

ICS 33.040.40

M 32



# 中华人民共和国通信行业标准

YD/T 1912-2009

---

## 基于软交换的媒体服务器 设备安全技术要求和测试方法

Security Technical Requirements and Test Methods for  
Media Server Based on Softswitch

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 术语、定义和缩略语.....1

4 媒体服务器在软交换网络中的位置.....2

5 通信安全要求.....3

6 可靠性要求.....3

    6.1 备份和冗余要求.....3

    6.2 系统重启时间.....3

    6.3 软件要求.....3

    6.4 连通性检查.....3

7 安全管理要求.....3

    7.1 权限管理.....3

    7.2 日志管理.....3

    7.3 远程管理.....3

    7.4 故障管理.....4

    7.5 消息跟踪.....4

8 测试方法.....4

    8.1 测试结构.....4

    8.2 测试项目.....5

参考文献.....14

## 前 言

本标准是软交换网络安全系列标准之一，该系列标准的结构和名称预计如下：

1. 软交换网络网管与运维安全技术要求
2. 软交换设备安全技术要求和测试方法
3. 基于软交换的应用服务器设备安全技术要求和测试方法
4. 基于软交换的媒体服务器设备安全技术要求和测试方法
5. 软交换业务接入控制设备安全技术要求和测试方法
6. 基于软交换的信令网关设备安全技术要求和测试方法
7. 媒体网关设备安全技术要求和测试方法
8. IP 智能终端设备安全技术要求和测试方法

随着技术的发展，还将制定后续的相关标准。

本标准与 YD/T 1386-2005《基于软交换的媒体服务器技术要求》、YD/T 1389-2005《基于软交换的媒体服务器测试方法》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：李 成、邱 钢

# 基于软交换的媒体服务器设备安全技术要求和测试方法

## 1 范围

本标准规定了软交换网络中媒体服务器设备在通信、可靠性和管理等方面的安全要求，并根据上述要求制定了相应的测试方法。

本标准适用于软交换网络中由运营商提供、维护 and 管理的媒体服务器设备。

## 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。

YDC 045-2007《基于软交换的网络组网总体技术要求》

## 3 术语、定义和缩略语

### 3.1 术语和定义

下列术语和定义适用于本标准。

#### 3.1.1

**软交换设备 Softswitch**

软交换设备是分组网的核心设备之一，它主要完成呼叫控制、媒体网关接入控制、资源分配、协议处理、路由、认证、计费等主要功能，并向用户提供各种基本业务和补充业务。

#### 3.1.2

**应用服务器 Application Server**

应用服务器是在软交换网络中向用户提供各类增强业务的设备，负责增强业务逻辑的执行、业务数据和用户数据的访问、业务的计费和管理等。它应能通过SIP协议控制软交换设备完成业务请求，通过SIP/H.248（可选）/MGCP（可选）协议控制媒体服务器设备提供各种媒体资源。

应用服务器可选地支持智能网协议，也可以向第三方开放API接口。

#### 3.1.3

**媒体服务器 Media Server**

媒体服务器是软交换网络中提供专用媒体资源功能的设备，为各种业务提供媒体资源和资源处理，包括DTMF信号的采集与解码，信号音的产生与发送。录音通知的发送，会议，不同编解码算法间的转换等各种资源功能、通信功能和管理维护功能。

### 3.2 缩略语

下列缩略语适用于本标准。

AS	Application Server	应用服务器
DTMF	Dual Tone Multiple Frequency	双音多频

IAD	Integrated Access Device	综合接入设备
HLSR	Home Location and Service Register	归属位置业务寄存器
MG	Media Gateway	媒体网关
Megaco	Media Gateway Controller	媒体网关控制器
MGCP	Media Gateway Control Protocol	媒体网关控制协议
MS	Media Server	媒体服务器
NBP	Network Border Point	网络边界点
NGN	Next Generation Network	下一代网络
SAC	Service Access Controller	软交换业务接入控制设备
SCN	Switched Circuit Network	电路交换网
SIP	Session Initiation Protocol	会话初始协议
SNMP	Simple Network Management Protocol	简单网络管理协议
TLS	Transport Layer Security	传输层安全协议
SS	Softswitch	软交换

#### 4 媒体服务器在软交换网络中的位置

媒体服务器的基本功能是在软交换网络中, 结合业务逻辑, 提供业务所需要的媒体资源, 广泛地应用于包括基本语音、IP Centrex、IP 会议、预付费业务、通知服务、Voice E-mail、统一通信等各种业务, 可以提供拨号音、忙音、回铃音、等待音和空号音等基本信号音以及会议、通知等复杂的媒体处理服务。根据实现方式的不同, 媒体服务器可由软交换或应用服务器控制。媒体服务器在软交换网络中的位置如图 1 所示。

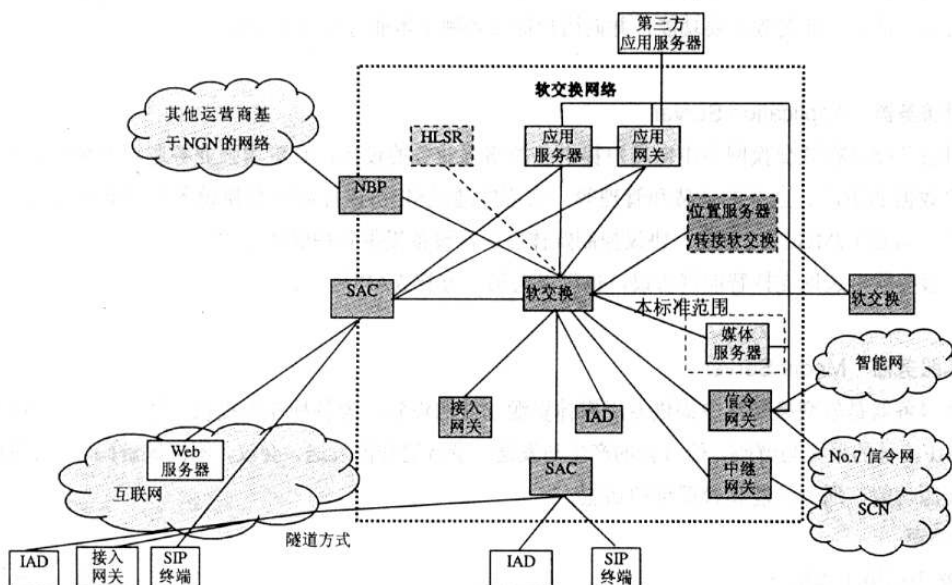


图1 媒体服务器在软交换网络中的位置

## 5 通信安全要求

媒体服务器与软交换、应用服务器之间的通信安全可优先通过承载网的规划构建安全信任域的方式实现。构建安全信任域的方式应符合 YDC 045-2007《基于软交换的网络组网总体技术要求》中对承载网的技术要求。

## 6 可靠性要求

### 6.1 备份和冗余要求

媒体服务器设备应提供对重要部件的冗余备份和容错管理。媒体服务器设备内关键的物理部件均支持冗余配置，如主CPU、时钟源输入接口、时钟系统等，主要单板采用热备份方式，所有单板均支持热插拔。当相关模块发生故障时，应能自动切换到备用处理模块而不影响当前呼叫的状态。

### 6.2 系统重启时间

媒体服务器设备的重新启动时间应小于20min。

### 6.3 软件要求

在不影响正常通信的情况下，能够对媒体服务器进行软件版本升级，支持软件版本的回退功能。

媒体服务器设备应能够实时地接受操作维护人员对配置数据的查询、修改、生成和删除，且不影响系统的正常运行。

### 6.4 连通性检查

媒体服务器设备与所连接的软交换设备或应用服务器设备之间应存在心跳消息，用于进行连通性检查。对于SIP协议使用OPTION作为心跳消息，对于H.248协议使用AuditValue或AuditCapabilities消息作为心跳消息，对于MGCP协议使用AuditEndpoint 或AuditConnection消息作为心跳消息。

## 7 安全管理要求

### 7.1 权限管理

在管理员进入系统之前，应鉴别管理员身份，鉴别时采用账户和密码机制，密码应不采用明文显示，在存储和传输时进行加密保护，系统对每次访问应进行记录。

媒体服务器应对管理员的访问权限有严格的规定。根据管理员的操作维护需要，系统可以对其权限进行分类，如系统管理员、配置管理员、维护管理员等，系统应能防止非授权登录和非授权操作。

在经过一定次数的身份鉴别失败以后，媒体服务器应锁定该账号。

### 7.2 日志管理

媒体服务器应记录所有操作员的所有操作日志，内容至少应包括：操作时间、命令执行时间、操作员、操作终端、输入的命令内容、命令的结果等。

### 7.3 远程管理

媒体服务器应具有本地和远端管理操作维护接口，以支持相关的监控、管理和维护。

媒体服务器应至少支持以下一种远程管理机制。

#### (1) SNMP

支持SNMPv2c作为远程管理安全机制。

#### (2) 远程登录

支持SSHv1和SSHv2，通过认证算法和加密算法实现对管理信息的机密性和完整性保护。

(3) Web管理

支持SSL/TLS安全协议，实现对管理信息的机密性和完整性保护。

(4) 其他

对于设备特定的远程管理机制，也应提供相应的机制实现对管理信息的机密性和完整性保护。

另外，设备应提供关闭远程管理功能和不必要服务端口的能力，且所有远程管理功能缺省是关闭的。

7.4 故障管理

媒体服务器应具有以下故障管理功能。

(1) 告警的级别

媒体服务器应具备完善的告警系统，并可以按照故障的严重程度分类，一般至少应分为两大类，即紧急告警和非紧急告警。

(2) 告警的记录

媒体服务器应能记录所有告警信息，并能够查询告警记录。

(3) 告警的显示

对于非紧急告警，操作维护管理终端、网管界面或设备上应该能够显示可视的警示信息；对紧急告警应可提供可视和可闻的警示信息。

7.5 消息跟踪

媒体服务器应具有消息（信令消息和/或媒体消息）跟踪的能力，可以根据管理员的指令，对各种消息进行跟踪，包括从设备发出的和收到的消息。可跟踪的消息协议类型至少包括：SIP、MGCP和H.248。

消息跟踪的结果可以显示在终端上，输出到文件或打印机。

8 测试方法

8.1 测试结构

图2为媒体服务器设备安全测试的测试结构1，本标准中的测试项均以软交换设备控制媒体服务器为例，如果采用应用服务器控制媒体服务器的方式，则需将图中的软交换设备更换为应用服务器。

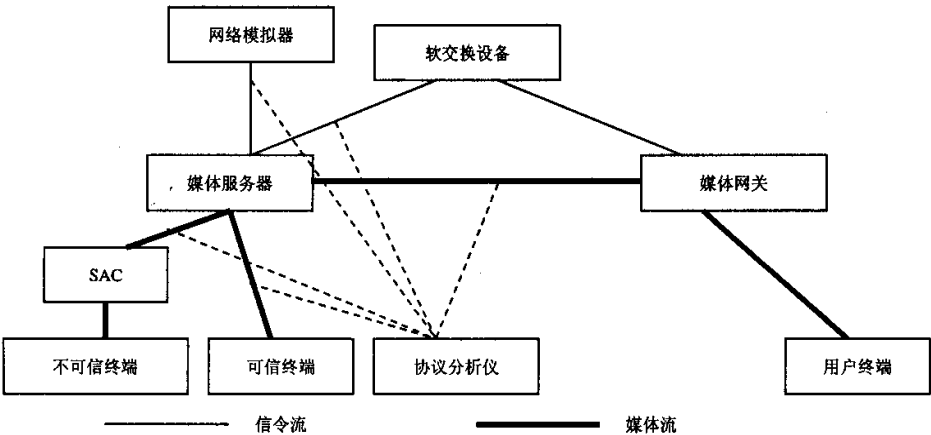


图2 媒体服务器安全测试的测试结构1

## 8.2 测试项目

### 8.2.1 可靠性测试

#### 8.2.1.1 备份和冗余要求

测试编号：1.1.1
测试项目：主、备电源的切换测试
测试配置：测试结构 1
预置条件： 1) 媒体服务器正常工作。 2) 媒体服务器配置主、备用电源
测试过程： 将媒体服务器主电源切断，使媒体服务器采用备用电源工作
预期结果： 媒体服务器应能自动启用备用电源，并且不影响正常通信
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：1.1.2
测试项目：主、备系统处理板的切换测试
测试配置：测试结构 1
预置条件： 1) 媒体服务器正常工作。 2) 媒体服务器配置主、备系统处理板
测试过程： 1) 拔掉主系统处理板； 2) 观察备用系统处理板是否进入工作状态，通信是否中断，并记录切换所用时间； 3) 将拔掉的系统处理板插回，观察该板卡是否进入（备用）工作状态
预期结果： 1) 在主系统处理板拔下后，能够在网管系统或设备的指示灯上看到用户处理板处于未安装状态。 2) 拔掉主系统处理板后，备用系统处理板进入（主用）工作状态，通信未中断。 3) 将拔掉的系统处理板插回后，该板卡可进入（备用）工作状态
判定原则：测试结果必须与预期结果相符，否则不符合要求



## 8.2.1.2 系统重启时间

测试编号：1.2.1
测试项目：系统重启时间
测试配置：测试结构 1
预置条件： 媒体服务器正常工作
测试过程： 1) 重新启动媒体服务器； 2) 记录媒体服务器从重启到正常工作的时间
预期结果： 媒体服务器重新启动到正常工作之间的时间小于 20min
判定原则：测试结果必须与预期结果相符，否则不符合要求

## 8.2.1.3 软件要求

测试编号：1.3.1
测试项目：在线软件版本升级
测试配置：测试结构 1
预置条件： 媒体服务器正常工作
测试过程： 1) 在媒体服务器上加载新版本的系统软件； 2) 查看版本升级后的媒体服务器是否可正常工作
预期结果： 1) 更新版本后的媒体服务器可正常工作； 2) 更新版本的操作不影响已有的通信
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：1.3.2
测试项目：在线软件版本回退
测试配置：测试结构 1
预置条件： 1) 媒体服务器正常工作。 2) 媒体服务器已经加载了新的软件版本
测试过程： 1) 在媒体服务器上进行操作，将软件版本回退到升级前的版本； 2) 查看版本回退后的媒体服务器是否可正常工作
预期结果： 1) 版本回退后的媒体服务器可正常工作； 2) 版本回退操作不影响已有的通信
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：1.3.3
测试项目：数据维护功能
测试配置：测试结构 1
预置条件： 1) 媒体服务器正常工作。 2) 系统管理人员可通过远程管理终端或本地操作维护终端登录到媒体服务器，进行数据维护操作
测试过程： 通过终端登录到媒体服务器，对媒体服务器的配置数据进行查询、修改、删除操作，查看是否影响媒体服务器的正常工作
预期结果： 系统管理人员对媒体服务器配置数据的维护操作不会影响媒体服务器的正常工作
判定原则：测试结果必须与预期结果相符，否则不符合要求

#### 8.2.1.4 连通性检查

测试编号：1.4.1
测试项目：连通性检查
测试配置：测试结构 1
预置条件： 媒体服务器工作正常
测试过程： 使用仪表跟踪媒体服务器与软交换设备之间的信令消息，查看是否存在用于连通性检查的心跳消息
预期结果： 1) 媒体服务器正常工作情况下，能够响应软交换设备发送来的心跳消息，也能够主动向软交换设备发送心跳消息。 2) 心跳消息的类型如下： — 当使用 SIP 协议时，心跳消息为 OPTION； — 当使用 H.248 协议时，心跳消息为 AuditValue 或 AuditCapabilities； — 当使用 MGCP 协议时，心跳消息为 AuditEndpoint 或 AuditConnection
判定原则：测试结果必须与预期结果相符，否则不符合要求

8.2.2 安全管理测试

8.2.2.1 权限管理

测试编号：2.1.1
测试项目：权限的设置
测试配置：测试结构 1
预置条件： 媒体服务器正常工作
测试过程： 1) 系统管理员登录设备进行权限管理； 2) 输入用户名和密码，进入系统； 3) 增加配置和维护管理员列表，并为不同用户设置不同的权限； 4) 设置身份鉴别失败后锁定该账号的次数； 5) 设置登录超时锁定的时长； 6) 管理员退出
预期结果： 1) 系统能够提供登录提示（允许用户输入用户名和密码），输入的密码不以明文显示； 2) 授权管理员可以为不同用户设置不同的权限； 3) 授权管理员可以设置身份鉴别失败后锁定账号的次数以及登录超时锁定的时长； 4) 管理员的登录操作有日志记录
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：2.1.2
测试项目：身份鉴别失败处理
测试配置：测试结构 1
预置条件： 媒体服务器正常工作
测试过程： 管理员输入 $N$ 次错误的用户名和密码（ $N$ 为设置的身份鉴别失败后锁定该账号的次数）
预期结果： $N$ 次登录不成功，退出登录界面，用户账号被锁定
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：2.1.3
测试项目：越权操作测试
测试配置：测试结构 1
预置条件： 媒体服务器正常工作
测试过程： 1) 管理员登入系统； 2) 管理员进行权限内的操作； 3) 管理员进行权限外的操作
预期结果： 1) 管理员可以进行权限内的操作，且有日志记录； 2) 管理员无法进行权限外操作
判定原则：测试结果必须与预期结果相符，否则不符合要求

#### 8.2.2.2 日志管理

测试编号：2.2.1
测试项目：安全日志的记录
测试配置：测试结构 1
预置条件： 媒体服务器正常工作
测试过程： 1) 以不存在的用户身份试图登录； 2) 以管理员用户名和错误的口令试图登录； 3) 检查设备是否记录了上述失败的登录
预期结果： 设备记录了登录尝试的时间、连接的方式（本地、Telnet 及远程地址）等
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：2.2.2
测试项目：操作日志的记录
测试配置：测试结构 1
预置条件： 媒体服务器正常工作
测试过程： 1) 以系统管理员的身份登录，增加一个新的管理员账号； 2) 检查是否记录了上述操作； 3) 以维护管理员的身份登录，增加一条配置数据； 4) 检查是否记录了上述操作
预期结果： 设备应记录操作时间、命令执行时间、操作员、操作终端、输入的命令内容、命令的结果等
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：2.2.3
测试项目：操作日志的查询和管理
测试配置：测试结构 1
预置条件： 媒体服务器正常工作
测试过程： 1) 查看日志文件； 2) 根据操作时间、操作员、操作终端等条件查询系统的日志
预期结果： 1) 可以根据操作时间、操作员、操作终端等条件查询系统的日志； 2) 系统日志能够存储到文件中
判定原则：测试结果必须与预期结果相符，否则不符合要求

### 8.2.2.3 远程管理

2.3.1~2.3.4 至少选一项进行测试。

测试编号：2.3.1（可选）
测试项目：支持 SNMPv2c
测试配置：测试结构 1
预置条件： 1) 媒体服务器正常工作； 2) 配置媒体服务器为 SNMPv2c 代理
测试过程： 管理员使用 SNMPv2c 客户端软件验证、查询并管理设备
预期结果： 管理员能正确查询和管理被测设备
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：2.3.2（可选）
测试项目：远程登录支持 SSH 连接
测试配置：测试结构 1
预置条件： 1) 媒体服务器正常工作； 2) 配置媒体服务器支持 SSH 远程登录
测试过程： 1) 管理员以 SSH 协议发起连接并登录系统； 2) 检查数据的加密算法； 3) 关闭 SSH 远程登录
预期结果： 1) 管理员成功登录； 2) 随后的数据被正确加密； 3) 设备上可以关闭 SSH 远程登录
判定原则：测试结果必须与预期结果相符，否则不符合要求

测试编号：2.3.3（可选）
测试项目：基于 Web 的管理支持 SSL/TLS 方式
测试配置：测试结构 1
预置条件： 1) 媒体服务器正常工作； 2) 配置媒体服务器支持 SSL/TLS 方式
测试过程： 1) 管理员以SSL/TLS方式基于Web对设备进行管理； 2) 检查数据的加密算法； 3) 关闭基于Web的管理
预期结果： 1) 管理员可以成功实现基于Web的管理； 2) 管理数据以SSL/TLS方式加密传输； 3) 设备上可以关闭基于Web的管理
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：2.3.4（可选）
测试项目：其他远程管理方式
测试配置：测试结构 1
预置条件： 1) 媒体服务器正常工作； 2) 媒体服务器配置其他的远程管理方式（可以是基于私有接口的远程管理软件）
测试过程： 通过其他远程管理方式对媒体服务器进行管理，包括登录、数据的维护等操作
预期结果： 1) 管理员可采用其他远程管理方式对媒体服务器进行管理。 2) 其他远程管理方式可保证管理操作所进行的数据交互的机密性和完整性
判定原则：测试结果必须与预期结果相符，否则不符合要求

8.2.2.4 故障管理

测试编号：2.4.1
测试项目：故障告警级别
测试配置：测试结构 1
预置条件： 媒体服务器正常工作
测试过程： 1) 媒体服务器正常工作时，观察是否有告警产生； 2) 构造条件使媒体服务器产生告警，分别产生硬件告警、系统资源告警、通信故障告警、传输质量告警； 3) 观察媒体服务器是否上报告警，告警信息是否正确； 4) 观察媒体服务器的告警是否分级
预期结果： 1) 媒体服务器正常工作时不产生告警。 2) 当媒体服务器出现故障时，媒体服务器能自动、正确地上报告警内容。 3) 媒体服务器的告警可以分级，至少包括紧急告警和非紧急告警两级
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：2.4.2
测试项目：告警记录
测试配置：测试结构 1
预置条件： 媒体服务器正常工作
测试过程： 1) 构造条件使媒体服务器产生告警，分别产生硬件告警、系统资源告警、通信故障告警、传输质量告警； 2) 查看媒体服务器是否记录告警内容，并以文件形式保存
预期结果： 媒体服务器可对故障告警的内容进行记录，并以文件形式保存
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：2.4.3
测试项目：告警显示
测试配置：测试结构 1
预置条件： 媒体服务器正常工作
测试过程： 1) 构造条件使媒体服务器产生告警，分别产生硬件告警、系统资源告警、通信故障告警、传输质量告警； 2) 对于非紧急告警，查看媒体服务器是否能在操作维护终端、网管系统或设备自身上产生可视的警示信息； 3) 对于紧急告警，查看媒体服务器是否能在操作维护终端、网管系统或设备自身上产生可视和可闻的警示信息
预期结果： 1) 媒体服务器可在出现非紧急告警的情况下采用可视的方式显示告警信息。 2) 媒体服务器可在出现紧急告警的情况下采用可视和可闻的方式显示告警信息
判定原则：测试结果必须与预期结果相符，否则不符合要求

#### 8.2.2.5 消息跟踪

测试编号：2.5.1
测试项目：消息跟踪
测试配置：测试结构 1
预置条件： 媒体服务器正常工作
测试过程： 1) 进入媒体服务器的操作维护界面，启用消息跟踪界面； 2) 使用终端或信令模拟器发起正常业务； 3) 检查媒体服务器是否能监测以下协议消息：MGCP或H.248或SIP； 4) 检查媒体服务器是否可根据用户标识、IP地址、端口、协议进行消息过滤
预期结果： 1) 媒体服务器可以提供消息监测功能； 2) 消息跟踪的结果可显示在终端上，输出到文件或打印机
判定原则：测试结果必须与预期结果相符，否则不符合要求



## 参 考 文 献

- [1] YDC 1003-2001 《软交换设备总体技术要求》
  - [2] YD/T 1386-2005 《基于软交换的媒体服务器技术要求》
  - [3] YD/T 1389-2005 《基于软交换的媒体服务器测试方法》
-

中 华 人 民 共 和 国  
通 信 行 业 标 准  
基于软交换的媒体服务器设备安全技术要求和测试方法  
YD/T 1912-2009

\*

人民邮电出版社出版发行  
北京市崇文区夕照寺街14号A座  
邮政编码：100061  
北京新瑞铭印刷有限公司印刷  
版权所有 不得翻印

\*

开本：880×1230 1/16 2009年8月第1版  
印张：1.25 2009年8月北京第1次印刷  
字数：36千字

ISBN 978 - 7 - 115 - 1891/09 - 133

定价：12元

本书如有印装质量问题，请与本社联系 电话：(010)67114922