

ICS 33.040.01

M 19

YD

中华人民共和国通信行业标准

YD/T 1980-2009

移动通信网 IMS 系统接口技术要求 Mg/Mi/Mj/Mk/Mw/Gm 接口

Technical requirements for Mg/Mi/Mj/Mk/Mw/Gm interface in IMS
system in mobile communication network

2009-12-11 发布

2010-01-01 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 术语、定义和缩略语	1
4 M 系列接口的定义	2
4.1 Mg 接口	2
4.2 Mi 接口	2
4.3 Mj 接口	2
4.4 Mk 接口	2
4.5 Mw 接口	2
4.6 Gm 接口	2
5 M 系列接口在网络中的位置	2
6 M 系列接口的协议	3
7 M 系列接口相关消息和参数的传送	3
7.1 Mg 接口	3
7.2 Mi 接口	5
7.3 Mj 接口	5
7.4 Mk 接口	6
7.5 Mw 接口	6
7.6 Gm 接口	10
附录 A (规范性附录) M 系列接口支持的消息	14
附录 B (规范性附录) M 系列接口支持的消息头	15

前 言

本标准是针对 IMS 系统 Mg/Mi/Mj/Mk/Mw/Gm 接口所做的技术要求，基于 3GPP R6 版本。

本标准是移动通信网络 IMS 系统系列标准之一，该系列标准的结构和名称如下：

- a) YD/T 1980-2009 《移动通信网 IMS 系统接口技术要求 Mg/Mi/Mj/Mk/Mw/Gm 接口》
- b) YD/T 1981-2009 《移动通信网 IMS 系统接口测试方法 Mg/Mi/Mj/Mk/Mw/Gm 接口》
- c) YD/T 1982-2009 《移动通信网 IMS 系统接口技术要求 ISC/Ma 接口》
- d) YD/T 1983-2009 《移动通信网 IMS 系统接口测试方法 ISC/Ma 接口》
- e) YD/T 1984-2009 《移动通信网 IMS 系统设备技术要求》
- f) YD/T 1985-2009 《移动通信网 IMS 系统设备测试方法》
- g) YD/T 1986-2009 《移动通信网 IMS 系统接口技术要求 Cx/Dx/Sh 接口》
- h) YD/T 1987-2009 《移动通信网 IMS 系统接口测试方法 Cx/Dx/Sh 接口》

本标准与 YD/T 1981-2009 《移动通信网 IMS 系统接口测试方法 Mg/Mi/Mj/Mk/Mw/Gm 接口》配套使用。

本标准的附录A、附录B均为规范性附录。

本标准由中国通信标准化协会提出并归口。

本标准起草单位：工业和信息化部电信研究院、诺基亚西门子通信（上海）有限公司、华为技术有限公司、上海贝尔股份有限公司、中兴通讯股份有限公司。

本标准主要起草人：杨红梅、朱 丽、杨雁飞、李 豹、严学强、郝振武。

移动通信网 IMS 系统接口技术要求

Mg/Mi/Mj/Mk/Mw/Gm 接口

1 范围

本标准规定了移动通信网IMS系统中M系列接口以及Gm接口的定义、M系列接口在网络中的位置、M系列接口的协议以及M系列接口相关消息和参数的传送。

本标准适用于移动通信网IMS系统中M系列接口以及Gm接口相关的网络设备和终端设备。

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（以下3GPP的规范暂定为2005年12月版，Release 6）。

3GPP TS 24.229：基于SIP和SDP的IP多媒体呼叫控制协议； Stage 3

3GPP TS 33.203：基于IP业务的接入安全

IETF RFC 2327：SDP：会话描述协议

IETF RFC 3261：SIP：会话初始化协议

IETF RFC 3262：SIP中的临时响应的可靠性

IETF RFC 3266：SDP中支持IPv6

IETF RFC 3311：会话初始化协议（SIP）的UPDATE方法

IETF RFC 3323：会话初始化协议（SIP）的私密性机制

IETF RFC 3329：会话初始化协议（SIP）的安全机制

IETF RFC 4028：会话初始化协议（SIP）中的会话定时器

IETF RFC 3325：在信任域中的Asserted Identity标识的SIP私人扩展

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标准。

3.1.1

注册消息

即SIP REGISTER消息。

3.1.2

初始消息

不包括SIP REGISTER消息；可以是一个新对话建立的发起消息（例如INVITE、SUBSCRIBE消息），也可以是一个独立事务消息（例如MESSAGE、OPTIONS等消息）。

3.1.3

后继消息

不包括SIP REGISTER消息；是已建立对话中的消息（例如UPDATE、ReINVITE、PRACK、BYE等消息）。

3.2 缩略语

下列缩略语适用于本标准。

HSS	Home Subscriber Server	归属用户服务器
P-CSCF	Proxy Call Session Control Function	代理呼叫会话控制功能
I-CSCF	Interrogating Call Session Control Function	查询呼叫会话控制功能
S-CSCF	Serving Call Session Control Function	服务呼叫会话控制功能
BGCF	Breakout Gateway Control Function	中断出口网关控制功能
MGCF	Media Gateway Control Function	媒体网关控制功能
SA	Security Association	安全联盟

4 M系列接口的定义

4.1 Mg 接口

Mg接口是MGCF和CSCF之间的接口，用于PSTN/CS会话互通。

4.2 Mi 接口

Mi接口在CSCF和BGCF之间，允许S-CSCF前转会话到BGCF，用于与PSTN网络的交互。

4.3 Mj 接口

Mj接口允许BGCF前转会话信令MGCF，用于与PSTN网络的交互。

4.4 Mk 接口

Mk接口允许BGCF前转会话信令到另一个BGCF。

4.5 Mw 接口

Mw接口在CSCF之间，支持IMS核心网络实体之间的所有信令流程，包括注册、会话建立、更新、释放等。

4.6 Gm 接口

Gm接口在终端和IMS网络之间，主要传输用户和CSCF之间的注册、用户业务控制以及鉴权等相关的流程。

5 M系列接口在网络中的位置

M系列接口在网络中的位置如图1所示，Mg接口位于MGCF和CSCF之间，Mi接口位于CSCF和BGCF之间，Mj接口位于BGCF和MGCF之间，Mk接口位于不同BGCF之间，Mw接口在不同CSCF之间，包括同一运营商的不同CSCF之间以及不同运营商的CSCF之间，Gm接口位于终端和IMS网络之间。

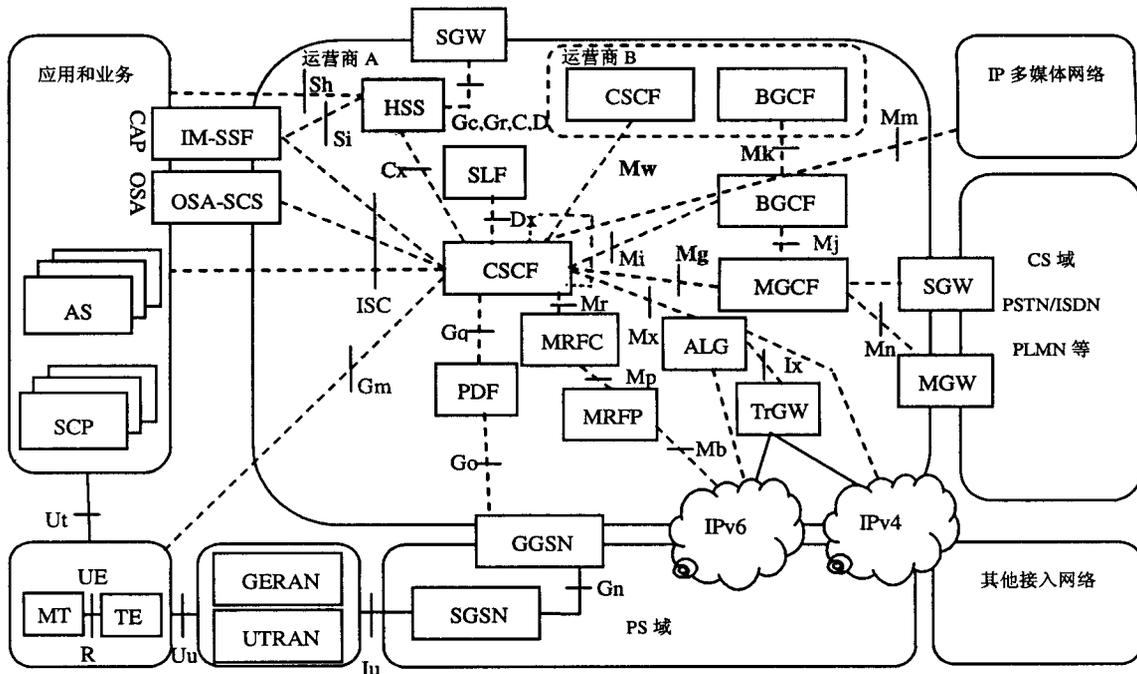


图1 M 系列接口在网络中的位置

6 M 系列接口的协议

M系列接口使用SIP协议，基本协议遵照IETF RFC3261，也应支持其他关于SIP扩展的IETF规范，具体扩展见附录A和附录B。

7 M 系列接口相关消息和参数的传送

7.1 Mg 接口

7.1.1 协议层次模型

Mg接口协议栈如图2所示。

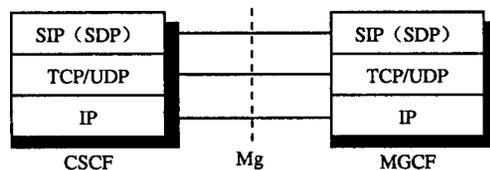


图2 Mg 接口协议栈

7.1.2 初始呼叫

7.1.2.1 PLMN/PSTN 始发的呼叫

当MGCF收到呼叫来源于PLMN/PSTN的指示时，MGCF应产生INVITE请求给I-CSCF。

- 将 Request-URI 设置成 E.164 地址 tel 格式。
- 在 Supported 头中含有标记 100rel。
- 根据电路域中的相应信息插入 P-Asserted-Identity 头。
- 建立新的惟一的 icid 值并将其插入 P-Charging-Vector 头。
- 插入第二类 orig-ioi，第二类 orig-ioi 应能够标识 MGCF 所在的网络。

- 说明本地 precondition 的状态。
- 在 SDP 中说明 MGW 所支持的编码格式，最希望采用的编码格式排在最前。
- 如果支持 DTMF，SDP 中的 MIME 子类型应包括“telephone-event”。

当发送 SDP 时，MGCF 不能包括“i=”，“u=”，“e=”，“p=”，“r=”，“z=”；当接收 SDP 时忽略上述参数。

当 MGCF 收到 1XX 或 2XX 初始请求的回应消息时，MGCF 应保存 P-Charging-Vector 头中的 term-ioi 值以标识发送初始请求回应消息的网络。

当 MGCF 收到 INVITE 消息的 183 响应时，应保存 P-Charging-Function-Addresses 头，并检查 SDP 中是否包含 MGW 所支持的编解码列表。

当 MGCF 收到 PRACK 的 200 OK 响应并且从 CS 域收到的 COT 消息中连续性指示（Continuity Indicators）设为“continuity check successful”，应发送 UPDATE 请求。

7.1.2.2 PLMN/PSTN 终结的呼叫

当 MGCF 收到 IMS 域的 INVITE 请求且其中 Supported 头的值为 100rel 时，MGCF 应：

- 1) 存储 P-Charging-Vector header 中的 orig-ioi 参数。
- 2) 向 IMS 域发送 100 Trying 消息。
- 3) 如果对 MGW 的编解码没有要求，或者对 MGW 的编解码有要求并找到匹配的编解码之后向 IMS 域发送 183 “Session Progress”。

- Require 头设成 100rel。
- 存储 P-Charging-Function-Addresses 中的参数值。
- 存储 P-Charging-Vector 头中的 icid 值。
- 向 P-Charging-Vector 插入从初始 INVITE 消息中携带的 orig-ioi 参数以及第二类 term-ioi 参数。第二类 term-ioi 参数应设置为 MGCF 所在的网络，orig-ioi 参数应设置为前面所存储的 orig-ioi 值。

- 在 SDP 中说明所选择的编解码，并可包括 MIME 子类型“telephone-event”。

- 4) 如果对 MGW 的编解码有要求而 MGCF 没有在 MGW 找到相匹配的编解码，MGCF 应：

- 如果编解码类型可接受但不可用，回应 503（Service Unavailable）。
- 如果编解码类型不支持，回应 488（Not Acceptable Here），并可以在消息体中包含 SDP 说明 MGCF/MGW 所支持的编解码。

当发送 SDP 时，MGCF 不能包括“i=”，“u=”，“e=”，“p=”，“r=”，“z=”；当接收 SDP 时忽略上述参数。

当 MGCF 收到 PLMN/PSTN CS 域被叫振铃的指示，应通过 IMS 域向主叫 UE 发送 180 Ringing 消息。

当 MGCF 收到 PLMN/PSTN CS 域被叫用户应答的指示时，应通过 IMS 域向主叫 UE 发送 200 OK 消息。如果从 CS 域中收到了相应的信息，200 OK 消息中应包括 P-Asserted-Identity 头域。

其中 Supported 头的值不包含 100rel 时，MGCF 在 200 OK 中返回编码的能力集，如果有 183，则应于 183 中的保持一致。

7.1.3 呼叫释放

7.1.3.1 CS 域发起的呼叫释放

当从 CS 域收到呼叫释放指示时，MGCF 应通过 IMS 域向 UE 发送 BYE 消息。

7.1.3.2 IMS 域发起的呼叫释放

当从 IMS 域收到 BYE 消息时，MGCF 应向 CS 域发起呼叫释放请求。

7.1.3.3 MGW 发起的呼叫释放

当从 MGW 收到承载丢失的指示时，MGCF 应通过 IMS 域向 UE 发送 BYE 消息，并向 CS 域发起呼叫释放请求。

7.2 Mi 接口

7.2.1 接口协议栈

Mi 接口位于 BGCF 与 S-CSCF 之间，用于选择电路域的出口网关 MGCF。S-CSCF 转发 SIP 请求到 BGCF，进而路由到 PSTN 或者 CS。

Mi 接口协议栈如图 3 所示。

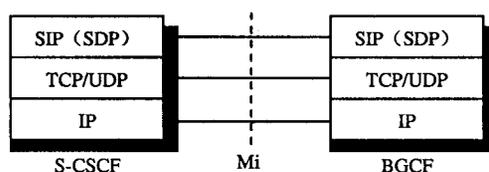


图3 Mi 接口协议栈

S-CSCF 将不能直接查询到下一跳路由的 SIP 初始 Invite 消息传递给 BGCF。S-CSCF 进行 Request-URI E.164 地址翻译，如果该翻译成功，会话按照返回的 SIP URI 路由。如果翻译失败，会话将路由至 BGCF。

BGCF 不需要支持 Path 和 Service-Route 头域的要求。

BGCF 在进一步转发所有非 ACK、CANCEL 的请求和响应消息时，都可以根据预先配置或者保存的数据插入 P-Charging-Vector 和 P-Charging-Function-Addresses 头域。

7.2.2 会话初始化事务的处理

BGCF 不需要记录 INVITE 消息的 Record-Route。由于 BGCF 的下一个转接网元可能是一个具有 UA 功能的 MGCF，BGCF 不需要按照 IETF RFC 3323 实现 privacy。

BGCF 收到 Mi 接口的 SIP 初始 Invite 消息时，应：

- 首先保存消息中 P-Charging-Function-Addresses 头域的地址信息，同时记录 P-Charging-Vector 中的 icid。
- 如果 BGCF 将本身的地址插入 Record-Route 头域，BGCF 可能根据 IETF RFC 4028 要求会话周期性的刷新状态。

BGCF 分析 SIP Invite 的 Request-URI 的电话号码，比对事先配置的编号方案，选择 MGCF 或者 BGCF。为了完成成功的选择，每个 Request-URI 的电话号码都应该与一定的 MGCF 或者 BGCF 相关联。

7.3 Mj 接口

7.3.1 接口协议栈

Mj 接口使用 SIP 协议，基本协议遵照 IETF RFC 3261 及关于 SIP 扩展的其他 IETF 规范。Mj 接口协议栈如图 4 所示。

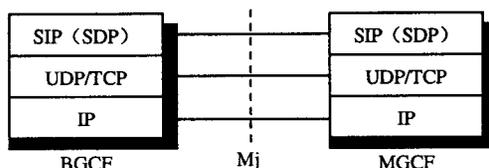


图4 Mj 接口协议栈

7.3.2 Mj 接口呼叫处理

Mj接口相关消息和参数的传递需遵循如下规定：

- a) Mj接口不需支持Service-Route和Path消息头；
- b) 当BGCF转发任何对话相关或独立事务处理的SIP请求/响应（除ACK/CANCEL请求及其响应）至MGCF时，可以插入以前存储的P-Charging-Vector和P-Charging-Function-Address；
- c) BGCF在转发INVITE请求至MGCF时，不需要添加Record-Route消息头；如果需要添加Record-Route消息头，BGCF可以根据IETF RFC4028要求进行会话的刷新（Refreshment）；
- d) BGCF在转发INVITE请求至MGCF时，BGCF应不执行IETF RFC 3323中关于Privacy的相关处理；
- e) BGCF应存储收到的P-Charging-Vector中的icid参数，P-Charging-Function-Address消息头；
- f) 除上述规定和IETF RFC 3261中Stateful Proxy的相关处理外，BGCF应能透传收到的响应，当BGCF将其放入Record-Route中时，BGCF应能透传后续的请求和响应。

7.4 Mk 接口

7.4.1 接口协议栈

Mk接口使用SIP协议，基本协议遵照IETF RFC3261及关于SIP扩展的其他IETF规范。不支持Path和Service-Route头字段的应用，同时不能应用IETF RFC 3323中与私密性相关的处理流程。Mk接口协议栈如图5所示。

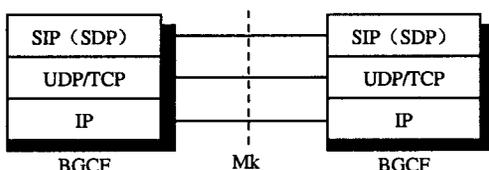


图5 Mk 接口协议栈

7.4.2 Mk 接口呼叫处理

当BGCF接收到请求时，将根据从其他协议或数据库获得的信息，决定请求的路由。如果需要将请求前转到其他网络，则通过Mk接口将请求前转到其他网络的BGCF。如果根据本地策略要求拓扑隐藏，BGCF通过I-CSCF将SIP信令转发到其他网络的BGCF。BGCF应保存接收到的P-Charging-Function-Addresses头字段和P-Charging-Vector头字段icid参数中的值，可以在前转接收到的后续请求和响应（除了ACK和CANCEL请求和响应）之前，插入保存的值。

在向下一个BGCF前转时，BGCF不需修改Request-URI，也不需要INVITE请求插入Record-Route。如果BGCF要求应用Record-Route，则BGCF应支持会话定时刷新功能，以避免会话挂起。

7.5 Mw 接口

7.5.1 接口协议栈

Mw接口协议栈如图6所示。

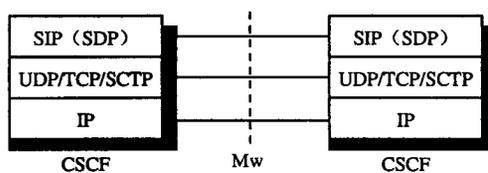


图6 Mw 接口协议栈

7.5.2 注册消息

7.5.2.1 从 P-CSCF 到 I-CSCF 的请求

P-CSCF通过对Request-URI进行DNS查询，最终得到其归属网络I-CSCF的地址，P-CSCF利用Mw接口向该I-CSCF前转请求，其中重要消息头和消息参数传送情况如下：

- 添加 Require 消息头，其中含有标记“Path”。
- 添加 Path 消息头，其值为 P-CSCF 的 SIP URI，并且含有表示“UE Terminating”情况的方向指示信息。
- 添加 P-Visited-Network-ID 消息头，其值为 P-CSCF 对应拜访网络的字符串标识。
- 添加 P-Charging-Vector 消息头，其中含有参数 icid-value 和其对应值。
- 删除 Security-Client 和 Security-Verify 消息头（如果存在）。
- 在 Authorization 消息头中增加 integrity-protected 参数，根据情况设置其对应值为“yes”或者“no”。

7.5.2.2 从 I-CSCF 到 S-CSCF 的请求

I-CSCF通过HSS返回的UAA消息（可能只包含S-CSCF的SIP URI，也可能只包含S-CSCF的能力集，或者两者兼而有之），最终得到S-CSCF的SIP URI，I-CSCF利用Mw接口前转请求给此S-CSCF，其中相关重要消息头和消息参数传送情况如下：更改Request-URI的对应值为S-CSCF的SIP URI。

7.5.2.3 从 S-CSCF 到 I-CSCF 的 401 响应

S-CSCF收到未受保护的注册请求后，通过与HSS的MAR/MAA交互，便利用Mw接口向I-CSCF返回401响应，其中相关重要消息头和消息参数传送情况如下：添加WWW-Authenticate消息头，其中realm字段设置为其对应归属网络标识，algorithm 字段设置为“AKAv1-MD5”，ck和ik字段设置为MAA返回五元组中的ck和ik，nonce字段则根据MAA返回五元组中的rand和auth以及其他数据组合的一个特殊值。

7.5.2.4 从 I-CSCF 到 P-CSCF 的 401 响应

I-CSCF直接利用Mw接口前转401响应给P-CSCF。

7.5.2.5 从 S-CSCF 到 I-CSCF 的 200 响应

S-CSCF收到已经受保护的注册请求后，通过与HSS的SAR/SAA交互，利用Mw接口向I-CSCF返回200响应，其中相关重要消息头和消息参数传送情况如下：

- 添加 Path 消息头，并复制其对应的注册请求消息中的 Path 消息头。
- 添加 Service-Route 消息头，其值为 S-CSCF 的 SIP URI，并且含有表示“UE Originating”情况的方向指示信息。
- 添加 P-Associated-URI 消息头，其中包含 SAR 返回的“公有标识”中所有非禁止的 IMPU。
- 添加 Contact 消息头，其中包含与该注册 IMPU 相绑定的所有 contact 地址。
- 如果 S-CSCF 与 P-CSCF 在同一网络中，那么添加 P-Charging-Function-Addresses 消息头，其 ccf 和 ecf 参数值从 SAA 返回的“Charging-Information”字段提取得来。

7.5.2.6 从 I-CSCF 到 P-CSCF 的 200 响应

I-CSCF直接利用Mw接口前转200响应给P-CSCF。

7.5.3 初始消息

7.5.3.1 终端始发流程

7.5.3.1.1 从 P-CSCF 到 S-CSCF 的请求

P-CSCF收到请求后,首先判断出该请求为MO流程的请求,然后通过Route消息头得到下一跳的地址,即S-CSCF的SIP URI, P-CSCF利用Mw接口前转请求给此S-CSCF,其中相关重要消息头和消息参数传送情况如下:

- 删除 Require 和 Proxy-Require 消息头中的“sec-agree”标记。
- 删除 Security-Verify 消息头(如果存在)。
- 删除 P-Preferred-Identity 消息头(如果存在)。
- 添加 P-Asserted-Identity 消息头,其值可以是 P-Preferred-Identity 消息头中的值,也可以是 7.5.2.5 节中 P-Associated-URI 消息头中的首个 URI 值。
- 添加 P-Charging-Vector 消息头,其中含有参数 icid-value 和其对应值。
- 如果该消息是一个新对话建立的发起消息,那么在 Record-Route 消息头的最顶端加上 P-CSCF 的 SIP URI。

7.5.3.1.2 从 S-CSCF 到 P-CSCF 的响应

S-CSCF直接利用Mw接口前转响应给P-CSCF,其中相关重要消息头和消息参数传送情况如下:删除 P-Charging-Vector消息头中的orig-ioi、term-ioi参数和其对应值(如果存在)。

7.5.3.2 终端终止流程

7.5.3.2.1 从 S-CSCF 到 P-CSCF 的请求

S-CSCF收到请求后,首先判断出该请求为MT流程的请求,然后在注册流程中自身保存预载路由列表得到下一跳的地址,即P-CSCF的SIP URI, S-CSCF利用Mw接口前转请求给此P-CSCF,其中相关重要消息头和消息参数传送情况如下:

- 更改 Request-URI 的对应值为被叫 UE 的 contact 地址。
- 添加 P-Called-Party-ID 消息头,其值为原先的 Request-URI 值,即被叫 UE 的 IMPU。
- 删除 P-Charging-Vector 消息头中 orig-ioi 参数和其对应值(如果存在)。
- 如果 P-CSCF 与 S-CSCF 在同一网络中,那么添加 P-Charging-Function-Addresses 消息头(如果原先消息不含此头),其 ccf 和 ecf 参数值从 SAA 返回的“Charging-Information”字段提取得来。
- 如果该消息是一个新对话建立的发起消息,那么在 Record-Route 消息头的最顶端加上 S-CSCF 的 SIP URI。

7.5.3.2.2 从 P-CSCF 到 S-CSCF 的响应

P-CSCF直接利用Mw接口前转响应给S-CSCF,其中相关重要消息头和消息参数传送情况如下:

- 删除 P-Preferred-Identity 消息头(如果存在)。
- 添加 P-Asserted-Identity 消息头,其值设置为在 MT 流程 P-CSCF 到 UE 的 Gm 接口流程中保存的 P-Called-Party-ID 消息头中的值。
- 添加 P-Charging-Vector 消息头,并含有参数 icid-value,其值设置为在 xxx 节中保存的 icid-value 值。

7.5.3.3 SS 流程（主叫 S-CSCF 到被叫 S-CSCF）

7.5.3.3.1 从 S-CSCF（主叫）到 I-CSCF（被叫）的请求

S-CSCF收到请求后，首先判断出该请求为MO流程的请求，然后通过对Request-URI进行ENUM/DNS查询，最终得到被叫UE归属网络的I-CSCF的地址，S-CSCF利用Mw接口前转请求给此I-CSCF，其中相关重要消息头和消息参数传送情况如下：

- 更改 Request-URI 的对应值为 ENUM 查询得到的 SIP URI 格式(如果原先 Request-URI 的值是 TEL URI 格式)。
- 如果原先 P-Asserted-Identity 中是一个 SIP URI 格式,并且 S-CSCF 能够感知与其相关联的 TEL URI 格式,那么在 P-Asserted-Identity 消息头中添加这个 TEL URI 格式。
- 在 P-Charging-Vector 消息头中添加 orig-ioi 参数,其值设为 S-CSCF 自身所在网络的标识符。
- 如果 I-CSCF 与 S-CSCF 在同一网络中,那么添加 P-Charging-Function-Addresses 消息头,其 ccf 和 ecf 参数值从 SAA 返回的“Charging-Information”字段提取得来。
- 如果该消息是一个新对话建立的发起消息,那么在 Record-Route 消息头的最前端加上 S-CSCF 的 SIP URI。

7.5.3.3.2 从 I-CSCF（被叫）到 S-CSCF（被叫）的请求

I-CSCF通过HSS返回的LIA消息（可能只包含S-CSCF的SIP URI，也可能只包含S-CSCF的能力集，或者可能两者兼而有之），最终得到被叫归属网络S-CSCF的SIP URI，I-CSCF利用Mw接口前转请求给此S-CSCF。

7.5.3.3.3 从 S-CSCF（被叫）到 I-CSCF（被叫）的响应

S-CSCF直接利用Mw接口前转响应给I-CSCF，其中相关重要消息头和消息参数传送情况如下：

- 添加 P-Charging-Function-Addresses 消息头,其 ccf 和 ecf 参数值从 SAA 返回的“Charging-Information”字段提取得来。
- 在 P-Charging-Vector 消息头中添加 term-ioi 参数,其值设为 S-CSCF 自身所在网络的标识符,并在 P-Charging-Vector 消息头中添加,其值设为 7.5.3.2.1 节中保存的 orig-ioi 值。
- 如果原先 P-Asserted-Identity 中是一个 SIP URI 格式,并且 S-CSCF 能够感知与其相关联的 TEL URI 格式,那么在 P-Asserted-Identity 消息头中添加这个 TEL URI 格式。

7.5.3.3.4 从 I-CSCF（被叫）到 S-CSCF（主叫）的响应

I-CSCF直接利用Mw接口前转响应给S-CSCF，其中相关重要消息头和消息参数传送情况如下：如果S-CSCF与I-CSCF不在同一个网络，那么删除P-Charging-Function-Addresses消息头。

7.5.4 后继消息

7.5.4.1 MO 流程

7.5.4.1.1 从 P-CSCF 到 S-CSCF 的请求

P-CSCF收到请求后，直接根据Route消息头得到下一跳的地址，即S-CSCF的SIP URI，P-CSCF利用Mw接口前转请求给此S-CSCF，其中相关重要消息头和消息参数传送情况如下：

- 删除 Require 和 Proxy-Require 消息头中的“sec-agree”标记。
- 删除 Security-Verify 消息头（如果存在）。

7.5.4.1.2 从 S-CSCF 到 P-CSCF 的响应

S-CSCF直接利用Mw接口前转响应给P-CSCF。

7.5.4.2 MT 流程

7.5.4.2.1 从 S-CSCF 到 P-CSCF 的请求

S-CSCF收到请求后，直接根据Route消息头得到下一跳的地址，即P-CSCF的SIP URI，S-CSCF利用Mw接口前转请求给此P-CSCF。

7.5.4.2.2 从 P-CSCF 到 S-CSCF 的响应

P-CSCF直接利用Mw接口前转响应给S-CSCF。

7.5.4.3 SS 流程

7.5.4.3.1 从 S-CSCF（发起端）到 S-CSCF（接受端）的请求

S-CSCF（发起端）收到请求后，直接根据Route消息头得到下一跳的地址，即S-CSCF（接受端）的SIP URI，S-CSCF（发起端）利用Mw接口前转请求给此S-CSCF（接受端）。

7.5.4.3.2 从 S-CSCF（接受端）到 S-CSCF（发起端）的响应

S-CSCF（接受端）直接利用Mw接口前转响应给S-CSCF（发起端）。

7.6 Gm 接口

7.6.1 接口协议栈

Gm接口是UE和P-CSCF之间的接口，主要负责注册和会话控制。

Gm接口协议栈如图8所示。

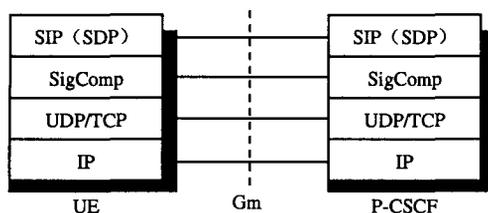


图8 Gm 接口协议栈

注：SIP/SDP主要遵循3GPP 24.229,IETF RFC3261、IETF RFC2327/IETF RFC3266以及相关的SIP扩展。SigComp遵循IETF RFC3320。

7.6.2 注册/注销

任何在注册成功前或者注销成功后收到的事务都应该被UE拒绝。

7.6.2.1 注册（UE 未注册）

UE发送REGISTER请求，需要在相关头域里面填写下列信息。

a) Authorization 头域，包含：

- 用户指示，设置成用户的私有 ID；
- 域名指示，设置成归属网络的域名；
- uri 指示，设置成归属网络的 SIP URI 域名；
- nonce 指示，设置成空；
- 响应指示，设置成空。

b) From 头域，设置成将要注册的用户公共 ID 的 SIP URI。

c) To 头域，设置成将要注册的用户公共 ID 的 SIP URI。

d) Contact 头域, SIP URI, 包含 UE 的 IP 地址或者 FQDN。如果 REGISTER 请求被 SA 保护, UE 的保护端口也应该在 Contact 中体现。

e) Via 头域, 设置成 UE 的 IP 地址或 FQDN。

f) Expires 头域, 或者在 Contact 头中的 expires 参数, 设置成 600 000s。

g) Request-URI, 设成归属网络的 SIP URI 域名。

h) Security-Client 头域, 表示了 UE 支持的安全机制, IPSec 算法, 以及安全联盟所需的参数。

i) Supported 头域, 保护可选 tag “path”。

j) 如果安全关联存在, P-Access-Network-Info 头域表示 UE 接入网络的类型和相关信息。

当 UE 收到 401 (未授权) 响应时, UE 应从响应中提取 RAND 和 AUTN, 按 TS 33.203 中的要求检查授权的有效性, 按 IETF RFC3329 检查 Security-Server 头域, 如果 Security-Server 不存在或者存在但不包含建立 SA 的参数, UE 需要放弃该次注册, 用新的 Call-ID 重新发起新的注册请求。

如果上述检查有效, UE 应按 TS33.203 计算出 RES 参数, 从 RAND 中得到 CK 和 IK, 并与 P-CSCF 建立临时的 SA。UE 需要发起另一个 REGISTER 请求, 使用临时的 SA 来保护消息。头域里面除了与初始请求相同的内容外, 增加了 Authorization、Security-Client 和 Security-Verify 头域。

— Authorization: 包含从收到的 401 响应 WWW-Authenticate 头域中得到的域名, 用户私有标识, 以及 UE 通过 RES 和其他参数计算出来的鉴权响应;

— Security-Client: 与之前 REGISTER 请求中的 Security-Client 相同;

— Security-Verify: 反应了接收到 401 响应中的 Security-Server 头域中的安全协定。

当 UE 收到 200 OK 响应时, 应该新建立 SA 替换掉原来临时的 SA, 并且在后续与 P-CSCF 消息交互中使用这个 SA。UE 需要保存 To 头域中的注册有效时长, 把 P-Associated-URI 中的 URI 列表的第一个 URI 作为默认的公共用户标识, 保存 Service-Route 并与 UE 相关联。

7.6.2.2 重注册

在初始注册完成后, UE可以在任何时候进行重注册, 但是应用在与contact地址相关的那个安全联盟上进行重注册。

7.6.2.3 隐式注册

如果是隐式注册, UE 将在收到的 200OK (对应 REGISTER 请求) 中得到多个 IMPU, 由 P-Associated-URI 标识。UE 需要根据 P-Associated-URI 头域中的信息保存已注册的 URI 列表。

有些 IMPU 可能会被禁止, P-Associated-URI 头域中包含的只是未被禁止的 ID。

UE 将使用 P-Associated-URI 的第一条作为默认的公共标识。

7.6.2.4 注册事件订阅

在收到初始注册请求2xx响应后, UE应通过SUBSCRIBE向S-CSCF订阅注册状态事件包。当注册状态发生变化时, S-CSCF可以通过NOTIFY通知UE。

UE可以使用默认的IMPU或者初始注册时使用的IMPU进行订阅。

在发送 SUBSCRIBE 请求时, UE 需要在相关头域里面填写下列信息:

a) Request URI, 设置成 UE 希望订阅的标识, 如 SIP URI。

b) From 头域。

c) To 头域。

- d) Event 头域, 设成 “reg”, 表示用户订阅的是注册状态包。
 - e) Expires 头域, 把订阅期限设成 600 000s。
 - f) P-Access-Network-Info 头域, 指示接入网络信息。
 - g) Contact 头域, 包含相同的 IP 地址或 FQDN, 以及初始注册时使用的保护端口。
 - h) Accpet 头域, 设置成 “application/reginfo+xml”。
- S-CSCF发送NOTIFY给UE, 通知UE注册状态的变化, P-CSCF转发该NOTIFY给UE。
NOTIFY请求中的消息体包含了用户的注册状态, 具体格式见3GPP TS24.229。

7.6.2.5 注销

a) UE发起的注销

在发起注销前, UE应该释放与需要注销的IMPU相关的所有会话。该过程与初始注册的过程相似, 在消息中的增加Expires: 0或者Contact头域的expires=0。这个REGISTER是经过鉴权的。

对UE来说, 如果已经没有注册的IMPU, UE应该删除SA和相关的密钥。如果所有的IMPU和SA都删除后, UE应该认为其订阅的注册事件包也被取消了。

b) 网络发起的注销

当UE收到注册事件包的NOTIFY表示网络发起的注销时, <registration>中:

- 状态属性设成 “terminated”, 并且事件属性设成 “rejected” 或 “deactivated”; 或者
- 状态属性设成 “active” 并且在<contact>中的状态属性设成 “terminated”, 相关的并且事件属性设成 “rejected” 或 “deactivated”。

UE需要删除与这些公共用户标识相关的注册细节, 以及与P-CSCF之间的SA。

7.6.3 会话管理

7.6.3.1 MO

对于发起会话的 UE, UE 应在 Via 和 Contact 头域中加入保护的服务器端口, 并插入 P-Access-Network-Info 头域。

UE 可以在任意的初始请求中插入 P-Preferred-Identity 头, 内容可以包括下面其中之一:

- 用户注册时使用的公共用户标识;
- 在注册状态事件包返回的 NOTIFY 中表示隐式注册成功的公共用户标识。

UE 应建立正确的预加载 Router 头域, 包含了在 P-CSCF 发现过程中获得的 P-CSCF 地址, 加上注册时得到的 Service-Route 里面的信息。P-CSCF URI 中的端口号是在安全一致性协商中获取的。

对于初始INVITE请求, UE需要支持precondition机制。如果UE不需要进行本地资源预留, 那UE发起会话时也可以不带precondition。

在成功预留资源后, UE 需要在后续 SIP 请求中进行确认。如果两端都使用 precondition 机制, UE 用 PRACK 或者 UPDATE 请求进行确认; 如果有一端不支持或者两端都不支持 precondition, 可以用 reINVITE 进行确认。

为了进行媒体授权, P-CSCF 和 S-CSCF 可能会对 SDP 负载进行检查, 所以 UE 不能对 SDP 负载进行加密。

7.6.3.2 MT

在会话被叫侧的UE，当UE发送任意响应时，UE应在Contact中增加被保护的Server端口，插入P-Access-Network-Info头域。

对于初始 INVITE 请求，如果被叫侧的 UE 需要从主叫侧那里得到可靠的 alerting 指示，UE 应该发送 180 响应。

7.6.3.3 匿名功能

当用户希望匿名时，可在 SIP From 中设置匿名（如 From:“Anonymous”<sip: anonymous@anonymous.invalid>; tag=1234567890），同时，为了说明网络需要给该用户提供私密性，UE还应在 SIP 消息中增加Privacy头部信息，值为“id”。这样在终结侧的P-CSCF就能在发送消息前删除SIP消息的P-Asserted-Identity和Privacy头。

7.6.4 安全

7.6.4.1 鉴权方法

Gm接口应该支持IMS AKA鉴权方法。

7.6.4.2 安全联盟

Gm接口需要建立安全联盟SA。

P-CSCF支持通过IMS AKA建立SA的过程，能够与UE协商安全模式来建立SA参数，建立SA的过程基于3GPP 33.203。

对TCP和UDP进行不同的处理。

- UDP的情况：P-CSCF在port_ps（被保护的server端口）接收来自UE的通过ESP保护的请求或相应消息。P-CSCF在port_pc（被保护的client端口）发送通过ESP保护的请求或响应消息到UE。

- TCP的情况：如果还没有到UE的TCP连接，P-CSCF在发送请求前先建立一个由它自己的port_pc端口到UE的port_us端口的TCP连接。

P-CSCF仅允在被保护的端口接收登记消息和错误信息，其他没有到达被保护端口的消息都将被P-CSCF拒绝或丢弃。

7.6.4.3 完整性保护

如果采用IMS AKA 鉴权方式，Gm接口中的SIP信令要求进行完整性保护。

可以采用IPSec ESP（IETF RFC 2406）协议来提供UE和P-CSCF间SIP信令的完整性保护，保护IP层的所有SIP信令。

7.6.4.4 机密性保护（可选）

可以对UE和P-CSCF间的SIP信令消息进行加密，作机密性保护。

7.6.5 信令压缩

为了节约链路带宽资源（特别是无线链路带宽资源），Gm接口如果是无线接入应使用信令压缩技术对SIP信令进行压缩处理，以便有效利用带宽，减少传输时延。

信令压缩可采用静态压缩或者动态压缩。

附 录 A
(规范性附录)
M 系列接口支持的消息

M系列接口应支持表A.1所列的SIP消息，并符合相应的IETF规范中对各消息的定义。

表A.1 SIP消息

消息名称	来 源
ACK	RFC3261
BYE	RFC3261
CANCEL	RFC3261
INVITE	RFC3261
MESSAGE	RFC3428
NOTIFY	RFC3265
OPTIONS	RFC3261
PRACK	RFC3262
PUBLISH	RFC3903
REFER	RFC3515
REGISTER	RFC3261
SUBSCRIBE	RFC3265
UPDATE	RFC3311

附录 B (规范性附录)

M 系列接口支持的消息头

B.1 基本的消息头

a) To

在非注册消息中，To消息头定义了消息的逻辑接收者，用户的record地址或资源。To消息头中可以包含SIP URI或者tel URL。

在注册消息中，To消息头定义了注册用户的AOR记录地址。

具体规定遵循IETF RFC 3261中的定义。

b) From

在非注册消息中，From消息头定义了消息的逻辑发起者，有可能是用户的record地址。From消息头中可以包含SIP URI或者tel URL以及一个display name。

在注册消息中，From消息头定义了发起注册实体的AOR记录地址。

具体规定遵循IETF RFC 3261中的定义。

c) Call-ID

Call-ID消息头用于惟一标识一个对话（dialog）。在一个dialog中，任何UA发送的所有请求和回应应相同。

具体规定遵循IETF RFC 3261中的定义。

d) Cseq

Cseq消息头用于标识transaction和对transaction进行排序。它由一个序列号和一个方法组成，方法应与请求相匹配。

具体规定遵循IETF RFC 3261中的定义。

e) Via

Via消息头用于指示一个transaction的传输层信息，它是消息响应路由的依据。Via消息头只有在即将跳到下一跳时才会插入。

Via消息头中应包括一个branch参数，用于区分当前请求所建立的transaction。

具体规定遵循IETF RFC 3261中的定义。

f) Max-Forwards

Max-Forwards消息头用于限制一个请求消息在到达目的地之前所经过的跳（hop）数。Max-Forwards由一个整数构成，每经过一跳减1。

UAC应向每个request插入Max-Forwards时，其值一般设为70。

具体规定遵循IETF RFC 3261中的定义。

g) Contact

Contact消息头提供了SIP URI，后续请求消息可以用它来联系该当前UA，一般采用主机地址标识。Contact消息头应存在于任何能够建立Dialog的请求中。

具体规定遵循IETF RFC 3261中的定义。

h) 其他

B.2 路由相关的消息头

a) Via

Via消息头用于对响应消息进行路由。

b) Route

Route消息头用于对请求消息进行路由，它指定了请求消息应经过它所设置的一系列的SIP Proxy列表。

在初始请求中，Route消息头可以由UA和SIP Proxy插入。

在后续请求中，Route消息头由UA插入，主叫UA将初始请求过程中获得的Record-Route消息头中的所有条目顺序颠倒插入到Route消息头中，被叫UA将初始请求过程中获得的Record-Route消息头中的所有条目插入到Route消息头中。

具体规定遵循IETF RFC 3261中的定义。

c) Record-Route

Record-Route消息头为后续请求记录Route消息头，它由SIP Proxy在初始请求中插入，保证了后继消息仍然需要经过Record-Route所设置的一系列的SIP Proxy列表。

具体规定遵循IETF RFC 3261中的定义。

B.3 其他SIP消息头 (P-header)

a) P-Asserted-Identity

P-Asserted-Identity消息头用于传递信任域内用户的标识，表明用户为通过鉴权的用户。当消息发送给非信任域的UE或SIP实体时，并且用户申请了privacy: id，则P-Asserted-Identity消息头应从消息中删掉。

具体规定遵循IETF RFC 3325和IETF RFC 3323中的定义。

b) P-Preferred-Identity

P-Preferred-Identity消息头用于由非信任域内的UA显式提供一个标识，并希望信任域内的Proxy对此标识进行鉴权，如果鉴权通过，那么该Proxy就把这个标识放入P-Asserted-Identity消息头中，并删除原P-Preferred-Identity消息头。

具体规定遵循IETF RFC 3325的定义。

c) Privacy

Privacy消息头用于让UA对某个SIP消息来设置一个特定的隐私级别，常见的隐私级别有“id”，“user”，“session”等。

具体规定遵循IETF RFC 3323的定义。

d) P-Charging-Vector

P-Charging-Vector消息头用于在网络实体之间进行计费关联，它包括处理同一会话相关的各个网元实体产生的CDR所需要的通用信息。

P-Charging-Vector消息头包括3类计费关联信息。

— IMS计费信息ICID (IMS Charging Identifier)：用于将CDR进行计费关联的惟一值。

— 运营商标识IOI (Inter-Operator Identifiers)：可以由主叫或被叫方产生用于标识各自所在的运营商网络。

— 接入网计费信息：包括接入层特定的网络标识，用于将IP-CAN CDR与IM域的CDR进行关联，也就是说将承载层与会话层相关联。

具体规定遵循IETF RFC 3455和3GPP 24.229的定义。

e) P-Charging-Function-Addresses

P-Charging-Function-Addresses消息头用于给SIP Proxy提供一套公共的地址以供SIP Proxy传送计费信息，它包含两个参数：CCF和ECF，其中CCF是CDF的地址，ECF是OCF的地址。

在IMS中，P-Charging-Function-Addresses可以由S-CSCF通过Cx接口获得，并由S-CSCF传递到其他实体。另外，P-Charging-Function-Addresses也可以由AS通过Sh接口获得。

具体规定遵循IETF RFC 3455和3GPP 24.229的定义。

f) Path

Path消息头用于在UA和Registrar之间建立一个途径Proxy的列表，只能被用于注册消息中。它类似于Record-Route消息头在Invite消息中的作用。

在IMS中，Path通常由P-CSCF在前转注册请求消息时被加入，其值通常设置成P-CSCF自身的SIP URI。

具体规定遵循IETF RFC 3327和3GPP 24.229的定义。

g) Service-Route

Service-Route消息头用于让Registrar通知UA一个可服务的路由集，而后当UA准备发起初始请求的时候通常会把这个路由集所预先设置到Route消息头中。Service-Route是通过注册消息的成功响应返回的。

在IMS中，Service-Route通常由S-CSCF在返回注册消息的200 OK响应的时候被加入，其值通常设置成S-CSCF自身的SIP URI。

具体规定遵循IETF RFC 3608和3GPP 24.229的定义。

h) P-Associated-URI

P-Associated-URI消息头用于让Registrar向UA返回一组注册的AOR记录地址，它是通过注册消息的成功响应返回的。

在IMS中，由于某IMPU被注册，可能导致User Profile中的其他IMPU也同样被隐式注册，所以P-Associated-URI通常包含了多个注册的IMPU。

具体规定遵循IETF RFC 3455和3GPP 24.229的定义。

i) P-Visited-Network-ID

P-Visited-Network-ID消息头用于让Home域的实体知道UAC所接入的Visit域的网络标识，最终该Home域的实体根据本身保存的漫游协议判断是否让该UAC接入。

在IMS中，P-Visited-Network-ID通常是在Register消息请求时由P-CSCF插入，而后Home域的I-CSCF通过与HSS的交互来决定是否允许该UE在某个接入网络中的注册。

具体规定遵循IETF RFC 3455和3GPP 24.229的定义。

j) P-Media-Authorization

P-Media-Authorization消息头用于在SIP协议中提供所需要建立的媒体流的QoS信息。

在IMS中，P-Media-Authorization通常只适用于INVITE消息。在MO情况下，P-Media-Authorization消息头在初始响应消息中由P-CSCF插入；而在MT流程下，P-Media-Authorization消息头在请求消息中就由P-CSCF插入。

具体规定遵循IETF RFC 3313和3GPP 24.229的定义。

k) P-Called-Party-ID

P-Called-Party-ID消息头通常只适用于Terminating流程。当远端Proxy在转发消息给UAS的过程中，它需要把Request-URI的值更改成该UAS注册时的Contact地址（即IP地址），而如果UAS存在多个可用的标识且这些标识都已经注册过，那么UAS收到消息后就不知道该消息具体是给它哪个标识的。所以在远端Proxy转发消息给UAS前，需要把原Request-URI的值保存下来并置入一个新的消息头中，而这个新的消息头即为P-Called-Party-ID。

在IMS中，P-Called-Party-ID通常是由S-CSCF在MT情况下插入的，其值为原先的Request-URI的值，即被叫UE的IMPU。

具体规定遵循IETF RFC 3455和3GPP 24.229的定义。

l) Security-Client

Security-Client消息头用于让UA指明它所支持的安全机制、算法、参数等。

具体规定遵循IETF RFC 3329和3GPP 33.203的定义。

m) Security-Server

Security-Server消息头用于让对端指明它所支持的安全机制、算法、参数等。

具体规定遵循IETF RFC 3329和3GPP 33.203的定义。
