ICS 33.060.01
M 36

YD

中华人民共和国通信行业标准

YD/T 2526-2013

数字蜂窝移动通信网
Web 网关设备技术要求

Technical requirements for digital cellular mobile telecommunication network web gateway

2013-04-25 发布　　2013-06-01 实施

中华人民共和国工业和信息化部　发布

目　次

前　言……III
1　范围……1
2　规范性引用文件……1
3　术语、定义和缩略语……1
3.1　术语和定义……1
3.2　缩略语……2
4　概述……2
5　Web 网关在网络中的位置……3
6　Web 网关功能要求……3
6.1　协议处理功能……3
6.2　管理控制功能……4
6.3　内容加速功能……10
6.4　内容适配功能……13
6.5　内容增强功能……16
6.6　内容过滤功能……17
7　性能指标和可靠性要求……18
7.1　可扩展性……18
7.2　可靠性要求……19
8　接口要求……19
9　网管要求……20
9.1　网络管理对象……20
9.2　网管接口协议……20
9.3　网管接口信息模型……20
9.4　网管功能……20
9.5　日志管理……22
10　计费……23
10.1　话单要求……23
10.2　计费支持……23
11　软硬件要求……24
11.1　Web 网关设备的软件和资源要求……24
11.2　Web 网关设备的硬件要求……24
12　操作维护要求……24
12.1　安全性……24

12.2 可管理性……25
12.3 可维护性……25
12.4 易用性……25
13 设备安全要求……25
13.1 物理安全……25
13.2 网络安全……25
13.3 系统安全……26
13.4 信息安全……26
13.5 安全防护……26
14 电源要求……27

前　言

本标准是数字蜂窝移动通信网Web网关系列标准之一，该系列标准的名称如下：

a）YD/T 2526-2013《数字蜂窝移动通信网Web网关设备技术要求》；

b）YD/T 2527-2013《数字蜂窝移动通信网Web网关设备测试方法》。

本标准按照GB/T 1.1-2009给出的规则起草。

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、华为技术有限公司。

本标准主要起草人：崔媛媛、李克鹏。

数字蜂窝移动通信网Web网关设备技术要求

1 范围

本标准对Web网关系统总体结构、网络架构、设备功能进行规定，并针对Web网关系统的网管、安全等方面提出相关的要求。

本标准适用于数字蜂窝移动通信网Web网关设备。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅所注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

GB 4943.1　　信息技术设备 安全 第1部分：通用要求

YD/T 1392-2005　WAP网关设备技术要求

YD/T 2055-2009　WAP网关内容过滤技术要求

ISO/IEC 14496　信息技术-音视频对象编码（Information technology – Coding of audio-visual objects）

IETF RFC 1951　简化压缩数据格式规范1.3版（DEFLATE Compressed Data Format Specification version 1.3）

IETF RFC 1952　GZIP文件格式（GZIP file format specification）

IETF RFC 2616　超文本传输协议-HTTP/1.1（Hypertext Transfer Protocol -- HTTP/1.1）

ITU-T H.264　用于通用音视频服务的增强视频编码（Advanced video coding for generic audiovisual services）

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文件。

3.1.1

Web网关　Web Gateway

为终端用户提供的Internet应用服务的接入设备，位于终端与Internet应用服务器之间，为用户提供增强的Web服务。

3.1.2

用户代理　User-Agent

浏览器用来向被访服务器表明“身份”的一个字符串，服务器可以根据这一信息向不同浏览器传送不同类型的信息。

3.1.3

互联网访问增强引擎　Advanced Engine for Internet Visit

由一些功能软件模块组成，负责浏览协议的优化、内容加速/压缩、内容过滤、内容增强和内容适配等。

3.1.4

轻量级目录访问协议　Lightweight Directory Access Protocol (LDAP)

根据用户标识查询用户数据库，得到用户档案，网关基于用户档案处理业务请求。

3.1.5

网络时间协议　Network time Procotol

在网络上指定若干时钟源网站，为用户提供授时服务，并且这些网站间应该能够相互比对，提高准确度的协议。NTP的目的是在国际互联网上传递统一、标准的时间。

3.1.6

通用路由封装　Generic routing Encapsulation (GRE)

一种隧道协议，能封装广泛的网络层协议在IP包里，通过IP网和远端创建虚拟点对点连接。

3.2 缩略语

下列缩略语适用于本文件。

BMP	Bitmap	比特图像
CP	Content Provider	因特网内容提供商
DNS	Domain Name System	域名系统
JPEG	Joint Photographic Experts GROUP	联合图像专家组
GIF	Graphics Interchange Format	图形交换格式
HTTP	Hyper Text Transfer Protocol	超文本传送协议
ICAP	Internet Content Adaptation Protoco l	互联网内容匹配协议
IWF	Internet Watch Foundation	互联网观察基金会
KPI	Key Performance Indicator	关键性能指标
MPEG	Moving Pictures Experts Group	动态图像专家组
MSA	Mobile Site Awareness	移动网站识别
PNG	Portable Network Graphic Format	可移植的网络图形格式
Radius	Remote Authentication Dial In User Service	远程用户拨号认证系统
SNMP	Simple Network Management Protocol	简单网络管理协议
SP	Service Provider	服务提供商
SSL	Secure Sockets Layer	套接字安全层
TLS	Transport Layer Security Protocol	安全传输层协议
URL	Uniform Resource Locator	统一资源定位
WAP	Wireless Application Protocol	无线应用协议。

4 概述

3G用户对互联网业务的需求越来越大，对于用户的不同的互联网业务需求，网络中需要有一个功能实体来做手机用户访问的Web业务和WAP业务的“交通枢纽”，起到代理服务器的作用，于是引入“Web网关”。Web网关可以面向所有移动终端用户提供浏览类业务的内容加速、内容适配、内容过滤等功能，

以提高终端用户的网页浏览体验。Web网关在移动数据业务中起着非常重要的作用，旨在解决各式的移动设备终端在访问互联网时，得到符合其移动设备属性的最佳用户体验，并且可以在此基础上开展业务。

5 Web 网关在网络中的位置

Web网关位于移动网络和互联网应用系统之间，可部署在WAP网关之后或与WAP网关并行部署。运营商和设备商可根据情况选取合适的部署方式。

Web 网关在网络中的位置如图 1 所示。在 Web 网关部署于 WAP 网关之后的情况下，Web 网关可以从 WAP 网关的 HTTP 消息中获取到用户号码，用户 IP 地址，用户归属网络等信息。在 Web 网关独立建设的情况下，Web 网关可以从核心网侧 Radius 消息中获取用户号码与 IP 地址之间的对应关系，并且获得用户归属网络的信息。

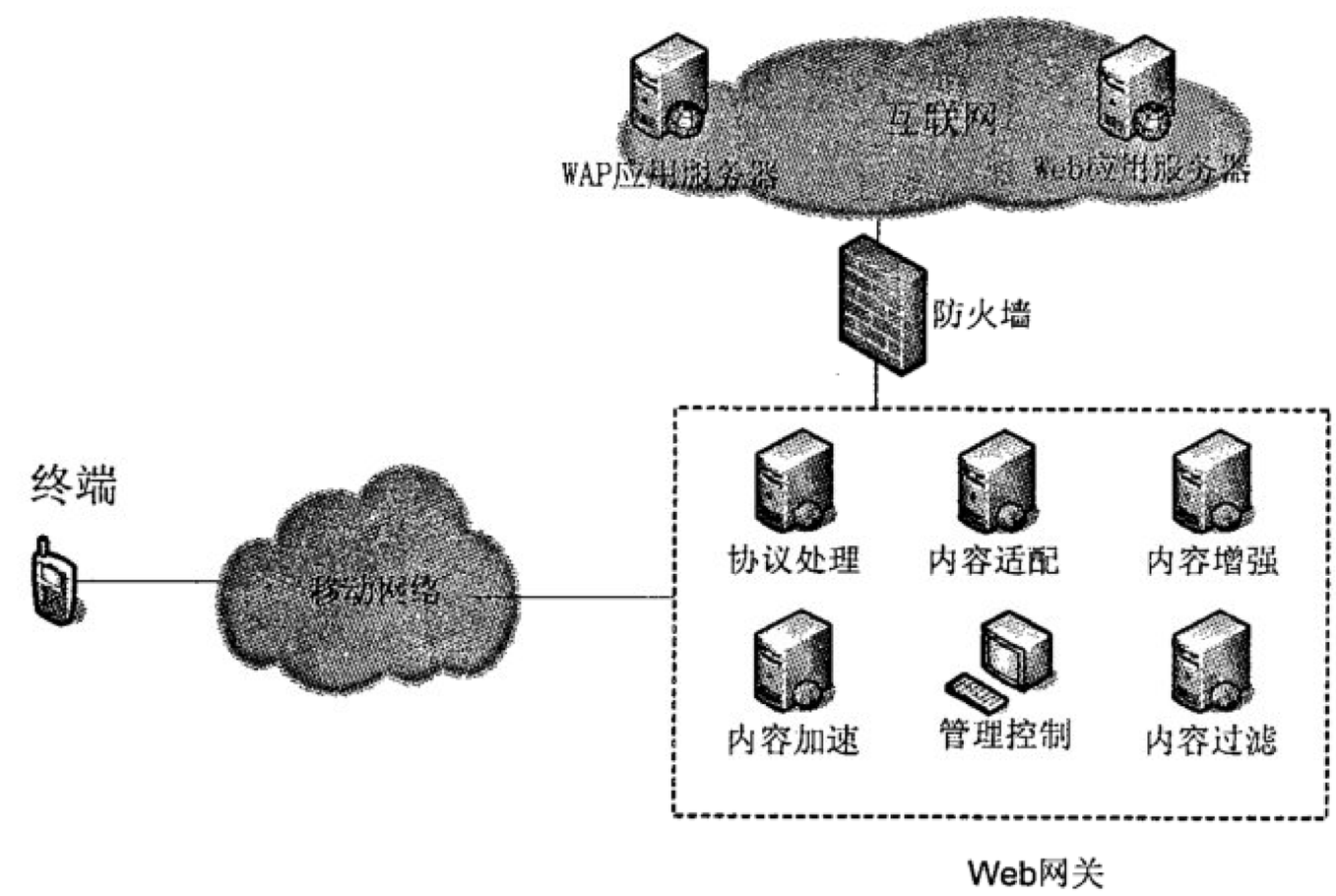

图 1 Web 网关在网络中的位置

Web 网关与互联网应用之间采用 HTTP 协议。

6 Web 网关功能要求

6.1 协议处理功能

6.1.1 HTTP 协议支持要求

Web网关应能够准确识别HTTP 1.0/1.1（IETF RFC 2616），能够进行HTTP代理访问，统计数据流量。Web网关对HTTP协议的支持包括：

——Web 网关应准确识别 HTTP 1.0/1.1（IETF RFC 2616）流量。

——Web 网关可以识别 HTTP 协议流量，统计数据流量，从而生成事务和计费记录。

——Web 网关应支持 HTTP 客户端功能，包括 GET、POST 和 OPTIONS；支持 HTTP 服务器功能，包括 GET、HEAD、POST、CONNECT 和 OPTIONS。

——Web 网关应准确识别 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 功能则由终端承担 HTTP 服务器的角色。

——Web 网关应支持响应消息体压缩，包括 IETF RFC 1951 中规定的 deflate 压缩编码方式、gzip（IETF RFC 1952）。

——Web 网关应支持使用 CONNECT 方式建立 TLS 安全隧道，以解决端到端的安全问题。

——Web 网关为了实现内容增强、内容适配等功能，在与 HTTP 服务器交互的过程中，能够对 HTTP 头进行增强处理。具体表现在如下的 HTTP 请求阶段和 HTTP 响应阶段：

- 在 HTTP 请求阶段，Web 网关应支持：
  - HTTP 请求合法检查，包括检查 Accept 头、Accept-Charset 头和 Accept-Encoding 头，进行必要的过滤。检查将依据 HTTP1.1/1.0 规范；
  - HTTP 头修正，参照终端属性数据，对 Accept 头、Accept-Charset 头和 Accept-Encoding 头进行适当的增减；
  - HTTP 头增强，参照网关能力，对 HTTP 头进行增强，从而支持更加广泛的数据格式及类型。
- 在 HTTP 响应阶段，Web 网关应支持：
  - HTTP 响应检查，与终端的原始请求进行对照，从而判断是否对接收到的数据进行转换或是否可以直接转发给终端；
  - HTTP 响应转换，当需要进行数据转换时，网关需要将数据转换为终端支持的格式。如果数据是被压缩过的，则首先要解压缩；
  - HTTP 响应合法性检查，参照终端属性数据，对 HTTP 头进行合法性检查，然后将响应转发给终端。

——Web 网关应支持 HTTP 管道线处理（HTTP pipelining），并行处理来自终端的多个请求；也支持 HTTP 内容管道线处理（content pipelining），只要得到的信息足够（如一些 HTTP 头已经得到），网关就转发消息，而不需要等到所有消息到达。

6.1.2 HTTPS 加密协议支持

对于HTTPS应用，Web网关应能够识别并进行代理访问，同时记录统计该部分流量。

6.1.3 WAP 协议支持要求

6.1.3.1 WAP 协议栈支持

Web网关要求支持WAP2.0协议栈，能够将识别出的WAP2.0协议的流量进行处理。

6.1.3.2 WAP2.0 协议要求

基于WAP 2.0 的协议要求见YD/T1392-2005。

6.1.4 TCP 报文处理功能

Web网关具备处理用户数据包、TCP和应用协议的软件，应支持对已定义的应用协议包括HTTP/HTTPS等进行协议优化处理。

6.2 管理控制功能

6.2.1 控制功能

6.2.1.1 适配重构控制

Web 网关应支持可配置的适配重构控制。通过 URL/IP 白名单以及 HTTP 头字段匹配，来控制是否对报文进行适配重构。

——通过 URL/IP 白名单进行控制：

Web 网关应提供适配重构白名单，在白名单中的内容 Web 网关不进行处理，白名单通过 URL/IP 进行配置。如报文的目的 IP/URL 在白名单中，则 Web 网关不进行适配重构，直接透传。

——根据 HTTP 头字段进行控制：

Web 网关应能通过 HTTP 头字段适配确定是否对报文进行重构适配。Web 网关能够根据头信息字段确定是否对报文进行处理，提供灵活的配置机制。

举例说明，对于采用HTTP协议传输的彩信应用，在实际应用中要求Web网关不予处理，则可在Web网关上通过配置过滤规则，不对报文进行处理，直接转发，确保其不受任何影响。

6.2.1.2 接入控制功能

Web网关应能对用户的上下线进行管理。Web网关需要内置Radius功能，能够识别和处理GGSN发送过来的Radius消息，并通过Radius实现对用户上下线的管理和控制。Web网关对用户上下线控制功能要求包括：

——黑名单控制功能——提供黑名单功能，黑名单中记录禁止上线用户的 MSISDN，利用黑名单机制对用户的上线请求进行控制，处于黑名单中的用户禁止任何访问。

——用户一次上线时长控制功能——Web 网关提供用户上线时长配置表。在配置表中，可以限制某一 MSISDN 的上线时长。当该用户一次上线若干时间后，Web 网关则清除用户在线信息，并对用户的请求返回错误响应，引导用户重新上线。

——用户上下线频率控制功能——Web 网关提供可配置的用户上下线频率。当发现用户单位时间间隔内上下线频率达到设定的阈值时，则 Web 网关在其后的一段时间内禁止该用户再次上线。

——多维度组合控制策略——Web 网关提供可配置的控制策略。对于用户接入，通过用户号码、协议类型、时间段、流量等四个维度的组合产生控制策略，Web 网关根据该控制策略进行接入控制。

6.2.1.3 连接控制功能

Web网关可以限制用户在同一个业务中的连接数。Web网关提供设定业务的单用户连接数阀值的功能，通过设定阀值限制每个用户在特定业务上的最大连接数。此外，Web网关还可根据不同的维度产生控制策略控制用户连接数。

Web网关通过记录同一用户使用业务及连接数的信息，发现该用户为使用同一业务而发起的连接数超过Web网关设定的为该业务设定的阈值时，Web网关应禁止用户后续的连接请求，并返回提示页面。

Web 网关限制连接数的业务类型包括：http 浏览业务和 ftp 业务。Web 网关可以对每类业务设置连接数阈值。

Web 网关应提供可配置的控制策略，对于连接数控制，通过用户号码、协议类型、时间段等维度的组合产生控制策略。如：用户号码为 13512345678 的 http 浏览业务在 15：00～16：00 的最大连接数为 20。

6.2.1.4 带宽控制功能（可选）

Web 网关提供带宽策略配置、管理和控制功能。Web 网关提供多维度组合控制策略，根据多个维度组合所产生的策略控制分配给用户的流量。Web 网关提供如下带宽控制能力：

a）支持的控制维度包括且不限于以下几个维度：用户、协议、时间段、流量、APN、承载类型。

Web 网关可根据以上维度进行组合所产生的策略来控制带宽。

b）支持区分协议的总带宽控制功能。

对于以下四种协议：HTTP、HTTPS、Mail、FTP，Web 网关可以限制各协议的总带宽。使所有以这四种协议流过 Web 网关的总带宽在限定的范围内。

c）QoS 控制功能。

Web 网关可包括有业务会话检测单元，用于检测业务会话请求及释放，还包括有：QoS 协商单元，用于在业务会话检测单元检测到业务会话请求时，向综合业务数据平台申请并获取 QoS 信息，及根据该 QoS 信息向策略决策功能实体请求 QoS 对应的业务服务所需资源，在业务检测单元检测到业务会话结束时，向策略决策功能实体请求释放 QoS 对应的业务服务资源。

6.2.1.5 访问控制

Web网关应支持对用户的访问请求进行控制。包括：

——支持 URL 分级功能：Web 网关能对互联网上网站的 URL 进行分级配置，以便于对访问目的地址进行管理。

——URL 过滤功能：支持直接与 URL 分级数据库交互或者集成第三方 URL 过滤程序。得到分类/分级结果后与用户 Profile（至少包括 General、Adult、Child 三类）综合，得到允许访问或禁止访问的结果。

——支持配置 URL 黑名单：配置 URL 黑名单列表，直接禁止访问，不再进行其他访问控制规则匹配。

——支持配置 URL 白名单：配置 URL 白名单列表，允许访问，不再进行其他访问控制规则匹配。

——支持 URL 替换：配置替换 URL 列表，独立于其他访问控制，最先进行处理。替换 URL 和目标 URL 都包括域名（可能包含端口），并且可以包括多个路径。如：目标 URL: http://aaa.bbb.ccc/ddd 替换 URL: http://mmm.nnn.ooo/ppp/qqq

替换结果：http://aaa.bbb.ccc/ddd/eee 替换为 http://mmm.nnn.ooo/ppp/qqq/eee。

——支持 URL 重定向：配置重定向 URL 列表，当匹配到后，进行 URL 重定向。如：目标 URL: http://aaa.bbb.ccc/重定向 URL: http://mmm.nnn.ooo/index.jsp

重定向结果：http://aaa.bbb.ccc/重定向到 http://mmm.nnn.ooo/index.jsp

http://aaa.bbb.ccc/ddd 重定向到 http://mmm.nnn.ooo/index.jsp。

——支持强制 SSL：为避免部分网站访问的安全问题，对一些网站进行强制 SSL。可以配置强制 SSL URL 列表，当匹配到后，进行强制 SSL。如：目标 URL：http://payment.bank.com/强制 SSL，重定向到 https://payment.bank.com/。

——支持主页推送：当用户在一次 PDP 会话中首次访问 HTTP 浏览类业务，进行主页推送。

——支持对隐藏 URL 进行访问控制：存在一些代理服务器，由代理服务器访问原始服务器，真正目标 URL 在参数中。如：http://www.google.com/gwt/n?u=http%3A%2F%2Fwww.abc.com，目标 URL 为 http://www.abc.com。访问控制的 URL 应该为 http://www.abc.com。

——支持对 URL 进行关键字过滤：配置关键字列表，当 URL 匹配到后，禁止访问。

——支持 User-Agent 访问控制：当 User-Agent 符合配置的规则时，禁止访问。支持通配符匹配。

——支持针对协议层访问控制：根据承载信息、用户 Profile 配置协议层访问控制规则，允许或禁止用户访问指定协议。

——支持针对业务层访问控制：根据承载信息、用户 Profile 配置业务层访问控制规则，允许或禁止用户访问指定业务。

——支持访问内容控制：可以接收到用户终端发起的携带目标地址的访问请求，判断所述目标地址

与内容控制服务器的地址是否相同，若不相同，根据预先设置的内容控制规则判断是否对所述访问请求进行内容控制，将需进行内容控制的访问请求发送至负责内容控制的服务器进行内容控制处理。

——支持对特定用户的访问控制：包括针对 URL、访问时间段、特定 SP 的业务来进行访问控制。

6.2.1.6 控制功能配置要求

Web网关应具备应提供对控制功能的配置管理。对控制功能的配置管理主要包括以下方面：

——接入控制策略配置：提供接入控制策略的配置界面，能够根据接入控制功能要求的中的各个维度，让管理员方便配置产生各种控制策略。

——连接控制策略配置：提供连接控制策略配置置界面，让管理员根据用户号码、协议类型（业务类型）、流量等维度等配置并产生连接控制策略。

——带宽控制策略配置：提供带宽控制策略配置界面，使管理员能根据带宽控制要求中的各维度配置并产生相应的带宽控制配置策略。

——适配重构 URL 白名单配置：提供 URL/IP 的白名单配置，在白名单内的地址和 URL,web 网关不进行管理。

——适配重构头字段配置：提供头字段匹配策略配置，如果 HTTP 报文的头字段符合预定策略，则不进行适配重构。

——访问控制策略配置：提供访问控制配置界面，根据访问控制功能要求配置各种策略。

6.2.2 日志管理记录功能要求

6.2.2.1 事件日志

Web网关的事件日志文件应至少包含以下内容：

——控制功能相关事件：记录 Web 网关控制功能相关的事件。如某用户不允许介入，某用户连接数达到阀值，连接被拒绝等。

——互联网访问增强引擎相关事件：Web 网关模块在进行互联网访问增强过程中发生的相关事件。

——异常事件：记录 Web 网关在流量处理过程中发生的异常事件（网络异常、处理过程异常等）的日志信息。

6.2.2.2 系统日志

Web网关的系统日志文件应至少包含以下内容：

——告警信息：记录 Web 网关运行过程中出现的系统异常信息。包括告警信息名称，发生时间，告警信息类型，告警信息级别等内容。

——进程启动/停止信息：记录 Web 网关运行过程涉及到的重点进程的启动及停止的日志信息。包括进程名称和进程启动/停止时间、完成情况等内容。

——系统配置变更信息：记录对 Web 网关的系统配置信息进行变更的日志情况。包括配置信息内容、变更时间、系统管理员名称、变更完成情况等内容。

6.2.2.3 管理员日志

Web网关的管理员日志文件应至少包含以下内容：

——管理员操作信息：记录管理员对 Web 网关进行操作和维护的相关日志信息。

6.2.2.4 报文处理日志

对于所有HTTP协议的访问，每次请求/响应都需要进行记录，记录的主要内容至少应包含：

——承载类型；

——用户手机号；

——用户 IP 地址；

——用户请求的 URL；

——用户请求的目的 IP 地址；

——目的地址的端口号；

——网关收到请求的时间；

——网关转发请求的时间；

——网关收到 URL 响应时间；

——网关转发响应到手机的时间；

——上行信息内容长度；

——下行信息内容长度；

——信息内容类型；

——CP 响应状态码；

——网关的 IP 地址；

——请求方法；

——业务种类；

——协议类型；

——返回状态代码；

——GGSN IP 地址。

而对于非HTTP访问，Web网关在不做任何适配加速处理保证应用正常使用情况下，对其进行透传。

6.2.2.5 日志保留与格式要求

对于原始日志，应支持至少在线存储90天，脱机存储6个月，能够支持磁盘容量告警。

能够将业务使用原始日志记录生成日志文件，定时定量传送给外部网元，时间长度和文件大小应可配置。文件传送接口支持FTP协议。

6.2.3 用户信息统计分析功能

6.2.3.1 统计范围

Web网关应能统计每一用户的详细使用情况，记录信息内容至少包括：

——源 IP，端口；

——目的 IP，端口；

——URL；

——MSISDN；

——终端型号；

——浏览器 User-Agent 信息；

——原始的和优化后的数据包大小；

——http 状态码；

——内容类型；

——请求方法；

——处理时间；

——时间戳；

——优化信息；

——Session ID。

6.2.3.2 统计分析

Web网关的统计分析功能单元能对采集到的日志记录进行统计分析后，支持通过特定的接口输出到外部数据库及报表工具。

为了保证统计分析结果的有效性和一致性，统计分析功能单元应该有相应的处理机制，确保日志记录的提取和分析处理不会相互造成影响。

当统计分析功能单元或系统发生故障或中断时，Web网关对日志记录进行保存。待统计分析功能恢复后，中断期间未处理过的日志记录能够继续被处理和分析，以达到统计数据的完整性和有效性。

6.2.3.3 统计报表

Web网关应具备生成相关统计报表的功能。

统计报表需要支持以小时、天、月、年为单位进行显示输出。

Web网关应支持按照用户级进行数据汇总统计，可以灵活地支持即席查询和统计报表的生成，用户级汇总结果至少包括以下内容：

——统计周期内用户访问量最多的前十名网站列表；

——统计时间段内记录用户最近访问的前十名网站列表；

——统计周期内，对指定的网站分类（URL 类别），该用户在不同网站分类上的访问请求频次列表。

Web网关应支持对网关整体运营情况进行统计分析，可以灵活地支持即时查询和统计报表的生成，统计报表结果至少包括以下内容：

——对用户的访问记录进行分析，获取访问量最多的网站列表；

——对用户的访问记录进行分析，获取访问量最多的设备类型列表；

——统计周期内访问用户数以及请求总数的报表；

——对指定的网站，获取访问量最大的客户端设备类型列表；

——对所有网站分类，获取访问量最大的类别以及用户数和请求数列表；

——对指定的网站分类，获取访问量最大的设备类型，用户数和请求数列表；

——对指定的网站分类，获取访问量最大的网站，用户数和请求数列表。

6.2.4 管理服务功能

6.2.4.1 用户 Profile 管理

Web网关应该能从HTTP请求报文中获取用户Profile，至少包括如下内容：

——用户主叫号码（MSISDN）；

——用户 IP 地址；

——用户终端 User-Agent（UA）；

——扩展参数，如承载类型、服务等级属性、签约带宽等等；

——Cookie：用户访问的 cookie 记录。

6.2.4.2 终端信息管理

Web网关应具备终端信息管理功能，能够从终端请求消息中获取到终端User-Agent，能到UAProf服务器或相关数据库查询终端设备Profile，用于确定重构适配的相关内容。Web网关对终端信息管理的要求如下：

a）终端类型库需包括但不限于终端描述、终端屏幕尺寸、终端对 WAP 和 XHTML 的支持以及终端对图像、媒体文件的支持等信息、硬件（CPU，内存大小等设备物理属性）、操作系统类型及版本（Symbian, Linux 等）、应用软件信息（浏览器类型及版本等）；

b）终端库需提供图形化的配置和管理界面，允许添加、删除、修改终端类型数据；

c）终端库需能够从厂家的支持站点下载最新的终端信息，并合并到本地终端库中；

d）终端数据库中支持根据 User-Agent 字段进行不同级别的终端类型匹配。

6.2.4.3 界面管理要求

Web网关应提供如下友好的管理界面：

——话单管理界面，对具备相应权限的管理员提供话单的查询、删除等功能。

——日志管理界面，对具备相应权限的管理员提供对 WAP 网关产生的运行日志和操作日志进行查询、删除等功能。

——局数据管理界面，对具备相应权限的管理员支持对局数据下载文件查询、局数据下发报告重传次数配置、局数据生效状态查询/删除、局数据文件上传等功能。

——管理员权限管理界面，支持对管理员角色、权限等分配等功能。

——性能查询界面，支持对当前系统的性能指标（至少包含主机 CPU、存储、磁盘空间和关键进程或者模块等的运行情况）进行查询等功能。

——各业务操作界面，对具备相应权限的管理员提供较高易用性的业务子系统管理界面，便于管理员对各个业务子系统进行日常操作维护等工作。

6.2.4.4 服务选择功能

Web网关应具备服务选择功能，控制应用服务平台上的各项服务应用，Web网关上通过一系列的工具实现对如下服务的控制和操作：

——内容适配服务：控制数据是否获得内容适配服务。

——内容过滤服务：控制数据是否获得内容过滤服务。

——内容加速服务：控制数据是否获得内容加速服务。

——内容增强服务：控制数据是否获得内容增强服务。

6.3 内容加速功能

6.3.1 概述

Web网关加速优化功能指提高诸如HTML内容、WAP2.0内容、FTP以及邮件传输的TCP/IP数据传递效率，提高门户浏览、普通网页访问和数据下载的速度和用户体验。Web网关需提供分类压缩、协议优化以及智能缓存等网络加速功能。

加速优化功能应支持无客户端和客户端模式，适用于笔记本、手机等不同类型终端的使用需求。

6.3.2 传输协议的优化

加速优化功能具备修改和调整TCP传输算法和规则的能力，以满足TCP数据在无线环境下的最优化传递，用于提高TCP数据从Internet侧到无线侧的快速传输。例如：加速优化功能应具备无论内容服务器关闭/打开与Web网关之间的连接与否，在数据传输过程中都能保持与终端的长久连接。

6.3.3 HTTP 应用协议的优化

Web网关针对HTTP/HTTPS应用协议，应具有显著优化效果，Web网关对HTTP协议的优化流程如图2所示。

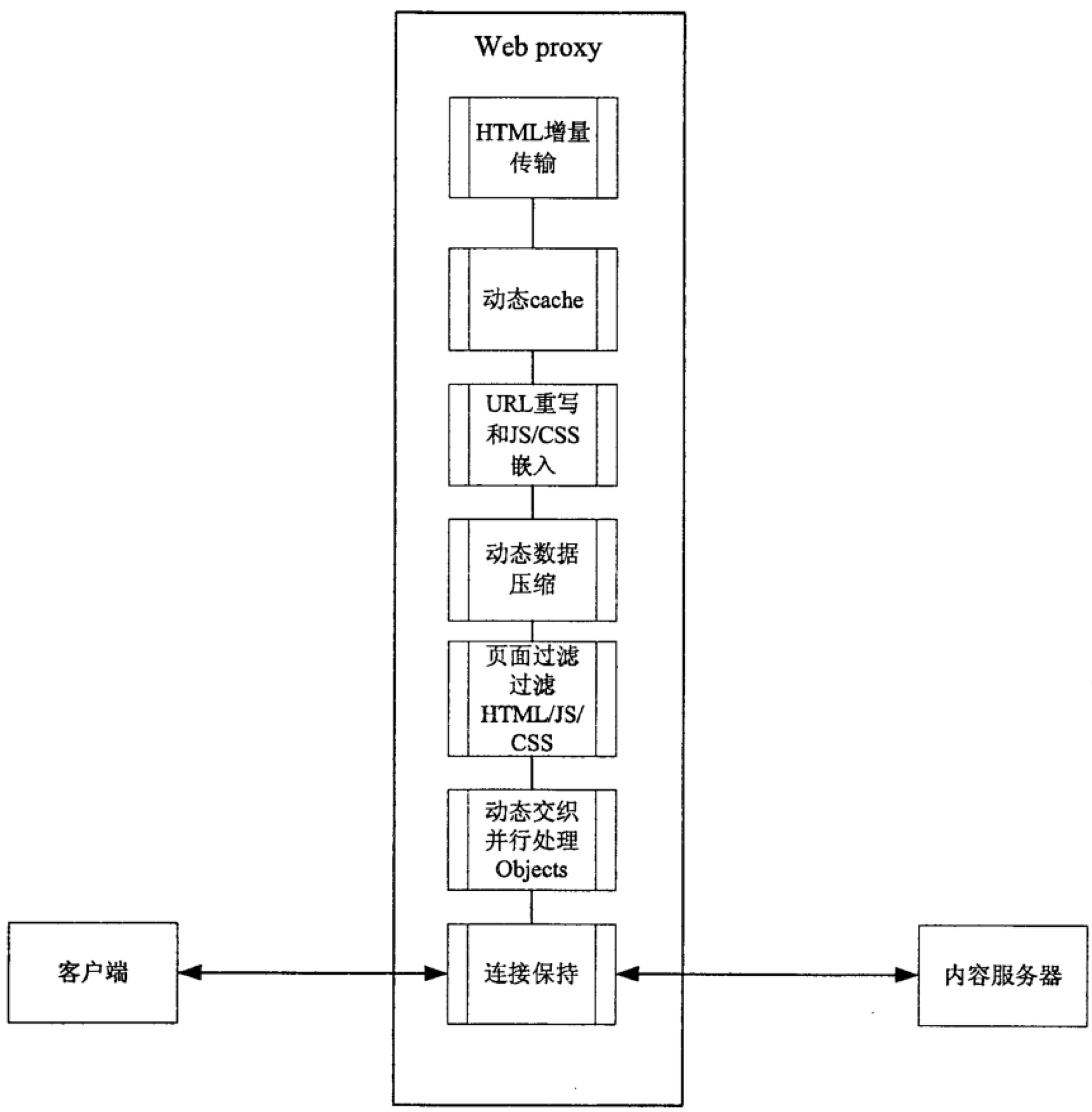

图2 HTTP协议优化流程

其中，Web网关对HTTP协议请求应至少具备以下优化流程，说明如下：

——连接保持。优化模块位于客户端与内容服务器连接的中间，分别与客户端和内容服务器建立数据连接，并且无论服务期端多次关闭/打开链接，其与客户端始终保持一长效连接，保证持续传输数据。

——动态交织，并行处理 Object。优化模块通过与客户端建立的长效连接，使得后者发送多组 Object 请求，实现并行请求，并行下载，并行传输，改变原先正常 HTTP 一次请求 2~3 个 Object 的方式，使传输由串行改为了并行。

——页面过滤。优化模块将 HTML，JavaScript，CSS 中原有的空白行、注释部分去除，减少在无线侧的数据传输。

——动态数据压缩。优化模块支持无损和有损的数据压缩。无损压缩主要针对 HTML 文本，txt，pdf，doc，ppt，xls 文件，采用终端浏览器支持的 Deflate，Gzip 通用压缩方式，保证数据传输的透明。有损压缩主要针对图片和多媒体对象，如 JPEG，GIF 和动态 GIF 图片，采用分级压缩，控制压缩级别，数值越低，压缩率越高，图片质量也就越低。

——URL 重写和 JS/CSS 导出。为了增加没有缓存情况下的页面首次访问速度，优化模块对 HTML 首页进行重写，内部的 JS 和 CSS 抽取放置到独立的 js 文件中。

——动态 cache。优化模块支持基于 HTTP1.0/1.1 的 cache，提高用户再次访问同一内容、同一对象所需的时间。对于图片，优化模块的 cache 将保存不同压缩级别的文件，向用户提供压缩过的和未压缩的不同对象。

——Web 网关与内容服务器的 HTML 增量传输。优化模块利用 HTML 或 XHTML 标记语言将 HTML 文本中发生变化的对象进行标注，使得再次传送时无需传送整个 HTML 页面而只是下载变化的对象即可，具体是结合 Web 网关动态缓存功能，对页面框架中发生变化的对象如图片、超链接等进行增量比对，仅将发生变化的对象从内容服务器获取，并替换到缓存中相应页面框架中，从而减少内容传输量。

6.3.4 数据和图像压缩

优化模块应根据业务需要对数据内容和图像进行压缩，从而降低在无线网络上传输的数据量，可节省网络带宽并降低网络延迟。

对数据和图像压缩的要求如下：

——优化模块至少需要支持 DEFLATE 和 GZIP 的数据压缩算法；

——支持对 JPEG、PNG、GIF、动态 GIF 等图像格式进行压缩处理；

——处理前后的图像质量比率可配置。

6.3.5 智能缓存

优化模块必须支持智能缓存能力，以加快内容的访问速度并节约网络资源，通过缓存Internet上的内容在缓存设备上，减少用户访问Internet时的延时，提升用户访问Internet上内容的速度。Web网关应支持以下智能缓存的要求：

——Web 网关应广泛支持各级对象的缓存，包括终端属性、用户属性、用户会话、用户页面对象、公共页面对象以及各类 Web 资源对象的缓存；

——系统应提供灵活的配置参数和策略选项，所有系统的缓存功能都基于缓存策略的限定，例如，缓存对象的类型、大小、有效期等，缓存应可被管理员手工清除；

——智能缓存需具有开关控制功能，打开开关时，启用智能缓存功能；关闭开关时，则禁止启用智能缓存功能；

——能缓存优化过/适配过的响应，能配置缓存内容的生命周期和能配置缓存内容的大小。

6.3.6 其他优化功能

Web网关提供的其他优化功能还包含：

——图片选择恢复功能。优化模块通过在优化过的 web 页面中增加对压缩图片的 Java script 脚本，使用户通过快捷键操作有针对性的获得原始未压缩图片对象，而无需重新下载整个页面和其中内容。

——对象预测下载（可选）。优化模块具备先于客户端发送 HTTP GET 请求，向内容服务器发送 HTTP GET，将页面中对象进行下载的优化技术，该技术需要优化模块配合 DNS 服务共同完成。具体是

指对同一页面内不同域名的对象，web 网关预先查询 DNS 并获取对象，同时重写页面中相关对象的 URL 并响应给终端，从而减少终端对 DNS 的请求次数。

——分类压缩算法。优化模块可根据终端设备能力以及用户设置，自动选择内容压缩算法，减少网络传输数据量，加快响应速度。

——Multipart 支持。优化模块应支持 Multipart 特性。当访问 Multipart web 资源时，网关能在一次交互的过程中取回所有相关资源并返回给终端，减少终端与无线网络的交互次数，达到网络加速的目的。

同时，也可以根据终端设备能力和请求上下文，对支持Multipart传输的设备，将网页内容和图像内容混合在同一会话中传输，减少不必要的会话，加速网页的展现。Web网关对重构后的页面分页，并进行缓存。当用户翻页时无需再次下载内容和进行重构分页。

——离线 Push 功能。Web 网关还可实现离线 Push 的功能。当接收 Push 消息的移动终端存在多个时，网关可逐个判断移动终端是否在线，如果在线，则将 Push 消息下发至所述移动终端；否则，通知网络侧发起包数据协议（PDP）上下文激活过程，将 Push 消息下发至激活成功的移动终端；如果激活失败，则记录相关信息；继续尝试发送，直到该 Push 消息对应的移动终端被全部尝试完毕，结束当前流程。

——对请求的处理。Web 网关可支持对业务请求的处理。Web 网关接收移动终端发送的请求消息，对请求消息进行处理，并记录对请求消息进行处理的时间。当时间超过预设请求超时时间，且没有收到或收全业务服务网发送的请求响应，则向移动终端发送保持会话连接的消息或重定向页面的消息。

6.4 内容适配功能

6.4.1 概述

Web网关的内容适配服务功能通过对Web页面进行内容重构、优化，实现移动用户在手机终端上访问互联网开放内容。内容适配功能将原始页面按照终端所能支持的程度重构为单一纵列，并保留原页面中主要对象，对于无法在单页显示的终端，适配后将分为多个子页面进行展示，并提供导航功能便于用户的使用。

对内容适配服务的适配规则要求能通过参数配置的方进行修改，并提供图形化的配置管理界面。

6.4.2 支持的内容格式和标准

6.4.2.1 页面内容格式适配要求

Web网关应支持如下的页面内容格式适配要求：

——内容适配功能需要支持将如下页面和对象格式进行适配：HTML、XHTML-MP、XHTML、WML、CSS 版本 1 和 2；

——可以根据用户设置启用或禁用网页内容适配；

——可根据设备屏幕分辨率，进行页面结构适配，将平面的 Web 页面转换为适应手机屏幕的垂直页面，方便用户无需横向滚动即可浏览所有网页内容；

——在内容适配过程中，可根据设备内存大小，自动对网页进行分页处理；

——支持分页后在网页头尾加入页面导航链接，方便用户进行翻页；

——支持自动添加和去除 CSS 元素，保证转换后的页面的显示效果。

6.4.2.2 图像格式适配要求

Web网关应支持如下的图像格式适配要求：

——内容适配功能需要将如下格式的图像进行大小调整和优化：GIF87、GIF89a、JPEG、BMP、ICO、

WBMP、PNG；

—— 适配之后的输出格式为 JPEG，PNG 和 GIF，同时将在适配后的图像下增加“图片下载”链接，用户可在此链接中选择不同大小的图片进行下载；

——可以根据用户设置进行图像文件的转换，图像转换选择包括不转换、适应设备屏幕、显示略缩图以及不显示图像等；

——图像转换质量可设置为高中低三个级别。

6.4.2.3 文字格式适配要求

内容适配功能按照不同终端类型提供适配后的页面字体，并可根据需要进行修改，字体大小划分等级为大，中，小。

6.4.2.4 标题提示

适配后支持增加标题提示功能，在适配后的首页及各子页上显示同一标题内容，如“(1/5) CNN News”。

6.4.2.5 表格适配要求

内容适配功能可根据终端支持情况，在适配后的页面中保留原有表格格式，同时为了避免横向浏览，也对表格进行重构，最大限度地显示在终端屏幕中。

对不支持Table元素的设备，自动将表格转换为Div方式显示。

6.4.2.6 支持多媒体对象访问

结合Web网关的多媒体适配服务功能，适配后的页面中提供访问多媒体对象的链接，用户点击链接后自动转到多媒体适配服务功能中进行多媒体适配和播放。

对于不支持Web网关多媒体适配服务的，可显示多媒体资源图片。如音频播放器图片或视频首帧图片。

6.4.2.7 支持的 JavaScript 格式

Web网关支持将原始页面中JavaScript进行分类，分成交互式和静态式（非交互式）两种，对于静态式JavaScript，Web网关采用去除原JavaScript代码，直接展现内容的处理方式。对于交互式JavaScript，Web网关将通过C/S模式的JavaScript代码或增加外部超链接形式模拟原有的交互式JavaScript，通过在Web网关系统端实现对JavaScript操作的模拟过程。

6.4.2.8 Cookie 的支持

内容适配服务功能支持长久的、用户个性化cookie存储，并在新的访问中根据用户调用其所属cookie进行内容适配服务。

6.4.3 支持安全站点适配和控制

内容适配功能支持对安全站点的适配，运营商可进行安全站点适配与否的配置：

——如果不启用安全站点适配，连接保持在用户终端与安全站点之间，Web 网关不会对安全页面做任何的修改。当 Web 网关识别出安全页面后，将其直接透传给用户。

——如果启用安全站点的适配，终端用户与安全站点的连接将变为两段：一段为终端用户与 Web 网关之间建立的通道，终端用户到内容适配模块使用 HTTP 协议并得到适配，Web 网关将把适配后的非安全页面送到用户终端，该通道的安全性可转由运营商网络的安全性来获得保障；另一段为 Web 网关与安全站点建立的安全连接，形成加密通道。

Web网关应并提供不同适配规则的控制：

——运营商级别的控制：

- 支持全局控制安全站点适配与否；
- 支持控制某一安全站点适配与否。

——用户级别的控制和提醒：

- 支持总是对安全站点进行适配的选择；
- 支持从不对安全站点进行适配的选择；
- 支持提示选择，是否对当前访问的安全站点进行适配。

6.4.4 支持手机终端的热键操作

内容适配服务功能应具备在适配页面中插入热键操作功能，用户在手机终端上使用特定键即可实现特定功能的操作，如转到上一页或返回上一站点等。

对于部分事先已定义热键操作的终端手机，则此功能不适用。

6.4.5 支持的终端库

Web网关内容适配服务功能具备涵盖所有类型手机的能力，具体如下：

——支持 XHTML-MP 的 WAP 2.0 终端；

——支持 Full-HTML 的智能终端。

6.4.6 多媒体适配服务功能

6.4.6.1 多媒体格式转换功能要求

Web网关能够支持将网页中的多媒体文件格式转化为手机能够支持的多媒体文件格式。如将Flash视频转化为Mpeg4格式。

Web网关应支持以下多媒体格式的发现：

——支持使用 Sorenson 或 VP6 视频编解码和 MP3 音频的 Adobe Flash 视频，并通过 HTTP 协议以 flv 视频格式进行传输。

——支持所有 Windows Media 视频编解码格式包括 WMV1、WMV2、WMV3、VC1、WMV1 和 WMV2 视频编解码格式，并通过 ASF、WMA、WMV 或 WM 承载的格式进行传输。

——支持使用.3gp、.3g2、.mp4、.m4a、.m4v、.mp3 承载通过 HTTP 传输的多种标准编解码格式包括 H.264、MPEG2、MPEG3、MPEG4、MP3、AAC、AAC+。

——支持通过 HTTP 和广播流协议传输的 MP3 音频。

——支持 HTTP 传输任意标准承载的 AAC/AAC+/MP2 音频。

Web网关支持转换后的多媒体格式为：

——视频格式：

- MPEG4 Part2 Video ISO/IEC 14496-2；
- MPEG4 Part 10 Video (a.k.a. Advanced Video Coding (AVC))；
- ISO/IEC 14496-10:2005；ITU-T H.264。

——音频格式：

- MPEG4 Audio，Low-overhead MPEG-4 Audio Transport (LATM)；
- ISO/IEC 14496-3 (Coding of MPEG 4 audio-visual objects)；

- Advanced Audio Coding Low Complexity (AAC – LC)。

6.4.6.2 多媒体格式下载功能要求

对于无法进行转换的格式，Web网关支持在资源所在的位置提供多媒体文件的下载链接。

6.4.6.3 动态带宽修整

多媒体适配模块为了流畅、平滑地播放视频片断，需支持动态带宽修整技术。

通过动态带宽修整，多媒体适配模块可避免在网络带宽降低时导致的视频播放停顿、抖动问题，它根据与终端在播放过程中交互 RTCP 的接收和发送信息报告，诊断网络质量，当发现网络速率降低时，自动地将视频播放的最大速率调低，保证视频流畅播放；当网络质量恢复之后，则自动恢复播放速率，视频播放不受到网络变化的影响，使用户得到最优的体验效果。

6.5 内容增强功能

6.5.1 广告插入

Web网关支持对运营商定制广告内容的插入，并提供图形化的管理工具，可方便的订制在浏览页面中插入的广告内容以及形式。广告来源可以通过第三方平台进行获得，Web网关只负责对相关的广告信息内容进行页面上的插入，包括如下内容：

——广告类型：包括文字广告、图片广告、多媒体广告、间隙广告等。

——广告插入类型：根据时间控制广告插入内容、根据终端类型控制广告插入内容、根据无线网络的不同访问点（APN）控制广告插入内容、根据目的 URL 控制广告插入内容。

——广告管理：包括广告合约管理、广告内容管理、广告属性管理、广告结算等。

6.5.2 定制信息插入

Web网关应支持对运营商定制信息的插入，包括：

——支持插入运营商 Logo；

——支持插入运营商自有业务及合作网站信息；

——支持插入用户信息：包括用户账单、流量等信息。该功能需要与帐务系统集成实时获取客户账单和分组数据流量；

——支持插入搜索框。

6.5.3 工具栏页面插入

Web网关应支持对工具栏页面的插入，工具栏页面包含各种浏览工具，如链接到导航主页，收藏夹，用户设置等。

Web网关应提供图形化的工具，方便的定义和集成现有的附加服务，并可以通过图形化管理工具，方便的维护工具栏页面中的内容和展现形式。

6.5.4 内容重定向

Web 网关应支持内容的重定向。网关在收到用户终端的页面请求时，向 SP 请求该用户终端所请求的页面，如果该 SP 返回的页面符合页面重定向条件，则网关代替用户终端进行页面重定向，并将重定向后得到的页面返回给该用户终端。页面重定向条件为页面中包含表示需进行重定向操作的重定向系列状态码，或者页面中包含“onenterforward”标记。网关通过对 SP 返回的页面中的“Cookie”信息进行保存。

6.5.5 内容重构

Web 网关应支持对内容的重构。内容重构过程如下：

——网关接收业务消息，识别业务消息的协议类型；

——根据协议类型的识别结果进行协议适配；

——根据业务消息对应的内容重构策略对协议适配后的业务消息进行内容重构，发送内容重构后的业务消息。

6.6 内容过滤功能

6.6.1 概述

Web网关必须具备内容过滤服务功能，内容过滤服务功能模块可以集成到Web网关中，也可以作为Web网关的内容过滤中心，通过ICAP接口与Web网关相连接提供相关服务。内容过滤模块的实现应该遵照YD/T 2055-2009的规定来进行，除此之外，本标准做如下的补充说明。

6.6.2 内容过滤规则配置模块

该模块作为内容过滤服务的核心部分，定义用户匹配的过滤规则和过滤措施，并作为内容分类数据库和加速服务功能中HTTP代理的接口，实现实时地动态内容过滤，同时也支持将被拒绝的访问请求重定向到特定提示页面。

6.6.2.1 网站过滤规则

网站过滤支持四种类型的过滤规则，每一种规则都支持定义黑名单和白名单，并根据规则执行相应过滤操作。

——基于内容类别的过滤规则：

- 支持查看既有的网站类别数据库（可支持集成第三方网站类别库），如新闻、艺术、体育等。
- 支持根据 URL 类别创建过滤规则，通过对不同内容类别定义规则和动作，可将不同类别的内容选择特殊的过滤操作，并支持重定向到指定的提示页面。

——基于 domain 后缀的过滤规则：

- 通过定义特殊 URL domain 后缀，如 yahoo.com, 定义过滤规则和操作，所有匹配该规则的 URL 都将执行过滤操作。

——基于 URL 目录前缀的过滤规则：

- 通过定义目录前缀，如/personals,所有包含此前缀的 URL 都将匹配该规则，并执行相应过滤操作。

——基于嵌入 URL 的过滤规则：

- 嵌入 URL 的过滤规则优先于其他过滤规则执行。
- 通过创建嵌入 URL 的过滤规则，提供符号分析规则辨认嵌入的 URL，提取出嵌入的 URL 同时进行相应过滤操作，可以过滤嵌在特殊 URL 中的黑、白名单页面，执行相应过滤操作，关闭绕开内容过滤的“后门”。防止终端用户通过缓存网站、代理网站等绕过内容过滤规则。

6.6.2.2 根据内容类型过滤

Web网关应支持根据内容类型进行过滤：

——提供内容类型设置功能，可以根据 MIME 类型（content-type）标识欲访问的内容的类型，访问黑名单中的内容类型时禁止访问。

——考虑带宽和响应速度，只对某些站点开放可以访问全部内容，其他站点，如一些免费知名站点，过滤其中的 java，下载图片，声音等内容。

6.6.2.3 根据时间段过滤

时间段过滤要求支持两种类型的过滤规则：

——支持定义在某段时间内哪些网站不能被用户访问，规则所包含的数据有网站的域名和时间段信息。

——支持定义在某段时间内哪些用户不能访问网站，规则所包含的数据有时间段信息和用户的MSISDN号。

6.6.2.4 根据用户信息过滤

Web网关应支持基于用户提供的一项或者多项属性信息定义过滤规则，规则的数据包括用户属性的集合和网站的域名信息，用来表明具有这些属性的用户不能访问的网站。

6.6.2.5 根据黑名单过滤

黑名单过滤要求支持两种类型的过滤规则：

——支持网站黑名单，位于网站黑名单中的网站不能被任何的用户访问，黑名单中包括网站的域名信息。

——支持用户黑名单，位于黑名单中的用户不能访问任何的网站，黑名单中的每个项包括用户的MSISDN。

6.6.2.6 Push 消息发送过滤

Web网关支持对于垃圾Push消息的阻止，承担推送代理网关的功能。

Web网关应保存两张对Push消息发起者鉴权表。第一鉴权表用于鉴权网关是否信任Push消息发起者，第二鉴权表用于鉴权目的终端是否信任Push发起者。当Push消息由发起者发送到网关，由网关控制并转发到目的终端，Web网关对Push发起者进行鉴权，如果发起者通过第一和第二鉴权表的鉴权，则将接收到的推送消息发送到目的终端，否则丢弃此Push消息。

6.6.3 内容过滤接口

Web网关应提供内容过滤接口，该接口用于Web网关以及外部运营商服务获得对用户Web访问的过滤结果，包含基于标准的ICAP接口，该接口可从外部系统作用于过滤请求。

6.6.4 网站内容分类数据库

Web网关应提供基于URL的访问内容分类，将网站或页面按照URL划分到某一类别中，使得过滤模块对其加载过滤规则。

该内容分类数据库可通过外部网络进行在线升级，并结合管理系统可实现定时升级，也可在管理系统界面中导入第三方定义的特殊类别如IWF（Internet Watch Foundation）定义的Illegal类别。此外，还支持创建自己定制的类别，用于特定的过滤规则实施。

6.6.5 过滤规则管理系统

Web网关的内容过滤模块应支持图形化或基于Web GUI的内容过滤规则管理系统，可运行在不同操作系统之上，通过该界面配置复杂的过滤规则，可以对过滤规则进行导入和导出。同时提供日志查看、管理功能，不仅可以查看实时和历史事件日志，也可以获得规则匹配的统计信息。

7 性能指标和可靠性要求

7.1 可扩展性

Web网关应具备以下可扩展性要求：

——内容适配和互联网访问服务器要求可以物理单独部署（物理上独立的服务器或服务器群），并可以独立线性扩容；

——要求具备高可扩展性，能够按照分布式多机处理的结构进行部署，以满足大规模并行处理的要求；

——要求能够按照一定的规则进行负载均衡处理；

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

——Web 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 地址设置，即可对网关进行扩充；

——Web 网关应具有热扩容能力，即不需关机就可进行扩容的能力。

7.2 可靠性要求

7.2.1 备份和恢复要求

系统对关键数据和配置文件应具备一定的备份措施，且在备份过程中保证数据的安全性和完整性。保证系统的不间断运行，系统应具有软件、硬件故障的在线恢复能力。

系统应有良好的备份和恢复策略，系统数据和业务数据可联机备份、联机恢复，恢复的数据必须保持其完整性和一致性。

7.2.2 容灾要求

网络设备应保证7×24小时不间断运行，系统应具备灾难预防机制。

系统应支持多站点架构的组网方式，实现网络设备在物理上的冗余和灾难预防。

Web网关应支持典型的组网结构如：每个单独的站点以集群方式配置，两个（或多个）冗余站点之间互为备份，形成多站点组网架构。网络设备如果出现但站点故障时，在备份站点能够承担所有的网络流量的正常处理任务，直到故障站点恢复正常。

7.2.3 稳定性要求

Web网关系统为了保障稳定运行，应具备在软、硬件故障或通信中断等情况下的容错和故障自动恢复能力。

Web网关应支持典型的容错机制如：进程自动重启与恢复、系统后台接入与操作、软件故障预防与告警、软件备份模块的自动接管等。

8 接口要求

Web 网关与其他网元之间的接口如图 3 所示，描述如下：

a）Web 网关与互联网内容服务器间的接口：通过 HTTP 协议连接到 Internet，支持安全连接，完成与互联网间完成业务信息交换。支持各种 Internet 协议与端口的访问。

b）Web 网关与 WAP 网关之间的接口：通过 HTTP 协议实现，WAP 网关根据 UA 信息将用户的互联网浏览请求与其他应用数据分开，传送到 Web 网关进行适配、加速优化处理，并通过 HTTP header 传送用户状态信息如 IP 地址，MSISDN，User-Agent 等。

c）Web 网关与网管间的接口：通过该接口网管信息的交互，实现网管中心对 Web 网关的集中管理，采用 SNMP 协议。支持 SNMPv1/v2/v3，可以连接基于 SNMP 的上级网管系统。

d）Web 网关与 DNS 的接口：实现基于 IP 的 DNS 域名解析，采用 DNS 协议。

e）Web 网关与 NTP 的接口：通过 NTP 统一系统时间。

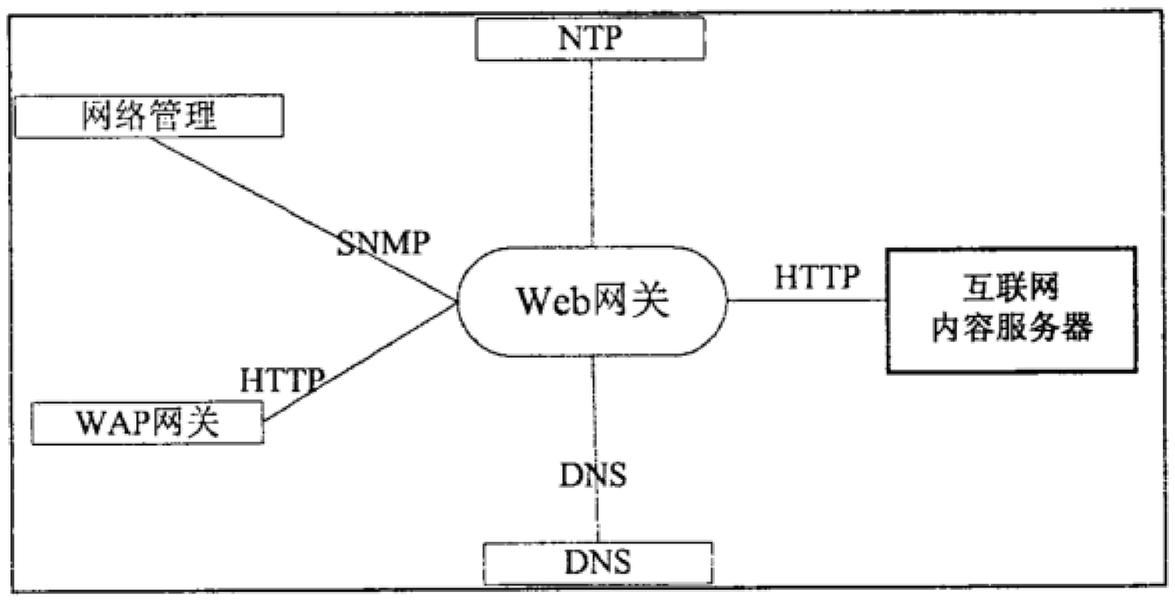

图3　Web网关与其他网元接口图

9　网管要求

9.1　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。网络管理的设备列表如下：

——网络设备；

——主机设备；

——存储设备；

——网络安全设备。

9.2　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，Web网关内部应用服务平台、负载均衡器、防火墙等网络设备须采用标准的SNMP通信协议。

9.3　网管接口信息模型

Web网关应用服务器、负载均衡器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。应支持基于SNMP协议以准实时方式向外围设备提供网络管理数据统计结果的功能。

9.4　网管功能

9.4.1　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。

——业务配置项的修改要求实时生效，如内容过滤规则配置等。

——对配置操作过程的记录统计。

——提供 Web 页面作为配置管理界面。

——支持配置内容的备份和恢复。

——支持配置内容核查。

——支持配置内容导入、导出。

——配置内容要相对独立，设备的升级不应该引起配置内容重新配置。

9.4.2 故障管理

故障管理负责监视Web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。

——自动监控：

- 可对设备的 CPU、内存、磁盘空间进行自动监控，当资源达到告警值时自动产生告警；
- 可自动监控进程的 CPU、内存、句柄数；
- 可自动监控话单的错误码；
- 可自动监控设备长时间无话单输出；
- 可自动监控设备的关键性能指标；
- 提供图形化界面查看所有自动监控任务；
- 提供图形化界面修改自动监控任务的监控周期、监控阀值。

——告警管理：

- 告警管理主要包括当前告警、历史告警的管理，告警过滤、告警适配等功能；
- 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）。

9.4.3 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。要求如下：

——对管理者实现身份鉴别机制。

——对管理者的管理范围进行划分。

——对关键数据实现备份。

——对管理操作进行记录。

9.4.4 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：当前性能监视、历史性能分析、性能控制、KPI的定义和管理。

a）性能监视对 Web 网关进行监控和轮询，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，如：

——集群性能指标；

——用户业务请求次数；

——事务数量；

——数据库访问错误数；

——License 超限数量；

——HTTP 业务流量；

——数据连接数量；

——数据流量流向统计。

b）性能分析对业务流量曲线（包括流量和流向）进行分析，如：

——日均用户曲线；

——非正常终止原因及出现概率等；

——闲时概率；

——忙时概率；

——用户平均每一次使用时长。

c）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。修改网元设备相关参数以优化性能。

d）KPI 的定义和管理。

9.4.5 同步要求

要求Web网关系统内部的所有服务器的时间必须同步。

全网的所有Web网关系统之间的时间必须保持同步。

Web网关系统和它连接的各个网元设备之间的时间必须保持同步。

时间同步精度达到100毫秒。

同步的源来自时间同步网。

设备具备自动在线时间校准功能。

9.5 日志管理

网管系统需要对Web网关业务系统的运行状况进行日志记录及管理。

日志包含三类，分别是Web网关业务系统日志、操作系统日志和配置生效日志。

——Web 网关业务系统日志：记录管理员对 Web 网关业务系统的操作，包括登录、退出业务系统，以及对业务系统的增删改等操作。

——操作系统日志：记录管理员对操作系统的操作，包括登录、退出操作系统，以及在操作系统命令行中键入的操作命令。

——配置生效日志：记录管理员对 Web 网关的关键配置文件、关键配置项的增删改等操作。

要求Web网关能将Web网关业务系统日志、操作系统日志和配置生效日志通过HTTP方式发送到第三方日志服务器上。

要求传送Web网关业务系统日志、操作系统日志、配置生效日志的模块必须在超级用户下运行，并且实时传输的时间粒度可配置。

当第三方日志服务器出现超时等现象时，允许Web网关业务系统、操作系统及关键配置的当次更改生效，并要求Web网关能自动告警。要求第三方日志服务器恢复正常工作状态后，Web网关能将第三方服务器出现超时等现象期间的操作日志重新发送到第三方日志服务器上。

10 计费

10.1 话单要求

Web网关本身不作为计费网关，但是它应提供必要的用户话单数据以便于追踪和核对。

Web网关提供以下几个方面的话单内容，应支持产生原始计费信息的功能。Web网关产生的原始计费信息中应至少包括：

——主叫号码/用户帐号；

——用户 IP 地址；

——用户访问的 URL；

- 用户访问该 URL 时的信息流量；
- 用户访问该 URL 的开始时间；
- 用户访问该 URL 的结束时间；

——内容类型：访问内容的媒体类型；

——Web 网关 IP 地址/标识；

——接入方式标识（GPRS/EDGE 方式，TD-SCDMA 方式，WCDMA 方式，cdma2000 等）。

对于原始服务使用记录，应支持如下存储功能：要其至少在线存储90天，脱机存储至少6个月，能够支持磁盘容量告警。

能够将原始服务使用记录生成原始话单文件，定时定量传送给外部网元，时间长度和文件大小应可配置。文件传送接口支持FTP和FTAM协议。

Web网关的计费精度应为流量精确到1字节；时间精确到1秒。

10.2 计费支持

Web网关支持实时流量计费费用提示功能，网关可获取流量计费信息，根据所述流量计费信息构建PUSH推送消息，并发送此PUSH推送消息至用户终端，根据用户终端对该PUSH推送消息的反馈，网关进行相应的数据处理。

Web网关实现对实时内容及流量计费的支持。在网络系统中，包括网络接入设备和计费部件，还包括路由平台和Web网关，Web网关作为协议解析部件。其中，路由平台接于网络接入设备与协议解析部件之间。路由平台对网络接入设备传来的报文进行分类，对于需要对其进行内容解析的每一个报文，则根据该报文的类别将其转发至相应的协议解析部件；如果判断不需要对报文进行内容解析，则在路由平台上进行普通流量累计，并定时定量触发给计费部件。协议解析部件对来自路由平台的报文做深层次的协议解析，对于需要对其进行内容计费的每一个报文，则解析出内容计费需要的业务信息并上报至计费部件；如果判断不需要对报文做深层次的协议解析，则在协议解析部件上对其进行普通流量累计，并定时定量触发给计费部件。计费部件用于完成内容和/或流量计费。

对于预付费用户的计费控制，Web网关可根据预付费用户的不同业务请求，与计费系统进行相应的信息交互，并根据交互的信息进行相应费用的采集和控制。

在业务开展中，当移动用户与SP/CP建立连接后，由SP/CP向Web网关发出计费请求，网关根据计费请求中的业务种类来决定向业务控制点上报内容计费信息和/或流量计费信息，业务控制点根据网关上报的计费信息进行内容计费和/或流量计费。

11 软硬件要求

11.1 Web 网关设备的软件和资源要求

Web网关设备软件和资源要求如下：

——Web 网关设备应采用安全度高的操作系统软件；

——Web 网关设备所在网络中应能够与 DNS 服务器、NTP 服务器、LDAP 服务器、Radius 服务器等信息系统实现互联互通；

——Web 网关设备所在网络中的业务数据流须完全经过该网关设备，即无线终端到 Internet 以及 Internet 返回到无线终端的双向数据都需要经过 Web 网关设备；

——Web 网关中每一功能模块都具有外部和内部健康检查机制，确保所有功能不受软件故障而中断。

11.2 Web 网关设备的硬件要求

Web网关设备硬件要求如下：

——Web 网关设备通常包含功能服务平台、负载均衡器、防火墙以及必要的网络设备；

——Web 网关设备中所有硬件设备应具有冗余或双机主备用配置；

——Web 网关设备中的功能服务平台应支持性能强大的多核处理器硬件，并支持具有扩展性强的集群式(Cluster)部署方式；

——Web 网关中的每一功能服务模块都具有 N+1 或者双机硬件的冗余硬件配置，同一功能软件分别运行在独立的硬件平台之上，一旦某台发生软件故障，其他同类型节点可接管并继续执行；

——Web 网关还配有负载均衡器设备，用于在功能模块外部进行冗余保障；

——Web 网关无论内部连接还是外部连接，都采用冗余链路配置，确保网络链路的冗余；

——硬件应采用模块化结构，便于容量扩充和引入新的硬件模块容纳新业务和新技术；

——设备平均无故障时间应大于 26280 小时；

——主机的处理能力要求能满足业务应用和用户规模的需求，系统设计时应考虑 30%的性能冗余；

——内存容量的配置要考虑到主机在正常运行状态下的内存利用率不应大于 70%，保证系统在业务高峰时仍具有较强的抗冲击能力；

——主机应支持高速连接接入核心局域网；

——主机的硬盘、网络接口、网络连接及电源均应考虑足够的冗余。

12 操作维护要求

12.1 安全性

Web网关安全性要求如下：

——需要支持网络级安全：能通过防火墙实施一定的安全策略；

——需要支持系统级安全：支持关闭平台不必要的服务，减少可能引起安全问题的原由；

——需要支持应用级安全：具备必要的防病毒软件；

——采取一定的认证和授权机制，杜绝无权操作人员进行操作，规范管理人员的行为；

——需要支持配置及修改各管理用户的管理范围；

——应对于关键的服务器进行冗余备份；

——需要有用户级权限管理，管理整个平台的用户级别；

——需要能够对访问平台的客户进行 IP、MAC 地址等限制；

——需要提供几类不同的备份/恢复策略，如系统级、应用级和数据级；

——需要提供操作人员的详细操作日志。

12.2 可管理性

Web网关应提供如下功能，实现可管理性：

——应用系统应提供完善的审计功能，对系统关键数据的每一次增加、修改和删除都能记录相应的修改时间、操作人和修改前的数据记录；应用系统的审计功能应提供根据时段、操作员、关键数据类型等条件组合查询系统的审计记录；

——应用软件的权限控制应要按照逐级管理的原则。

12.3 可维护性

Web网关应具备以下功能，实现可维护性：

——应用系统应采用组件化设计思想，系统框架与业务逻辑分离；要求具备开放的体系架构；

——应用系统应支持通过统一的图形界面访问系统各组件、接口的版本信息及相应的功能说明；

——应用系统出现异常错误报告时，必须能够提供详细的异常信息和明确的错误编号，并能在系统的相应维护手册中查到错误处理方法与步骤；

——当系统负荷加大时，应在不更改整个系统架构的前提下，确保服务的正常运行；

——应用系统必须支持各组件的单独升级，实现在线升级功能。应用软件中的任一模块更新、加载时，在不改变与上下模块接口的前提下，应不影响业务运转和服务。

12.4 易用性

Web网关应具备以下功能，实现易用性：

——应用系统必须提供统一的图形用户界面风格；

——应用系统应支持同时打开多个管理窗口以对不同任务进行并行的操作；

——在导致系统数据发生变化的操作执行之前，系统应明确提示用户确认；

——当应用系统正在执行用户提交的请求而无法返回时，应明确标识系统处于繁忙阶段；

——应用系统功能菜单应按照功能域、功能组的分类方法进行组织；

——对于操作员无权限使用的菜单功能，应用系统应不显示该菜单或将其设置为不可用状态；

——系统应提供在线帮助功能，对于每一个操作功能都能查找到相应的使用说明；

——操作员登录系统后，系统应能主动提醒等待该操作员处理的任务。

13 设备安全要求

13.1 物理安全

Web网关服务器放在运营商自有的机房，符合机房相关设备的物理安全要求。

Web网关设备电源和接地安全要求应遵循GB 4943.1中相关要求。

13.2 网络安全

网络安全方面应当支持访问控制、安全检测、攻击监控、操作审计等一系列安全功能，应提供完整的网络安全监控、报警和故障处理功能：

——网络应具备一定的冗余能力，带有关键性业务应用的网络链路应实现冗余，当出现故障时应支

持自动路由切换；

——网络应当划分合理的安全区域，如 INTERNET 区、业务功能区、数据库区、外部系统区等，并针对每个安全区域制定合理的访问控制策略，进行 IP 地址限制及端口限制；

——网络系统和服务器系统应具有入侵检测的功能，可监控可疑的连接、非法访问等，采取的措施包括实时报警、自动阻断通信连接或执行用户自定义的安全策略；

——网络和服务器系统应能定期检查安全漏洞，根据扫描的结果更正网络安全漏洞和系统中的错误配置；

——进行远程维护（管理）时应：

- 通过 VPN、令牌等方式进行接入认证；
- 维护（管理）操作数据流应经过加密，禁止明文传输；
- 远程维护（管理）操作须接入独立的审计系统进行审计，对操作内容进行存储。

13.3 系统安全

系统应关闭不必要的端口及服务，不安装不必要的软件。系统应在必要并经测试验证稳定运行的基础上，安装厂商发布的最新版本安全补丁等。系统应具有完善的日志功能，能够记录系统异常情况及其他安全事件。审计日志应至少保存1年。

13.4 信息安全

Web网关系统应具备用户对安全站点（如网上银行、网上支付平台等）的访问控制和风险提示机制，保证用户私密信息的安全。系统对安全站点的访问控制可以从运营商级别和用户级别分别进行控制和选择。

Web网关应能对用户的访问历史、邮件、网页插件、用户配置等信息，在系统或数据库中进行加密保存，防止用户私密信息的外泄。

Web网关与其他网络设备（如网管系统、认证/计费系统等等）应可以采用完整性校验、数据加密等方式来保证通信时的数据安全

系统应具备访问权限的识别和控制功能，对应用管理员、系统管理员、数据库管理员根据不同的应用需求提供多级密码。系统应能自动实现下列控制：

——防猜测口令功能，例如，系统登陆时需要输入验证码，或者当口令输入错误达到一定次数系统自动将帐号锁定并告警；

——具有验证密码复杂度功能，密码复杂度应达到：密码长度大于 8 位，密码是大小写字母、数字，以及特殊字符混合使用；

——应当具有定期强制修改密码功能，强制用户每 3 个月进行一次密码更改工作。

13.5 安全防护

由于Web网关需要与互联网相连，必须建立完善的安全防护机制，包括防火墙系统、入侵检测系统、病毒防范系统等。Web网关系统设备应具有电信级可靠、多种冗余、备份和集群处理机制功能，关键部件采用双备份配置。

Web网关应具有安全漏洞扫描、入侵检测、防病毒等功能：

a）安全漏洞扫描。工作方式在于主动进行扫描，找出系统中存在的安全漏洞和隐患，扫描对象包括两类：网络设备和主机设备，网络设备主要扫描防火墙、路由器等设备的配置是否存在安全漏洞，主机

设备主要检查操作系统是否存在安全漏洞。

b）入侵检测系统。实时监测系统中的数据包，对进出系统的网络流量进行检测，识别非法连接请求及网络入侵，自动阻断连接，报警并记录日志；通过分析关键服务器上的内核级事件、主机日志和网络活动，执行实时的入侵检测并阻止恶意活动。入侵检测的监测点为系统的互联点和系统与外部其他系统的连接点，也可以对每台主机进行检测。

c）防病毒。用于防止病毒在系统传播和扩散，病毒防护系统应具有网络病毒防护能力，可以动态升级病毒库。主要功能：病毒定义更新（自动/手动）；病毒检测（自动/手动）；病毒清除；病毒信息统计；病毒防御策略定制等。防病毒软件应至少每星期更新一次病毒库。

Web网关也要具备如下安全要求：

a）查询用户信息行为的记录和日志审计功能：由于 Web 网关系统掌握大量的用户信息，信息保密问题非常必要，因此设备本身应对登录、查询用户信息的行为进行记录，以提供日志审计的相关功能，确保记录日志的有效性和安全性。

b）对 DOS 攻击的防范和保障措施。

c）对用户权限、访问规则配置的管理和控制。

d）内容重构安全要求。

Web网关系统提供内容重构功能，可以对Web网页进行重新布局和构造，并对内容元素根据手机终端特点进行转换。因此，在内容重构过程中，如HTML转换，多媒体格式转换，须保证转换后的代码应为安全代码，不应出现被植入恶意代码或被入侵的安全漏洞。

14 电源要求

直流电压及其波动范围要求如下：

——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－57V～－40V。网关在此范围内应工作正常。

交流电压及其波动范围要求如下：

——单相 220V(1±10%)，频率 50Hz(1±5%)；

——线电压波形畸变率小于 5%。

中 华 人 民 共 和 国
通 信 行 业 标 准
数字蜂窝移动通信网 Web 网关设备技术要求
YD/T 2526–2013
*
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
宝隆元（北京）印刷技术有限公司印刷
版权所有　不得翻印
*
开本：880×1230　1/16　　2013 年 5 月第 1 版
印张：2.25　　2013 年 5 月北京第 1 次印刷
字数：57 千字
15115・224

本书如有印装质量问题，请与本社联系 电话：(010)67114922