAC 地址不是 DUT 配置的特定 MAC 地址； 4. 从测试仪表端口 A 向仪表端口 B 发送数据包，目的 MAC 地址是 DUT 配置的特定 MAC 地址
预期结果： 1. 在步骤 3 中，测试仪表端口 B 没有收到数据包； 2. 在步骤 4 中，测试仪表端口 B 可以收到数据包
判定原则： 应符合预期结果要求，否则为不合格

测试编号：8
测试项目：全局 ACL 测试
测试目的：检验 DUT 是否实现全局 ACL
测试配置：测试环境 1
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 上配置全局 ACL（拒绝）条目； 3. 从测试仪表端口 A 向测试仪表端口 B 发送符合过滤条件的数据包； 4. 从测试仪表端口 B 向测试仪表端口 A 发送符合过滤条件的数据包
预期结果： 1. 在步骤 3 中，测试仪表端口 B 没有收到数据包； 2. 在步骤 4 中，测试仪表端口 A 没有收到数据包
判定原则： 应符合预期结果要求，否则为不合格

测试编号：9
测试项目：接口 ACL 测试
测试目的：检验 DUT 是否实现接口 ACL
测试配置：测试环境 1
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 接口 1 上配置 ACL（拒绝）条目； 3. 从测试仪表端口 A 向测试仪表端口 B 发送符合过滤条件的数据包； 4. 从测试仪表端口 B 向测试仪表端口 A 发送符合过滤条件的数据包
预期结果： 1. 在步骤 3 中，测试仪表端口 B 没有收到数据包； 2. 在步骤 4 中，测试仪表端口 A 可以收到数据包
判定原则： 应符合预期结果要求，否则为不合格

测试编号：10
测试项目：配置 ACL 情况下的性能测试
测试目的：检验 DUT 在配置 ACL 情况下的性能
测试配置：测试环境 2
测试过程： 1. 按测试环境连接设备； 2. 按照 DUT 声明值的 80%在接口 1 上配置相互无关联的 ACL（拒绝）条目； 3. 从测试仪表端口 A 向测试仪表端口 B 发送不符合过滤条件的数据包，进行性能测试
预期结果： 配置 ACL 后应不会对 DUT 的转发造成严重影响
判定原则： 应符合预期结果要求，否则为不合格

6.3 流量控制

测试编号：11
测试项目：流分类功能测试（基于 IP 五元组的流分类）
测试目的：检验 DUT 基于 IP 五元组（源 IP 地址、目的 IP 地址、协议类型、源端口号、目的端口号）进行流分类的功能
测试配置：测试环境 1
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 上分别为 IP 五元组配置流分类策略，并对命中的数据流采用流量限制，限制速率为 M，M 小于接口速率； 3. 测试仪表端口 A 向测试仪表端口 B 以接口速率发送符合分类策略的数据流； 4. 停止步骤 3 中数据流的发送，从测试仪表端口 A 向测试仪表端口 B 以接口速率发送不符合分类策略的数据流
预期结果： 1. 在步骤 3 中，测试仪表端口 B 可以收到数据流，数据流速率为 M（误差<10%）； 2. 在步骤 4 中，测试仪表端口 B 可以收到数据流，数据流速率为接口速率
判定原则： 应符合预期结果要求，否则为不合格

测试编号：12
测试项目：流分类功能测试（基于源 MAC 地址）
测试目的：检验 DUT 基于源 MAC 地址进行流分类的功能
测试配置：测试环境 1
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 上配置基于源 MAC 地址的流分类策略，并对命中的数据流采用流量限制，限制速率为 M，M 小于接口速率； 3. 测试仪表端口 A 向测试仪表端口 B 以接口速率发送符合分类策略的数据流； 4. 停止步骤 3 中数据流的发送，从测试仪表端口 A 向测试仪表端口 B 以端口速率发送不符合分类策略的数据流
预期结果： 1. 在步骤 3 中，测试仪表端口 B 可以收到数据流，数据流速率为 M（误差<10%）； 2. 在步骤 4 中，测试仪表端口 B 可以收到数据流，数据流速率为接口速率
判定原则： 应符合预期结果要求，否则为不合格

测试编号：13
测试项目：流分类功能测试（基于目的 MAC 地址）
测试目的：检验 DUT 基于目的 MAC 地址进行流分类的功能
测试配置：测试环境 1
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 上配置基于目的 MAC 地址的流分类策略，并对命中的数据流采用流量限制，限制速率为 M，M 小于接口速率； 3. 测试仪表端口 A 向测试仪表端口 B 以接口速率发送符合分类策略的数据流； 4. 停止步骤 3 中数据流的发送，从测试仪表端口 A 向测试仪表端口 B 以端口速率发送不符合分类策略的数据流
预期结果： 1. 在步骤 3 中，测试仪表端口 B 可以收到数据流，数据流速率为 M（误差<10%）； 2. 在步骤 4 中，测试仪表端口 B 可以收到数据流，数据流速率为接口速率
判定原则： 应符合预期结果要求，否则为不合格

测试编号：14
测试项目：流量整形功能测试
测试目的：检验 DUT 的流量整形功能
测试配置：测试环境 1
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 上为接口 2 配置流量整形，限制速率为 M，M 小于接口 2 的速率； 3. 由测试仪表端口 A 向测试仪表端口 B 以端口速率发送数据流
预期结果： 在步骤 3 中，测试仪表端口 B 可以收到数据流，数据流速率为 M（误差<10%）
判定原则： 应符合预期结果要求，否则为不合格

6.4 802.3ad 链路聚合

测试编号：15
测试项目：链路聚合功能测试
测试目的：检验 DUT 实现 802.3ad 规定的链路聚合功能
测试配置：测试环境 3
测试过程： 1. 按测试环境连接设备； 2. DUT1 和 DUT2 之间连接的端口设置为聚合在一个组内； 3. 测试仪表端口 A 向端口 B 发送广播流量（MAC 目的地址为全“F”）； 4. 断开其中一条链路； 5. 测试仪表端口 A 向端口 B 发送 *N* 个单播流（*N* 大于被聚合链路的数目）； 6. 断开其中一条链路； 7. 测试仪表端口 A 向端口 B 发送两个优先级相同的单播数据流。数据流 1 的流量大于聚合端口线速，数据流 2 的流量小于聚合端口线速
预期结果： 1. 在步骤 4、6 中，测试仪表端口 B 应可以收到端口 A 发送的数据包； 2. 在步骤 7 中，测试仪表端口 B 应可以收到端口 A 发送的两个数据流
判定原则： 应符合预期结果要求，否则为不合格

6.5 802.1x

测试编号：16
测试项目：802.1x 本地认证
测试目的：检验 DUT 实现 802.1x 本地认证功能
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 配置 DUT 连接 PC 端口使用 802.1x 本地认证，配置相应的用户名和密码； 3. PC 不运行 802.1x 客户端情况下 Ping 服务器； 4. PC 运行 802.1x 客户端并输入错误用户名和密码情况下 Ping 服务器； 5. PC 运行 802.1x 客户端并输入正确用户名和密码情况下 Ping 服务器
预期结果： 1. 在步骤 3 和 4 中，PC 不能 Ping 通； 2. 在步骤 5 中，PC 能 Ping 通
判定原则： 应符合预期结果要求，否则为不合格

测试编号：17
测试项目：RADIUS 802.1x 认证（客户端）
测试目的：检验 DUT 作为 RADIUS 客户端实现 802.1x 用户的接入认证
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 配置 DUT 连接 PC 端口使用 802.1x 认证以及作为 RADIUS 客户端所指向的 RADIUS 服务器地址； 3. 配置相应的用户名和密码； 4. PC 不运行 802.1x 客户端情况下 Ping 服务器； 5. PC 运行 802.1x 客户端并输入错误用户名和密码情况下 Ping 服务器； 6. PC 运行 802.1x 客户端并输入正确用户名和密码情况下 Ping 服务器
预期结果： 1. 在步骤 4 和 5 中，PC 不能 Ping 通； 2. 在步骤 6 中，PC 能 Ping 通
判定原则： 应符合预期结果要求，否则为不合格

测试编号：18
测试项目：RADIUS 802.1x 认证（服务器端）
测试目的：检验 DUT 作为 RADIUS 服务器端实现 802.1x 用户的接入认证
测试配置：测试环境 3
测试过程： 1. 按测试环境连接设备； 2. 配置 DUT1 连接 PC 端口使用 802.1x 认证以及作为 RADIUS 客户端所指向的 RADIUS 服务器地址； 3. 配置 DUT2 作为 RADIUS 服务器及相应的用户名和密码； 4. PC 不运行 802.1x 客户端情况下 Ping 服务器； 5. PC 运行 802.1x 客户端并输入错误用户名和密码情况下 Ping 服务器； 6. PC 运行 802.1x 客户端并输入正确用户名和密码情况下 Ping 服务器
预期结果： 1. 在步骤 4 和 5 中，PC 不能 Ping 通服务器； 2. 在步骤 6 中，PC 能 Ping 通服务器
判定原则： 应符合预期结果要求，否则为不合格

6.6 MAC 地址数目限制

测试编号：19
测试项目：端口 MAC 地址数目限制
测试目的：检验 DUT 实现 MAC 地址数目限制功能
测试配置：测试环境 1
测试过程： 1. 按测试环境连接设备； 2. 配置 DUT 的端口 MAC 地址限制功能，限制的数目为 N； 3. 测试仪表端口 A 向端口 B 发送数据流，数据流的数目从 1 递增到 M（$M>N$）
预期结果： 在步骤 3 中，当数据流数目小于等于 N 时，测试仪表端口 B 应可以收到端口 A 发送的全部数据流；当数据流数目大于 N 时，测试仪表端口 B 只能收到 N 个数据流
判定原则： 应符合预期结果要求，否则为不合格

测试编号：20
测试项目：VLAN MAC 地址数目限制
测试目的：检验 DUT 实现 MAC 地址数目限制功能
测试配置：测试环境 1
测试过程： 1. 按测试环境连接设备； 2. 配置 DUT 的 VLAN MAC 地址限制功能，限制的数目为 N； 3. 测试仪表端口 A 向端口 B 发送数据流，数据流的数目从 1 递增到 M（$M>N$）
预期结果： 在步骤 3 中，当数据流数目小于等于 N 时，测试仪表端口 B 应可以收到端口 A 发送的全部数据流；当数据流数目大于 N 时，测试仪表端口 B 只能收到 N 个数据流
判定原则： 应符合预期结果要求，否则为不合格

6.7 MAC 地址绑定功能

测试编号：21
测试项目：MAC 地址绑定功能
测试目的：检验 DUT 实现 MAC 地址绑定功能
测试配置：测试环境 3
测试过程： 1. 按测试环境连接设备； 2. 配置 DUT 的 MAC 地址分别绑定端口、VLAN； 3. 测试测试仪表端口 A 发送两个数据流，其中数据流 1 的 MAC 地址已经绑定，数据流 2 的 MAC 地址没有绑定
预期结果： 在步骤 3 中，测试仪表端口 B 应可以收到端口 A 发送的数据流 1，不能收到数据流 2
判定原则： 应符合预期结果要求，否则为不合格

6.8 端口镜像

测试编号：22
测试项目：端口镜像
测试目的：检验 DUT 可以提供端口镜像功能
测试配置：测试环境 2
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 上配置端口镜像，镜像的源端口为接口 1，目的端口为接口 3； 3. 由测试仪表端口 A 向测试仪表端口 B 发送数据包； 4. 在 DUT 上配置端口镜像，镜像的源端口为接口 1 和接口 2，目的端口为接口 3，从测试仪表端口 A 和 B 互相发送数据包
预期结果： 1. 在步骤 3 中，从 DUT 接口 3 上也能观察到端口 A 发出的测试流量； 2. 在步骤 4 中，从 DUT 接口 3 上能够观察到端口 A 和端口 B 发出的测试流量
判定原则： 应符合预期结果要求，否则为不合格

6.9 广播风暴抑制

测试编号：23
测试项目：广播风暴抑制
测试目的：检验 DUT 对广播风暴的抑制功能
测试配置：测试环境 1
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 端口 1 上配置广播风暴抑制比 *N*（*N* 为端口线速的百分比）； 3. 测试仪表端口 A 以线速率发送广播包
预期结果： 从测试仪表上观察，端口 B 中收到的广播流速率为 *N*（误差不应超过 10%）
判定原则： 应符合预期结果要求，否则为不合格

7 控制平面安全测试

7.1 VLAN 安全测试

测试编号：24
测试项目：VLAN 数据泄漏测试
测试目的：检验 DUT 在大流量情况下是否可以保证 VLAN 的数据安全
测试配置：测试环境 1
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 上配置端口 1、端口 2 为 VLAN1，端口 3、端口 4 为 VLAN2； 3. 测试仪表端口 A 和 B 在 VLAN1 以线速率发送数据流，测试仪表端口 C 和 D 在 VLAN2 以线速率发送数据流量
预期结果： 在步骤 4 中，从测试仪表上观察，VLAN1 和 VLAN2 中不应收到对方的流量
判定原则： 应符合预期结果要求，否则为不合格

7.2 STP/RSTP 功能测试

测试编号：25
测试项目：RSTP 生成树功能测试
测试目的：验证生成树的产生 1
测试配置：测试环境 5
测试过程： 1. 按测试环境连接设备； 2. 配置生成树协议； 3. 流量发生器发送流量； 4. 验证只有一条链路可用； 5. 使用协议分析仪验证协议流程
预期结果： 只有一条链路可用
判定原则： 应符合预期结果要求，否则为不合格

测试编号：26
测试项目：RSTP 生成树功能测试
测试目的：验证生成树的产生 2
测试配置：测试环境 6
测试过程： 1. 按测试环境连接设备； 2. 配置生成树协议； 3. 流量发生器发送流量； 4. 验证只有一个交换机可用； 5. 使用协议分析仪验证协议流程
预期结果： 只有一条链路可用
判定原则： 应符合预期结果要求，否则为不合格

测试编号：27
测试项目：RSTP 生成树功能测试
测试目的：重新生成生成树 1
测试配置：测试环境 5
测试过程： 1. 按测试环境连接设备； 2. 配置生成树协议； 3. 流量发生器发送流量； 4. 验证只有一条链路可用； 5. 使用协议分析仪验证协议流程； 6. 断开所使用的链路
预期结果： 另一条链路恢复使用
判定原则： 应符合预期结果要求，否则为不合格

测试编号：28
测试项目：RSTP 生成树功能测试
测试目的：重新生成生成树 2
测试配置：测试环境 6
测试过程： 1. 按测试环境连接设备； 2. 配置生成树协议； 3. 流量发生器发送流量； 4. 验证只有一个交换机可用； 5. 使用协议分析仪验证协议流程； 6. 关闭所使用的交换机
预期结果： 另一个交换机恢复使用
判定原则： 应符合预期结果要求，否则为不合格

测试编号：29
测试项目：Root Guard 功能测试
测试目的：验证 DUT 支持 Root Guard 功能
测试配置：测试环境 7
测试过程： 1. 按测试环境连接设备； 2. 配置交换机 1 生成树优先级为 1，交换机 2 生成树优先级为 2，交换机 3 生成树优先级为 3，交换机 4 生成树优先级为 0，配置交换机 1 的 Root Guard 功能； 3. 交换机 1、2、3 加电； 4. 交换机 4 加电，重新进行 STP 的计算
预期结果： 在步骤4之后，交换机1仍是Root交换机
判定原则： 应符合预期结果要求，否则为不合格

测试编号：30
测试项目：BPDU Guard 功能测试
测试目的：验证 DUT 支持 BPDU Guard 功能
测试配置：测试环境 7
测试过程： 1. 按测试环境连接设备； 2. 配置交换机 1 生成树优先级为 1，交换机 2 生成树优先级为 2，交换机 3 生成树优先级为 3，交换机 4 生成树优先级为 0，关闭交换机 3 的 BPDU Guard 功能； 3. 交换机 1、2、3、4 加电； 4. 配置交换机 3 的 BPDU Guard 功能； 5. 交换机 1、2、3、4 重新加电
预期结果： 1. 在步骤3之后，交换机4是Root交换机； 2. 在步骤5之后，交换机1是Root交换机
判定原则： 应符合预期结果要求，否则为不合格

7.3 IGMP Snooping 功能测试

测试编号：31
测试项目：IGMP Snooping 功能测试
测试目的：验证 DUT 支持 IGMP Snooping 功能
测试配置：测试环境 8
测试过程： 1. 按测试环境连接设备； 2. 测试仪表端口 1 仿真组播源 A.B.C.D； 3. 关闭交换机的 IGMP Snooping 功能； 4. 测试仪表端口 B 申请加入组播 A.B.C.D； 5. 测试仪表端口 A 发送组播数据流； 6. 配置交换机的 IGMP Snooping 功能，测试仪表端口 B 重新申请加入组播 A.B.C.D； 7. 测试仪表端口 A 发送组播数据流
预期结果： 1. 在步骤5中，测试仪表端口B和端口C都可以收到组播流； 2. 在步骤7中，测试仪表端口B可以收到组播流，端口C收不到组播流
判定原则： 应符合预期结果要求，否则为不合格

7.4 DHCP Snooping 功能测试

测试编号：32
测试项目：DHCP Snooping 功能测试
测试目的：验证 DUT 支持 DHCP Snooping 功能
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 配置交换机的 DHCP Snooping 功能
预期结果： 在步骤2中，交换机可以记录DHCP的流程
判定原则： 应符合预期结果要求，否则为不合格

8 管理平面安全测试

8.1 用户访问控制

测试编号：33
测试项目：用户访问控制功能测试
测试目的：检验 DUT 的用户访问控制功能
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 上为远程连接配置用户和相应的密码，由 PC 向 DUT 发起 Telnet 连接，验证接入控制的有效性； 3. 在 DUT 上将用户认证方式改为通过认证服务器认证，在认证服务器上配置相应用户，由 PC 向 DUT 发起 Telnet 连接，验证接入控制的有效性
预期结果： 在步骤 2 和 3 中，Telnet 可正常建立
判定原则： 应符合预期结果要求，否则为不合格

测试编号：34
测试项目：用户的分级分权控制
测试目的：检验 DUT 的用户分级分权控制功能
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 或认证服务器上配置两个用户 User1 和 User2； 3. 在 DUT 上为 User1 和 User2 分配不同的权限，能够对 DUT 进行不同级别的控制； 4. 用 User1 和 User2 分别访问 DUT，并对 DUT 进行操作
预期结果： 在步骤 4 中，每个用户只能进行其级别所允许的操作
判定原则： 应符合预期结果要求，否则为不合格

8.2 Telnet

测试编号：35
测试项目：Telnet 访问连接数量限制
测试目的：检验 DUT 能够限制 Telnet 访问的数目
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 上配置 Telnet 访问连接数量限制，最大连接数为 N； 3. 用 M（$M>N$）个客户端对 DUT 进行 Telnet 访问
预期结果： 在步骤 3 中，第 $N+1$ 个用户之后应访问不成功
判定原则： 应符合预期结果要求，否则为不合格

8.3 Web 管理功能测试

测试编号：36
测试项目：Web 管理功能
测试目的：检验 DUT 能否支持 Web 管理
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 上启用 Web 服务； 3. 使用客户端 PC 以 https 登录 DUT
预期结果： 在步骤 3 中，PC 应能用 https 正常登录 DUT
判定原则：
应符合预期结果要求，否则为不合格

8.4 SSH

测试编号：37
测试项目：SSH 连接建立测试
测试目的：检验 DUT 能否正常建立 SSH 连接
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 上启用 SSH； 3. 使用客户端以正确的 SSH 配置登录 DUT
预期结果： 在步骤 3 中，DUT 应能正常建立 SSH 连接
判定原则：
应符合预期结果要求，否则为不合格

测试编号：38
测试项目：SSH 连接数量限制
测试目的：检验 DUT 能够限制 SSH 连接的数目
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 上配置 SSH 连接数量限制，最大连接数为 N； 3. 用 M（$M>N$）个客户端对 DUT 进行 SSH 连接
预期结果： 在步骤 3 中，第 $N+1$ 个用户之后访问应不成功
判定原则： 应符合预期结果要求，否则为不合格

测试编号：39
测试项目：SSH 协议版本兼容测试
测试目的：检验 DUT 对 SSH 协议版本进行兼容处理
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 上启用 SSH，并配置 SSH 版本 2 与版本 1.x 的兼容； 3. 使用客户端，分别以 SSHv2 和 SSHv1.x 与 DUT 建立 SSH 连接
预期结果： 在步骤 3 中，DUT 对 SSHv2 和 SSHv1.x 的连接请求均能进行处理
判定原则： 应符合预期结果要求，否则为不合格

测试编号：40
测试项目：算法协商测试
测试目的：检验 DUT 支持 SSH 协议中各种算法的协商
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 上启用 SSH； 3. 从客户端发送 SSH_MSG_KEXINIT 消息进行算法协商
预期结果： 在步骤 3 中，DUT 应支持 3DES-CBC 加密算法（Blowfish-CBC、IDEA-CBC、CAST128-CBC、AES128-CBC、AES256-CBC 算法为可选）；DUT 应支持 diffie-hellman-group1-sha1 的 Diffie-Hellman（Oakley 组 2（1024bit MODP Group，RFC2409）、Oakley 组 14（2048bit MODP Group，RFC3526））密钥交换算法；DUT 应支持 HMAC-SHA1 认证算法（HMAC-SHA1-96 为可选）；DUT 应支持 SSH-DSS 公钥算法或 SSH-RSA
判定原则： 应符合预期结果要求，否则为不合格

测试编号：41
测试项目：定期重协商测试
测试目的：检验 DUT 支持定期重协商
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 上启用 SSH
预期结果： DUT 应可以配置定期重协商（根据通信的总数据量或时间），并在到达期限时进行算法的重协商
判定原则： 应符合预期结果要求，否则为不合格

测试编号：42
测试项目：SSH 中断消息测试 1
测试目的：检验 DUT 支持中断消息（SSH_MSG_DISCONNET）的主动发送
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 上启用 SSH； 3. 采用算法协商过程所得到的算法组合进行通信； 4. 在客户端主动改变加密/认证/压缩算法
预期结果： DUT 应发送 SSH_MSG_DISCONNET 消息，并立即中断连接
判定原则： 应符合预期结果要求，否则为不合格

测试编号：43
测试项目：SSH 中断消息测试 2
测试目的：检验 DUT 支持中断消息（SSH_MSG_DISCONNET）的处理
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 上启用 SSH； 3. 采用算法协商过程所得到的算法组合进行通信； 4. 从客户端发送中断消息
预期结果： DUT 应立即中断连接
判定原则： 应符合预期结果要求，否则为不合格

测试编号：44
测试项目：用户认证方式测试
测试目的：检验 DUT 支持用户认证
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 上启用 SSH； 3. 完成算法协商过程； 4. PC 登录 DUT
预期结果： PC 可以登录 DUT
判定原则： 应符合预期结果要求，否则为不合格

8.5 SNMPv3

测试编号：45
测试项目：SNMPv3 Get 原语功能测试
测试目的：检验 DUT 支持 SNMPv3 Get 原语功能
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 使用终端上的 SNMPv3 客户端软件读取 DUT 的系统描述； 3. 使用终端上的 SNMPv3 客户端软件读取 DUT 上不存在的对象
预期结果： 1. 在步骤 2 中应得到正确的系统描述； 2. 在步骤 3 中应得到错误状态“noSuchName”以及相应的错误索引
判定原则： 应符合预期结果要求，否则为不合格

测试编号：46
测试项目：SNMPv3 Get Next 原语功能测试
测试目的：检验 DUT 支持 SNMPv3 Get Next 原语功能
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 使用终端上的 SNMPv3 客户端软件读取 DUT 的系统描述； 3. 使用终端上的 SNMPv3 客户端软件的 Get Next 原语读取下一属性
预期结果： 1. 在步骤 2 中应得到正确的系统描述； 2. 在步骤 3 中应得到下一属性的值
判定原则： 应符合预期结果要求，否则为不合格

测试编号：47
测试项目：SNMPv3 Get Bulk 原语功能测试
测试目的：检验 DUT 支持 SNMPv3 Get Bulk 原语功能
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 终端上的 SNMPv3 客户端以 Get Bulk 命令读取 DUT 的系统描述
预期结果： 在步骤 2 中应得到正确的批量系统描述值
判定原则： 应符合预期结果要求，否则为不合格

测试编号：48
测试项目：SNMPv3 Set 原语功能测试
测试目的：检验 DUT 支持 SNMPv3 Set 原语功能
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 使用终端上的 SNMPv3 客户端以 Set 命令设置 DUT 的系统描述； 3. 读取 DUT 的系统描述
预期结果： 在步骤 3 中应得到重新设置的系统描述值
判定原则： 应符合预期结果要求，否则为不合格

测试编号：49
测试项目：SNMPv3 Trap 功能测试
测试目的：检验 DUT 支持 SNMPv3 Trap 原语功能
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 配置 DUT，使其在设备冷启动时向网管工作站发送 Trap（ColdStart），并冷启动设备； 3. 配置 DUT，使其在设备热启动时向网管工作站发送 Trap（WarmStare），并热启动设备； 4. 配置 DUT，使其在设备链路连接失败时向网管工作站发送 Trap（LinkDown），并断开某一接口； 5. 配置 DUT，使其在设备链路恢复正常时向网管工作站发送 Trap（LinkUp），并使链路恢复正常； 6. 配置 DUT，使其在设备鉴权失败时向网管工作站发送 Trap（AuthenticationFailure），并用错误的用户名/密码登录设备
预期结果： 在步骤 2~6 中应得到正确的 Trap 信息
判定原则： 应符合预期结果要求，否则为不合格

测试编号：50
测试项目：SNMPv3 安全性测试
测试目的：检验 DUT 支持 SNMPv3 不同的安全级别
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 上配置 SNMPv3 工作在 noAuthnoPriv 方式，使用 SNMPv3 客户端以明文方式对 DUT 进行 SNMP 操作； 3. 在 DUT 上配置 SNMPv3 工作在 AuthnoPriv 方式，SNMPv3 客户端使用 HMAC-MD5（HMAC-SHA 为可选）认证； 4. 算法与 DUT 进行认证，并进行 SNMP 操作； 5. 在 DUT 上配置 SNMPv3 工作在 AuthPriv 方式，SNMPv3 客户端使用 HMAC-MD5（HMAC-SHA 为可选）； 6. 认证算法与 DUT 进行认证，使用 DES-CBC 加密算法对数据进行加密，并进行 SNMP 操作
预期结果： 在步骤 2~4 中，应能正常进行 SNMP 操作
判定原则： 应符合预期结果要求，否则为不合格

测试编号：51
测试项目：对 SNMPv3 管理工作站的验证
测试目的：检验 DUT 支持对 SNMPv3 管理工作站的验证
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 在 DUT 上配置 SNMPv3 管理工作站地址为 X.X.X.X； 3. 在 DUT 上配置与管理工作站（PC）间的地址为 Y.Y.Y.Y，配置管理工作站地址为 Y.Y.Y.Y+1
预期结果： 在步骤 3 中，管理工作站对 DUT 无法进行 SNMP 操作
判定原则： 应符合预期结果要求，否则为不合格

8.6 安全审计

测试编号：52
测试项目：安全日志功能测试
测试目的：检验 DUT 支持安全日志功能
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 从终端以错误的账号登录 DUT
预期结果： 1. DUT 应在本地安全日志中对非法登录进行记录； 2. DUT 可以将安全日志输出至日志服务器； 3. 日志内容应符合《高端路由器安全技术要求》8.2.5.1 节中的规定（安全事件来源、发生时间、事件描述等）
判定原则： 应符合预期结果要求，否则为不合格

测试编号：53
测试项目：操作日志功能测试
测试目的：检验 DUT 支持操作日志功能
测试配置：测试环境 4
测试过程： 1. 按测试环境连接设备； 2. 从终端以合法用户登录 DUT； 3. 进行各种配置操作
预期结果： 1. DUT 应在本地操作日志中对用户登录 IP 地址、登录时间、所进行的操作、退出时间进行记录； 2. DUT 可以将操作日志输出至日志服务器
判定原则： 应符合预期结果要求，否则为不合格