

**YD**

# 中华人民共和国通信行业标准

YD/T 1393-2005

---

## 无线应用协议(WAP) 网关设备测试方法

Testing methods of Wireless Application Protocol(WAP) gateway

2005-09-01 发布

2005-12-01 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 测试环境要求	2
4.1 测试连接结构	2
4.2 设备要求	2
5 系统功能测试	3
5.1 测试环境	3
5.2 测试内容	4
6 业务功能测试	25
6.1 测试环境	25
6.2 测试内容	25
7 网关性能测试	35
7.1 测试环境	35
7.2 测试内容	35
8 协议测试	41
8.1 测试环境	41
8.2 测试内容	41
9 操作维护及网管功能测试	43
9.1 测试结构	43
9.2 测试内容	43
附录 A (规范性附录) 测试项目总表	55

## 前 言

本标准是“WAP 网关设备”系列标准之一。该系列标准的名称及结构预计如下：

1. 《无线应用协议（WAP）网关设备技术要求》；
2. 《无线应用协议（WAP）网关设备测试方法》。

本标准与《无线应用协议（WAP）网关设备技术要求》配套使用。

本标准的附录A是规范性附录。

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：信息产业部电信研究院

本标准起草人：谢 玮

## 无线应用协议 (WAP) 网关设备测试方法

### 1 范围

本标准规定了WAP网关设备的测试方法, 测试内容包括系统功能、业务功能、设备性能、协议支持和网管操作维护功能等。其中每项测试内容均规定了测试环境、测试连接、测试步骤、判定方法等。

本标准适用于WAP网关设备<sup>1</sup>。

### 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 1392-2005

无线应用协议(WAP)网关设备技术要求

### 3 缩略语

下列缩略语适用于本标准。

CDMA	Code Division Multiple Access	码分多址
CDPD	Cellular Digital Packet Data	蜂窝数字分组数据
CPI	Capabilities and Preference Information	能力和优先级别信息
CSD	Circuit Switched Data	电路交换数据
DNS	Domain Name System	域名系统
GPRS	General Packet Radio Service	公用分组无线业务
GSM	Global System for Mobile Communication	全球移动通信系统
GGSN	Gateway GPRS Support Node	关口GPRS支持节点
HTTP	Hyper Text Transfer Protocol	超文本传送协议
HTML	Hyper Text Markup Language	超文本标记语言
MSISDN	Mobile Subscriber ISDN	移动用户ISDN
NAS	Network Access Server	网络接入服务器
OTA-HTTP	Over the Air HTTP	空中HTTP
OTA-WSP	Over the Air WSP	空中WSP
PAP	Push Access Protocol	Push访问协议

<sup>1</sup> 本标准适用于WAP网关设备的测试, 全部的测试项适用于支持双协议栈(WAP1.x和WAP2.0)的WAP网关。在本标准第10章的表1“测试项目总表”中的备注栏, 将标注该测试项适用于哪种单协议栈类型的WAP网关。

PPG	Push Proxy Gateway Push	代理网关
PKI	Public Key Infrastructure	公共密钥体系
POTA	Push Over-the-Air Protocol Push	空中协议
PDSN	Packet Data Service Node	分组数据服务节点
SI	Service Indication	业务指示
SMS	Short Message Service	短消息业务
SSL	Secure Sockets Layer	套接字安全层
TLS	Tunnel Layer Security	隧道层安全
TCP/IP	Transport Control Protocol/Internet Protocol	传输控制协议 / 因特网协议
URL	Uniform Resource Locator	统一资源定位
WAE	Wireless Application Environment	无线应用环境
WAP	Wireless Application Protocol	无线应用协议
WBXML	WAP Binary Extensible Markup Language	WAP二进制扩展标记语言
WCSS	Wireless profile Cascading Style Sheet	无线轮廓层叠类型表单
WDP	Wireless Datagram Protocol	无线数据报协议
WML	Wireless Markup Language	无线标记语言
WSP	Wireless Session Protocol	无线会话协议
WTA	Wireless Telephony Application	无线电话应用
WTLS	Wireless Transport Layer Security	无线传输层安全
WTP	Wireless Transaction Protocol	无线事务协议
WHTTI	Wireless Profiled HTTP	无线优化HTTP协议
WTCP	Wireless Profiled TCP	无线优化TCP协议
XHTML	Extensible Hyper Text Markup Language	扩展超文本标记语言

## 4 测试环境要求

### 4.1 测试连接结构

详见各章节的测试连接图。

### 4.2 设备要求

#### 4.2.1 被测设备要求

被测设备包括WAP网关系统一套（包括全部功能模块）。

被测WAP网关系统应具有局域网接口，能够支持各种系统、业务、管理功能。

#### 4.2.2 辅助设备要求

测试所需的辅助设备包括：

- 局域网环境；
- 无线网络环境；
- AAA 服务器；
- DNS 服务器；

- 短消息系统；
- 参考 WAP1.x 终端及 WAP2.0 终端若干；
- 其他设备（如参考 WWW 服务器、Push 应用服务器、Java 应用服务器、WTA 服务器以及支持 UAProf、Provisioning 等业务所需的服务器或相关设备）。

参考 WAP 终端应能进行各种业务参数配置，支持各种需测试的业务（包括 Java、WTLS、SSL、Provisioning、UAProf、Push、WTA 等）。

参考 WWW 服务器中应预置好相应的参考网页（包括 XHTML / WCSS / WML / HTML 等）。

Java 应用服务器中应预置好相应的 Java 应用。

Push 应用服务器中应预置好相应的 Push 消息。

#### 4.2.3 测试仪表要求

协议分析仪应支持 WAP1.x 和 WAP2.0 各层协议的解析，包括 WHHTTP、TLS、WTCP、SSL、WSP、WTP、WTLS、PAP、OTA 等协议。

### 5 系统功能测试

#### 5.1 测试环境

WAP 网关系统功能测试结构如图 1 所示。

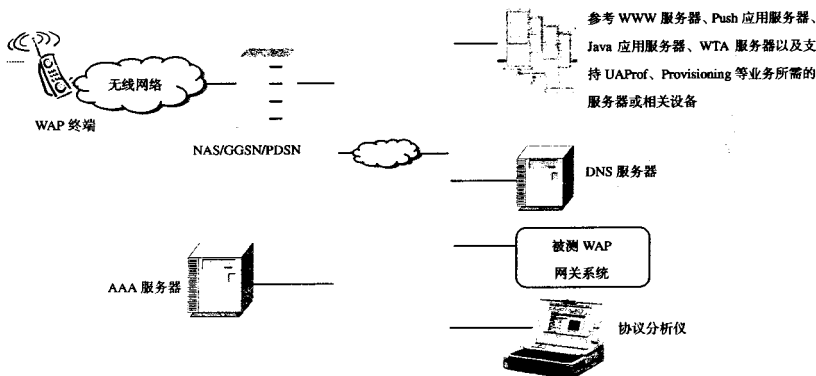


图 1 WAP 网关系统功能测试结构示意图

## 5.2 测试内容

测试编号：1
测试项目：用户认证功能
测试子项目：用户主叫号码认证功能
测试目的：验证系统是否支持用户主叫号码验证功能，同时验证 WAP 网关是否实现用户的主叫号码和 IP 地址对应关系功能
测试配置：连接如图 1 所示
<p>测试步骤：</p> <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接，并在系统中加入 WAP 终端的基本用户信息；</li> <li>2) WAP 终端正确进行配置；</li> <li>3) 从 WAP 终端登录被测 WAP 网关；</li> <li>4) 验证登录是否正常；</li> <li>5) 更换 WAP 终端主叫号码（该用户信息在 WAP 系统中不存在），再次登录被测 WAP 网关，验证登录是否能够被拒绝；</li> <li>6) 利用协议分析仪观察信令交互流程</li> </ol>
<p>预期结果：</p> <ol style="list-style-type: none"> <li>1) 用户认证结果准确；</li> <li>2) 如果认证通过，WAP 网关的用户数据库中能查到 IP—主叫号码的对应关系；</li> <li>3) 协议分析仪中的信令流程准确，包括 Accounting Req /Accept 等</li> </ol>
<p>判定原则：</p> <p>达到以上预期结果则通过</p>

测试编号：2
测试项目：用户认证功能
测试子项目：账号密码认证功能
测试目的：验证系统是否支持账号密码验证功能
测试配置：连接如图 1 所示
测试步骤： <ol style="list-style-type: none"><li>1) 将 WAP 系统正确连接，并在系统中加入参考 WAP 终端的基本用户信息；</li><li>2) 参考 WAP 终端，正确进行用户账号和密码配置；</li><li>3) 从 WAP 终端登录被测 WAP 网关；</li><li>4) 验证登录是否正常；</li><li>5) 更换账号密码设置（该用户信息在系统中不存在），再次登录被测 WAP 网关，验证登录是否能够被拒绝；</li><li>6) 利用协议分析仪观察信令交互流程</li></ol>
预期结果： <ol style="list-style-type: none"><li>1) 用户认证结果准确；</li><li>2) 如果认证通过，WAP 网关的用户数据库中能查到 IP—账号的对应关系；</li><li>3) 协议分析仪中的信令流程准确</li></ol>
判定原则： <p>达到以上预期结果则通过</p>



测试编号: 3
测试项目: 用户认证功能
测试子项目: 用户下线处理功能
测试目的: 验证 WAP 网关在用户下线 (用户关闭浏览器、关机或费用到达门限值等) 后, 能否自动删除该用户相关的临时信息
测试配置: WAP 网关正常运行
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接, WAP 终端正在使用数据业务;</li> <li>2) 用户关机、关闭浏览器或费用到达门限值</li> </ol>
预期结果: <p>WAP 网关收到 Accounting Request (STOP) 消息, 在 IP—主叫号码对应表中删除相应的对应关系</p>
判定原则: <p>达到以上预期结果则通过</p>

测试编号: 4
测试项目: 缓存经常访问的信息功能
测试目的: 验证 WAP 网关是否具备缓存经常访问的信息的功能
测试配置: 按照图 1 连接设备
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接;</li> <li>2) WAP 终端通过被测网关访问参考 WWW 服务器上的测试网页;</li> <li>3) 重复步骤 2) 共 3 次;</li> <li>4) 观察 WAP 终端是否正常显示该网页;</li> <li>5) 利用 IP 协议分析仪检验从 Web 服务器到网关之间的网络上是否仍出现对该页面的请求命令 (可用网络分析软件代替协议分析仪), 或检查 Web 服务器上应无重复的浏览记录</li> </ol>
预期结果: <p>协议分析仪应该只记录下第一次访问的请求流程, 而没有随后的几次访问请求</p>
判定原则: <p>达到以上预期结果则通过; 如果仍有后几次的请求流程则不通过</p>

测试编号: 5
测试项目: WML 页面编码功能
测试目的: 验证 WAP 网关是否支持 WML 页面编/解码
测试配置: 连接如图 1 所示
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接;</li> <li>2) 通过 WAP1.2 终端访问 WML 测试网页, 该测试页应包括文本格式、WML Script (WML 脚本)、标准 Bitmap 格式、Multipart-Container 格式;</li> <li>3) 观察 WAP 终端是否正常显示所有内容</li> </ol>
预期结果: <p>WAP 终端能够正确显示所要访问的 WML 网页, 没有乱码</p>
判定原则: <p>达到以上预期结果则通过</p>

测试编号: 6
测试项目: XHTML 页面压缩功能
测试目的: 验证 WAP2.0 网关是否支持 XHTML 页面压缩功能
测试配置: 连接如图 1 所示
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接;</li> <li>2) 通过 WAP2.0 终端访问 XHTML 测试网页;</li> <li>3) 观察 WAP2.0 终端是否正常显示该网页的所有内容;</li> <li>4) 通过协议分析仪查看从网关发往终端的测试页内容, 与从 WWW 服务器发往网关的网页内容进行比较, 检查是否经过压缩</li> </ol>
预期结果: <p>WAP2.0 终端能够正确显示所要访问的测试网页, 且通过协议分析仪分析得出网页内容是经过压缩的</p>
判定原则: <p>达到以上预期结果则通过</p>

测试编号: 7
测试项目: 字符集的转换功能
测试目的: 验证 WAP 网关是否支持字符集的转换
测试配置: 连接如图 1 所示
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接;</li> <li>2) WAP 终端配置为仅支持 UTF-8 编码;</li> <li>3) 通过 WAP 终端访问以字符集 GB 2312 编写的 WML/XHTML 测试网页;</li> <li>4) 观察 WAP 终端是否正常显示该网页;</li> <li>5) 通过 WAP 终端访问以字符集 BIG5 编写的网页;</li> <li>6) 观察 WAP 终端是否正常显示该网页;</li> <li>7) 通过 WAP 终端访问以其他字符集 (如 UCS-2) 编写的网页 (可选);</li> <li>8) 观察 WAP 终端是否正常显示该网页</li> </ol>
预期结果: <p>WAP 终端能够正确显示所要访问的测试网页, 没有乱码</p>
判定原则: <p>达到以上预期结果则通过</p>

测试编号: 8
测试项目: HTML 浏览功能
测试目的: 验证 WAP 网关是否支持 WAP 终端浏览 HTML 测试网页
测试配置: 连接如图 1 所示
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接;</li> <li>2) WAP 终端正确配置;</li> <li>3) 从 WAP 终端浏览测试 HTML 网页 (该测试页应包括文本、图片等内容);</li> <li>4) 验证是否正常显示</li> </ol>
预期结果: <p>WAP 终端能够基本正确显示所要访问的 HTML 网页</p>
判定原则: <p>达到以上预期结果则通过</p>

测试编号：9
测试项目：DNS 支持功能
测试目的：验证 WAP 网关系统是否支持 DNS
测试配置：连接如图 1 所示
测试步骤： <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接；</li> <li>2) WAP 终端正确配置；</li> <li>3) 从 WAP 终端输入域名浏览测试 WML/XHTML 网页；</li> <li>4) 验证是否正常显示</li> </ol>
预期结果： <p>WAP 终端能够正确显示所要访问的测试网页，没有乱码</p>
判定原则： <p>达到以上预期结果则通过</p>

测试编号：10
测试项目：存取访问控制功能
测试子项目：网关对到 SP 的访问控制
测试目的：验证 WAP 网关是否实现对到 SP 的存取访问控制功能
测试配置：连接如图 1 所示
测试步骤： <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接；</li> <li>2) 对网关进行允许及禁止访问的 URL 的参数设置；</li> <li>3) 使用 WAP 终端上网，分别访问终端可以访问的测试网页和不允许访问的测试网页；</li> <li>4) 检查 WAP 终端上显示的信息</li> </ol>
预期结果： <p>WAP 终端可以正常显示允许访问的测试网页，不能显示不允许访问的测试网页</p>
判定原则： <p>达到以上预期结果则通过</p>

测试编号: 11
测试项目: 存取访问控制功能
测试子项目: 网关对用户的业务权限控制
测试目的: 验证 WAP 网关是否实现对用户的业务权限控制功能
测试配置: 连接如图 1 所示
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接;</li> <li>2) 网关进行针对用户群的业务允许及禁止权限设置, 例如, 限制用户允许访问的 URL 等;</li> <li>3) 使用限定号码的 WAP 终端上网, 分别访问终端可以使用的业务和不允许使用的业务;</li> <li>4) 检查 WAP 终端上显示的信息</li> </ol>
预期结果: <p>WAP 终端可以正常使用允许使用的业务, 不能使用未允许使用的业务</p>
判定原则: <p>达到以上预期结果则通过</p>

测试编号: 12
测试项目: Cookies 支持功能
测试子项目: Persistent Cookies 功能支持
测试目的: 验证 WAP 网关系统是否支持 Persistent Cookies
测试配置: 连接如图 1 所示
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接;</li> <li>2) WAP2.0 终端正确配置;</li> <li>3) 终端通过 WAP 网关访问包含 Cookies 的页面, 此页面可以显示对于会话是否有 Cookies 存在;</li> <li>4) 中断此次会话, 然后再次访问此页面;</li> <li>5) 页面应显示此 Cookies</li> </ol>
预期结果: <p>WAP 终端能够正确显示 Cookies 内容</p>
判定原则: <p>达到以上预期结果则通过</p>

测试编号: 13
测试项目: Cookies 支持功能
测试子项目: Session Cookies 功能支持
测试目的: 验证 WAP 网关系统是否支持 Session Cookies
测试配置: 连接如图 1 所示
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接;</li> <li>2) WAP2.0 终端正确配置;</li> <li>3) 终端通过 WAP 网关访问包含 Cookies 的页面, 此页面可以显示会话中是否有 Cookies 存在;</li> <li>4) 此时 Cookies 应为空;</li> <li>5) 访问其他页面, 然后再次访问此页面;</li> <li>6) 页面应显示此 Cookies;</li> <li>7) 中断此次会话, 然后再次连接并访问此页面;</li> <li>8) 此时页面应显示 Cookies 为空</li> </ol>
预期结果: <p>WAP 终端能够正确显示 Cookies 内容</p>
判定原则: <p>达到以上预期结果则通过</p>

测试编号: 14
测试项目: 图像功能的支持
测试子项目: 各种图像格式转换功能(可选)
测试目的: 验证 WAP 网关系统是否支持相应的图像格式转换
测试配置: 连接如图 1 所示
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接;</li> <li>2) 使用仅支持 WBMP 或 PNG 的 WAP 终端进行访问;</li> <li>3) 从 WAP2.0 终端输入域名浏览测试 WAP 网页, 页面包含多种图像格式, 如 GIF、JPEG、PNG、BMP 等;</li> <li>4) WAP 网关应将相应的图像格式(GIF、JPEG、PNG、BMP 等)转化为 WBMP 或 PNG;</li> <li>5) 验证图像是否正常显示</li> </ol>
预期结果: <p>WAP 终端能够正确显示图像内容</p>
判定原则: <p>达到以上预期结果则通过</p>

测试编号：15
测试项目：图像功能的支持
测试子项目：彩色图像格式到黑白图像格式的转换功能（可选）
测试目的：验证 WAP 网关系统是否支持彩色图像格式到黑白图像的转换
测试配置：连接如图 1 所示
测试步骤： <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接；</li> <li>2) 使用单色 WAP 终端进行访问；</li> <li>3) 从 WAP2.0 终端输入域名浏览测试 WAP 网页，页面包含多种彩色图像格式，如 GIF、JPEG、PNG、BMP、WBMP 等；</li> <li>4) 验证图像是否正常显示</li> </ol>
预期结果： <p>WAP 终端能够基本正确显示图像内容</p>
判定原则： <p>达到以上预期结果则通过</p>

测试编号：16
测试项目：用户访问日志功能
测试目的：验证 WAP 网关是否可以记录终端访问的相应日志
测试配置：连接如图 1 所示
测试步骤： <ol style="list-style-type: none"> <li>1) 检查 WAP 网关的日志文件，比对本项测试前被测网关的用户访问行为，观察是否准确；</li> <li>2) 日志文件应包括相应的访问信息，如 MSISDN 号码、IP 地址、访问时间、访问的 URL 等</li> </ol>
预期结果： <p>日志内容准确反映用户访问的信息</p>
判定原则： <p>达到以上预期结果则通过</p>

测试编号：17
测试项目：预配置（Provisioning）功能的支持
测试子项目：使用 SMS 的预配置功能
测试目的：检验系统是否支持使用 SMS 的预配置功能
测试配置：连接如图 1 所示；测试终端支持 Provision 功能；测试终端此时未进行网页浏览
测试步骤： <ol style="list-style-type: none"><li>1) 将 WAP 系统正确连接；</li><li>2) 测试终端用户通过拨打客服号码或其他手段触发预配置请求；</li><li>3) 请求触发成功后，在 2min 内，WAP 网关会向该用户下发配置的短消息；</li><li>4) 终端通过收到的消息完成预配置</li></ol>
预期结果： <ol style="list-style-type: none"><li>1) 检查测试终端中相关的配置信息，如短消息中心地址、apn 配置、网关地址等的配置应与运营商要求配置的内容相符；</li><li>2) 使用 Provision 配置后的终端进行短消息发送，可成功发送短消息；</li><li>3) 使用 Provision 配置后的终端进行 Web 页面浏览，可以成功浏览 Web 页面</li></ol>
判定原则： <p>达到以上预期结果则通过</p>



测试编号：18
测试项目：预配置（Provisioning）功能的支持
测试子项目：使用 WSP / HTTP 的预配置功能（可选）
测试目的：验证 WAP 网关是否支持使用 WSP / HTTP 的预配置
测试配置：连接如图 1 所示；测试终端连接上 GPRS 网络，处于在线状态，终端已分配 IP
测试步骤： <ol style="list-style-type: none"><li>1) 终端收到配置更改通知；</li><li>2) 终端向 TPS 发起 WSP / HTTP 请求；</li><li>3) TPS 返回 WSP / HTTP 请求，并携带 Provisioning 内容；</li><li>4) 终端根据收到的 Provisioning 信息进行配置更新</li></ol>
预期结果： <ol style="list-style-type: none"><li>1) 检查测试终端中相关的配置信息，如短消息中心地址、apn 配置、网关地址等的配置应与要求更改的配置内容相符；</li><li>2) 使用 Provision 配置后的终端进行短消息发送，可成功发送短消息；</li><li>3) 使用 Provision 配置后的终端进行 Web 页面浏览，可以成功浏览 Web 页面</li></ol>
判定原则： <p>达到以上预期结果则通过</p>

测试编号: 19
测试项目: 用户代理定制 (UAProfile) 功能的支持
测试子项目: 支持 UAProfile 的终端
测试目的: 验证 WAP 网关是否实现 UAProfile 的支持
测试配置: 连接如图 1 所示
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接;</li> <li>2) 分别使用支持 WAP1.2 和 WAP2.0 UAProfile 的 WAP 终端上网, 向网关发送 UAProfile 信息, 并访问测试网页;</li> <li>3) 查看协议分析仪记录的 HTTP 头中是否包含 URL 和相应的参数 “x-wap-profile” (WAP2.0) 或 UserAgent (设备支持的能力) (WAP1.2) 信息</li> </ol>
预期结果: <p>在 WSP 和 HTTP 两种方式下, 网关发送给网站的信息中应检测到 WAP 终端设备的支持能力</p>
判定原则: <p>达到以上预期结果则通过</p>

测试编号: 20
测试项目: 用户代理定制 (UAProfile) 功能的支持
测试子项目: 不支持 UAProfile 的终端 (可选)
测试目的: 验证 WAP 网关是否实现对不支持 UAProfile 的 WAP 终端的支持
测试配置: 连接如图 1 所示
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接;</li> <li>2) 使用不支持 UAProfile 的 WAP 终端上网, 访问测试网页;</li> <li>3) 检查网关发送给网站的信息中是否包含了 Agent Name, 能够使网站知道 WAP 终端所用的浏览器和终端类型</li> </ol>
预期结果: <p>在网关发送给网站的信息中检测到 Agent Name</p>
判定原则: <p>达到以上预期结果则通过</p>

测试编号: 21
测试项目: HTTP 头信息传送功能
测试目的: 验证 WAP 网关是否能够通过 HTTP 头信息传送 IP/主叫号码及 UAProf 信息
测试配置: 连接如图 1 所示
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接;</li> <li>2) WAP2.0 终端正确配置;</li> <li>3) 终端发送 HTTP 请求给 WAP 网关;</li> <li>4) 在协议分析仪或 WAP 网关的系统日志中可以观察到 WAP 网关发送的 HTTP 请求的头中包含 IP/主叫号码及 UAProf 的 URL</li> </ol>
预期结果: <p>HTTP 头信息中记录的信息准确</p>
判定原则: <p>达到以上预期结果则通过</p>

测试编号: 22
测试项目: 内容转换功能 (XHTML 到 WML1.x 的转换)
测试目的: 验证 WAP 网关是否实现对 XHTML 到 WML 1.1/1.2 转换的支持
测试配置: 连接如图 1 所示
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接;</li> <li>2) 使用不支持 XHTML 的 WAP 终端上网, 访问 WAP 2.0 的 XHTML 测试网页;</li> <li>3) 检查 WAP 终端上是否能正确显示转换后的 WML 网页;</li> <li>4) 使用不同复杂程度的测试网页进行多次测试</li> </ol>
预期结果: <p>WAP 终端对简单的 XHTML 网页应能正确显示, 复杂网页能基本显示主要内容</p>
判定原则: <p>达到以上预期结果则通过</p>

测试编号: 23
测试项目: Push Proxy Gateway 功能
测试子项目: PI 验证功能
测试目的: 验证 WAP 网关是否实现对 PI 验证的支持
测试配置: WAP 网关正常运行
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接;</li> <li>2) 将 PI 的 IP 地址加入允许 / 不允许访问的 PI 行列;</li> <li>3) PI 向手机进行 OTA 的 Push 或 SMS Push;</li> <li>4) 将 PI 的 IP 地址从允许 / 不允许访问行列中删除;</li> <li>5) PI 向手机进行 OTA 的 Push 或 SMS Push;</li> <li>6) 利用协议分析仪跟踪 PI 收到的来自 PPG 的响应消息</li> </ol>
预期结果: <ol style="list-style-type: none"> <li>1) 执行测试步骤 3) 后, PI 应能够 / 不能够向手机 Push 内容;</li> <li>2) 执行测试步骤 5) 后, PI 向手机的 Push 被拒绝 / PI 可以顺利向终端 Push 内容;</li> <li>3) 网关允许的 PI 收到发送成功或失败的回应包 / 网关拒绝的 PI 收到拒绝 Push 的回应包</li> </ol>
判定原则: <p>达到以上预期结果则通过</p>

测试编号: 24
测试项目: Push Proxy Gateway 功能
测试子项目: PAP 接口功能
测试目的: 验证 WAP 网关对 PAP 协议的支持情况
测试配置: WAP 网关正常运行
测试步骤: <ol style="list-style-type: none"> <li>1) PI 提交一条 Push 到终端, 终端收到该 Push;</li> <li>2) PI 提交一条 Push 消息到终端, 在终端未收到消息之前, PI 发起一条取消该 Push 的消息;</li> <li>3) PI 提交一条 Push 消息到终端, 在终端未收到消息之前, PI 发起用另一条 Push 消息的替代;</li> <li>4) PI 提交一条 Push 消息到终端, 在终端未收到消息之前, PI 发起一条对上次 Push 的查询;</li> <li>5) 执行测试步骤 4) 后, 当终端收到 Push 消息后, PI 再次发起对上次 Push 的查询</li> </ol>
预期结果: <ol style="list-style-type: none"> <li>1) 执行测试步骤 1) 后, PI 应收到一条来自 PPG 的结果通知消息;</li> <li>2) 执行测试步骤 2) 后, 终端将收不到来自 PI 的 Push;</li> <li>3) 执行测试步骤 3) 后, 终端将收到替代的 Push 消息;</li> <li>4) 执行测试步骤 4) 后, PI 应获得查询结果, 结果表面终端未收到 Push 的消息;</li> <li>5) 执行测试步骤 5) 后, PI 应获得查询结果, 结果表面终端已收到 Push 的消息</li> </ol>
判定原则: <p>达到以上预期结果则通过</p>

测试编号：25
测试项目：Push Proxy Gateway 功能
测试子项目：SMS Push 功能
测试目的：验证 WAP 网关是否实现使用 SMS 进行 Push 的支持
测试配置：WAP 网关正常运行
测试步骤： <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接；</li> <li>2) 使用网关允许的 PI 发送 PAP 数据到 PPG；</li> <li>3) PAP 数据中分别包含 MSISDN 的用户信息，该用户未上网；</li> <li>4) 检查用户的 WAP 终端是否能收到 Push 信息</li> </ol>
预期结果： <p>用户收到包含 Push 信息的短消息</p>
判定原则： <p>达到以上预期结果则通过</p>

测试编号：26
测试项目：Push Proxy Gateway 功能
测试子项目：多点 Push 功能
测试目的：验证 WAP 网关是否实现多点 Push 的支持
测试配置：WAP 网关正常运行
测试步骤： <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接；</li> <li>2) 使用网关允许的 PI 发送 PAP 数据到 PPG；</li> <li>3) PAP 数据中包含多个用户号码的用户信息；</li> <li>4) 检查用户的 WAP 终端是否能收到 Push 信息</li> </ol>
预期结果： <p>每个用户都收到 Push 信息且内容准确</p>
判定原则： <p>达到以上预期结果则通过</p>

测试编号：27
测试项目：数据安全传输功能
测试子项目：WTLS 功能
测试目的：验证 WAP 网关是否支持 WTLS 协议以保证终端和网关之间的数据安全传输
测试配置： <ol style="list-style-type: none"><li>1) WAP 网关系统运行正常；</li><li>2) 使用支持 WTLS 的测试终端进行测试；</li><li>3) 配置 WAP 网关使其支持 WTLS；</li><li>4) WAP 系统连接如图 1 所示</li></ol>
测试步骤： <ol style="list-style-type: none"><li>1) 将 WAP 系统正确连接；</li><li>2) WAP 终端以安全方式与网关连接，一般应将连接端口设为 9203 或者选择安全连接选项；</li><li>3) WAP 终端通过网关访问具有安全连接的网页</li></ol>
预期结果： <ol style="list-style-type: none"><li>1) 查看协议分析仪，WAP 终端与网关之间有 WTLS 协议的握手交互，例如，Client Hello 等；</li><li>2) 查看协议分析仪，WAP 网关与服务器之间有 TLS / SSL 安全协议握手；</li><li>3) 在终端上应有明显的标记，表明现在的连接是安全连接</li></ol>
判定原则： 达到以上预期结果则通过

测试编号：28
测试项目：数据安全传输功能
测试子项目：SSL 功能
测试目的：验证 WAP 网关是否支持 SSL 协议以保证数据从网关到服务器的安全传输
测试配置： <ol style="list-style-type: none"><li>1) WAP 网关正常运行；</li><li>2) 使用支持 WTLS 的测试终端进行测试；</li><li>3) 配置 WAP 网关使其支持 WTLS 和 SSL；</li><li>4) 使用协议跟踪工具对交互的包进行分析</li></ol>
测试步骤： <ol style="list-style-type: none"><li>1) 将 WAP 系统正确连接；</li><li>2) WAP 终端以安全方式与网关连接，一般应将连接端口设为 9203 或者选择安全连接选项；</li><li>3) WAP 终端通过网关访问具有安全连接的网页；</li><li>4) 利用协议分析仪检查从网关到服务器的数据交互</li></ol>
预期结果： <ol style="list-style-type: none"><li>1) 终端应能够成功登陆到该 SSL 网页；</li><li>2) 从协议工具跟踪到的数据包来看，从网关到服务器之间的安全协议交互正确，且传输数据均是经过加密的；</li><li>3) 登录成功且协议正确</li></ol>
判定原则： 达到以上预期结果则通过

测试编号：29
测试项目：数据安全传输功能
测试子项目：重定向功能
测试目的：验证 WAP 网关是否支持重定向功能以保证数据端到端的安全传输
<p>测试配置：</p> <ol style="list-style-type: none"> <li>1) 需要两台 WAP 网关，一台作为公共主网关，另外一台作为安全域内的附属网关；</li> <li>2) 使用支持重定向功能的测试终端进行测试；</li> <li>3) 源服务器支持安全数据传输时，进行重定向操作；</li> <li>4) 使用协议跟踪工具对交互的包进行分析</li> </ol>
<p>测试步骤：</p> <ol style="list-style-type: none"> <li>1) WAP 终端通过公共 WAP 网关访问源服务器上的安全数据网页，且需要开始进行安全数据传输；</li> <li>2) 重定向开始，WAP 终端转而使用安全域内的附属网关传送数据给需要该安全数据的服务器；</li> <li>3) 安全数据传送完毕后，WAP 终端自动恢复使用公共 WAP 网关传输数据；</li> <li>4) 利用协议分析仪检查从网关到服务器的数据交互</li> </ol>
<p>预期结果：</p> <ol style="list-style-type: none"> <li>1) 终端应能够成功进行重定向工作，且数据传输成功；</li> <li>2) 从协议工具跟踪到的数据包跟踪重定向的协议交互，分析从源服务器返回的 HTTP 300 命令</li> </ol>
<p>判定原则：</p> <p>重定向成功且协议正确则通过；否则不通过</p>



测试编号：30
测试项目：数据安全传输功能
测试子项目：TLS 功能
测试目的：验证 WAP 网关是否支持 TLS 协议以保证数据端到端的安全传输
测试配置： <ol style="list-style-type: none"><li>1) WAP 网关正常运行；</li><li>2) 使用支持 TLS 的测试终端进行测试；</li><li>3) 配置 WAP 网关使其支持 TLS；</li><li>4) 使用协议跟踪工具对交互的包进行分析</li></ol>
测试步骤： <ol style="list-style-type: none"><li>1) 终端向 WAP 网关发起建立到源服务器的 TLS 隧道请求；</li><li>2) WAP 网关帮助终端与源服务器之间建立 TLS 隧道，其后的数据传输均为透明的；</li><li>3) 终端浏览源服务器上的安全信息；</li><li>4) 终端下线，TLS 隧道连接释放；</li><li>5) 利用协议分析仪检查数据交互</li></ol>
预期结果： <ol style="list-style-type: none"><li>1) 在 TLS 连接建立后，终端应能够浏览源服务器上的安全信息；</li><li>2) 从协议工具跟踪到的数据包来看，进出网关的数据包应一样，网关仅起透明传输的作用，且数据包是经过加密的；</li><li>3) 在网关上查看收到的数据包，应无法看到所收到的数据包的内容</li></ol>
判定原则： 达到以上预期结果则通过

测试编号: 31
测试项目: 信息内容过滤功能
测试子项目: 关键字文本过滤功能
测试目的: 验证 WAP 网关是否支持对文本内容的关键字过滤
测试配置: <ol style="list-style-type: none"> <li>1) WAP 网关正常运行;</li> <li>2) WAP 网关的信息内容过滤功能打开;</li> <li>3) 源服务器上的网页内容中加入预定的关键字信息, 包括单字、单词、词组、以及关键字的逻辑组合;</li> <li>4) 被测 WAP 网关内容过滤关键字列表中加入预定的关键字</li> </ol>
测试步骤: <ol style="list-style-type: none"> <li>1) 终端浏览源服务器上的包含关键字文字的网页、其他正常网页、下载包含关键字信息的文件下载其他正常文件;</li> <li>2) 终端下线;</li> <li>3) 在 WAP 网关提供的人机界面上更改关键字内容, 重复以上操作;</li> <li>4) 利用协议分析仪检查数据交互</li> </ol>
预期结果: <ol style="list-style-type: none"> <li>1) WAP 网关可以通过系统配置 / 软开关的方式, 开启信息内容过滤功能;</li> <li>2) 终端无法浏览包含关键字信息的网页;</li> <li>3) 终端可以正常浏览其他不包含关键字信息的网页;</li> <li>4) 终端无法下载包含关键字信息的文件;</li> <li>5) 终端可以正常下载其他不包含关键字信息的文件;</li> <li>6) 从协议工具跟踪到的数据包看, 包含关键字信息的网页内容到达 WAP 网关, 但没有被送给终端;</li> <li>7) WAP 网关应能够记录包含关键字信息的网页域名和 IP 地址;</li> <li>8) WAP 网关能够支持实时更改所过滤的关键字</li> </ol>
判定原则: <p>达到以上预期结果则通过</p>

测试编号：32
测试项目：信息内容过滤功能
测试子项目：图像过滤功能（可选）
测试目的：验证 WAP 网关是否支持对图像内容的过滤功能
测试配置： <ol style="list-style-type: none"><li>1) WAP 网关正常运行；</li><li>2) WAP 网关的信息内容过滤功能打开；</li><li>3) 源服务器上的网页内容中加入预定的图像信息，图像格式应包括 WBMP、JPEG、GIF、动态 GIF 等；</li><li>4) 被测 WAP 网关内容过滤列表中加入预定的过滤图像属性</li></ol>
测试步骤： <ol style="list-style-type: none"><li>1) 终端浏览源服务器上的包含需要过滤的图像的网页、其他正常网页、下载包含需要过滤的图像文件，下载其他正常文件；</li><li>2) 终端下线；</li><li>3) 利用协议分析仪检查数据交互</li></ol>
预期结果： <ol style="list-style-type: none"><li>1) 终端无法浏览包含需要过滤图像的网页；</li><li>2) 终端可以正常浏览其他的网页；</li><li>3) 终端无法下载包含需要过滤的图像文件；</li><li>4) 终端可以正常下载其他不包含过滤信息的文件；</li><li>5) 从协议工具跟踪到的数据包看，包含需要过滤图像的网页内容到达 WAP 网关，但没有被送给终端；</li><li>6) WAP 网关应能够记录包含需要过滤图像的网页域名和 IP 地址</li></ol>
判定原则： 达到以上预期结果则通过

测试编号: 33
测试项目: 网关侧的书签功能(可选)
测试目的: 验证 WAP 网关是否支持网关侧的书签功能
测试配置: WAP 网关正常运行
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接;</li> <li>2) WAP 终端上网, 并在网关设置书签;</li> <li>3) WAP 终端下线;</li> <li>4) WAP 终端上网, 调用刚才设置的书签;</li> <li>5) 相关内容应在终端正确显示</li> </ol>
预期结果: WAP 网关能够存储终端设置的书签, 终端可以正常使用该书签
判定原则: 达到以上预期结果则通过

## 6 业务功能测试

### 6.1 测试环境

WAP网关的业务功能测试结构如图1所示。

### 6.2 测试内容

测试编号: 34
测试项目: 浏览类业务功能
测试子项目: 基于 HTTP 协议栈的浏览业务
测试目的: 验证 WAP 网关是否支持基于 HTTP 协议栈的浏览业务功能
测试配置: 连接如图 1 所示
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 网关系统正确连接;</li> <li>2) WAP2.0 终端正确配置, 使用 HTTP 协议栈;</li> <li>3) 从 WAP2.0 终端浏览 XHTML 测试网页, 记录时间;</li> <li>4) 验证是否正常显示;</li> <li>5) 在 WAP 网关上可以看到有用户接入 WAP 网关, 包括 IP/MSISDN 的对应关系等;</li> <li>6) 在 WAP 网关上观察是否建立 TCP 连接;</li> <li>7) 在网关与终端之间使用协议分析仪, 分析终端和 WAP 网关交互的信息;</li> <li>8) 在协议分析仪上应可以观察到网关与终端之间使用 HTTP 协议进行通信;</li> <li>9) 观察系统日志是否已经记录终端的访问信息</li> </ol>
预期结果: 终端显示内容准确, 协议分析仪中的信令交互流程正确
判定原则: 达到以上预期结果则通过

测试编号：35
测试项目：浏览类业务功能
测试子项目：基于 WSP 协议栈的浏览业务
测试目的：验证 WAP 网关是否支持基于 WSP 协议栈的浏览业务功能
测试配置：连接如图 1 所示
测试步骤： <ol style="list-style-type: none"><li>1) 将 WAP 网关系统正确连接；</li><li>2) WAP1.x 终端正确配置使用 WSP 协议栈，分别使用 9200、9201、9202、9203 共 4 个端口进行连接；</li><li>3) 从 WAP 终端浏览 WAP 网页，记录时间；</li><li>4) 验证是否正常显示；</li><li>5) 在 WAP 网关上可以看到有用户接入 WAP 网关，包括 IP/MSISDN 的对应关系等；</li><li>6) 在网关与终端间使用协议分析仪，分析终端和 WAP 网关交互的信息；</li><li>7) 在协议分析仪上应可以观察到网关与终端之间使用 WSP 协议进行通信；</li><li>8) 观察系统日志是否已经记录终端的访问信息</li></ol>
预期结果： <p>终端显示内容准确，协议分析仪中的信令交互流程正确</p>
判定原则： <p>达到以上预期结果则通过</p>

测试编号: 36
测试项目: 下载类业务功能
测试子项目: 基于 HTTP 的 Java 下载
测试目的: 验证 WAP 网关是否支持基于 HTTP 的 Java 下载功能
测试配置: 连接如图 1 所示; WAP2.0 终端支持 Java 功能, 在下载服务器系统中已经开户; 已经有 SP 在下载服务器系统中发布了 Java 应用
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 网关系统正确连接;</li> <li>2) 从 WAP2.0 终端浏览 Java 应用下载的网页;</li> <li>3) 验证是否正常显示;</li> <li>4) 选择一个 Java 应用, 进行下载;</li> <li>5) 在 WAP 网关上观察是否建立 TCP 连接;</li> <li>6) 在网关与终端间使用协议分析仪, 分析终端和 WAP 网关交互的信息;</li> <li>7) 下载 Java 应用后, 在终端上观察 Java 应用是否可以正常使用</li> </ol>
预期结果 WAP 终端能够正确收到和使用下载的 Java 应用
判定原则: 达到以上预期结果则通过

测试编号: 37
测试项目: 下载类业务功能
测试子项目: 基于 WSP 的 Java 下载
测试目的: 验证 WAP 网关是否支持基于 WSP 的 Java 下载功能
测试配置: 连接如图 1 所示; 测试 WAP1.x 终端支持 Java 功能, 在下载服务器系统中已经开户; 已经有 SP 在下载服务器系统中发布了 Java 应用
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 网关系统正确连接并配置;</li> <li>2) 从 WAP1.x 终端可以浏览 Java 应用下载的网页;</li> <li>3) 验证是否正常显示;</li> <li>4) 选择一个 Java 应用, 进行下载;</li> <li>5) 下载完 Java 应用后, 在终端上观察 Java 应用是否可以正常使用</li> </ol>
预期结果 WAP 终端能够正确收到和使用下载的 Java 应用
判定原则: 达到以上预期结果则通过

测试编号：38
测试项目：下载类业务功能
测试子项目：基于 HTTP 的基本下载业务
测试目的：验证 WAP 网关是否支持基于 HTTP 的基本下载业务
测试配置：连接如图 1 所示
测试步骤： <ol style="list-style-type: none"> <li>1) 将 WAP 网关系统正确连接；</li> <li>2) 从 WAP2.0 终端浏览可以进行下载的网页；</li> <li>3) 验证是否正常显示；</li> <li>4) 选择一个可以下载的内容，如铃声、图片、视频等，进行下载；</li> <li>5) 在网关与终端间使用协议分析仪，分析终端和 WAP 网关交互的信息；</li> <li>6) 下载完相应内容后，在终端上观察下载的内容是否可以正常使用</li> </ol>
预期结果 WAP 终端能够正确收到和使用下载内容
判定原则： 达到以上预期结果则通过

测试编号：39
测试项目：下载类业务功能
测试子项目：基于 WSP 的基本下载业务
测试目的：验证 WAP 网关是否支持基于 WSP 的基本下载业务
测试配置：连接如图 1 所示
测试步骤： <ol style="list-style-type: none"> <li>1) 将 WAP 网关系统正确连接；</li> <li>2) WAP2.0 终端正确配置使用 WSP 协议栈；</li> <li>3) 从 WAP2.0 终端浏览可以进行下载的网页；</li> <li>4) 验证是否正常显示；</li> <li>5) 选择一个可以下载的内容，如铃声、图片、视频等，进行下载；</li> <li>6) 在网关与终端间使用协议分析仪，分析终端和 WAP 网关交互的信息；</li> <li>7) 下载完相应内容后，在终端上观察下载的内容是否可以正常使用</li> </ol>
预期结果 WAP 终端能够正确收到和使用下载内容。
判定原则： 达到以上预期结果则通过

测试编号: 40
测试项目: Push 业务
测试子项目: SI、SL 和 CO 内容类型
测试目的: 验证终端是否支持 SI、SL 和 CO 内容类型
测试配置: 连接如图 1 所示。终端可以是离线状态也可以是连线状态
测试步骤: <ol style="list-style-type: none"> <li>1) PI 向终端发送带有 SI 内容类型的 Push 消息;</li> <li>2) PI 向终端发送带有 SL 内容类型的 Push 消息;</li> <li>3) PI 向终端发送带有 CO 内容类型的 Push 消息;</li> <li>4) 检查终端是否正确收到并显示上述消息;</li> <li>5) 终端应能够访问 SI 页面中的 URL;</li> <li>6) 终端应能够从 SL 页面中的 URL 自动下载服务;</li> <li>7) 终端应能够自动执行 CO 页面中要求的操作 (比如禁用终端中的某项应用)</li> </ol>
预期结果: <ol style="list-style-type: none"> <li>1) 终端浏览器应能够在 Push 消息到达时, 提供声光 / POP 窗口 / 告警图标等方式的提示;</li> <li>2) WAP 终端能够正确收到和显示来自 Push 服务器的信息, 且正确执行相应操作</li> </ol>
判定原则: 达到以上预期结果则通过

测试编号: 41
测试项目: Push 业务
测试子项目: 终端有激活的 IP 连接时的 Push 业务
测试目的: 验证终端是否支持在有激活的数据连接情况下的 Push 业务
测试配置: 连接如图 1 所示。连接建立, 终端已分配 IP
测试步骤: <ol style="list-style-type: none"> <li>1) WAP 系统正确连接;</li> <li>2) Push 应用服务器 (PI) 的用户信息中配置好 WAP 终端的用户信息;</li> <li>3) PI (平台或 SP) 将 PAP 请求发送给 PPG, PPG 查询终端在网关中有激活的连接;</li> <li>4) PPG 将 Push 内容通过 HTTP/WSP Post 发给终端;</li> <li>5) 通过协议分析仪检查 HTTP/WSP 协议流程</li> </ol>
预期结果: WAP 终端能够正确收到和显示来自 Push 服务器的信息, 没有乱码
判定原则: 达到以上预期结果则通过



测试编号：42
测试项目：Push 业务
测试子项目：终端没有使用数据连接时的 Push 业务
测试目的：验证终端是否支持在没有数据连接情况下的 Push 业务
测试配置：连接如图 1 所示。终端没有激活的 IP 连接
测试步骤： <ol style="list-style-type: none"><li>1) PI 将 PAP 请求发送给 PPG，PPG 查询终端在网关中没有激活的连接；</li><li>2) PPG 通过 SMSC 向终端发送 Session Initiate Request 请求；</li><li>3) 终端主动向 SGSN / PDSN 发起一个分组连接请求；</li><li>4) 终端建立到 WAP 网关的连接后，WAP 网关向终端发送 HTTP/WSP Post 命令，传送后续内容</li></ol>
预期结果： WAP 终端能够正确收到和显示来自 Push 服务器的信息，没有乱码
判定原则： 达到以上预期结果则通过

测试编号: 43
测试项目: Push 业务
测试子项目: 基于 SMS 承载的 Push 业务
测试目的: 验证终端是否支持基于 SMS 承载的 Push 业务
测试配置: 连接如图 1 所示。终端没有激活的 IP 连接
测试步骤: <ol style="list-style-type: none"> <li>1) PI 将 PAP 请求发送给 PPG;</li> <li>2) PPG 通过 SMSC 向终端发送 Push 业务的信息;</li> <li>3) 终端接收到 PPG 发来的 Push 内容</li> </ol>
预期结果: <p>WAP 终端能够正确收到和显示来自 Push 服务器的信息, 没有乱码</p>
判定原则: <p>达到以上预期结果则通过</p>

测试编号: 44
测试项目: 电子邮件业务功能
测试目的: 验证 WAP 网关是否能够发送 / 接收 Email
测试配置: 连接如图 1 所示
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接;</li> <li>2) WAP 终端正确配置被测 WAP 网关的 Mail 配置;</li> <li>3) 从 WAP 终端发送 Mail;</li> <li>4) 验证目标账户是否正确收到该 Mail;</li> <li>5) 从服务器端向该 WAP 终端中的账户发送 Mail;</li> <li>6) 验证 WAP 终端是否能正确接收该测试 Mail</li> </ol>
预期结果: <p>目标账户和 WAP 终端均能够正确接收邮件, 没有乱码</p>
判定原则: <p>达到以上预期结果则通过</p>

测试编号：45

测试项目：WTA 业务功能（可选）

测试目的：检查 WAP 网关是否支持 WTA 业务

测试配置：连接如图 2 所示。参考手机必须支持 WTA 功能

测试步骤：

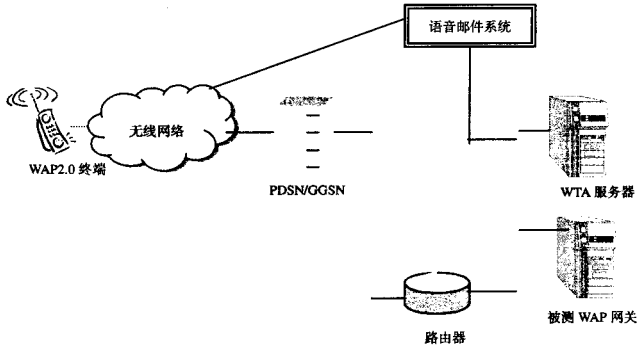


图 2 测试结构示意图

- 1) 通过电话网给 WAP 参考终端的语音邮箱发送一个语音邮件；
- 2) 语音邮件系统应能够定时将邮件标题列表送给 WTA 服务器；
- 3) WTA 服务器通过 WAP 网关将邮件到达通知 Push 给 WAP 参考终端；
- 4) 在终端选择查看邮件；
- 5) WTA 服务器将邮件列表送给终端；
- 6) 在终端中选择接收该语音邮件；
- 7) 语音邮件系统通过无线网络与终端建立语音通道，播放该语音邮件

预期结果：

语音邮件通知能在较短时间内到达参考终端，参考终端选择播放后，该语音邮件能通过移动网络正确在参考手机上播放

判定原则：

达到以上预期结果则通过

测试编号：46
测试项目：基于 WCSS 的浏览业务功能
测试目的：检查 WAP 网关是否支持基于 WCSS 的浏览业务
测试配置： <ol style="list-style-type: none"><li>1) 连接如图 1 所示；</li><li>2) 需要多款 WAP 终端(包括不同输出硬件手机、PDA 等)，且终端浏览器均应支持 WCSS 功能；</li><li>3) Web 服务器支持 WCSS 功能，且存放有适用于各种 WAP 终端类型的 WCSS 页面，和相应的测试 XHTML 的测试网页；</li><li>4) 利用协议分析仪跟踪终端与服务器之间的协议交互</li></ol>
测试步骤： <ol style="list-style-type: none"><li>1) WAP 系统正确连接；</li><li>2) 使用不同类型的 WAP 终端访问 Web 服务器上的相同测试网页；</li><li>3) 利用协议分析仪跟踪终端与服务器之间的协议交互</li></ol>
预期结果： <ol style="list-style-type: none"><li>1) 不同类型的 WAP 终端得到的显示结果应适合其输出硬件的规格；</li><li>2) 在协议分析仪中应能够看到终端浏览器与 Web 服务器之间正确的协议交互，包括对应于相应 CSS 页面的连接标记等</li></ol>
判定原则： 达到以上预期结果则通过

测试编号：47
测试项目：多媒体消息业务功能
测试目的：检查 WAP 网关是否支持多媒体消息业务
测试配置：连接如图 1 所示
测试步骤： <ol style="list-style-type: none"><li>1) 被测终端开机但没有使用数据连接；</li><li>2) 从参考多媒体消息服务器上向该终端发送多条多媒体消息，消息类型应包括：普通文本、图像（彩色&amp;黑白&amp;动态）、声音、影像以及在一条消息中包含多种信息类型的 MMS 等；</li><li>3) 消息应该通过 WAP Push 发送到被测终端；</li><li>4) 查看终端是否能够正确显示刚才发送的各条多媒体消息</li></ol>
预期结果： <p>终端能够正确收到并显示刚才发送的各条多媒体消息</p>
判定原则： <p>达到以上预期结果则通过</p>

## 7 网关性能测试

### 7.1 测试环境

测试结构如图1所示。

应配置一台模拟呼叫发生器，可以按照需求向被测WAP网关发起数据连接请求，并进行性能数据统计。

### 7.2 测试内容

测试编号：48
测试项目：网关的处理能力
测试子项目：网关同时处理的会话数
测试目的：了解网关能同时处理的会话数
测试配置：如图1所示
<p>测试步骤：</p> <ol style="list-style-type: none"> <li>1) 利用测试软件同时（或间隔1s）向WAP网关发起一定数量的（根据被测网关提供的最大能力，以1000个为基础，每次测试增加1000，直到网关的最大能力）连接建立请求（基于WAP2.0协议栈），访问测试网页（可以是若干不同的测试网页，如大、中、小3种类型的网页，以保证参考WWW服务器不成为瓶颈。同时，对于所有厂商，外部测试环境均相同）。</li> <li>2) 检查所有会话是否都能够成功建立并保持（应当由测试软件自动完成检查）。</li> <li>3) 记录测试结果，最大可以支持的会话数</li> </ol>
<p>预期结果：</p> <p>网关应能够在测试进行一定时间（至少15min）之后，与测试软件之间建立并保持一定数量的连接</p>
<p>判定原则：</p> <p>网关能同时处理的会话数应&gt;7000，否则不通过</p>
<p>测试说明：</p> <p>被测试网关系统应以一个节点系统的基本硬件配置作为一个单元进行考量。也就是说，本节的性能指标要求均是针对一个WAP网关节点系统的</p>

测试编号：49
测试项目：网关的处理能力
测试子项目：网关每秒处理的 Transaction 数
测试目的：了解网关每秒处理的 Transaction（终端—网关—CP—网关—终端）数
测试配置：如图 1 所示（WAP 网关关闭 Cache 功能）
<p>测试步骤：</p> <ol style="list-style-type: none"> <li>1) 利用测试软件在 1s 之内，发起若干 URL 请求（根据被测网关提供的最大能力，从小到大，每次增加 100），访问测试网页（可以是若干不同的测试网页，测试网页的大小以 4k 为参考标准，以保证参考 WWW 服务器不成为瓶颈）；</li> <li>2) 检查所有访问是否都能够成功，并正确返回测试网页内容；</li> <li>3) 记录最大值</li> </ol>
<p>预期结果：</p> <p>测试软件发起的所有请求均应成功，并达到网关的最大能力</p>
<p>判定原则：</p> <ol style="list-style-type: none"> <li>1) WAP1.x 网关每秒处理的 Transaction 数应&gt;300，否则不通过；</li> <li>2) WAP2.0 网关每秒处理的 Transaction 数应&gt;600，否则不通过</li> </ol>
<p>测试说明：</p> <p>被测网关系统应以一个节点系统的基本硬件配置作为一个单元进行考量。也就是说，本节性能指标要求均是针对一个 WAP 网关节点系统的</p>

测试编号: 50
测试项目: 可靠性
测试子项目: 长时保持率
测试目的: 检验长时保持率(系统中轻载状况)
测试配置: 如图 1 所示
测试步骤: 1) 利用测试软件同时发起一定数量的用户浏览(网关中轻度负载, 达到网关同时可支持会话数量的 40%), 保持 1h; 2) 检验有多少个浏览仍保持
预期结果: 网关应能够保持绝大多数测试软件发起的用户浏览
判定原则: 长时保持率应>99%, 否则不通过
测试说明: 被测测试网关系统应以一个节点系统的基本硬件配置作为一个单元进行考量。也就是说, 本节的性能指标要求均是针对一个 WAP 网关节点系统的



测试编号：51
测试项目：可靠性
测试子项目：平均掉线率
测试目的：检验系统平均掉线率
测试配置：如图 1 所示
测试步骤： 1) 利用测试软件维持一定数量（网关中轻度负载，达到网关同时可支持会话数量的 40%）的用户浏览，设定每用户在线时长为 5min，下线后，另一个用户再上线，测试保持 24h； 2) 统计平均掉线率
预期结果： 网关能够在测试期间保持性能平稳
判定原则： 平均掉线率应 $<1\%$ ，否则不通过
测试说明： 被测试网关系统应以一个节点系统的基本硬件配置作为一个单元进行考量。也就是说，本节的性能指标要求均是针对一个 WAP 网关节点系统的

测试编号：52
测试项目：网关系统重新启动的时间
测试目的：网关出现故障后，重新启动所需要的时间
测试配置：如图 1 所示
测试步骤： <ol style="list-style-type: none"> <li>1) 将网关重新启动；</li> <li>2) 检验网关重新启动到正常工作的时间</li> </ol>
预期结果： <p>网关应能够在重新启动后正常工作</p>
判定原则： <p>网关系统重新启动的时间应&lt;30min，否则不通过</p>

测试编号：53
测试项目：冗余设备平滑过渡及恢复能力
测试目的：验证 WAP 网关能够进行冗余设备之间的平滑过渡
测试配置：
测试步骤： <ol style="list-style-type: none"> <li>1) 正在工作的某台设备断电或者发生网络故障；</li> <li>2) 检测系统冗余设备（可以是备用设备，也可以是集群设备中的其他设备）是否正常运行；</li> <li>3) 检测已连接的终端会话，用户是否掉线；</li> <li>4) 记录冗余设备的启动时间和业务恢复时间</li> </ol>
预期结果： <ol style="list-style-type: none"> <li>1) 冗余设备正常运行；</li> <li>2) 记录已连接的用户是否掉线、冗余设备启动的时间或者所有业务转移到集群设备中其他设备所需要的时间</li> </ol>
判定原则： <p>达到以上预期结果则通过</p>
测试说明： <p>被测试网关系统应以一个节点系统的基本硬件配置作为一个单元进行考量。也就是说，本节性能指标要求均是针对一个 WAP 网关节点系统的</p>

测试编号：54
测试项目：设备在线平滑扩容能力
测试目的：验证 WAP 网关能够不影响在线业务的情况下进行平滑设备扩容
测试配置：
测试步骤： <ol style="list-style-type: none"><li>1) 增加一个设备节点；</li><li>2) 记录业务是否中断；</li><li>3) 验证设备性能是否提高</li></ol>
预期结果： <p>扩容设备正常运行，不影响在线业务，并且性能有所提高</p>
判定原则： <p>达到以上预期结果则通过</p>
测试说明： <p>被测试网关系统应以一个节点系统的基本硬件配置作为一个单元进行考量。也就是说，本节的性能指标要求均是针对一个 WAP 网关节点系统的</p>

## 8 协议测试

### 8.1 测试环境

本章规定了WAP2.0和WAP1.x 的协议测试方法。测试结构参如图1所示。主要通过协议分析仪进行跟踪。

### 8.2 测试内容

测试编号: 55
测试项目: HTTP1.1 协议
测试子项目: HTTP1.1 保持连接命令
测试目的: 验证 WAP 网关是否支持 HTTP1.1 保持连接命令
测试配置: 连接如图 1 所示
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接;</li> <li>2) 通过 WAP2.0 终端访问 XHTML 测试网页;</li> <li>3) 启动协议跟踪工具对 WAP 网关上 WAP2.0 服务端口进行跟踪</li> </ol>
预期结果: 在 WAP2.0 终端浏览过程中始终保持一个 TCP 连接
判定原则: 达到以上预期结果则通过

测试编号: 56
测试项目: HTTP1.1 协议
测试子项目: HTTP1.1 Get 命令
测试目的: 验证 WAP 网关是否支持 HTTP1.1 Get 命令
测试配置: 连接如图 1 所示
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接;</li> <li>2) 通过 WAP2.0 终端访问 XHTML 测试网页;</li> <li>3) 检查浏览结果;</li> <li>4) 通过协议分析仪查看 HTTP 协议中 Get 命令</li> </ol>
预期结果: WAP2.0 终端正确显示测试网页, 没有乱码, 协议分析仪中记录的 HTTP 的 Get 命令也正确
判定原则: 达到以上预期结果则通过

测试编号: 57
测试项目: HTTP1.1 协议
测试子项目: HTTP1.1 Post 命令
测试目的: 验证 WAP 网关是否支持 HTTP1.1 Post 命令
测试配置: 连接如图 1 所示
测试步骤: <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接;</li> <li>2) 通过 WAP2.0 终端访问 XHTML 测试网页, 通过操作向参考服务器提交一些简单信息 (应使用 Post 命令);</li> <li>3) 检查服务器是否正确接收所提交的信息;</li> <li>4) 通过协议分析仪查看 HTTP 协议中 Post 命令</li> </ol>
预期结果: <p>WAP2.0 终端收到来自服务器提交的确认消息, 服务器正确接收终端提交的信息, 协议分析仪中记录的 HTTP Post 命令也正确</p>
判定原则: <p>达到以上预期结果则通过</p>

测试编号: 58
测试项目: WAP1.2 协议
测试目的: 检查网关支持 WAP 1.2 的所有 100% 必选特性
测试配置: 使用专用 WAP 自动测试软件
测试步骤: <p>使用 WAP 论坛的 Protocol Implementation Conformance System (PICS) J2K 测试组件或同类产品进行本项测试。该系统检查网关支持 WAP 1.2 的所有 100% 必选特性</p>
预期结果: <p>测试软件给出的结果判定 WAP 网关支持 WAP1.2 协议</p>
判定原则: <p>达到以上预期结果则通过</p>

## 9 操作维护及网管功能测试

本章规定了 WAP 网关操作维护及网管功能和协议的测试, 主要包括各种操作维护功能测试、SNMP v2 协议测试、安全管理以及计费管理测试等。

### 9.1 测试结构

WAP 网关网管功能测试结构如图 3 所示。

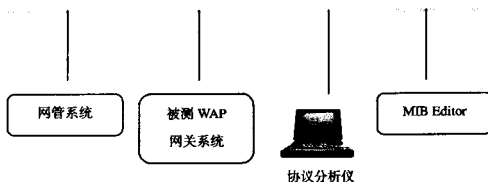


图 3 WAP 网关网管功能测试结构

### 9.2 测试内容

测试编号: 59
测试项目: SNMP 协议测试
测试子项目: Get Request 命令
测试目的: 本测试项目验证 WAP 网关是否支持 SNMP Get Request 命令
测试配置: 连接如图 3 所示
测试步骤: <ol style="list-style-type: none"> <li>1) 使用 MIB Editor 读取系统描述, 应得到正确的系统描述;</li> <li>2) 使用 MIB Editor 读取不存在的对象, 应得到错误状态: 'noSuchName' 以及相应的错误索引;</li> <li>3) 使用 MIB Editor 读取类型为聚合类的对象, 应得到错误状态: 'noSuchName' 以及相应的错误索引;</li> <li>4) 使用 MIB Editor 请求超过范围的 PDU, 应得到错误状态: 'tooBig', 错误索引: '0';</li> <li>5) 在其他原因的错误下应得到错误状态: 'genErr', 错误索引: 对象名索引;</li> <li>6) 使用协议分析仪监视</li> </ol>
预期结果: MIB Editor 读取正确值
判定原则: 达到以上预期结果则通过

测试编号：60
测试项目：SNMP 协议测试
测试子项目：Get Next 命令
测试目的：本测试项目验证 WAP 网关是否支持 SNMP Get Next 命令
测试配置：连接如图 3 所示
测试步骤： <ol style="list-style-type: none"><li>1) 使用 MIB Editor 读取系统描述，应得到正确的系统描述；使用 Get Next 后应得到下一个属性；</li><li>2) 使用 MIB Editor Get Next, 如果 Variable-Bindings 域的对象名不在某 Get 操作可用对象名之前，应得到错误状态：‘noSuchName’ 以及相应的错误索引；</li><li>3) 使用 MIB Editor 请求超过范围的 PDU，应得到错误状态：‘tooBig’，错误索引：‘0’；</li><li>4) 在其他原因的错误下应得到错误状态：‘genErr’，错误索引：对象名索引；</li><li>5) 使用协议分析仪监视</li></ol>
预期结果： MIB Editor 读取正确值
判定原则： 达到以上预期结果则通过

测试编号：61
测试项目：SNMP 协议测试
测试子项目：Get Response 命令
测试目的：本测试项目验证 WAP 网关是否支持 SNMP Get Response 命令
测试配置：连接如图 2 所示
测试步骤： <ol style="list-style-type: none"><li>1) 使用 MIB Editor 读取系统描述，应得到正确的系统描述；</li><li>2) 使用 MIB Editor 读取不存在的对象，应得到错误状态：‘noSuchName’ 以及相应的错误索引；</li><li>3) 使用 MIB Editor 读取类型为聚合类的对象，应得到错误状态：‘noSuchName’ 以及相应的错误索引；</li><li>4) 使用 MIB Editor 请求超过范围的 PDU，应得到错误状态：‘tooBig’，错误索引：‘0’；</li><li>5) 在其他原因的错误下应得到错误状态：‘genErr’，错误索引：对象名索引；</li><li>6) 使用协议分析仪监视</li></ol>
预期结果： MIB Editor 读取正确值
判定原则： 达到以上预期结果则通过



测试编号: 62
测试项目: SNMP 协议测试
测试子项目: Set Request 命令
测试目的: 本测试项目验证 WAP 网关是否支持 SNMP Set Request 命令
测试配置: 连接如图 2 所示
测试步骤: <ol style="list-style-type: none"><li>1) 使用 MIB Editor 设置系统描述, 重新读取;</li><li>2) 使用 MIB Editor 设置不存在的对象, 应得到错误状态: 'noSuchName' 以及相应的错误索引;</li><li>3) 使用 MIB Editor 设置 Variable-Bindings 域的对象名不符合规定, 应得到错误状态: 'badValue' 以及相应的错误索引;</li><li>4) 使用 MIB Editor 请求超过范围的 PDU, 应得到错误状态: 'tooBig', 错误索引: '0';</li><li>5) 在其他原因的错误下应得到错误状态: 'genErr', 错误索引: 对象名索引;</li><li>6) 使用协议分析仪监视</li></ol>
预期结果: MIB Editor 读取正确值
判定原则: 达到以上预期结果则通过

测试编号：63
测试项目：通用 Trap 测试
测试子项目：冷启动
测试目的：本测试项目验证 WAP 网关冷启动时，是否能够按照配置向指定的网管工作站发送 Trap
测试配置：连接如图 2 所示
测试步骤： <ol style="list-style-type: none"> <li>1) 配置 WAP 网关，使其冷启动时能向指定网管工作站发送 Trap；</li> <li>2) 冷启动 WAP 网关；</li> <li>3) 观察网管工作站事件列表；</li> <li>4) 察看协议分析仪数据记录</li> </ol>
预期结果： <p>协议分析仪得到正确消息</p>
判定原则： <p>达到以上预期结果则通过</p>

测试编号：64
测试项目：通用 Trap 测试
测试子项目：热启动
测试目的：本测试项目验证 WAP 网关热启动时，是否能够按照配置向指定的网管工作站发送 Trap
测试配置：连接如图 2 所示
测试步骤： <ol style="list-style-type: none"> <li>1) 配置 WAP 网关，使其热启动时能向指定网管工作站发送 Trap；</li> <li>2) 热启动 WAP 网关；</li> <li>3) 观察网管工作站事件列表；</li> <li>4) 察看协议分析仪数据记录</li> </ol>
预期结果： <p>协议分析仪得到正确消息</p>
判定原则： <p>达到以上预期结果则通过</p>

测试编号: 65
测试项目: 通用 Trap 测试
测试子项目: 链路故障
测试目的: 本测试项目验证系统发生链路故障时, 是否能够按照配置向指定的网管工作站发送 Trap
测试配置: 连接如图 2 所示
测试步骤: <ol style="list-style-type: none"> <li>1) 配置 WAP 网关, 使其链路失败时能向指定网管工作站发送 Trap;</li> <li>2) 制造链路失败故障, 例如, 拔除 WAP 网关的网线;</li> <li>3) 观察网管工作站事件列表;</li> <li>4) 察看协议分析仪数据记录</li> </ol>
预期结果: 协议分析仪得到正确消息
判定原则: 达到以上预期结果则通过

测试编号: 66
测试项目: 通用 Trap 测试
测试子项目: 链路故障恢复
测试目的: 本测试项目验证系统当链路故障恢复时, 是否能够按照配置向指定的网管工作站发送 Trap
测试配置: 连接如图 2 所示
测试步骤: <ol style="list-style-type: none"> <li>1) 配置 WAP 网关, 使其链路恢复时能向指定网管工作站发送 Trap;</li> <li>2) 制造链路失败故障, 例如, 拔除 WAP 网关的网线;</li> <li>3) 恢复链路;</li> <li>4) 观察网管工作站事件列表;</li> <li>5) 察看协议分析仪数据记录</li> </ol>
预期结果: 协议分析仪得到正确消息
判定原则: 达到以上预期结果则通过

测试编号: 67
测试项目: 人机接口, 图形用户界面
测试目的: 检验 WAP 网关的人机接口、图形用户界面的可用性
测试配置: 连接如图 2 所示
测试步骤: <ol style="list-style-type: none"> <li>1) 打开 WAP 网关的操作维护界面;</li> <li>2) 依次检查各个基本操作界面</li> </ol>
预期结果: <p>WAP 网关人机界面能够直观、准确地了解当前系统的状况, 对系统参数进行配置等相应的操作; 能够进行远程操作维护; 对操作员的维护权限应有所区分</p>
判定原则: <p>达到以上预期结果则通过</p>

测试编号: 68
测试项目: 配置管理功能
测试目的: 检验 WAP 网关的配置管理功能
测试配置: 连接如图 2 所示。WAP 网关处于运行状态
测试步骤: <ol style="list-style-type: none"> <li>1) 配置管理数据库, 创建并维护一个数据库, 其中包含网络设备、软件、操作级别、负责维护设备的人员等信息;</li> <li>2) 管理设备的配置文件, 可以访问被管理设备的配置文件, 并可对配置文件进行分析和编辑;</li> <li>3) 对网络节点设备部件、端口的配置;</li> <li>4) 对网络节点设备系统软件的配置;</li> <li>5) 对网络业务配置、网络节点各种数据的初始配置与修改, 网络各种业务政策的配置与管理</li> </ol>
预期结果: <p>配置过程正确</p>
判定原则: <p>达到以上预期结果则通过</p>

测试编号：69
测试项目：故障管理功能
测试目的：检验 WAP 网关的故障管理功能
测试配置：连接如图 2 所示。WAP 网关处于运行状态
测试步骤： <ol style="list-style-type: none"><li>1) 对以下几种信息类型的告警进行触发：设备告警、环境告警、通信告警、服务质量告警等；</li><li>2) 对以下几个级别的告警进行触发：严重告警、重大告警、次要告警、警告告警、已清除的告警及未确定告警；</li><li>3) 对产生的告警进行清除</li></ol>
预期结果： <p>告警服务器能对外发出声光等告警或通过其他方式进行告警，并能反映出相应的异常事件，且可以及时清除告警</p>
判定原则： <p>达到以上预期结果则通过</p>

测试编号：70
测试项目：性能管理功能
测试目的：检验 WAP 网关的性能管理功能
测试配置：连接如图 2 所示
<p>测试步骤：</p> <ol style="list-style-type: none"> <li>1) 通过网管对以下几个性能指标进行查询：网络节点的 CPU 利用率、当前活跃的安全会话、全部会话数量、流量流向统计、非正常终止的终端信息；</li> <li>2) 通过网管对以下几个性能指标进行分析：网络节点设备的故障率、业务流量曲线（包括流量和流向）、日均用户量曲线、非正常终止原因及出现概率、用户平均每次使用时长</li> <li>3) 通过 WAP 网关对以下性能指标进行测试：网关最大传输时延、网关最小传输时延、网管平均传输时延</li> </ol>
<p>预期结果：</p> <ol style="list-style-type: none"> <li>1) 执行测试步骤 1)，可以查询到相关的性能指标；</li> <li>2) 执行测试步骤 2)，可以得到相应的分析数据；</li> <li>3) 执行测试步骤 3)，可以得到相应的测试结果</li> </ol>
<p>判定原则：</p> <p>达到以上预期结果则通过</p>

测试编号：71
测试项目：安全管理功能
测试目的：检验 WAP 网关的安全管理功能
测试配置：连接如图 2 所示
<p>测试步骤：</p> <ol style="list-style-type: none"> <li>1) 使用不同身份的管理者登陆 WAP 网关系统进行管理；</li> <li>2) 检查关键数据的备份情况</li> </ol>
<p>预期结果：</p> <ol style="list-style-type: none"> <li>1) 执行测试步骤 1)，可以发现不同身份的管理者具有不同的权限；</li> <li>2) 执行测试步骤 2)，可以发现关键的数据已经进行了备份</li> </ol>
<p>判定原则：</p> <p>达到以上预期结果则通过</p>

测试编号: 72
测试项目: 原始计费信息记录功能
测试目的: 验证 WAP 网关系统是否支持原始计费信息记录功能
测试配置: 连接如图 1 所示
<p>测试步骤:</p> <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接;</li> <li>2) WAP 终端正确进行配置;</li> <li>3) 从 WAP 终端登录被测 WAP 网关, 并访问参考 WWW 服务器上的测试网页;</li> <li>4) 正常退出浏览, 下线;</li> <li>5) 再次登录网关, 并访问另外的测试网页;</li> <li>6) 直接关机, 非正常退出浏览;</li> <li>7) 更换另外一部可以登录的 WAP 终端, 重复 3) ~6);</li> <li>8) 验证 WAP 系统是否能够提供至少包括以下内容的原始计费信息记录: <ul style="list-style-type: none"> <li>- 主叫号码/用户账号;</li> <li>- 用户 IP 地址;</li> <li>- WAP 网关地址/标识;</li> <li>- 接入方式标识 (CSD 方式/CDMA 方式 / GPRS 方式);</li> <li>- 接入地 NAS/GGSN/PDSN 的 IP 地址;</li> <li>- 所访问的 URL; 访问该 URL 时的信息流量;</li> <li>- 访问该 URL 的开始和结束时间等。</li> </ul> </li> <li>9) 检查 WAP 系统的原始计费信息记录是否正确</li> </ol>
<p>预期结果:</p> <p>设备能够提供内容正确的 CDR, 并可以方便的输出</p>
<p>判定原则:</p> <p>达到以上预期结果则通过</p>

测试编号：73
测试项目：统计功能
测试目的：验证 WAP 网关系统是否支持统计功能
测试配置：连接如图 1 所示
测试步骤： <ol style="list-style-type: none"> <li>1) 将 WAP 系统正确连接；</li> <li>2) 用终端接入访问各种测试页面及 SP 网站；</li> <li>3) 当前会话的统计：对当前会话的流量、访问时间等进行详细统计，对目的站点访问的流量、累计时间进行统计；</li> <li>4) 浏览页面的统计：需要对目的地址的访问流量进行详细的统计，包括地址、累计流量、累计访问时间；</li> <li>5) 用户访问时间、访问流量的统计：根据对会话的数据统计，提取用户的访问量、用户主叫号码、累计时间、累计访问流量等</li> </ol>
预期结果： <p>设备能够提供内容正确的统计信息</p>
判定原则： <p>达到以上预期结果则通过</p>

测试编号：74
测试项目：用户数据管理功能
测试目的：检验 WAP 网关的用户数据管理功能
测试配置：连接如图 2 所示。WAP 网关处于运行状态
测试步骤： <ol style="list-style-type: none"> <li>1) 在 WAP 网关平台上增加测试终端用户，并且配置相关有效信息；</li> <li>2) 通过 WAP 网关平台查询该测试终端用户信息；</li> <li>3) 通过 WAP 网关平台修改该测试终端用户信息；</li> <li>4) 通过 WAP 网关平台删除该测试终端用户信息</li> </ol>
预期结果： <ol style="list-style-type: none"> <li>1) 执行测试步骤 1) 后，该用户可以通过 WAP 网关进行 Web 访问；</li> <li>2) 执行测试步骤 2) 后，可以查询该测试手机的用户信息；</li> <li>3) 执行测试步骤 3) 后，通过相应地访问可以验证手机用户信息已被修改；</li> <li>4) 执行测试步骤 4) 后，此时通过该测试手机进行 Web 访问应被 WAP 网关拒绝</li> </ol>
判定原则： <p>达到以上预期结果则通过</p>



测试编号：75
测试项目：系统事件日志功能
测试目的：检验 WAP 网关是否支持事件日志功能
测试配置：WAP 配置好日志的记录格式、记录方式、存放地点
测试步骤： 1) 检查 WAP 网关的人机界面，检索系统的日志、对日志进行分析（按照时间段）； 2) WAP 网关应能够产生如下日志信息：CDR 文件、事件和系统日志、用户日志等； 3) 对日志的内容进行核对
预期结果： 网关能够产生各种日志，并且内容准确
判定原则： 达到以上预期结果则通过

附录 A  
(规范性附录)  
测试项目总表

测试项目总表见表 A.1。表 A.1 中备注栏的星号 (\*) 表示该测试项仅适用于支持 WAP2.0 协议栈的网关, 其余测试项则适用于支持 WAP1.x 和 / 或 WAP2.0 协议栈的网关。

表 A.1 测试项目总表

编号	测试项目	测试子项目	备注
1	用户识别功能	用户主叫号码认证功能	
2		账号密码认证功能 (可选)	
3		用户下线处理功能	
4	缓存经常访问的信息功能		
5	WML 页面编码功能		
6	XHTML 页面压缩功能		*
7	字符集的转换功能		
8	HTML 浏览功能 (可选)		
9	DNS 支持功能		
10	访问控制功能	网关对 SP 的访问控制功能	
11		用户业务权限控制功能	
12	Cookies 支持功能	Persistent Cookies 功能支持	
13		Session Cookies 功能支持	
14	图像功能的支持	各种图像格式转换功能 (可选)	
15		彩色图像格式到黑白图像格式转换功能 (可选)	
16	用户访问日志功能		
17	预配置功能的支持	使用 SMS 的预配置功能	*
18		使用 WSP / HTTP 的预配置功能 (可选)	*
19	用户代理定制功能的支持	支持 UAProfile 的终端	
20		不支持 UAProfile 的终端 (可选)	
21	HTTP 头信息传送功能		
22	内容转换功能 (XHTML 到 WML1.x 的转换)		*
23	Push Proxy Gateway 功能	PI 验证功能	*
24		PAP 数据分析功能	*
25		SMS Push 功能	
26		多点 Push 功能	*
27		WTLS 功能	
28	数据安全传输功能	SSL 功能	
29		重定向功能	*
30		TLS 功能	*
31	信息内容过滤功能	关键字文本过滤功能	
32		图像过滤功能 (可选)	
33	网关侧的书签功能 (可选)		
34	浏览类业务功能	基于 HTTP 协议栈的浏览业务	*
35		基于 WSP 协议栈的浏览业务	

表 A.1(续)

编号	测试项目	测试子项目	备注
36	下载类业务功能	基于 HTTP 的 Java 下载	*
37		基于 WSP 的 Java 下载	
38		基于 HTTP 的基本下载业务	*
39		基于 WSP 的基本下载业务	
40	Push 业务功能	SI、SL 和 CO 内容类型	*
41		终端有激活的 IP 连接时的 Push 业务	*
42		终端没有使用数据连接时的 Push 业务	*
43		基于 SMS 承载的 Push 业务	
44	电子邮件业务功能		
45	WTA 业务功能(可选)		*
46	基于 WCSS 的浏览业务功能		*
47	多媒体消息业务功能		
48	网关的处理能力	网关同时处理的会话数	
49		网关每秒处理的 Transaction 数	
50	可靠性	长时保持率	
51		平均掉线率	
52	网关系统重新启动的时间		
53	冗余设备平滑过渡及恢复能力		
54	设备在线平滑扩容能力		
55	HTTP1.1 协议	HTTP1.1 保持连接功能	*
56		HTTP1.1 Get 命令	*
57		HTTP1.1 Post 命令	*
58	WAP1.2 协议测试		
59	SNMP 协议测试	Get Request 命令	
60		Get Next 命令	
61		Get Response 命令	
62		Set Request 命令	
63	通用 Trap 测试	冷启动	
64		热启动	
65		链路故障	
66		链路故障恢复	
67	人机接口, 图形用户界面		
68	配置管理功能		
69	故障管理功能		
70	性能管理功能		
71	安全管理功能		
72	原始计费信息记录功能		
73	统计功能		
74	用户数据管理功能		
75	系统事件日志功能		