

中国移动通信企业标准

QB-XX-XX-XX-XX

中国移动终端公司终端管理 (DM) 平台技术规范

China Mobile Device Management
Platform Specification

版本号：1.0.0

XXXX-XX-XX 发布

XXXX-XX-XX 实施

中国移动终端公司 发布

目 录

前言	5
1. 范围	6
2. 规范性引用文件	6
3. 术语、定义和缩略语.....	6
3.1 术语及定义	6
3.2 缩略语	6
4. 基本描述	7
5. 系统架构	7
5.1 网络接入层	8
5.2 数据处理层	8
5.3 数据存储层	8
5.4 数据表现层	9
6. 功能要求	9
6.1 功能概述	9
6.2 网络接入功能	9
6.3 海量连接接入功能	10
6.4 UE 身份标识识别功能.....	10
6.5 UE 激活记录.....	10
6.6 UE 源地址识别功能.....	10
6.7 数据解析功能	10
6.8 海量数据存储功能	10
6.9 数据操作功能	11
7. 业务流程	11
7.1 引导---Bootstrap	11
7.2 注册---register	12
7.3 更新注册---update.....	13
7.4 注销---de_register.....	14
7.5 设备离线---offline.....	14
7.6 设备管理操作---read/write/exec/create/delete/discover/write attribute（可选）. 15	
7.7 信息订阅---observe（可选）	16
7.8 取消订阅---cancel observe（可选）	17

7.9 订阅参数设置---write attributes（可选）	17
7.10 数据上报---notify（可选）	18
8. DMP 与 UE 接口要求	18
8.1 协议适配要求	19
8.2 Bootstrap 流程及要求	20
8.2.1 Bootstrap Request	21
8.2.2 Bootstrap Write	21
8.2.3 Bootstrap Finish	22
8.3 设备注册及注销	23
8.3.1 设备注册	23
8.3.2 设备注册更新消息	24
8.3.3 设备注销消息	25
8.4 消息观察、取消观察、消息上报、设定 Notify 策略（可选）	26
8.4.1 设定 Notify 策略	28
8.4.2 观察消息	28
8.4.3 取消观察消息	29
8.4.4 数据上报	30
8.5 设备管理消息（可选）	30
8.5.1 读取资源	30
8.5.2 写入资源	31
8.5.3 执行资源	32
8.5.4 资源发现	32
8.5.5 资源创建	33
8.5.6 资源删除	33
9. 安全要求	34
9.1 数据解析层安全能力要求	34
9.2 数据存储层安全能力要求	34
9.3 设备通用安全要求	34
10. 性能要求	35
附录	35
附录 A UE 与 DMP 通信协议及格式	35

仅供中国移动合作伙伴使用，请注意保密

前言

本标准对中国移动终端公司终端管理平台提出技术性规范，是中国移动蜂终端公司终端管理平台建设过程中遵循的技术文件。

本标准包括以下几个方面主要内容：系统结构及组网、业务流程、功能要求、接口要求、安全要求以及性能指标。

本标准的附录A UE与DMP通信协议及格式为标准性附录。

本标准由中移 号文件印发。

本标准由中国移动终端公司提出，终端公司归口。

本标准起草单位：中国移动通信研究院

本标准主要起草人：金杰敏、刘玮哲、路鹏、刘悦、张普、刘聪、骆正虎、龙容、张勇浩

1. 范围

本标准制定了中国移动终端公司终端设备管理（Device Management, DM）平台的技术要求，是公司开展 DM 平台建设和运营管理的依据，DM 平台必须符合本标准制定的技术要求。

本规范主要包括以下几方面内容：基本描述、系统结构及组网、业务流程、功能要求、接口要求、安全要求以及性能指标。

本规范内容分为必选和可选内容，必选为中国移动终端公司 DM 平台所需要的必要功能和技术要求，可选部分可以根据实际需要进行选择性配置。

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。

序号	标准编号	标准名称	发布单位
[1]	IETF RFC7252	The Constrained Application Protocol (CoAP)	IETF
[2]		OMA Lightweight M2M v1.0	OMA

3. 术语、定义和缩略语

3.1 术语及定义

下列术语、定义和缩略语适用于本标准：

表3-1 术语/定义

词语	解释
终端设备管理	一种对终端进行远程管理的技术

3.2 缩略语

表3-2 缩略语

缩略语	英文全称	中文含义
CMEI	China Mobile Equipment Identity	中国移动设备标识码
DM	Device Management	设备管理

DMP	Device Management Platform	设备管理平台
IEEE	Insitute of Electrical and Electronic Engineers	美国电气和电子工程师协会
IMEI	International Mobile Equipment Identity	国际移动装备标识码
IMSI	International Mobile Subscriber Identity	国际移动用户识别码
IP	Internet Protocol	互联网协议
IPv4	Internet Protocol version 4	互联网协议版本4
IPv6	Internet Protocol version 6	互联网协议版本6
LWM2M	Lightweightmachine-to-machine protocol	轻量级机器到机器协议
OMA	Open Mobile Alliance	开放移动联盟
UE	User Equipment	终端设备

4. 基本描述

DM 平台（Device Management Platform， DMP），是中国移动终端公司为终端设备（User Equipment， UE）提供注册、管理、统计等功能的管理平台。满足《中国移动终端公司 DM 终端技术规范》的终端可以接入到 DMP， 由 DMP 完成对终端的管理功能。

5. 系统架构

系统架构如图所示：

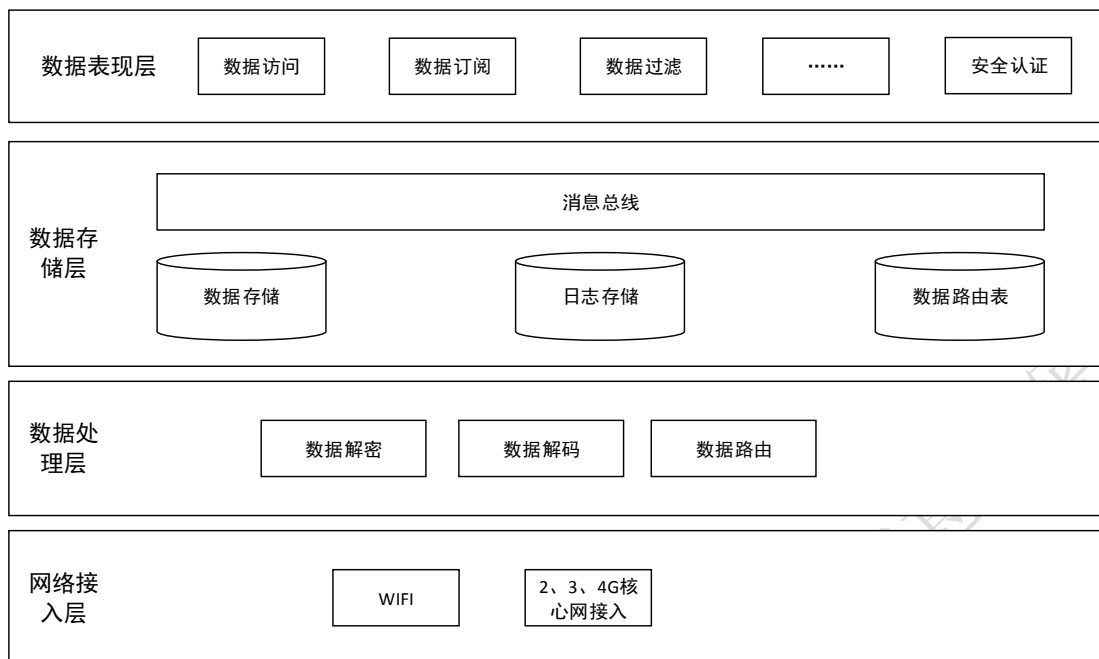


图 5-1 DMP 系统架构图

5.1 网络接入层

网络接入层主要负责实现 DMP 与终端设备对接。

5.2 数据处理层

数据处理层主要包含数据解密、数据安全保护服务和数据路由服务，实现数据存储层和数据表现层对于数据存储转发的功能需求。

其中，数据解密服务负责将网络接入数据进行解码，导入数据库进行存储。数据解析流程参见 7.业务流程。

数据安全保护服务负责将终端上行到 DMP 平台的数据进行解密和完整性验证，将第三方平台下行到终端的数据进行加密和完整性保护。安全保护服务功能为可选，推荐使用安全保护服务功能。

数据路由服务，负责将经过 DMP 但无需进行数据沉淀和解析的数据根据其目标地址进行路由。

5.3 数据存储层

数据存储层主要包含消息总线、数据存储、标识存储、日志存储、数据路由表几个服务，实现数据高效存储的需求。

其中，消息总线服务是针对物联网数据特点，为高吞吐量、快速响应数据、指令、通知等的收发和转发需求，而实现的实时数据处理服务。

数据存储服务是 DMP 的核心服务之一，用于将物联网数据进行存储汇聚，并通过表现层对外提供数据访问功能。

数据存储层需要对访问数据存储层的来源进行合法性验证，确保所有来源的身份合法。根据不同场景、不同应用需求对访问数据存储层的用户、应用和 IP 进行细粒度的权限控制，防止越权访问。对从数据存储层输出的敏感数据进行脱敏处理，而且脱敏算法可以根据不同场景、用户等具体需求分别配置。对所有访问数据存储层的操作提供集中的日志审计及行为溯源，发现可疑操作、系统热点等。

数据存储层需要支持密文存储功能，支持加密数据传输。

日志存储服务将系统日志、连接日志、数据日志、接口调用日志等内容进行分类存储，方便系统进行维护。

数据路由表记录数据路由的目标地址，为数据路由提供服务。

5.4 数据表现层

数据表现层包括数据访问服务、数据订阅服务等。

数据访问服务响应来自 DMP 的数据访问合法请求。

数据订阅服务根据 DMP 和 UE 的数据订阅关系将全量数据或增量数据进行指向性推送。

6. 功能要求

6.1 功能概述

DMP 的主要设计功能是为了管理终端(UE)，因此 DMP 应主要包含以下功能：

- 网络接入
- 海量连接接入
- UE 身份标识识别
- UE 激活记录
- UE 源地址识别
- 数据解析
- 海量数据存储
- 数据操作功能

6.2 网络接入功能

网络接入功能主要是为了实现 DMP 和 UE 之间的 IP 连接，从而为后续流程建立前提条件。

DMP 必须支持 IPv4 接入类型及 IP 数据的收发。IP 数据是指传统的可以通过 IP 网络承载的数据包，根据 IP 网络协议进行路由。

6.3 海量连接接入功能

由于 DMP 需要支持海量级 UE 设备的管理，DMP 必须支持负载均衡技术，支持海量连接接入。

6.4 UE 身份标识识别功能

接入 DMP 的所有 UE 要求具备终端身份标识（End Point Identity, EPI）。每个终端 EPI 是唯一的，DMP 依据 EPI 标识每一个 UE 设备。UE 在与 DMP 交互时需要上报其 UE 身份名称（End Point Name, EPN），EPN 包含的信息及格式参考终端规范 7.1 命名规则定义。

由于不同类型设备 EPN 组成各不相同，DMP 必须解析 EPN 的组成，依据以下规则确定 EPI：

- （1）EPN 中同时包含 CMEI、IMEI 时，使用 CMEI 和 IMEI 拼接的字符串作为 EPI；
- （2）EPN 仅包含 CMEI 时，使用 CMEI 作为 EPI；
- （3）EPN 仅包含 IMEI 时，使用 IMEI 作为 EPI；

当 EPN 包含版本信息时，DMP 也必须记录版本信息，并在后续流程中携带版本信息。

当 DMP 无法依据 EPN 确定 EPI 时，应将 UE 视为无效 UE 加以丢弃或拒绝。

6.5 UE 激活记录

UE 首次在 DMP 上注册成功即为激活。DMP 必须记录 UE 身份标识、激活时间和激活属地（参见 6.6 UE 源地址识别）。

6.6 UE 源地址识别功能

所有接入 DMP 的 UE 必须具备源 IP 地址。DMP 必须记录 UE 的源 IP 地址，用于 UE 地理位置的统计分析。

6.7 数据解析功能

DMP 必须支持对来自 UE 的数据解析，包括但不限于 IP、UDP、CoAP、LwM2M 等协议数据。

6.8 海量数据存储功能

DMP 必须支持对 UE 上报的信息、事件等进行持久化存储，包括但不限于以下功能：

- （1）支持高速写入、读取；

- (2) 支持数据存储空间动态扩展;
- (3) 支持数据基于权限的受控访问;
- (4) 支持存储数据访问认证;
- (5) 支持操作日志审计功能;

6.9 数据操作功能

数据操作是指 DMP 可以对 UE 上报的信息进行操作,包括但不限于数据查询、数据统计、数据过滤等:

- (1) 数据查询: 获得授权后, 可以对 UE 上报数据进行读取;
- (2) 数据统计: 获得授权后, 可以对 UE 各个维度进行统计, 包括但不限于: 时间范围、设备名称、设备型号、地理位置、设备状态、活跃度以及相关条件组合的统计;
- (3) 数据过滤: 对异常数据可以安全过滤或标记;

7. 业务流程

DMP 与 UE 之间的主要业务包括引导、注册、注销、设备离线、设备管理操作、信息订阅、取消订阅、订阅参数设置、数据上报, DMP 与 UE 之间的通讯协议应遵循《OMA Lightweight M2M v1.0》。

本规范中按照 LwM2M 业务流程划分方式, 进行了端到端业务流程的划分。

7.1 引导---Bootstrap

引导流程是对使用 LwM2M 协议定义的一种特殊的业务流程, 其作用是使用 LwM2M 的 Client 向 Server 进行注册, 以获取 LwM2M Server 的信息, 来完成 LwM2M Client 的引导注册流程。此业务流程与 7.2 注册流程所针对的业务阶段是不同的。引导是所有流程的第一步, 完成 LwM2M C/S 间的握手, OMA 定义能力的同步, 以及 server 负载的调度, 而 7.2 注册过程是对于 UE 自带的数据类型和设备类型的注册。其具体流程如下:

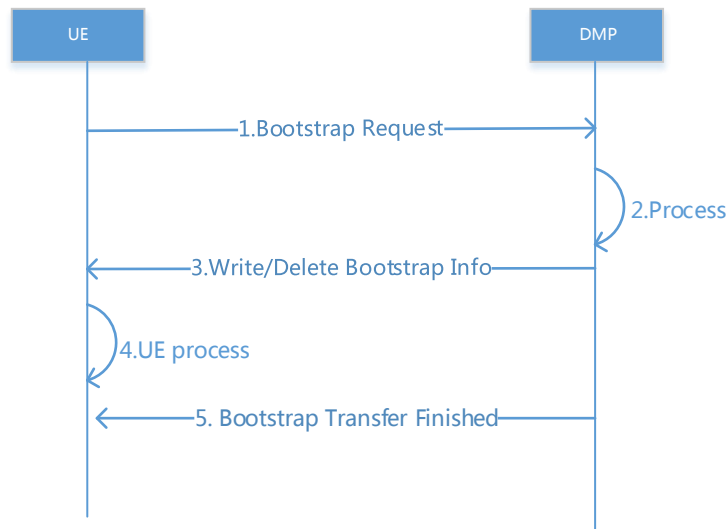


图7-1引导流程示意

引导业务流程说明：

1. UE 向 DMP 发送 Bootstrap 的请求，消息格式信息满足《OMA Lightweight M2M v1.0》中 8.2.2 的要求，可协商的能力项应满足《OMA Lightweight M2M v1.0》中 Appendix E 的要求
2. DMP 处理 Bootstrap 请求，配置 UE 要求的信息
3. 将 DMP 能力以 Write 或 Delete 消息的格式要求发还给 UE，格式满足《OMA Lightweight M2M v1.0》8.2.2 要求，可协商的能力项应满足《OMA Lightweight M2M v1.0》中 Appendix E 的要求
4. UE 按照 Bootstrap 的指令进行处理
5. DMP 将 Bootstrap 结束消息向 UE 下发，格式满足《OMA Lightweight M2M v1.0》8.2.2 要求

7.2 注册---register

注册是 UE 在使用 DMP 时,向 DMP 发起的起始流程，主要用于 UE 首次向设备注册自身能力和 DMP 通讯以及设备离线后再次和服务握手。具体流程如下：

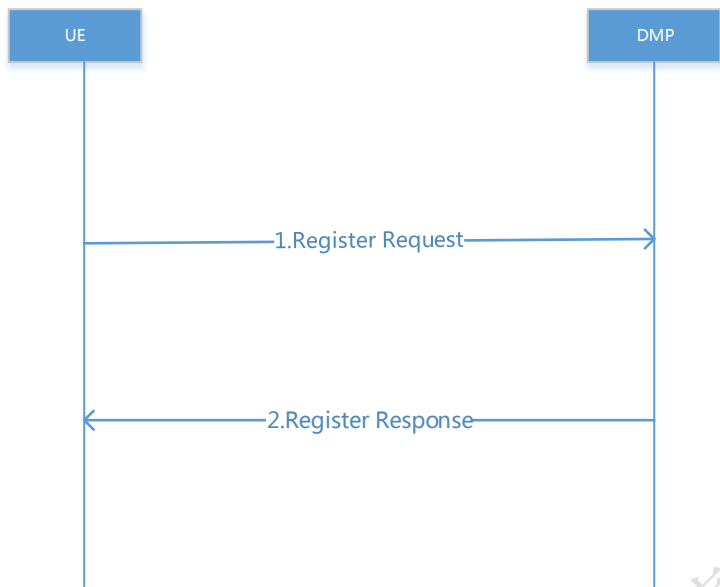


图7-2注册流程

- 注册流程如下：
- 1. UE 在初始化阶段，向 DMP 发送注册请求
 - 2. DMP 接收到 UE 的注册请求后，将 UE 注册信息保存在 DMP，并向 UE 返回确认信息

7.3 更新注册---update

当有注册信息或状态需要更新时，发起更新注册流程。

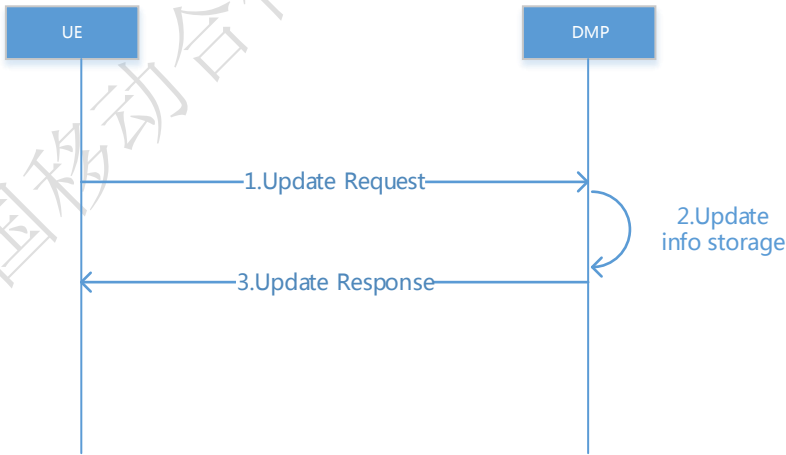


图7-3更新注册流程

- 更新注册流程说明如下：
- 1. UE 向 DMP 发起更新注册请求，此请求的目标地址为 DMP 平台
 - 2. DMP 接收到 UE 的更新注册请求后
 - 3. 将 UE 更新的注册信息保存在 DMP

7.4 注销---de_register

当 UE 设备不再驻留服务时，可向 DMP 发起注销流程，流程图如下：

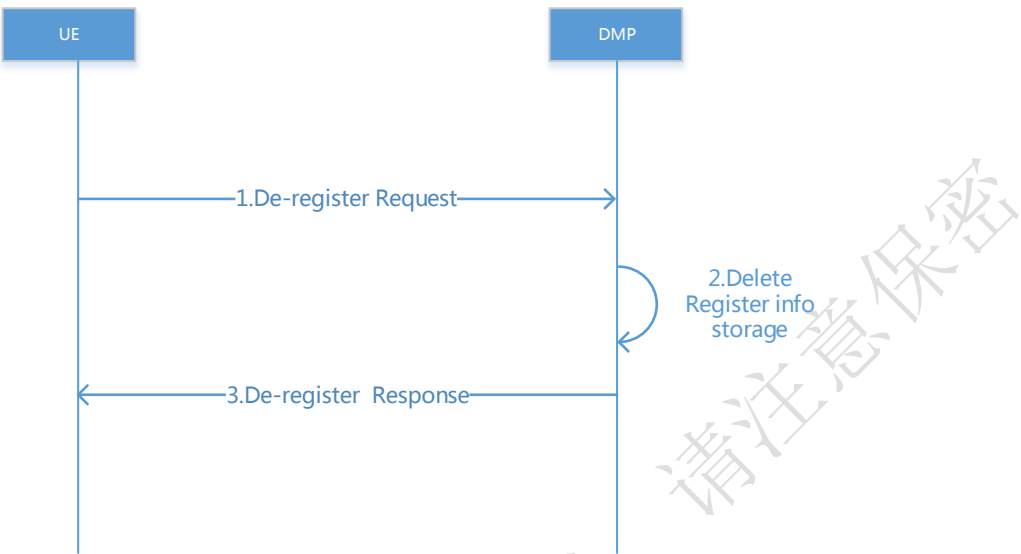


图 7-4 注销流程

注销流程说明如下：

- 1. UE 向 DMP 发起注销请求
- 2. DMP 删除该 UE 对应的注册
- 3. DMP 返回确认消息

7.5 设备离线---offline

当 UE 与 DMP 的连接超过《OMA Lightweight M2M v1.0》中定义的 UE LifeTime 属性所设置的时间时，UE 在 DMP 上的状态将会变为离线（Offline）状态。具体流程如下所示：

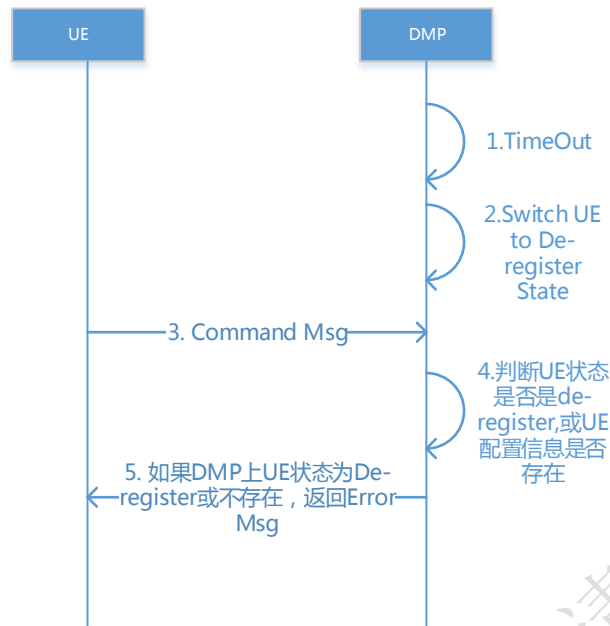


图 7-5 设备离线流程

设备离线流程说明：

1. DMP 按照 UE 配置的 LifeTime 信息监测 UE 是否出现 TimeOut，如果 UE 在 LifeTime 时间内没有新的消息，则 DMP 认为此 UE 出现 TimeOut 状态
2. 将 DMP 对应的 UE 执行注销操作，DMP 将此 UE 对应的注册信息移除
3. 在 UE 被标记为注销状态下，UE 向 DMP 发送非 Register 消息
4. DMP 判断此 UE 的状态为注销，此消息被拒接
5. 返回错误信息给 UE，错误消息满足《OMA Lightweight M2M v1.0》应答消息格式要求

7.6 设备管理操作——read/write/exec/create/delete/discover/write attribute(可选)

DMP 与 UE 之间的设备管理操作遵循《OMA Lightweight M2M v1.0》要求，分为 read、write、write attribute、execute、create、delete、discover 7 种操作，其业务流程基本一致，业务流程图如下：

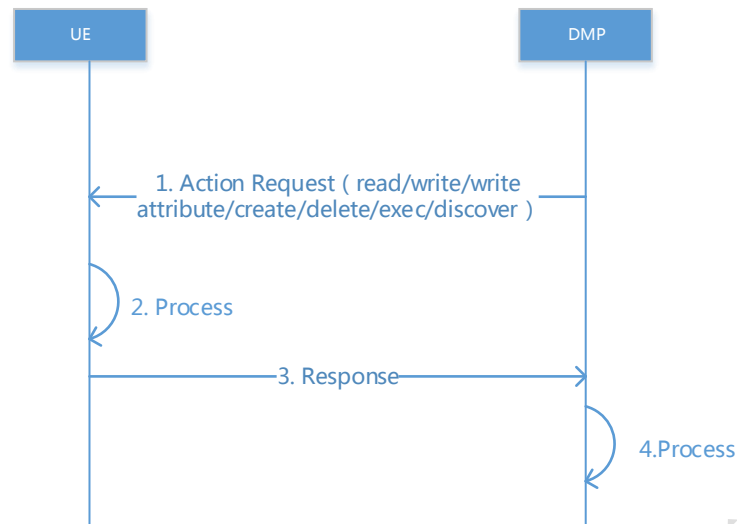


图7-6设备管理操作流程

设备管理操作流程如下：

1. DMP 向 UE 发起设备管理操作指令
2. UE 根据 Action Request 进行相应的处理动作
3. UE 将处理结果打包,将信息返回到 DMP, 消息格式符合《OMA Lightweight M2M v1.0》的定义及附录 B 的要求
4. DMP 接收到 UE 上行数据后进行相应的动作处理

7.7 信息订阅——observe（可选）

用户如果需要对 UE 信息发起订阅，使 UE 可以自动进行信息上报，应遵循以下流程：

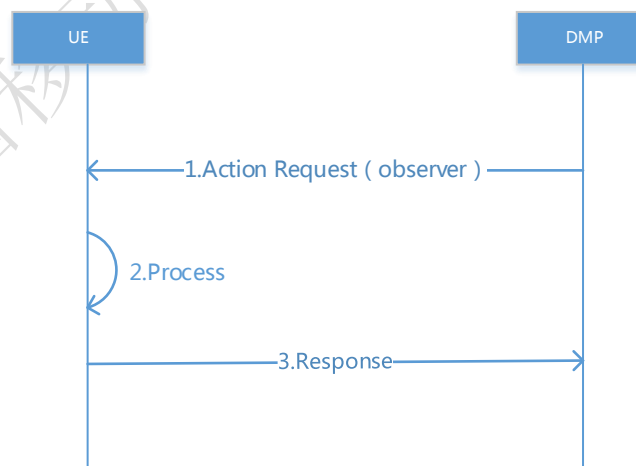


图 7-7 信息订阅流程

信息订阅流程如下：

1. DMP 向 UE 发起设备信息订阅操作指令
2. UE 根据 Action Request 进行相应的处理动作

3. UE 将处理结果打包，数据包目标地址为 DMP 平台，消息格式符合《OMA Lightweight M2M v1.0》的定义及附录 B 的要求

7.8 取消订阅——cancel observe（可选）

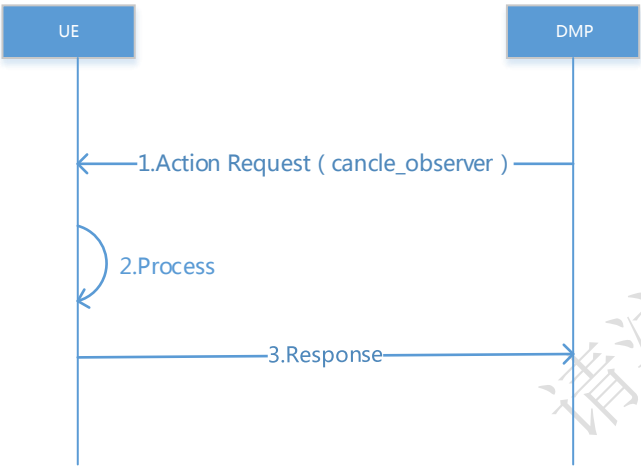


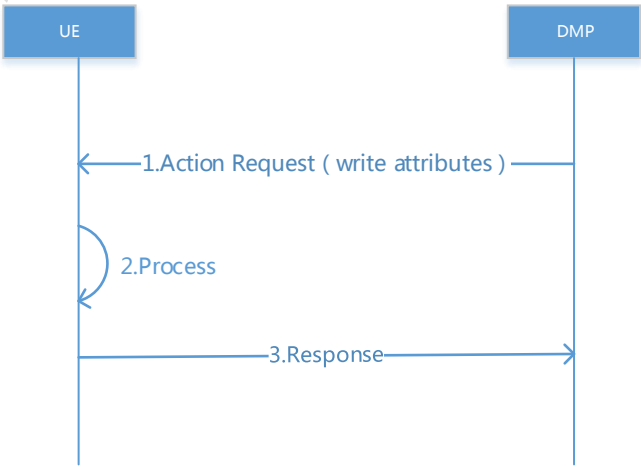
图 7-8 取消订阅流程

取消订阅流程如下：

- 1. DMP 向 UE 发起取消设备信息订阅操作指令
- 2. UE 根据 DMP 的 Action Request 进行相应的处理动作
- 3. UE 将处理结果打包，数据包目标地址为 DMP 平台，消息格式符合《OMA Lightweight M2M v1.0》的定义及附录 B 的要求

7.9 订阅参数设置——write attributes（可选）

如 DMP 需要设置或修改 UE 的数据上报的参数，需要调用订阅参数设置流程，具体流程如下：



图表 7-9 订阅参数设置流程图

订阅参数设置流程如下：

1. DMP 向 UE 发起设备信息订阅参数设置操作指令
2. UE 根据 DMP 的 Action Request 进行相应的处理动作
3. UE 将处理结果打包, 数据包目标地址为 DMP 平台, 消息格式符合《OMA Lightweight M2M v1.0》的定义及附录 B 的要求

7.10 数据上报——notify (可选)

数据上报是 UE 主动向 DMP 上报其数据的业务方式, 数据上报要求 UE 已经接收到了 DMP 的信息订阅请求, 并按照请求中的指令进行了内容配置, 然后 UE 将根据 DMP 要求的上报周期进行数据定时上报, 其具体业务流程如下:

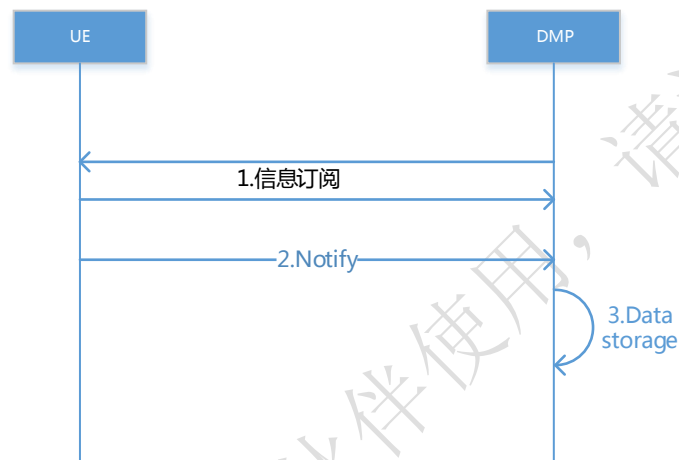


图 7-10 数据上报流程示意图

数据上报流程说明:

1. 根据 7.6 信息订阅业务流程的要求, 完成 DMP 向 UE 的信息订阅, 使 UE 可以按照 DMP 要求的时间周期和内容, 做好数据上报的初始化
2. UE 向 DMP 发起数据上报消息, 消息内容格式符合《OMA Lightweight M2M v1.0》中要求, 同时满足 DMP 信息订阅消息内的配置要求
3. DMP 接收到 UE 的上报数据后, 将 UE 数据进行存储

8. DMP 与 UE 接口要求

DMP 与 UE 间的通信接口基于 LwM2M 协议, 在 LwM2M 协议以下基于 CoAP 协议, 通信消息包括三部分:

- 第一部分是注册、注销、更新注册消息;
- 第二部分是观测消息、取消观测、消息上报;
- 第三部分是设备管理操作, 包括 read/write/execute/discover 操作。

8.1 协议适配要求

表 8-1 协议适配要求

协议功能	平台状态	终端要求
Client Registration Interface (客户端注册)	支持	UE 注册默认选择的 Binding Mode 为 U (UDP)
Device Management Interface (设备管理)	支持	UE 要求能支持 Read, Write, Execute 指令
Resource Observe and Information Reporting Interface (资源订阅与数据上报)	支持	UE 要求支持 Observe/Cancel observe /Notify
Data Format (数据传输格式)	支持	见 Data Format 表
Transport Layer Bingding & Encoding (传输层模式绑定与编码)	支持	UE 要求支持 U (UDP) 模式

数据传输的类型如下表：

表 8-2 Data Format 表

Data Format	IANA Media Type	Numeric Content-Formats [CoAP]
Plain Text	text/plain	0
Opaque	application/octet-stream	42
TLV	application/vnd.oma.lwm2m+tlv	11542

TLV 示例如下：

08 00 13
C1 01 01
C4 02 3F 80 00 00
C1 03 01
C5 04 54 65 73 74 31

TLV 即 Type-Length-Value 格式，其中 Type 字段表示报文类型，Length 字段表示报文长度，Value 字段表示报文内容。

具体定义如下：

表 8-3 TLV 格式定义

字段	格式与长度	说明
Type	8bit，其中第7位为最高位，第0位为最低位	第 7 和 第 6 位表征 ID 的类型：00 表示 Object Instance，11表示Resource，01、10暂未使用。

		第5位表示ID的长度：0表示ID为8bit，1表示ID为16bit。 第4和第3为表征Length的类型：00表示没有Length字段，第2-第0位即为内容长度；01表示Length字段为8bit，此时应忽略Type字段第2-第0位；10表示Length字段为16bit，此时应忽略Type字段第2-第0位；11表示Length字段为24bit，此时应忽略Type字段第2-第0位。
ID	8bit或16bit无符号整型值	Object Instance或Resource的ID
Length	与Type字段中长度部分对应的0-24bit无符号整型值	内容字段的长度
Value	报文内容	

字段解析如下表：

表 8-4 TLV 示例解析

Type	ID	Length	Value	说明
08(0b00 00 10 00)	0x00	0x13(19字节)	以下四行内容	Object Instance
C1(0b11 00 00 01)	0x01	-	0x01	Resource
C4(0b11 00 01 00)	0x02	-	0x3F 80 00 00	Resource
C1(0b11 00 00 01)	0x03	-	0x01	Resource
C5(0b11 00 01 01)	0x04	-	0x54 65 73 74 31	Resource

UE 读取信息上报的可以是一个 Object Instance 或者一个 Resource，平台侧下发的写消息是一个或者多个 Resource。

8. 2Bootstrap 流程及要求

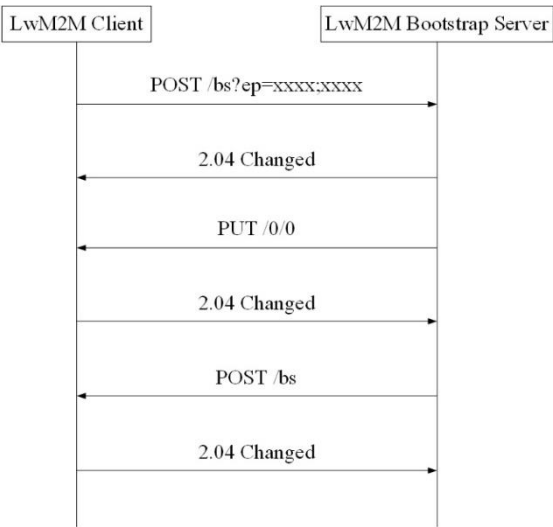


图 8-1 Bootstrap 流程

如图 8-1 所示，DMP 关于 bootstrap 流程主要有 UE 设备上传 bootstrap request 请求，bootstrap server 下发 bootstrap write 请求，bootstrap server 下发 Bootstrap Finish 请求。下面是对三个请求接口的说明。

8.2.1 Bootstrap Request

请求的主要作用为 UE 连接 Bootstrap Server，请求 Bootstrap Server 分配接入机地址。

表 8-5 Bootstrap Request 接口定义

操作	Bootstrap request
LwM2M参数	/bs?ep={endpoint name}
参数说明	{endpoint name}：必选，设备的endpoint name（endpointname 字段可能包含CMEI号码、IMEI号码， IMSI的号码等，各部分内容由特殊的分隔符分开）
CoAP-Method	POST
CoAP-Option	Option 1: Uri-Path (11) : bs, 说明：括号里面的为Option编号 Option 2: Uri-Query (15) : {endpoint name}
CoAP-payload	
Success	2.04 Changed
Failure	4.00 Bad Request, 4.15 Unsupported content format

8.2.2 Bootstrap Write

该接口由 Bootstrap Server 发起，用于 Bootstrap 服务器分配一个接入机地址，写入设备。写入资源路径为/0/0 的 Security 资源模型中。Security Object 的 resource id 为

0 的资源用于承载接入机地址。

表 8-6 Bootstrap Write 接口定义

操作	Bootstrap write
LwM2M参数	/ {Object ID} / {Object Instance ID} / {Resource ID}
参数说明	{Object ID}：必选，标识Object {Object Instance ID}：可选，标识Instance，若未携带该参数，则payload中必须指定Object Instance ID {Resource ID}：可选，标识Resource，若未携带该参数，则payload中必须指定Resource ID
CoAP-Method	PUT
CoAP-Option	Option 1: Uri-Path (11) : {Object ID} Option 2: Uri-Path (11) : {Object Instance ID} Option 3: Uri-Path (11) : {Resource ID} Option 4: Content-Format (12) : 格式为Content Format表中的几种格式，如application/vnd.oma.lwm2m+tlv
CoAP-payload	数据格式为Option4中指定的数据格式
Success	2.04 Changed
Failure	4.00 Bad Request

资源模型简要列表如下：

Resource definitions

ID	Name	Operations	Instances	Mandatory	Type	Range or Enumeration	Units	Description
0	LWM2M Server URI		Single	Mandatory	String	0-255 bytes		Uniquely identifies the LWM2M Server or LWM2M Bootstrap Server, and is in the form: "coaps: //host:port", where host is an IP address or FQDN, and port is the UDP port of the Server.
1	Bootstrap Server		Single	Mandatory	Boolean			Determines if the current instance concerns a LWM2M Bootstrap Server (true) or a standard LWM2M Server (false)
2	Security Mode		Single	Mandatory	Integer	0-3		Determines which UDP payload security mode is used 0: Pre-Shared Key mode 1: Raw Public Key mode 2: Certificate mode 3: NoSec mode

图 8-2 Security Object 资源模型图

8.2.3 Bootstrap Finish

该接口由 Bootstrap Server 发起，用于通知设备整个 bootstrap 过程完成。

表 8-7Bootstrap Finish 接口定义

操作	Bootstrap Finish
LwM2M参数	/bs
CoAP-Method	POST
CoAP-Option	Option 1: Uri-Path (11) : bs, 说明: 括号里面的为Option编号
CoAP-payload	
Success	2.04 Changed
Failure	4.00 Bad Request

8.3 设备注册及注销

8.3.1 设备注册

UE 在每次完成 Bootstrap 流程后向平台发起注册请求，流程如下：

1、UE 向服务器端发送注册请求，服务器端地址为 Bootstrap 过程中由 Bootstrap Server 向 UE 写入的 Security object 中的 resource id 为 0 的资源内容，即接入机地址；

2、服务器端接收到 UE 的注册请求，获取到 EPN，通过对 EPN 提取 EPI，对 EPI 进行鉴权，如果鉴权成功，则返回 success，否则鉴权失败；成功返回的响应中包含 location 值，DMP 为每个 UE 分配一个唯一的 location，默认为 EPI 以及版本号（以“EPI;版本号”格式拼接）。

3、UE 接入后服务器端会记录 UE 的状态信息（如生存时间），并记录 UE 的状态为在线（ONLINE）。

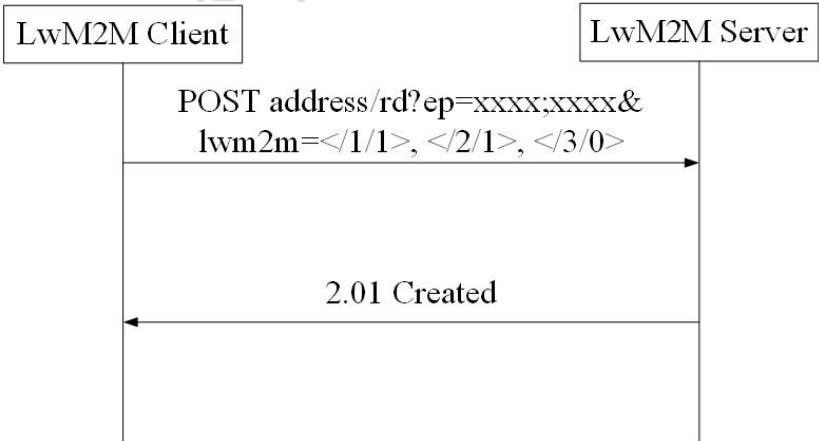


图 8-3 设备注册

表 8-8 注册消息接口详细说明

操作	Register（设备注册消息）
LwM2M 参数	/rd?ep={endpoint name}<={lifetime} &lwm2m={version}&b={binding}&{ObjectLinks}
参数说明	{endpoint name}：必选，设备的 endpoint name（EPN 字段可能包含 CMEI 号码、IMEI 号码， IMSI 号码、版本号等，各部分内容由特

	殊的分隔符分开) {lifetime}: 可选, 默认值为 86400 s (24 小时) {version}: 可选, 默认为 1.0 {binding}: 可选, 默认为 U (即 UDP) {ObjectLinks} : 必选, 如</1/1>, </2/1>, </3/0>
CoAP-Method	POST
CoAP-Option	Option 1: Uri-Path (11): rd, 说明: 括号里面的为 Option 编号 Option 2: Content-Format (12): application/link-format Option 3: Uri-Query (15): {binding} Option 4: Uri-Query (15): {lifetime} Option 5: Uri-Query (15): {endpoint name}
CoAP-payload	LwM2M 协议相关参数加上 {ObjectLinks}, 例如</>;rt="oma.lwm2m",</1/0>,</3/0>,</6/0>
Success	2.01 Created
Failure	4.00 Bad Request, 4.03 Forbidden

8.3.2 设备注册更新消息

- UE 在 lifetime 到期前需要向 DMP 发送注册更新消息, 交互流程如下:
- 1、UE 向平台侧发送 Update 消息, 并携带 UE 注册时平台返回的 location、相应的更新信息(如 lifetime)以及 ObjectLinks 等;
 - 2、平台侧对消息进行鉴权, 如果鉴权成功, 则将对 UE 的相关注册信息进行更新并刷新 lifetime。

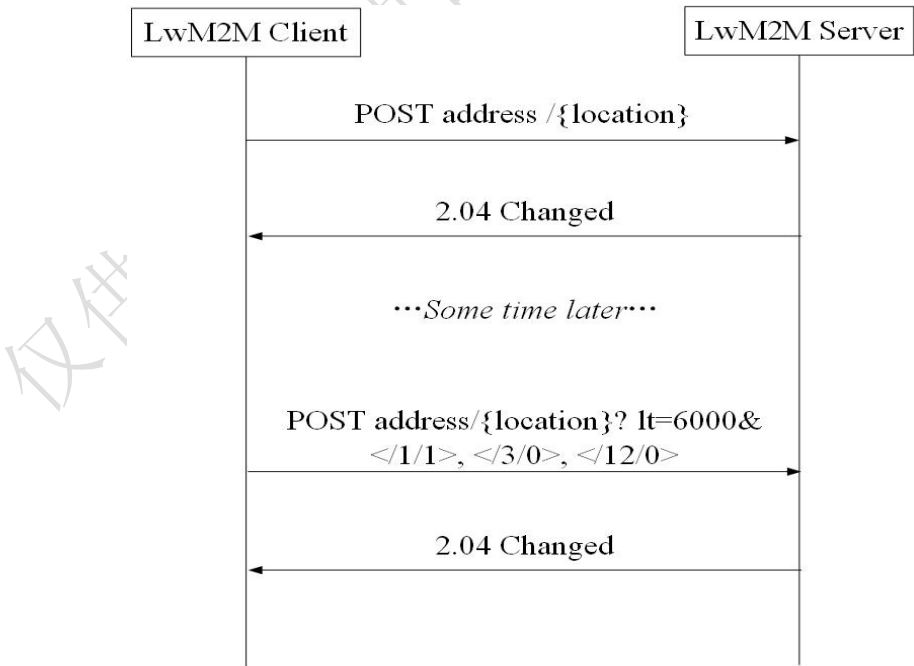


图 8-4 设备注册更新消息

表 8-9 注册消息更新接口详细说明

操作	Update(设备注册更新)
Lwm2m 参数	/ {location} ? lt= {lifetime} & lwm2m= {version} & b= {bingding} & {objectLinks}
参数说明	{location}: 必选，默认值为注册流程中返回的 location。DMP 将 UE 的 EPI 以及版本号（以“EPI;版本号”格式拼接）作为 location 返回 {lifetime}: 可选，默认值为 Register 消息中的 lifetime {version}: 可选，默认为 1.0 {bingding}: 可选，默认为 U（UDP） {ObjectLinks} : 可选，如</1/1>, </2/1>, </3/0>
CoAP-Method	POST
CoAP-Option	Option 1: Uri-Path (11): {location} Option 3: Uri-Query (15): {binding} Option 4: Uri-Query (15): {lifetime}
CoAP-payload	lwm2m 协议相关参数加上 {ObjectLinks}, 例如</>;rt="oma.lwm2m", </1/0>, </3/0>, </6/0>
Success	2.04 Changed
Failure	4.00 Bad Request, 4.04 Not Found

8.3.3 设备注销消息

UE 向 DMP 发起注销消息，脱离 DMP 连接。

- 1、UE 向平台侧发送 De-register 消息，并携带 UE 注册时平台返回的 location；
- 2、平台根据 location 找到对应的设备，删除 UE 的状态信息并设置 UE 状态为下线状态（OFFLINE）。

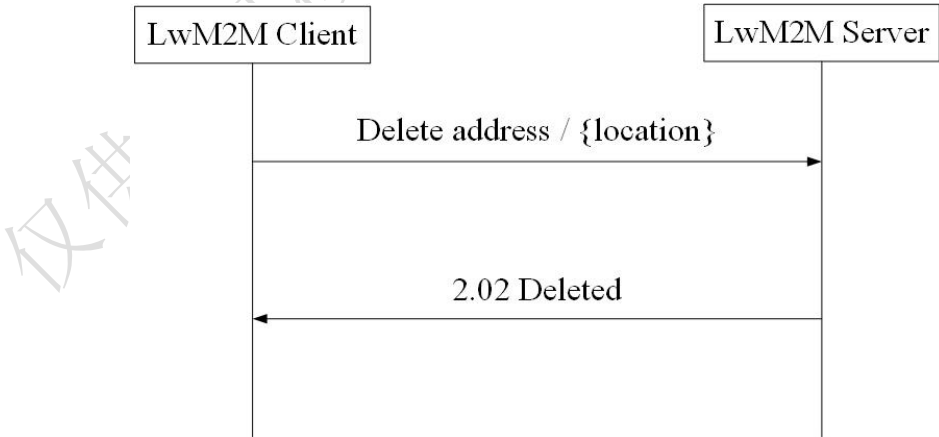


图 8-5 设备注销消息

表 8-10 注销注册消息接口详细说明

操作	De-register（设备注销消息）
LwM2M 参数	/ {location}
CoAP-Method	DELETE
CoAP-Option	Option 1: Uri-Path (11): {location}
CoAP-payload	
参数说明	{location}：必选，默认值为注册流程中返回的 location。DMP 将 UE 的 EPI 以及版本号（以“EPI;版本号”格式拼接）作为 location 返回
Success	2.02 Deleted
Failure	4.00 Bad Request, 4.04 Not Found

8.4 消息观察、取消观察、消息上报、设定 Notify 策略（可选）

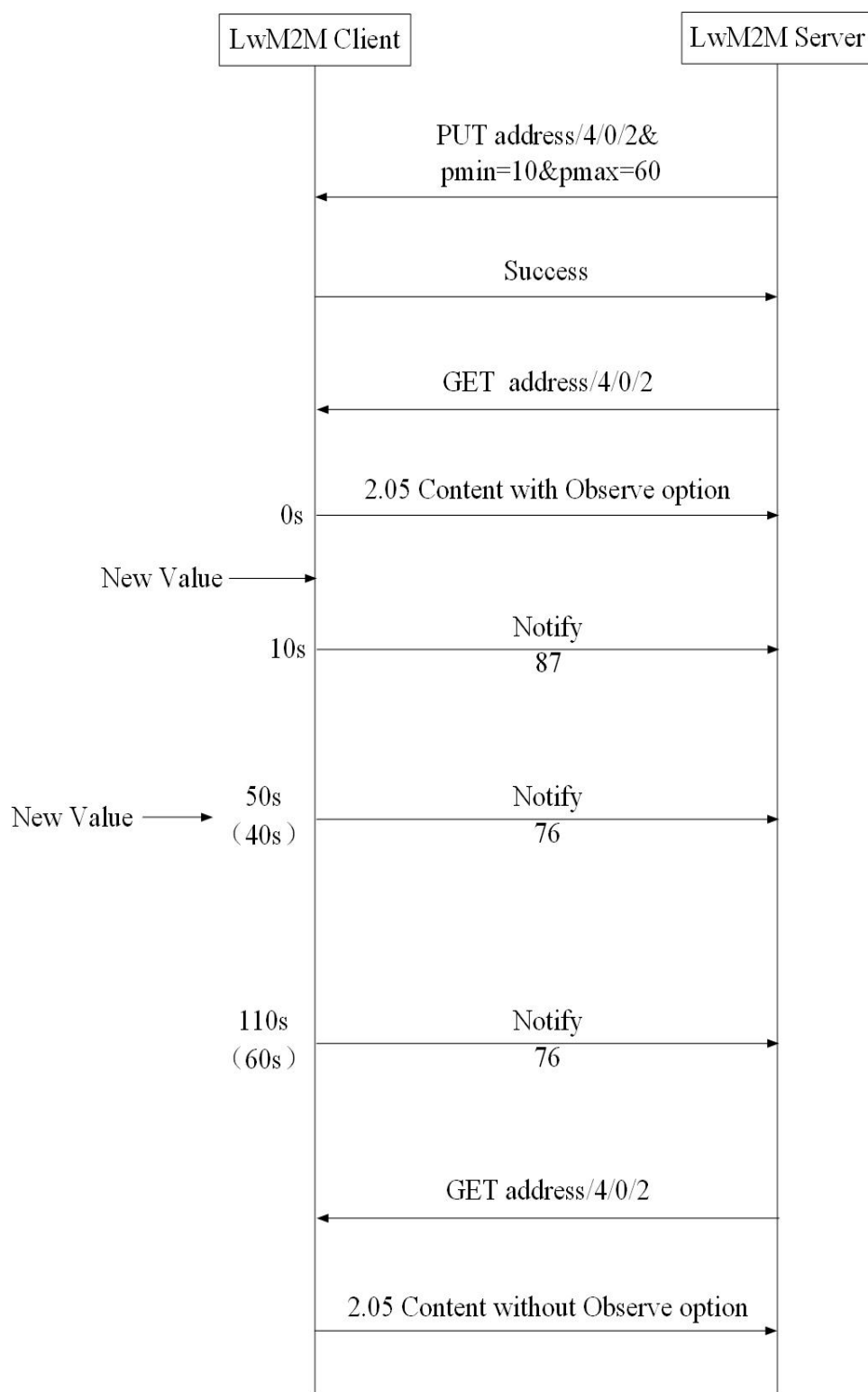


图8-6设定Notify策略、消息观察、取消观察、消息上报

8.4.1 设定 Notify 策略

DMP 会主动向 UE 发送观察参数设置消息 (Write Attributes) 来配置观测资源的策略, UE 收到该消息则返回 Success。

表 8-11 设定 Notify 策略详细说明

操作	Write Attributes (设置)
Lwm2m 参数	/ {ObjectID} / {Object Instance ID} / {Resource ID} & pmin= {Minimum Period} & pmax= {Maximum Period} & gt= {Greater Than} & lt= {Less Than} & stp= {Step}
参数说明	{Object ID}: 必选, 如 UE 上的资源对象 {Object Instance ID}: 可选, 如 UE 资源对象实例的编号 {Resource ID}: 可选, 如 UE 上的资源编号 {Minimum Period}: 可选, 两次上报的最小间隔 {Maximum Period}: 可选, 两次上报的最大间隔 {Greater Than}: 可选, 上报的数值需要大于的数值 {Less Than}: 可选, 上报的数值需要小于的数值 {Step}: 可选, 两次上报数据最小要求的值的变化
CoAP-Method	PUT
CoAP-Option	Option 1: Uri-Path (11): {Object ID} Option 2: Uri-Path (11): {Object Instance ID} Option 3: Uri-Path (11): {Resource ID} Option 4: Uri-Query (15): {Minimum Period} Option 5: Uri-Query (15): {Maximum Period} Option 6: Uri-Query (15): {Greater Than} Option 7: Uri-Query (15): {Less Than} Option 8: Uri-Query (15): {Step}
CoAP-payload	
Success	2.04Changed
Failure	4.00 Bad Request, 4.04 Not Found, 4.01 Unauthorized, 4.05 Method Not Allowed

8.4.2 观察消息

- 1、DMP 主动向 UE 发送观测消息 (Observe) 来观测资源列表中所有可观测的资源, UE 收到该消息后, 检查需要观测的资源是否可以被订阅且状态正常, 如果是则返回 Success;
- 2、UE 在返回 Success 后, 会按照数据上报规则, 上传携带订阅资源具体数值的 Notify 消息 (即相应观测的资源数据值);

表 8-12 观察消息详细说明

操作	Observe (观察消息)
----	----------------

LwM2M 参数	/ {Object ID} / {Object Instance ID} / {Resource ID}
参数说明	{Object ID}：必选，如 UE 上的资源对象 {Object Instance ID}：可选，如 UE 资源对象实例的编号 {Resource ID}：可选，如 UE 上的资源编号
CoAP-Method	GET
CoAP-Option	Option 1: Observe (6): 0 (订阅) Option 2: Uri-Path (11): {Object ID} Option 3: Uri-Path (11): {Object Instance ID} Option 4: Uri-Path (11): {Resource ID} Option 5: Accept (17): Content Format 表中的类型，如 application/vnd.oma.lwm2m+tlv 参数表示订阅后数据上报的格式。
CoAP-payload	
Success	2.05 Content with Observe option
Failure	4.00 Bad Request, 4.04 Not Found, 4.01 Unauthorized, 4.05 Method Not Allowed

8.4.3 取消观察消息

- 1、DMP 端会主动向 UE 发送取消观察消息（Cancel Observe）来取消对资源列表中资源的观察，例如 Cancel Observe /1/0/5，UE 收到该消息则返回 Success；
- 2、UE 在返回 Success 后，会停止上报/1/0/5 的 Notify 消息。

表 8-14 取消观察消息详细说明

操作	Cancel Observe（取消观察消息）
LwM2M 参数	/ {Object ID} / {Object Instance ID} / {Resource ID}
参数说明	{Object ID}：必选，如 UE 上的资源对象 {Object Instance ID}：可选，如 UE 资源对象实例的编号 {Resource ID}：可选，如 UE 上的资源编号
CoAP-Method	GET
CoAP-Option	Option 1: Observe (6): 1 (取消订阅) Option 2: Uri-Path (11): {Object ID} Option 3: Uri-Path (11): {Object Instance ID} Option 3: Uri-Path (11): {Resource ID}
CoAP-payload	
Success	2.05 Content without Observe option
Failure	4.00 Bad Request, 4.04 Not Found, 4.01 Unauthorized, 4.05 Method Not Allowed

8.4.4 数据上报

在满足观察规则的情况下，UE 上报 DMP 需要的信息，直到 DMP 取消观察。

表 8-15 数据上报详细说明

操作	Notify（数据上报）
LwM2M 参数	
CoAP-Method	Asynchronous Response
CoAP-Option	Option 1: Observe (6): 2（数据上报） Option 2: Content-Format (12)，即为 Observe Accept Option 中设置的数据格式
CoAP-payload	{newValue}：上报的数据值
Success	2.05 Content (with Values)
Failure	

8.5 设备管理消息（可选）

UE 资源操作的前提是 UE 和 DMP 保持连接，即 lifetime 未过期。UE 上的资源都具有一定权限，比如可读（R），可写（W），可执行（E）或其组合，如果对一个不支持 R 或者不支持 W 的资源进行读写操作则会返回 Failure 消息到 DMP。

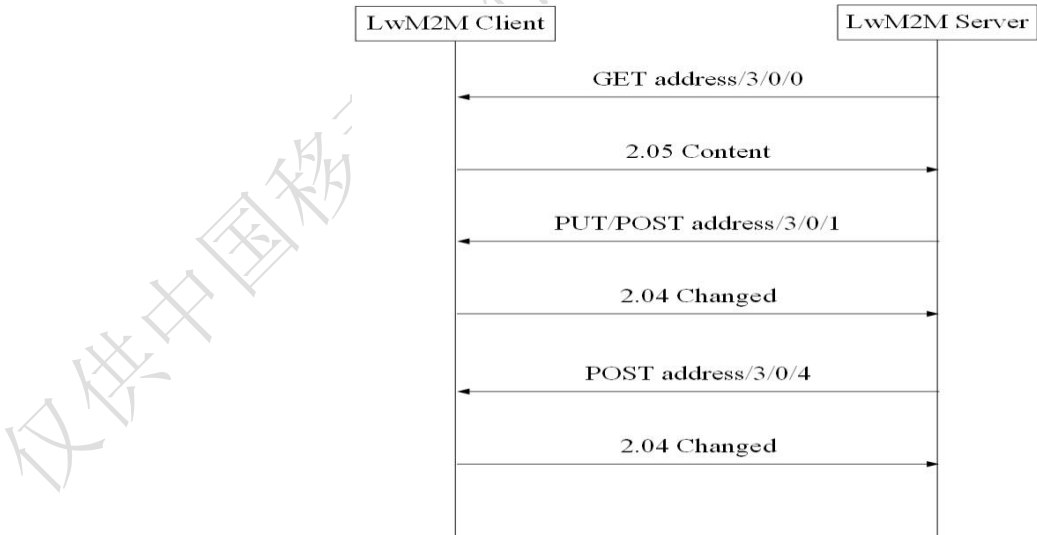


图 8-6 设备管理消息（Read/Write/Execute）

8.5.1 读取资源

- 1、DMP 向 UE 发送 Read 消息
- 2、UE 收到 Read 消息后，获取相应的资源属性值，根据 Read 消息的格式，将读取到的

资源值返回给 DMP，并携带返回码。

表 8-16 读取资源详细说明

操作	Read（资源读取）
Lwm2M 参数	/ {Object ID} / {Object Instance ID} / {Resource ID}
参数说明	{Object ID}：必选，如 UE 上的资源对象 {Object Instance ID}：可选，如 UE 资源对象实例的编号 {Resource ID}：可选，如 UE 上的资源编号
CoAP-Method	GET
CoAP-Option	Option 1: Uri-Path (11): {Object ID} Option 2: Uri-Path (11): {Object Instance ID} Option 3: Uri-Path (11): {Resource ID} Option 4: Accept (17): 第 1 节中的 Content Format 表中的类型， 如 application/vnd.oma.lwm2m+tlv 参数是表示读取数据的格式为 tlv
CoAP-payload	
Success	2.05 Content
Failure	4.00 Bad Request, 4.01 Unauthorized, 4.04 Not Found, 4.05 Method Not Allowed

8.5.2 写入资源

- 1、DMP 向 UE 发送 Write 消息，如 Write /6/0/5 并在消息的负载中携带资源的属性值，资源属性值是单个的，具体根据 Write 消息的格式；
- 2、UE 接收到 Write 消息后，查看对应的资源是否可写，如果可写则将数据写入资源中，然后返回 Success 给 DMP，否则返回 Failure 消息。

表 8-17 写入资源详细说明

操作	Write（资源写入）
Lwm2M 参数	/ {Object ID} / {Object Instance ID} / {Resource ID} / {NewValue}
参数说明	{Object ID}：必选，如 UE 上的资源对象 {Object Instance ID}：必选，如 UE 资源对象实例的编号 {Resource ID}：可选，如 UE 上的资源编号 {NewValue}：必选，写入的资源属性值
CoAP-Method	PUT/POST
CoAP-Option	Option 1: Uri-Path (11): {Object ID} Option 2: Uri-Path (11): {Object Instance ID} Option 3: Uri-Path (11): {Resource ID} Option 4: Content-Format (12): 格式为 Content Format 表中的几

Lwm2M 参数	/ {Object ID} / {Object Instance ID} / {Resource ID}
参数说明	{Object ID}：必选，如 UE 上的资源对象 {Object Instance ID}：可选，如 UE 资源对象实例的编号 {Resource ID}：可选，如 UE 上的资源编号
CoAP-Method	GET
CoAP-Option	Option 1: Uri-Path (11): {Object ID} Option 2: Uri-Path (11): {Object Instance ID} Option 3: Uri-Path (11): {Resource ID}
CoAP-payload	
Success	2.05Content
Failure	4.00 Bad Request, 4.01 Unauthorized, 4.04 Not Found, 4.05 Method Not Allowed

8.5.5 资源创建

- 1、DMP 向终端发送 Create 消息；
- 2、当 UE 接收到 Create 消息后，根据请求的 ObjectLink，创建对应的资源对象，并返回创建成功或失败的响应。

操作	Create（创建资源）
lwm2m-URI	/ {Object ID}
参数说明	{Object ID}：必选，如 UE 上的资源对象
CoAP-Method	POST
CoAP-Option	Option1: Uri-Path (11): {Object ID} Option2: Content-Format (12): 格式为 Content Format 表中的几种格式，如 application/vnd.oma.lwm2m+tlv
CoAP-payload	Value 封装成 TLV 格式放在 payload 里
Success	2.01 Created
Failure	4.00 Bad Request, 4.01 Unauthorized, 4.04 Not Found, 4.05 Method Not Allowed, 4.06 Not Acceptable

8.5.6 资源删除

- 1、DMP 向 UE 发送 Delete 消息；
- 2、当 UE 接收到 Delete 消息后，根据请求的 ObjectLink，删除对应的资源对象，并返回删除成功或失败的响应。

操作	Delete（删除资源）
----	--------------

lwm2m-URI	/ {Object ID} / {Object Instance ID}
参数说明	{Object ID}：必选，如 UE 上的资源对象 {Object Instance ID}：必选，如 UE 资源对象实例的编号
CoAP-Method	DELETE
CoAP-Option	Option1: Uri-Path (11): {Object ID} Option2: Uri-Path (11): {Object Instance ID}
CoAP-payload	
Success	2.02 Deleted
Failure	4.01 Unauthorized, 4.04 Not Found, 4.05 Method Not Allowed

9. 安全要求

9.1 数据解析层安全能力要求

DMP 数据解析层应提供数据安全保护服务，包括数据的权限管理、完整性验证、安全防护、数据备份等。

9.2 数据存储层安全能力要求

- 1. 数据存储层应对访问数据存储层的来源进行合法性验证，确保所有来源的身份合法。
- 2. 数据存储层应根据不同场景、不同应用需求对访问数据存储层的用户、应用和IP进行细粒度的权限控制，防止越权访问。
- 3. 数据存储层应对从数据存储层输出的敏感数据进行脱敏处理，而且脱敏算法可以根据不同场景、用户等具体需求分别配置。
- 4. 数据存储层应对所有访问数据存储层的操作提供集中的日志审计和行为溯源，及时发现可疑操作、系统热点等。
- 5. 数据存储层需要支持密文存储功能，支持加密数据传输。

9.3 设备通用安全要求

网络攻击防范	防止各种网络攻击手段	10G 高性能入侵防御系统设备
Ddos 攻击防范	防范网络 Ddos 攻击	40G 流量清洗设备
鉴权管理	多级权限管理体系，保证访问安全可监控	用户鉴权，应用鉴权，设备鉴权
备份	数据备份	定期备份和热备份

带有资源描述。

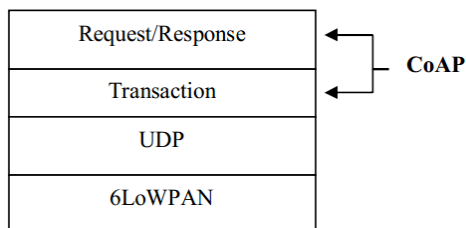


图 A-1 CoAP 协议栈示意图

CoAP 协议采用了双层的结构。事务层(Transaction layer)处理节点间的信息交换，同时，也提供对多播和拥塞控制的支持。请求/响应层(Request/Response layer)用以传输对资源进行操作的请求和相应信息。CoAP 协议的 REST 构架基于该层的通信，REST 请求附在一个 CON 或者 NON 消息上，而 REST 响应附在匹配的 ACK 消息上。CoAP 的双层处理方式，使得 CoAP 没有采用 TCP 协议，也可以提供可靠的传输机制。利用默认的定时器和指数增长的重传间隔时间实现 CON 消息的重传，直到接收方发出确认消息。另外，CoAP 的双层处理方式支持异步通信。

CoAP 协议参见 IETF RFC7252。

2. 应用层协议：

LWM2M 是 OMA 组织制定的轻量化的 M2M 协议。LWM2M 定义了三个逻辑实体：

- LWM2M Server 服务器
- LWM2M client 客户端负责执行服务器的命令和上报执行结果
- LWM2M 引导服务器 Bootstrap server 负责配置 LWM2M 客户端。

在这三个逻辑实体之间有 4 个逻辑接口：

- Device Discovery and Registration: 客户端注册到服务器并通知服务器客户端所支持的能力；
- Bootstrap: Bootstrap server 配置 Client；
- Device Management and Service Enablement: 指令发送和接收；
- Information Reporting: 上报其资源信息的。

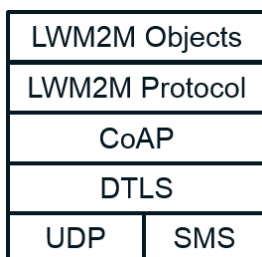


图 A-2 LWM2M 协议栈

1. LWM2M Objects: 每个对象对应客户端的某个特定功能实体. LWM2M 规范定义了一下标准 Objects, 比如
 - 1.2 urn:oma:lwm2m:oma:2; (LWM2M Server Object)
 - 1.3 urn:oma:lwm2m:oma:3; (LWM2M Access Control Object)
 - 1.4 每个 object 下可以有很多 resource. 比如 Firmware object 可以有 Firmware 版本号, size 等 resource.
 - 1.5 Vendor 可以自己定义 object

2. LWM2M Protocol: 定义了一些逻辑操作，比如 Read, Write, Execute, Create or Delete.
 3. CoAP: 是 IETF 定义的 Constrained Application Protocol 用来做 LWM2M 的传输层，下层可以是 UDP 或 SMS.UDP 是必须支持的，SMS 是可选的。CoAP 有自己的消息头，重传机制等。
 4. DTLS: 是用来保证客户端和服务端间的安全性的。
- LWM2M 协议具体参见 OMA Lightweight M2M v1.0。

3. 数据包格式:

a) 传输层协议报文格式:

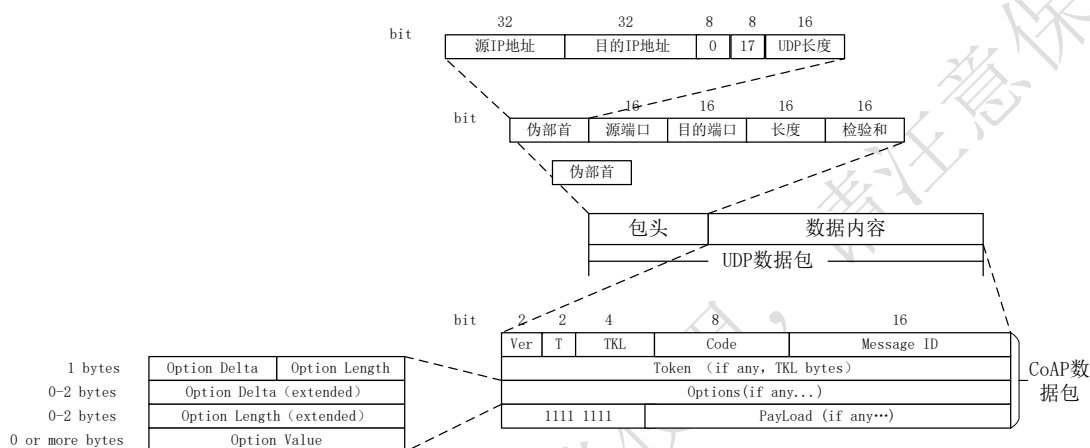


图 A-3 传输层协议报文示意图

传输层为 CoAP 协议报文格式，CoAP 由 UDP 作为承载，遵循 UDP 基本的协议报文格式，UDP 数据内容部分按照 CoAP 协议报文格式进行写入传输。

CoAP 协议格式说明如下：

- **【Ver】** 版本号，指示 CoAP 协议的版本号。类似于 HTTP 1.0 HTTP 1.1。版本号占 2 位，取值为 01B。
- **【T】** 报文类型，CoAP 协议定了 4 种不同形式的报文，CON 报文，NON 报文，ACK 报文和 RST 报文。
- **【TKL】** CoAP 标识符长度。CoAP 协议中具有两种功能相似的标识符，一种为 Message ID（报文编号），一种为 Token（标识符）。其中每个报文均包含消息编号，但是标识符对于报文来说是非必须的。
- **【Code】** 功能码/响应码。Code 在 CoAP 请求报文和响应报文中具有不同的表现形式，Code 占一个字节，它被分成了两部分，前 3 位一部分，后 5 位一部分，为了方便描述它被写成了 c.dd 结构。其中 0.XX 表示 CoAP 请求的某种方法，而 2.XX、4.XX 或 5.XX 则表示 CoAP 响应的某种具体表现。
- **【Message ID】** 报文编号
- **【Token】** 标识符具体内容，通过 TKL 指定 Token 长度。
- **【Option】** 报文选项，通过报文选项可设定 CoAP 主机，CoAP URI，CoAP 请求参数和负载媒体类型等等。
- **【1111 1111B】** CoAP 报文和具体负载之间的分隔符。

CoAP 支持多个 Option，CoAP 的 Option 的表示方法比较特殊，采用增量的方式描述。

一般情况下 Option 部分包含 Option Delta、Option Length 和 Option Value 三部分：

- 【Option Delta】表示 Option 的增量，当前的 Option 的具体编号等于之前所有 Option Delta 的总和。
- 【Option Length】表示 Option Value 的具体长度。
- 【Option Value】表示 Option 具体内容

CoAP 协议报文中具体数值的意义参考 CoAP 协议：IETF RFC7252。

b) 应用层数据包格式：

应用层数据包遵循 LWM2M 协议，根据 LWM2M 定义分为 Read、Discover、Write、Write Attribute、Execute、Create、Delete 7 种操作和 Observe、Notify、Cancel Observation 三种信息上报方式，应用层数据包依赖于 CoAP 协议报文中的【Option】部分进行承载。

以 Read 操作为例：

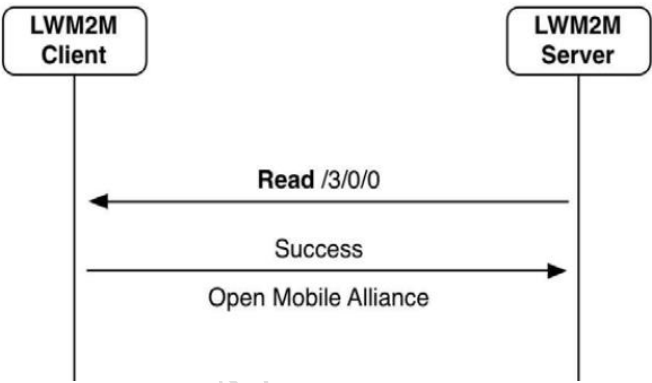


图 A-4 数据读取过程

Server 的 Read 请求数据包：

Ver	T	TKL	01 (GET)	Message ID
Token (if any, TKL bytes)				
Option Delta		Option Length	Object ID (Option Value)	
		Option Length	Object Instance ID (Option Value)	
		Option Length	Resource ID (Option Value)	
1111 1111			PayLoad (if any...)	

图 A-5Read 请求报文

Client 回复数据包：

Ver	T	TKL	01 (GET)	Message ID
Token (if any, TKL bytes)				
Options (if any...)				
1111 1111			Result	

图 A-6 Read 回复报文