

ICS 33.040.50

M 19

YD

中华人民共和国通信行业标准

YD/T 2049-2009

接入网设备安全测试方法 ——DSL 接入复用器（DSLAM）设备

Test method of security for access network equipment
——Digital subscriber line access multiplexer

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 缩略语.....1

4 用户平面安全功能测试.....2

5 控制平面安全功能测试.....9

6 管理平面安全功能测试.....12

7 其他安全功能测试.....17

附录 A（资料性附录） 安全相关性能测试方法.....19

前 言

本标准是接入网安全系列标准之一，该系列标准预计结构及名称如下：

1. YD/T 2046-2009 接入网安全技术要求——xDSL用户端设备
2. YD/T 2047-2009 接入网设备安全测试方法——xDSL用户端设备
3. YD/T 2048-2009 接入网安全技术要求——DSL接入复用器（DSLAM）设备
4. YD/T 2049-2009 接入网设备安全测试方法——DSL接入复用器（DSLAM）设备
5. YD/T 2050-2009 接入网安全技术要求——无源光网络（PON）设备
6. YD/T 2051-2009 接入网设备安全测试方法——无源光网络（PON）设备
7. YD/T 1910-2009 接入网安全技术要求——综合接入系统
8. 接入网设备安全测试方法——综合接入系统

本标准与YD/T 2048-2009《接入网安全技术要求——DSL接入复用器（DSLAM）设备》配套使用。

在本标准的制定过程中保持了与下列标准的协调统一：

1. YD/T 1323-2004 接入网技术要求——不对称数字用户线（ADSL）
2. YD/T 1239-2002 接入网技术要求——甚高速数字用户线（VDSL）
3. YD/T 1055-2005 接入网设备测试方法——带话音分离器的不对称数字用户线（ADSL）
4. YD/T 1530-2006 接入网技术要求——频谱扩展的第二代不对称数字用户线（ADSL2+）
5. YD/T 1706-2007 接入网技术要求——数字用户线（DSL）承载宽带业务
6. YD/T 1996-2009 接入网技术要求——第二代甚高速数字用户线（VDSL2）

本标准附录A为资料性附录。

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、上海贝尔股份有限公司。

本标准主要起草人：程 强、李云洁、陈 洁、葛 坚、姚亦峰。

接入网设备安全测试方法

——DSL 接入复用器（DSLAM）设备

1 范围

本标准规定了数字用户线接入复用设备（DSLAM）用户平面安全功能测试方法、控制平面安全功能测试方法、管理平面安全功能测试方法和其它安全功能的测试方法。

本标准适用于公众电信网的局端数字用户线接入复用器设备，对于放置在远端的DSL接入复用设备可以参考使用。专用电信网也可参考使用。

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 1808-2008 接入网设备测试方法——第二代及频谱扩展的第二代不对称数字用户线（ADSL2/2+）

YD/T 1706-2007 接入网技术要求——数字用户线（DSL）承载宽带业务

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
ADSL	Asymmetric Digital Subscriber Line	不对称数字用户线
ARP	Address Resolution Protocol	地址解析协议
BNG	Broadband Network Gateway	宽带网络网关
CPE	Customer Premise Equipment	客户驻地设备
C-VID	Customer VLAN IDentifier	客户VLAN标识
DHCP	Dynamic Host Config Protocol	动态主机配置协议
DLF	Destination Lookup Failure	目的查找失败
DoS	Denial of Service	拒绝服务
DSL	Digital Subscriber Line	数字用户线
DSLAM	Digital Subscriber Line Access Multiplexer	数字用户线接入复用器
HTTP	HyperText Transfer Protocol	超文本传输协议
HTTPS	Hypertext Transfer Protocol over Secure Socket Layer	安全套接字层上的HTTP
IGMP	Internet Group Management Protocol	因特网组管理协议
IP	Internet Protocol	互联网协议
MAC	Media Access Control	媒质访问控制

PC	Personal Computer	个人电脑
RSTP	Rapid Spanning Tree Protocol	快速生成树协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SSH	Secure Shell	安全Shell
SSL	Secure Socket Layer	安全套接字层
S-VID	Service VID	业务VLAN标识
TLS	Transport Layer Security	传送层安全
UDP	User Datagram Protocol	用户数据报协议
VID	VLAN ID	VLAN标识
VLAN	Virtual Local Area Network	虚拟局域网
xDSL	Any of the various types of Digital Subscriber Lines (DSL)	指代任何类型的DSL

4 用户平面安全功能测试

4.1 二层隔离功能

4.1.1 测试目的

DSLAM设备应对用户侧的所有DSL端口之间提供二层隔离的功能，即同一DSLAM设备下的不同DSL端口上的用户不应通过DSLAM设备上的二层桥接功能直接互通。

4.1.2 测试配置

测试配置如图1所示。

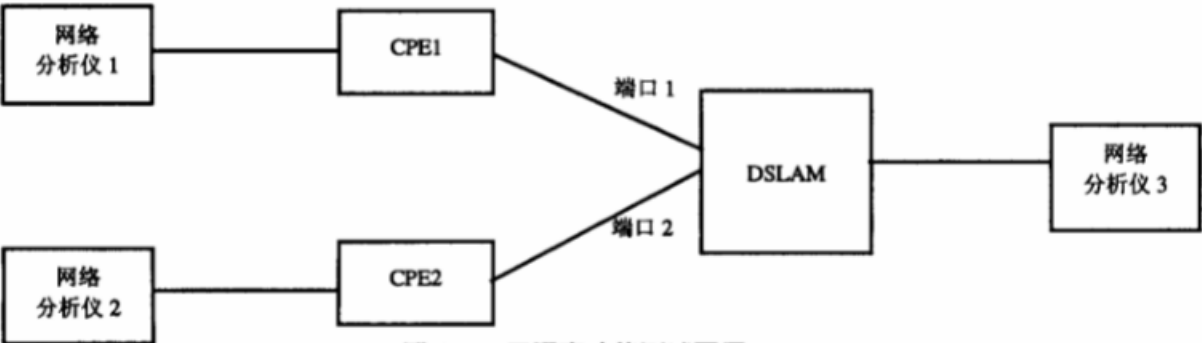


图 1 二层隔离功能测试配置

4.1.3 测试步骤

- (1) 如图 1 所示，任选 DSLAM 两个用户端口，配置两个桥接模式的 CPE 设备；
- (2) 配置两个 CPE 用户流量为无 VLAN 标签方式，网络侧为 N:1 VLAN 模式，设定 S-VID 的值为 X (0<X<4095)；
- (3) 发送地址学习帧；
- (4) 网络分析仪 1 与网络分析仪 3 互发以太网广播与单播报文；
- (5) 网络分析仪 2 与网络分析仪 3 互发以太网广播与单播报文；
- (6) 网络分析仪 1 和网络分析仪 2 互发以太网广播与单播报文。

4.1.4 预期结果

- (1) 在步骤 (4) 中，网络分析仪1和3应可以互通，且网络分析仪2不应收到除来自网络分析仪3的广播报文的任何报文。

(2) 在步骤(5)中, 网络分析仪2和3应可以互通, 且网络分析仪1不应收到除来自网络分析仪3的广播报文的任何报文。

(3) 在步骤(6)中, 网络分析仪1和2不应有任何流量互通。

4.2 VLAN 功能

见YD/T 1808-2008《接入网设备测试方法——第二代及频谱扩展的第二代不对称数字用户线ADSL2/ADSL2+》10.2。

4.3 帧过滤功能

4.3.1 测试目的

DSLAM应能根据MAC源地址和/或目的地址设置过滤条目。对于预定义和保留地址的MAC帧(见表1), DSLAM缺省应过滤掉, 不进行转发, 但设备可以提供改变缺省行为的配置选项。

表1 对预定义和保留地址的MAC帧处理

目的 MAC 地址	作用	缺省行为	可选配置
01-80-C2-00-00-00	桥组地址 (BPDUs)	Block	None
01-80-C2-00-00-01	PAUSE	Block	None
01-80-C2-00-00-02	慢速协议 (LACP, EFM OAM PDUs)	Block	Peer
01-80-C2-00-00-03	EAP over LANs	Block	Peer
01-80-C2-00-00-04 - 01-80-C2-00-00-0F	保留	Block	None
01-80-C2-00-00-10	所有 LAN 的桥管理地址	Block	None
01-80-C2-00-00-20	GMRP	Block	None
01-80-C2-00-00-21	GVRP	Block	None
01-80-C2-00-00-22 - 01-80-C2-00-00-2F	保留 GARP 应用地址	Block	Forward
01-80-C2-xx-xx-xy	CFM	Forward	Block

建议DSLAM支持基于MAC目的地址、MAC源地址、MAC协议类型、IP目的地址、IP源地址的部分和全部的过滤规则功能。

DSLAM应可配置为过滤从用户端口发出目的地址为组播地址的UDP数据流。

4.3.2 测试配置

测试配置如图1所示。

4.3.3 测试步骤

(1) 按照图1建立组网连接, 配置DSLAM和CPE1, 使网络分析仪1和网络分析仪3之间能正常收发数据流;

(2) 设置DSLAM过滤MAC源和/或目的地址规则;

(3) 网络分析仪1向网络分析仪3发送MAC源和/或目的地址为被过滤MAC源和/或目的地址的测试帧;

(4) 取消之前的配置, 网络分析仪1向网络分析仪3发送MAC目的地址为表1的地址的测试帧;

(5) 配置DSLAM, 将DSLAM中的MAC帧的处理方式由“缺省行为”改变为“可选配置”;

(6) 网络分析仪1向网络分析仪3发送MAC目的地址为表1中的地址的测试帧;

(7) 取消之前的配置, 设置DSLAM基于MAC目的地址、MAC源地址、MAC协议类型、IP目的地址、

IP源地址的部分和全部过滤规则进行过滤；

(8) 网络分析仪1向网络分析仪3发送符合步骤(7)中设置的规则的MAC帧，以及违反符合步骤(7)中设置的规则的MAC帧的两条流；

(9) 设置DSLAM过滤从用户端口发出组播UDP流；

(10) 网络分析仪2向网络分析仪3发送目的MAC和IP地址为组播地址的UDP数据流。

4.3.4 预期结果

(1) 在步骤(3)中，网络分析仪3不能收到测试帧；

(2) 在步骤(4)中，DSLAM对测试帧的处理应符合表1中的缺省行为；

(3) 在步骤(6)中，DSLAM对测试帧的处理应符合表1中的可选配置；

(4) 在步骤(8)中，网络分析仪3不能收到测试帧；

(5) 在步骤(10)中，网络分析仪3不能收到测试帧。

4.4 MAC地址控制功能

4.4.1 测试目的

DSLAM应当可以配置并限制从每个用户端口学习到的源MAC地址的数量。

DSLAM应能防止用户盗用BNG（例如接入服务器或业务路由器）端口的MAC地址。

DSLAM应可以拒绝向存在MAC地址重复的用户提供业务。

4.4.2 测试配置

测试配置如图1所示。

4.4.3 测试步骤

(1) 按照图 1 建立组网连接；

(2) 设置 DSLAM 从每个用户端口学习到的源 MAC 地址数量；

(3) 网络分析仪 1 连续发送具有不同源 MAC 地址的测试帧，其中源 MAC 地址数目大于 DSLAM 预设值；

(4) 查看 DSLAM MAC 地址表中学习到的源 MAC 地址数目以及对超过源 MAC 数量限定的流是否丢弃；

(5) 在 DSLAM 中配置 BNG 的 MAC 地址；

(6) 配置网络分析仪 2 发送源 MAC 地址为 BNG 的 MAC 地址的测试帧；

(7) 清除 DSLAM 中的 MAC 地址表；

(8) 配置网络分析仪 1 和 2 先后使用相同的源 MAC 地址 A 发送测试帧；

(9) 网络分析仪 3 向地址 A 发送以太网报文。

4.4.4 预期结果

(1) 在步骤(4)中，DSLAM学习到的MAC地址数量应等于配置的数量限值，且对于超出的流应进行丢弃；

(2) 在步骤(6)中，网络分析仪3应无法收到网络分析仪2发送的流；

(3) 在步骤(9)中，网络分析仪1可以收到网络分析仪3发送的报文，网络分析仪2不应收到。

4.5 广播/组播/DLF 速率抑制

4.5.1 测试目的

DSLAM应具备对MAC目的地址为广播或组播地址的报文以及未知单播（DLF）报文进行速率限制的功能，在上行方向应默认开启此功能。

DSLAM应支持基于全局的抑制方式，建议支持基于VLAN和端口的抑制方式。

4.5.2 测试配置

测试配置如图1所示。

4.5.3 测试步骤

全局抑制方式的测试步骤见步骤（2）至步骤（6），基于VLAN抑制方式的测试步骤见步骤（7）至步骤（9），基于端口抑制方式的测试步骤见步骤（10）至步骤（12）。

（1）按照图 1建立组网连接；

（2）网络分析仪1和2向网络分析仪3发送协议特定的广播/组播包和DLF报文；

（3）网络分析仪3向网络分析仪1和2发送协议特定的广播/组播包和DLF报文；

（4）通过网管控制台配置DSLAM全局抑制对应的广播/组播包和DLF报文的速率；

（5）网络分析仪1和2向网络分析仪3发送广播/组播包和DLF报文，发送速率选择大于配置的抑制速率，小于CPE与DSLAM间的DSL链路速率；

（6）网络分析仪3向网络分析仪1和2发送广播/组播包和DLF报文，发送速率选择大于配置的抑制速率，小于CPE与DSLAM间的DSL链路速率；

（7）配置DSLAM取消全局抑制广播/组播包的策略，配置DSLAM抑制VLAN ID=10的广播/组播包和DLF报文，并且DSLAM的上联口和CPE的用户端口为trunk模式；

（8）网络分析仪1和2向网络分析仪3发送两条广播/组播包流，一条VLAN ID=10，另一条配置为其它已知VLAN，发送速率选择大于配置的抑制速率，小于CPE与DSLAM间的DSL链路速率；

（9）网络分析仪3向网络分析仪1和2发送两条广播/组播包流，一条VLAN ID=10，另一条配置为其它已知VLAN，发送速率选择大于配置的抑制速率，小于CPE与DSLAM间的DSL链路速率；

（10）配置DSLAM取消基于VLAN抑制广播/组播包的策略，配置DSLAM抑制与CPE1连接的端口的广播/组播包和DLF报文；

（11）网络分析仪1和2向网络分析仪3发送广播/组播包和DLF报文，发送速率选择大于配置的抑制速率，小于CPE与DSLAM间的DSL链路速率；

（12）网络分析仪3向网络分析仪1和2发送广播/组播包和DLF报文，发送速率选择大于配置的抑制速率，小于CPE与DSLAM间的DSL链路速率。

4.5.4 预期结果

（1）在步骤（2）和步骤（3）中，双向都能收到全部的广播/组播包；

（2）在步骤（5）和步骤（6）中，双向收到的广播/组播包应符合预先设置的抑制策略；

（3）对于支持基于VLAN抑制方式的DSLAM设备，在步骤（8）和步骤（9）中，VLAN ID=10的广播/组播流应符合预先设置的抑制策略，其它VLAN的广播/组播包和DLF报文应全部收到。

（4）对于支持基于端口抑制方式的DSLAM设备，在步骤（11）和步骤（12）中，CPE2上下行方向的广播/组播流应全部被DSLAM设备转发，CPE1上下行方向的广播/组播流应符合预先设置的抑制策略。

4.6 静态绑定功能

4.6.1 测试目的

DSLAM应支持基于静态配置用户IP地址与DSL端口或VLAN的绑定功能。

被绑定的地址仅限于该端口使用，且该端口不能使用任何非绑定的地址。

4.6.2 测试配置

测试配置如图1所示。

4.6.3 测试步骤

- (1) 配置DSLAM静态分配IP地址192.168.0.10绑定到CPE1的用户端口；
- (2) 网络分析仪1和网络分析仪2向网络分析仪3发送源IP地址是192.168.0.10的数据流；
- (3) 网络分析仪3向网络分析仪1和网络分析仪2发送目的IP地址是192.168.0.10的数据流；
- (4) 网络分析仪1向网络分析仪3发送源IP地址是192.168.0.11的数据流；
- (5) 网络分析仪3向网络分析仪1发送目的IP地址是192.168.0.11的数据流；
- (6) 取消之前的绑定策略，配置DSLAM建立VLAN1（VLAN ID=10）和VLAN2（VLAN ID=20），静态分配IP地址段192.168.0.0/24绑定到VLAN1，并将DSLAM的上联口、CPE1加入到VLAN1，DSLAM的上联口和CPE2的用户端口加入到VLAN2；
- (7) 网络分析仪1向网络分析仪3发送源IP地址是192.168.0.10的数据流；
- (8) 网络分析仪2向网络分析仪3发送源IP地址是192.168.0.10的数据流；
- (9) 网络分析仪1向网络分析仪3发送源IP地址是192.168.1.10的数据流；
- (10) DSLAM修改CPE1的VLAN，将其从VLAN1中删除，接入到VLAN2；
- (11) 网络分析仪1向网络分析仪3发送源IP地址是192.168.0.10的数据流。

4.6.4 预期结果

- (1) 在步骤（2）中，网络分析仪3仅能收到网络分析仪1发送的数据流；
- (2) 在步骤（3）中，网络分析仪1能收到数据流，网络分析仪2不能收到数据流；
- (3) 在步骤（4）中，网络分析仪3不能收到数据流；
- (4) 在步骤（5）中，网络分析仪1不能收到数据流；
- (5) 在步骤（7）中，网络分析仪3能收到VLAN ID=10的数据流；
- (6) 在步骤（8）中，网络分析仪3不能收到网络分析仪2发出的数据流；
- (7) 在步骤（9）中，网络分析仪3不能收到网络分析仪1发出的数据流；
- (8) 在步骤（11）中，网络分析仪3不能收到网络分析仪1发出的数据流。

4.7 动态绑定功能（可选）

4.7.1 测试目的

DSLAM可选支持跟踪DHCP中的IP地址分配过程进行端口、MAC地址和IP地址的动态绑定功能。

被绑定的地址仅能限于该端口使用，且该端口不能使用任何非绑定的地址。

4.7.2 测试配置

测试配置如图1所示。

4.7.3 测试步骤

- (1) 在DSLAM配置CPE1和CPE2线路的动态IP地址绑定功能；
- (2) 网络分析仪3仿真DHCP服务器功能，配置地址池10.10.10.2~10.10.10.254，网关地址为10.10.10.1，更新时间为3600s；

- (3) 网络分析仪 3 配置端口地址为 10.10.10.1;
- (4) 网络分析仪 1 仿真 DHCP 客户端发起 DHCP 请求过程, 获得分配地址 10.10.10.A;
- (5) 网络分析仪 2 仿真 DHCP 客户端发起 DHCP 请求过程, 获得分配地址 10.10.10.B;
- (6) 网络分析仪 1 利用地址 10.10.10.A 与网络分析仪 3 互发 IP 数据流;
- (7) 网络分析仪 2 利用地址 10.10.10.B 与网络分析仪 3 互发 IP 数据流;
- (8) 配置网络分析仪 1 端口地址为 10.10.10.B;
- (9) 配置网络分析仪 2 端口地址为 10.10.10.C, 其中 $2 < C < 254$ 且 C 不等于 A 或 B ;
- (10) 网络分析仪 1 利用地址 10.10.10.B 与网络分析仪 3 互发 IP 数据流;
- (11) 网络分析仪 2 利用地址 10.10.10.C 与网络分析仪 3 互发 IP 数据流;
- (12) 网络分析仪 1 仿真 DHCP 客户端发起 DHCP 释放过程, 释放地址 10.10.10.A;
- (13) 解除 CPE2 对应线路端口的动态地址绑定功能;
- (14) 网络分析仪 2 利用地址 10.10.10.A 与网络分析仪 3 互发 IP 数据流。

4.7.4 预期结果

- (1) 在步骤 (6) 中, 网络分析仪 1 和 3 的 IP 数据流应可互相可达;
- (2) 在步骤 (7) 中, 网络分析仪 2 和 3 的 IP 数据流应可互相可达;
- (3) 在步骤 (10) 中, 网络分析仪 1 和 3 的 IP 数据流应互相不可达;
- (4) 在步骤 (11) 中, 网络分析仪 2 和 3 的 IP 数据流应互相不可达;
- (5) 在步骤 (14) 中, 网络分析仪 2 和 3 的 IP 数据流应互相可达。

4.8 上联口链路聚集功能测试

见 YD/T 1808-2008 《接入网设备测试方法——第二代及频谱扩展的第二代不对称数字用户线 (ADSL2/2+)》10.6.3。

4.9 上联口快速生成树(RSTP)功能测试

见 YD/T 1808-2008 《接入网设备测试方法——第二代及频谱扩展的第二代不对称数字用户线 (ADSL2/2+)》10.6.2。

4.10 端口镜像功能(可选)

4.10.1 测试目的

DSLAM 设备建议支持对特定的物理端口或逻辑端口 (PVC 或 VLAN) 的流镜像功能。

4.10.2 测试配置

测试配置如图 2 所示。

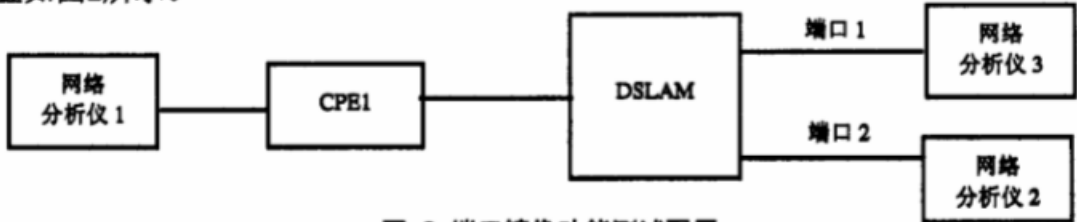


图 2 端口镜像功能测试配置

4.10.3 测试步骤

- (1) 如图 2 连接测试环境, 配置 DSLAM 上联端口 1 为镜像源端口, 上联端口 2 为镜像目的端口, 镜像端口 1 双向的流;
- (2) 网络分析仪 1 和网络分析仪 3 互发广播与组播和单播以太网帧。

4.10.4 预期结果

在步骤（2）中，网络分析仪1和3应可正常通信，网络分析仪2应可以收到网络分析仪1和网络分析仪3发出的帧。

4.11 协议报文限速

4.11.1 测试目的

DSLAM设备应支持对每用户端口发送的特定协议报文（例如，DHCP、IGMP、ICMP等）进行限速处理。

4.11.2 测试配置

测试配置如图1所示。

4.11.3 测试步骤

（1）在 DSLAM 中开启对特定协议报文的限速功能，设定每端口的限制速率 X ；

（2）配置网络分析仪 1 分别发送类型为 DHCP Discover、IGMP Report (v1、v2) 和 PING 的流，速率 Y ($Y > X$)。

4.11.4 预期结果

网络分析仪3接收到的网络分析仪1发送的各种协议流的速率均小于等于 X 。

4.12 用户环网检测

4.12.1 测试目的

DSLAM设备应支持对用户侧端口是否成环的检测，防止环网形成。

4.12.2 测试配置

测试配置如图3所示。

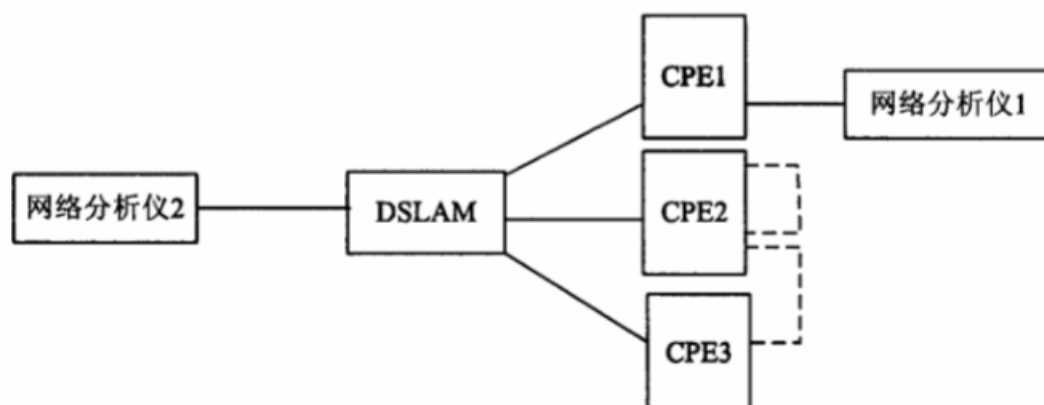


图3 用户环网检测功能测试配置

4.12.3 测试步骤

（1）按照图3建立组网连接，其中虚线部分不进行连接，并开启DSLAM的用户环网检测功能；

（2）网络分析仪1分别与CPE1、CPE2和CPE3相连，确认3个CPE都能和DSLAM正常收发包；

（3）将CPE2的用户端口用交叉网线连接成环，网络分析仪1与CPE1相连，并与网络分析仪2之间发送双向数据流；

（4）将CPE2的用户端口环解除，将CPE2的用户端口与CPE3的用户端口用交叉网线相连；

（5）网络分析仪1与CPE1相连，并与网络分析仪2之间发送双向数据流。

4.12.4 预期结果

(1) 在步骤(3)中, DSLAM应报告用户侧环网事件, 并主动断开成环的链路, CPE1/2/3与DSLAM之间能够正常收发数据流;

(2) 在步骤(5)中, DSLAM应报告用户侧环网事件, 并主动断开成环的链路, CPE1/2/3与DSLAM之间能够正常收发数据流。

5 控制平面安全功能测试

5.1 IGMP Snooping 代理功能和可控组播功能

5.1.1 测试目的

DSLAM设备应支持IGMP Snooping代理功能, 该功能定义见YD/T 1706-2007《接入网技术要求——数字用户线(DSL)承载宽带业务》3.8。

DSLAM设备应支持基于用户和组播组的访问控制功能, 防止非法用户获得无权限收看的内容。

5.1.2 测试配置

测试配置如图1所示。

5.1.3 测试步骤

(1) 按图1连接测试环境, 开启DSLAM中的IGMP Snooping代理功能和快速离开功能;

(2) 配置网络分析仪3仿真组播路由器功能, 配置组播频道239.1.1.1, 并周期性发送IGMP Query消息;

(3) DSLAM中增加节目239.1.1.1, 并将端口1和端口2用户加入观看权限;

(4) 网络分析仪1发送IGMP report报文申请加入239.1.1.1的节目组;

(5) 网络分析仪2发送IGMP report报文申请加入239.1.1.1的节目组;

(6) 网络分析仪1发送IGMP leave报文申请离开239.1.1.1的节目组;

(7) 网络分析仪2发送IGMP leave报文申请离开239.1.1.1的节目组;

(8) DSLAM配置改变端口2的用户为禁止;

(9) 网络分析仪1发送IGMP report报文申请加入239.1.1.1的节目组;

(10) 网络分析仪2发送IGMP report报文申请加入239.1.1.1的节目组。

5.1.4 预期结果

(1) 在步骤(4)中, 网络分析仪3应收到DSLAM发出的IGMP report报文请求239.1.1.1的节目, 网络分析仪1应收到该节目流;

(2) 在步骤(5)中, 网络分析仪3不应收到DSLAM发出的请求239.1.1.1的节目的IGMP report报文, 网络分析仪2应收到该节目流;

(3) 在步骤(6)中, 网络分析仪3不应收到IGMP leave报文, 网络分析仪1收到的节目流应停止;

(4) 在步骤(7)中, 网络分析仪3应收到DSLAM发出的IGMP leave报文, 网络分析仪2收到的节目流应停止;

(5) 在步骤(9)中, 网络分析仪1应接收到该节目流;

(6) 在步骤(10)中, 网络分析仪2不应接收到该节目流。

5.2 非法组播源过滤

5.2.1 测试目的

DSLAM应可配置为过滤从用户端口发出的IGMP查询包。

DSLAM应支持对网络侧合法组播源的配置和对非法组播源进行过滤的配置。

5.2.2 测试配置

测试配置如图1所示。

5.2.3 测试步骤

- (1) 按图 1 连接测试环境，在 DSLAM 中配置组播频道 239.1.1.1,并将端口 1 设为观看权限；
- (2) 网络分析仪 1 分别发送针对 239.1.1.1 和 239.1.1.2 的 IGMP query 报文；
- (3) 配置网络分析仪 3 仿真组播路由器功能，配置组播频道 239.1.1.1，并周期性发送相应的 IGMP query 消息；
- (4) 网络分析仪 1 和 2 分别发送对频道 239.1.1.1 的 IGMP report 报文；
- (5) 网络分析仪 1 和 2 分别发送对频道 239.1.1.2 的 IGMP report 报文。

5.2.4 预期结果

- (1) 在步骤 (2) 中，网络分析仪3不应收到任何IGMP query报文；
- (2) 在步骤 (4) 中，网络分析仪1应接收到来自网络分析仪3的组播流239.1.1.1，网络分析仪2不应接收到任何组播流；
- (3) 在步骤 (5) 中，网络分析仪1和2都不应接收到任何组播流。

5.3 ARP 代理功能

5.3.1 测试目的

建议DSLAM支持对ARP协议的代理功能。

对于支持三层转发功能的DSLAM，该功能为必选。

5.3.2 测试配置

测试配置如图1所示。

5.3.3 测试步骤

- (1) 按图 1 连接测试环境，在 DSLAM 中配置启动 proxy ARP 功能；
- (2) 配置 DSLAM 端口 1 和端口 2 分别位于不同的 C-VLAN；
- (3) 配置网络分析仪 1 的端口 IP 地址和 MAC 地址分别为 10.10.10.10 和 00-00-10-10-10-10；
- (4) 配置网络分析仪 2 的端口 IP 地址和 MAC 地址分别为 10.10.10.12 和 00-00-10-10-10-12；
- (5) 配置网络分析仪 1 和 2 都自动响应 ARP 查询；
- (6) 网络分析仪 1 发送针对 IP 地址 10.10.10.12 的 ARP 查询报文；
- (7) 网络分析仪 2 发送针对 IP 地址 10.10.10.10 的 ARP 查询报文。

5.3.4 预期结果

- (1) 在步骤 (6) 中，网络分析仪1应接收到DSLAM以自身MAC地址响应的ARP响应报文；
- (2) 在步骤 (7) 中，网络分析仪2应接收到DSLAM以自身MAC地址响应的ARP响应报文。

5.4 端口定位功能测试

见YD/T 1808-2008《接入网设备测试方法——第二代及频谱扩展的第二代不对称数字用户线(ADSL2/2+)》10.3。

5.5 防 DoS 攻击

5.5.1 测试目的

应具备对攻击目标为本设备的DoS攻击抵御能力，例如Ping of Death、SYN Flood、LAND等攻击。

5.5.2 测试配置

测试配置如图4所示。

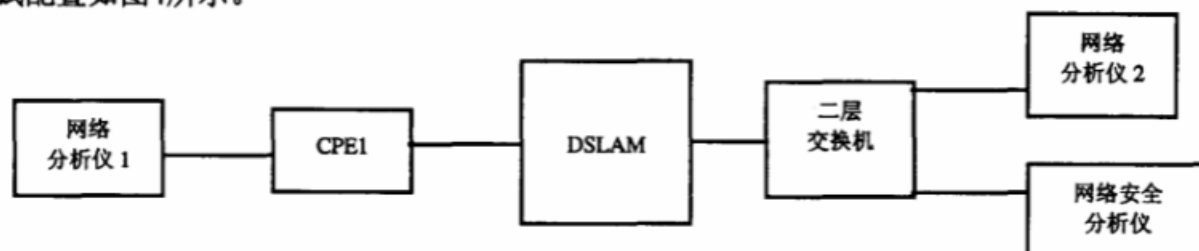


图 4 防 DoS 攻击功能测试配置

5.5.3 测试步骤

- (1) 按图 4 连接测试环境，配置 DSLAM 网络侧管理地址 A.B.C.D；
- (2) 配置网络分析仪 1 和网络分析仪 2 互发广播和一定速率的单播以太网帧；
- (3) 网络安全分析仪以地址 A.B.C.D 为目标进行 DoS 攻击测试，攻击报文速率为 100Mbit/s 以太网口线速速率。

5.5.4 预期结果

在步骤（3）中，网络分析仪1和网络分析仪2之间的以太网数据流应正常转发，不出现丢包。

5.6 DHCP 下行安全功能测试

5.6.1 测试目的

针对特定用户的下行DHCP响应报文不应被转发到其它用户端口，防止其它用户通过嗅探该报文获得该用户的IP地址。

5.6.2 测试配置

测试配置如图5所示。

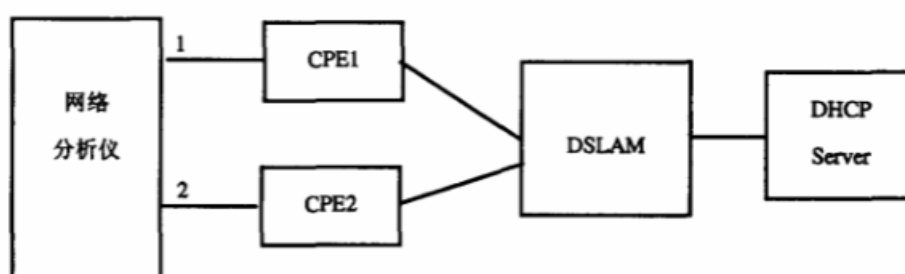


图 5 DHCP 下行安全功能测试配置

5.6.3 测试步骤

- (1) 按图 5 连接测试环境；
- (2) CPE1 和 CPE2 配置为桥接模式；
- (3) 验证 CPE1 和 CPE2 上线后，验证网络分析仪可以经 DSLAM 与 DHCP Server 互通。
- (4) 网络分析仪端口 2 启动接收抓取；
- (5) 网络分析仪端口 1 启动 DHCP Client 的地址获取过程；
- (6) 等待网络分析仪端口 1 从 DHCP Server 获得地址过程成功完成；
- (7) 停止网络分析仪端口 2 的抓取，观察收到的报文。

5.6.4 预期结果

在步骤（7）中，网络分析仪端口2不应接收端口1与DHCP Server交互的任何报文。

6 管理平面安全功能测试

6.1 口令安全检查机制测试

6.1.1 测试目的

用户进行网络管理时所使用的登录口令的长度应不少于8个字符，并且应由数字、字母或特殊符号组成，DSLAM网管系统应提供检查机制，保证每个口令至少是由前述的三类符号中的两类组成。

6.1.2 测试配置

测试配置如图6所示。

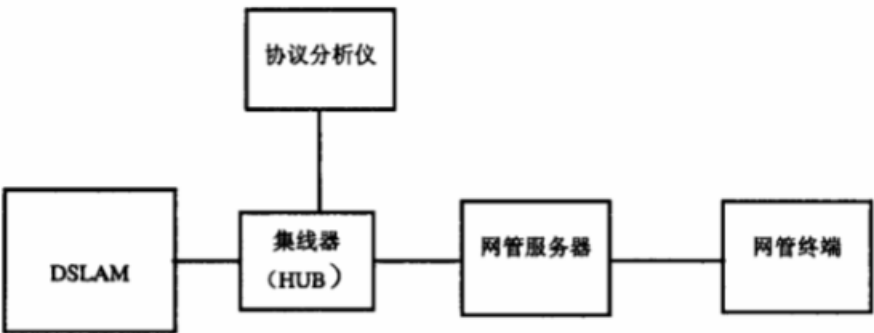


图 6 网管功能测试配置

6.1.3 测试步骤

- (1) 以管理员身份登录网管服务器；
- (2) 选择配置管理员口令；
- (3) 更改为 8 位全数字口令；
- (4) 更改为 8 位全字母口令；
- (5) 更改为小于 8 位的任意口令；
- (6) 更改为 8 位包含数字、字母、特殊符号中两类的口令。

6.1.4 预期结果

- (1) 在步骤 (3)、(4)、(5) 中，系统拒绝更改口令，并给出相应安全提示；
- (2) 在步骤 (6) 中，口令更改成功，可以使用新口令重新登录系统。

6.2 SNMP 管理访问安全测试

6.2.1 测试目的

验证设备和网管之间SNMP v1/v2c管理的安全性。

6.2.2 测试配置

测试配置如图6所示。

6.2.3 测试步骤

- (1) 在设备上配置允许使用 SNMP 访问设备的网管站的地址 A；
- (2) 修改网管服务器地址为非 A，通过网管服务器进行管理操作；
- (3) 配置网管服务器地址为 A，通过网管服务器进行管理操作；
- (4) 通过协议分析仪分析 SNMP 报文。

6.2.4 预期结果

- (1) 在步骤 (2) 中，设备应可拒绝非法网管接入设备；
- (2) 在步骤 (4) 中，管理过程中不应使用public/private作为团体名，只读团体名和读写团体名称不

能相同。

6.3 Telnet 管理访问安全测试（可选）

6.3.1 测试目的

验证设备Telnet管理的安全性。

6.3.2 测试配置

测试配置如图7所示。

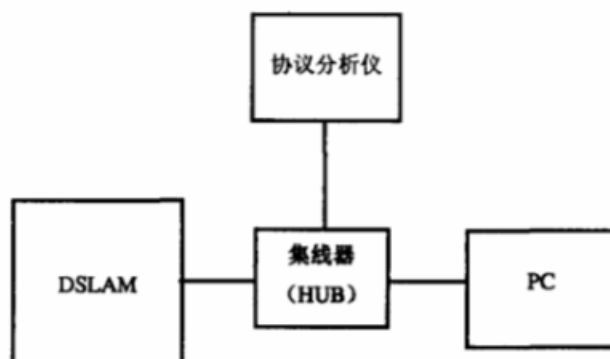


图7 Telnet 安全功能测试配置

6.3.3 测试步骤

- (1) 关闭 DSLAM 设备上的 Telnet 管理功能；
- (2) 在 PC 上启动 Telnet 客户端，使用最高等级管理员身份登录 DSLAM；
- (3) 开启 DSLAM 设备上的 Telnet 管理功能；
- (4) 在 PC 上启动 Telnet 客户端，使用最高等级管理员身份登录 DSLAM；
- (5) 通过 Telnet 客户端在 DSLAM 上创建一个低等级 Telnet 管理员；
- (6) 设定可同时访问的 Telnet 用户数量为 1；
- (7) 在 PC 上启动 Telnet 另一个客户端，使用在步骤（3）中创建的用户登录；
- (8) 解除步骤（6）中的数量限定；
- (9) 在 PC 上启动 Telnet 另一个客户端，使用在步骤（3）中创建的用户登录；
- (10) 在 DSLAM 上设定允许 Telnet 方式访问的客户端主机地址为 PC 当前地址；
- (11) 注销 PC 上的所有 Telnet 连接，修改自身地址为同一网段其它地址；
- (12) 在 PC 上启动 Telnet 客户端，试图登录 DSLAM；
- (13) 将 PC 自身地址改回；
- (14) 在 PC 上启动 Telnet 客户端，登录 DSLAM，不进行任何操作，等待超时；
- (15) 在 PC 上重新启动 Telnet 客户端，使用错误的用户名或密码连续进行登录试探。

6.3.4 预期结果

- (1) 在步骤（2）中，Telnet客户端应无法连接成功；
- (2) 在步骤（4）中，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；
- (3) 在步骤（5）中，DSLAM应提供对Telnet用户权限的控制功能；
- (4) 在步骤（7）中，Telnet客户端应无法登录；
- (5) 在步骤（9）中，Telnet客户端应登录成功；
- (6) 在步骤（12）中，Telnet客户端应无法连接成功或无法通过登录验证；

(7) 在步骤(14)中, 在设定的时间内不进行交互, 用户应自动被注销, 提供终端超时锁定功能;

(8) 在步骤(15)中, DSLAM应通过延时响应或限定错误尝试次数等方式防范密码试探攻击。

6.4 本地终端(Console)管理访问安全测试

6.4.1 测试目的

验证设备本地终端管理的安全性。

6.4.2 测试配置

使用Console口在本地连接设备。

6.4.3 测试步骤

(1) 在 PC 上启动终端, 使用最高等级管理员身份登录 DSLAM;

(2) 通过终端在 DSLAM 上创建一个低等级 Console 管理员;

(3) 在 PC 上启动 Console 终端, 登录 DSLAM, 不进行任何操作, 等待超时;

(4) 在 PC 上重新启动 Console 终端, 使用错误的用户名或密码连续进行登录试探。

6.4.4 预期结果

(1) 在步骤(1)中, 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;

(2) 在步骤(2)中, DSLAM应提供对Console用户权限的控制功能;

(3) 在步骤(3)中, 在设定的时间内不进行交互, 用户应自动被注销, 提供终端超时锁定功能;

(4) 在步骤(4)中, DSLAM应通过延时响应或限定错误尝试次数等方式防范密码试探攻击。

6.5 Web 管理访问安全测试(可选)

6.5.1 测试目的

验证设备Web管理的安全性。

6.5.2 测试配置

测试配置如图7所示。

6.5.3 测试步骤

(1) 关闭 DSLAM 设备上的 Web 管理功能;

(2) 在 PC 上启动 HTTPS 客户端, 使用最高等级管理员身份登录 DSLAM;

(3) 开启 DSLAM 设备上的 Web 管理功能;

(4) 在 PC 上启动 HTTPS 客户端, 使用最高等级管理员身份登录 DSLAM;

(5) 在 DSLAM 上设定允许 Web 方式访问的客户端主机地址为 PC 当前地址;

(6) 关闭 PC 上的 HTTPS 客户端, 修改 PC 自身地址为同一网段其它地址;

(7) 在 PC 上启动 HTTPS 客户端, 试图登录 DSLAM;

(8) 将 PC 自身地址改回;

(9) 在 PC 上启动 HTTPS 客户端, 登录 DSLAM, 不进行任何操作, 等待超时;

(10) 在 PC 上重新启动 HTTPS 客户端, 使用错误的用户名或密码连续进行登录试探。

6.5.4 预期结果

(1) 在步骤(2)中, HTTPS客户端应无法连接成功;

(2) 在步骤(4)中, 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;

(3) 在步骤(7)中, HTTPS客户端应无法登录;

- (4) 在步骤(9)中, HTTPS客户端应登录成功;
- (5) 在步骤(9)中, 在设定的时间内不进行交互, 用户应自动被注销, 提供终端超时锁定功能;
- (6) 在步骤(10)中, DSLAM应通过延时响应或限定错误尝试次数方式防范密码试探攻击。

6.6 安全策略管理功能测试

6.6.1 测试目的

网管系统应能提供统一的安全策略控制。

6.6.2 测试配置

测试配置如图6所示。

6.6.3 测试步骤和预期结果

在图形网管中检查下列网管项目的配置。

- (1) 登录策略管理: 提供设置非法登录系统的次数及锁定时间, 设置管理用户的账号有效期, 设置登录超时退出时间、账号登录时间段、限制同一账号最大连接数等功能。
- (2) 提供管理用户的功能。
- (3) 管理用户密码设置策略: 限制管理用户设置的密码长度、密码组成, 提供密码重置功能, 设置用户密码有效天数等。
- (4) 支持管理用户登录的IP管理策略, 将登录的管理用户与IP地址绑定。

6.7 角色管理功能测试

6.7.1 测试目的

网管系统应能提供灵活的角色控制功能。

6.7.2 测试配置

测试配置如图6所示。

6.7.3 测试步骤和预期结果

在图形网管中检查下列网管项目的配置。

角色管理功能应包含:

- (1) 增加、删除、修改角色;
- (2) 给角色分配管理资源(可管理的对象范围)和操作权限。

网管系统应可以提供以下三类缺省的角色。

- (1) 系统管理员: 可以执行网管系统提供的所有功能项, 包括权限分配功能。
- (2) 配置管理员: 可以执行网管系统提供的对设备和系统自身有数据修改权限的功能(不包括权限分配功能), 如资源维护、设备配置、版本升级、系统维护等。
- (3) 监控管理员: 可以执行网管系统提供的对设备的监控和网管系统自身的查询和审计等功能, 如资源查询、告警监控、性能统计、日志查询等。

网管系统应提供灵活的角色创建功能。

6.8 账号管理功能测试

6.8.1 测试目的

网管系统应能提供完善的账号管理功能。

6.8.2 测试配置

测试配置如图6所示。

6.8.3 测试步骤和预期结果

在图形网管中检查下列网管项目。

对使用网管系统的管理用户账号进行管理维护，包括：

- (1) 增加账号；
- (2) 删除账号；
- (3) 修改账号信息；
- (4) 查询账号信息。

管理用户的账号信息包括：

- (1) 用户账号；
- (2) 用户密码；
- (3) 密码有效期；
- (4) 用户所属角色；
- (5) 附加说明。

6.9 用户登录管理测试

6.9.1 测试目的

网管系统应能提供完善的用户登录管理功能。

6.9.2 测试配置

测试配置如图6所示。

6.9.3 测试步骤和预期结果

在图形网管中检查下列网管项目：

- (1) 只有在服务器中已经注册的用户才能登录到网管系统，如果启动了访问控制列表功能，则客户端必须同时满足存在于网管系统 ACL 表中的用户才能登录到网管系统；
- (2) 登录的用户只具有已经被授权的指定操作；
- (3) 登录失败告警，使用同一管理账号连续多次登录失败时，网管系统应产生非法登录告警，并对该管理账号进行锁定；
- (4) 手工注销登录的用户；
- (5) 手工或超时自动锁定客户端或退出。

6.10 在线用户管理功能测试

6.10.1 测试目的

网管系统应能提供在线用户管理功能。

6.10.2 测试配置

测试配置如图6所示。

6.10.3 测试步骤和预期结果

在图形网管中检查下列网管项目。

- (1) 网管系统应能对在线用户进行监视，能够实时监视在线用户的登录情况，包括：
 - 登录用户；

- 登录时间;
- 操作终端信息。

(2) 网管系统应能对在线用户进行管理, 超级用户能够查看一般用户所做的操作, 并强制其退出。

6.11 日志管理功能测试

6.11.1 测试目的

管理用户可以根据给定条件对日志进行查询, 并可对查询到的日志进行排序。

6.11.2 测试配置

测试配置如图6所示。

6.11.3 测试步骤和预期结果

在图形网管中检查下列网管项目。

日志查询的条件为:

- (1) 给定时间或时间段进行查询;
- (2) 给定用户进行查询;
- (3) 给定的日志类型。

可以查询到的信息包括:

- (1) 日志类型, 包括操作日志、系统日志、安全日志;
- (2) 操作时间;
- (3) 操作人;
- (4) 操作名称;
- (5) 操作对象;
- (6) 操作内容;
- (7) 操作终端;
- (8) 操作结果(例如成功或失败)。

7 其他安全功能测试

7.1 线路故障诊断功能测试

见 YD/T 1808-2008 《数字设备测试方法——第二代及频谱扩展的第二代不对称数字用户线(ADSL2/2+)》 9.4。

7.2 主控板主备倒换功能测试

见 YD/T 1808-2008 《数字设备测试方法——第二代及频谱扩展的第二代不对称数字用户线(ADSL2/2+)》 10.8。

7.3 环境监控功能测试

7.3.1 测试目的

DSLAM设备应能提供对设备风扇工作情况、内部温度等环境信息的收集和上报功能。

7.3.2 测试配置

测试配置如图6所示。

7.3.3 测试步骤

- (1) 登录 DSLAM 网管系统;

(2) 在网管系统中查看设备内环境监控信息。

7.3.4 预期结果

在步骤(2)中,应可看到设备风扇工作情况、内部温度等环境信息。

7.4 电源安全性测试

7.4.1 测试目的

对于采用单独电源模块集中供电设备,应支持双电源模块热备份功能。

对于分散单板供电设备,应提供两个互为备份的电源接口。

7.4.2 测试配置

见图 1,并按照设备情况接通双路电源。

7.4.3 测试步骤

(1) 配置网络分析仪 1 和网络分析仪 3 按照线路带宽互发单播数据流;

(2) 断掉其中一路电源供应。

7.4.4 预期结果

在步骤(2)中在电源切换过程中,业务应不受影响。

附录 A

(资料性附录)

安全相关性能测试方法

A.1 概述

本附录提供了对安全功能启用后对设备转发性能的影响的测试方法。由于安全性能的指标和全面的评估方法仍需进一步研究，本附录仅作为资料性内容供参考使用。

A.2 MAC地址过滤条目测试

A.2.1 测试目的

测试DSLAM设备可以支持的最大MAC地址过滤条目数以及对转发性能的影响。

A.2.2 测试配置

测试配置如图A.1所示。

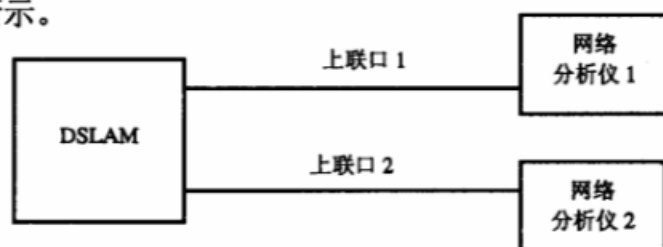


图 A.1 MAC 地址过滤条目测试配置

A.2.3 测试步骤

- (1) 按照图 A.1 连接，使用网络分析仪测试 DSLAM 上联口间吞吐量；
- (2) 配置 DSLAM 设置对 MAC 源地址 M_1 的过滤规则，继续增加配置过滤条目，若设备可支持 n 条规则，则配置到设备支持最大条目 M_n ；
- (3) 配置流量发生器发送 n 条流，其 MAC 源地址分别为 $M_1 \dots M_n$ ，验证这 n 条流是否可以通过；
- (4) 使用网络分析仪测试 DSLAM 上联口间吞吐量，其中测试流的 MAC 地址不属于 $\{M_1, \dots, M_n\}$ ；
- (5) 比较步骤 (4) 与步骤 (1) 中的测试结果。

A.2.4 预期结果

- (1) 在步骤 (3) 中， n 条流应不能通过 DSLAM 转发；
- (2) 在步骤 (5) 中，步骤 (4) 测得吞吐量与步骤 (1) 中相比应无明显下降。