

ICS 33 040 40
M 32



中华人民共和国通信行业标准

YD/T 1659-2007

宽带网络接入服务器安全测试方法

Testing Methods of Security for Broadband Network Access Server

2007-07-20 发布

2007-12-01 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 缩略语	1
4 测试环境配置	2
5 数据转发平面安全测试	3
5.1 IPSec协议测试（可选）	3
5.2 L2TP协议功能测试	3
5.3 常见网络攻击抵抗能力测试	4
5.4 uRPF功能测试	6
5.5 访问控制列表（ACL）功能测试	8
5.6 网络地址翻译（NAT）测试（可选）	12
5.7 流量控制 / 分类功能测试	14
6 控制平面安全测试	17
6.1 IP地址分配控制	17
6.2 防止IP地址盗用功能	19
6.3 用户接入认证与授权控制	20
6.4 路由协议安全测试	23
6.5 TCP/IP协议安全测试	31
6.6 VPN安全测试	32
6.7 路由过滤功能测试	33
6.8 GTSM功能测试	35
7 管理平面的安全测试	36
7.1 端口镜像	36
7.2 访问控制安全测试	36
7.3 用户密码保护功能测试	43
7.4 SNMP安全功能测试	43
7.5 安全审计功能测试	47

前 言

本标准是“宽带网络接入服务器安全”系列标准之一。该系列标准预计的结构及名称如下：

1. YD/T 1658-2007 宽带网络接入服务器安全技术要求
2. YD/T 1659-2007 宽带网络接入服务器安全测试方法

其中，YD/T 1658-2007 《宽带网络接入服务器安全技术要求》是本标准的配套标准。

本标准由中国通信标准化协会提出并归口。

本标准主要起草单位：信息产业部电信研究院

本标准主要起草人：马军锋、魏 亮

宽带网络接入服务器安全测试方法

1 范围

本标准规定了宽带网络接入服务器涉及安全方面的测试内容，包括数据转发平面安全测试、控制平面测试和管理平面安全测试。

本标准适用于宽带网络接入服务器。

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 1265-2003 网络接入服务器（NAS）测试方法

YD/T 1467-2006 IP安全协议（IPSec）测试方法

3 缩略语

下列缩略语适用于本标准。

ACL	Access Control List	访问控制列表
ATU-R	ADSL Transceiver Unit Remote	非对称数字用户环路远端终止单元
BGP	Border Gateway Protocol	边界网关协议
BNAS	Broadband Network Access Server	宽带网络接入服务器
CE	Customer Edge	用户边界设备
DSLAM	Digital Subscriber Line (DSL) Access Module	数字用户线接入模块
DUT	Device Under Test	被测设备
EBGP	Exterior Border Gateway Protocol	外部边界网关协议
GTSM	Generalized TTL Security Mechanism	通用TTL安全机制
IBGP	Interior Border Gateway Protocol	内部边界网关协议
ICMP	Internet Control Message Protocol	网络控制报文协议
IP	Internet Protocol	网际互连协议
IPSec	IP Security	IP安全机制
IS-IS	Intermediate System to Intermediate System Protocol	中间系统到中间系统协议
L2TP	Layer Two Tunneling Protocol	二层隧道协议
MPLS	Multi-Protocol Label Switch	多协议标记交换
NAT	Network Address Translation	网络地址转换
OSPF	Open Shortest Path First	开放最短路径优先协议

PE	Provider Edge	网络边界设备
PPP	Point to Point Protocol	点到点协议
RADIUS	Remote Authentication Dial In User Service	远程验证用户拨入服务
RIP	Route Information Protocol	路由信息协议
SSH	Secure Shell	安全外壳程序协议
TCP	Transport Control Protocol	传输控制协议
UDP	User Data Protocol	用户数据报协议
uRPF	Unicast Reverse Path Forwarding	单播逆向路径转发
VPN	Virtual Private Network	虚拟专用网

4 测试环境配置

测试环境配置如图1~图9。

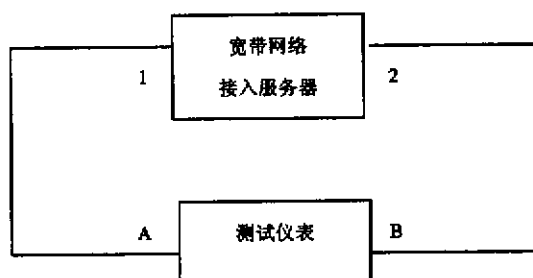


图1 测试配置环境1

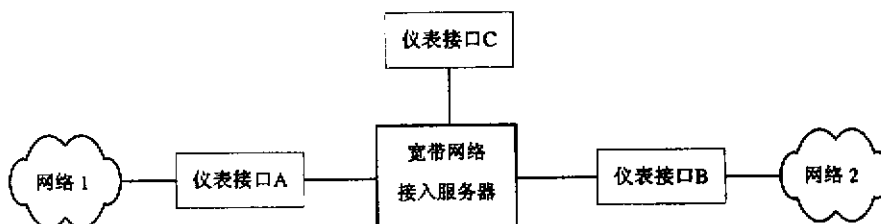


图2 测试配置环境2

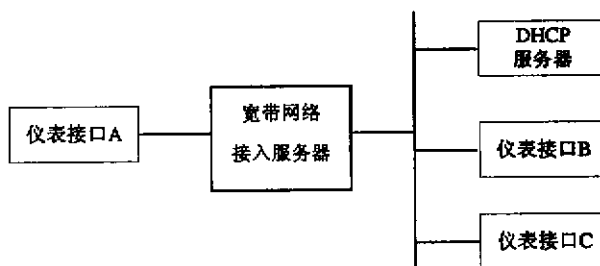


图3 测试配置环境3

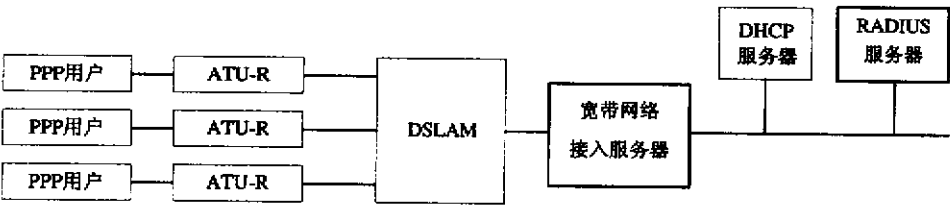


图4 测试配置环境4

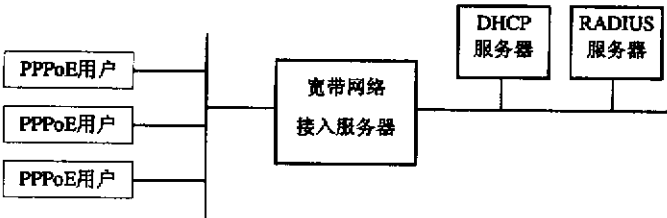


图5 测试配置环境5

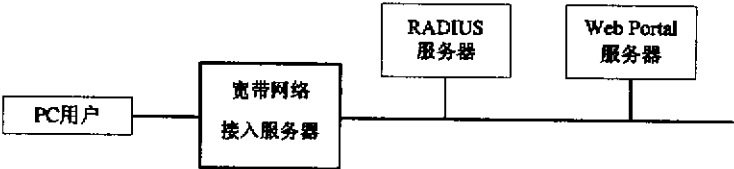


图6 测试配置环境6

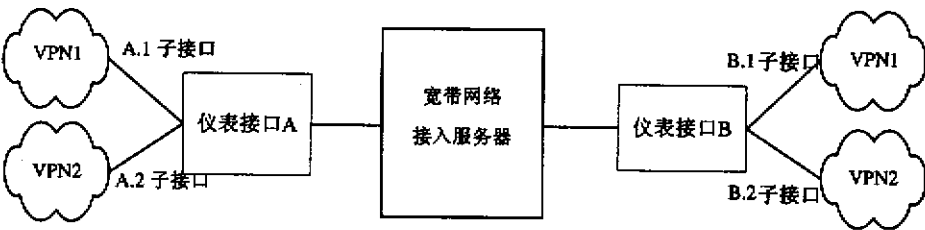


图7 测试配置环境7

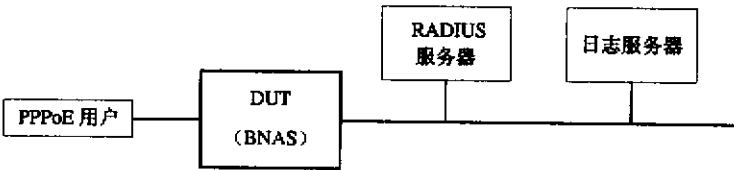


图8 测试配置环境8

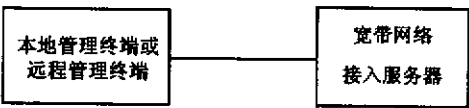


图9 测试配置环境9

5 数据转发平面安全测试

5.1 IPSec 协议测试（可选）

IPSec协议测试内容参见YD/T 1467-2006《IP安全协议（IPSec）测试方法》。

5.2 L2TP 协议功能测试

L2TP协议功能测试内容参见YD/T 1265-2003 《网络接入服务器（NAS）测试方法》。

5.3 常见网络攻击抵抗能力测试

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：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 从测试仪表 A 接口向 B 接口线速发送背景数据流； 3) 在 DUT1 接口启用路由协议，测试仪表 A 接口通告路由信息
预期结果： DUT 能够更新路由表，不受背景流量的影响
判定原则： 应符合预期结果要求，否则不合格

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：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 从测试仪表 A 接口向 B 接口发送小于接口速率的背景数据流； 3) 由仪表接口 A 以接口剩余带宽速率向 DUT1 接口发送报文长度(包括 IP 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，由仪表 A 接口向 DUT 环回地址发送多个 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，由仪表 A 接口向 B 接口发送链路层错误（如以太网的 FCS 错误帧）报文； 6) 停止步骤 5 中报文的发送，由仪表 A 接口向 B 接口发送长度小于 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，由仪表 A 接口向 B 接口发送长度大于 1518 字节（以太网链路）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，错误的数据帧应被丢弃，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，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，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：测试配置环境 2
测试过程： <ol style="list-style-type: none"> 1) 按测试环境连接设备； 2) 在仪表 B 接口与直连的 DUT 接口间启用路由协议（如 OSPF），并通过仪表仿真向 DUT 通告到网络 2 的路由； 3) 从测试仪表 A 接口向网络 2 中的某个 IP 地址以小于接口线速的速率发送背景流量，并验证仪表 B 接口能够正常接收； 4) 从测试仪表 C 接口向 DUT 环回地址以线速发送 ICMP Echo Request 数据包； 5) 停止步骤 4 中流量的发送，从测试仪表接口 C 向网络 2 中的某个 IP 地址以接口线速发送 ICMP Echo Request 数据包
预期结果： <ol style="list-style-type: none"> 1) 在步骤 4 中，DUT 应对超量的 ICMP 报文进行丢弃或限速，记录攻击对背景流量的影响； 2) 在步骤 5 中，DUT 应对超量 ICMP 报文进行丢弃或限速，记录攻击对背景流量的影响
判定原则： <p>应符合预期结果要求，否则不合格</p>

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：测试配置环境 2
测试过程： <ol style="list-style-type: none"> 1) 按测试环境连接设备； 2) 在仪表 A、B 接口分别与直连的 DUT 接口间启用路由协议，并通过仪表仿真向 DUT 通告到网络 1 和 2 的路由； 3) 从测试仪表 A 接口向网络 2 中的某个 IP 地址以小于接口线速的速率发送背景流量，并验证仪表 B 接口能够正常接收； 4) 从测试仪表 A 接口向网络 2 以剩余带宽发送 TCP SYN 数据包，源地址属于网络 1 的 IP 地址； 5) 停止步骤 4 中流量的发送，从测试仪表接口 A 向 DUT 的环回地址以剩余带宽发送 TCP SYN 数据包，源地址属于网络 1 的 IP 地址； 6) 停止步骤 5 中流量的发送，从测试仪表接口 A 向 DUT 的环回地址以剩余带宽发送 TCP SYN 数据包，源地址为 DUT 不可达的 IP 地址
预期结果： <ol style="list-style-type: none"> 1) 在步骤 4 和 5，DUT 应对过量的 TCP SYN 数据包进行丢弃或降低优先级的排队处理，记录攻击对背景流量的影响； 2) 在步骤 6，DUT 应丢弃 TCP SYN 数据包，记录攻击对背景流量的影响
判定原则： <p>DUT 能够对过量的 TCP SYN 数据包进行丢弃或者降低优先级的排队处理，背景流的流量和时延不受影响</p>

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：测试配置环境 2
测试过程： 1) 按测试环境连接设备； 2) 测试仪表 A、B 接口分别与其直连的 DUT 接口启用路由协议（如 OSPF），并向 DUT 通告到网络 1 和网络 2 的路由； 3) 从测试仪表接口 A 向网络 2 中的某个地址以小于接口速率的流量发送背景流量，并验证仪表接口 B 上能够正常接收； 4) 从测试仪表接口 C 向网络 1 中的某个 IP 地址以接口线速发送 ICMP Echo Request 数据包，数据包源地址为网络 2 的有限广播地址； 5) 停止步骤 4 中流量的发送，从测试仪表接口 C 向 DUT 的环回地址以接口线速发送 ICMP Echo Request 数据包，数据包源地址为网络 2 的有限广播地址； 6) 停止步骤 5 中流量的发送，从测试仪表接口 C 向网络 1 以接口线速发送 ICMP Echo Request 数据包，数据包源地址为网络 2 中的某个 IP 地址，目的地址为网络 1 的有限广播地址
预期结果： 从步骤 4 到 6 中，DUT 应对 ICMP 报文进行丢弃，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，否则不合格

5.4 uRPF 功能测试

测试编号：6
测试项目：严格 uRPF 功能测试（可选）
测试目的：检验 DUT 严格 uRPF 功能的实现
测试配置：测试配置环境 2
测试过程： 1) 按测试环境连接设备； 2) 测试仪表 B 接口与其直连的 DUT 接口启用路由协议（如 OSPF），并向 DUT 通告到网络 2 的路由，在 DUT 上配置静态路由 A.A.A.0/24，下一跳指向仪表的 C 接口，发送流量验证路由的有效性； 3) DUT 启用严格 uRPF； 4) 从测试仪表 A 接口发送到网络 2 中某个 IP 地址的数据流，数据包的源地址与接口 A 直连的 DUT 的接口地址在同一网段； 5) 停止步骤 4 数据流的发送，从仪表接口 A 发送到网络 2 中某个 IP 地址的数据流，数据包的源地址为 A.A.A.X； 6) 停止步骤 5 数据流的发送，从仪表接口 A 发送到网络 2 中某个 IP 地址的数据流，数据包的源地址为 DUT 不可达网络的 IP 地址
预期结果： 1) 在步骤 4 中，仪表接口 B 应能够收到测试数据包； 2) 在步骤 5 和 6 中，仪表接口 B 不能收到测试数据包
判定原则： 应符合预期结果要求，否则不合格
测试结果：

测试编号：7
测试项目：松散 uRPF 功能测试（可选）
测试目的：检验 DUT 松散 uRPF 功能的实现
测试配置：测试配置环境 2
测试过程： 1) 按测试环境连接设备； 2) 测试仪表 B 接口与其直连的 DUT 接口启用路由协议（如 OSPF），并向 DUT 通告到网络 2 的路由，在 DUT 上配置静态路由 A.A.A.0/24，下一跳指向仪表的 C 接口，发送流量验证路由的有效性； 3) DUT 启用松散 uRPF； 4) 从测试仪表 A 接口发送到网络 2 中某个 IP 地址的数据流，数据包的源地址与接口 A 直连的 DUT 的接口地址在同一网段； 5) 停止步骤 4 数据流的发送，从仪表接口 A 发送到网络 2 中某个 IP 地址的数据流，数据包的源地址为 A.A.A.X； 6) 停止步骤 5 数据流的发送，从仪表接口 A 发送到网络 2 中某个 IP 地址的数据流，数据包的源地址为 DUT 不可达网络的 IP 地址
预期结果： 1) 在步骤 4 和 5 中，仪表接口 B 应能够收到测试数据包； 2) 在步骤 6 中，仪表接口 B 不能收到测试数据包
判定原则： 应符合预期结果要求，否则不合格

测试编号：8
测试项目：基于 ACL 的 uRPF 功能测试（可选）
测试目的：检验 DUT 基于 ACL 的 uRPF 功能实现
测试配置：测试配置环境 2
测试过程： 1) 按测试环境连接设备； 2) 测试仪表 B 接口与其直连的 DUT 接口启用路由协议（如 OSPF），并向 DUT 通告到网络 2 的路由，在 DUT 上配置静态路由 C.C.C.0/24，下一跳指向仪表的 A 接口，发送流量验证路由的有效性； 3) 在 DUT 上启用基于 ACL 的 uRPF，并配置 ACL 禁止 C.C.C.Y 的流量通过 DUT； 4) 从测试仪表 A 接口发送到网络 2 中某个 IP 地址的数据流，数据包的源地址与接口 A 直连的 DUT 的接口地址在同一网段； 5) 停止步骤 4 数据流的发送，从仪表接口 A 发送到网络 2 中某个 IP 地址的数据流，数据包的源地址为 C.C.C.X； 6) 停止步骤 5 数据流的发送，从仪表接口 A 发送到网络 2 中某个 IP 地址的数据流，数据包的源地址为 C.C.C.Y
预期结果： 1) 在步骤 4 和 5 中，仪表接口 B 应能够收到测试数据包； 2) 在步骤 6 中，仪表接口 B 不能收到测试数据包
判定原则： 应符合预期结果要求，否则不合格

5.5 访问控制列表（ACL）功能测试

测试编号：9
测试项目：基于源地址的 ACL 测试
测试目的：检验 DUT 是否实现基于源地址的 ACL 过滤
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 上配置基于源地址的 ACL 拒绝条目； 3) 从仪表 A 接口发送到仪表 B 接口符合过滤条件的数据流； 4) 从仪表 A 接口发送到仪表 B 接口不符合过滤条件的数据流
预期结果： 1) 仪表 B 接口无法收到测试数据流； 2) 仪表 B 接口能够收到测试数据流
判定原则： 应符合预期结果要求，否则不合格

测试编号：10
测试项目：基于目的地址的 ACL 测试
测试目的：检验 DUT 是否实现基于目的地址的 ACL 过滤
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 上配置基于目的地址的 ACL 拒绝条目； 3) 从仪表 A 接口发送到仪表 B 接口符合过滤条件的 IP 数据流； 4) 从仪表 A 接口发送到仪表 B 接口不符合过滤条件的 IP 数据流
预期结果： 1) 步骤 3，仪表 B 接口无法收到测试数据流； 2) 步骤 4，仪表 B 接口能够收到测试数据流
判定原则： 应符合预期结果要求，否则不合格

测试编号：11
测试项目：基于协议的 ACL 测试
测试目的：检验 DUT 是否实现基于协议的 ACL 过滤
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 上配置基于协议的 ACL 拒绝条目； 3) 从仪表 A 接口发送到仪表 B 接口符合过滤条件的 IP 数据流； 4) 从仪表 A 接口发送到仪表 B 接口不符合过滤条件的 IP 数据流
预期结果： 1) 步骤 3，仪表 B 接口无法收到测试数据流； 2) 步骤 4，仪表 B 接口能够收到测试数据流
判定原则： 应符合预期结果要求，否则不合格

测试编号：12
测试项目：基于源接口的 ACL 测试
测试目的：检验 DUT 是否实现基于源接口的 ACL 过滤
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 上配置基于源接口的 ACL 拒绝条目； 3) 从仪表 A 接口发送到仪表 B 接口符合过滤条件的 IP 数据流； 4) 从仪表 A 接口发送到仪表 B 接口不符合过滤条件的 IP 数据流
预期结果： 1) 步骤 3，仪表 B 接口无法收到测试数据流； 2) 步骤 4，仪表 B 接口能够收到测试数据流
判定原则： 应符合预期结果要求，否则不合格

测试编号：13
测试项目：基于目的接口的 ACL 测试
测试目的：检验 DUT 是否实现基于目的接口的 ACL 过滤
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 上配置基于目的接口的 ACL 拒绝条目； 3) 从仪表 A 接口发送到仪表 B 接口符合过滤条件的 IP 数据流； 4) 从仪表 A 接口发送到仪表 B 接口不符合过滤条件的 IP 数据流
预期结果： 1) 步骤 3，仪表 B 接口无法收到测试数据流； 2) 步骤 4，仪表 B 接口能够收到测试数据流
判定原则： 应符合预期结果要求，否则不合格

测试编号：14
测试项目：基于五元组的 ACL 测试
测试目的：检验 DUT 是否实现基于五元组的 ACL 过滤
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 上配置基于五元组（源、目的地址，源、目的接口，协议号）的 ACL 拒绝条目； 3) 从仪表 A 接口发送到仪表 B 接口符合过滤条件的 IP 数据流； 4) 从仪表 A 接口发送到仪表 B 接口不符合过滤条件的 IP 数据流
预期结果： 1) 步骤 3，仪表 B 接口无法收到测试数据流； 2) 步骤 4，仪表 B 接口能够收到测试数据流
判定原则： 应符合预期结果要求，否则不合格

测试编号：15
测试项目：全局 ACL 测试
测试目的：检验 DUT 是否实现全局 ACL 的配置模式
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) DUT 在全局模式下配置 ACL 拒绝条目； 3) 从仪表 A 接口发送到仪表 B 接口符合过滤条件的 IP 数据流； 4) 从仪表 A 接口发送到仪表 B 接口不符合过滤条件的 IP 数据流
预期结果： 1) 步骤 3，仪表 B 接口无法收到测试数据流； 2) 步骤 4，仪表 B 接口能够收到测试数据流
判定原则： 应符合预期结果要求，否则不合格

测试编号：16
测试项目：配置 ACL 情况下的转发性能
测试目的：测试 DUT 在配置 ACL（五元组）情况下的转发性能
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 上配置基于五元组（源、目的地址，源、目的接口，协议号）的 ACL 拒绝条目； 3) 从仪表 A 接口以线速发送到仪表 B 接口不符合过滤条件的 IP 数据流
预期结果： 在配置 ACL 情况下，DUT 的转发性能没有较大变化
判定原则： DUT 的吞吐量和时延不受 ACL 的太大影响

5.6 网络地址翻译（NAT）测试（可选）

测试编号：17
测试项目：静态 NAT 测试
测试目的：检验 DUT 是否实现静态 NAT 地址翻译功能
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 上配置静态 NAT 地址翻译策略； 3) 从仪表 A 接口以不同源地址发送到仪表 B 接口符合 NAT 策略的 IP 数据流
预期结果： 仪表 B 接口能够收到测试数据流，并且源地址被修改为静态 NAT 翻译后的地址
判定原则： 应符合预期结果要求，否则不合格

测试编号：18
测试项目：动态 NAT 测试
测试目的：检验 DUT 是否实现动态 NAT 地址翻译功能
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 上配置动态 NAT 地址翻译策略； 3) 从仪表 A 接口以不同源地址发送到仪表 B 接口符合 NAT 策略的 IP 数据流
预期结果： 仪表 B 接口能够收到测试数据流，并且源地址属于 IP 地址池中的地址
判定原则： 应符合预期结果要求，否则不合格

测试编号：19
测试项目：接口地址翻译（PAT）测试
测试目的：检验 DUT 是否实现接口地址翻译功能
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 上配置 PAT 地址翻译策略； 3) 从仪表 A 接口以相同源地址、不同源接口发送到仪表 B 接口符合 PAT 策略的 UDP 数据流
预期结果： 仪表 B 接口能够收到测试数据流，源接口符合 PAT 配置策略
判定原则： 应符合预期结果要求，否则不合格

测试编号：20
测试项目：网络地址/接口翻译（NATPT）测试
测试目的：检验 DUT 是否实现 NATPT 翻译功能
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 上配置 NATPT 地址翻译策略； 3) 从仪表 A 接口发送到仪表 B 接口符合 NATPT 配置策略的 UDP 数据流
预期结果： 仪表 B 接口能够收到测试数据流，并且源地址、源接口符合 NATPT 配置策略
判定原则： 应符合预期结果要求，否则不合格

5.7 流量控制/分类功能测试

测试编号：21
测试项目：流量限速（CAR）功能测试
测试目的：检验 DUT 流量限速功能
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 接口 1 上配置流量限速 M ， M 小于接口的速率； 3) 从仪表 A 接口以大于 M 的速率向 B 接口发送数据流
预期结果： 仪表 B 接口能够以 M 的速率（误差 $<10\%$ ）接收数据流
判定原则： 应符合预期结果要求，否则不合格

测试编号：22
测试项目：流量分类功能测试_1
测试目的：检验 DUT 基于源 IP 地址段的流分类功能
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 上配置基于网段 A.A.A.0/24 的流分类策略，对命中的数据流采用流量限制，限制速率为 M ， M 小于接口线速； 3) 从测试仪表 A 接口以源地址为 A.A.A.X/24 线速发送到接口 B 的数据流； 4) 停止步骤 4 数据流的发送，从接口 A 以线速向接口 B 发送不符合分类策略的数据流
预期结果： 1) 在步骤 3 接口 B 能够以 M 速率（误差 $<10\%$ ）接收数据流； 2) 在步骤 4 接口 B 能够以线速接收数据流
判定原则： 应符合预期结果要求，否则不合格

测试编号：23
测试项目：流量分类功能测试_2
测试目的：检验 DUT 基于目的 IP 地址段的流分类功能
测试配置：测试配置环境 1
测试过程： <ol style="list-style-type: none"> 1) 按测试环境连接设备； 2) 在 DUT 和测试仪表 B 接口启用路由协议（如 BGP），注入路由 A.A.A.0/24； 3) 在 DUT 上配置基于网段 A.A.A.0/24 的流分类策略，对命中的数据流采用流量限制，限制速率为 M，M 小于接口线速； 4) 从测试仪表 A 接口以线速发送到目的地址为 A.A.A.X/24 的数据流； 5) 停止步骤 4 数据流的发送，从接口 A 以线速向接口 B 发送不符合分类策略的数据流
预期结果： <ol style="list-style-type: none"> 1) 在步骤 4 接口 B 能够以 M 速率（误差<10%）接收数据流； 2) 在步骤 5 接口 B 能够以线速接收数据流
判定原则： <p>应符合预期结果要求，否则不合格</p>

测试编号：24
测试项目：流量分类功能测试_3
测试目的：检验 DUT 基于 IP 五元组（源地址、目的地址、源接口、目的接口、协议）的流分类功能
测试配置：测试配置环境 1
测试过程： <ol style="list-style-type: none"> 1) 按测试环境连接设备； 2) 在 DUT 上配置基于 IP 五元组的流分类策略，对命中的数据流采用流量限制，限制速率为 M，M 小于接口线速； 3) 从接口 A 以线速向接口 B 发送符合分类策略的数据流； 4) 停止步骤 3 数据流的发送，从接口 A 以线速向接口 B 发送不符合分类策略的数据流
预期结果： <ol style="list-style-type: none"> 1) 在步骤 3 接口 B 能够以 M 速率（误差<10%）接收数据流； 2) 在步骤 4 接口 B 能够以线速接收数据流
判定原则： <p>应符合预期结果要求，否则不合格</p>

测试编号: 25
测试项目: 流量分类功能测试_4 (可选)
测试目的: 检验在 ATM 接入模式下 DUT 基于 VPI/VCI 的流分类功能
测试配置: 测试配置环境 1
测试过程: 1) 按测试环境连接设备; 2) 在 DUT 上配置基于 ATM VPI/VCI 的流分类策略, 对于命中的数据流采用流量限制, 限制速率为 M , M 小于接口的线速; 3) 从仪表 A 接口以线速向接口 B 发送符合分类策略的数据流; 4) 停止步骤 3 数据流的发送, 从仪表 A 接口以线速向接口 B 发送不符合分类策略的数据流
预期结果: 1) 在步骤 3 接口 B 能够以 M 速率 (误差<10%) 接收数据流; 2) 在步骤 4 接口 B 能够以线速接收数据流
判定原则: 应符合预期结果要求, 否则不合格

测试编号: 26
测试项目: 流量分类功能测试_5
测试目的: 检验在以太网接入模式下 DUT 基于 VLAN ID 的流分类功能
测试配置: 测试配置环境 1
测试过程: 1) 按测试环境连接设备; 2) 在 DUT 上配置基于 VLAN ID 的流分类策略, 对于命中的数据流采用流量限制, 限制速率为 M , M 小于接口的线速; 3) 从仪表 A 接口以线速向接口 B 发送符合分类策略的数据流; 4) 停止步骤 3 数据流的发送, 从仪表 A 接口以线速向接口 B 发送不符合分类策略的数据流
预期结果: 1) 在步骤 3 接口 B 能够以 M 速率 (误差<10%) 接收数据流; 2) 在步骤 4 接口 B 能够以线速接收数据流
判定原则: 应符合预期结果要求, 否则不合格

测试编号：27
测试项目：流量分类功能测试_6
测试目的：检验 DUT 基于接口流量分类类别进行流量限速的功能
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 上配置基于接口的流分类策略（如基于接口 1 配置策略），对于命中的数据流采用流量限制，限制速率为 M ， M 小于接口的线速； 3) 从仪表 A 接口以线速向接口 B 发送数据流； 4) 停止步骤 3 数据流的发送，从仪表 B 接口以线速向接口 C 发送数据流
预期结果： 1) 在步骤 3 接口 B 能够以 M 速率（误差 $<10\%$ ）接收数据流； 2) 在步骤 4 接口 C 能够以线速接收数据流
判定原则： 应符合预期结果要求，否则不合格

6 控制平面安全测试

6.1 IP 地址分配控制

测试编号：28
测试项目：基于用户权限的地址分配
测试目的：验证 DUT 是否能够基于不同的用户权限从不同的 IP 地址池为用户分配地址
测试配置：测试配置环境 3
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 上配置 PPPoE 以及 DHCP 中继功能； 3) 在 DUT 上预先设定不同权限的用户从不同地址池中分配 IP 地址（如 User1 对应地址空间： $X.X.X.0/24$ ，User2 对应地址空间： $Y.Y.Y.0/24$ ）； 4) 在 DUT 上对不同的主叫 IP 地址设置不同的过滤能力（如属于 $X.X.X.0/24$ 网段的 IP 可以访问仪表 B 接口，属于 $Y.Y.Y.0/24$ 网段的 IP 可以访问仪表 C 接口）； 5) 仪表 A 接口以不同的用户（如 User1 和 User2）发起 PPP 呼叫，建立 PPP 连接； 6) 仪表 A 接口以分配的地址分别作为源地址同时向接口 B、C 发送流量
预期结果： 1) B 接口能够收到源地址属于 $X.X.X.0/24$ 网段的数据流； 2) C 接口能够收到源地址属于 $Y.Y.Y.0/24$ 网段的数据流
判定原则： 应符合预期结果要求，否则不合格

测试编号：29
测试项目：限制 ADSL 同一 PVC 下的 IP 地址数目
测试目的：验证 DUT 是否能够限制 ADSL 同一 PVC 下的 IP 地址数目
测试配置：测试配置环境 4
测试过程： 1) 按测试环境连接设备； 2) DUT 上设置用户属性，限制同一个 PVC_ID 下同时接入的用户数，例如 Permit=2； 3) 采用仪表的 3 个接口，在 A、B 两个接口通过 DHCP 申请 IP 地址并通过认证后，C 接口不能通过 DHCP 申请到 IP 地址； 4) 通过认证的 B 接口断开连接后，则 C 接口能够获得 IP 地址并认证通过
预期结果： 通过限制同一 PVC_ID 下分配的 IP 地址数量限制用户数，能实现对 DHCP 服务器的保护
判定原则： 应符合预期结果要求，否则不合格

测试编号：30
测试项目：限制同一 VLAN（以太网接入）下的 IP 地址数目
测试目的：验证 DUT 是否能够限制同一 VLAN_ID 下的 IP 地址数目
测试配置：测试配置环境 5
测试过程： 1) 按测试环境连接设备； 2) DUT 上设置用户属性，限制同一个 VLAN_ID 下同时接入的用户数，例如 Permit=2； 3) 采用仪表的 3 个接口，在 A、B 两个接口通过 DHCP 申请 IP 地址并通过认证后，C 接口不能通过 DHCP 申请到 IP 地址； 4) 通过认证的 B 接口断开连接后，则 C 接口能够获得 IP 地址并通过认证
预期结果： 通过限制同一 VLAN_ID 下分配的 IP 地址数量限制用户数，能实现对 DHCP 服务器的保护
判定原则： 应符合预期结果要求，否则不合格

6.2 防止 IP 地址盗用功能

测试编号: 31
测试项目: ADSL 专线用户 IP 地址防盗用
测试目的: 测试 DUT 对 ADSL 专线用户的 IP 地址保护能力
测试配置: 测试配置环境 4
测试过程: 1) 按测试环境连接设备; 2) 在 DUT 上增加两个 ADSL 桥接专线用户 A 和用户 B, 两个用户使用不同的 RTU, 采用 RFC1483B 协议、VC MUX 方式, 为用户 A 设置地址保护策略; 3) 两个合法用户的计算机通过 ADSL RTU 连至 DUT, 能正常上网, 两个 ADSL 用户属于相同的 IP 子网; 4) 将用户 B 的 IP 地址设成与合法用户 A 的 IP 地址相同, 但 MAC 地址不同, 测试用户 A 和用户 B 上网是否正常; 5) 将用户 A 的网线拔掉, 再测试用户 B 上网是否正常; 6) 将非法用户 B 的 IP 地址和 MAC 地址设成与合法用户 A 相同, 当 A 和 B 的网线都接上时, 测试 A 和 B 上网是否正常; 7) 将用户 A 的网线拔掉, 再测试用户 B 上网是否正常
预期结果: 1) 在测试过程 4、5、6、7 中, B 始终不能上网; 2) 在测试过程 4、6 中, A 上网一直正常, 不受 B 的影响
判定原则: 应符合预期结果要求, 否则不合格

测试编号: 32
测试项目: LAN 专线用户 IP 地址防盗用
测试目的: 测试 DUT 对 LAN 专线用户的 IP 地址保护能力
测试配置: 测试配置环境 5
测试过程: 1) 按测试环境连接设备; 2) 在 DUT 上增加两个 LAN 专线用户 A 和用户 B, 两个用户属于同一个 IP 子网, 但二层隔离; 3) 两个合法用户的计算机通过以太网连至 BNAS, 能正常上网; 4) 将用户 B 的 IP 地址设成与合法用户 A 的 IP 地址相同, 但 MAC 地址不同, 测试用户 A 和用户 B 上网是否正常; 5) 将用户 A 的网线拔掉, 再测试用户 B 上网是否正常; 6) 将非法用户 B 的 IP 地址和 MAC 地址设成与合法用户 A 相同, 当 A 和 B 的网线都接上时, 测试 A 和 B 上网是否正常; 7) 将用户 A 的网线拔掉, 再测试用户 B 上网是否正常
预期结果: 1) 在测试过程 4、5、6、7 中, B 始终不能上网; 2) 在测试过程 4、6 中, A 上网一直正常, 不受 B 的影响
判定原则: 应符合预期结果要求, 否则不合格

6.3 用户接入认证与授权控制

测试编号：33
测试项目：PPPoE 接入控制
测试目的：验证 DUT 是否实现基于 PPPoE 的用户接入控制
测试配置：测试配置环境 6
测试过程： 1) 按测试环境连接设备； 2) 在 BNAS 上配置 PPPoE； 3) 在 BNAS 上配置使用 RADIUS 服务器； 4) 用户主机发起 PPP 呼叫； 5) 用户通过 BNAS 访问外部服务
预期结果： 用户认证通过，可以通过 BNAS 访问外部服务
判定原则： 应符合预期结果要求，否则不合格

测试编号：34
测试项目：Web 接入控制
测试目的：验证 DUT 是否实现基于 Web 的用户接入控制
测试配置：测试配置环境 6
测试过程： 1) 按测试环境连接设备； 2) 在 BNAS 上配置 Web Portal 认证方式； 3) 配置 Web Portal 服务器，配置 RADIUS 服务器； 4) 用户通过浏览器访问 Web Server，输入用户认证信息； 5) 用户获取 IP 地址，通过 BNAS 访问外部服务
预期结果： 用户认证通过，可以通过 BNAS 访问外部服务
判定原则： 应符合预期结果要求，否则不合格

测试编号：35
测试项目：802.1x 接入控制—接口管理（可选）
测试目的：验证 DUT 是否实现接口的控制管理，实现基于 802.1x 的用户接入控制
测试配置：测试配置环境 5
测试过程： 1) 按测试环境连接设备； 2) 在 BNAS 上配置 802.1x 认证，配置使用 RADIUS 服务器； 3) 在 RADIUS 服务器上配置用户记录； 4) 用户主机发起访问请求； 5) 输入不正确的用户名和密码，访问外网资源； 6) 输入正确的用户名和密码，访问外网资源
预期结果： 1) 步骤 4，BNAS 能够将用户访问请求转发到 RADIUS 认证服务器； 2) 步骤 5，用户认证不通过，不能访问外网资源； 3) 步骤 6，用户认证通过，可以访问外网资源
判定原则： 应符合预期结果要求，否则不合格

测试编号：36
测试项目：802.1x 接入控制—MAC 绑定功能（可选）
测试目的：验证 DUT 是否支持基于 802.1x 接入控制的 MAC 地址绑定功能
测试配置：测试配置环境 5
测试过程： 1) 按测试环境连接设备； 2) 在 BNAS 上配置 802.1x 认证，配置使用 RADIUS 服务器； 3) 在 RADIUS 服务器上配置用户 A 的相关记录（绑定 MAC）； 4) 用户 A 发起访问请求，访问系统提供的外部服务； 5) 用户 B（不同的 MAC 地址）冒充用户 A 身份发起访问请求，访问系统提供的外部服务
预期结果： 1) 步骤 4，用户认证通过，可以访问系统提供的外部服务； 2) 步骤 5，用户认证不通过，不能访问系统提供的外部服务
判定原则： 应符合预期结果要求，否则不合格

测试编号：37
测试项目：ADSL 接入用户的账号捆绑
测试目的：DUT 能实现 ADSL 用户接入账号和接口绑定（基于 PVC、接口）
测试配置：RADIUS 服务器有账号与接口的绑定功能。如果没有，则改变判断标准，见“预期结果”中的描述 测试配置环境 4
测试过程： 1) 按测试环境连接设备； 2) 在 RADIUS 服务器中增加一项预付费卡号用户，并设定卡号与 PVC ID 绑定； 3) 用户使用指定的 RTU 接口用 PPPoE 上网，测试是否能通过认证； 4) RADIUS 服务器上能看到 BNAS 上报的 PVC_ID (NAS_PORT_ID) 属性； 5) 用户换用另一个 RTU 接口用 PPPoE 上网，测试是否能正常通过认证
预期结果： 1) 在测试过程 2 中用户能通过认证，在测试过程 4 中用户不能通过认证； 2) 如果测试用的 RADIUS 服务器没有账号与接口绑定功能，判断标准改为设备应能实现上报信息中包含接口号的功能 (NAS_PORT_ID)
判定原则： 应符合预期结果要求，否则不合格

测试编号：38
测试项目：LAN 接入用户的账号捆绑
测试目的：验证 DUT 是否实现 LAN 接入用户的账号绑定（基于 VLAN_ID、接口）
测试配置：测试配置环境 5
测试过程： 1) 按测试环境连接设备； 2) 在 RADIUS 服务器中增加一预付费卡号用户，并设定卡号与 VLAN_ID 绑定； 3) 用户使用指定的 VLAN 用 PPPoE 上网，测试是否能通过认证； 4) RADIUS 服务器上能看到 BNAS 上报的 VLAN ID(NAS_PORT)属性； 5) 用户换用另一个 VLAN 用 PPPoE 上网，测试是否能够认证
预期结果： 1) 在测试过程 3 中用户能通过认证，在测试过程 5 中用户不能通过认证； 2) 如果测试用的 RADIUS 服务器没有账号与接口的绑定功能，则判定标准改为设备应能实现上报信息中包含设备接口号的功能 (NAS_PORT)
判定原则： 应符合预期结果要求，否则不合格

6.4 路由协议安全测试

6.4.1 RIP 路由协议安全测试

测试编号：39
测试项目：RIPv2 简单明文认证
测试目的：检验 DUT 是否支持 RIPv2 简单明文认证
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 与仪表 B 接口直连的接口 2 启用 RIP 协议，并且配置明文认证； 3) 从仪表 B 接口注入带明文认证的路由信息，A.A.A.X/24； 4) 从仪表 A 接口发送到 A.A.A.X 网段的 IP 数据流（如 A.A.A.2）； 5) 停止步骤 4 数据流的发送，从仪表 B 接口注入不带明文认证的路由信息，B.B.B.X/24； 6) 从仪表 A 接口发送到 B.B.B.X 网段的 IP 数据流（如 B.B.B.2）
预期结果： 1) 步骤 4，仪表 B 接口能够收到数据流； 2) 步骤 6，仪表 B 接口不能收到数据流
判定原则： 应符合预期结果要求，否则不合格

测试编号：40
测试项目：RIPv2 MD5 认证
测试目的：检验 DUT 是否支持 RIPv2 MD5 认证
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 与仪表 B 接口直连的接口 2 启用 RIP 协议，并且配置 MD5 认证； 3) 从仪表 B 接口注入带 MD5 认证的路由信息，A.A.A.X/24； 4) 从仪表 A 接口发送到 A.A.A.X 网段的 IP 数据流（如 A.A.A.2）。 5) 停止步骤 4 数据流的发送，从仪表 B 接口注入不带 MD5 认证的路由信息，B.B.B.X/24； 6) 从仪表 A 接口发送到 B.B.B.X 网段的 IP 数据流（如 B.B.B.2）
预期结果： 1) 步骤 4，仪表 B 接口能够收到数据流； 2) 步骤 6，仪表 B 接口不能收到数据流
判定原则： 应符合预期结果要求，否则不合格

6.4.2 OSPFv2 路由协议安全测试

测试编号：41
测试项目：OSPFv2 链路的简单明文认证
测试目的：检验 DUT 是否支持 OSPFv2 邻居间链路的简单明文认证功能
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 和测试仪表 B 接口上启用 OSPFv2 协议，并在接口 B 和 DUT 上分别配置链路明文验证； 3) 在 DUT 和仪表 B 接口上配置相同的密码； 4) 在 DUT 和仪表 B 接口上配置不同的密码
预期结果： 1) 步骤 3，DUT 和接口 B 能够正常建立 OSPF 邻接关系； 2) 步骤 4，DUT 和接口 B 不能正常建立 OSPF 邻接关系
判定原则： 应符合预期结果要求，否则不合格

测试编号：42
测试项目：OSPFv2 链路的 MD5 认证
测试目的：检验 DUT 是否支持 OSPFv2 链路间的 MD5 认证功能
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 和测试仪表 B 接口上启用 OSPFv2 协议，并在接口 B 和 DUT 上分别配置链路 MD5 验证； 3) 在 DUT 和仪表 B 接口上配置相同的密码； 4) 在 DUT 和仪表 B 接口上配置不同的密码
预期结果： 1) 步骤 3，DUT 和接口 B 能够正常建立 OSPF 邻接关系； 2) 步骤 4，DUT 和接口 B 不能正常建立 OSPF 邻接关系
判定原则： 应符合预期结果要求，否则不合格

测试编号：43
测试项目：OSPFv2 区域明文认证
测试目的：检验 DUT 是否支持 OSPFv2 区域内的简单明文认证功能
测试配置：测试配置环境 1
测试过程： <ol style="list-style-type: none"> 1) 按测试环境连接设备； 2) 在 DUT 和测试仪表 B 接口上启用 OSPFv2 协议，属于同一个区域，并在接口 B 和 DUT 上分别配置区域明文验证； 3) 在 DUT 和仪表 B 接口上配置相同的密码； 4) 在 DUT 和仪表 B 接口上配置不同的密码
预期结果： <ol style="list-style-type: none"> 1) 步骤 3，DUT 和仪表 B 接口能够正常建立 OSPF 邻接关系； 2) 步骤 4，DUT 和仪表 B 接口不能正常建立 OSPF 邻接关系
判定原则： <p>应符合预期结果要求，否则不合格</p>

测试编号：44
测试项目：OSPFv2 区域 MD5 认证
测试目的：检验 DUT 是否支持 OSPFv2 区域内的 MD5 认证功能
测试配置：测试配置环境 1
测试过程： <ol style="list-style-type: none"> 1) 按测试环境连接设备； 2) 在 DUT 和测试仪表 B 接口上启用 OSPFv2 协议，属于同一个区域，并在接口 B 和 DUT 上分别配置区域 MD5 验证； 3) 在 DUT 和仪表 B 接口上配置相同的密码； 4) 在 DUT 和仪表 B 接口上配置不同的密码
预期结果： <ol style="list-style-type: none"> 1) 步骤 3，DUT 和 B 接口能够正常建立 OSPF 邻接关系； 2) 步骤 4，DUT 和 B 接口不能正常建立 OSPF 邻接关系
判定原则： <p>应符合预期结果要求，否则不合格</p>

6.4.3 IS-IS 路由协议安全测试

测试编号：45
测试项目：IS-IS 协议接口 Level1 明文认证
测试目的：检验 DUT 是否支持 IS-IS 协议接口的 Level1 明文认证
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 和仪表 B 上分别启用 IS-IS 路由协议，在接口间建立 Level-1 邻接关系，并且分别配置明文认证； 3) 在 DUT 和仪表 B 接口上配置相同的密码； 4) 在 DUT 和仪表 B 接口上配置不同的密码
预期结果： 1) 在步骤 3 中，DUT 和仪表 B 接口可以正常建立 IS-IS Level-1 邻接关系； 2) 在步骤 4 中，DUT 和仪表 B 接口不能正常建立 IS-IS Level-1 邻接关系
判定原则： 应符合预期结果要求，否则不合格

测试编号：46
测试项目：IS-IS 协议接口 Level1 MD5 认证
测试目的：检验 DUT 是否支持 IS-IS 协议接口的 Level1MD5 认证
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 和仪表 B 接口上分别启用 IS-IS 路由协议，在接口间建立 Level-1 邻接关系，并且分别配置 MD5 认证； 3) 在 DUT 和仪表 B 接口上配置相同的密码； 4) 在 DUT 和仪表 B 接口上配置不同的密码
预期结果： 1) 在步骤 3 中，DUT 和仪表 B 接口可以正常建立 IS-IS Level-1 邻接关系； 2) 在步骤 4 中，DUT 和仪表 B 接口不能正常建立 IS-IS Level-1 邻接关系
判定原则： 应符合预期结果要求，否则不合格

测试编号：47
测试项目：IS-IS 协议接口 Level2 明文认证
测试目的：检验 DUT 是否支持 IS-IS 协议接口的 Level2 明文认证
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 和 DUT2 仪表接口 B 上分别启用 IS-IS 路由协议，在接口建立 Level-2 邻接关系，并且分别配置明文认证； 3) 在 DUT 和仪表接口 B 上配置相同的密码； 4) 在 DUT 和仪表接口 B 上配置不同的密码
预期结果： 1) 在步骤 3 中，DUT 和仪表接口 B 可以正常建立 IS-IS Level-2 邻接关系； 2) 在步骤 4 中，DUT 和仪表接口 B 不能正常建立 IS-IS Level-2 邻接关系
判定原则： 应符合预期结果要求，否则不合格

测试编号：48
测试项目：IS-IS 协议接口 Level2 MD5 认证
测试目的：检验 DUT 是否支持 IS-IS 协议接口的 Level2 MD5 认证
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 和仪表接口 B 上分别启用 IS-IS 路由协议，在接口间建立 Level-2 邻接关系，并且分别配置 MD5 认证； 3) 在 DUT 和仪表接口 B 上配置相同的密码； 4) 在 DUT 和仪表接口 B 上配置不同的密码
预期结果： 1) 在步骤 3 中，DUT 和仪表接口 B 可以正常建立 IS-IS Level-2 邻接关系； 2) 在步骤 4 中，DUT 和仪表接口 B 不能正常建立 IS-IS Level-2 邻接关系
判定原则： 应符合预期结果要求，否则不合格

测试编号：49
测试项目：IS-IS 协议区域内的明文认证
测试目的：检验 DUT 是否支持 IS-IS 协议区域内的明文认证功能
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 和仪表接口 B 上分别启用 IS-IS 路由协议，并分别配置区域内的明文认证，在接口间建立 Level-1 邻接关系； 3) 在 DUT 和仪表接口 B 上配置相同的密码； 4) 在 DUT 和仪表接口 B 上配置不同的密码
预期结果： 1) 在步骤 3 中，DUT 和仪表接口 B 可以正常建立 IS-IS Level-1 邻接关系； 2) 在步骤 4 中，DUT 和仪表接口 B 不能正常建立 IS-IS Level-1 邻接关系
判定原则： 应符合预期结果要求，否则不合格

测试编号：50
测试项目：IS-IS 协议区域内的 MD5 认证
测试目的：检验 DUT 是否支持 IS-IS 协议区域内的 MD5 认证功能
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 和仪表接口 B 上分别启用 IS-IS 路由协议，并分别配置区域内的 MD5 认证，在接口间建立 Level-1 邻接关系； 3) 在 DUT 和仪表接口 B 上配置相同的密码； 4) 在 DUT 和仪表接口 B 上配置不同的密码
预期结果： 1) 在步骤 3 中，DUT 和仪表接口 B 可以正常建立 IS-IS Level-1 邻接关系； 2) 在步骤 4 中，DUT 和仪表接口 B 不能正常建立 IS-IS Level-1 邻接关系
判定原则： 应符合预期结果要求，否则不合格

测试编号：51
测试项目：IS-IS 协议区域间的明文认证
测试目的：检验 DUT 是否支持 IS-IS 协议区域间的明文认证功能
测试配置：测试配置环境 1
测试过程： <ol style="list-style-type: none"> 1) 按测试环境连接设备； 2) 在 DUT 和仪表接口 B 上分别启用 IS-IS 路由协议，DUT 属于 Level-1，仪表接口 B 属于 Level-2，并分别配置区域间明文认证，在接口间建立 Level-1/2 邻接关系； 3) 在 DUT 和仪表接口 B 上配置相同的密码； 4) 在 DUT 和仪表接口 B 上配置不同的密码
预期结果： <ol style="list-style-type: none"> 1) 在步骤 3 中，DUT 和仪表接口 B 可以正常建立 IS-IS Level-1/2 邻接关系； 2) 在步骤 4 中，DUT 和仪表接口 B 不能正常建立 IS-IS Level-1/2 邻接关系
判定原则： <p>应符合预期结果要求，否则不合格</p>

测试编号：52
测试项目：IS-IS 协议区域间的 MD5 认证
测试目的：检验 DUT 是否支持 IS-IS 协议区域间的 MD5 认证功能
测试配置：测试配置环境 1
测试过程： <ol style="list-style-type: none"> 1) 按测试环境连接设备； 2) 在 DUT 和仪表接口 B 上分别启用 IS-IS 路由协议，DUT 属于 Level-1，仪表接口 B 属于 Level-2，并分别配置区域间 MD5 认证，在接口间建立 Level-1/2 邻接关系； 3) 在 DUT 和仪表接口 B 上配置相同的密码； 4) 在 DUT 和仪表接口 B 上配置不同的密码
预期结果： <ol style="list-style-type: none"> 1) 在步骤 3 中，DUT 和仪表接口 B 可以正常建立 IS-IS Level-1/2 邻接关系； 2) 在步骤 4 中，DUT 和仪表接口 B 不能正常建立 IS-IS Level-1/2 邻接关系
判定原则： <p>应符合预期结果要求，否则不合格</p>

6.4.4 BGP 路由协议安全测试

测试编号：53
测试项目：IBGP 的 MD5 认证
测试目的：检验 DUT 是否支持 IBGP MD5 认证
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 和仪表接口 B 直连接口启用 BGP 协议，配置相同的自治系统号； 3) 在 DUT 和仪表接口 B 配置 MD5 认证，密码不同； 4) 在 DUT 和仪表接口 B 配置 MD5 认证，密码相同
预期结果： 1) 在步骤 3，DUT 和仪表接口 B 无法建立 IBGP 对等关系； 2) 在步骤 4，DUT 和仪表接口 B 能够建立 IBGP 对等关系
判定原则： 应符合预期结果要求，否则不合格

测试编号：54
测试项目：EBGP 的 MD5 认证
测试目的：检验 DUT 是否支持 EBGP MD5 认证
测试配置：测试配置 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 和仪表接口 B 直连接口启用 BGP 协议，配置不同的自治系统号； 3) 在 DUT 和仪表接口 B 配置 MD5 认证，密码不同； 4) 在 DUT 和仪表接口 B 配置 MD5 认证，密码相同
预期结果： 1) 在步骤 3，DUT 和仪表接口 B 无法建立 EBGP 对等关系； 2) 在步骤 4，DUT 和仪表接口 B 能够建立 EBGP 对等关系
判定原则： 应符合预期结果要求，否则不合格

6.5 TCP/IP 协议安全测试

6.5.1 IP 协议安全测试

测试编号：55
测试项目：关闭 IP 源路由选项
测试目的：检验 DUT 是否支持关闭 IP 源路由选项
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 上配置关闭 IP 源路由选项； 3) 从仪表 A 接口向 B 接口发送带有 IP 源路由选项（类型为 131 和 137）的 IP 数据包
预期结果： 仪表 B 接口不能收到数据包
判定原则： 应符合预期结果要求，否则不合格

6.5.2 ICMP 协议安全测试

测试编号：56
测试项目：拒绝已作废的 ICMP 报文
测试目的：检验 DUT 拒绝已作废的某些类型的 ICMP 的功能
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 从仪表 A 接口向 DUT 接口 1 发送已过时或作废类型的 ICMP 协议报文，包括信息请求报文(Type 15, Code 0)、信息应答报文 (Type 16, Code 0)
预期结果： 在步骤 2 中，DUT 应丢弃仪表发送的 ICMP 报文
判定原则： 应符合预期结果要求，否则不合格

测试编号：57
测试项目：ICMP 重定向关闭功能
测试目的：验证 DUT 能否过滤 ICMP 重定向消息
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 关闭 DUT ICMP 重定向功能； 3) 从仪表 A 接口向 DUT 接口 1 发送 ICMP 重定向消息（Type 5，Code 0）
预期结果： 在步骤 3 中，DUT 应丢弃仪表发送的 ICMP 重定向报文
判定原则： 应符合预期结果要求，否则不合格

6.6 VPN 安全测试

测试编号：58
测试项目：MPLS VPN 数据隔离
测试目的：验证 DUT 不同 VPN 的数据相互隔离
测试配置：测试配置环境 7
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 上配置 MPLS VPN（作 PE），并存在 VPN1 和 VPN2 两个 VPN； 3) 在仪表接口 A 上模拟两个 CE 设备（A.1 子接口属于 VPN1，A.2 子接口属于 VPN2），仪表 B 接口模拟 P 路由器和其他 PE 路由器（B.1 子接口属于 VPN1，B.2 子接口属于 VPN2）； 4) 在仪表子接口 A.1 和 B.1 之间线速发送 VPN1 的数据流量
预期结果： 在步骤 4 中，从仪表上观察，VPN2 中不应收到任何 VPN1 中的流量
判定原则： 应符合预期结果要求，否则不合格

测试编号：59
测试项目：MPLS VPN 路由泄漏测试
测试目的：验证 DUT 不会发生 VPN 路由的泄漏
测试配置：测试配置环境 7
测试过程： <ol style="list-style-type: none"> 1) 按测试环境连接设备； 2) 在 DUT 上配置 MPLS VPN（作 PE），并存在 VPN1 和 VPN2 两个 VPN； 3) 在仪表接口 A 上模拟两个 CE 设备（A.1 子接口属于 VPN1，A.2 子接口属于 VPN2），仪表 B 接口模拟 P 路由器和其他 PE 路由器（B.1 子接口属于 VPN1，B.2 子接口属于 VPN2）； 4) 从仪表 B 仿真的 PE 路由器上通告 VPN1（X.X.X.0/24）和 VPN2（Y.Y.Y.0/24）的路由； 5) 从仪表 A.1 子接口发送到目的网段为 X.X.X.0/24 和 Y.Y.Y.0/24 的数据流； 6) 从仪表 A.2 子接口发送到目的网段为 X.X.X.0/24 和 Y.Y.Y.0/24 的数据流
预期结果： <ol style="list-style-type: none"> 1) 在 BNAS 上查看 Vrf 路由表，其中 X.X.X.0/24 包含在 Vrf1 中，Y.Y.Y.0/24 包含在 Vrf2 中； 2) 在步骤 5 中，仪表 B 接口 B.1 子接口接收到数据流，子接口 B.2 不能收到数据流； 3) 在步骤 6 中，仪表 B 接口 B.2 子接口接收到数据流，子接口 B.1 不能收到数据流
判定原则： <p>应符合预期结果要求，否则不合格</p>

6.7 路由过滤功能测试

测试编号：60
测试项目：BGP 入口路由过滤
测试目的：验证 DUT 是否支持 BGP 入口路由过滤功能
测试配置：测试配置环境 1
测试过程： <ol style="list-style-type: none"> 1) 按测试环境连接设备； 2) 在仪表 A、B 接口与 DUT1、2 接口之间分别建立 BGP 邻接关系； 3) 在 DUT 上配置入向路由过滤，过滤前缀为 X.X.X.0/24 的路由； 4) 从仪表 A 向 DUT 通告 BGP 路由，路由前缀为 X.X.X.0/24 和 Y.Y.Y.0/24
预期结果： <p>在步骤 4 中，从 DUT 上查看路由表，应不存在 X.X.X.0/24 的 BGP 路由</p>
判定原则： <p>应符合预期结果要求，否则不合格</p>

测试编号：61
测试项目：BGP 出口路由过滤
测试目的：验证 DUT 是否支持 BGP 出口路由过滤功能
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在仪表 A、B 接口与 DUT1、2 接口之间分别建立 BGP 邻接关系； 3) 在 DUT 上配置出向路由过滤，过滤前缀为 X.X.X.0/24 的路由； 4) 从仪表 A 向 DUT 通告 BGP 路由，路由前缀为 X.X.X.0/24 和 Y.Y.Y.0/24
预期结果： 1) 在步骤 4 中，从 DUT 上查看路由表，应存在 X.X.X.0/24 的路由表项； 2) 在步骤 4 中，从仪表 B 接口观察，应只从 DUT 接收到前缀为 Y.Y.Y.0/24 的路由
判定原则： 应符合预期结果要求，否则不合格

测试编号：62
测试项目：基于 BGP 属性的路由过滤
测试目的：验证 DUT 是否支持基于 BGP 属性的路由过滤功能
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在仪表 A、B 接口与 DUT1、2 接口之间分别建立 BGP 邻接关系； 3) 在 DUT 上配置路由过滤，如过滤 AS_PATH 中含有 AS1 的路由； 4) 从仪表接口 A 向 DUT 通告 BGP 路由，路由前缀为 X.X.X.0/24，AS_PATH 为 AS1、AS2
预期结果： 在步骤 4 中，从 DUT 上查看路由表，应不存在 X.X.X.0/24 的 BGP 路由
判定原则： 应符合预期结果要求，否则不合格

测试编号：63
测试项目：路由重分布的路由过滤
测试目的：验证 DUT 是否支持路由重分布的路由过滤功能
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在仪表 A 接口与 DUT 接口 1 之间建立 OSPF 邻居关系，在仪表 B 接口与 DUT 接口 2 之间建立 BGP 邻接关系； 3) 在 DUT 上配置路由从 OSPF 重分布到 BGP，并且配置过滤前缀为 X.X.X.0/24 的路由； 4) 从仪表接口 A 向 DUT 通告 OSPF 路由，路由前缀为 X.X.X.0/24 和 Y.Y.Y.0/24
预期结果： 在步骤 4 中，仪表的 B 接口能够收到 Y.Y.Y.0/24 的路由，而不能收到 X.X.X.0/24 的路由
判定原则： 应符合预期结果要求，否则不合格

6.8 GTSM 功能测试

测试编号：64
测试项目：GTSM 安全机制测试（可选）
测试目的：验证被测设备是否支持 GTSM 安全机制
测试配置：测试配置环境 1
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 设备接口 1、2 上启用 BGP 协议，并在接口上应用 GTSM 功能； 3) 在仪表接口 A、B 仿真 BGP 路由协议，且均不使用 GTSM 功能
预期结果： 仪表接口 A 与 DUT 接口 1 能建立 BGP 对等体，仪表接口 B 与 DUT 接口 2 不能建立 BGP 对等体
判定原则： 应符合预期结果要求，否则不合格

7 管理平面的安全测试

7.1 接口镜像

测试编号：65
测试项目：接口镜像功能测试
测试目的：验证 DUT 是否可以提供接口镜像功能
测试配置：测试配置环境 2
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 上配置接口镜像，镜像的源接口接口为 1，目的接口接口为 3； 3) 从仪表 A 接口向 B 接口发送流量
预期结果： 仪表 C 接口能够收到 A 接口发出的数据流
判定原则： 应符合预期结果要求，否则不合格

7.2 访问控制安全测试

7.2.1 用户访问控制测试

测试编号：66
测试项目：用户访问控制功能测试
测试目的：验证 DUT 是否支持用户的访问控制
测试配置：测试配置环境 8
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 连接可以正常建立
判定原则： 应符合预期结果要求，否则不合格

测试编号：67
测试项目：用户分级分权访问控制功能测试
测试目的：验证 DUT 是否支持用户分级分权的访问控制功能
测试配置：测试配置环境 8
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： 用户能够正常登录，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，否则不合格

7.2.2 Telnet 访问安全测试

测试编号：68
测试项目：Telnet 访问连接数量限制
测试目的：验证 DUT 是否能够限制同时远程登录的用户数量
测试配置：测试配置环境 8
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 上配置限制同时登录的 Telnet 访问连接数，如 Permit=2； 3) 用 3 个客户端对 DUT 进行 Telnet 访问
预期结果： 先登录的两个用户可以正常访问，第三个用户被拒绝登录
判定原则： 应符合预期结果要求，否则不合格

测试编号：69
测试项目：防止 Telnet 用户口令猜测功能测试
测试目的：验证 DUT 是否具有防止 Telnet 用户口令猜测功能
测试配置：测试配置环境 8
测试过程： 1) 按测试环境连接设备； 2) 在 DUT 上配置用户 User 及访问密码，并配置限制同一用户尝试登录的次数 (N)； 3) 从客户端以用户 User 发起 Telnet 登录请求，以错误的密码尝试 M ($M > N$) 次
预期结果： 用户的 Telnet 连接被拒绝，退出登录界面
判定原则： 应符合预期结果要求，否则不合格

7.2.3 HTTPS 访问安全测试

测试编号：70
测试项目：用户通过 HTTPS 安全协议访问网管信息（可选）
测试目的：验证 DUT 是否支持 HTTPS 安全协议访问控制功能
测试配置：测试配置环境 9
测试过程： 1) 按测试环境连接设备； 2) 网管客户端使用 HTTPS 协议加密访问设备的网管信息
预期结果： 用户能够正常读取和修改设备的网管信息
判定原则： 应符合预期结果要求，否则不合格

7.2.4 SSH 协议安全功能测试

测试编号：71
测试项目：SSH 连接建立
测试目的：验证 DUT 能否正常建立 SSH 连接
测试配置：测试配置环境 8
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，否则不合格

测试编号：72
测试项目：SSH 连接数量限制
测试目的：验证 DUT 能否限制同时连接的 SSH 连接数量
测试配置：测试配置环境 8
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，如 Permit=2； 3) 用 3 个客户端对 DUT 进行 SSH 连接
预期结果： 先登录的两个用户能够正常建立 SSH 连接，正常访问，第 3 个用户 SSH 连接被拒绝
判定原则： 应符合预期结果要求，否则不合格

测试编号: 73
测试项目: SSH 版本兼容测试
测试目的: 检验 DUT 能够对 SSH 版本进行兼容处理
测试配置: 测试配置环境 8
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, 否则不合格

测试编号: 74
测试项目: SSH 算法协商测试
测试目的: 检验 DUT 是否具有协商 SSH 连接中各种算法的能力
测试配置: 测试配置环境 8
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_KEXINT 消息进行算法协商。
预期结果: 在步骤 3 中, DUT 应能支持 3des-cbc 加密算法 (aes128-cbc 算法为可选); DUT 应能支持 diffie-hellman-group1-sha1 或 diffie-hellman-group14-sha1 密钥交换算法; DUT 应能支持 hmac-sha1 认证算法 (hmac-sha1-96 为可选); DUT 可选支持对数据压缩; DUT 应能支持 ssh-dss 公钥算法 (ssh-rsa 为可选)
判定原则: 应符合预期结果要求, 否则不合格

测试编号: 75
测试项目: 定期重协商测试
测试目的: 检验 DUT 是否支持定期重协商
测试配置: 测试配置环境 8
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 应能够配置定期重协商 (如根据通信的总数据量或时间), 并在到达期限时进行算法密钥的重协商
判定原则: 应符合预期结果要求, 否则不合格

测试编号: 76
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_DISCONNECT) 的主动发送
测试配置: 测试配置环境 8
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_DISCONNECT 消息, 并立即中断连接
判定原则: 应符合预期结果要求, 否则不合格

测试编号：77
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_DISCONNECT）的处理
测试配置：测试配置环境 8
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的算法组合进行通信； 4) 从客户端发送中断连接消息
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，否则不合格

测试编号：78
测试项目：SSH 用户认证方式测试
测试目的：检验 DUT 是否支持 SSH 用户认证方式
测试配置：测试配置环境 8
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) 终端向 DUT 发送 SSH_MSG_USERAUTH_REQUEST 消息，“method name”字段为“publickey”
预期结果： DUT 应能支持公钥方式的用户认证
判定原则： 应符合预期结果要求，否则不合格

7.3 用户密码保护功能测试

测试编号: 79
测试项目: 用户密码保护功能
测试目的: 验证 DUT 是否能够以密文方式显示用户密码
测试配置: 测试配置环境 8
测试过程: 1) 按测试环境连接设备; 2) 在 DUT 上配置用户 User 及访问密码, 并配置密码密文显示模式
预期结果: 在 DUT 系统配置参数显示中, 用户密码以密文的方式显示
判定原则: 应符合预期结果要求, 否则不合格

7.4 SNMP 安全功能测试

测试编号: 80
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: 测试配置环境 8
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 中应得到错误的状态 “noSuchName” 以及相应的错误索引
判定原则: 应符合预期结果要求, 否则不合格

测试编号：81
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：测试配置环境 8
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 客户端软件使用 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 中应得到下一属性值
判定原则： 应符合预期结果要求，否则不合格

测试编号：82
测试项目：SNMPv3 GETBulk 原语功能测试
测试目的：检验 DUT 支持 SNMPv3 GETBulk 原语功能
测试配置：测试配置环境 8
测试过程： 1) 按测试环境连接设备； 2) 使用终端上的 SNMPv3 客户端软件使用 GetBulk 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，否则不合格

测试编号: 83
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: 测试配置环境 8
测试过程: 1) 按测试环境连接设备; 2) 使用终端上的 SNMPv3 客户端软件使用 Set 命令设置 DUT 的系统描述; 3) 使用终端上的 SNMPv3 客户端软件读取系统描述
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, 否则不合格

测试编号: 84
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: 测试配置环境 8
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 (WarmStart), 并热启动设备; 4) 配置 DUT, 使其在设备链路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, 否则不合格

测试编号：85
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：测试配置环境 8
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）认证算法与 DUT 进行认证，并进行 SNMP 操作； 4) 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）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，否则不合格

测试编号：86
测试项目：对 SNMPv3 管理工作站的验证
测试目的：检验 DUT 支持 SNMPv3 管理工作站的验证
测试配置：测试配置环境 8
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）间地址为 Y.Y.Y.Y，配置管理工作站地址为 Y.Y.Y.Z
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，否则不合格

7.5 安全审计功能测试

测试编号：87
测试项目：安全日志功能测试
测试目的：验证 DUT 是否支持安全日志功能
测试配置：测试配置环境 8
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
判定原则： 应符合预期结果要求，否则不合格

测试编号：88
测试项目：操作日志功能测试
测试目的：验证 DUT 是否支持操作日志功能
测试配置：测试配置环境 8
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的 IP 地址、登录时间、所进行的操作、执行结果进行记录； 2) DUT 可以将操作日志输出到日志服务器
判定原则： 应符合预期结果要求，否则不合格