

中华人民共和国通信行业标准

YD/T 3016-2016

面向移动互联网的业务托管和 运行平台技术要求

Technical Requirement of Internet based Service
Deployment and Operation Platform

2016-01-15 发布

2016-04-01 实施

中华人民共和国工业和信息化部 发布

目 次

前 言	II
1 范围	1
2 规范性引用文件	1
3 缩略语	1
4 面向移动互联网的业务托管和运行平台基本要求	1
5 面向移动互联网的业务托管和运行平台的功能框架	2
6 业务部署	5
7 业务请求处理流程	7
8 平台服务	10
9 安全性要求	12

前 言

本标准按照 GB/T 1.1-2009给出的规则起草。

本标准参考了《基于表述性状态转移（REST）技术的电信业务能力开放平台技术要求》中对业务运行环境的功能需求。

本标准参考了国内相关行业标准进行制定。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

标准起草单位：中国科学院计算技术研究所、中国联通网络通信有限公司、中国信息通信研究院、中国移动通信集团公司

标准主要起草人：李彦君、张国清、傅 川、谢健清、康 鹏、王志军、刘晓靖、吴 伟、王煜炜、杨 景。

面向移动互联网的业务托管和运行平台技术要求

1 范围

本标准规定了面向移动互联网的业务托管和运行平台的功能框架、业务部署流程、业务请求处理流程、平台服务和安全性等方面的技术要求。

本标准适用于网络运营商为第三方的基于移动互联网的业务提供业务托管和开放性接口服务。

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。

RFC2068	超文本传输协议——HTTP/1.1
RFC1738	统一资源定位符
ISO 9075:1989	具有完整增强的数据库语言SQL
JSR 53	Java Servlet 2.3和JSP1.2规范

3 缩略语

下列缩略语适用于本文件。

API	Application Programming Interface	应用编程接口
HTTP	Hypertext Transfer Protocol	超文本传输协议
IP	Internet Protocol	互联网协议
MIME	Multipurpose Internet Mail Extensions	多用途互联网邮件扩展
URL	Uniform Resource Locator	统一资源定位符

4 面向移动互联网的业务托管和运行平台基本要求

面向移动互联网的业务托管和运行平台是各种移动互联网增值业务的驻留和运行平台，能够动态地为业务提供运行所需的资源，并根据业务的实际资源使用情况计费，因此，业务能够随着访问量和数据存储需求的增长而轻松扩展。平台能够根据业务的访问量、存储需求等信息，动态分配系统的软硬件资源，将海量的业务高效、便捷地部署在统一的平台中，保障业务的可靠运行，不受节点加入和退出的影响。

开发者在使用面向移动互联网的业务托管和运行平台时，不需要自己维护任何服务器。开发者无需关心业务的部署细节，只要按照平台提供的应用编程接口和业务规范开发业务，使用平台提供的业务部署工具，即可将业务发布到平台中，实现一键式部署，真正做到业务在运营商侧的有效托管。

面向移动互联网的业务托管和运行平台需要具备以下基本要求：

- 海量部署：平台能够托管海量的业务，业务之间相互隔离，业务的运行不会相互干扰；

YD/T 3016-2016

- 一键部署：开发者不必关心部署细节，只需根据平台提供的应用编程接口和业务规范开发业务，并通过平台提供的业务部署工具，按照标准的业务部署流程，即可将业务发布到平台上；
- 高可用性：平台必须保障业务持久、不间断地运行，并且能够快速响应大量用户的并发请求；
- 可扩展性：平台能够根据业务的用户访问量以及资源使用统计情况等信息，动态地分配业务运行所需的资源；
- 管理便捷：开发者无需考虑平台的安全性、可靠性以及性能等其他因素，由运营商统一监控和维护平台和在平台上运行的业务；
- 按需计费：开发者无需一次性购买全部资源，而是根据实际使用情况计费。

5 面向移动互联网的业务托管和运行平台的功能框架

5.1 平台架构

5.1.1 概述

面向移动互联网的业务托管和运行平台总体架构如图1所示，其完整服务链至少应当包括前端负载均衡层、Web缓存层、动态路由层、业务运行层、平台服务层、平台监控层几个部分。

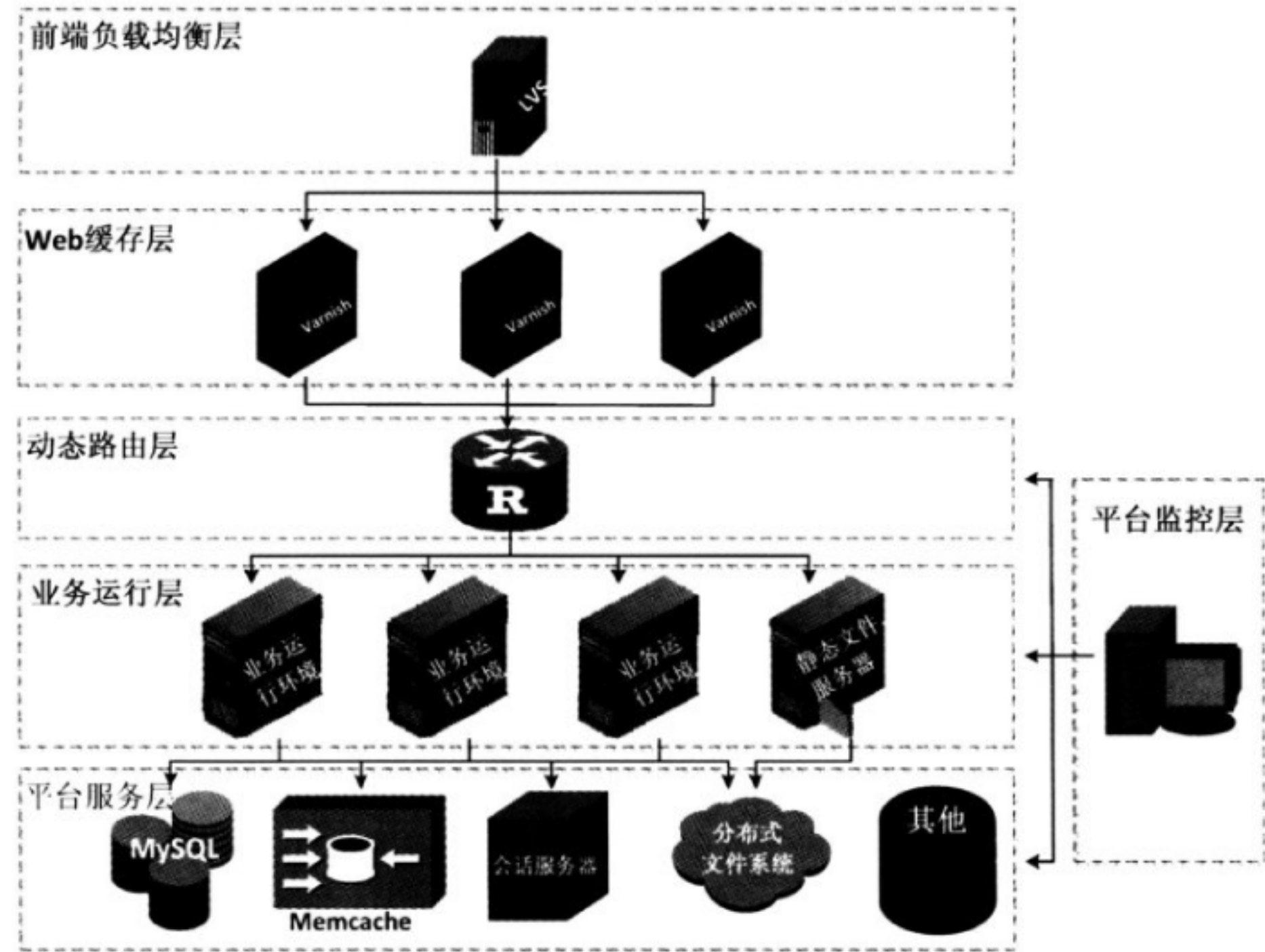


图1 面向移动互联网的业务托管和运行平台架构

5.1.2 前端负载均衡层

在面向移动互联网的业务托管和运行平台中，开发者的业务将部署在数量庞大的服务器集群之上，而前端负载均衡层是保证平台高效运行的重要功能组件之一。前端负载均衡层应满足下列技术要求：

- 对用户屏蔽平台内部结构，对外部世界表现为一个单独的“虚拟”服务器，并提供一个或者多个统一的网络地址，用以访问平台中托管的所有业务；
- 前端负载均衡层可将用户请求分发到 Web 缓存服务器之上。

5.1.3 Web 缓存层

Web缓存层是业务数据的临时存储场所，用于缓存数据，这些数据是先前平台响应业务请求操作的结果。如果用户请求的数据在Web缓存层中存在，则可以直接将Web缓存层中的数据返回，无需将请求转发到业务运行环境当中。由于业务托管和运行平台上部署了海量的业务，Web缓存层可降低部署在后端的业务运行环境的负载压力。

5.1.4 动态路由层

面向移动互联网的业务托管和运行平台上可部署海量的业务。每个业务运行环境中可以部署多个业务，一个业务也可以拥有多个运行实例，分别部署在多个业务运行环境当中。动态路由层需要保证机器级别的负载均衡和业务级别的负载均衡。动态路由层应具备以下的技术要求：

- 在保证服务质量的前提下，最大化利用服务器的性能，使得活跃的业务运行环境的数量最少，减少平台的开销。平台能够根据自身的整体负载情况，自动创建新的业务运行环境，或回收已有的业务运行环境。
- 一个业务运行环境上可以部署多个业务，一个业务也可以拥有多个运行实例，分别部署在多个业务运行环境当中，动态路由层需要保证机器级别的负载均衡和业务级别的负载均衡。
- 能够重用已经存在的用户会话，减少冗余的会话信息，提高平台的响应速度。

5.1.5 业务运行层

业务运行层为业务的运行提供支持。每一台应用服务器对应为一个业务运行环境。业务运行层的功能设计应满足以下的技术要求：

- 复用性，即单个业务运行环境可部署多个业务，单个业务也可以拥有多个运行实例，分别部署在多个业务运行环境当中，业务运行层应保证同一个业务的、部署在不同业务运行环境之中的运行实例之间的数据同步；
- 支持业务的隔离，保证各业务之间互不影响，并且能够在不同的业务运行环境之间动态地迁移业务。

5.1.6 平台服务层

平台服务层提供平台服务的实现，并以应用编程接口的形式提供给业务开发者。业务通过调用应用编程接口来访问这些平台服务。平台服务层应提供下列最基本的服务：

- 数据库服务；
- 分布式缓存服务；
- URL 访问服务；
- 任务调度服务；
- 大数据对象的数据库存储服务；
- 数据存储区服务；
- 多租户服务；
- 认证授权服务。

5.1.7 平台监控层

平台监控层是面向移动互联网的业务托管和运行平台的控制中心，应具备下列功能要求：

- 资源使用情况汇总功能，每个业务可以拥有多个运行实例，平台能够统计每一个运行实例的资源使用情况，并汇总为该业务的资源使用情况；

YD/T 3016-2016

- 业务生命周期管理功能，平台能够实时地根据业务的资源使用情况，动态创建新的运行实例，或者停止已有的运行实例；
- 动态路由网更新功能，平台能够根据业务运行实例的资源使用情况，动态调整用户请求的转发规则。

5.2 业务运行环境体系结构

业务运行环境可以划分为六个逻辑层次，从上到下分别是业务层、业务扩展层、业务驻留层、虚拟运行环境层、环境监控层以及操作系统层。这六个层次组成业务运行栈，提供一个可控、安全的业务运行环境。业务运行环境体系结构如图2所示。

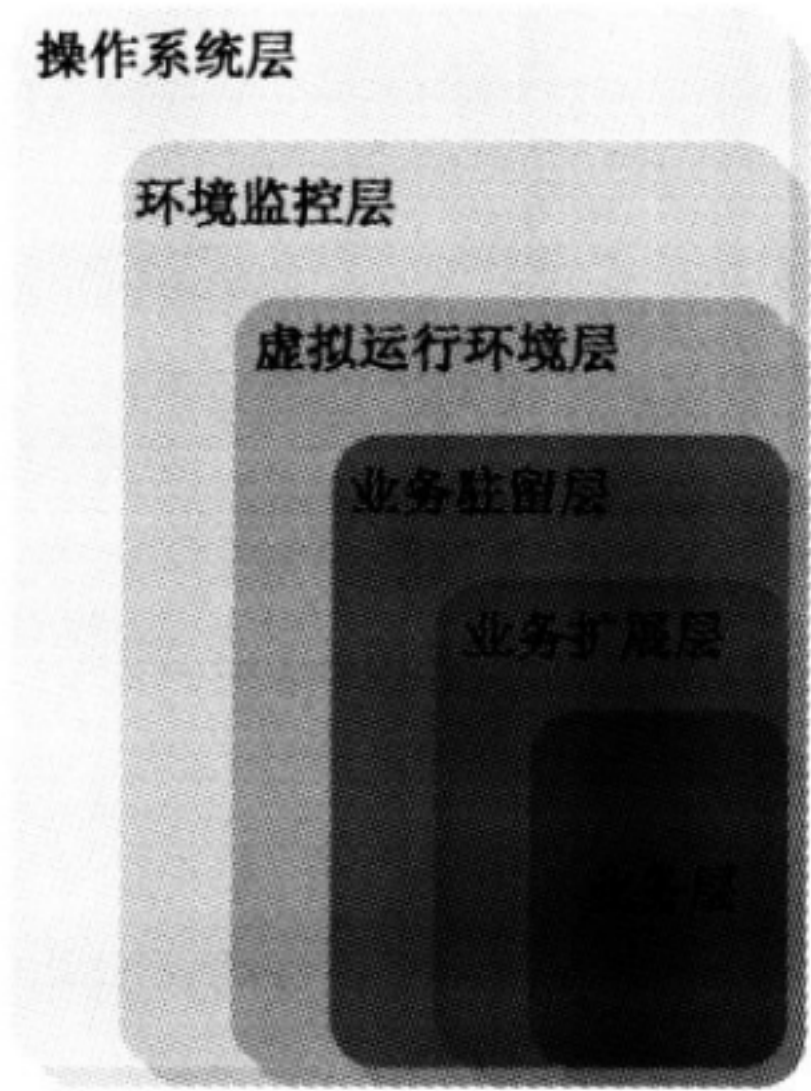


图2 业务运行环境体系结构

5.2.1 业务层

业务，即开发者开发并部署到面向移动互联网的业务托管和运行平台上的应用。业务可以在平台上部署的基本要求为：

- 使用平台支持的开发语言和开发框架；
- 符合平台对业务的安全性限制。

5.2.2 业务扩展层

面向移动互联网的业务托管和运行平台应当支持流行的应用框架和第三方库，例如Java开发框架struts、Spring、Hibernate等。同时，平台应提供访问平台服务的接口。平台服务以应用编程接口的形式提供给开发者。因此，平台应将对应用编程接口的访问转换成对相应平台服务的访问。

5.2.3 业务驻留层

业务驻留层负责运行业务，解析页面编程语言，响应用户请求并返回响应页面。

5.2.4 虚拟运行环境层

为保证面向移动互联网的业务托管和运行平台的安全性和稳定性，业务应当被隔离、并在受限制的运行环境中运行。虚拟运行环境支持不同业务的隔离和保护，保证业务之间互不影响、彼此安全，并且支持在不同的业务运行环境之间迁移业务。

5.2.5 环境监控层

环境监控层监控业务运行环境中每个业务运行实例的资源使用情况，包括CPU使用率、内存使用量以及网络带宽使用量等信息，并和平台监控层进行交互。环境监控层的基本功能要求如下：

- 环境监控层能够统计业务运行环境中每个业务运行实例的资源使用统计信息，并将统计信息发送到平台监控层，由平台监控层进行汇总，以统计业务的整体资源使用情况，用于支持对业务进行计费以及管理业务的生命周期；
- 环境监控层能够接受平台监控层的指令，创建新的业务运行实例，或者停止并回收已有的业务运行实例；
- 平台监控层可根据业务的汇总信息，统计业务运行环境的负载，并向环境监控层发送指令，调整业务运行环境中运行的业务。

5.2.6 操作系统层

操作系统是管理电脑硬件与软件资源的程序，同时也是计算机系统的内核与基石，其主要功能需包括：

- 硬件资源管理能力，即可对硬件资源如处理器、内存以及网卡等进行操作并使之透明地被用户使用；
- 进程管理能力，即对进程进行调度以及控制进程的生命周期；
- 文件系统管理能力，即屏蔽底层存储资源细节，使用户能够方便地以文件形式访问存储资源，无论该文件是在本地还是在远程分布式文件系统上。

6 业务部署

6.1 业务的创建

在将业务部署到面向移动互联网的业务托管和运行平台上之前，第三方开发者应先在开发者平台上注册业务，获取唯一的业务标识，并由平台自动创建相关联的远程仓库。远程仓库可支持业务资源的版本控制、用户代码存储以及代码所需资源文件的存储与管理。在进行业务部署时，指定业务所对应的业务标识即可。

6.2 URL 到业务标识的映射

系统可以支持三种不同的方法，用于将URL映射到业务标识。这三种方法包括独立域名方法、子域名方法以及子目录方法。

6.2.1 独立域名方法

独立域名，即该业务对应的域名与平台的域名无关。平台保存独立域名到业务标识的映射（见表1），直接根据独立域名查找对应的业务标识。如果业务请求采用独立域名，则应在HTTP请求的Host头部中指出该独立域名。

表 1 独立域名到业务标识的映射表

描述字段	示例	说明	备注
domainName	*.abc.com	表示独立域名	支持正则查找
appId	HelloWorld	表示该独立域名对应的业务标识	该标识为字符串序列，每一个业务均有唯一的标识

6.2.2 子域名方法

YD/T 3016-2016

如果将系统的域名记为`www.xxx.com`，那么业务对应的子域名是`{appId}.xxx.com`。从子域名当中可以直接获得该业务对应的业务标识。如果业务请求采用子域名方法，则应在HTTP请求的Host头部中指出该请求对应的子域名。

6.2.3 子目录方法

如果将系统的域名记为`www.xxx.com`，将系统的根目录记为`/`，那么业务对应的子目录是`www.xxx.com/{appId}`。从子目录中可以直接获得该业务对应的业务标识。如果业务请求采用子目录方法，则无需在HTTP请求头部中附带Host信息。

6.3 项目的目录结构

本节内容以Java Web应用为例，详细描述了每一个项目需要遵循的目录结构标准。在Java Web应用的目录结构中，所有文件都位于项目根目录之下。可以用J2EE SDK提供的工具将其打包成一个war（Web Application Archive，Web应用的一种压缩格式）。项目根目录下至少应包含WEB-INF目录，该目录中至少应包含以下内容：

- `/WEB-INF/web.xml`，用于配置 Web 应用，描述 Servlet 和其他 Web 应用组成部分，以及这些组成部分的初始化参数等属性的 XML 文档；
- `/WEB-INF/appengine-web.xml`，用于配置平台参数，如描述动静分离配置中的目录参数；
- `/WEB-INF/classes`，用于存储所有 Java 类文件和相关资源文件，如 Servlet 类、普通 Java 类、图片、语言信息等文件；
- `/WEB-INF/lib`，用于存放 Web 应用所需的所有库文件，这些库文件是以压缩的.jar 文件格式存储的。
- 除了必须的 WEB-INF 目录之外，项目根目录之下也可包含 js、css、images 等目录，分别用于组织 javascript、css 以及图片等资源。

6.4 业务部署流程

第三方开发者可以直接将业务资源打包并部署到平台上，或者采用SVN、Git等版本控制工具部署业务。采用版本控制工具部署业务的详细流程如图3所示，包含以下步骤：

- 1) 在向平台上传业务内容之前，第三方开发者应向平台申请创建业务，请求中包括业务标识，用户通过由该标识产生的 URL 即可访问业务；
- 2) 平台创建与该业务相关的远程仓库，第三方开发者可将业务的内容通过客户端程序上传到该远程仓库中；
- 3) 第三方开发者使用客户端，如 svn 客户端、Git 客户端等，创建本地仓库；
- 4) 第三方开发者准备完整的业务资源，并加入本地仓库；
- 5) 第三方开发者发出上传指令，可以通过命令行，亦可以集成到 IDE 当中；
- 6) 第三方开发者通过客户端程序将业务同步到远程仓库上，需要输入用户名和密码进行身份认证，远程仓库上保存着业务所有版本的内容；
- 7) 第三方开发者选择需要的业务版本；
- 8) 平台将该版本的业务资源部署到业务运行平台中。

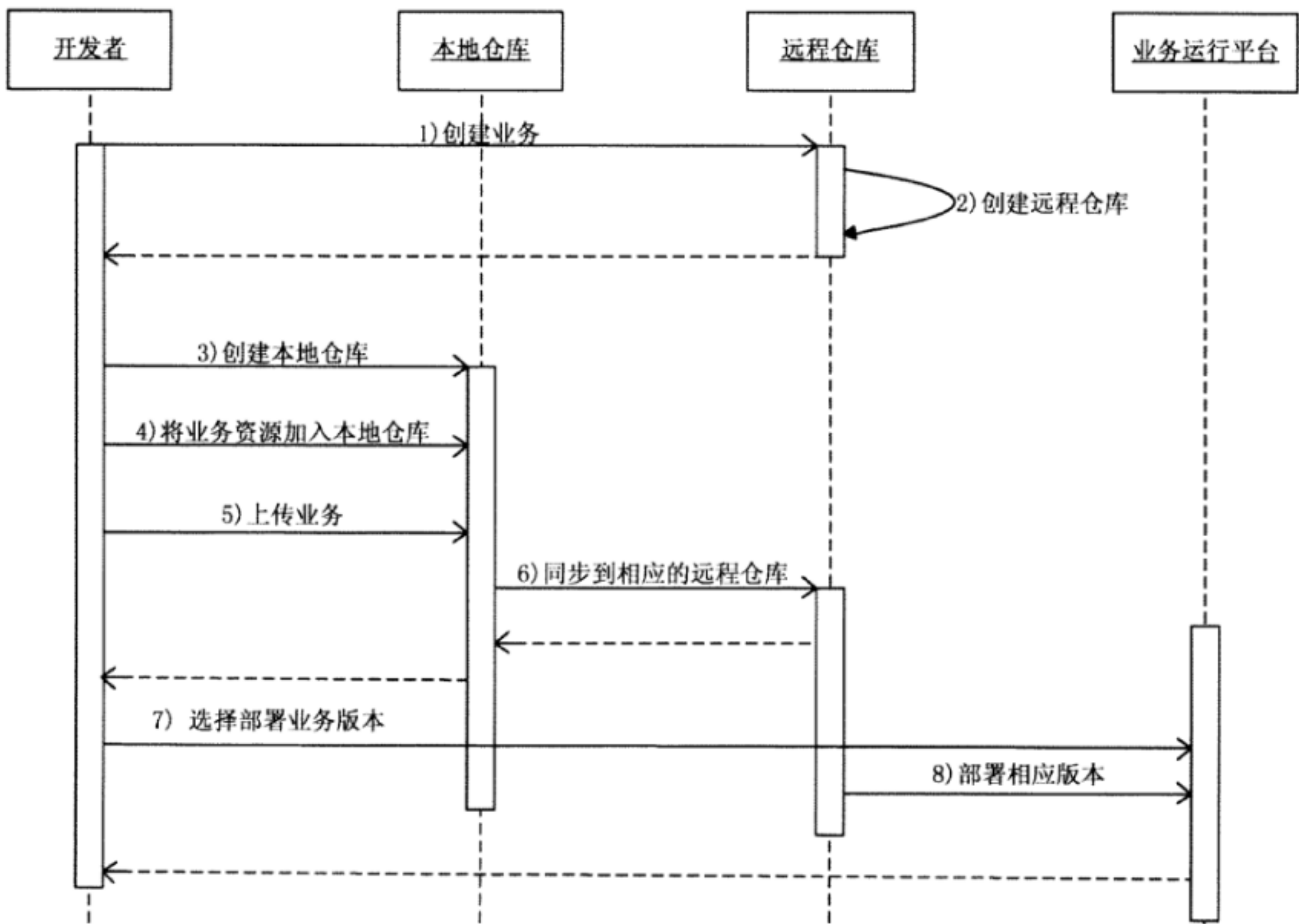


图3 业务部署流程

7 业务请求处理流程

7.1 标准业务请求处理流程

图4所示是业务请求的标准处理流程,描述从面向移动互联网的业务托管和运行平台接收业务请求到返回业务响应内容的整个过程。该业务请求所对应的业务已经运行。详细流程如下所述:

- 平台接收业务请求,该请求进入前端负载均衡层;
- 前端负载均衡层将请求分发到缓存服务器;
- 缓存服务器查找是否缓存命中,即缓存服务器是否包含缓存数据,这些数据是先前响应业务请求操作的结果;
- 未找到缓存的响应内容,业务请求进入动态路由层处理;
- 动态路由层根据业务请求查找对应的业务标识,根据业务标识查找业务所在的业务运行环境,如果查找结果中存在多个业务运行环境,则选择其中一个;
- 将业务请求转发到相应的业务运行环境中,业务运行环境将业务请求分配到相应的业务运行实例;
- 业务运行实例调用平台用户认证服务,获取发送业务请求的用户;
- 处理业务请求,在处理业务请求当中,可调用平台的其他服务;
- 返回业务请求响应内容,如 HTML 文件、javascript 文件等,完成业务请求处理流程。

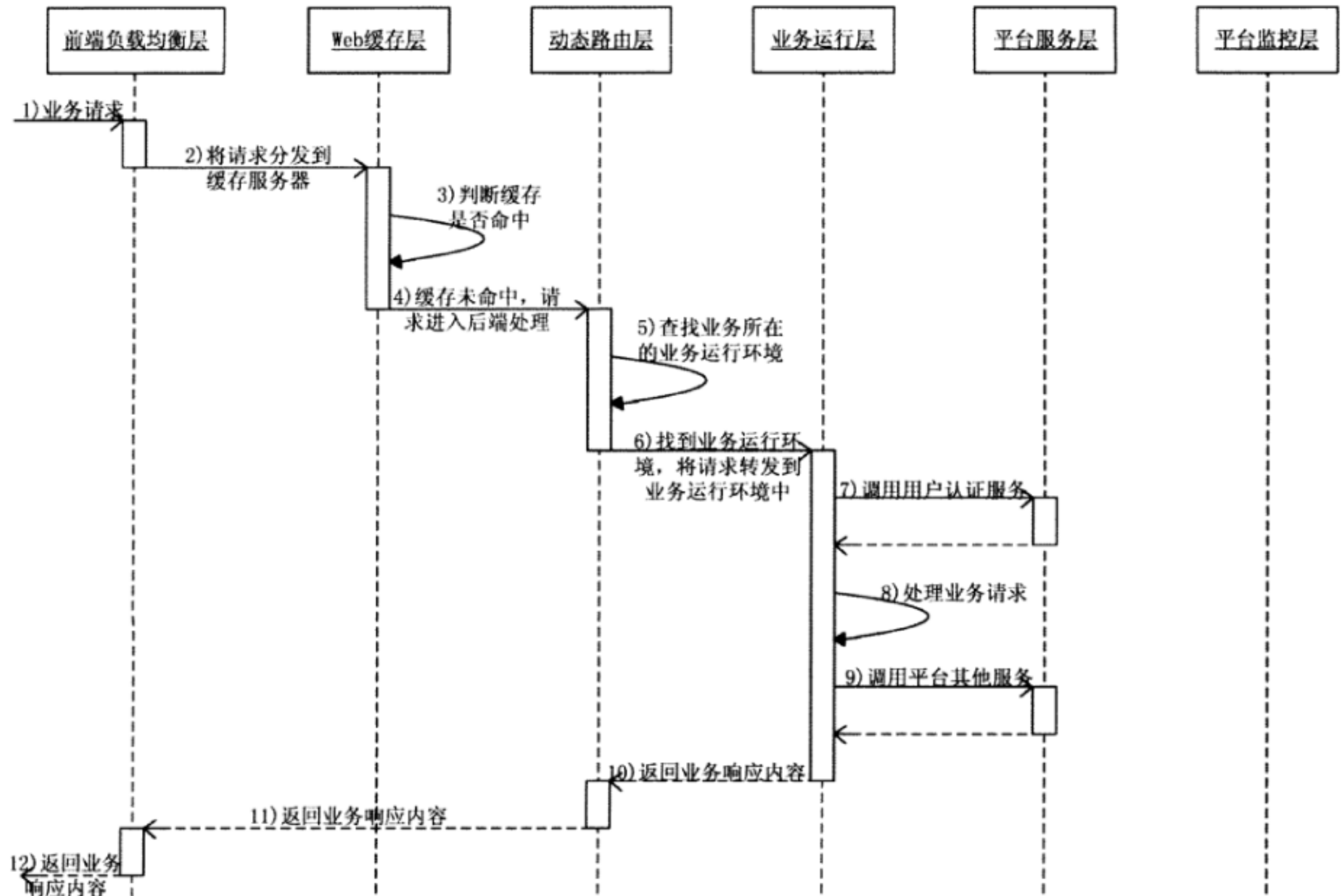


图4 标准业务请求处理流程

7.2 带缓存命中的业务请求处理流程

图5所示是带缓存命中的业务请求处理流程,描述从面向移动互联网的业务托管和运行平台接收业务请求到返回业务响应内容的整个过程。该业务请求所对应的业务已经运行,且已经处理过相同业务请求。详细流程如下所述:

- 平台接收业务请求,该请求进入前端负载均衡层;
- 前端负载均衡层将请求分发到缓存服务器;
- 缓存服务器查找是否缓存命中,即缓存服务器是否包含缓存数据,这些数据是先前响应业务请求操作的结果;
- 找到缓存的响应内容,直接返回业务请求响应内容,如HTML文件、javascript文件等,完成业务请求处理流程。

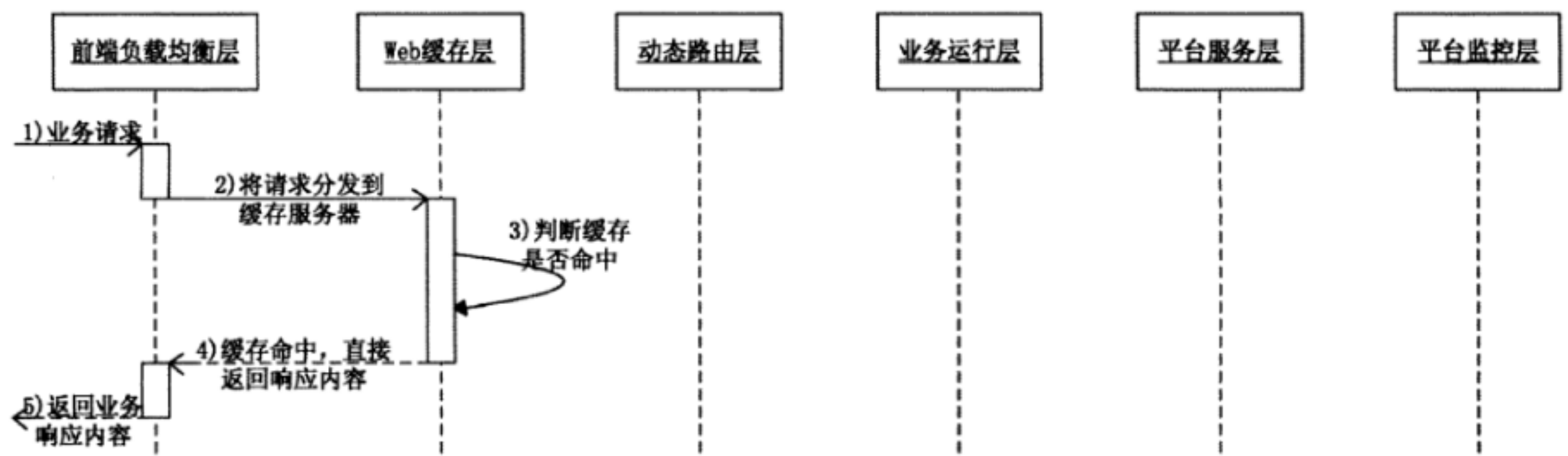


图5 带缓存命中的业务请求处理流程

7.3 首次业务请求的处理流程

图6所示是首次业务请求的处理流程，描述从面向移动互联网的业务托管和运行平台接收业务请求到返回业务响应内容的整个过程。该业务请求所对应的业务尚未运行。详细流程如下所述：

- 平台接收业务请求，该请求进入前端负载均衡层；
- 前端负载均衡层将请求分发到缓存服务器；
- 缓存服务器查找是否缓存命中，即缓存服务器是否包含缓存数据，这些数据是先前响应业务请求操作的结果；
- 未找到缓存的响应内容，业务请求进入动态路由层处理；
- 动态路由层根据业务请求查找对应的业务标识，根据业务标识查找业务所在的业务运行环境；
- 未查找到对应的业务运行环境，表明该业务尚未运行，将请求转发到平台监控层，由平台监控层负责初始化业务；
- 平台监控层查找空闲的业务运行环境，该业务运行环境具有额外的 CPU、内存和网络带宽来运行新的业务；
- 平台监控层向业务运行环境发送初始化业务的指令，在业务运行环境中初始化新的业务；
- 平台监控层接收到初始化成功消息后，将业务请求转发到相应的业务运行环境中，业务运行环境将业务请求分配到相应的业务；

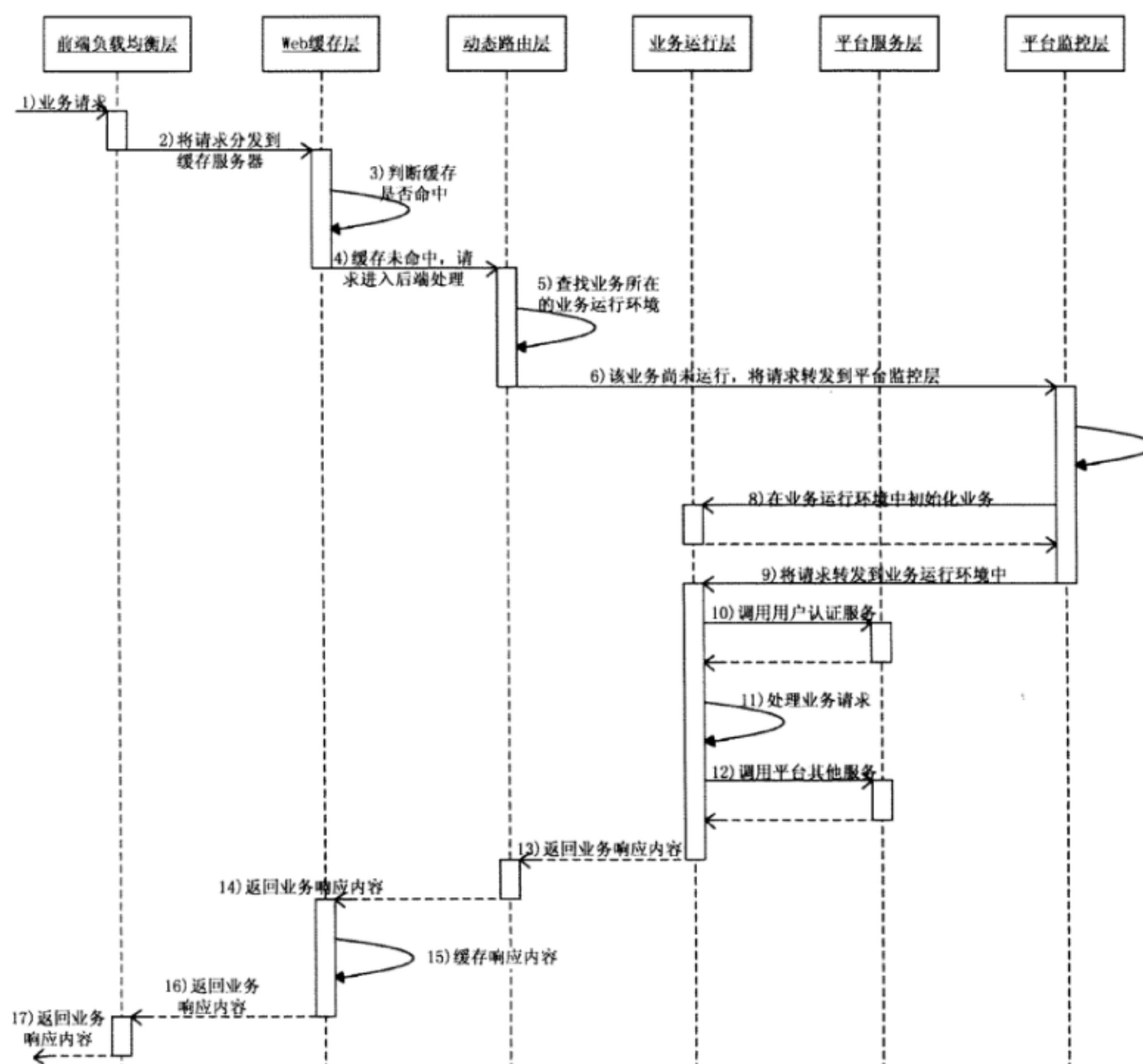


图6 首次业务请求的处理流程

- 业务调用平台用户认证服务，获取发送业务请求的用户；
- 处理业务请求，在处理业务请求当中，可能调用平台其他服务；
- 返回业务请求响应内容，如 HTML 文件、javascript 文件等，完成业务请求处理流程。

8 平台服务

平台服务层应当提供面向移动互联网的业务托管和运行平台所需的服务，并支持开发者的业务通过调用应用编程接口来访问这些服务。基本的环境服务类型应当包括数据库服务、大数据对象的数据库存储服务、分布式缓存服务、数据存储区服务、URL 访问服务、邮件服务、图片服务、多租户服务、认证授权服务、任务调度服务、短信服务以及地理位置信息服务等。

8.1 数据库服务

至少提供一种数据库的访问功能，如 MySQL 数据库。

8.2 大数据对象的数据库存储服务

支持图片、声音、视频等多媒体大数据对象的数据库存储服务。支持大数据对象的集中移动、备份，同时支持简单的权限和配置管理功能。

8.3 内存缓存服务

平台内存缓存服务应当满足以下要求：

- 可利用分布式和可扩展的内存管理系统提供高性能的业务运行；
- 可提升常见数据存储区查询速度。如相同参数执行查询、会话数据查询、用户偏好设置查询等功能。

8.4 数据存储区服务

平台内存数据存储区应当满足以下要求：

- 可保存多类型数据对象，如字符串、整数或对另一对象的引用等；
- 可在单个事务中执行多个操作，支持多用户同时访问或操纵相同的数据；
- 提供低级别应用编程接口，这些接口包含对实体执行的简单操作，包括 GET、PUT、DELETE 和 QUERY；
- 可以使用低级别应用编程接口来实现其他的接口适配器，或者业务中直接使用。

8.5 URL 访问服务

在面向移动互联网的业务托管和运行平台上，由于安全因素，需要禁用业务运行环境的 socket 功能。因此，需要提供 URL 访问服务，以通过 URL 和其他业务进行通信或访问网络上的资源。

8.6 邮件服务

平台邮件服务包含的基本内容应有：

- 可接收不同地址的电子邮件；
- 可将电子邮件发送到一个或多个收件人，邮件包含主题、纯文本正文以及可选的 HTML 正文和文件附件；
- 邮件的发件人地址应当为业务管理员的电子邮件地址、当前登录用户的电子邮件地址或业务的任何有效电子邮件接收地址；
- 邮件可包含“回复”地址，该地址满足上一条限制。

8.7 图片服务

平台提供应当提供专用图片服务处理功能，主要包括：

- 可调整图片大小以及旋转、翻转和裁剪图片；
- 可将多个图片合并为一个图片以及在几种格式之间转换图片数据；
- 可提供有关图片的信息，包括图片格式、宽度、高度以及颜色值直方图；
- 可直接从业务中接收图片数据，也可使用大数据对象的数据库服务存储的数据。

8.8 多租户服务

面向移动互联网的业务托管和运行平台中的一个业务可以同时为很多客户组织（称为租户）提供服务。平台提供便捷的租户间数据划分功能。每个租户拥有唯一的命名空间字符串，可直接使用命名空间管理器，在全局范围内为租户设置命名空间。

8.9 用户认证服务

面向移动互联网的业务托管和运行平台支持三种类型的用户，即开发者用户、业务用户以及平台管理员。平台可以检测当前用户是否已经认证，并且可以将用户重定向到登录页面，以登录或创建一个新的帐户。当用户登录后，平台可以检测当前用户是否为平台管理员，以显示仅限平台管理员能执行的操作。

开发者用户能够执行的操作包括：利用平台分配的资源，在平台上创建和部署新的业务；根据业务运营情况，向平台提出资源的再分配请求；查询计费信息。

业务用户能够执行的操作包括：当业务需要获取用户的身份信息时，可以直接使用平台提供的认证服务，无需业务本身提供认证手段；可以在多个不同业务之间共享用户信息。

平台管理员能够执行的操作包括：对平台资源分配与运营环境的全面监控和管理；对平台用户信息的认证与管理。

8.10 任务调度服务

8.10.1 后台任务服务

面向移动互联网的业务托管和运行平台的后台任务服务应当满足以下基本要求：

- 提供分布式定时服务，支持特定动作的定时触发；
- 可进行分布式环境部署，具有高可靠性；
- 任务间相互隔离，可以同时触发，支持基于优先级的分布式执行。

8.10.2 任务队列服务

面向移动互联网的业务托管和运行平台支持分布式任务队列服务，以异步HTTP方式执行用户任务。用户可通过创建队列，并向队列中添加任务，来执行业务代码。平台任务队列服务支持分布式环境部署，并具有高可靠性。

8.11 消息服务（可选）

平台支持运营商网络的短信业务以及开放式的即时消息服务。

8.12 地理位置信息服务（可选）

平台提供的地理位置信息服务可查询路线、公交、IP位置以及地图等地理位置相关的信息。

9 安全性要求

面向移动互联网的业务托管和运行平台上部署了海量的业务，因此，平台应限制授予业务的访问权限。通过将各个不同的业务隔离保护在不同的安全沙盒中，业务之间互不影响、彼此安全，从而实现业务的安全访问和操作限制，而且能够在不同机器上迁移业务，以应对节点故障。

业务来自第三方开发者，其行为非运营商可以预知。因此，应对这些业务所能访问的本地接口进行限制，以起到保护平台的作用：

- 禁止往本地文件系统中写数据，业务只能读取该业务根目录下的静态文件，不得读取其他业务的任何内容，以保护本地文件系统和其他业务的数据；

- 限制对依赖本地系统的接口的访问，如图形接口、硬件接口等；

- 只能访问本业务目录下的扩展库，不能访问其他业务下的扩展库；

- 提供对网络的有限访问，业务只能通过系统提供的标准网络访问服务来获取其他站点的资源，防止业务访问恶意的链接给业务运行环境造成破坏，通过平台网络服务获取的数据不能作为代码执行，防止恶意代码破坏业务运行环境；

- 禁止创建新的线程，保证单线程运行，不能在业务运行环境中大量生成线程或进程，只能在相应业务请求处理线程上执行；

- 限制对硬件资源的使用，对 CPU 请求、内存、网络流量等必须定额，任何业务请求都必须在有限时间内返回，保证各个业务之间不会相互干扰，并且使得单个业务不会占用大量的系统资源。
