

YD

中华人民共和国通信行业标准

YD/T 1392-2005

无线应用协议(WAP) 网关设备技术要求

Technical requirements 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	III
1 范围	1
2 规范性引用文件	1
3 定义	2
4 缩略语	2
5 WAP 网关设备在网络中的位置	4
6 WAP 网关功能要求	4
6.1 WAP 网关的基本功能要求	4
6.2 WAP 网关业务功能要求	5
6.3 WAP 网关接口要求	5
6.4 WAP 网关预配置 (Provisioning) 功能要求	5
6.5 WAP 网关认证与授权功能要求	6
6.6 WAP 网关计费功能要求	6
6.7 WAP 网关的业务管理功能	6
6.8 WAP 网关安全要求	7
7 WAP 网关协议要求	9
7.1 WAP1.x 网关协议栈要求	9
7.2 WAP2.0 代理 / 网关协议栈要求	13
8 Push 功能要求	16
8.1 Push 总体要求	16
8.2 Push 代理网关 (PPG) 功能要求	17
8.3 PAP 协议要求	17
8.4 OTA 协议要求	18
8.5 Push 的媒体类型	18
9 UAPProf 功能要求	18
9.1 UAPProf 的结构描述	18
9.2 UAPProf 对 Pull 网关要求	19
9.3 UAPProf 对 Push 网关的要求	20
9.4 UAPProf 服务器的要求	20
10 支持 WTA 的网关要求 (可选)	21
10.1 WTA 框架	21
10.2 WTA 功能实现对 WAP 网关的要求	22
10.3 WTA 服务器的要求	22

11	WAP 网关的性能要求	22
11.1	单机处理能力	22
11.2	WAP 网关处理最大时延	22
11.3	可靠性指标	22
11.4	可扩展性	23
12	WAP 设备操作维护及网管技术要求	23
12.1	网络管理方式	23
12.2	网络管理对象	23
12.3	网管接口协议	23
12.4	网管接口信息模型	23
12.5	网管功能	23
13	环境要求	24
13.1	工作环境要求	24
13.2	防电磁干扰要求	25
13.3	WAP 网关抗电磁干扰的能力	25
14	电源与接地	26
14.1	电源要求	26
14.2	WAP 网关接地要求	26
15	例行试验	26
15.1	低温试验	26
15.2	高温试验	26
15.3	恒定湿热试验	26
15.4	运输试验	26
15.5	贮存要求	26
15.6	标志、包装、运输	26
附录 A (规范性附录)	WAE2.0 支持的媒体类型	28
附录 B (资料性附录)	UAProf CPI 信息格式	30

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）网关设备测试方法》配套使用。

本标准与 WAP 论坛制定的 WAP2.0 系列标准的技术内容保持一致，但考虑到我国无线和数据网络的实际情况，仅对我国目前拥有的以及今后有可能发展的 2G、2.5G 以及 3G 无线技术作出规定，而对一些可能基本上在我国没有或很少应用的技术，则未作具体规定。随着 WAP2.0 系列标准的不断完善，本标准应作相应的更新或补充。

本标准的附录 A 是规范性附录，附录 B 是资料性附录。

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：信息产业部电信研究院
中兴通讯股份有限公司
华为技术有限公司

本标准起草人：谢 玮 孙元宁 刘 治

无线应用协议 (WAP) 网关设备总技术要求

1 范围

本标准规定了WAP网关设备的定义和术语、设备构成、功能、技术指标、业务、环境条件、设备系列及设备的兼容性。

本标准适用于WAP网关设备。

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。

GB/T 191-2000	包装储运图示标志
GB/T 2423.1-2001	电工电子产品基本环境试验规程 第2部分 试验方法 试验A: 低温
GB/T 2423.2-2001	电工电子产品基本环境试验规程第2部分 试验方法 试验B: 高温
GB/T 2423.9-2001	电工电子产品环境试验 第2部分: 试验方法 试验 Cb: 设备用恒定湿热
GB/T 3873-1983	通信设备产品包装通用技术条件
YD/T 1045-2000	网络接入服务器 (NAS) 技术规范
IETF RFC 758 (1979)	号码分配
IETF RFC 791 (1981)	因特网协议
IETF RFC 792 (1981)	Internet控制消息协议
IETF RFC 793 (1981)	传输控制协议
IETF RFC 821 (1982)	简单邮件传输协议
IETF RFC 1112 (1989)	对于IP多点传送的主机扩展名
IETF RFC 1213 (1991)	基于TCP/IP的互连网的网络管理的管理信息库: MIB-II
IETF RFC 1229 (1991)	一般接口MIB的扩展
IETF RFC 1398 (1993)	以太网类接口类型管理目标的定义
IETF RFC 1725 (1994)	邮局协议V3
IETF RFC 1951 (1996)	简化压缩数据格式规范V1.3
IETF RFC 1952 (1996)	GZIP文件格式规范V4.3
IETF RFC 2045 (1996)	多目标Internet邮件扩展 第一部分: Internet消息主体 格式
IETF RFC 2046 (1996)	多目标Internet邮件扩展 第二部分: 媒体类型

IETF RFC 2047 (1996)	多目标Internet邮件扩展第三部分: 非ASCII文本消息头的扩展
IETF RFC 2048 (1996)	多目标Internet邮件扩展第四部分: 注册过程
IETF RFC 2049 (1996)	多目标Internet邮件扩展第五部分: 一致性标准和样板
IETF RFC 2138 (1997)	RADIUS协议
IETF RFC 2139 (1997)	RADIUS计费协议
IETF RFC 2211 (1997)	可控负载网络元素业务的规范
IETF RFC 2581 (1999)	TCP拥塞控制
IETF RFC 2616 (1999)	超文本传输协议—HTTP/1.1
IETF RFC 2817 (2000)	HTTP/1.1中TLS的升级
IETF RFC 3023 (2001)	可扩展标记语言媒体类型
WAP-182-ProvArch-20010314-a	预配置结构描述
WAP-183-ProvCont-20010724-a	预备内容类型
WAP-187-TransportE2ESec-20010628-a	传输端到端安全
WAP-191-WML-20000219-a	无线标记语言
WAP-202-WCMP-20010624-a	无线控制消息协议
WAP-210-WAPArch-20010712-a	WAP结构描述
WAP-224-WTP-20010710-a	无线事务协议
WAP-225-TCP-20010331-a	无线优化TCP规范
WAP-229-HTTP-20010329-a	无线优化HTTP规范
WAP-230-WSP-20010705-a	无线会话协议
WAP-235-PushOTA-20010425-a	Push空中传输协议
WAP-236-WAESpec-20020207-a	无线应用环境规范
WAP-247-PAP-20010429-a	Push接入协议
WAP-248-UAPProf-20010530-p	用户代理特征
WAP-249-PPGService-20010713-a	Push代理网关服务
WAP-250-PushArchOverview-20010703-p	Push结构描述
WAP-259-WDP-20010614-a	无线数据报协议
WAP-261-WTLS-20010406-a	无线传输层安全
WAP-266-WTA-20010711-p	无线电话应用

3 定义

本标准采用下列定义。

WAP业务: 专门为无线终端用户提供的Internet应用服务。

WAP网关: WAP业务接入设备, 位于移动终端与Internet应用服务器之间, 为用户提供WAP业务。

4 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
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
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
XHTML	Extensible Hyper Text Markup Language	扩展超文本标记语言

5 WAP 网关设备在网络中的位置

WAP业务通常由以下几方面的设备合作实现：WAP终端、无线传输网络（GSM CSD / GSM GPRS/CDMA / WCDMA / CDMA2000 / TD-SCDMA等）、WAP网关设备、WAP应用服务器、防火墙等。

WAP网关设备可以分为若干功能模块：WAP Pull代理、WAP Push代理、WTA服务器、WAP支持服务器、操作与维护平台（O&M）等。WAP网关设备在网络中的位置如图1所示，其功能模块的组成如图2所示。

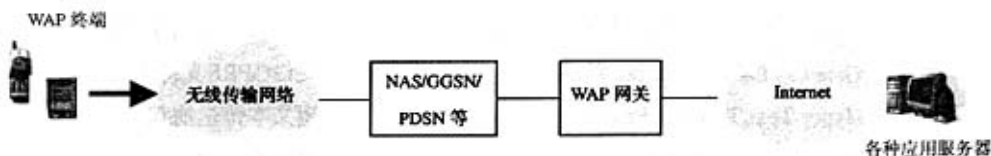


图1 WAP 网关设备在网络中的位置

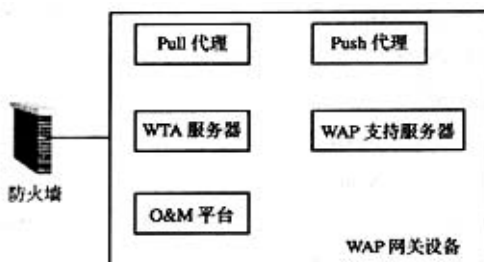


图2 WAP 网关设备的功能模块

图2中Pull代理和Push代理是实现WAP基本业务的重要功能模块。

WAP支持服务器能够为终端设备、代理以及应用提供服务。目前WAP系统至少应提供以下3种类型的支持服务器：

- PKI入口：允许终端设备开始一个新的公共密钥证书的创作；
- UAProf服务器：允许应用程序获取客户机能力、用户代理和独立用户的个人定制值（参见9.4节）；
- 预配置服务器（Provisioning Server）：WAP终端设备可信赖的、能够提供其预配置信息的服务器（参见6.4.2节）。

WTA服务器是实现WTA（无线电话应用）业务的重要设备，WTA用户代理使用URL指向WTA服务器的内容。URL指向WTA服务器上的应用来创建和移动网络实体（例如，智能网节点或话音邮件系统）互通的业务（参见10.3节）。

本标准对WAP网关设备的功能进行了明确规定。对其他设备如防火墙、WAP终端等设备的要求在本标准范围之外。

6 WAP 网关¹功能要求

6.1 WAP 网关的基本功能要求

本章规定了WAP1.x网关和WAP2.0代理/网关均应具有的功能要求。对某类网关的单独要求见标注。WAP网关应实现以下基本功能。

¹ 本章中规范了WAP网关的各种功能要求，某些需要详细描述的功能如Push、UAProf、WTA等可参见下面章节。

1) 协议网关: 协议网关功能将来自无线协议栈的请求 (如 WSP、WTP、WTLS、WDP、无线优化 HTTP、无线优化 TCP 等) 翻译成 WWW 协议栈 (如 HTTP、SSL 和 TCP/IP), 协议网关还应该能够支持 DNS 查找功能;

2) 内容编/解码器: 内容编码器将 Web 内容翻译成压缩编码的格式, 以减少通过无线数据网络传输的数据分组的大小和数量;

3) 用户代理特征值管理: 用户代理特征值描述了终端能力和用户代理定制 (UAProf), WAP 网关应能管理并为各种应用提供这些信息, WAP 网关还应支持用户信息 (如 MSISDN、IP 地址等) 转发等功能;

4) 高速缓存代理: 高速缓存代理可以通过保持经常访问资源的高速缓存, 以提高性能和网络效率。

6.2 WAP 网关业务功能要求

WAP 网关应能够至少支持以下几种基本业务功能:

- 浏览业务, 基于 WML 和 XHTML 页面的浏览是必备的, 而基于 HTML 页面的浏览是可选的;
- Push 业务, WAP 网关系统应支持从服务器发起的 Push 业务;
- 邮件业务, WAP 网关系统至少应支持 POP3、SMTP、IMAP 等用于电子邮件的协议中的一种;
- 多媒体消息 (MMS) 业务, WAP 网关系统必须支持多媒体消息业务对网关的要求;
- 无线电话应用 (WTA) 业务, WAP 网关应支持 WTA 业务对网关的要求 (可选);
- 基于 WCSS 开发的业务, WAP 网关应支持基于 WCSS 开发的各种应用对网关的要求;
- WAP 网关应支持 KJava 应用、书签 (可选)、Cookie 等业务功能;

6.3 WAP 网关接口要求

WAP 网关与无线网络的连接由无线网中的网关设备 (如接入服务器、GGSN、SMC 等) 完成, 与因特网的连接通过防火墙完成。

6.3.1 WAP 网关物理接口要求

WAP 网关可以通过下列以太网接口连接到局域网:

- 10Mbit/s 以太网接口 (符合 IEEE 802.3);
- 100Mbit/s 快速以太网接口 (符合 IEEE 802.3u);
- 千兆以太网接口 (符合 IEEE 802.3ab)。

6.4 WAP 网关预配置 (Provisioning) 功能要求²

6.4.1 总体要求

应符合 WAP2.0 规范要求 (WAP-182-ProvArch)。

要求 Bootstrap 和 Continuous Provisioning 机制相互分离。Bootstrap Provisioning 提供给用户足够的 TPS (可信赖预配置服务器) 配置信息, Continuous Provisioning 用于配置信息的更新。

Bootstrap Provisioning 的方式应符合运营商相应要求。

要求支持用户请求的 Continuous Provisioning 和网络侧发起的 Continuous Provisioning, 以更新配置信息。

6.4.2 TPS (可信赖预配置服务器) 技术要求

6.4.2.1 预配置内容类型

² 本节要求仅适用于 WAP2.0 网关。

应符合WAP2.0规范要求（WAP-183-ProvCont）。

要求支持WBXML。

要求支持预配置内容的文本形式和二进制形式之间的转化和编解码。

6.4.2.2 安全要求

TPS与客户端之间应建立相应的安全机制。安全机制的建立可以在Bootstrap Provisioning过程中完成。

采用的安全策略应符合运营商的相应要求。

6.5 WAP 网关认证与授权功能要求

WAP业务的认证可以分为3个层次：

- WAP 终端在无线承载网络上的鉴权；
- 接入认证（在 GSM CSD 方式下由接入服务器实现，GSM GPRS 方式下由 GGSN 实现，CDMA 分组数据方式下由 PDSN 实现，一般使用 RADIUS 协议）；
- 网关认证。

本标准仅规定在网关的认证要求。

WAP网系统应支持对来访的用户进行身份认证，以防止非授权用户的使用，并根据认证结果授权用户使用WAP业务，并启动计费服务器。WAP网系统应支持IP地址限制功能，即可以限制公网上任何用户地址的访问。WAP网关应支持以下两种认证方式：

- 主叫号码认证方式；
- 用户名+密码认证方式。

6.6 WAP 网关计费功能要求

WAP网关应支持产生原始计费信息的功能。

WAP网关产生的原始计费信息中应至少包括：

- 主叫号码/用户账号；
- 用户 WAP 访问接入 NAS 的 IP 地址 / GGSN 或 PDSN 的 IP 地址；
- 用户 IP 地址；
- WAP 网关地址/标识；
- 接入方式标识（GSM CSD 方式/GSM GPRS 方式/CDMA 方式），同时 WAP 网关应该具有向外部网元送出用户 WAP 访问的承载方式的功能；
- 所访问的 URL；
- 访问该 URL 时的信息流量；
- 访问该 URL 的开始和结束时间等。

WAP网关必须支持按主叫号码和按用户账号统计用户计费信息的两种不同方式，并能够将计费信息送往计费中心生成账单。

WAP网关的计费精度应为流量精确到1k字节；时间精确到1s。

6.7 WAP 网关的业务管理功能

WAP网关的业务管理功能可以在WAP网关上实现，也可以独立在操作与维护终端上实现。应允许用户利用WAP终端在线登录。业务管理必须至少提供下列功能：

- 用户管理功能，包括新建、删除、更改和显示用户；

- 提供各种事件的记录（包括系统事件、WAP 事务事件和用户行为事件等）；
- 提供各种业务限制功能（包括业务访问限制和用户接入限制等）。

WAP 网关应当提供两种界面：

- 友好的人机界面，例如，基于 WWW 的界面；
- 客户管理界面 Customer Administrator Interface (CAI)。

WAP 网关必须提供二次开发接口。

WAP 网关需要具有业务相关信息的统计功能，包括能够对用户统计、访问站点相关信息功能。

6.8 WAP 网关安全要求

6.8.1 WAP 网关信息内容安全要求

WAP 网关必须提供信息内容过滤功能。

WAP 网关应能够通过软件或者硬件方式对所传送的未加密信息实现信息过滤功能，被过滤的信息类型应包括文字、图片（可选）等。过滤的文本关键字信息应能够做到：1）可以实时更新；2）支持关键字的逻辑组合（例如，支持正则表达式）。

WAP 网关所提供的信息内容过滤功能应能够通过系统配置 / 软件开关等方式来决定是否启用。

6.8.2 WAP 网关自身安全

WAP 网关的安全主要包括以下几大部分：

- 物理设备安全；
- 内容数据传送的安全性和可靠性；
- 系统管理或用户数据传送的安全性和可靠性；
- 系统数据保存的安全性和可靠性。

WAP 网关的物理设备安全主要是指关键设备或部件必须采用冗余设计。

内容数据的传送指从 WAP 终端到应用服务器之间的信息传送。在 WAP1.x 协议中，它的安全保障可以分段实现：WAP 终端到 WAP 网关使用 WTLS 协议，WAP 网关到应用服务器采用 SSL 协议。WAP 网关支持 WTLS 到 SSL 的协议转换。WAP2.0 网关产品应能够支持端到端数据传送安全解决方案。

系统管理或用户数据传送安全主要指 WAP 网关系统与其他网络设备（如网管系统、认证/计费系统等）通信时的数据安全，通常可以采用完整性校验、数据加密等方式来保证。

WAP 网关系统应能提供多重安全保护机制，以保证系统数据的安全保存，比如，利用防火墙防止来自网络的侵袭；建立合理的操作维护安全策略（包括用户验证、操作/访问权限设定、系统数据加密等）。

6.8.3 WAP 网关对传输端到端安全要求

要实现真正的传输端到端安全，WAP 网关就必须支持重定向功能。

图3给出了WAP业务真正的传输端到端安全结构。图3中的各元素均为功能模块，某些功能可以在一个物理实体中实现。图4给出了WAP业务传输端到端安全的典型流程。

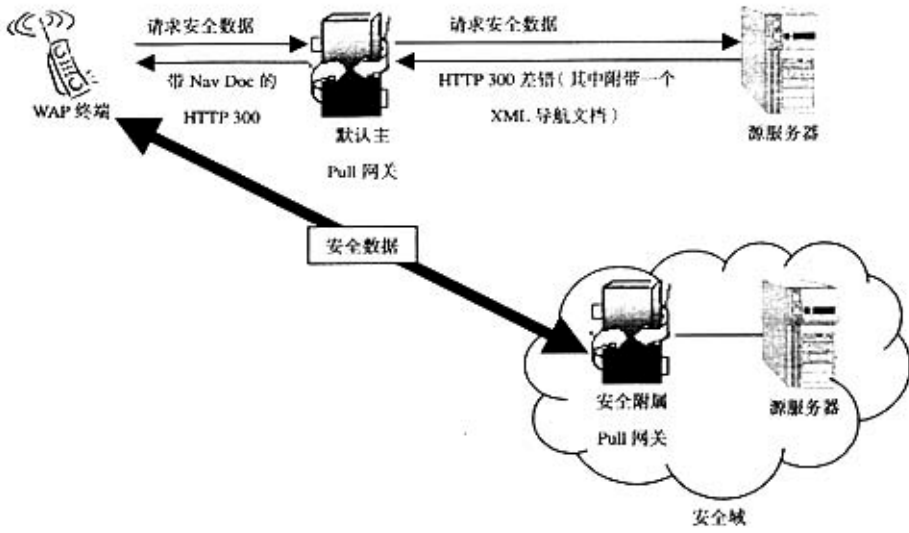


图3 WAP 业务传输端到端安全的结构

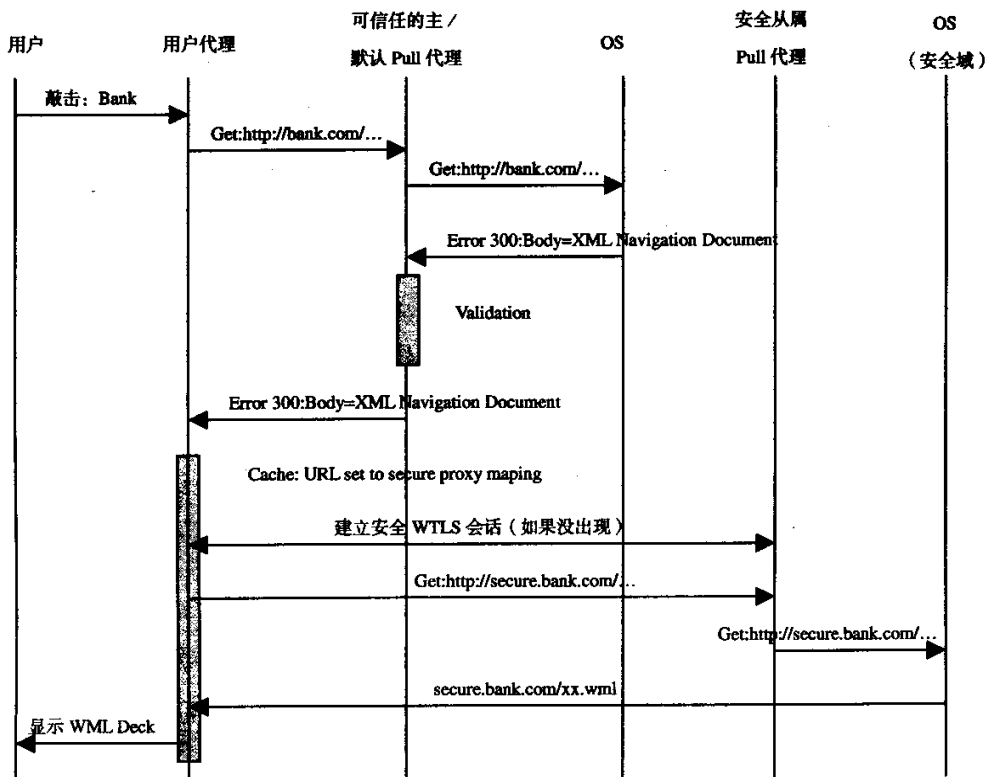


图4 传输端到端安全流程

WAP端到端安全解决方案的原理是“重定向”。

— 当 WAP 终端发出需要安全数据传送（例如，账号密码等）的 URL 请求后，默认主 WAP 网关透

明传送给源服务器。

— 源服务器以 HTTP 状态 300 重定向消息响应，其中附带了一个 XML 导航文档（Navigation Document）。

— 默认主 WAP 网关收到差错响应后，开始对导航文档进行有效性分析（包括导航文档的内容格式以及重定向的源），以确定其包含与在该文档中规定的策略以及主 WAP 网关本身策略一致的有效参数。

— 然后主 WAP 网关使用一个 HTTP300 响应将有效的导航文档发到 WAP 终端的用户代理上。

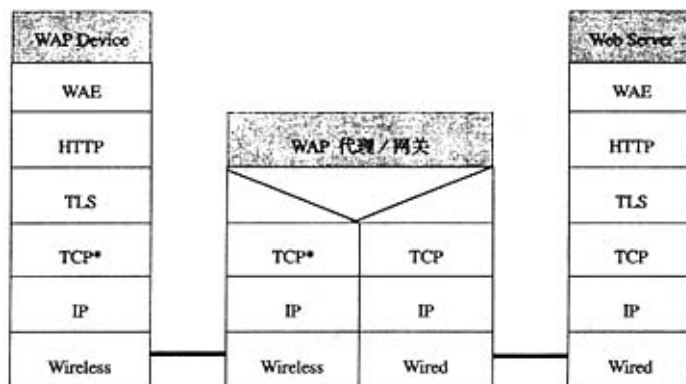
— WAP 终端通过 Nav Doc 中的信息得到与安全 WAP 源服务器相关联的安全附属 WAP 网关的 IP 地址。

— 用户代理将与所选择的安全附属 WAP 网关建立一个 WTLS 会话。

— 随后的端到端安全数据传送便直接通过安全附属 WAP 网关在 WAP 终端和安全 WAP 源服务器之间进行。

— 当安全数据传送完成后，WAP 终端仍将利用主 WAP 网关访问服务器。

除了利用重定向的方式做到用户数据传送的端到端安全以外，在 WAP2.0 协议中，可以将 WAP 代理按图 5 进行配置，以满足用户数据端到端的安全传送。



注：TCP*为无线优化的TCP协议。

图5 使用 TCP*的 WAP 代理

图5中终端与Web服务器建立了一个面向连接的隧道。使用这种配置是为了允许TLS在移动终端和源服务器之间提供端到端的安全。

7 WAP 网关协议要求

7.1 WAP1.x 网关协议栈要求

WAP结构采用分层设计的协议栈，如图6所示。每一层均提供一组功能或服务，通过定义好的接口以用于其他服务或应用。WAP网关将移动终端上的WAP协议与因特网中承载于TCP/IP上的HTTP相互映射。WAP网关首先将用户的请求内容翻译成HTTP请求，然后通过URL寻址到HTTP服务器，最终将取得的内容转换成WML Deck返回给移动用户。

WTP与WTLS在使用时可选，它们的使用与否取决于移动用户的请求（WDP层的端口号）。



图6 WAP1.x 网关协议栈

7.1.1 无线应用框架 (WAE)

无线应用框架位于因特网协议栈和WAP协议栈之上。在移动客户侧，WAE层作为服务器；在因特网侧，WAE层作为客户。该层协议将WSP请求/应答与HTTP请求/应答相互转换。

在WAE层必须实现下列功能：

- 实现 WAP 终端用户在 WAP 网关的认证。
- 缓存频繁地使用 WML Deck。
- 编/解码
 - 将Web页面压缩编码，使之更适合于无线网络环境传送；
 - 将HTTP头压缩编码，使之更适合于无线网络环境传送；
 - 将WML脚本、标准Bitmap格式、Multipart-container格式、Vcard和Vcalendar格式进行编/解码。
- 字符代码转换。
 - HTML与WML转换（可选）；
 - 支持汉字编码及转换功能（内部字符集支持UTF-8，并可将GB 2312、UCS-2、BIG5转换为UTF-8）。
- 添加或删除静态会话头。

7.1.2 无线会话协议 (WSP)

WAP网关应支持WSP协议。

WSP协议应具有以下基本特性：

- 建立一个从客户（WAP 终端）到服务器的可靠会话，并释放该会话；
- 允许会话能力协商（包括会话服务的具体功能、协议参数、内容头的编码页等）；
- 使用压缩编码在客户与服务器之间交换内容；
- 挂起、恢复一个会话。

除去以上基本特性，WSP还应具备以下扩展特性：

- 支持 HTTP/1.1 功能
 - 可扩展的请求—应答方法；
 - 对象聚合（Composite Objects）；
 - 内容类型协商；

- 交换客户和服务器会话头；
- 中途打断正在进行的事务；
- 以非同步方式将内容从服务器推（Push）给客户；
- 协商支持多个、同时的异步事务。

WSP的核心功能即以二进制方式实现HTTP，并同时提供推（Push）和拉（Pull）两种数据传输服务。推（Pull）服务是利用HTTP/1.1的请求/响应机制实现的。WSP提供3种Push机制以用于数据传输：

- 在已存在的会话上下文中，带确认的数据推送（Push）；
- 在已存在的会话上下文中，不带确认的数据推送（Push）；
- 不带确认的数据推送（Push），且没有已存在的会话上下文。³

7.1.3 无线事务协议（WTP）

WAP网关应支持WTP协议。

WTP定义在无线数据报协议（WDP）和可选的安全服务（WTLS）之上，是一个轻量级的面向事务⁴的协议，能在无线数据网络中有效运行。

WTP是为WSP面向连接的业务提供数据传送服务，主要完成事务的处理、消息的重传和确认、重复消息的删除、分段和重组等。由于WTP是利用重传和确认机制保证数据报服务的可靠性，因此不需要明显地建立连接、终止连接的过程，提高了面向连接服务的效率。

WTP协议应具有以下基本特性：

— WTP应实现3种不同事务类别：类别0、类别1和类别2。

● 类别0：不可靠的消息传输，无结果消息。也就是不可靠地单向数据报服务。通常它用在不可靠的Push业务中。该事务只有一个动作，即发起者发送请求消息。它不是发送数据报的主要手段。如果应用程序需要发送大量的数据报，应使用WDP。

● 类别1：可靠的消息传输，无结果消息。它主要用于可靠的Push业务中。它与类别0的区别在于，发起者发送请求消息后，响应者会确认该消息。

● 类别2：可靠的消息传输，无结果消息。它提供基本的请求/回事务服务。一个WSP会话可能包含多个该服务类的事务。实际上它是一个二次握手过程，即发起者发送请求，响应者对该请求发结果确认，发起者发送结果确认的确认。

— 可靠性通过惟一的事务标识、确认、重传及删除重复消息获得。

— 没有明显地连接建立或拆除阶段。

— 用户到用户可靠性支持，即WTP用户确认每一个接收的消息（可选）。

— 事务的最后确认可以包含与本事务有关的带外信息。例如，性能测量（可选）。

— 在适合的情况下可以使用串联的方式，在数据报传输的一个服务数据单元（Service Data Unit）中运送多个协议数据单元（Protocol Data Units）。

— 面向消息。交换的基本单元是一个完整的消息而不是字节流。

— 协议提供机制以保证最小化被重传事务的数量。

— 支持显式的事务退出，包括冲掉客户端和服务器中的未发送的数据。该退出可以由用户取消一个其请求的服务来触发。

³ 通常用于在不可靠的传输通路上发送单向消息。

⁴ 事务：在一个浏览会话中，客户向服务器请求信息，然后服务器返回信息给客户。一个请求/回应对被描述成一个事务。

— 为了可靠地调用消息，无论成功或失败都有相应报告。如果一个调用未被响应者处理，应返回给初始者一个异常中断消息。

— 协议允许异步事务。如果数据有效，响应者应返回结果。

7.1.4 无线传输层安全性 (WTLS)

网关应支持WTLS协议。

WTLS的主要功能应包括：保证数据传输一致性、数据传输保密性、提供鉴权机制、丢弃未经证实的数据和加密运算等。

WTLS定义3种类别，下列功能必须由不同类别提供：

— 1类服务能使用交换的公共密钥建立安全传输，使用对称算法加密、解密数据，使用消息授权编码算法、协商算法和安全性参数检查数据完整性。

— 2类服务除完成1类服务的功能外，能交换服务器确认（服务器确认用于对服务器授权）。

— 3类服务除完成2类服务的功能外，能交换客户确认（客户确认用于对客户授权）。

表1给出了3种WTLS类别所提供的具体功能特性。

表1 WTLS类别

功能特性	1类	2类	3类
公共密钥交换	M	M	M
服务器证书	O	M	M
客户证书	O	O	M
Shared-secret握手	O	O	O
压缩	—	O	O
加密	M	M	M
MAC	M	M	M
智能卡界面	—	O	O

注：M 表示该参数是必备的；O 表示该参数是用户可选的。

安全的WTLS连接必须在对等双方握手时进行协商。在握手过程中协商各种参数并交换公共密钥信息。WTLS可以提供完全或简略握手两种不同类型的握手过程。

要求安全层必须至少支持密钥交换算法（Diffie-Hellman、RSA、ECDH等），批量加密算法（包括DES、RC5、IDEA等）和MAC（消息验证码）算法（包括SHA、MD5等）。

7.1.5 无线数据报协议 (WDP)

WAP网关应支持WDP协议。

无线数据报协议具有运行于不同网络类型支持的数据承载能力。WDP是一般数据报服务，使用下层承载能力为上层提供一致的服务。

WDP为上层协议提供通用接口，使上层协议可以与下层承载网络无关。WDP使传输层适配到指定的下层承载网络中。

WDP必须支持：

— 基于IP的承载网络，如GSM的CSD、GSM的GPRS、CDMA等；

— GSM的SMS、CDMA的SMS。

其他下层承载网络WDP均可选支持。

WDP的主要功能包括：

- 根据端口号访问应用；
- 数据包分段和重组（可选）；
- 错误检测（可选）。
- WDP 能够同时传输几个来自高层，面向单一低层承载的业务。端口号负责识别高层实体。

7.1.6 无线控制消息协议（WCMP）

WAP网关支持WCMP协议（可选）。

WCMP协议位于WDP适配层中，为WDP提供有效的差错控制机制，以用于提高WAP协议和应用的性能。WCMP包含类似Internet 控制消息协议（ICMP）消息的控制消息。它也能够用于诊断和信息报告。

WCMP协议适用于不提供IP承载的环境，例如，SMS等。WCMP消息通常由WDP层、管理实体或某高层协议生成。

在不同网络环境下，WAP支持的控制消息协议见表2：

表2 在不同网络环境下 WAP 支持的 WCMP

网络	ICMP	WCMP	描述
GSM SMS		*	WAP特定
GSM CSD	*		标准
GSM GPRS	*		标准
CDMA	*		标准

7.1.7 TCP/IP 协议栈

WAP网关必须支持IP协议，参见RFC 791。

WAP网关必须支持UDP协议，参见RFC 758。

WAP网关必须支持TCP协议，参见RFC 793。

WAP网关必须支持HTTP协议，参见RFC 2616。

WAP网关必须支持ICMP协议，参见RFC 792。

WAP网关必须支持IGMP协议，参见RFC 1112。

WAP网关必须支持SMTP协议，参见RFC 821。

WAP网关必须支持MIME协议，参见RFC 2045、RFC 2046、RFC 2047、RFC 2048、RFC 2049。

WAP网关必须支持POP3协议，参见RFC 1725。

WAP网关必须实现相关MIB：RFC 1213、RFC 1229、RFC 1398中相关部分。

7.2 WAP2.0 代理 / 网关协议栈要求

WAP2.0代理 / 网关应支持两种协议栈，两种协议栈的操作是独立的。

如图7所示，WAP2.0代理 / 网关的通用应用环境可以在任何一个协议栈上运行。代理 / 网关设备应能够支持并辨别使用不同协议栈的手持设备，并自动适应。

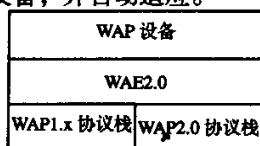


图7 双 WAP 栈支持

图8给出了一个WAP2.0代理/网关协议栈模型。这种配置下WAP代理/网关置于有线和无线网络之间，通过使用无线优化的TCP (TCP*)和无线优化的HTTP (HTTP*)协议增强网络性能。

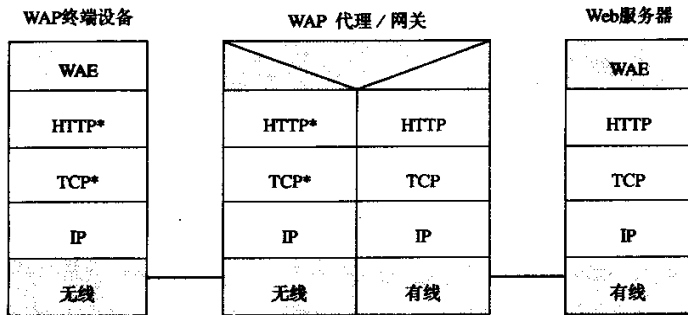


图8 使用 TCP*和 HTTP*的 WAP HTTP 代理

WAP2.0代理/网关应当支持WAP2.0协议栈，即：

- WAE2.0 (无线应用环境)；
- 无线优化 HTTP 协议；
- 无线优化 TCP 协议；
- IP 协议。

7.2.1 WAE2.0 要求

7.2.1.1 WAE 媒体类型

附录B给出了WAE2.0支持的MIME (Multipurpose Internet Mail Extensions) 媒体类型。

WAP2.0代理/网关应支持基于WCSS内容类型开发的各种应用对网关的要求。

7.2.1.2 WAE 特性

WAP2.0代理/网关必须支持以下WAE特性：

- WAP代理/网关必须支持超媒体⁵传输服务。
- WAP代理/网关必须支持WSP和/或WP-HTTP协议。
- WAE定义了一个附加可选机制以使WAP代理/网关能够代替UserAgent存储和管理Cookies。
- 支持WSP Connect原语的WAP代理/网关在WSP连接服务原语中必须使用其缓存的请求头 (Request Header) 作为客户端头 (Client Headers)。
- 支持WSP Resume原语的WAP代理/网关在WSP连接服务原语中必须使用其缓存的请求头 (Request Header) 作为客户端头 (Client Headers)。
- WAP代理/网关必须能够处理至少1024个字节的URI。
- WAP代理/网关必须支持HTTP URI方案。
- 当用户代理不支持源服务器送来的字符编码时，WAP代理/网关应当转换内容的字符编码。
- WAP代理/网关必须同时支持UTF-8和UTF-16编码方式。
- 处理XML文档时，要求按照RFC 3023中的规定字符编码进行解释，如果文档中包含未知字符，WAP代理/网关必须将差错通知发送给用户。

- WAP代理/网关必须按照HTTP1.1的规定假设Accept、Accept-Charset、Accept-Encoding和

⁵一种包含文字 (Text)、影像 (Movie)、图片 (Image)、动画 (Animation)、声音 (Audio) 等图文声光的文件。

Accept-Language 头的值。如果 WAP 代理/网关不能发送 WAE 用户代理可接受的响应,则 WAP 代理/网关应当按照 HTTP1.1 的规定进行响应。

— WAP 代理/网关应当尽可能满足用户代理所希望的 HTTP 属性。

— WAP 代理/网关不应当发送用户代理不接受的内容,例如,如果用户代理仅接受 WML2, WAP 代理应当将 WML1 转换为 WML2。

— 当用户代理更希望得到原始媒体类型时, WAP 代理/网关必须不作任何改变地发送原始媒体类型的内容。例如,当用户代理希望使用二进制格式时, WAP 代理/网关则不应当将 WML1 的二进制格式转换成为文本格式。

7.2.2 WP-HTTP 协议要求

7.2.2.1 完全兼容 HTTP/1.1 (RFC 2616)

WP-HTTP 的核心即 HTTP/1.1 (RFC 2616)。

7.2.2.2 支持 Pull 和 Push 两种业务应用

Pull 使用 HTTP/1.1 的请求/响应机制来实现;而 Push 功能则由 WAP 终端承担 HTTP 服务器的角色。

7.2.2.3 WP-HTTP 支持响应消息体压缩

这样做可以使空中传输效率增加。WAP2.0 代理/网关至少支持在 RFC 1951 中规定的 Deflate 压缩编码方式。Gzip (RFC 1952)、Compress (出自通用 UNIX 文件压缩程序) 这两种压缩方式可选。

7.2.2.4 支持安全隧道建立

WP-HTTP 还应支持使用 Connect 方式建立安全隧道,以用于端到端安全问题的解决。

7.2.2.5 支持 HTTP 客户端功能

WAP2.0 代理/网关中的 HTTP 客户端必须支持以下 HTTP 定义的方法 (RFC 2616):

- Get;
- Post;
- Options。

7.2.2.6 支持 HTTP 服务器功能

WAP2.0 代理/网关中的 HTTP 服务器必须支持以下 HTTP 定义的方法 (RFC 2616):

- Get;
- Head;
- Post;
- Connect。

WAP 代理/网关中的 HTTP 服务器可以支持以下 HTTP 定义的方法 (RFC 2616): (可选的)

- Options。

7.2.2.7 支持标准的 HTTP 特性

WAP 代理/网关应当支持内容编码。内容编码机制应遵循 RFC 2616 中 14.11 节的规定。如果 WAP 代理/网关支持内容编码,则必须至少提供在 RFC 1951 中规定的 Deflate 编码,以供与终端协商。

HTTP 服务器应当支持对 HTTP 响应中的消息体进行内容编码。

7.2.2.8 支持扩展的 HTTP 特性

HTTP 服务器必须支持使用 Connect 方式 (RFC 2817 中第 5 节中规定) 建立隧道。

HTTP客户端必须支持使用Connect方式（RFC 2817 中第5节中规定）建立隧道，如果它支持TLS协议的话。

7.2.3 WP-TCP 协议要求

WAP代理/网关必须支持TCP相关协议，包括RFC 0792、RFC 2211、RFC 2581。

WAP代理/网关必须支持无线优化TCP（WP-TCP）的要求。

WAP代理/网关应当支持表3所列项目，支持程度参照表3中要求。

表3 无线优化 TCP（WP-TCP）的要求

项 目	限定	支持程度
基于 BDP（带宽与延迟乘积）的最大窗口尺寸		Should
Window Scale Option（RFC 1323）	窗口尺寸 \geq 64kB	Must
	窗口尺寸 < 64kB	May
用于 RTTM（Round Trip Time Measurement）的时间戳选项（RFC 1323）	窗口尺寸 \geq 64kB	Should
	窗口尺寸 < 64kB	May
最大初始窗口（cwnd \geq 2）（RFC 2581）		Must
最大初始窗口（cwnd > 2）（RFC 2414）		May
可选确认选项（SACK）（RFC 2018）		Must
MTU（最大传输单位）路线发现（RFC 1191、RFC 1981）		Should
MTU 大于默认 IP MTU	不支持 MTU 路线发现	May
明确的拥塞提示（ECN）（RFC 2481）		May

8 Push 功能要求⁶

8.1 Push 总体要求

WAP网关应支持有确认的Push和无确认的Push两种业务类型。

在WAP环境中，Push的结构分为三大部分：Push代理网关（PPG）、Push发起者（PI）和WAP终端。PPG与Push发起者之间采用PAP（Push访问协议）协议进行通信，而通过Push-OTA（Over-the-air）协议在一个可设置的超时（Timeout）⁷时间内将需要Push的信息转发给WAP客户，如图9所示。

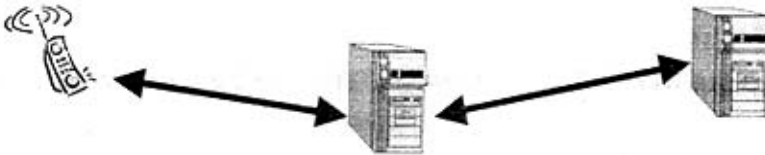


图9 Push 结构

Push发起者可以和Push代理网关PPG合设。

⁶ 除了 P-OTA 协议外，本章的内容是对 WAP1.x 和 WAP2.0 网关的共同要求。P-OTA 协议是对 WAP2.0 代理/网关的要求。

⁷ Timeout：该超时时长可由 Push 发起者设置，也可按移动运营商的策略设定。

在WAP1.x系统中，Push业务的消息内容通常需要利用现有的短消息系统，实现从WAP网关到WAP终端的推送。Push业务可以做到在新的信息到达手机时通知用户。通知方式可以是声音或可视信号，也可以根据不同业务采取不同的处理方式。与传统的短信息服务（SMS）根本的区别是：后者只能提供静态信息，而Push提供可点击的URL链接，使用户有选择采取下一步行动的权利。

在WAP2.0系统中，Push消息的内容应能够通过Push-OTA（Over-the-air）协议直接到达移动终端。此时的用户终端可能处于以下状态：

- 关机。此时无法进行任何业务（包括Push业务），也无法激活终端。
- 开机但不在线（与网络无IP连接）。需要激活IP连接后（激活终端）才能进行Push业务；
- 开机并且在线（与网络有IP连接）。可以直接进行Push业务。

当WAP终端开机但不在线时，PPG可以采用SIR命令激活终端，但此时SIR命令应通过短消息承载。终端收到SIR命令之后，应开始登录网络（PPP建立、得到IP地址等），IP通道建立后，终端应向PPG发起TCP连接请求，建立连接后PPG将需要Push的内容发给WAP终端。

当WAP终端开机并且在线时，PPG可以采用SIR命令激活终端（SIR命令的承载可以是短消息，也可以是IP连接），终端的SIA收到SIR命令后，主动向PPG发起TCP连接请求，建立连接后PPG将需要Push的内容发给WAP终端。另外PPG也可以直接向WAP终端的监听程序发起TCP连接请求，建立连接后，PPG将需要Push的内容发给WAP终端。

8.2 Push 代理网关（PPG）功能要求

PPG必须支持Push访问协议（Push Access Protocol），以便与Push发起者交换Push信息；必须支持Push空中协议（Push Over-the-Air Protocol），以便与WAP客户交换Push信息。

Push业务的核心任务均由PPG来完成。它能够提供的服务包括：

- Push发起者（PI）的识别、认证以及访问控制；
- 对Push的内容以及控制信息进行分析并检测错误；
- 客户（包括客户的能力）发现服务；
- Push内容接受者的地址解析；
- 对特定类型内容进行二进制编码或编译（WAP1.x），或进行一般压缩（WAP2.0），以提高OTA协议传输的有效性；
- 协议转换；
- PPG还应支持向服务器提供客户机性能参数的功能，使服务器能够根据特定WAP设备的具体能力创建更为适合该客户机的内容格式。

8.3 PAP 协议要求

PAP协议是PI与PPG之间的通信协议。PAP可以利用隧道方式在任何Internet协议上运行。目前HTTP协议是必选支持，其他如SMTP协议等为可选支持。

PAP支持以下操作：

- Push提交（PI到PPG）；
- 结果通知（PPG到PI）；
- Push取消（PI到PPG）；
- Push代替（PI到PPG）；
- 状态查询（PI到PPG）；

— 客户机性能查询 (PI 到 PPG)。

以上所有操作都是基于请求/响应模式的。

8.4 OTA 协议要求

在面向WAP终端一侧, PPG所使用的协议为POTA。POTA运行在WSP (OTA-WSP) 或HTTP (OTA-HTTP) 之上。PPG必须支持OTA-WSP和OTA-HTTP。

当PPG收到内容信息后会尝试查找正确的目的设备, 将WAP内容编译成二进制编码后 (该工作也可在PI预先完成), 以POTA协议将内容发送给客户。

Push OTA-HTTP是一个轻量协议且无状态。它主要功能有:

- 利用 WSP 进行推送;
- 应用程序寻址, 该功能在 WAP 客户端实现;
- 在空中交换 Push 控制信息;
- 承载选择和控制, PPG 可以利用 OTA 源语中承载标识, 提供本功能;
- 认证 PI, PPG 可以通过 OTA 协议告之客户机, PI 已经经过认证。

8.5 Push 的媒体类型

8.5.1 已知的 MIME 媒体类型

Push业务必须支持已知的任何MIME媒体类型, 参见附录B。

8.5.2 业务指示 (SI)

业务指示 (SI) 是一般的带有 URL 的消息。

Push业务必须支持SI媒体类型。

除SI的基本功能外, SI还应允许以下功能控制:

- 用户打扰级别 (分配给 SI 一个特定优先级);
- 代替 (以新接收到的 SI 代替旧的);
- 删除 (删除一个已经处理过的 SI);
- 过期 (分配给 SI 一个生存时间)。

8.5.3 业务载入 (SL)

该内容类型提供一种能力使移动终端中的用户代理能够下载并执行某种业务, 而无须用户干涉。SL中包含一个 URI 指示该业务。

Push业务应当支持SL媒体类型。

8.5.4 Cache 操作 (CO)

该内容类型提供一种方法以使用户代理内存的某些内容无效。一般用于有使用时间限制的应用。

Push业务应当支持CO媒体类型。

9 UAProf 功能要求⁸

9.1 UAProf 的结构描述

用户代理定制 (UAProf) 扩展了WAP的能力。源服务器、网关保证用户收到的内容适合它提供的环境, 允许源服务器选择和发送适合客户请求功能的业务, 加强基于用户优先级和其他条件的内容个性化。

⁸ 本章是对 WAP1.x 和 WAP2.0 网关的共同要求。

UAProf定义了描述终端、用户和网络信息的CPI（能力和优先级别信息），收集包括硬件、软件、用户和应用优选、WAP特性和网络的定制信息。CPI的具体信息格式参见附录B。

当请求从终端设备传送到源服务器，CPI信息和请求一起传送，经过的每一个网络单元可以向传输的消息附加CPI信息。这些体现网络单元的具体信息，附加或覆盖终端发出的CPI信息。

CPI信息在移动终端、WAP网关和源服务器之间的传输采用W3C定义的存储能力和优先级别框架（CC/PP）。CC/PP框架由Component组成，每个Component包含一系列Attribute-Value对或者Property。Component可选提供一个缺省的描述块，包含一套Attribute的Value或一个URI，集中了缺省Attribute的Value。Component中的Attribute的Value要覆盖缺省值。

CPI信息的端到端传输结构如图10所示。WAP1.x终端通过基于WAP的CC/PP（即CC/PP-WAP）和WAP网关之间传送CPI信息，在另一侧WAP网关通过基于HTTP的CC/PP（即CC/PP-HTTP）。W-HTTP终端通过基于W-HTTP的CC/PP直接连接源服务器或使用性能属性加强的代理。

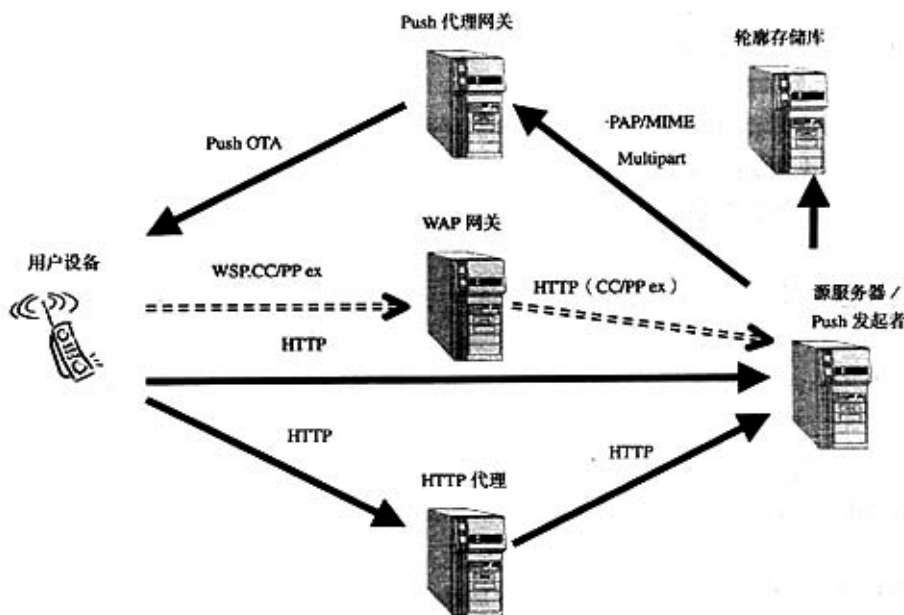


图10 UAProf 端到端结构

在CC/PP-WAP上传送的CPI信息经过二进制编码，同时网关支持WSP和HTTP简单互操作以高效传输和缓存来节省网络带宽。

9.2 UAProf 对 Pull 网关要求

用户代理定制将终端设备软硬件信息、用户和应用优先选择以及网络的定制信息通知服务器，以便源服务器发出更适合用户和网络的业务内容。

对WAP1.x网关的要求：

- 正确响应终端发送的带有定制信息的 WSP 会话建立请求；
- 会话期间保存用户定制信息；
- 支持 WSP 会话暂停和恢复的网关可以在暂停 WSP 会话时保存用户的定制信息；
- 支持 WSP 会话暂停和恢复的网关可以在会话期间或恢复 WSP 会话时接收用户更新的定制信息，

并正确响应；

— 用户业务请求（WSP 请求）中带有定制信息时网关可以用覆盖或扩展网关内保存的定制信息向服务器发起业务请求（HTTP 请求）；

— 网关可以附加网络定制信息到业务请求（HTTP 请求）；

— 前转服务器的业务响应和内容给 WAP 终端，可以根据保存的用户需求修改业务响应；

— 支持 WSP 消息和 HTTP 消息间定制信息的转换，互换符合 WAP2.0 的 UAProf 规范第 7 章的定义；

— 支持 WSP 消息和 HTTP 消息间定制信息的编解码，编码格式应符合 WAP2.0 的 UAProf 规范第 8 章。

对 WAP2.0 代理 / 网关的要求：

— 前转并存储用户发起的带有定制信息的业务请求；

— 前转并存储服务器返回的带有定制信息支持回答的响应。

WAP 网关应该支持的用户代理定制信息，CPI 的具体信息格式参见附录 B。

9.3 UAProf 对 Push 网关的要求

PPG 能够正确响应 PI 的用户能力请求，将当前保存的用户定制信息送回 PI。接收了 Push 消息中的用户能力要求，PPG 分别与每个请求发送 Push 消息的、用户当前的定制信息相匹配，前转 Push 消息给符合要求的用户。对于不符合要求的用户，PPG 可以改变 Push 消息内容以适应发送，也可以丢弃消息并向 PI 返回 Push 状态报告。

对 WAP1.x 网关的要求：支持 WSP 承载 Push 消息的网关应在 Push 会话建立时接受并正确响应带有用户定制信息的 Push 会话请求，并在会话期间保存定制信息。定制信息符合 WAP2.0 的 UAProf 规范第 7 章的定义。采用 WBXML 编码，编码格式应符合 WAP2.0 的 UAProf 规范第 8 章。Push 会话在 WSP 上的功能应符合 WAP2.0 的 OTA-WSP 规范。

对 WAP2.0 代理 / 网关的要求：支持 HTTP 承载 Push 消息的网关应能发送登记请求获得用户的定制信息。定制信息符合 WAP2.0 的 UAProf 规范第 7 章的定义。Push 会话在 HTTP 上的功能应符合 WAP2.0 的 OTA-HTTP 规范。

PPG 应该支持的用户代理定制信息，CPI 的具体信息格式参见附录 B。

9.4 UAProf 服务器的要求

用户代理定制服务器应当可以收集并存储终端设备软硬件信息、用户和应用优先选择以及网络的定制信息，并允许源服务器查询用户定制信息，以便发出更适合用户和网络的业务内容。UAProf 服务器应支持以下功能：

— 支持用 CPI 标记对 CPI 的查询、存储及维护。

— 支持对查询服务器进行鉴权。

— 支持 RDF。

— 支持缺省的 UAProf 能力的存储、查询及维护。

— 终端只下发 URI 时，支持代理向其他 URAProf 服务器查询、存储、修改。

10 支持 WTA 的网关要求 (可选)⁹

WTA是WAP应用的扩展,支持WTA的终端可以通过WAP激活设备进行通信,比如拨打电话、接听电话、访问电话簿等。WTA终端通过WTA接口(WTAI)接收到电话相关的网络事件时产生的WML页面,用户对页面中的内容作出选择,如果触发了电话应用时,WTA通过WTAI接通移动网络。

10.1 WTA 框架

WTA框架支持WAP终端和移动网络接口的无线电话应用。WTA框架扩展了WAE框架,增加以下功能的支持:

- WTAI 接口: WML 和 WMLScript 到终端设备上电话相关功能的接口。
- 网络事件处理: WTA 用户代理可以探知移动网络发起的事件并作出响应。
- 存储容器: 存储容器永久保存 WTA 业务的内容, 保证实时性的要求。
- WTA 用户代理状态和 WTA 上下文管理的模型。
- 安全模型。

图11阐述了WTA用户代理、存储器(永久存储)和WTAI(电话应用接口)之间以及它们和WTA终端设备中其他的实体之间的相互作用。

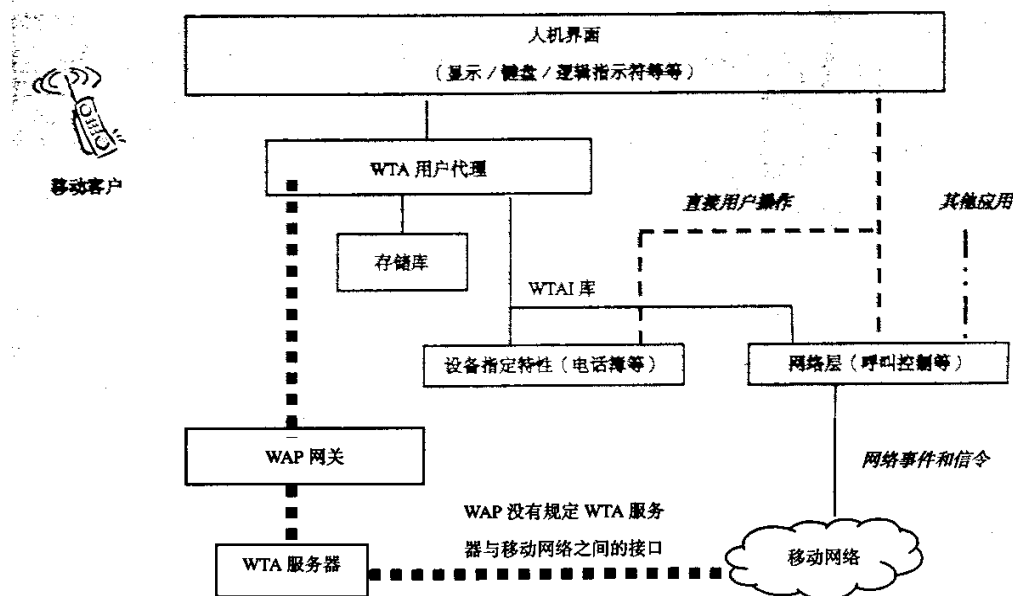


图11 WTA 结构

另外, WTA定义了一个特别的库——WTAI公共库,使得WAE用户代理具有简单的电话支持能力。

WTA业务会以不同的内容形式出现,例如,WML2、WMLScript等,WTA用户代理执行保存在存储器中或从WTA服务器取得的内容,还负责处理移动网络发出的事件(例如,电话呼入、语音邮件)。

对于有连接的WTA会话业务,WTA用户代理像WAE用户代理一样通过WSP会话获得WTA服务器上的内容。WAP网关必须支持WSP协议以建立会话。

⁹ 本章是对 WAP1.x 和 WAP2.0 网关的共同要求。

WTA用户代理使用URL指向WTA服务器的内容。URL指向WTA服务器上的应用来创建和移动网络实体（例如，智能网节点或语音邮件系统）互通的业务。WTA服务器还可以发送SI（业务指示）将网络消息Push到用户，这种业务要求WAP网关支持SI。

WTA业务可以由移动网络运营商或第三方提供。WAP网关通过WDP端口号区分WTA业务和其他WAE业务。在用户侧，用户代理访问WTA功能需要经过用户许可。

WTA的安全模型保证只使用可以信赖的网关，同时网关检验WTA推或拉的内容是经过批准的。使用WTLS，WTA业务可以通过安全管道经过网关传送到客户。网关到WTA服务器之间的安全性由SSL/TLS或其他方案解决。

10.2 WTA 功能实现对 WAP 网关的要求

WTA功能的实现十分依赖WTA终端和WTA服务器的支持，WAP网关仅仅要求：

- 支持 SI：用于特定业务（例如，语音邮件）中服务器将 SI 消息传送至用户。
- 安全模型：网关支持 WTA 专用的 WDP 端口号将 WTA 业务准确定向到 WTA 服务器；网关支持 WTLS 协议确保 WTA 业务的安全性。

10.3 WTA 服务器的要求

WTA服务器可以被看作一个分发客户端需要内容的Web服务器。与一个普通的Internet Web浏览器类似，WTA用户代理使用URL指向WTA服务器的内容。URL指向WTA服务器上的应用来创建和移动网络实体（例如，智能网节点或语音邮件系统）互通的业务。WTA服务器还可以发送SI（业务指示）将网络消息Push到用户。

网关到WTA服务器之间的安全性由SSL/TLS或其他方案解决。

11 WAP 网关的性能要求¹⁰

11.1 单机处理能力

WAP网关单机处理能力由每秒处理的事务Transaction与会话Session并发数衡量。

当每事务为4k数据量时，Pull处理能力：

- 每秒处理的事务数>300；
- 并发会话数>7000。

Push 处理能力：

- 每秒处理的事务数>300；
- 并发会话数>7000。

11.2 WAP 网关处理最大时延

WAP业务的服务质量（QoS）可以用处理一个请求所需等待的时间来衡量。

具体指标待定。

11.3 可靠性指标

WAP网关设备必须采用冗余及容错技术设计，利用双备份、多级分散控制、多通道、互助及系统重组等方法实现最大限度的系统可靠性。当WAP网关设备出现故障时，应能在尽可能短的时间内得以维护而恢复功能。

¹⁰本章是对 WAP1.x 和 WAP2.0 网关的共同要求。

- 系统故障恢复时间 < 1h;
- 无故障工作时间>26280h。

11.4 可扩展性

WAP网关应具有良好的可扩展性，要求既可支持增加CPU的方式进行扩容，也可支持多机集群（Cluster）的扩容方式。

WAP网关应支持多个物理以太网卡地址与一个IP地址进行映射对应的功能。在增加网关数量时，不需终端用户改变网关IP地址的设置，即可对网关进行第二层的扩充。

WAP网关应能支持虚拟IP地址功能。

WAP网关应具有热扩容能力，即不需关机就可进行扩容的能力。

12 WAP 设备操作维护及网管技术要求

12.1 网络管理方式

网络管理采取集中管理方式，设置全网网管中心，负责完成各项管理功能。

12.2 网络管理对象

网管中心着重进行设备管理，其管理对象为各节点设备。

管理的设备列表如下：

- WAP 网关；
- 接入服务器（CSD 方式）；
- 某些应用服务器；
- 防火墙；
- 计费/结算中心。

12.3 网管接口协议

为保证不同设备能够接入一个统一的网管平台并实现上述各项网络管理功能，接入服务器、WAP网关及防火墙设备须采用标准的SNMP通信协议。

12.4 网管接口信息模型

WAP接入服务器、网关/代理及防火墙系统内应设置网管代理模块，采集网络相应的系统信息、配置信息、告警信息、性能统计信息并负责维护MIB库。网管中心和被管设备之间的网管信息模型采用统一的MIB库，MIB库的标准格式将在相应网管标准中予以明确。

12.5 网管功能

12.5.1 配置管理

配置管理具有下列功能：

- 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。
- 管理设备的配置文件。可以访问被管理设备的配置文件，并在必要时分析和编辑。
- 网络节点设备部件、端口配置。
- 网络节点设备系统软件的配置。
- 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。

- 对配置操作过程的记录统计。

12.5.2 故障管理

故障管理负责监视WAP设备的故障告警、进行故障诊断及定位分析、告警日志的创建及维护，并通过冗余设备或冗余路由即时恢复措施重新提供服务。

告警信息应可通过图形方式对不同的运行状态和告警级别进行显示，并同时产生告警日志，供查询。

告警类型分为：设备告警、环境告警、通信告警、服务质量告警等。

告警级别分为：严重告警(Critical)、重大告警(Major)、次要告警(Minor)、警告告警(Warning)、已清除的告警(Cleared)、未确定(Indeterminate)。

告警状态分为：存在(Raised)、清除(Cleared)。

12.5.3 性能管理

性能管理是向网络运营者提供网络设备的性能特征，以供网络趋势分析、网络扩建、网络控制时参考。性能管理主要包括：性能监视、性能分析、性能控制、性能测试。

1) 性能监视

通过对被管理的WAP设备的监控和轮询，获取有关网络运行的信息及统计数据；提供网络的性能统计，例如：

- WAP 网关/代理中当前活跃的安全会话（基于网关）；
- 会话数量（基于网关）；
- 流量流向统计（基于网关）。

2) 性能分析

- 业务流量曲线（包括流量和流向）（基于网关/代理）；
- 日均用户曲线（基于网关/代理）；
- 非正常终止原因及出现概率等（基于网关/代理）；
- 用户平均每一次使用时长（基于网关/代理）。

3) 性能控制

以上述性能分析为基础，对制约网络性能的相关参数进行调整。

修改WAP设备相关参数优化性能。

12.5.4 安全管理

安全是指通过采用合适的安全技术，确保设备及网络上的信息和服务不被未经授权的用户使用。安全机制应保障所有信息网内部的资源不受意外事件的侵袭。

- 对管理者实现身份鉴别机制。
- 对关键数据实现备份。

13 环境要求

13.1 工作环境要求

13.1.1 WAP 网关应在以下的温度、湿度条件下正常工作

- 长期工作条件：温度为 15℃ ~ 30℃、相对湿度为 40% ~ 65%；
- 短期工作条件：温度为 0℃ ~ 45℃、相对湿度为 20% ~ 90%。

- 注：1) WAP 网关的正常工作时温度和相对湿度的测量点指在地板以上 2m 和 WAP 网关前方 0.4m 处的测量值。
 2) 短期工作条件指连续不超过 48h 和每年累计不超过 15 天。
 3) 相对湿度低于 20% 的环境应采用防静电地面。

13.1.2 WAP 网关的防尘要求

机房内直径大于 $5\mu\text{m}$ 的灰尘浓度应 $\leq 3 \times 10^4$ 粒 / m^3 ，机房中应无爆炸、导电、导磁性及腐蚀性尘埃。

13.2 防电磁干扰要求

WAP 网关产生的电磁干扰应满足以下要求：

- (1) 由 WAP 网关射出的无线电电磁干扰应符合表 4 的规定。

表4 WAP 网关射出的无线电电磁干扰

频率 (MHz)	电磁强度 dB ($\mu\text{V/m}$)	频率 (MHz)	电磁强度 dB ($\mu\text{V/m}$)
0.01-0.024	148.6-60lgd	47.7/d-88	59.1-20lgd
0.024-0.8	116.2-60lgd-20lgf	88-216	63.6-20lgd
0.8-1.59	118.2-60lgd	2160-10000	66.6-20lgd
1.59-47.7/d	120.2-60lgd-40lgf		

注：

- 1) d 为测试天线与靠近被测物间水平距离；单位为 m， d 限于 30m 内；
 2) f 为频率，以 MHz 为单位；
 3) dB ($\mu\text{V/m}$) 表示微伏 ($\mu\text{V/m}$) 为参考单元的分贝数。
- (2) 由 WAP 网关进入交流馈电线的无线电电磁干扰应符合表 5 的规定。

表5 由 WAP 网关进入交流馈电线的无线电电磁干扰

频率 (MHz)	最大线路电流 (dB μA)
0.000061-0.001	$I-20\lg f-84.4$
0.001-0.01	$(124.4-I)\lg f+348.8-2I$
0.01-0.8	$-21.05\lg f+57.9$
0.8-100	60

注：
 1) f 为频率，以 MHz 为单位；
 2) I 为接入到交流电源处的输入线路电流电平；
 3) dB μA 表示微安 (μA) 为参考单元的分贝数。

- (3) 由 WAP 网关进入直流馈线和信号线的无线电电磁干扰应符合表 6 的规定。

表6 由 WAP 网关进入直流馈线和信号线的无线电电磁干扰

频率 (MHz)	最大线路电流 (dB μA)
0.01 ~ 0.8	$-21.05\lg f+57.9$
0.8 ~ 100	60

13.3 WAP 网关抗电磁干扰的能力

WAP 网关在受到 0.01 ~ 1000MHz 频率范围，并且电场强度为 140dB $\mu\text{V/m}$ 的外界电磁干扰时，应不出现故障和性能下降。

在直流或交流电源线受到表 7 所示的频率时，0.01 ~ 100MHz 频率范围的外界电磁干扰电流时应不出现故障和性能下降。

表7 0.01 ~ 100MHz 频率范围的外界电磁干扰电流

频率 (MHz)	最大线路电流 (dB μ A)
0.01 ~ 0.8	$-21.05\lg f + 67.9$
0.8 ~ 100	70

14 电源与接地

14.1 电源要求

1) 直流电压及其波动范围要求

— 额定电压为-48V 的直流电源。

— 电压波动范围: 在直流输入端子处测量-48V 电压允许变动范围为-57 ~ -40V。WAP 网关在此范围内应工作正常。

2) 交流电压及其波动范围要求。

— 单相 220V \pm 10%，频率 50Hz \pm 5%；

— 线电压波形畸变率 < 5%。

14.2 WAP 网关接地要求

1) 接地方式应符合工作地、保护地和建筑防雷接地公用一组接地体的联合接地方式。

2) 接地线截面积

接地线截面积根据可能通过的最大电流负荷确定。应采用良导体导线，不能使用裸导线布放。

接地电阻值: 联合接地的电阻值应 < 1 Ω 。

15 例行试验

15.1 低温试验

应符合 GB 2423.1 的要求。

15.2 高温试验

应符合 GB 2423.2 的要求。

15.3 恒定湿热试验

符合 GB 2423.9 的要求。

15.4 运输试验

WAP 网关按包装文件要求完整包装后,置于载重汽车中后部,在三级公路上以 25 ~ 40km/h 的速度行驶 200km 后, 包装箱应完好无损。开箱检查 WAP 网关无机械损伤、紧固件无松脱接通电源、开机工作应符合质量要求。

15.5 贮存要求

产品的贮存应符合 GB 3873 的有关规定。

15.6 标志、包装、运输

15.6.1 产品标志

在产品适当位置应有铭牌, 铭牌的形式和尺寸应符合相关标准的规定。

15.6.2 包装标志

外包装应有包装储运图示标志，应按 GB 191 有关规定执行。

15.6.3 包装

随机文件有产品合格证、使用说明书、产品随机备附件清单。

产品包装要求应符合GB 3873的有关规定。

15.6.4 运输

产品可由火车、汽车、飞机、轮船等运输，但在运输过程中必须有遮蓬，不应有剧烈的震动和撞击，并按包装箱上标明方向放置。

附录 A
(规范性附录)

WAE2.0 支持的媒体类型

WAE2.0支持的媒体类型见表A.1。

表 A.1 WAE2.0 支持的媒体类型

数据类型	MIME媒体类型	文件扩展名
WML1 文本格式	text/vnd.wap.wml	.wml
WML1 二进制格式	application/vnd.wap.wmlc	.wmlc
WML2	application/vnd.wap.wml+xml (the registration of application/wml+xml is on-going)	.wml
XHTML Basic	application/xhtml+xml text/html 1	.xhtml, .xht
XHTML Mobile Profile	application/vnd.wap.xhtml+xml application/xhtml+xml; profile="http://www.wapforum.org/xhtml" text/html	.xhtml, .xht
WAP CSS	text/css	.css
WMLScript 文本格式	text/vnd.wap.wmlscript	.wmls
WMLScript 二进制格式	application/vnd.wap.wmlscriptc	.wmlsc
WBXML	application/vnd.wap.wbxml	
WBMP	image/vnd.wap.wbmp	.wbmp
vCard	text/x-vCard	.vcf
vCalendar	text/x-vCalendar	.vcs
WTA-WML 文本格式	text/x-wap-wta-wml	
WTA-WML 二进制格式	application/x-wap-wta-wmlc	
Multipart 消息(在消息体的各部分是独立的,且需要按特定顺序捆绑在一起的时候使用)的文本格式	multipart/mixed	
Multipart 消息(在消息体的各部分是独立的,且需要按特定顺序捆绑在一起的时候使用)的二进制格式	application/vnd.wap.multipart.mixed	
Multipart 消息(描述与 MIME 消息体各部分相关的聚合在一起的客体)的文本格式	multipart/related	
Multipart消息(描述与MIME消息体各部分相关的聚合在一起的客体)的二进制格式	application/vnd.wap.multipart.related	
Multipart消息(在消息体的各个部分均为一个相同信息的不同版本的时候使用)的文本格式	multipart/alternative	
Multipart消息(在消息体的各个部分均为一个相同信息的不同版本的时候使用)的二进制格式	application/vnd.wap.multipart.alternative	
Multipart消息(用于返回来自表格的值)的文本格式	multipart/form-data	
Multipart消息(用于返回来自表格的值)的二进制格式	application/vnd.wap.multipart.form-data	

表 A.1 (续)

数据类型	MIME媒体类型	文件扩展名
文本格式的Channels	text/vnd.wap.channel	
二进制格式的Channels	application/vnd.wap.channelc	
文本格式的Service指示	text/vnd.wap.si	
二进制格式的Service指示	application/vnd.wap.sic	
文本格式的Service载入	text/vnd.wap.sl	
二进制格式的Service 载入	application/vnd.wap.slc	
文本格式的Cache操作	text/vnd.wap.co	
二进制格式的Cache操作	application/vnd.wap.coc	
文本格式的Provisioning文档	text/vnd.wap.connectivity-xml	
二进制格式的Provisioning文档	application/vnd.wap.connectivity-wbxml	

附录 B
(资料性附录)
UAProf CPI 信息格式

B.1 硬件内容

UAProf CPI硬件方面的信息格式见表B.1。

表 B.1 UAProf CPI 硬件方面的信息格式

参 数	描 述	类 型	示 例
BitsPerPixel	每像素的比特数	Number	"2", "8"
ColorCapable	设备是否支持彩色显示	Boolean	"Yes", "No"
CPU	CPU 类型	Literal	"Pentium III", "PowerPC 750"
ImageCapable	是否支持图像显示	Boolean	"Yes", "No"
InputCharSet	支持的输入字符集	Literal (bag)	"US-ASCII", "ISO-8859-1", "Shift_JIS"
Keyboard	支持的键盘类型	Literal	"Disambiguating", "Qwerty", "PhoneKeypad"
Model	终端设备型号	Literal	"Mustang GT", "Q30"
NumberOfSoftKeys	设备支持的软键盘数	Locked Number	"3", "2"
OutputCharSet	支持的输出字符集	Literal (bag)	"US-ASCII", "ISO-8859-1", "Shift_JIS"
PixelAspectRatio	像素宽高比	Dimension	"1x2"
PointingResolution	设备支持的解析方式	Literal	"Character", "Line", "Pixel"
ScreenSize	屏幕尺寸	Dimension	"160x160", "640x480"
ScreenSizeChar	屏幕可显示的字符数	Dimension	"12x4", "16x8"
SoundOutputCapable	是否支持声音输出	Boolean	"Yes", "No"
TextInputCapable	是否支持文本输入	Boolean	"Yes", "No"
Vendor	生产厂商	Literal	"Ford", "Lexus"
VoiceInputCapable	是否支持任何形式的语音输入, 包括语音识别	Boolean	"Yes", "No"

B.2 软件内容

UAProf CPI软件方面的信息格式见表B.2。

表 B.2 UAProf CPI 软件方面的信息格式

参 数	描 述	类 型	示 例
BitsPerPixel	每像素的比特数	Number	"2", "8"
AcceptDownloadable Software	用户选择是否接受可下载的软件	Boolean	"Yes", "No"
AudioInputEncoder	语音输入编码	Literal (bag)	"G.711"
CcppAccept	内容类型	Literal (bag)	"text/html", "text/plain", "text/html", "image/gif"
CcppAccept-Charset	字符集	Literal (bag)	"US-ASCII", "ISO-8859-1", "Shift_JIS"
CcppAccept-Encoding	传送编码	Literal (bag)	"base64", "quoted- printable"
CcppAccept-Language	用户喜好的语言	Literal (sequence)	"zh-CN", "en", "fr"
DownloadableSoftwareSupport	设备支持的可执行内容类型, 且希望网络也支持	Literal (bag)	"application/x-msdos-exe"
JavaEnabled	是否支持 Java 虚拟机	Boolean	"Yes", "No"
JavaPlatform	Java 平台	Literal (bag)	"Pjava/1.1.3-compatible", "MIDP/1.0-compatible", "J2SE/1.0-compatible"
JVMVersion	本机安装的 Java 虚拟机列表	Literal (bag)	"SunJRE/1.2", "MSJVM/1.0"
OSName	OS 名称	Literal	"Mac OS", "Windows NT"
OSVendor	OS 制造商	Literal	"Apple", "Microsoft"
OSVersion	OS 版本	Literal	"6.0", "4.5"
RecipientAppAgent	与当前请求相关的用户代理	Literal	"BrowserMail"
SoftwareNumber	设备固件版本	Literal	"2"
VideoInputEncoder	视频输入编码	Literal (bag)	"MPEG-1", "MPEG-2", "H.261"

B.3 网络特性

UAProf CPI网络特性方面的信息格式见表B.3。

表 B.3 UAProf CPI 网络特性方面的信息格式

参 数	描 述	类 型	示 例
CurrentBearerService	当前打开的会话承载	Literal	"OneWaySMS", "GUTS", "TwoWayPacket"
SecuritySupport	安全机制类型	Literal (bag)	"WTLS-1", "WTLS-2", "WTLS-3" "signText", "PPTP"
SupportedBearers	设备支持的承载	Literal (bag)	"GPRS", "CDMA", "GUTS", "SMS", "CSD", "USSD"

B.4 浏览器特性

UAProf CPI浏览器特性方面的信息格式见表B.4。

表 B.4 UAProf CPI 浏览器特性方面的信息格式

参 数	描 述	类 型	示 例
BrowserName	浏览器名称	Literal	"Mozilla", "MSIE", "WAP42"
BrowserVersion	浏览器版本	Literal	"1.0"
DownloadableBrowserApps	浏览器支持的内容类型, 且希望网络接受	Literal (bag)	"application/x- java-vm/java- applet"
FramesCapable	浏览器是否支持框架显示	Boolean	"Yes", "No"
HtmlVersion	HTML 版本	Literal	"2.0", "3.2", "4.0"
JavaAppletEnabled	浏览器是否支持Java Applets	Boolean	"Yes", "No"
JavaScriptEnabled	浏览器是否支持 JavaScript	Boolean	"Yes", "No"
JavaScriptVersion	JavaScript 语言版本	Literal	"1.4"
PreferenceForFrames	用户选择是否接受包含框架的HTML内容	Boolean	"Yes", "No"
TablesCapable	浏览器是否支持显示表格	Boolean	"Yes", "No"
XhtmlVersion	XHTML 版本	Literal	"1.0"
XhtmlModules	浏览器支持的 XHTML 模块列表	Literal (bag)	"XHTML1-struct", "XHTML1- blkstruct", "XHTML1-frames"

B.5 WAP特性

UAProf CPI WAP特性方面的信息格式见表B.5。

表 B.5 UAProf CPI WAP 特性方面的信息格式

参 数	描 述	类 型	示 例
SupportedPictogram Set	设备支持的图片类型	Literal (bag)	"core", "core/operation", "human"
WapDeviceClass	WAP 设备类型	Literal	"A"
WapVersion	WAP 版本	Literal	"1.1", "1.2.1", "2.0"
WmlDeckSize	一个 WML Deck 的最大尺寸	Number	"4096"
WmlScriptLibraries	设备 WMLScript 虚拟机支持的 必备和可选库	Literal (bag)	"Lang", "Float", "String", "URL", "WMLBrowser", "Dialogs", " PSTOR"
WmlScriptVersion	WMLScript 版本	Literal (bag)	"1.1", "1.2"
WmlVersion	WML 语言的版本	Literal (bag)	"1.1", "2.0"