YD

中华人民共和国通信行业标准

YD/T 1900-2009

深度包检测设备测试方法

Test Method of Deep Packet Inspection Device

2009-06-15 发布　　2009-09-01 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　定义、术语及缩略语……1
4　测试拓扑……4
5　接口测试……5
6　接入方式测试……10
7　QoS 测试……11
8　业务识别功能测试……16
9　业务控制功能测试……25
10　可靠性测试……34
11　可扩展性测试……36
12　统计报表功能测试……37
13　管理功能测试……38
14　附加功能测试……46
15　系统性能测试……47
16　供电测试……50
17　电气安全测试……50

前　言

本标准是“互联网业务识别”系列标准之一。该系列标准的预计结构和名称如下：

1.YD/T 1901-2009《互联网业务识别系统应用场景和总体需求》；

2.《互联网业务识别系统总体框架》；

3. YD/T 1899-2009《深度包检测设备技术要求》；

4. YD/T 1900-2009《深度包检测设备测试方法》；

YD/T 1899-2009《深度包检测设备技术要求》是本标准的技术依据，使用时需与其配套使用。

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　科、田　辉、唐　浩、田慧蓉

深度包检测设备测试方法

1 范围

本标准规定了深度包检测设备的测试方法，包括：接口测试、组网方式测试、QoS 测试、业务识别功能测试、业务控制功能测试、可靠性测试、可扩展性测试、统计报表功能测试、管理功能测试、附加功能测试和性能测试。

本标准适用于深度包检测设备，其他集成深度包检测功能的网络设备也可参考使用。

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 1156　　路由器测试规范——高端路由器

YD/T 1167-2001　　STM-64 分插复用（ADM）设备技术要求

3 术语、定义及缩略语

3.1 术语和定义

下列术语和定义适用于本标准。

3.1.1

业务数据流识别　Application Awareness

指利用端口号检测、报文特征检测、协议解析、关联识别、行为特征检测等技术对网络中业务数据流量的业务类型、业务状态、流量比例和用户行为等进行分类统计和标识。

3.1.2

业务数据流控制　Application Control

指在业务数据流识别结果的基础上，参照业务数据流控制策略信息，利用流量管理、资源调度等流量控制手段，对网络业务数据流量进行精细化管理。

3.1.3

深度包检测设备　Deep Packt Inspection Device

指具备业务数据流识别、业务数据流控制能力，主要工作在 OSI 模型传输层到应用层，具备高数据流处理能力，能够对网络所承载的业务进行识别和流量管理的，可部署在网络骨干层、城域网和企业内部的网络设备。

3.1.4

流量整形　Traffic Shaping

根据业务数据流识别的结果，对数据流量采用阻塞、随机丢包、或者提供 QoS 控制等方式，对符合策略控制条件的数据流量进行流量管理和资源调度。

3.1.5

连接干扰/信令干扰　Connections/Signals Disturb

根据业务数据流识别的结果，复制数据流的 IP 五元组信息，并交换源/目的 IP、源/母的端口。针对 TCP 流量，伪造成为业务数据流连接的对端，发送标准的 TCP RST/FIN 数据包，中断业务数据流 TCP 连接，或者引发业务数据流 TCP 连接的重传，实现业务数据流控制；针对 UDP 流量，伪造成业务数据流会话的对端，发送业务数据流的应用层信令消息，中断 UDP 会话，或者发送干扰数据包，劣化 UDP 会话性能，实现业务数据流控制。

3.1.6

串联接入方式　Serial Connection

深度包检测设备实现业务数据流识别与业务数据流控制的一种方式，如图 1 所示。深度包检测设备串联在被监控链路中间，业务流量穿过深度包检测设备，深度包检测设备对业务流量实施业务识别与业务控制，适用于采用流量整形的业务数据流控制方法。

图 1　深度包检测设备串联接入方式

3.1.7

并联接入方式　Parallel Connection

深度包检测设备实现业务数据流识别与业务数据流控制的一种方式，如图 2 所示。深度包检测设备通过流量分离设备，复制被监控链路的业务流量到深度包检测设备实施业务流量识别，并通过被控系统预留的接口实施业务控制，适用于采用连接/信令干扰的业务数据流控制方法。

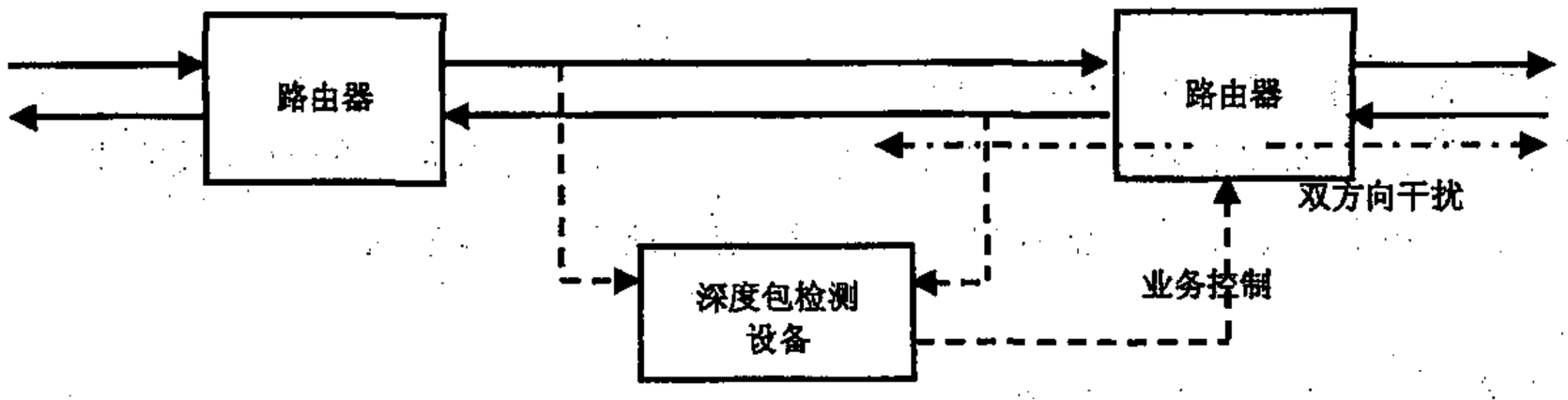


图 2　深度包检测设备并联接入方式

3.1.8

被测设备　DUT

被测设备指具备业务数据流识别和业务数据流控制功能的实际系统，本标准中指代深度包检测设备。

3.1.9

用户/用户组　User/User Group

用户是指使用某种具体应用，并参与应用数据交换的单独的终端，由用户 ID 标识，该用户 ID 可以是 MAC 地址、IP 地址、VLAN Tag、IP 地址或者是地理位置上的某一个点。用户组是满足特定条件的用户的集合。

3.2　缩略语

下列缩略语适用于本标准。

API	Application Programming Interface	应用编程接口
ARP	Address Resolution Protocol	地址解析协议

BGP	The Border Gateway Protocol	边界网关协议
BRAS	Broadband Remote Access Server	宽带接入服务器
BSS	Business Support System	运营支撑系统
CDN	Content Delivery Network	内容分发网络
CPU	Center Processing Unit	中央处理单元
CSV	Comma Separated Value	逗号分隔值
DFI	Deep Flow Inspection	深度流检测
DHCP	Dynamic Host Configuration Protocol	动态主机配置协议
DNS	Domain Name System or Service	域名系统/服务
DPI	Deep Packet Inspection	深度包检测
DSCP	Diffserv Service Code Point	差分服务编码点
DSLAM	Digital Subscriber Line Access Multiplexer	数字用户线接入复用器
EGP	Exterior Gateway Protocol	外部网关协议
FTP	File Transfer Protocol	文件传输协议
GRE	General Routing Encapsulation	通用路由封装
HTML	HyperText Markup Language	超文本标记语言
HTTP	HyperText Transfer Protocol	超文本传输协议
HTTPS	Secure Hypertext Transfer Protocol	安全超文本传输协议
ICMP	Internet Control Message Protocol	互联网控制消息协议
IGMP	Internet Group Management Protocol-	互联网群组管理协议
IM	Instant Message	即时消息
IMAP	Internet Message Access Protocol	互联网信息访问协议
IP	Internet Protocol	互联网协议
IPSec	Internet Protocol Security	互联网安全协议
L2TP	Level 2 Tunneling Protocol	二层隧道协议
LDAP	Lightweight Directory Access Protocol	轻量级目录访问协议
MGCP	Media Gateway Control Protocol	媒体网关控制协议
MIB	Management Information Base	管理信息
MMS	Microsoft Media Server Protocol	微软媒体服务器协议
MPLS	Multi-Protocol Label Switching	多协议标记交换
NPP	Network Printing Protocol	网络打印协议
NTP	Network Time Protocol	网络时间协议
OSI	Open System Interconnect	开放式系统互联
OSPF	Open Shortest Path First	开放最短路径优先
P2P	Peer to Peer	对等端
POP	Post Office Protocol	邮局协议
PPPoE	Point-to-Point Protocol over Ethernet	基于局域网的点对点通讯协议
PPTP	Point-to-point tunneling protocol	点对点隧道协议

QoS	Quality of Service	服务质量
RADIUS	Remote Authentication Dial In User Service	远程认证拨入用户协议
RDP	Remote Desktop Protocol	远程桌面协议
RDT	Real Data Transport	实时数据传输
RIP	Routing Information Protocol	路由信息协议
RMON	Remote Network Monitoring	远程网络监控
RTP	Real Time Transport Protocol	实时传输协议
RTSP	Real Time Streaming Protocol	实时流协议
SAP	Service Advertising Protocol	服务广告协议
SIP	Session Initiation Protocol	会话初始协议
SMTP	Simple Mail Transfer Protocol	简单邮件传输协议
SNMP	Simple Network Management Protocol	简单网络管理协议
SQL	Structured Query Language	结构化查询语言
SSH	Secure Shell Protocol	安全外壳协议
SSL	Secure Sockets Layer	安全套接层
TCP	Transmission Control Protocol	传输控制协议
TFTP	Trivial File Transfer Protocol	普通文件传输协议
TACACS	Terminal Access Controller Access-Control System	终端接入控制器接入控制系统
UDP	User Datagram Protocol	用户数据报协议
VLAN	Virtual Local Area Network	虚拟局域网
VoIP	Voice over IP	IP 电话
VPN	Virtual Private Protocol	虚拟专用网
XML	eXtended Markup Language	扩展标记语言

4 测试拓扑

下列测试拓扑适用于本标准。其中，图3的测试拓扑1适用于采用串联接入方式的深度包检测设备的功能测试；图4的测试拓扑2适用于采用并联接入方式的深度包检测设备的功能测试；图5的测试拓扑3适用于深度包检测设备的性能测试。

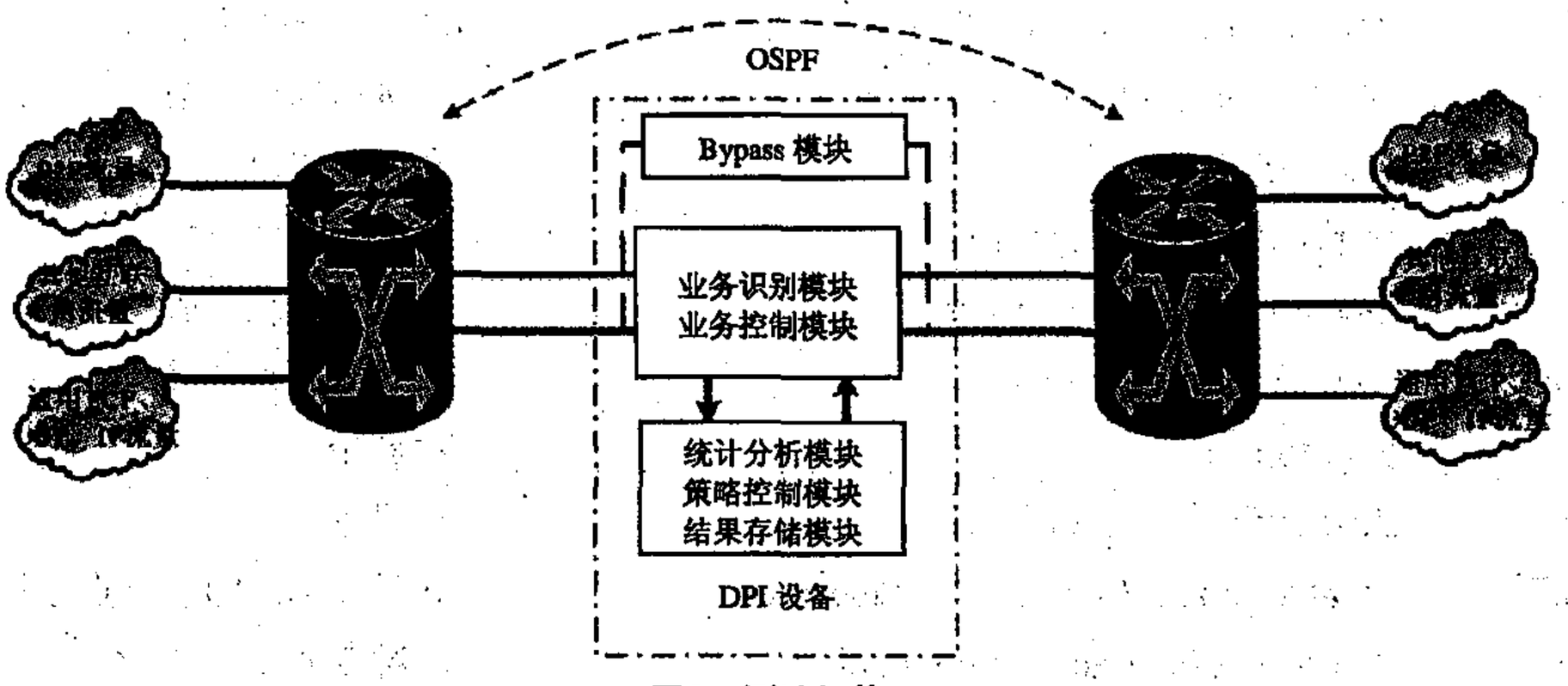


图3 测试拓扑1

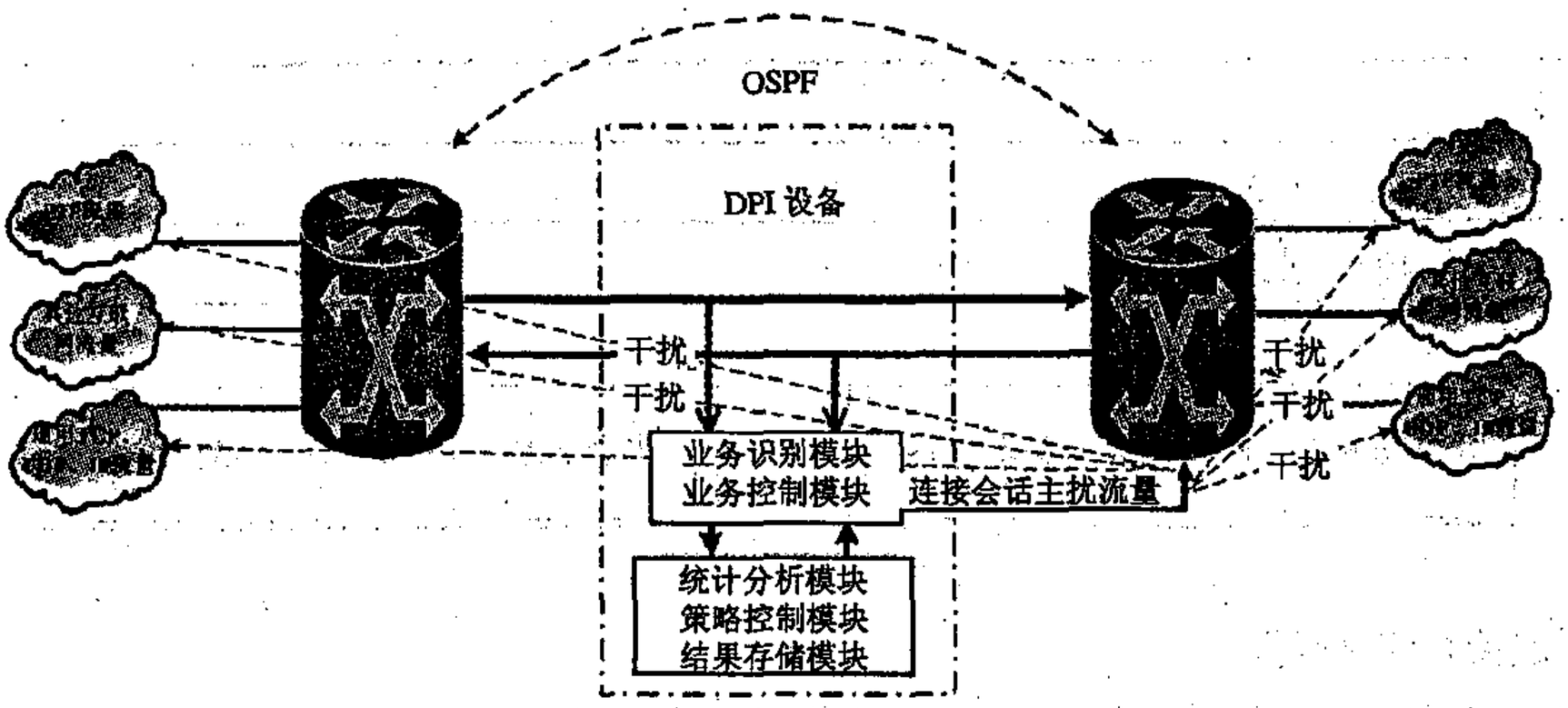


图4 测试拓扑2

图5 测试拓扑3

5 接口测试

5.1 概述

本章规定了深度包检测设备的接口测试方法，包括：吉比特以太网接口、STM-16 POS 接口和 STM-64 POS 接口。

5.2 吉比特以太网接口测试

吉比特以太网接口测试参见 YD/T 1156《路由器测试规范—高端路由器》第 4.3 节。

5.3 POS 接口测试

5.3.1 STM-16 POS 接口测试

STM-16 POS 接口测试参见 YD/T 1156《路由器测试规范—高端路由器》第 4.4 节。

5.3.2 STM-64 POS 接口测试

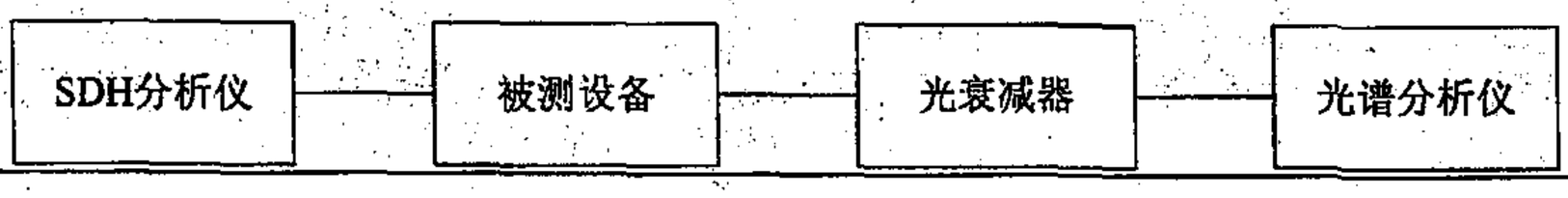
测试编号：1
分项目编号：POS_STM-64_1
测试项目：光源工作波长
测试配置： 被测设备 —— 多波分析仪
测试步骤： （1） 如图连接好测试配置； （2） 设置多波长分析仪的显示波长范围并将波形显示在屏幕中央，调节纵向光标处于波形的峰值出，读出并记录峰值处的中心波长值
预期结果：1530~1565nm
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：2

分项目编号：IF_STM-64_2

测试项目：最小边模抑制比

测试配置：



测试步骤：

（1） 如图连接好测试配置；

（2） 调节光衰减器，使输出光功率在光谱分析仪要求的范围内；

（3） 测量主纵模的功率 M_1；

（4） 测量最显著边模的功率 M_2；

（5） 计算最小边模抑制比

预期结果：≥30dB

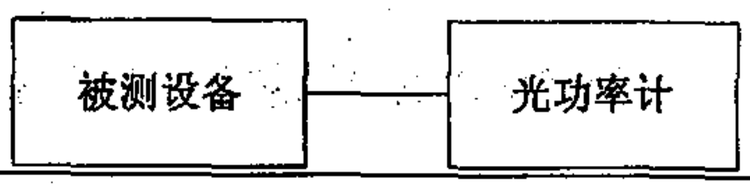
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：3

分项目编号：IF_STM-64_3

测试项目：平均发送光功率

测试配置：



测试步骤：

（1） 如图连接好测试配置；

（2） 将光功率计设置在适当的波长窗口，待读数稳定后，读出并记录光功率数值

预期结果：－1~－5dBm

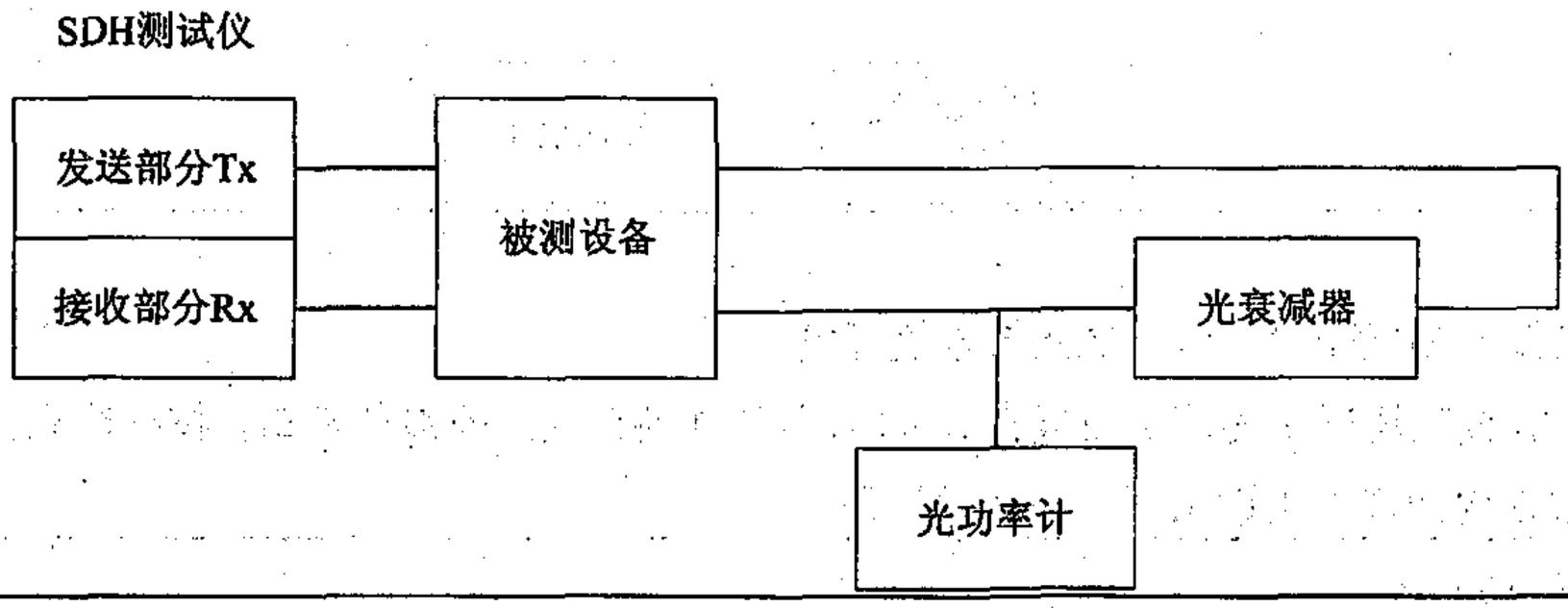
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：4

分项目编号：IF_STM-64_4

测试项目：接收灵敏度

测试配置：



测试步骤：

（1） 如图连接好测试配置；

（2） 使误码仪向发送机送入 PRBS 测试信号；

（3） 调整光衰减器，用误码仪测量使误码率保持在 10^{-6} 量级；

（4） 从光功率计上读出并记录光功率值；

（5） 重复上述步骤，分别测出误码率处于 10^{-7}、10^{-6} 和 10^{-9} 量级时被检测设备接收点的功率值；

（6） 按照外推法，在对数坐标纸（纵坐标应取两次对数，横坐标为线性）上画出误码率

（7） 与接收光功率(P-BER)的对应曲线，BER 为规定误码率所对应的光功率即为接收机的灵敏度

预期结果：≤－14dBm

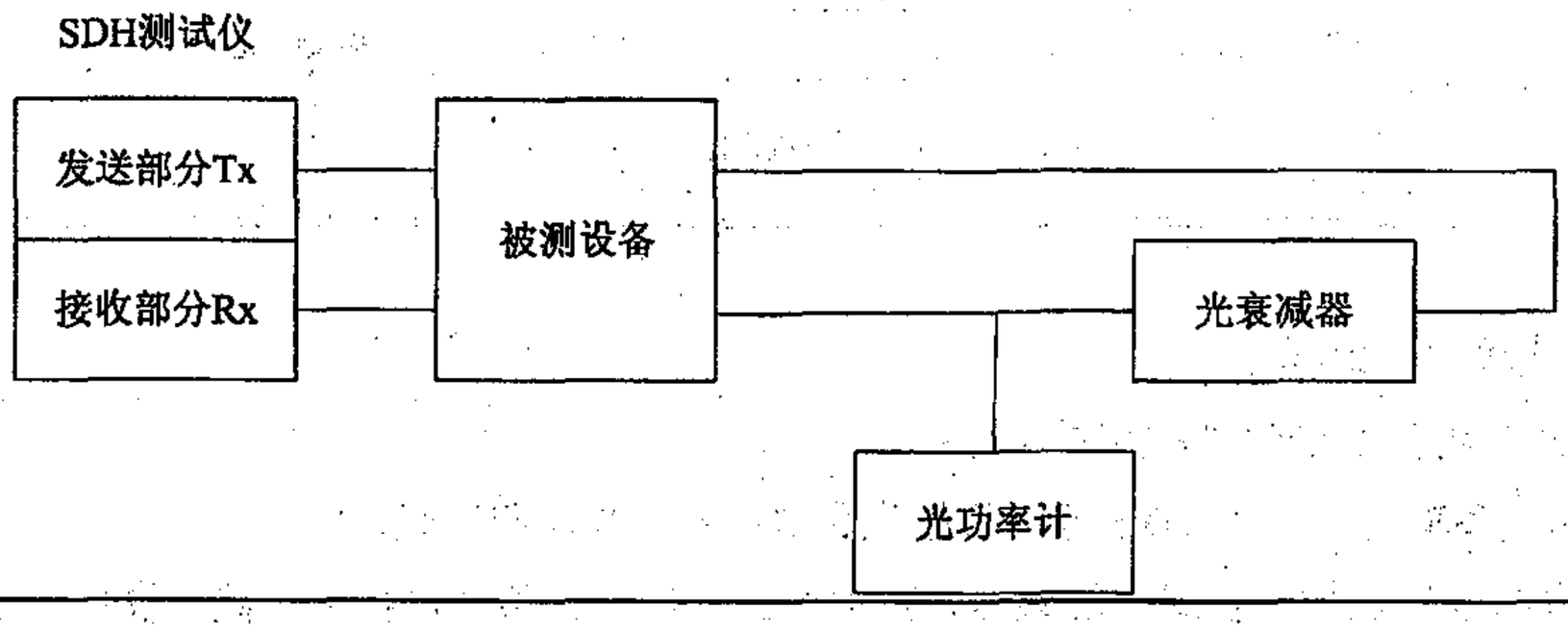
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：5

分项目编号：IF_STM-64_5

测试项目：接收机过载功率

测试配置：



测试步骤：

（1） 如图连接好测试配置；

（2） 使误码仪向发送机送入 PRBS 测试信号；

（3） 调节光衰减器，逐渐减小衰减值，使误码仪测量的误码率尽量接近但不大于规定的误码率；

（4） 从光功率计上读出并记录光功率值

预期结果：≥－1dBm

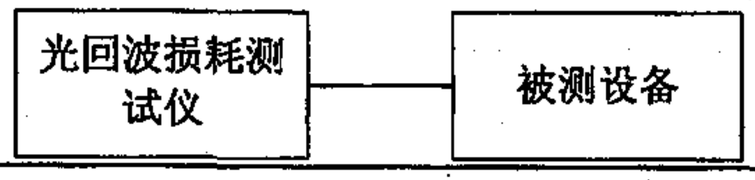
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：6

分项目编号：IF_STM-64_6

测试项目：接收机反射系数

测试配置：



测试步骤：

（1） 如图连接好测试配置，将集成式接收机开机；

（2） 将光回波损耗测试仪的波长设置在 SDH 设备被测端口的工作波长窗口，校准好光回波损耗测试仪，从光回波损耗测试仪上读出反射系数并记录

预期结果：≤−27dB

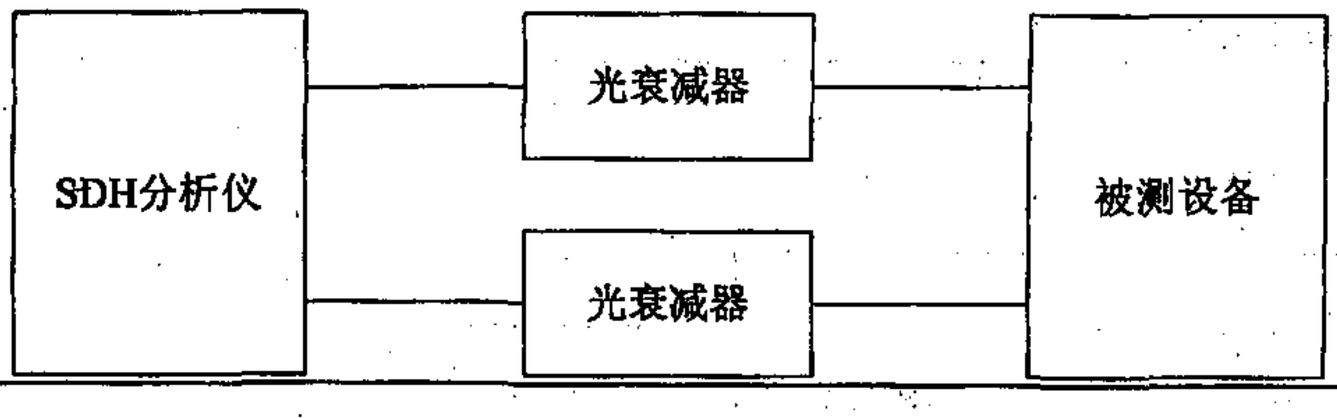
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：7

分项目编号：IF_STM-64_7

测试项目：输入口允许频偏

测试配置：



测试步骤：

（1） 如图连接好测试配置；

（2） 由 SDH 分析仪发送适当的测试信号；

（3） 在被测设备输出口，用 SDH 分析仪接收测试信号，并检测误码；

（4） SDH 分析仪发送加入正或负的频偏，范围在$\pm 20\times 10^{-6}$，整个过程中，被测设备不应出现误码

预期结果：$\pm 20\times 10^{-6}$传输无误码

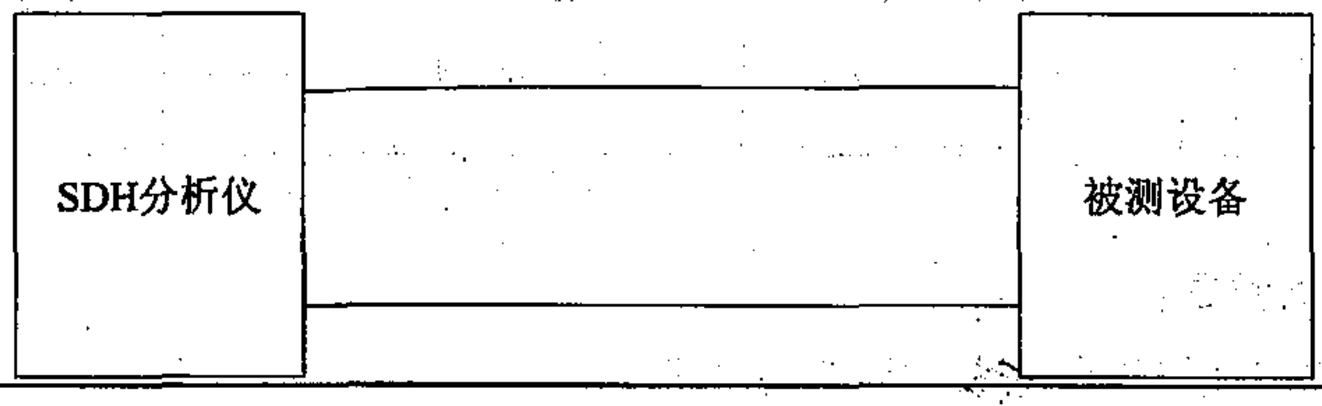
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：8

分项目编号：IF_STM-64_8

测试项目：输入口抖动容限

测试配置：



测试步骤：

（1） 如图连接好测试配置；

（2） 在 SDH 分析仪上选择合适的 PRBS 作为输入信号，使得这个测试配置正常工作；

（3） 在 SDH 分析仪上选择抖动容限的测试选项，选择合适的测试频率点数目（建议为 25 个），仪表开始自动测试；

（4） 将测试所得的抖动容限测试结果与被测端口速率的抖动容限模板进行比较，得出测试结果

预期结果：符合行标YD/T 1167-2001《STM-64分插复用（ADM）设备技术要求》表5

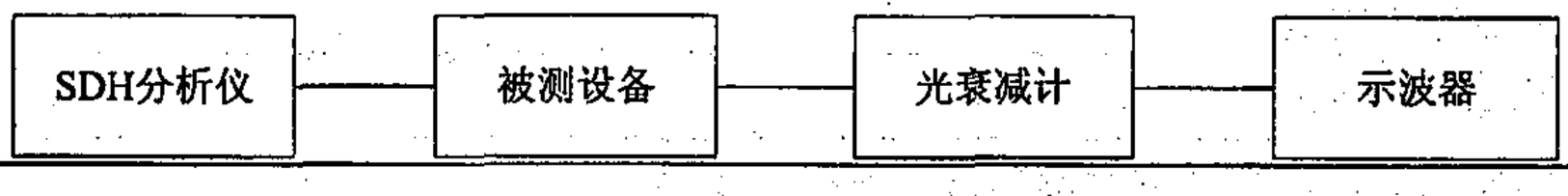
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：9

分项目编号：IF_STM-64_9

测试项目：最小消光比

测试配置：



测试步骤：

（1） 如图连接好测试配置；

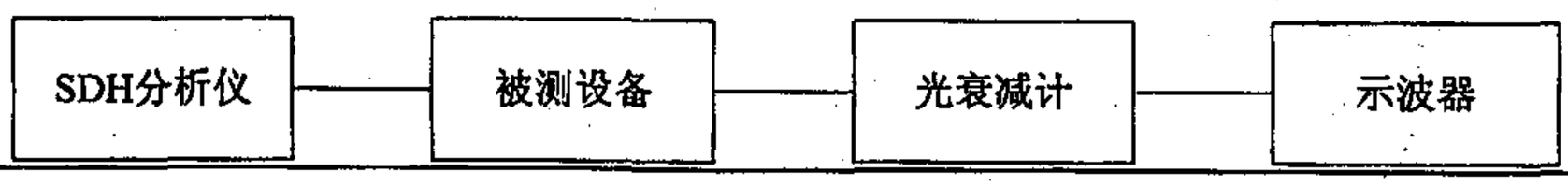
（2） 调整光衰减器，使光示波器有合适的输入光功率并获得稳定的波形；

（3） 读出传号和空号的功率 A 和 B；

（4） 计算出消光比

预期结果：≥8.2dB

判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：10
分项目编号：IF_STM-64_10
测试项目：发送信号眼图
测试配置： 
测试步骤： （1） 如图连接好测试配置； （2） 由 SDH 分析仪向被测设备送入适当的测试信号； （3） 调整示波器并调用相应的模框，获得稳定的波形，并由人工校整或由仪器自动校准，使波形与模框之间位置最佳； （4） 按模框参数记录相应的数值
预期结果：符合行标YD/T 1167-2001《STM-64分插复用（ADM）设备技术要求》图6
判定原则：测试结果必须与预期结果相符，否则不符合要求

6 接入方式测试

6.1 概述

本章规定了深度包检测设备接入网络方式的测试方法和非对称路由测试方法，以验证被测系统的接入方式和非对称路由功能是否便于在实际网络中部署。

被测设备至少要支持串联接入方式和并联接入方式中的一种。

6.2 测试拓扑

本章规定的测试方法使用第 4 章中规定的测试拓扑 1 和测试拓扑 2。

6.3 串联接入方式测试

测试编号：11
分项目编号：串联接入方式
测试项目：设备接入网络的方式
测试目的：验证深度包检测设备所支持的接入网络的方式
测试步骤： （1） 测试配置如测试拓扑； （2） 被测系统串联接入到网络中，进行业务识别和流量控制； （3） 测试仪表发送基础测试流量； （4） 被测系统对测试流量进行识别统计，及流量控制； （5） 查看被测系统的统计结果
预期结果：业务识别和流量控制功能正常
判定原则：测试结果必须与预期结果相符，否则不符合要求

6.4 并联接入方式测试

测试编号：12
分项目编号：并联接入方式
测试项目：设备接入网络的方式
测试目的：验证深度包检测设备所支持的接入网络的方式
测试步骤： （1） 测试配置如测试拓扑； （2） 被测系统并联接入到网络中，进行业务识别和流量控制； （3） 测试仪表发送基础测试流量； （4） 被测系统对测试流量进行识别统计，及流量控制； （5） 查看被测系统的统计结果
预期结果：业务识别和流量控制功能正常
判定原则：测试结果必须与预期结果相符，否则不符合要求

6.5 非对称路由组网方式测试

测试编号：13
分项目编号：非对称路由接入
测试项目：设备接入网络的方式
测试目的：验证深度包检测设备是否支持非对称路由功能
测试步骤： （1） 配置路由器设备，使得同一连接的上、下行流量经由不同路径； （2） 测试仪表发送基础测试流量，上行（客户端—服务器）、下行（服务器—客户端）； （3） 被测系统对上、下行链路都进行流量识别与流量控制； （4） 被测系统关联上、下行相关连接，进行业务识别和流量控制。 （5） 查看被测系统的统计结果
预期结果： （1） 被测系统能够关联不同路径上的连接为同一连接； （2） 能分别对上行、下行流量进行流量识别与控制； （3） 能对总连接进行流量识别与控制
判定原则：测试结果必须与预期结果相符，否则不符合要求

7 QoS 测试

7.1 概述

本章规定了深度包检测设备的 QoS 功能测试方法，以验证被测设备是否具备了实现差异化服务、精细化运营和区分特定网络业务所必须的 QoS 能力。

测试项目包括：业务数据流识别标记功能（源 IP 地址、DSCP 重标记、MPLS EXP）、业务数据流控制功能（连接干扰/性能劣化、限速和优先级保证等）、业务数据流优先级调度功能（基于业务的优先级调

度功能、基于用户的优先级调度功能、基于用户和业务的优先级调度功能）和 QoS 性能测试方法。

其中，数据流控制功能中的连接干扰/性能劣化控制方式适用于并联接入方式，流量限速控制方式适用于串联接入方式；数据流识别标记功能中的标记功能、数据流优先级调度功能和 QoS 性能对并联接入方式为可选。

7.2 测试拓扑

本章规定的测试方法使用第 4 章中规定的测试拓扑 1 和测试拓扑 2。

7.3 数据流识别标记功能测试

测试编号：14
分项目编号：业务数据流识别功能
测试项目：业务数据流识别标记功能测试
测试目的：验证深度包检测设备能够根据规定的源 IP 地址、DSCP 码点、MPLS EXP 对业务数据流量进行识别和区分
测试步骤： （1） 测试配置如测试拓扑； （2） 客户端/测试仪表发送基础测试流量（源 IP = 1.1.1.x）； （3） 客户端/测试仪表发送携带 DSCP 码点 = 100001 的基础测试流量； （4） 客户端/测试仪表发送携带 MPLS EXP = 011 的基础测试流量； （5） 被测系统对数据流量进行识别，查看被测系统的统计结果； （6） 在流量终端点，通过协议分析仪捕获流量
预期结果： （1） 被测系统能够识别数据流量，并能够根据源 IP 地址、DSCP 码点和 MPLS EXP 对数据流量进行正确识别； （2） 协议分析仪捕获的流量正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：15
分项目编号：数据流标记功能
测试项目：数据流识别标记功能测试
测试目的：验证深度包检测设备能够根据规定的源 IP 地址、DSCP 码点对数据流量进行标记和重标记，进行数据流量区分
测试步骤： （1） 测试配置如测试拓扑； （2） 客户端/测试仪表发送基础测试流量（sIP = 1.1.1.x）； （3） 客户端/测试仪表发送携带 DSCP 码点 = 100001 的基础测试流量； （4） 被测系统对数据流量进行识别，查看被测系统的统计结果； （5） 被测系统根据数据流量的 DSCP 标记对数据流量进行 DSCP 标记或者重标记； （6） 在流量终端点，通过协议分析仪捕获流量
预期结果： （1） 被测系统能够识别数据流量，并能够根据源 IP 地址和 DSCP 对数据流量进行正确标记或者重标记； （2） 协议分析仪捕获的流量正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

7.4 数据流控制功能测试

测试编号：16
分项目编号：连接干扰/性能劣化
测试项目：数据流控制功能测试
测试目的：验证深度包检测设备是否能够识别特定数据流量，并通过连接干扰/性能劣化的方式对相关的数据流量进行控制
测试步骤： （1） 测试配置如测试拓扑； （2） 客户端/测试仪表发送满测试接口带宽发送单协议构造流量； （3） 被测系统对 P2P 流量进行识别，并进行连接干扰/性能劣化； （4） 查看被测系统的统计结果； （5） 在流量终端点，通过协议分析仪捕获流量
预期结果： （1） 能正确识别 P2P 流量； （2） P2P 流量的连接干扰/性能劣化生效，其他流量不受影响
判定原则：并联接入设备测试结果必须与预期结果相符，否则不符合要求

测试编号：17
分项目编号：流量限速
测试项目：数据流控制功能测试
测试目的：验证深度包检测设备是否能够识别特定数据流量，并对相关数据流量进行流量限速，实施数据流量控制
测试步骤： （1） 客户端/测试仪表发送满测试接口带宽发送单协议构造流量； （2） 被测系统对 P2P 流量进行识别，并对 P2P 流量进行流量控制； （3） 可以设置流量阻断（Block），或者进行流量限速（CAR）； （4） 查看被测系统的统计结果； （5） 在流量终端点，通过协议分析仪捕获流量
预期结果： （1） 能正确识别 P2P 流量； （2） P2P 流量的流量控制生效，其他流量不受影响
判定原则：串联接入设备测试结果必须与预期结果相符，否则不符合要求

7.5 数据流优先级调度功能测试（可选）

深度包检测设备可选支持业务数据流的优先级调度功能。

测试编号：18
分项目编号：业务优先级保证
测试项目：数据流优先级调度
测试目的：验证深度包检测设备是否能够实现基于业务的优先级调度，当出现拥塞时，能够保障某种特定业务的优先级，实现数据流量的队列调度
测试步骤： （1） 客户端/测试仪表发送超出接口带宽的单协议构造流量，造成网络拥塞； （2） 被测系统对测试流量进行识别，并为不同的业务流量设定不同的 QoS 优先级； （3） 设定 HTTP 的优先级为最高，优先保证转发；FTP 优先级次之，P2P 流量优先级最低； （4） 查看被测系统的统计结果； （5） 在流量终端点，通过协议分析仪捕获流量
预期结果： （1）. 能正确识别流量； （2） 优先级设置生效，基于业务的优先级调度生效
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：19
分项目编号：用户优先级保证
测试项目：数据流优先级调度功能
测试目的：验证深度包检测设备是否能够实现基于用户的优先级调度，当出现拥塞时，能够保障某些特定用户的优先级，实现数据流量的队列调度
测试步骤： （1） 测试配置如测试拓扑； （2） 客户端/测试仪表发送超出接口带宽的单协议构造流量，造成网络拥塞； （3） 被测系统对测试流量进行识别，并为不同的用户流量设定不同的 QoS 优先级； （4） 设定用户 A/用户组 A 的优先级为最高，优先保证转发；用户 B/用户组 B 的优先级次之，其他用户/用户组的优先级最低； （5） 查看被测系统的统计结果； （6） 在流量终端点，通过协议分析仪捕获流量
预期结果： （1） 能正确识别流量； （2） 优先级设置生效，基于用户的优先级调度生效
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：20
分项目编号：用户+业务优先级保证
测试项目：数据流优先级调度功能
测试目的：验证深度包检测设备是否能够实现基于用户+业务的优先级调度，当出现拥塞时，能够保障某些特定用户的某些特定业务的优先级，实现数据流量的队列调度
测试步骤： （1） 客户端/测试仪表发送超出接口带宽的单协议构造流量，造成网络拥塞； （2） 被测系统对测试流量进行识别，并为不同的用户流量设定不同的 QoS 优先级； （3） 设定用户 A/用户组 A 的 HTTP 优先级为最高，优先保证转发；用户 B/用户组 B 的 FTP 优先级次之，其他用户/用户组的优先级最低； （4） 查看被测系统的统计结果； （5） 在流量终端点，通过协议分析仪捕获流量
预期结果： （1） 能正确识别流量； （2） 优先级设置生效，基于用户+业务的优先级调度生效
判定原则：测试结果必须与预期结果相符，否则不符合要求

7.6 QoS 性能测试

测试编号：21
分项目编号：流量控制最小粒度测试
测试项目：QoS 性能测试
测试目的：验证深度包检测设备能够进行流量控制的最小粒度
测试步骤： （1） 客户端/测试仪表发送满测试接口带宽发送单协议构造流量； （2） 被测系统对 P2P 流量进行识别，并设置承诺流量阈值进行流量控制，控制粒度为最小粒度； （3） 查看被测系统的统计结果； （4） 在流量终端点，通过协议分析仪捕获流量
预期结果：无
测试说明：参考项

测试编号：22
分项目编号：QoS 队列数量
测试项目：QoS 性能
测试目的：验证深度包检测设备能够支持的 QoS 队列数量
测试步骤： （1） 客户端/测试仪表发送满测试接口带宽发送单协议构造流量； （2） 被测系统分别对 HTTP、FTP、P2P 等流量进行识别，并将不同的数据流量放入不同的队列中； （3） 被测系统为不同的 QoS 队列实施不同的控制策略； （4） 查看被测系统的统计结果； （5） 在流量终端点，通过协议分析仪捕获流量
预期结果：无
测试说明：参考项

8 业务识别功能测试

8.1 概述

本章规定深度包检测设备的业务识别功能的测试方法，包括：链路流量识别功能测试、传统数据业务识别功能测试、P2P 流量识别功能测试、VoIP 流量识别功能测试、IM 识别功能测试、网络游戏流量识别功能测试、隧道流量识别功能测试和异常流量识别功能测试。

8.2 测试拓扑

本章规定的测试方法使用第 4 章中规定的测试拓扑 1 和测试拓扑 2。

8.3 链路流量识别功能测试

链路流量包括链路总流量、链路上行流量和链路下行流量。

测试编号：23
分项目编号：链路总流量识别
测试项目：链路流量识别功能
测试目的：验证深度包检测设备是否能够准确的识别出链路总流量
测试步骤： （1） 客户端/测试仪表满接口测试流量； （2） 被测系统对链路总流量进行识别、统计； （3） 查看被测系统的统计结果
预期结果：被测设备能够准确识别出链路总流量
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：24
分项目编号：链路上行流量识别
测试项目：链路流量识别功能
测试目的：验证深度包检测设备是否能够准确的识别出链路上行流量
测试步骤： （1） 客户端/测试仪表满接口测试流量； （2） 被测系统对链路上行流量进行识别、统计； （3） 查看被测系统的统计结果
预期结果：被测设备能够准确识别出链路上行流量
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：25
分项目编号：链路下行流量识别
测试项目：链路流量识别功能
测试目的：验证深度包检测设备是否能够准确的识别出链路下行流量
测试步骤： （1） 客户端/测试仪表满接口测试流量； （2） 被测系统对链路下行流量进行识别、统计； （3） 查看被测系统的统计结果
预期结果：被测设备能够准确识别出链路下行流量
判定原则：测试结果必须与预期结果相符，否则不符合要求

8.4 传统数据业务流量的识别功能测试

传统数据业务流量包括HTTP业务流量、FTP业务流量和Mail业务流量。

测试编号：26
分项目编号：HTTP 业务识别
测试项目：传统数据业务流量识别
测试目的：验证深度包检测设备是否能够准确的识别出 HTTP 业务流量
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，测试流量中包含 HTTP 流量； （2） 被测系统分别对 HTTP 业务流量进行识别、统计； （3） 查看被测系统的统计结果
预期结果：步骤（2）中的 HTTP 业务流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：27
分项目编号：FTP 业务识别
测试项目：传统数据业务流量识别
测试目的：验证深度包检测设备是否能够准确的识别出 FTP 业务流量
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，测试流量中包含 FTP 流量； （2） 被测系统分别对 FTP 业务流量进行识别、统计； （3） 查看被测系统的统计结果
预期结果：步骤（2）中的 FTP 业务流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：28
分项目编号：Mail 业务识别
测试项目：传统数据业务流量识别
测试目的：验证深度包检测设备是否能够准确的识别出 Mail 业务流量
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，测试流量中包含 POP3 流量； （2） 被测系统分别对 POP3 业务流量进行识别、统计； （3） 客户端/测试仪表满接口带宽发送测试流量，测试流量中包含 SMTP 流量； （4） 被测系统分别对 SMTP 业务流量进行识别、统计； （5） 查看被测系统的统计结果
预期结果： （1） 步骤（2）中的 POP3 业务流量识别、统计正确； （2） 步骤（4）中的 SMTP 业务流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

8.5 P2P 流量识别功能测试

P2P业务流量识别包括P2P文件下载类流量识别、P2P流媒体类流量识别和P2P加密类流量识别。

测试编号：29
分项目编号：P2P 文件下载类流量识别
测试项目：P2P 流量识别功能
测试目的：验证深度包检测设备是否能够准确识别出 P2P 文件下载类流量
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，测试流量中包含 P2P 文件下载类流量（Bittorrent、eMule/eDonkey、POCO、Kazza 等）； （2） 被测系统对 P2P 文件下载类流量进行识别、统计； （3） 查看被测系统的统计结果
预期结果：步骤（2）中，P2P 文件下载类流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：30
分项目编号：P2P 流媒体流量识别
测试项目：P2P 流量识别功能
测试目的：验证深度包检测设备是否能够准确识别出 P2P 流媒体类流量
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，测试流量中包含 P2P 流媒体类流量（PPLive、PPStream、QQLive、USee 等）； （2） 被测系统对 P2P 流媒体类流量进行识别、统计； （3） 查看被测系统的统计结果
预期结果：步骤（2）中，P2P 流媒体类流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：31
分项目编号：P2P 加密类流量识别
测试项目：P2P 流量识别功能
测试目的：验证深度包检测设备是否能够准确识别出 P2P 加密类流量
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，测试流量中包含 P2P 加密类流量（Skype 等）； （2） 被测系统对 P2P 加密类流量进行识别、统计； （3） 查看被测系统的统计结果
预期结果：步骤（2）中，P2P 加密类流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

8.6 VoIP 流量识别功能测试

VoIP流量为标准信令的VoIP流量和Skype流量，包括：SIP流量、H.323流量、MGCP流量和Skype Voice流量。

测试编号：32
分项目编号：SIP 流量识别
测试项目：VoIP 流量识别功能
测试目的：验证深度包检测设备是否能够准确识别出 SIP 流量
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，测试流量中包含 SIP 流量； （2） 被测系统对 SIP 流量进行识别、统计； （3） 查看被测系统的统计结果
预期结果：步骤（2）中，SIP 流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：33
分项目编号：H.323 流量识别
测试项目：VoIP 流量识别功能
测试目的：验证深度包检测设备是否能够准确识别出 H.323 流量
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，测试流量中包含 H.323 流量； （2） 被测系统对 H.323 流量进行识别、统计； （3） 查看被测系统的统计结果
预期结果：步骤（2）中，H.323 流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：34
分项目编号：MGCP 流量识别
测试项目：VoIP 流量识别功能
测试目的：验证深度包检测设备是否能够准确识别出 MGCP 流量
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，测试流量中包含 MGCP 流量； （2） 被测系统对 MGCP 流量进行识别、统计； （3） 查看被测系统的统计结果
预期结果：步骤（2）中，MGCP 流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：35
分项目编号：Skype Voice 流量识别
测试项目：VoIP 流量识别功能
测试目的：验证深度包检测设备是否能够准确识别出 Skype Voice 流量
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，测试流量中包含 Skype Voice 流量； （2） 被测系统对 Skype Voice 流量进行识别、统计； （3） 查看被测系统的统计结果
预期结果：步骤（2）中，Skype Voice 流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

8.7 IM 流量识别功能测试

IM流量为互联网中常见的即时消息流量，包括：腾讯QQ流量、Windows Live Messenger流量、Yahoo Messenger流量、Skype流量和Google Talk流量。

测试编号：36
分项目编号：腾讯 QQ 流量识别
测试项目：腾讯 QQ 流量识别功能
测试目的：验证深度包检测设备是否能够准确识别出腾讯 QQ 流量
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，测试流量中包含腾讯 QQ 流量； （2） 被测系统对腾讯 QQ 流量进行识别、统计； （3） 查看被测系统的统计结果
预期结果：步骤（2）中，腾讯 QQ 流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：37
分项目编号：Windows Live Messenger 流量识别
测试项目：Windows Live Messenger 流量识别功能
测试目的：验证深度包检测设备是否能够准确识别出 Windows Live Messenger 流量
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，测试流量中包含 Windows Live Messenger 流量； （2） 被测系统对 Windows Live Messenger 流量进行识别、统计； （3） 查看被测系统的统计结果
预期结果：步骤（2）中，Windows Live Messenger 流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：38
分项目编号：Yahoo Messenger 流量识别
测试项目：Yahoo Messenger 流量识别功能
测试目的：验证深度包检测设备是否能够准确识别出 Yahoo Messenger 流量
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，测试流量中包含 Yahoo Messenger 流量； （2） 被测系统对 Yahoo Messenger 流量进行识别、统计； （3） 查看被测系统的统计结果
预期结果：步骤（2）中，Yahoo Messenger 流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：39
分项目编号：Skype Chat 流量识别
测试项目：Skype Chat 流量识别功能
测试目的：验证深度包检测设备是否能够准确识别出 Skype Chat 流量
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，测试流量中包含 Skype Chat 流量； （2） 被测系统对 Skype Chat 流量进行识别、统计； （3） 查看被测系统的统计结果
预期结果：步骤（2）中，Skype Chat 流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：40
分项目编号：Google Talk 流量识别
测试项目：Google Talk 流量识别功能
测试目的：验证深度包检测设备是否能够准确识别出腾讯 Google Talk 流量
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，测试流量中包含 Google Talk 流量； （2） 被测系统对 Google Talk 流量进行识别、统计； （3） 查看被测系统的统计结果
预期结果：步骤（2）中，Google Talk 流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

8.8 网络游戏流量识别功能测试

测试编号：41
分项目编号：网络游戏流量识别
测试项目：网络游戏流量识别功能
测试目的：验证深度包检测设备是否能够准确识别出网络游戏流量
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，测试流量中包含网络游戏流量（QQGame、联众游戏、魔兽争霸等）； （2） 被测系统对网络游戏流量进行识别、统计； （3） 查看被测系统的统计结果
预期结果：步骤（2）中，网络游戏流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

8.9 隧道流量识别功能测试

隧道流量包括：GRE流量、L2TP流量和MPLS VPN流量。被测系统可选支持隧道流量识别功能。

测试编号：42
分项目编号：GRE 隧道流量识别
测试项目：隧道流量识别功能
测试目的：验证深度包检测设备是否能够准确识别出 GRE 隧道内的流量
测试步骤： （1） 在客户端和测试仪表之间建立 GRE 隧道； （2） 客户端/测试仪表满接口带宽发送测试流量，测试流量穿过 GRE 隧道； （3） 被测系统对 GRE 隧道内的流量进行识别、统计； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，GRE 隧道内的流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：43
分项目编号：L2TP 隧道流量识别
测试项目：隧道流量识别功能
测试目的：验证深度包检测设备是否能够准确识别出 L2TP 隧道内的流量
测试步骤： （1） 在客户端和测试仪表之间建立 L2TP 隧道； （2） 客户端/测试仪表满接口带宽发送测试流量，测试流量穿过 L2TP 隧道； （3） 被测系统对 L2TP 隧道内的流量进行识别、统计； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，L2TP 隧道内的流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：44
分项目编号：MPLS VPN 隧道流量识别
测试项目：隧道流量识别功能
测试目的：验证深度包检测设备是否能够准确识别出 MPLS VPN 隧道内的流量
测试步骤： （1） 在客户端和测试仪表之间建立 MPLS VPN； （2） 客户端/测试仪表满接口带宽发送测试流量，测试流量穿过 MPLS VPN； （3） 被测系统对 MPLS VPN 内的流量进行识别、统计； （4） 查看被测系统的统计结果； （5） 统计被测试系统能够识别的标签层数
预期结果：步骤（3）中，MPLS VPN 内的流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

8.10 异常流量识别功能测试

异常流量主要指网络中的DDoS攻击流量，包括：SynFlood攻击流量、UDPFlood攻击流量和PingofDeath攻击流量。深度包检测设备可选支持异常流量的识别。

测试编号：45（可选）
分项目编号：SynFlood 攻击流量识别
测试项目：异常流量识别功能
测试目的：验证深度包检测设备是否能够准确识别出 SynFlood 攻击流量
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，同时发送 SynFlood 攻击流量； （2） 被测系统对测试流量进行识别统计； （3） 被测系统对 SynFlood 攻击流量进行识别、统计； （4） 查看被测系统的统计结果
预期结果： （1） 步骤（2）中，测试流量识别、统计正确； （2） 步骤（3）中，SynFlood 攻击流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：46（可选）
分项目编号：UDPFlood 攻击流量识别
测试项目：异常流量识别功能
测试目的：验证深度包检测设备是否能够准确识别出 UDPFlood 攻击流量
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，同时发送 UDPFlood 攻击流量； （2） 被测系统对测试流量进行识别统计； （3） 被测系统对 UDPFlood 攻击流量进行识别、统计； （4） 查看被测系统的统计结果
预期结果： （1） 步骤（2）中，测试流量识别、统计正确； （2） 步骤（3）中，UDPFlood 攻击流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：47（可选）
分项目编号：PingofDeath 攻击流量识别
测试项目：异常流量识别功能
测试目的：验证深度包检测设备是否能够准确识别出 PingofDeath 攻击流量
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，同时发送 PingofDeath 攻击流量； （2） 被测系统对测试流量进行识别统计； （3） 被测系统对 PingofDeath 攻击流量进行识别、统计； （4） 查看被测系统的统计结果
预期结果： （1） 步骤（2）中，测试流量识别、统计正确； （2） 步骤（3）中，PingofDeath 攻击流量识别、统计正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

9 业务控制功能测试

9.1 概述

本章规定了深度包检测设备的业务控制功能的测试方法，包括：链路流量控制功能测试、传统数据业务控制功能测试、P2P流量控制测试、VoIP流量控制功能测试、IM流量控制功能测试、网络游戏流量控制功能测试、隧道流量控制功能测试和异常流量控制功能测试。

9.2 测试拓扑

本章规定的测试方法使用第 4 章中规定的测试拓扑 1 和测试拓扑 2。

9.3 链路流量控制功能测试

链路流量包括链路总流量、链路上行流量和链路下行流量。

测试编号：48
分项目编号：链路总流量控制
测试项目：链路流量控制功能
测试目的：验证深度包检测设备是否能够准确的对链路总流量进行控制
测试步骤： （1） 客户端/测试仪表满接口测试流量； （2） 被测设备对链路总流量进行识别、统计； （3） 被测设备对链路总流量进行绝对带宽限制，限制为不大于链路带宽的 50%； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对链路总流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：49
分项目编号：链路上行流量控制
测试项目：链路流量控制功能
测试目的：验证深度包检测设备是否能够准确的对链路上行流量进行控制
测试步骤： （1） 客户端/测试仪表满接口测试流量； （2） 被测设备对链路上行流量进行识别、统计； （3） 被测设备对链路上行流量进行绝对带宽限制，限制为不大于链路带宽的 30%； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对链路上行流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：50
分项目编号：链路下行流量控制
测试项目：链路流量控制功能
测试目的：验证深度包检测设备是否能够准确的对链路下行流量进行控制
测试步骤： （1） 客户端/测试仪表满接口测试流量； （2） 被测设备对链路下行流量进行识别、统计； （3） 被测设备对链路下行流量进行绝对带宽限制，限制为不大于链路带宽的 20%； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对链路总流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

9.4 传统数据业务流量控制功能测试

传统数据业务流量包括 HTTP 业务流量、FTP 业务流量和 Mail 业务流量。

测试编号：51
分项目编号：HTTP 业务流量控制
测试项目：链路流量控制功能
测试目的：验证深度包检测设备是否能够准确的对 HTTP 业务流量进行控制
测试步骤： （1） 客户端/测试仪表满接口测试流量，测试流量中包含 HTTP 业务流量； （2） 被测设备对 HTTP 业务流量进行识别、统计； （3） 被测设备对 HTTP 业务流量进行绝对带宽限制，限制为不大于链路带宽的 30%； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对 HTTP 业务流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：52
分项目编号：FTP 业务流量控制
测试项目：链路流量控制功能
测试目的：验证深度包检测设备是否能够准确的对 FTP 业务流量进行控制
测试步骤： （1） 客户端/测试仪表满接口测试流量，测试流量中包含 FTP 业务流量； （2） 被测设备对 FTP 业务流量进行识别、统计； （3） 被测设备对 FTP 业务流量进行绝对带宽限制，限制为不大于链路带宽的 10%； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对 FTP 业务流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：53
分项目编号：Mail 业务流量控制
测试项目：链路流量控制功能
测试目的：验证深度包检测设备是否能够准确的对 Mail 业务流量进行控制
测试步骤： （1） 客户端/测试仪表满接口测试流量，测试流量中包含 POP3、SMTP 业务流量； （2） 被测设备对 POP3、SMTP 业务流量进行识别、统计； （3） 被测设备对 POP3、SMTP 业务流量进行绝对带宽限制，限制为不大于链路带宽的 10%； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对 POP3、SMTP 业务流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

9.5 P2P 流量控制功能测试

P2P流量包括：TCP类P2P流量、UDP类P2P流量和加密类P2P流量。

测试编号：54
分项目编号：TCP 类 P2P 流量控制
测试项目：P2P 流量控制功能
测试目的：验证深度包检测设备是否能够准确的对 TCP 类 P2P 流量进行控制
测试步骤： （1） 客户端/测试仪表满接口测试流量，测试流量中包含 TCP 类 P2P 流量； （2） 被测设备对 TCP 类 P2P 流量进行识别、统计； （3） 被测设备对 TCP 类 P2P 流量进行绝对带宽限制，限制为不大于链路带宽的 30%； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对 TCP 类 P2P 流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：55
分项目编号：UDP 类 P2P 流量控制
测试项目：P2P 流量控制功能
测试目的：验证深度包检测设备是否能够准确的对 UDP 类 P2P 流量进行控制
测试步骤： （1） 客户端/测试仪表满接口测试流量，测试流量中包含 UDP 类 P2P 流量； （2） 被测设备对 UDP 类 P2P 流量进行识别、统计； （3） 被测设备对 UDP 类 P2P 流量进行绝对带宽限制，限制为不大于链路带宽的 30%； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对 UDP 类 P2P 流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：56
分项目编号：加密类 P2P 流量控制
测试项目：P2P 流量控制功能
测试目的：验证深度包检测设备是否能够准确的对加密类 P2P 流量进行控制
测试步骤： （1） 客户端/测试仪表满接口测试流量，测试流量中包含加密类 P2P 流量； （2） 被测设备对加密类 P2P 流量进行识别、统计； （3） 被测设备对加密类 P2P 流量进行绝对带宽限制，限制为不大于链路带宽的 30%； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对加密类 P2P 流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

9.6 VoIP 流量控制功能测试

VoIP 流量为标准信令的 VoIP 流量和 Skype 流量，包括：SIP 流量、H.323 流量、MGCP 流量和 Skype Voice 流量。

测试编号：57
分项目编号：SIP 流量控制
测试项目：VoIP 流量控制功能
测试目的：验证深度包检测设备是否能够准确的对 SIP 流量进行控制
测试步骤： （1） 客户端/测试仪表满接口测试流量，测试流量中包含 SIP 流量； （2） 被测设备对 SIP 流量进行识别、统计； （3） 被测设备对 SIP 流量进行绝对带宽限制，限制为不大于链路带宽的 10%；； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对 SIP 流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：58
分项目编号：H.323 流量控制
测试项目：VoIP 流量控制功能
测试目的：验证深度包检测设备是否能够准确的对 H.323 流量进行控制
测试步骤： （1） 客户端/测试仪表满接口测试流量，测试流量中包含 H.323 流量； （2） 被测设备对 H.323 流量进行识别、统计； （3） 被测设备对 H.323 流量进行绝对带宽限制，限制为不大于链路带宽的 10%； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对 H.323 流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：59
分项目编号：MGCP 流量控制
测试项目：VoIP 流量控制功能
测试目的：验证深度包检测设备是否能够准确的对 MGCP 流量进行控制
测试步骤： （1） 客户端/测试仪表满接口测试流量，测试流量中包含 MGCP 流量； （2） 被测设备对 MGCP 流量进行识别、统计； （3） 被测设备对 MGCP 流量进行绝对带宽限制，限制为不大于链路带宽的 10%； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对 MGCP 流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：60
分项目编号：Skype Voice 流量控制
测试项目：VoIP 流量控制功能
测试目的：验证深度包检测设备是否能够准确的对 Skype Voice 流量进行控制
测试步骤： （1） 客户端/测试仪表满接口测试流量，测试流量中包含 Skype Voice 流量； （2） 被测设备对 Skype Voice 流量进行识别、统计； （3） 被测设备对 Skype Voice 流量进行绝对带宽限制，限制为不大于链路带宽的 30%； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对 Skype Voice 流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

9.7 IM 流量控制功能测试

IM 流量为互联网中常见的即时消息流量。

测试编号：61
分项目编号：腾讯 QQ 流量控制
测试项目：腾讯 QQ 流量控制功能
测试目的：验证深度包检测设备是否能够准确的对腾讯 QQ 流量进行控制
测试步骤： （1） 客户端/测试仪表满接口测试流量，测试流量中包含腾讯 QQ 流量； （2） 被测设备对腾讯 QQ 流量进行识别、统计； （3） 被测设备对腾讯 QQ 流量进行绝对带宽限制，限制为不大于链路带宽的 5%；； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对腾讯 QQ 流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：62
分项目编号：Windows Live Messenger 流量控制
测试项目：Windows Live Messenger 流量控制功能
测试目的：验证深度包检测设备是否能够准确的对 Windows Live Messenger 流量进行控制
测试步骤： （1） 客户端/测试仪表满接口测试流量，测试流量中包含 Windows Live Messenger 流量； （2） 被测设备对 Windows Live Messenger 流量进行识别、统计； （3） 被测设备对 Windows Live Messenger 流量进行绝对带宽限制，限制为不大于链路带宽的 5%； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对 Windows Live Messenger 流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：63
分项目编号：Yahoo Messenger 流量控制
测试项目：Yahoo Messenger 流量控制功能
测试目的：验证深度包检测设备是否能够准确的对 Yahoo Messenger 流量进行控制
测试步骤： （1） 客户端/测试仪表满接口测试流量，测试流量中包含 Yahoo Messenger 流量； （2） 被测设备对 Yahoo Messenger 流量进行识别、统计； （3） 被测设备对 Yahoo Messenger 流量进行绝对带宽限制，限制为不大于链路带宽的 5%； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对 Yahoo Messenger 流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：64
分项目编号：Skype 流量控制
测试项目：Skype 流量控制功能
测试目的：验证深度包检测设备是否能够准确的对 Skype 流量进行控制
测试步骤： （1） 客户端/测试仪表满接口测试流量，测试流量中包含 Skype 流量； （2） 被测设备对 Skype 流量进行识别、统计； （3） 被测设备对 Skype 流量进行绝对带宽限制，限制为不大于链路带宽的 5%； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对 Skype 流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：65
分项目编号：Google Talk 流量控制
测试项目：Google Talk 流量控制功能
测试目的：验证深度包检测设备是否能够准确的对 Google Talk 流量进行控制
测试步骤： （1） 客户端/测试仪表满接口测试流量，测试流量中包含 Google Talk 流量； （2） 被测设备对 Google Talk 进行识别、统计； （3） 被测设备对 Google Talk 进行绝对带宽限制，限制为不大于链路带宽的 5%； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对 Google Talk 流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

9.8 网络游戏流量控制功能测试

测试编号：66
分项目编号：网络游戏流量控制
测试项目：网络游戏流量控制功能
测试目的：验证深度包检测设备是否能够准确的对网络游戏流量进行控制
测试步骤： （1） 客户端/测试仪表满接口测试流量，测试流量中包含网络游戏流量； （2） 被测设备对网络游戏流量进行识别、统计； （3） 被测设备对网络游戏流量进行绝对带宽限制，限制为不大于链路带宽的 10%； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对网络游戏流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

9.9 隧道流量控制功能测试

隧道流量包括：GRE流量、L2TP流量和MPLS VPN流量。被测系统可选支持隧道流量控制功能。

测试编号：67
分项目编号：GRE 隧道流量控制
测试项目：隧道流量控制功能
测试目的：验证深度包检测设备是否能够准确的对 GRE 隧道内的流量进行控制
测试步骤： （1） 在客户端和测试仪表之间建立 GRE 隧道； （2） 客户端/测试仪表满接口带宽发送测试流量，测试流量穿过 GRE 隧道； （3） 被测系统对 GRE 隧道内的流量进行识别、统计； （4） 被测设备对 GRE 隧道内的流量进行绝对带宽限制，限制为不大于链路带宽的 30%； （5） 查看被测系统的统计结果
预期结果：步骤（4）中，被测设备能够准确对 GRE 隧道内的流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：68
分项目编号：L2TP 隧道流量控制
测试项目：隧道流量控制功能
测试目的：验证深度包检测设备是否能够准确的对 L2TP 隧道内的流量进行控制
测试步骤： （1） 在客户端和测试仪表之间建立 L2TP 隧道； （2） 客户端/测试仪表满接口带宽发送测试流量，测试流量穿过 L2TP 隧道； （3） 被测系统对 L2TP 隧道内的流量进行识别、统计； （4） 被测设备对 L2TP 隧道内的流量进行绝对带宽限制，限制为不大于链路带宽的 30%； （5） 查看被测系统的统计结果
预期结果：步骤（4）中，被测设备能够准确对 L2TP 隧道内的流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：69
分项目编号：MPLS VPN 流量控制
测试项目：隧道流量控制功能
测试目的：验证深度包检测设备是否能够准确 MPLS VPN 内的流量进行控制
测试步骤： （1） 在客户端和测试仪表之间建立 MPLS VPN； （2） 客户端/测试仪表满接口带宽发送测试流量，测试流量穿过 MPLS VPN； （3） 被测系统对 MPLS VPN 内的流量进行识别、统计； （4） 被测设备对 MPLS VPN 内的流量进行绝对带宽限制，限制为不大于链路带宽的 30%； （5） 查看被测系统的统计结果
预期结果：步骤（4）中，被测设备能够准确对 MPLS VPN 内的流量进行绝对带宽限制
判定原则：测试结果必须与预期结果相符，否则不符合要求

9.10 异常流量控制功能测试

异常流量主要指网络中的DDoS攻击流量，包括：SynFlood攻击流量、UDPFlood攻击流量和PingofDeath攻击流量。深度包检测设备可选支持对异常流量的控制。

测试编号：70
分项目编号：SynFlood 攻击流量控制
测试项目：异常流量控制功能
测试目的：验证深度包检测设备是否能够准确的对 SynFlood 攻击流量进行控制
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，同时发送 SynFlood 攻击流量； （2） 被测系统对测试流量进行识别统计； （3） 被测系统对 SynFlood 攻击流量进行控制； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对 SynFlood 流量内的流量进行控制
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：71
分项目编号：UDPFlood 攻击流量控制
测试项目：异常流量控制功能
测试目的：验证深度包检测设备是否能够准确的对 UDPFlood 攻击流量进行控制
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，同时发送 UDPFlood 攻击流量； （2） 被测系统对测试流量进行识别统计； （3） 被测系统对 UDPFlood 攻击流量进行控制； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对 UDPFlood 流量内的流量进行控制
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：72
分项目编号：PingofDeath 攻击流量控制
测试项目：异常流量控制功能
测试目的：验证深度包检测设备是否能够准确的对 PingofDeath 攻击流量进行控制
测试步骤： （1） 客户端/测试仪表满接口带宽发送测试流量，同时发送 PingofDeath 攻击流量； （2） 被测系统对测试流量进行识别统计； （3） 被测系统对 PingofDeath 攻击流量进行控制； （4） 查看被测系统的统计结果
预期结果：步骤（3）中，被测设备能够准确对 PingofDeath 流量内的流量进行控制
判定原则：测试结果必须与预期结果相符，否则不符合要求

10 可靠性测试

10.1 概述

本章规定了深度包检测设备的可靠性测试方法，以验证被测系统是否具备电信级的可靠性。包括：主备电源冗余切换、主备控制卡冗余切换、主备交换卡冗余切换、业务板卡热插拔、Bypass 功能和软件升级对系统的影响等。

本项测试对于串联接入的设备，等同于设备可靠性；对于并联接入的设备，包含分光设备可靠性和流量分析设备可靠性。对于不支持插卡式设计的系统，主备控制卡冗余切换、主备交换卡冗余切换及业务板卡热插拔为可选。

10.2 测试拓扑

本章规定的测试方法采用第 4 章中规定的测试拓扑 1 和测试拓扑 2。

10.3 系统冗余测试

测试编号：73
分项目编号：主备电源冗余切换
测试项目：系统冗余测试
测试目的：验证深度包检测设备是否支持主备电源冗余切换
测试步骤： （1） 客户端/测试仪表发送测试流量； （2） 被测系统对数据流量进行识别、标记和流量控制； （3） 查看被测系统统计结果； （4） 被测系统关闭主用电源，切换到备用电源； （5） 查看被测系统统计结果
预期结果： （1） 被测系统支持主备电源冗余切换； （2） 在电源切换过程中，业务识别与控制功能不受影响
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：74
分项目编号：主备控制卡冗余切换
测试项目：系统冗余测试
测试目的：验证深度包检测设备是否支持主备控制卡冗余切换
测试步骤： （1） 客户端/测试仪表发送测试流量； （2） 被测系统对数据流量进行识别、标记和流量控制； （3） 查看被测系统统计结果； （4） 热插拔被测系统的主用控制卡，被测试系统切换到备用控制卡； （5） 查看被测系统统计结果
预期结果： （1） 被测系统支持主备控制卡冗余切换； （2） 在电源切换过程中，业务识别与控制功能不受影响
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：75
分项目编号：主备交换卡冗余切换
测试项目：系统冗余测试
测试目的：验证深度包检测设备是否支持主备交换卡冗余切换
测试步骤： （1） 客户端/测试仪表发送测试流量； （2） 被测系统对数据流量进行识别、标记和流量控制； （3） 查看被测系统统计结果； （4） 关闭被测系统的主用交换卡，被测试系统切换到备用交换卡； （5） 查看被测系统统计结果
预期结果： （1） 被测系统支持主备交换卡冗余切换； （2） 在电源切换过程中，业务识别与控制功能不受影响
判定原则：测试结果必须与预期结果相符，否则不符合要求

10.4 Bypass 功能测试

测试编号：76
分项目编号：Bypass 功能测试
测试项目：Bypass 功能测试
测试目的：验证深度包检测设备是否支持 Bypass 功能，在插拔光纤/Shundown 端口/手动切换/切断电源/系统软件故障等情况下，能迅速切换到 Bypass 链路，继续保证网络的连通性
测试步骤： （1） 客户端/测试仪表发送测试流量； （2） 被测系统对数据流量进行识别、标记和流量控制； （3） 查看被测系统的统计结果； （4） 分别通过插拔光纤/Shundown 端口/手动切换/切断电源//系统软件故障的方式，触发系统切换到 Bypass 链路； （5） 查看被测系统的统计结果； （6） 分别记录切换时间； （7） 恢复原状态，记录回切方式和时间
预期结果： （1） 被测系统能够迅速切换到 Bypass 链路； （2） 切换后，数据流量转发正常； （3） 支持手动或者自动的回切
判定原则：测试结果必须与预期结果相符，否则不符合要求

11 可扩展性测试

11.1 概述

本章定义了深度包检测设备的可扩展性测试方法，包括硬件扩展性测试和软件扩展性测试。对于采用一体化设计的深度包检测设备，硬件扩展性测试可选。

11.2 测试项目

测试编号：77
分项目编号：硬件模块化设计
测试项目：可扩展性测试
测试目的：验证深度包检测设备是否支持硬件的模块化设计
测试步骤： （1） 被测系统正常加电启动； （2） 被测系统支持模块化设计，支持多种接口的板卡； （3） 能够通过扩充板卡实现系统容量、处理能力的升级
预期结果：被测系统支持硬件模块化设计
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：78
分项目编号：级联设计
测试项目：可扩展性测试
测试目的：验证深度包检测设备是否支持硬件的级联设计
测试步骤： （1） 被测系统正常加电启动； （2） 被测系统支持三套系统级联，具备级联接口； （3） 能够通过设备级联实现系统容量、处理能力的升级
预期结果：被测系统支持级联设计
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：79
分项目编号：软件/特征库升级功能
测试项目：可扩展性测试
测试目的：验证深度包检测设备是否支持系统软件/特征库的升级
测试步骤： （1） 被测系统正常加电启动； （2） 系统管理员通过正确的用户名和密码登录系统； （3） 系统能够在线/离线对系统软件/特征库进行升级； （4） 重新启动系统
预期结果：系统能够进行系统软件/特征库的升级，并且重新启动系统后，配置生效
判定原则：测试结果必须与预期结果相符，否则不符合要求

12 统计报表功能测试

12.1 概述

本章定义了深度包检测设备的统计报表功能测试方法，以检验被测系统对网络各类业务和流量的分析、评估，以及策略制定和管理的能力。具体测试方法包括：实时流量统计功能（分协议流量统计、分业务流量统计等）、历史流量统计功能（按分钟、按小时、按天、按月、按年统计、流量趋势分析统计等）、以及统计报表输出功能的测试。

12.2 测试项目

测试编号：80
分项目编号：实时流量统计功能
测试项目：统计报表功能测试
测试目的：验证深度包检测设备是否支持实时分协议总流量/上行流量/下行流量统计功能
测试步骤： （1） 客户端/测试仪表发送多协议混合构造流量； （2） 被测系统进行实时的混合总流量/上行流量/下行流量统计； （3） 被测系统进行实时分协议的总流量/上行流量/下行流量统计； （4） 记录实时刷新时间
预期结果：统计结果正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：81
分项目编号：历史流量统计功能
测试项目：统计报表功能测试
测试目的：验证深度包检测设备是否支持按（分钟/小时/天/月/年）的历史分协议总流量/上行流量/下行流量统计功能
测试步骤： （1） 客户端/测试仪表发送多协议混合构造流量； （2） 被测系统按（分钟/小时/天/月/年）对总流量/上行流量/下行流量统计； （3） 被测系统按（分钟/小时/天/月/年）对分协议总流量/上行流量/下行流量统计； （4） 记录后台采用时间
预期结果：统计结果正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：82
分项目编号：统计报表输出功能（图形输出/文件输出）
测试项目：统计报表功能测试
测试目的：验证深度包检测设备是否支持统计报表输出功能
测试步骤： （1） 客户端/测试仪表发送多协议混合构造流量； （2） 被测系统进行流量统计； （3） 被测系统的统计报表支持报表统计，支持曲线图、柱形图、饼图、3D 等多种图形格式。 （4） 被测系统将流量统计报表输出为文件（.CSV、.HTML、.TXT 等）
预期结果： （1） 统计结果正确； （2） 正确输出统计报表
判定原则：测试结果必须与预期结果相符，否则不符合要求

13 管理功能测试

13.1 概述

本章定义了深度包检测设备的管理功能测试方法，包括系统管理功能测试方法，策略管理功能测试方法，告警、日志管理功能测试方法，网络管理功能测试方法和系统软件/特征库升级管理功能测试方法。

13.2 测试拓扑

本章规定的测试方法采用第 4 章中规定的测试拓扑 1 和测试拓扑 2。

13.3 系统管理功能测试

测试编号：83
分项目编号：基于命令行/图形界面的配置管理
测试项目：系统管理功能测试
测试目的：验证深度包检测设备是否支持基于命令行/图形界面的配置管理
测试步骤： （1） 被测系统正常加电启动； （2） 系统管理员通过串口，或者 Telnet 接入设备； （3） 系统管理员能够通过命令行对系统进行配置管理； （4） 系统管理员 Web 方式接入设备； （5） 系统管理员能够通过图形界面对系统进行配置管理； （6） 验证配置是否生效
预期结果：能正确通过命令行和图形界面进行配置管理，配置生效
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：84
分项目编号：SSH/SSL 接入
测试项目：系统管理功能测试
测试目的：验证深度包检测设备是否支持 SSH/SSL 接入
测试步骤： （1） 被测系统正常加电启动； （2） 系统管理员通过 SSH 接入设备； （3） 系统管理员能够通过命令行对系统进行配置管理； （4） 系统管理员通过 SSL 接入设备； （5） 系统管理员能够通过命令行对系统进行配置管理； （6） 验证配置是否生效
预期结果： （1） 步骤（2）、（3）中，被测系统支持 SSH 接入； （2） 步骤（4）、（5）中，被测系统支持 SSL 接入； （3） 配置生效
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：85
分项目编号：用户的分级分权
测试项目：系统管理功能测试
测试目的：验证深度包检测设备是否支持分级分权的用户管理
测试步骤： （1） 被测系统正常加电启动； （2） 系统管理员通过正确的用户名和密码进入系统； （3） 系统管理员能够为不同用户配置不同权限； （4） 验证配置是否生效
预期结果：不同级别的用户享有不同程度的权限
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：86
分项目编号：登录失败后的保护
测试项目：系统管理功能测试
测试目的：验证深度包检测设备是否支持登录失败后的保护，保证系统的安全，防止暴力破解
测试步骤： （1） 被测系统正常加电启动； （2） 系统管理员通过不正确的用户名和密码登录系统； （3） 连续重复若干次
预期结果：连续登录失败三次后，系统在一定时间内不允许再登录
判定原则：测试结果必须与预期结果相符，否则不符合要求

13.4 流量控制策略管理功能测试

测试编号：87
分项目编号：基于 IP 地址的流量控制策略管理
测试项目：流量控制策略管理功能测试
测试目的：验证深度包检测设备是否支持基于 IP 地址的流量控制策略管理，并能够灵活组织，针对单一 IP 地址、针对 IP 地址段
测试步骤： （1） 客户端发送多协议混合构造流量； （2） 系统根据单个 IP 地址进行策略控制，分别对 SourceIP = 1.1.1.1，或者 DesIP = 1.1.1.1 的数据流进行性能劣化，或者流量限速； （3） 系统根据源/目的 IP 地址进行策略控制，对 Source IP = 1.1.1.1 Des IP = 2.2.2.2 的流量进行性能劣化，或者流量限速； （4） 系统根据 IP 地址段进行策略控制，对 IP Range 1.1.1.x/24 的流量进行性能劣化，或者流量限速； （5） 被测系统必须能够对发出的干扰包进行统计，并支持查询； （6） 在流量终端点，通过协议分析仪捕获流量
预期结果：策略生效
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：88
分项目编号：基于用户/用户组的流量控制策略管理
测试项目：流量控制策略管理功能测试
测试目的：验证深度包检测设备是否支持基于用户/用户组的流量控制策略管理，并能灵活设置流量控制方式
测试步骤： （1） 测试配置如测试拓扑； （2） 客户端发送多协议混合构造流量； （3） 系统设置用户/用户组 A 和用户/用户组 B； （4） 系统设置用户/用户组 A 的流量控制为通过；系统设置用户/用户组 B 的流量控制为性能劣化； （5） 系统将 IP=1.1.1.x 关联到用户/用户组 A；将 IP= 2.2.2.x 关联到用户/用户组 B； （6） 系统调换用户/用户组 A 和 B 的流量控制方式； （7） 被测系统必须能够对发出的干扰包进行统计，并支持查询； （8） 在流量终端点，通过协议分析仪捕获流量
预期结果：策略生效
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：89
分项目编号：基于用户/用户组的多链路汇聚流量控制策略管理
测试项目：流量控制策略管理功能测试
测试目的：验证深度包检测设备是否支持基于用户/用户组的多链路汇聚流量控制策略管理，并能灵活设置流量控制方式（通过性能劣化）
测试步骤： （1） 客户端发送多协议混合构造流量，测试流量被负载均担多条链路上； （2） 系统设置用户/用户组 A 和用户/用户组 B； （3） 系统设置用户/用户组 A 的流量控制为通过；系统设置用户/用户组 B 的流量控制为性能劣化； （4） 系统将 IP=1.1.1.x 关联到用户/用户组 A；将 IP= 2.2.2.x 关联到用户/用户组 B； （5） 被测系统必须能够对发出的干扰包进行统计，并支持查询； （6） 在流量终端点，通过协议分析仪捕获流量
预期结果：策略生效
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：90
分项目编号：基于业务类型的流量控制策略管理
测试项目：流量控制策略管理功能测试
测试目的：验证深度包检测设备是否支持基于业务类型的流量控制策略管理，并能够灵活的为不同业务类型设置流量控制方式
测试步骤： （1） 客户端发送多协议混合构造流量； （2） 系统根据不同业务类型流量的协议特征值进行流量控制，选择将一种流量性能劣化为总带宽的50%，第二种流量性能劣化为总带宽的30%；第三种流量性能劣化为总带宽的10%； （3） 被测系统必须能够对发出的干扰包进行统计，并支持查询； （4） 在流量终端点，通过协议分析仪捕获流量
预期结果：策略生效
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：91
分项目编号：总数据流量/上行/下行带宽的流量控制策略管理
测试项目：流量控制策略管理功能测试
测试目的：验证深度包检测设备是否支持基于总数据流量/上行/下行带宽的流量控制策略管理
测试步骤： （1） 客户端发送多协议混合构造流量； （2） 系统对总带宽进行策略控制，限制总带宽流量为带宽的30%； （3） 在流量终端点，通过协议分析仪捕获流量； （4） 系统对下行带宽进行流量控制，限制下行带宽流量为总带宽的30%； （5） 在流量终端点，通过协议分析仪捕获流量； （6） 系统对上行带宽进行流量控制，限制上行带宽流量为总带宽的30%； （7） 在流量终端点，通过协议分析仪捕获流量； （8） 被测系统必须能够对发出的干扰包进行统计，并支持查询
预期结果：步骤（2）、（4）、（6）中，策略生效
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：92
分项目编号：基于时间的流量控制策略管理
测试项目：流量控制策略管理功能测试
测试目的：验证深度包检测设备是否支持基于时间的流量控制策略管理，并能够灵活的设置参数
测试步骤： （1） 客户端发送多协议混合构造流量； （2） 系统基于时间进行策略控制（例如，在工作时间内限制带宽流量）； （3） 在流量终端点，通过协议分析仪捕获流量； （4） 被测系统必须能够对发出的干扰包进行统计，并支持查询； （5） 设备必须支持多维度的时间策略（如，每周定时、节假日等）
预期结果：策略生效
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：93
分项目编号：同一用户下的连接/会话数限制策略控制管理
测试项目：流量控制策略管理功能测试
测试目的：验证深度包检测设备是否支持同一用户下的连接数限制的策略控制管理
测试步骤： （1） 客户端发送多协议混合构造流量； （2） 系统对同一用户下的连接数进行限制，最多 3 个连接/会话； （3） 在流量终端点，通过协议分析仪捕获流量
预期结果：策略生效
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：94
分项目编号：混合流量控制策略管理
测试项目：流量控制策略管理功能测试
测试目的：验证深度包检测设备是否支持混合的流量控制策略管理
测试步骤： （1） 客户端发送多协议混合构造流量； （2） 系统配置混合的/嵌套的流量控制策略，限制某一 IP 地址网段的 P2P 流媒体数据流量在 10 分钟内的流量； （3） 在流量终端点，通过协议分析仪捕获流量
预期结果：所有策略都生效
判定原则：测试结果必须与预期结果相符，否则不符合要求

13.5 告警日志管理功能测试

测试编号：95
分项目编号：告警功能
测试项目：告警日志管理功能测试
测试目的：验证深度包检测设备是否支持告警功能
测试步骤： （1） 被测系统正常加电启动； （2） 系统管理员通过正确的用户名和密码登录系统； （3） 插拔接口、或者以不正确的用户名/密码登录系统； （4） 系统能够收到相关告警信息
预期结果：被测系统支持告警管理功能
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：96
分项目编号：日志功能
测试项目：告警日志管理功能测试
测试目的：验证深度包检测设备是否支持日志查询
测试步骤： （1） 被测系统正常加电启动； （2） 系统管理员通过正确的用户名和密码登录系统； （3） 能够通过时间、连接、业务等进行日志查询； （4） 配置 Syslog 服务器，能够将日志导出到 Syslog 服务器上；或者已文本文件的形式对日志进行保存； （5） 也能够重 Syslog 服务器中导入相关日志；或者导入相关文本文件
预期结果： （1） 日志查询正确； （2） 支持日志的导入/导出
判定原则：测试结果必须与预期结果相符，否则不符合要求

13.6 网络管理功能测试

测试编号：97
分项目编号：集中网络管理功能
测试项目：网络管理功能测试
测试目的：验证深度包检测设备是否支持集中网络管理
测试步骤： （1） 被测系统正常加电启动； （2） 系统管理员通过正确的用户名和密码登录系统； （3） 配置 SNMP Agent； （4） 由网管系统集中进行管理
预期结果： （1） 被测系统支持 SNMPv1/v2 协议； （2） 网管能够通过 SNMP 对被测系统进行网络管理，读取到被测系统的 MIB
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：98
分项目编号：增加/删除节点
测试项目：网络管理功能测试
测试目的：验证深度包检测设备是否支持集中网络管理
测试步骤： （1） 被测系统正常加电启动； （2） 网管系统能够对被测系统进行远程管理； （3） 在拓扑图中增加/删除节点
预期结果：操作成功
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：99
分项目编号：配置管理
测试项目：网络管理功能测试
测试目的：验证深度包检测设备是否支持集中网络管理
测试步骤： （1） 被测系统正常加电启动； （2） 网管系统能够对被测系统进行远程管理； （3） 网管配置被测系统的系统管理员密码； （4） 网管配置被测系统的流量策略等
预期结果：操作成功
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：100
分项目编号：故障管理
测试项目：网络管理功能测试
测试目的：验证深度包检测设备是否支持集中网络管理
测试步骤： （1） 被测系统正常加电启动； （2） 被测系统关闭主电源、热插拔板卡、链路失效； （3） 被测系统能够向网管中心发送 Trap 信息； （4） 网管能够实现故障管理
预期结果：操作成功
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：101
分项目编号：性能管理
测试项目：网络管理功能测试
测试目的：验证深度包检测设备是否支持集中网络管理
测试步骤： （1） 被测系统正常加电启动； （2） 网管能够实现性能管理
预期结果：操作成功
判定原则：测试结果必须与预期结果相符，否则不符合要求

14 附加功能测试

14.1 概述

本章规定了深度包检测设备附加功能的测试方法，包括：用户特征信息识别功能测试。深度包检测设备可选进行附加功能的测试。

14.2 测试拓扑

本章规定的测试方法使用第 4 章中规定的测试拓扑 1 和测试拓扑 2。

14.3 用户特征信息识别功能测试

测试编号：102 （可选）
分项目编号：绑定用户认证信息
测试项目：用户特征信息识别功能测试
测试目的：验证深度包检测设备是否支持绑定用户认证信息功能，支持 IP 地址和用户认证 ID 的绑定
测试步骤： （1） 被测系统跟踪识别用户认证信息和所获得的特殊属性； （2） 被测系统绑定用户认证 ID 和用户 IP 地址（a@cnc.com， 10.10.10.10）； （3） 被测系统对用户认证 ID 为 a@cnc.com 的用户流量进行性能劣化，或者流量限速； （4） 被测系统针对用户获得的特殊属性进行策略控制； （5） 用户下线，重新上线； （6） 在流量终端点，通过协议分析仪捕获流量
预期结果： （1） 绑定正确； （2） 策略生效； （3） 用户重新上线后，策略依然正确
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：103 （可选）
分项目编号：系统生成用户的计费信息
测试项目： 用户特征信息识别功能测试
测试目的：验证深度包检测设备是否支持用户计费信息的生成
测试步骤： （1） 被测系统跟踪识别上送到 Radius 的用户认证信息； （2） 被测系统统计用户名为 a@cnc.com 的流量信息，并生成账单； （3） 将账单转换为 Radius 计费信息，上送到 Radius Server
预期结果： （1） 绑定正确； （2） 账单正确，能生成标准的 Radius 计费报文
判定原则：测试结果必须与预期结果相符，否则不符合要求

15 系统性能测试

15.1 概述

本章定义了深度包检测设备性能的测试方法，包括：两端口和线卡/整机分别在单条流和多条流有策略和无策略时的交换性能、整机最大并发连接数、整机最大每秒新建连接数、业务识别时间、业务识别准确度、业务控制略生效时间和控制准确度测试。

15.2 测试拓扑

本章规定的测试方法使用第 4 章中规定的测试拓扑 1、测试拓扑 2 和测试拓扑 3。

15.3 测试项目

测试编号：104
分项目编号：单条流交换性能（两端口）
测试项目：性能测试
测试目的：验证深度包检测设备的单条流交换性能
测试步骤： （1） 系统不配置任何策略控制； （2） 测试仪表发送 Internet 混合流量； （3） 测试时间为 120s； （4） 分别记录吞吐量、延时、和线速丢包率，测试时延时，流量为吞吐量的 99.5%； （5） 系统配置 1000 条策略； （6） 重复步骤（2）～（4）
测试说明：参考项

测试编号：105
分项目编号：多条流交换性能（两端口）
测试项目：性能测试
测试目的：验证深度包检测设备的多条流交换性能
测试步骤： （1） 系统不配置任何策略控制； （2） 测试仪表发送 10000 条 Internet 混合流量； （3） 测试时间为 120s； （4） 分别记录吞吐量、延时、和线速丢包率，测试时延时，流量为吞吐量的 99.5%； （5） 系统配置 1000 条策略； （6） 重复步骤（2）～（4）
测试说明：参考项

测试编号：106
分项目编号：单条流交换性能（整机/线卡）
测试项目： 性能测试
测试目的：验证深度包检测设备的单条流交换性能
测试步骤： （1） 系统不配置任何策略控制； （2） 测试仪表发送 Internet 混合流量； （3） 测试时间为 120s； （4） 分别记录吞吐量、延时、和线速丢包率，测试时延时，流量为吞吐量的 99.5%； （5） 系统配置 1000 条策略； （6） 重复步骤（2）～（4）
测试说明：参考项

测试编号：107
分项目编号：多条流交换性能（整机/线卡）
测试项目： 性能测试
测试目的：验证深度包检测设备的多条流交换性能
测试步骤： （1） 系统不配置任何策略控制； （2） 测试仪表发送 10000 条 Internet 混合流量； （3） 测试时间为 120s； （4） 分别记录吞吐量、延时、和线速丢包率，测试时延时，流量为吞吐量的 99.5%； （5） 系统配置 1000 条策略； （6） 重复步骤（2）～（4）
测试说明：参考项

测试编号：108
分项目编号：最大并发连接数
测试项目：性能测试
测试目的：验证深度包检测设备能够支持的最大并非连接数
测试步骤： （1） 测试配置如测试拓扑； （2） 系统不配置任何策略控制； （3） 测试仪表尽力而为的发送 TCP 连接； （4） 记录系统能够支持的最大 TCP 连接数； （5） 测试时间为 500s
测试说明：参考项

测试编号：109
分项目编号：业务识别时间
测试项目：性能测试
测试目的：验证深度包检测设备业务识别时间
测试步骤： （1） 测试配置如测试拓扑； （2） 系统不配置任何策略控制； （3） 测试仪表发送 500000 条多协议混合构造流量； （4） 系统在正常转发流量后，针对传统数据业务、P2P 流量、VoIP 流量、IM 流量分别进行识别； （5） 记录识别时间
测试说明：参考项

测试编号：110
分项目编号：业务识别误差率
测试项目：性能测试
测试目的：验证深度包检测设备业务识别误差率
测试步骤： （1） 测试配置如测试拓扑； （2） 系统不配置任何策略控制； （3） 测试仪表发送 500000 条多协议混合构造流量； （4） 系统在正常转发流量后，针对传统数据业务、P2P 流量、VoIP 流量、IM 流量分别进行识别； （5） 记录业务识别误差率
测试说明：参考项

测试编号：111
分项目编号：业务控制生效时间
测试项目：性能测试
测试目的：验证深度包检测设备策略生效时间
测试步骤： （1） 测试配置如测试拓扑； （2） 系统不配置任何策略控制； （3） 测试仪表发送 500000 条多协议混合构造流量； （4） 系统在正常转发流量后，针对测试流量配置策略控制，对测试流量进行限速，并下发生效； （5） 记录策略生效时间
测试说明：参考项

测试编号：112
分项目编号：流量控制误差率
测试项目：性能测试
测试目的：验证深度包检测设备的流量控制误差率
测试步骤： （1） 测试配置如测试拓扑； （2） 测试仪表满接口带宽发送多协议混合构造流量； （3） 系统在正常转发流量后，针对流量配置策略控制，对测试流量进行限速为总带宽的 10%，并下发生效； （4） 计算流量控制误差率
测试说明：参考项

16 供电测试

供电测试方法参见 YD/T 1156《路由器测试规范—高端路由器》第 13 章。

17 电气安全测试

电气安全测试方法参见 YD/T 1156《路由器测试规范—高端路由器》第 13 章。