

ICS 33.040.40  
M 32



# 中华人民共和国通信行业标准

YD/T 1899-2009

---

## 深度包检测设备技术要求

Technical Requirements 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 总体要求	4
5 功能要求	5
6 可靠性要求	7
7 安全要求	8
8 接口要求	8
9 操作维护要求	8
10 可扩展性要求	9
11 性能要求	9
12 电气安全	10
13 定时同步要求	10
14 电源要求	10
附录 A (资料性附录) 业务数据流分类	11
附录 B (资料性附录) 深度包检测设备性能指标参考	17

## 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. 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. 深度包检测设备技术要求
4. 深度包检测设备测试方法

本标准的附录 A、附录 B 均为资料性附录。

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

本标准主要起草人：马 科、田 辉、唐 浩、田慧蓉

# 深度包检测设备技术要求

## 1 范围

本标准规定了深度包检测设备的各项技术要求，包括：功能要求、可靠性要求、安全要求、接口要求、操作维护要求、可扩展性要求、性能要求以及功耗、电气安全、定时与同步等。

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 1097 路由器设备技术规范——高端路由器

## 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 Packet 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/目的端口。针对 TCP 流量，伪造成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。

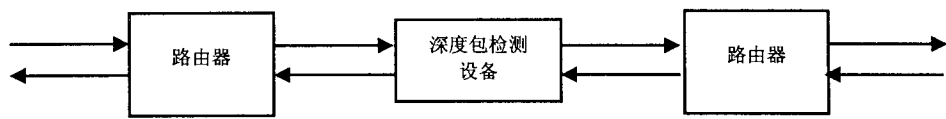


图 1 深度包检测设备串联接入方式

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。

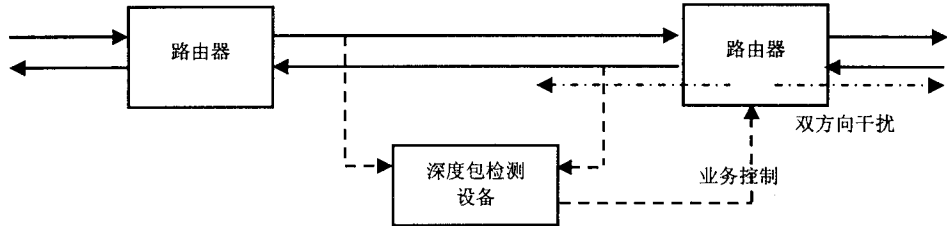


图 2 深度包检测设备并联接入方式

3.1.8

用户/用户组 User/User Group

用户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 总体要求

深度包检测设备的主要功能是通过识别网络业务，对特定网络业务实施有针对性的业务控制，同时对网络业务占用资源情况进行了解和分析，跟踪不同业务流量的发展变化趋势，为流量分析、网络规划和网络资源的管理提供依据，实现对网络业务应用的精细化管理，综合平衡用户的各种业务体验，发挥出现有网络的最大效益。

深度包检测设备应包括如下功能模块：

- (1) 业务数据流识别模块；
- (2) 业务数据流控制模块；
- (3) 业务特征信息库；
- (4) 业务控制策略库；
- (5) 统计模块等。

其中，业务特征信息库和业务控制策略库可位于深度包检测设备内部，也可单独实现。

深度包检测设备应满足如下功能和性能要求：

- (1) 具备业务数据流的识别功能、业务数据流的控制功能、业务流量的统计分析功能、用户管理功能和系统升级功能等；
- (2) 具备电信级的可靠性，支持关键部件的主备冗余，支持关键数据的备份恢复；

- (3) 具备一定的硬件和软件扩展性，支持软件的本地和远程升级；
- (4) 具备良好的系统安全性，支持系统的安全管理；在遭遇到网络攻击时，仍能正常工作；
- (5) 具备良好的开放性，支持开放的第三方开发接口；
- (6) 具备良好的人机界面和操作管理；
- (7) 在应用中，系统性能不应成为被监控链路的瓶颈，并满足相关要求。

## 5 功能要求

### 5.1 业务数据流识别功能

#### 5.1.1 业务数据流识别能力

深度包检测设备应支持以下业务数据流识别能力：

- (1) 特定封装类型的数据流识别，包括 802.1Q VLAN 流量、PPPoE 流量和 MPLS 流量；
- (2) IP 五元组识别，包括源 IP 地址、目的 IP 地址、协议类型、源端口号、目的端口号；
- (3) IP QoS 标记识别，包括 IP ToS 字段和 DSCP 码点；
- (4) 业务数据流报文特征字段识别；
- (5) 业务数据流流量行为特征识别；
- (6) 支持上下型不对称的业务数据流的识别；
- (7) 支持业务数据流信令流量和数据流量的关联识别。

深度包检测设备可选支持以下业务数据流识别能力：

- (1) 其他封装类型的数据流识别，如 GRE、L2TP 等；
- (2) 加密业务数据流识别，如 SSL、IPSec 等；
- (3) 用户识别，如用户认证 ID、用户标识信息、用户特殊属性等。

#### 5.1.2 识别业务数据流种类

深度包检测设备应支持对表 1 所列业务数据流的识别。

表 1 深度包检测设备应能够识别的业务流量

序 号	业务分类	业务名称
1	传统数据业务	Web 业务
		文件传输
		邮件服务
2	流媒体业务	RTSP
		MMS
3	P2P 应用	P2P 文件下载类应用
		P2P 流媒体类应用
		加密类 P2P 应用
4	VoIP 业务	信令消息
		媒体数据
5	网络游戏	
6	即时通信	文本信息
		文件传输数据
		语音信令和媒体数据
7	异常流量	攻击流量



深度包检测设备还可支持附录 A 中列出的其他业务数据流的识别。

注：随着网络业务的发展，表 1 和附录 A 将不定期修订。

## 5.2 业务数据流控制功能

在业务数据流识别的基础上，深度包检测设备应能够对业务数据流实施有针对性的业务数据流控制。深度包检测应该支持以下的业务数据流控制功能：

- (1) 能够对业务数据流进行阻塞、限速、QoS 控制或者连接/信令干扰；
- (2) 能够对业务数据流总流量、上行业务数据流和下行业务数据流分别实施业务数据流控制，且互不影响；
- (3) 能够对业务数据流实施绝对，或者相对的带宽分配；
- (4) 能够根据应用（组）类型（包含应用层协议，TCP/UDP 端口映射和协议字段）实施业务数据流控制；
- (5) 能够根据内/外网单独 IP 地址，或者 IP 地址段实施业务数据流控制；
- (6) 能够根据黑/白名单实施业务数据流控制；
- (7) 能够根据时间段实施业务数据流控制，且能够灵活配置包括每分钟、每小时、每天、每周、每月、每年、节假日在内的多个时间维度的设置；
- (8) 能够支持业务控制策略的实时下发、撤销和恢复操作；
- (9) 能够支持业务控制策略优先级的调整。

深度包检测设备可选支持以下业务数据流控制功能：

- (1) 能够根据用户/用户组实施业务数据流控制；
- (2) 能够对加密数据流实施业务数据流控制；
- (3) 能够对隧道内的业务数据流实施业务数据流控制，如 GRE、L2TP、MPLS 等。

## 5.3 业务数据流统计分析功能

深度包检测设备除应实现业务数据流识别功能和业务数据流控制功能外，还应实现对业务数据流识别和控制结果的分类统计、深度分析和报表输出。

深度包检测设备应支持如下的业务数据流统计分析功能：

- (1) 能够对监控链路的数据流量大小和数据流量分布进行统计分析；
- (2) 能够对监控链路的业务数据流总流量、上行业务数据流量、下行业务数据流量和分协议业务数据流量分别进行统计分析；
- (3) 能够对业务数据流量的数据速率、包速率以及并发连接数进行统计分析；
- (4) 能够对业务数据流量的流量流向、趋势、分布情况进行统计分析；
- (5) 能够根据业务数据流类型对业务数据流进行统计分析；
- (6) 能够根据 IP 地址或者 IP 地址段对业务数据流进行统计分析；
- (7) 能够根据时间对业务数据流进行统计分析，包括每分钟、每小时、每天、每周、每月、每年、节假日等多个时间维度；
- (8) 能够对业务数据流控制策略进行统计分析，包括业务数据流控制策略数目、业务数据流控制策略执行情况和业务数据流控制策略优先级等；
- (9) 支持灵活的统计分析方式，如：饼图、柱状图、曲线图、数据表和 TOP 10 等；
- (10) 支持统计结果的报表输出，并支持灵活的报表输出格式，如：CSV、HTML 和 XML 等。

深度包检测设备可选支持如下的业务数据流统计分析功能：

能够对用户行为进行统计分析，包括用户行为分析和用户兴趣分析等。

#### 5.4 附加功能

深度包检测设备可选支持用户特征信息识别功能，并支持将用户特征信息和业务数据流关联。

- (1) 能够识别用户认证信息，并获取用户认证 ID、获得的 IP 地址和特殊属性；
- (2) 能够识别用户计费信息，并获取用户计费特殊属性；
- (3) 支持用户认证 ID 和用户获得的 IP 地址的关联；
- (4) 支持用户认证 ID 和用户特殊属性的关联；
- (5) 支持用户认证 ID 和业务数据流的关联，并实施基于用户的业务数据流控制；
- (6) 支持用户计费信息和业务数据流的关联，并生成基于用户的原始计费信息。

#### 5.5 系统升级功能

深度包检测设备应支持软件和硬件的升级，其中软件升级可采用本地升级或者远程升级两种方式。

- (1) 支持定期或者不定期的业务识别特征库的升级更新；
- (2) 支持定期或者不定期的业务流量控制策略库的升级更新；
- (3) 支持定期或者不定期的系统软件的升级更新。

### 6 可靠性要求

#### 6.1 系统冗余

深度包检测设备应能够提供电信级的设备可靠性，应支持电源的主备冗余备份，并且在切换过程中，设备的正常工作不受影响；

如果深度包检测设备支持硬件模块化设计，还应支持如下的关键部件的主备冗余备份：

- (1) 支持控制卡的主备冗余备份、并且控制卡热插拔时，深度包检测设备正常工作不受影响；
- (2) 支持交换卡的主备冗余备份、并且交换卡热插拔时，深度包检测设备正常工作不受影响；
- (3) 支持业务板卡的热插拔，并且业务板卡热插拔时，深度包检测设备正常工作不受影响。

如果深度包检测设备不支持硬件模块化设计，上述规定不做要求。

#### 6.2 旁路流量机制

采用串联接入方式实现业务数据流识别和控制的深度包检测设备必须具备旁路监控链路流量的机制，并且满足如下要求：

- (1) 当链路或接口出现中断时，深度包检测设备应能够自动切换到旁路链路；
- (2) 当设备断电的时，深度包检测设备应能够自动切换到旁路链路；
- (3) 当系统软件出现故障而不能正常工作时，深度包检测设备应能够自动切换到旁路链路；
- (4) 在切换到旁路链路后，监控链路业务数据流转发正常；
- (5) 支持自动或手动的回切功能，并且业务数据流的转发不受影响。

#### 6.3 数据恢复与备份

深度包检测设备应具备关键数据的备份和恢复能力：

- (1) 系统配置参数表的备份和恢复；
- (2) 用户权限表的备份和恢复；

- (3) 业务识别特征库的备份和恢复;
- (4) 业务控制策略库的备份和恢复;
- (5) 灵活的数据备份策略制定。

本标准针对深度包检测设备的可靠性进行规定, 建议系统无故障工作时间>10000h, 建议系统故障恢复时间<1h。

## 7 安全要求

(1) 深度包检测设备自身应具备良好的安全性, 应能够抵御 DDoS 攻击, 并且在受到攻击时, 设备的正常工作不受影响, 并发出告警。

(2) 深度包检测设备应具备安全管理功能, 支持系统管理员的密码保护和防暴力破解功能; 深度包检测设备应支持系统管理用户的分级分权管理。

(3) 深度包检测设备应支持系统日志的记录和管理功能, 能够对系统操作和关键配置的改动进行记录, 支持系统日志的查询、导入和导出。

(4) 深度包检测设备应提供安全的管理接入方式, 如 SSH 接入和 SSL 接入等。

## 8 接口要求

### 8.1 概述

深度包检测设备应具备功能扩展能力, 应能够提供到网管系统、计费系统的接口, 应支持开放的第三方开发接口, 以满足必要的功能扩展。

### 8.2 网管系统接口

深度包检测设备应支持以下与第三方网管系统的接口:

- (1) 标准的 SNMP 接口;
- (2) 标准的 SysLog 接口;
- (3) 标准的 MIB 库结构。

接口方式: 应使用网管系统认可的接口方式, 可选采用自定义 API 方式、WebService 方式等。

### 8.3 计费系统接口

深度包检测设备应支持与计费系统的接口。

接口方式: 应采用计费账务系统认可的接口方式, 可选采用自定义 API 方式、WebService 方式等。

### 8.4 第三方开发接口

深度包检测设备应支持开放的第三方开发接口。

接口方式: 应使用标准的开发功能相关的接口方式, 可选采用自定义 API 方式、WebService 方式等。

## 9 操作维护要求

### 9.1 网络管理

深度包检测设备应支持集中的网络管理、统一的系统配置和业务数据流控制策略下发, 集中的设备性能监控和故障报警, 统一的设备系统软件、业务识别特征库和业务控制策略库的升级更新。

### 9.2 权限管理

深度包检测设备应支持如下权限管理功能:

- (1) 分级的权限管理；
- (2) 不同角色的管理；
- (3) 角色权限分配管理。

### 9.3 系统参数管理

深度包检测设备应支持管理用户设置系统相关参数，如：配置文件、版本号、系统命名、数据库设置、系统设置、路径设置等。

### 9.4 日志管理

深度包检测设备应支持完善的日志记录和管理功能，包括：

- (1) 日志记录，包括时间、访问者账号、访问者客户端 IP 以及访问者的所有配置操作；
- (2) 日志查询，支持根据账号、访问操作的日志查询；
- (3) 日志备份，支持人工和自动两种备份方式；
- (4) 日志删除：支持人工和自动两种删除方式。

### 9.5 系统监控

深度包检测设备应支持如下自身系统的性能监控：

- (1) 提供监控界面监控系统的自身运行状态，包括数据库状态、网络连接状态、检测 CPU 性能、内存消耗、硬盘占用情况、登录用户状态等；
- (2) 当系统级监控的内容达到预设的门限值，或业务级监控的内容出现异常，则由各功能模块产生监控告警事件发送给监控模块；
- (3) 监控模块负责将监控信息写入数据库表中，并按照级别要求通知管理员；
- (4) 告警通知可以是：SNMP Trap、Email 或是与第三方的事件管理平台接口。

## 10 可扩展性要求

深度包检测设备可以具备一定程度的软件或者硬件扩展性：

- (1) 可选支持硬件模块化设计；
- (2) 可选支持硬件级联设计；
- (3) 可选支持软件模块化设计，通过软件模块的扩充实现系统功能的扩展。

## 11 性能要求

深度包检测设备的性能参数包括：

- (1) 总体业务数据流识别误差率；
  - (2) 单业务识别性能参数：单业务数据流识别误差率（包括误识别率和漏识别率）、单业务数据流识别时间；
  - (3) 总体业务数据流控制误差率；
  - (4) 单业务控制性能参数：单业务数据流控制误差率、业务控制策略生效时间；
  - (5) 在连接干扰/信令干扰的业务数据流控制方式下，业务性能参数还应包括干扰流量总带宽；
  - (6) 交换性能参数：吞吐量、时延和最大并发连接数，其中并联接入方式不包括吞吐量和时延。
- 本标准中对所有性能参数指标不做规定，仅作为重要指标以附录 B 的形式列出供参考。

YD/T 1899-2009

## 12 电气安全

电气安全要求应符合YD/T 1097《路由器设备技术规范——高端路由器》第15章的规定。

## 13 定时同步要求

定时同步要求应符合YD/T 1097《路由器设备技术规范——高端路由器》第10章的规定。

## 14 电源要求

电源要求应符合YD/T 1097《路由器设备技术规范——高端路由器》第17章的规定。

附 录 A  
(资料性附录)  
业务数据流分类

### A.1 概述

本附录提供深度包检测设备设备可以支持识别的业务数据流分类，作为现阶段应用参考。

### A.2 网络业务分类

网络业务分类表如表A.1所示。

表 A.1 网络业务分类

序 号	业务种类		业务名称	具体应用
1	传统数据业务	Web 业务	HTTP	HTTP
				HTTP-PROXY
				HTTP-Tunnel
			HTTPS/SSL	HTTPS
			NNTP	NNTP
				NNTPS
		File Transfer	FTP	FTP
				FTP-Data
				FTPS
				FTPS-Data
			TFTP	TFTP
			Others	CMD
				NetBIOS (IP)
				NFS
				PRINTER
				PRINT-SRV
				RCP
				SUNRPC
				SYSLOG
		Email/News	CCMAIL	CCMAIL
			IMAP	IMAP2-TCP
				IMAP3-TCP
				IMAP2-UDP
				IMAP3-UDP
				IMAPS (Secure IMAP)
			Lotus-Notes	Lotus-Notes-TCP
				Lotus-Notes-UDP
			MS Exchange	MS Exchange
			POP	POP2
				POP2-UDP
				POP3
				POP3S
				Hybrid-POP
			SMTP	SMTP
				SMTP by Sender Domain

表 A.1 (续)

序 号	业务种类	业务名称	具体应用	
2	P2P 应用	P2P 文件下载	BitTorrent	
			eMule/eDonkey	
			Gnutella	
			POCO	
			Kazaa	
			PPPoint	
			迅雷	
		P2P 流媒体	PPstream	
			QQlive	
			PPlive	
			SNS	
			CCIPTV	
			UUSee	
		P2P 加密类	Skype	Skype PC to PC
				Skype out
3	IM/Chat	AOL/ICQ		美国在线
				AOL/ICQ-File
				AOL/ICQ-Message
				AOL/ICQ-Video
				AOL/ICQ-Voice
		MSN		MSN
				MSN-File
				MSN-Message
				MSN-Video
				MSN-Voice
		QQ		QQ
				QQ-File
				QQ-Message
				QQ-Video
				QQ-Voice
				QQ-NetDisk
		Skype		Skype-File
				Skype-Message
				Skype-Voice
		Yahoo		Yahoo-File
				Yahoo-Message
				Yahoo-Video
				Yahoo-Voice
		Sina-UC		SinaUC
				Sina-File
				Sina-Messege
				Sina-Video
				Sina-Voice
				Sina-Chatroom
		Google Talk		GTalk-Message
				GTalk-Voice
		Lava-Lava		Lava-Lava Message
				Lava-Lava File
				Lava-Lava Voice
				Lava-Lava Video

表 A.1 (续)

序 号	业务种类	业务名称	具体应用
4	流媒体业务	MMS	MMS
		PNS	PNS
		RDT	RDT
		RTP	RTP
			RTCP
		RTSP	RTSP-TCP
			RTSP-UDP
		Streaming-Tool	iTunes
			NetShow
			Quicktime
			RealAudio
			RealOne
			Winamp
			Windows Media Player
5	网络游戏	BianFeng/边锋	
		China Game Online/中国游戏在线	
		CS/反恐精英	
		Diablo	
		DOOM	
		HaoFang/浩方	
		Heaven/天堂	
		King of Kings	
		Legend/传奇	
		OurGame/联众	
		MSN Game	
		QQ Game/QQ 游戏	
		Quake	
		SINA Game/新浪游戏	
		WOW/魔兽世界	
		Basketball/街头篮球	
		剑侠情缘	
		QQ 音速	
		QQ 幻想	
6	VoIP	H.323	H.323-TCP
			H.323-UDP
			H.323 Q.931
			H.323 G.711-64K Codec
			H.323 G.711-56K Codec
			H.323 G.722-64K Codec
			H.323 G.722-56K Codec
			H.323 G.722-48K Codec
			H.323 G.723 Codec
			H.323 G.728 Codec
			H.323 G.729 Codec



表 A.1 (续)

序 号	业务种类	业务名称	具体应用
6	VoIP	H.323	H.323 H.261 Codec
			H.323 H.262 Codec
			H.323 H.263 Codec
		MGCP	MGCP-Audio
			MGCP-Video
			MGCP-Data
		SIP	SIP-TCP
			SIP-UDP
		Skype	Skype PC to PC
			Skype PC to Phone/ Skypeout
			SkypeIn
7	Terminal	T.120	T.120
		Others	Philips-VC-TCP
			VocalTec-Internet Phone
		Citrix	Citrix
			Citrix Datacollec
			Citrix-ICA
			Citrix IMA Client
			Citrix MgmtConsole
			Citrix Published Applications
			Citrix User Name
		Citrix Nfuse	Citrix Nfuse
		PCAnywhere	PCAnywhere
		RDP	MS-RDP-Client
		RLogin	RLogin
		SSH	SSH
		Telnet	RTelnet
			Telnet
			TelnetS
		X11	X11
8	Transactions/Databases	CORBA	CORBA-IIOP
			CORBA-IIOP-SSL
		CyberCash	CyberCash
		DaZhiHui	大智慧
		EXEC	EXEC
		LDAP	LDAP
			LDAPS
		Oracle	Oracle Service
			Oracle-CoAuthor
			Oracle-EM1
			Oracle-EM2

表 A.1 (续)

序 号	业务种类	业务名称	具体应用
8	Transactions/Databases	Oracle	Oracle .Net
			Oracle-ORASRV
			Oracle-Remote-Database
			Oracle-TLISRV
			Oracle-VP1/VP2
		SAP	SAP-DialogService
			SAP-InfoService
			SAP-Router
			SAP-to-ADABAS
			SAP-to-Infomix
		SQL	MS SQL Server
			SQL .NET
			SQL Service
9	Security	GRE	GRE
		IPSec	IPSec-AH
			IPSec-ESP
			IPSec-IKE
			IPSec-ISAKMP
		L2TP	L2TP
		PPTP	PPTP
		SUGP	SUGP
		Trojans	Millenium
			SpyBot
			Trojan
10	Network Infrastructure	ARP	ARP
		BGP	BGP
		BOOTP (DHCP)	BOOTP-Client
			BOOTP-Server
		CHARGEN	CHARGEN
		CMIP	CMIP-Agent
			CMIP-MAN
		DNS	DNS
		ECHO	ECHO
		EGP	EGP
		ICMP	ICMP
		ICMP	IGMP
		IPv6	IPv6
		NetFlow	NetFlow
		NPP	NPP
		NTP	NTP
		OSPF	OSPF
		PPPoE	PPPoE-Control
			PPPoE-Discovery

表 A.1 (续)

序 号	业务种类	业务名称	具体应用
10	Network Infrastructure	RADIUS	RADIUS-AUTH
			RADIUS-ACCT
		RIP	RIP
		RMON	RMON
		SNMP	SNMP-MON
			SNMP-TRAP
		STP	STP
		SYSLOG	SYSLOG
		TACACS	TACACS
		TIME	TIME

## 附录 B

(资料性附录)

## 深度包检测设备性能指标参考

## B.1 概述

本附录提供深度包检测设备性能参数的定义、公式表示和参考值，作为评估深度包检测设备性能的参考。

## B.2 深度包检测设备性能参数定义

## (1) 总体业务数据流识别误差率

该性能参数是评价深度包检测设备总体性能的性能指标之一，是测试中各业务数据流识别误差率的平方，与权重系数的乘积和的均方根，由 $\sigma_{SZ}$ 表示，单位：%。

公式表示如下： $\sigma_{SZ} = \sqrt{\sigma_{SD1}^2 \lambda_1 + \sigma_{SD2}^2 \lambda_2 + \dots + \sigma_{SDn}^2 \lambda_n}$ ,  $0 \leq \sigma_{SZ} \leq 1$

式中：

$\sigma_{SDi}$ ——被监控链路中各业务识别误差率， $-1 \leq \sigma_{SDi} \leq 1$ ,  $i=1,2,\dots,n, n \in N$ ;

$\lambda_i$ ——被监控链路中各业务对应的权重系数， $0 \leq \lambda_i \leq 1$ ,  $\sum_{i=1}^n \lambda_i = 1$ ,  $i=1,2,\dots,n, n \in N$ 。

## (2) 单业务数据流识别误差率

指特定业务总会话数（或者带宽）和业务识别与管理系统识别出的该业务的会话数（或者带宽）的差，与该业务总会话数（或者带宽）的比值，由 $\sigma_{SD}$ 表示，单位：%。

— 如果计算值 $>0$ ，表示单业务识别的漏识别率；

— 如果计算值 $<0$ ，表示单业务识别的误识别率；

公式表示为： $\sigma_{SD} = \frac{\alpha - \alpha_s}{\alpha}$ ,  $-1 \leq \sigma_{SD} \leq 1$

式中：

$\alpha$ ——特定业务总会话数（或者带宽）；

$\alpha_s$ ——业务识别与管理系统识别出的特定业务会话数（或者带宽）。

## (3) 单业务数据流识别时间

指从特定业务第一个数据包进入业务识别与管理系统，到业务识别与管理系统给出正确的业务类型识别结果所耗费的时间，由 $t_{SD}$ 表示，单位：秒。

公式表述如下： $t_{SD} = t_2 - t_1$ ,  $t_{SD} > 0$

式中：

$t_2$ ——业务识别与管理系统正确识别除特定业务的时间；

$t_1$ ——特定业务第一个数据包进入业务识别与管理系统的時間。

## (4) 总体业务数据流控制误差率

该性能参数是评价深度包检测设备总体性能的性能指标之一，指被监控链路中各业务管理误差率的平方，与权重系数乘积和的均方根，由 $\sigma_{KZ}$ 表示，单位：%。

公式表示如下： $\sigma_{KZ} = \sqrt{\sigma_{KD1}^2 \lambda_1 + \sigma_{KD2}^2 \lambda_2 + \dots + \sigma_{KDn}^2 \lambda_n}$ ,  $0 \leq \sigma_{KZ} \leq 1$

式中：

$\sigma_{KDi}$ ——被监控链路中各业务管理误差率， $-1 \leq \sigma_{KDi} \leq 1$ ,  $i=1,2,\dots,n, n \in N$ ;

$\lambda_i$ ——被监控链路中各业务对应的权重系数， $0 \leq \lambda_i \leq 1$ ,  $\sum_{i=1}^n \lambda_i = 1$ ,  $i=1,2,\dots,n, n \in N$ 。

#### (5) 单业务数据流控制误差率

指业务识别与管理系统设定的特定业务会话数（或者带宽）管理阈值和经过业务管理后的该业务的实际会话数（或者带宽）的差的绝对值，与业务识别与管理系统设定的该业务会话数（或者带宽）管理阈值的比值，由 $\sigma_{KD}$ 表示，单位：%。

具体公式表示如下： $\sigma_{KD} = \frac{|\beta - \beta_k|}{\beta}$ ,  $0 \leq \sigma_{KD} \leq 1$

式中：

$\beta$ ——业务识别与管理系统设定的特定业务会话数（或者带宽）管理阈值；

$\beta_k$ ——经过业务管理后的该业务的实际会话数（或者带宽）。

#### (6) 单业务数据流控制策略生效时间

指从业务管理策略下发生效开始，到经过管理后的业务会话数（或者带宽）达到设定的管理阈值正负误差 10% 的范围内，且流量稳定时所耗费的时间，由 $t_{KD}$ 表示，单位：秒。

具体公式表述如下： $t_{KD} = t_2 - t_1$ ,  $t_{KD} > 0$

式中：

$t_2$ ——业务会话数（或者带宽）到达管理阈值 $\pm 10\%$ 范围内，且流量稳定的时间；

$t_1$ ——业务管理策略下发生效时间。

#### (7) 干扰流量总带宽

指在连接/信令干扰业务数据流控制方式下，为实现特定业务的业务数据流控制，深度包检测设备向被监控链路中发送的干扰数据包的总带宽，由 $B_{KI}$ 表示，单位 bit/s。

#### (8) 交换吞吐量

指深度包检测设备在进行业务数据流识别，且业务数据流控制策略生效的情况下，在没有帧丢失的情况下，设备能够接收的最大速率，单位 pps。

#### (9) 交换时延

指深度包检测设备在进行业务数据流识别，且业务数据流控制策略生效的情况下，数据帧第一个字节进入系统到数据帧最后一个字节离开系统所耗费的时间，单位 $\mu s$ 。

#### (10) 最大并发连接

指深度包检测设备在进行业务数据流识别，且业务数据流控制策略生效的情况下，设备能够同时处理的连接的最大数目，单位：个。

### B.3 深度包检测设备性能参数参考值

深度包检测设备性能参数参考值见表 B.1。

表 B.1 深度包检测设备性能参数参考值

性能参数	参考值
总体业务数据流识别误差率	$0<\sigma_{SZ}<10\%$
单业务数据流识别误差率	$-10\%<\sigma_{SD}<10\%$
单业务数据流识别时间	$t_{SD}<60\text{ s}$
总体业务数据流控制误差率	$0<\sigma_{KZ}<10\%$
单业务数据流识别误差率	$0<\sigma_{SK}<10\%$
单业务数据流识别时间	$t_{KD}<30\text{ s}$
干扰流量总带宽	$B_{KI}<\text{被监控链路带宽的 }5\%$
交换吞吐量	被监控链路线速的 90%
交换时延	$<200\mu\text{s}$
最大并发连接数	$>150\text{ 万}$