

YD

中华人民共和国通信行业标准

YD/T 1522.3-2006

会话初始协议 (SIP) 技术要求 第 3 部分: ISDN 用户部分 (ISUP) 和 会话初始协议 (SIP) 的互通

Technical Requirments for Session Initiation Protocol

Part 3:Interworking between ISUP and SIP

2006-12-11 发布

2007-01-01 实施

中华人民共和国信息产业部 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
3.1 术语和定义	1
3.2 缩略语	2
4 综述	4
4.1 互通一般原则	4
4.2 封装/解封装ISUP消息的详细程序	5
4.3 sip: URI和sips: URIs	8
5 I-IWU中从SIP到ISUP的人局呼叫的互通	8
5.1 I-IWU的基本要求	8
5.2 初始地址消息 (IAM) 的发送	8
5.3 后续INVITE的接收	14
5.4 COT的发送	15
5.5 连接消息 (CON) 的接收	15
5.6 ACM的接收	15
5.7 CPG的接收	15
5.8 应答消息 (ANM) 的接收	16
5.9 承载通道的直通连接	16
5.10 网络发起的暂停消息 (SUS) 的接收	16
5.11 网络发起的恢复消息 (RES) 的接收	16
5.12 I-IWU的释放程序	16
6 O-IWU中从ISUP 到 SIP的出局呼叫的互通	20
6.1 第一个INVITE的发送	20
6.2 发出INVITE之后的SAM的接收	25
6.3 18X响应的接收	26
6.4 定时器超时及Early ACM的发送	27
6.5 200 OK (INVITE) 的接收	27
6.6 ISUP承载通道的直通连接	27
6.7 O-IWU的释放程序	28
6.8 O-IWU的定时器	32
附录A(规范性附录) SIP头字段P-Asserted-Identity扩展	33
附录B(资料性附录) ISUP补充业务的互通	44
附录C(资料性附录) SIP/SIP-I 信令的 Profile	47

前 言

《会话初始协议（SIP）技术要求》分为5个部分：

- 第1部分：基本的会话初始协议；
- 第2部分：基于会话初始协议（SIP）的呼叫控制的应用；
- 第3部分：ISDN用户部分（ISUP）和会话初始协议（SIP）的互通；
- 第4部分：软交换网络中基于呼叫控制的会话初始协议（SIP）技术要求；
- 第5部分：支持移动应用部分。

本部分为《会话初始协议技术要求》的第3部分。

本部分是会话初始协议系列标准之一。该系列标准的预计结构为：

1. 《会话初始协议（SIP）技术要求》

- 第1部分：基本的会话初始协议；
- 第2部分：基于会话初始协议（SIP）的呼叫控制的应用；
- 第3部分：ISDN用户部分（ISUP）和会话初始协议（SIP）的互通；
- 第4部分：软交换网络中基于呼叫控制的会话初始协议（SIP）技术要求；
- 第5部分：支持移动应用部分。

2. 《会话初始协议测试方法》

- 第1部分：基本的会话初始协议；
- 第2部分：基于会话初始协议（SIP）的基本呼叫控制。

3. 《会话初始协议（SIP）服务器设备技术要求》

4. 《会话初始协议（SIP）服务器设备测试方法》

随着技术的发展，还将制定后续的相关标准。

本部分参考了ITU-T Q.1912.5。

本部分的附录A为规范性附录，附录B和附录C为资料性附录。

本部分由中国通信标准化协会提出并归口。

本部分起草单位：信息产业部电信研究院

上海贝尔阿尔卡特股份有限公司

华为技术有限公司

北京西门子通信网络股份有限公司

UT斯达康（重庆）有限公司

本部分主要起草人：续合元 吕 军 李海花 吴宏建 刘志强 徐培利 胡一军 潘 旭

会话初始协议 (SIP) 技术要求

第3部分 ISDN用户部分 (ISUP) 和会话初始协议 (SIP) 的互通

1 范围

本部分规定了ISDN用户部分协议 (ISUP) 和会话初始协议 (SIP) 以及与SIP协议相关联的会话描述协议 (SDP) 之间的信令互通技术要求。本部分仅描述在ISUP和SIP互通中涉及到的程序、方法和信息单元 (消息、参数、指示语、头字段、等等)。

本部分内容适用于ISUP和SIP协议互通的应用场景；仅具有本地意义 (例如，仅和单个信令系统，如SIP或ISUP相关) 的程序、方法和信息单元不属于本部分的规定范围。

2 规范性引用文件

下列文件中的条款通过本部分的引用而成为本部分的条款。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部分，然而，鼓励根据本部分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部分。

YDN 038-1997	国内No.7信令方式技术规范 综合业务数字网用户部分 (ISUP)
YD/T 1522.1-2006	会话初始协议 (SIP) 技术要求 第1部分：基本的会话初始协议
YD/T 1157-2001	网间主叫号码的传送
YD/T 1157.2-2003	网间主叫号码的传送 (补充件2)
YD/T 1157.3-2005	网间主叫号码的传送 (补充件3)
ITU-T Q.850	No.1数字用户信令系统和No.7信令系统ISDN用户部分中的原因值和位置用法
RFC 2234	扩展型BNF语法规则：ABNF
RFC 3267	自适应多速率 (AMR) 和自适应多速率宽带 (AMR-WB) 语音编码器的实时传输协议 (RTP) 净荷格式和文件存储格式
RFC 3312	资源管理的综合和会话初始协议 (SIP)
RFC 3323	会话初始协议 (SIP) 的私密机制
RFC 3326	会话初始协议 (SIP) 的Reason头字段

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部分。

3.1.1

入局/出局

指示相对于参考点的呼叫的方向 (而非信令信息)。

3.1.2

入局互通单元 (I-IWU)

该物理实体可以和 ISUP 交换机合设，终结使用 SIP 协议的人局呼叫，并发起 ISUP 呼叫。

3.1.3

入局 SIP/ISUP

指 IWU 的人局侧和呼叫始发实体之间采用的 SIP/ISUP 协议。

3.1.4

出局互通单元 (O-IWU)

该物理实体可以和 ISUP 交换机合设，终结使用 ISUP 协议的人局呼叫，并发起 SIP 呼叫。

3.1.5

相邻 SIP 节点 (ASN)

已经与入局和出局 IWU 实体建立直接信任关系的 SIP 节点 (SIP 代理或背靠背用户代理)。

3.1.6

出局 SIP/ISUP

指 IWU 的出局侧和呼叫终结实体之间使用的 SIP/ISUP 协议。

3.1.7

SIP 预置条件

指按照 RFC3312 中定义的 SIP 预置程序。

3.1.8

封装 ISUP 的 SIP 协议 (SIP-I)

指在 SIP 的消息体中封装了 ISUP 信息。

3.2 缩略语

下列缩略语适用于本部分。

通用

ABNF	Augmented Backus-Naur Form (see RFC 2234)	扩展型 BNF (见 RFC2234)
AMR	Adaptive Multirate (codec)	自适应多速率编码器
ASN	Adjacent SIP Node	相邻 SIP 节点
ATM	Asynchronous Transfer Mode	异步转移模式
B2BUA	Back-to-Back User Agent	背靠背用户代理
BC-IWF	Bearer Control - Interworking Function	承载控制 - 互通功能
BNC	Backbone Network Connection	骨干网络连接
BNF	Backus-Naur Form	巴克斯范式
CC	Country Code	国家码
CLI	Calling Line Identification	主叫线标识
CONN	Connect message (Q.931)	连接消息
DISC	Disconnect message (Q.931)	断开连接消息
IANA	Internet Assigned Numbers Authority	互联网号码分配局
IC	Identification Code (E.164)	网络标识码 (E.164)
IETF	Internet Engineering Task Force	互联网工程任务组

I-IWU	Incoming (to ISUP) Interworking Unit	入局互通单元
IPBCP	Internet Protocol Bearer Control Protocol	互联网协议承载控制协议
ISDN	Integrated Services Digital Network	综合业务数字网
ISN	Interface Serving Node	接口服务节点
ISUP	ISDN User Part	ISDN 用户部分
IWU	Interworking Unit	互通单元
MIME	Multi-purpose Internet Mail Extensions	多用途互联网邮件扩展
NDC	National Destination Code	国内目的码
NNI	Network To Network Interface	网络到网络的接口
O-IWU	Outgoing (from ISUP) Interworking Unit	出局互通单元
PSTN	Public Switched Telephone Network	公共交换电话网
PT	Payload Type	净荷类型
RFC	Request For Comments	互联网草案
RTP	Real-Time Transport Protocol	实时传送协议
SCCP	Signalling Connection Control Part	信令连接控制部分
SDP	Session Description Protocol	会话描述协议
SIP	Session Initiation Protocol	会话初始协议
SIP-I	SIP with encapsulated ISUP	封装 ISUP 的 SIP
SN	Subscriber Number	用户号码
TLS	Transport Layer Security	传输层安全
UA	User Agent	用户代理
UAC	User Agent Client	用户代理客户
UAS	User Agent Server	用户代理服务器
UNI	User To Network Interface	用户网络接口
URI	Universal Resource Identifier	通用资源标识
ISUP 消息		
ACM	Address Complete Message	地址全消息
ANM	Answer Message	应答消息
CGB	Circuit Group Blocking	电路群闭塞
CON	Connect	连接
COT	Continuity	导通消息
CPG	Call Progress	呼叫进展
GRS	Circuit Group Reset	电路群复原
IAM	Initial Address Message	初始地址消息
REL	Release	释放
RES	Resume	继续
RLC	Release Complete	释放完成

RSC	Reset Circuit	电路复原
SGM	Segmentation Message	分段消息
SAM	Subsequent Address Message	后续地址消息
SUS	Suspend	暂停
ISUP 参数和值		
APRI	Address Presentation Restricted Indicator	地址提供限制指示语
ATP	Access Transport Parameter	接入转送参数
BCI	Backward Call Indicators	后向呼叫指示语
CgPN	Calling Party Number	主叫用户号码
CIC	Circuit Identification Code (ISUP)	电路标识码 (ISUP)
FCI	Forward Call Indicators	前向呼叫指示语
HLC	High Layer Compatibility	高层兼容性
NOA	Nature of Address indicator	地址性质指示语
NP	"network provided" (Screening Indicator value)	网络提供 (过滤指示语的值)
TMR	Transmission Medium Requirement	传输媒介请求
UPVP	"user provided, verified and passed" (Screening Indicator value)	用户提供, 认证, 通过 (过滤指示语的值)
USI	User Service Information	用户业务信息

4 综述

4.1 互通一般原则

IWU 的 SIP 接口应作为 UA 并支持附录 C 所列的标准, ISUP 接口应符合 YDN 038-1997 中定义的 ISUP 协议。

当 IWU 和 ISUP 交换机合设时, IWU 应当提供 SIP 和 ISUP 的承载网络的互通。

当 IWU 要在 SIP 侧发送任何信息时, 它应当先查看一下本地信任策略, 以确定后续 SIP 节点是否值得信任接收这些信息。当已确定 ASN 不能接收这些信息, IWU 应当采取适当的动作 (如省略这些信息, 提供其他值或释放呼叫)。

类似地, 当从 SIP 侧接收信息时, IWU 应当先查看一下本地信任策略, 发起 SIP 消息的节点发出或传递这些信息是否可信。当已确定 ASN 提供这些信息不可信, IWU 应当采取适当的动作 (如忽略这些信息, 使用默认值或释放呼叫)。

IWU 应在 SIP 对话和 ISUP 呼叫/承载控制实例之间建立一对一的关系, 以便关联和同一个呼叫相关的信令信息。

4.1.1 Profile C (SIP-I) 互通的一般原则

ISUP 封装时使用下面所述的一般规则:

(a) 收到 SIP 消息的 IWU 应去掉 SIP 消息中封装的 ISUP 消息。对于 SIP 消息 (例如: 头字段和 SDP) 与 ISUP 消息之间的差异使用本部分中定义的程序进行处理。在任何情况下, 经过处理后得到的 ISUP 信息都应传送到对应的 ISUP 程序。

(b) 收到 ISUP 信息的 IWU 如果在确定被叫用户是 ISUP 用户, 或不能确定被叫用户是否是 SIP 用户时, 将 ISUP 消息封装在 SIP 消息的消息体中发送出去。4.2 节给出了 ISUP 封装程序的详细描述。这些详细程序包括不能封装在 SIP 中的 ISUP 消息列表。

任何情况下, IWU 发觉 SIP 消息中应当封装 ISUP 消息但并没有封装 ISUP 消息时, IWU 应使用在 SIP 头字段和 SDP 消息体 (如果存在) 中收到信息重新构造适当的 ISUP 消息。第 5 章和第 6 章给出了有关 IWU 重新构造 ISUP 消息的所有信息。

注: 无论收到的 SIP 消息中是否封装有 ISUP 消息, 均可使用第 5 章和第 6 章中的规定。当接收的 SIP 消息中封装有 ISUP 信息时, 这些封装的 ISUP 信息在 SIP 头字段和相关的 ISUP 参数之间提供了互通所必需的信息, 这样在向 ISUP 程序传送 ISUP 消息之前可以修改或更新封装的 ISUP 信息。当收到的 SIP 消息中不包含任何封装的 ISUP 信息时, IWU 也可以使用第 5 章和第 6 章中的规定, 完全根据 SIP 头字段 (和 SDP 消息体) 中的信息构造适当的 ISUP 消息。

4.1.2 ISUP 重叠信令发送方式的互通

如果某个 IWU 连接到使用重叠信令方式的网络, 则使用本节 (以及相关的后续章节) 所描述的程序。

本部分对向 SIP 网络传送重叠信令和在 O-IWU 将重叠信令转换成成组信令所使用的互通程序进行了描述。另外, 第 6 章对在 I-IWU 的 SIP 侧收到重叠信令时所采用的程序进行了概述。虽然本部分涉及所有 (共 4 种) 重叠互通情况 (ISUP 重叠方式到 SIP 成组方式、ISUP 重叠方式到 SIP 重叠方式、SIP 重叠方式到 ISUP 成组方式、SIP 重叠到 ISUP 重叠方式), 但建议仅使用 SIP 成组信令方式, 即在 SIP 网中应避免使用重叠信令方式。因此, 最常出现的情况是在 O-IWU 上将 ISUP 重叠信令方式转换成 SIP 成组信令方式。对于重叠信令方式在特定的某个 IWU 上如何进行配置依赖于本地策略或网络配置。

本部分的第 5 章和第 6 章提供了详细的重叠方式处理程序。

注 1: 当 O-IWU 确定 SIP 网络是作为两个 PSTN 端点之间的转接网, IWU 可以采用适当的方式通过 SIP 网络传送重叠信令, 这样在目的地 ISUP 网络中仍使用 ISUP 重叠信令方式。

注 2: INVITEs 消息被希望是按顺序传送到 I-IWU。I-IWU 并不会对重叠发送模式下收到的 INVITEs 进行缓存和重新排序, 而是通过分析 Request-URI, 比较本次收到的 INVITE 消息中提供的地址位数和已经收到的位数来决定这个 INVITE 是否是最先接收到的 INVITE。第 5 章中提供的程序将大致描述 I-IWU 如何处理错序的 INVITEs。

4.2 封装/解封装 ISUP 消息的详细程序

本节仅涉及在 IWU 的 SIP 接口上发送的或接收的 SIP 消息中封装有 ISUP 信息 (或期望封装 ISUP 信息) 时相关的程序, 主要基于 4.1.1 (b) 中所描述的一般原则。

4.2.1 向相邻 SIP 节点发送封装的 ISUP 信息

4.2.1.1 概述

在发送封装有 ISUP 信息的 INVITE 消息之前, O-IWU 应根据本地策略确定 ISUP 信息是否可以传送给 ASN。如果确定 ASN 有权接收 ISUP 信息, 则 O-IWU 应处理在相关的 SIP 消息中 (见 4.2.1.3 节) 封装的 ISUP 信息 (第 4.2.3 节中描述的消息除外)。和 ISUP 消息体相关的头字段的设置在 4.2.1.2 节中规定。

同样, 在后向上收到后向 ISUP 信息的 I-IWU 应在相关的 SIP 消息中 (见 4.2.1.3 节) 封装收到的 ISUP 信息 (第 4.2.3 节中描述的消息除外), 并且应确定 SIP 消息要发往的节点有权接收 ISUP 信息。4.2.1.2 节规定了和 ISUP 消息体处理相关的头字段的设置。

4.2.1.2 与 ISUP MIME 消息体相关的头字段

与 ISUP MIME 消息体关联的“Content-Type”头字段应如下填写：

Content-Type: application/ISUP; version= CHN;

注：CHN 表示封装的 ISUP 信令遵循 YDN 038-1997 及后续版本所规定的内容，网间主叫号码传送遵循 YD/T1157-2001。IWU 不对“version”参数采取任何动作。

与 ISUP MIME 消息体关联的 Content-Disposition 头字段应如下填写：

Content-Disposition: signal; handling = required.

4.2.1.3 对封装 ISUP 消息的 SIP 消息的确定

对于基本的呼叫建立，用于封装 ISUP 消息的 SIP 消息是首先被触发并作为互通的结果从 IWU 发送出去的 SIP 消息。本部分和 ISUP 的特定附录对此互通进行了规范。

例如，在 6.1 (B) 中接收的 ISUP IAM 消息应封装在 INVITE 消息中，并由 O-IWU 发送。

对于基本呼叫建立过程中不涉及的消息或不是因为收到 ISUP 消息而产生的 SIP 消息，处理方式请参见 4.2.3 节。

4.2.2 ISUP 信息的接收

4.2.2.1 提取封装的 ISUP 信息

当收到封装 ISUP 消息的 SIP 消息，IWU 应从 SIP 消息中提取封装的 ISUP 消息。向 ISUP 网络发送 ISUP 消息之前，还要经过许多附加的处理。附加的处理程序参见 4.2.2.1.1 节和 4.2.2.1.2 节。

4.2.2.1.1 协调 SIP 头字段和 ISUP 消息体的内容

当收到封装 ISUP 消息的 SIP 消息，并且当 ISUP 消息中的参数和 SIP 头字段有冲突时（例如，由于在 SIP 网中起用了某些业务），IWU 应使用本部分中所描述的程序。用哪个 SIP 头字段来修改 ISUP 的参数，或者用哪个 ISUP 参数来修改 SIP 头字段，这个规则依赖于具体的应用/业务。

对于 Profile A 和 Profile B，如果第 5 章和第 6 章已经定义了默认值，则使用这些值。对于 Profile C，ISUP 参数应当从封装的 ISUP 消息和本地策略中导出。

当已经定义了某个 SIP 头字段和特定的 ISUP 的参数的映射时，例如，Request-URI 映射成 ISUP 的被叫号码（见 5.2.3.1 节），则在协调过程中优先采用 SIP 头字段而不是封装的 ISUP 消息，除非有另外的声明。

4.2.2.1.2 设置 ISUP 参数

当完成所有 ISUP 参数（和相应字段）的协调之后，为了方便互通，IWU 应自动按照第 5 章（对于 I-IWU）和第 6 章（对于 O-IWU）描述的程序设置解封装后的 ISUP 消息的参数。

4.2.2.1.3 向 ISUP 程序传送最终的 ISUP 消息/发送 ISUP 消息

在执行完 4.2.2.1.2 所描述的处理之后，IWU 应将该 ISUP 消息传送给相应的 ISUP 程序，并且将通过出局 ISUP 接口发送。

4.2.3 例外和特殊考虑

对于表 1 描述的 ISUP 消息，或者不封装在任何 SIP 消息中，或者需要对封装的 ISUP 消息进行特殊处理。

表1 需要特殊考虑的 ISUP 消息

ISUP 消息	参考章节
电路复原消息 (RSC)	4.2.3.1 (注 1)
电路群闭塞消息 (CGB)	4.2.3.1
电路群闭塞证实消息 (CGBA)	4.2.3.1
电路群复原消息 (GRS)	4.2.3.1
电路群复原证实消息 (GRA)	4.2.3.1
闭塞消息 (BLO)	4.2.3.1
闭塞证实消息 (BLA)	4.2.3.1
导通检验请求 (CCR)	4.2.3.1
导通消息 (COT)	4.2.3.1
解除闭塞消息 (UBL)	4.2.3.1
解除闭塞证实消息 (UBA)	4.2.3.1
电路群解除闭塞消息 (CGU)	4.2.3.1
电路群解除闭塞证实消息 (CGUA)	4.2.3.1
用户部分测试消息 (UPT)	4.2.3.1
用户部分可用消息 (UPA)	4.2.3.1
话务员消息 (OPR)	4.2.3.1
计次脉冲消息 (MPM)	4.2.3.1
混乱消息 (CFN)	4.2.3.1 或 4.2.3.2 (注 2)
性能拒绝消息 (FRJ)	4.2.3.1 或 4.2.3.2 (注 2)
主叫用户挂机 (CCL)	4.2.3.2
用户到用户信息消息 (USR)	4.2.3.2
前向转移消息 (FOT)	4.2.3.2
暂停消息 (SUS)	4.2.3.2
恢复消息 (RES)	4.2.3.2
性能接受消息 (FAA)	4.2.3.2
性能请求消息 (FAR)	4.2.3.2
性能消息 (FAC)	4.2.3.2
网络资源管理消息 (NRM)	4.2.3.2
识别请求消息 (IDR)	4.2.3.2
识别响应消息 (IRS)	4.2.3.2
分段消息 (SGM)	4.3.3.3
释放完成消息 (RLC)	4.2.3.4
注 1: 如果 ISUP 程序想向一个 ISUP 交换机发送电路复原消息 RSC, IWU 可发送封装 REL 消息的 SIP 消息, REL 消息中的释放原因值填 31 (正常, 未定义)。	
注 2: 这些消息是在本地终接还是透传, 取决于它们是发给 IWU 还是发往另一个交换机。	

4.2.3.1 仅和 ISUP 端相关的程序

这些消息将不封装在 SIP 消息中, 因为这消息仅和 ISUP 侧相关, 最典型的一种情况是这些消息仅涉及到 ISUP 电路的维护。如果在 SIP 消息中封装有这些 ISUP 消息, 则这些 ISUP 信息应该被丢弃。

4.2.3.2 需要透明传送的消息

在这些情况下, ISUP 消息通过封装在下列 SIP 消息中进行透明传递:

- (1) “183”临时响应，如果这是一个在确认对话建立之前，由 I-IWU 发出的后向消息；
- (2) 在其他情况下使用 INFO 消息。

这些消息必须透明传送以便维护端到端的业务。

4.2.3.3 ISUP 分段和 ISUP 封装

分段消息不能封装在 SIP 消息中，IWU（ISUP 侧接口）应对分段的 ISUP 消息进行组装，并且检查任选前向呼叫指示语或任选后向呼叫指示语参数，按照下面的说明采取相应的动作。

IWU 对任选前向呼叫指示语或任选后向呼叫指示语所采取的动作取决于“简单分段指示语”是否是该参数中惟一需要设置的指示语。

如果任选前向呼叫指示语参数/任选后向呼叫指示语参数中除了“简单分段指示语”没有其他的指示语需要设置，则丢弃整个参数。

如果任选前向呼叫指示语参数/任选后向呼叫指示语参数中有另一个指示语需要设置，则 IWU 将“简单分段指示语”置成“0”，表示没有附加的信息可发送。

之后，IWU 应按以上程序将处理后的 ISUP 消息封装在 SIP 消息体中。

4.2.3.4 RLC 的封装

RLC 消息应封装在 200 OK BYE 消息中作为对封装了 ISUP REL 消息的 SIP BYE 消息的响应。

4.3 sip: URI 和 sips: URIs

本部分中所提到的 sip: URI 在使用时等同于 sips: URIs。这两种类型的 URI 仅在 SIP 网络中有意义，并不影响互通。

5 I-IWU 中从 SIP 到 ISUP 的入局呼叫的互通

5.1 I-IWU 的基本要求

I-IWU 分别从“入局 SIP”和“出局 ISUP”侧接收前向和后向信令信息。在接收到信令信息并执行适当的呼叫/业务处理之后，入局 IWU 可将信令向下一 ISUP 节点或向前一 SIP 实体发送信令。根据 IWU 的出局 ISUP 接口发送或者接收到的消息，本章分成一些子章节。本章的互通只考虑 IWU 的入局 SIP 侧互通所产生的消息。本部分不描述本地协议状态机所产生的消息。

本章基于以下主要假设：

- (a) 入局 IWU 只支持始发的基本呼叫；
- (b) 从 SIP 网络域始发的呼叫不要求具有等同的 PSTN/ISDN 业务。

部分 PSTN/ISDN 补充业务与 SIP 的互通参见附录 B。

为了建立初期对话，I-IWU 应该在第一个非“100”的后向临时响应中包含 To tag。

5.2 初始地址消息 (IAM) 的发送

如果收到一个 INVITE 消息，这个 INVITE 消息包含能路由到 ISUP 网络的足够多的号码数字，而且它所指示的呼叫与 ISUP 网络中已存在的呼叫都没有任何联系，应依据 5.2.1 和 5.2.2 或 5.2.3 (对于 SIP-I, IAM 的解封装) 的互通程序，由收到的 INVITE 生成一个 IAM 消息。

对于重叠信令方式，如果收到的 INVITE 消息的 Call-ID 和 From tag 的值与前一个 INVITE 消息相同，并且该前一个 INVITE 已经激活了一个呼叫，则采用 5.3 节的处理程序。

注：如果收到的 INVITE 消息包含的号码不足以选路到 ISUP 网络中，使用正常的 SIP 处理程序，这个 INVITE 不会被映

射到ISUP网络。

5.2.1 节和 5.2.2 节描述的是第一个 INVITE 消息接收，并且发出了 IAM 消息。IAM 消息的发送程序依赖于从 SIP 网络接收到的 INVITE 是否包含 SDP Offer，见 5.2.1 和 5.2.2 节。

IAM 参数按 5.2.3 节进行编码。

5.2.1 接收到的 INVITE 不包含 SDP Offer

接收到 INVITE 后，I-IWU 应判断所接收到的 INVITE 是否指明了支持可靠的临时响应。

(1) 如果支持可靠的临时响应，I-IWU 应立即在 183 Session Progress 消息中发送一个包含媒体描述的 SDP Offer。此时，分以下两种情况：

- (a) 如果未使用 SIP 预置条件，接收到包含媒体描述的 SDP answer 后，I-IWU 应发送 IAM；
 - (b) 如果使用 SIP 预置条件，I-IWU 应按下面 5.2.2 (2) 所述的程序发送 IAM。
- (2) 如果不支持可靠的临时响应，I-IWU 应立即发送 IAM。

5.2.2 接收的 INVITE 含 SDP Offer 或 5.2.1 (1) 节的延续

- (1) 如果没有使用 SIP 预置条件，应立即发送 IAM。
- (2) 如果使用了 SIP 预置条件，则：

(a) 如果在后续网络中的出局 ISUP 信令支持导通检验程序，应立即发出 IAM 消息，IAM 消息内的连接性质指示语字段的导通检验指示语应置为“在前面电路中执行导通检验”，或“在本电路中要求导通检验”。如果导通检验要在出局电路中执行，则可能使用后一设置。

(b) 如果后续网络中的出局 ISUP 信令不支持导通检验程序，则 I-IWU 将推迟发送 IAM，直到满足所有的预置条件。

对所有情况，5.2.3 节给出了与 IAM 特定参数相关的特定细节。表 2 列出了从 INVITE 消息映射过来的 IAM 消息参数所对应的参考章节，在这些章节中会有特定的互通描述。

5.2.3 IAM 参数

表 2 给出了 IAM 的参数以及这些参数与 SIP 的互通内容所在的章节。

表2 初始地址消息参数的互通内容

参 数	参考章节
连接性质指示语	5.2.3.3 节
前向呼叫指示语	5.2.3.4 节
主叫用户类别	5.2.3.2 节
传输媒介请求	5.2.3.5 节
被叫用户号码	5.2.3.1 节
主叫用户号码	5.2.3.6 节
用户业务信息	5.2.3.8 节
跳计数器	5.2.3.9 节
通用号码	5.2.3.7 节

5.2.3.1 被叫用户号码 (必选)

Request-URI 需要包含 SIP: URI，且带有 user=phone 参数，URI 的 userinfo 部分采用 E.164 号码。

在 Request-URI 的 userinfo 成分中包含的信息应映射成 IAM 消息中的被叫用户号码参数。

内部网号码指示语置成“不允许选路到内部网号码”。

对其他 URI 格式的支持：如 TEL:URI 或者 SIPS-URI，URI 成分值和 URI 参数都是可选的。

表3 被叫用户号码的编码

INVITE→	IAM→
Request-URI	被叫用户号码
Userinfo (带 user=phone 的 SIP URI)	地址信号

5.2.3.2 主叫用户类别 (必选)

对于 Profile A 和 Profile B, I-IWU 应将以下编码置为主叫用户类别字段的缺省值。

比特/编码	含义
0000 1010	普通主叫用户

对于 SIP-I, 主叫用户类别的值应从封装的 ISUP 消息内的主叫用户类别参数中导出。

5.2.3.3 连接性质指示语 (必选)

I-IWU 所需设置的连接性质指示语参数如下:

比特	连接性质指示语参数
BA	卫星指示语
DC	导通检验指示语 (ISUP)
E	出局回声控制设备

连接性质指示语的其他字段应遵从国内的 ISUP 建议。

I-IWU 应将以下编码置为连接性质指示语参数字段的缺省值。

比特	编码	含义	条件
BA	01	连接中一段卫星电路	Profile A 和 B
	00	不要求导通检验 (ISUP)	无未决的预置条件请求
DC (注)	10	导通检验在前一电路中执行 (ISUP)	有未决的预置条件请求
	1	包含出局回声控制设备	Profile A

注: 若应用这些值, I-IWU 应当忽略封装的 IAM 中的导通检验设置, COT 没有被封装; 当需要时, I-IWU 创建 COT, 参见 5.4 节。

对于 SIP-I, 除了 5.2.1 和 5.2.2 节所描述的处理方法处理过的导通检验指示语外, 连接性质指示语宜利用封装的 IAM 消息中的连接性质指示语参数生成。

5.2.3.4 前向呼叫指示语 (必选)

IWU 所设置的 FCI 参数指示语如下:

比特	FCI 参数中的指示语
D	互通指示语
F	ISUP 指示语
HG	ISUP 优先级指示语
I	ISDN 接入指示语

FCI 指示语的其他字段应遵从目前的 ISUP 建议。

对于 Profile A, I-IWU 应将以下指示语的值置为 FCI 参数的缺省值:

比特	编码	含义
D	1	遇到互通
F	0	全程不使用 ISDN 用户部分
HG	01	全程不需要 ISDN 用户部分
I	0	始发接入非 ISDN

对于 Profile B，应基于对 I-IWU 中各种参数（来自信令、内部状态或配置）的分析来确定合适的 FCI 值。

对于 Profile C，前向呼叫指示语应当利用封装的 ISUP 消息中的前向呼叫指示语参数生成。

5.2.3.5 传输媒介请求 (TMR) (必选)，用户业务信息 (USI) (可选)，接入转送参数内的高层兼容信息元素参数 (HLC) (可选)

5.2.3.5.1 基本处理程序

(1) 对于 Profile A

TMR 参数设置成 3.1kHz 音频；一般不发送 USI，如需要可采用编解码。

(2) 对于 Profile B

如果在发出 IAM 之前从远端收到 SDP，而且 I-IWU 不支持编解码，则 TMR、USI 和 HLC 的生成将基于 SDP，见 5.2.3.5.1 节。否则将根据本地策略做相应的处理。

(3) 对于 Profile C

TMR、USI 和 HLC 将从封装的 ISUP 消息中提取。

5.2.3.5.2 I-IWU 无编解码可用 (只适用于 Profile B)

I-IWU 所接收到的 SDP 媒体描述部分宜仅指示一个媒体流。

只考虑 SDP 媒体描述部分的“m=”，“b=”和“a=”行与 IAM 参数 TMR、USI 和 HLC 进行互通。

“m=”行的第一个子字段（即<media>）指示目前定义的下述值之一：“audio”，“video”，“application”，“data”，“image”或“control”。其中，“video”，“application”或“control”，待定。

如果<media>为“audio”，其向上取舍的带宽是 64kbit/s，或没有“b=”行，则 TMR 应置为“3.1kHz”，且要评估<transport>和<fmt-list>以确定 USI 参数的用户信息 1 层协议指示语是否应置为“G.711 μ-law”或是“G.711 A-law”。

表 4 给出了基于以上程序的默认映射关系。

表4 源自 SDP 的 TMR/USI 编码：SIP 到 ISUP

m=行			b=行	a=行	TMR 参数	USI 参数		HLC 参数
<media>	<transport>	<fmt-list>	<modifier>: <bandwidth-value>	rtptime : <dynamic-PT> <encoding-name>/<clock-rate>/<encoding-parameters>	TMR 编码	信息传输能力	用户信息 1 层协议指示语	高层特性识别
			注：AS 的 <modifier> 的 <bandwidth-value> 被评估为 B kbit/s					
audio	RTP/AVP	8	无或高至 64 kbit/s	无	3.1kHz audio	3.1kHz audio	G.711A-law	电话
audio	RTP/AVP	动态 PT	无或高至 64 kbit/s	rtptime: <dynamic-PT> PCMA/8000	3.1KHz audio	3.1kHz audio	G.711A-law	电话
audio	RTP/AVP	9	AS: 64 kbit/s	Rtptime: 9 G.722/8000	64 kbit/s 无限制	无限制数字信息		

表 4 (续)

m=行			b=行	a=行	TMR 参数	USI 参数		HLC 参数
audio	RTP/AVP	动态 PT	AS: 64 kbit/s	rtpmap: <dynamic-PT> CLEARMODE /8000 (注 2)	64 kbit/s 无限制	无限制数字信息		
Image	udptl	t38	无或高至 64 kbit/s	基于 T.38	3.1 kHz audio	3.1kHz audio		传真组 2/3
Image	tcptl	t38	无或高至 64 kbit/s	基于 T.38	3.1 kHz audio	3.1kHz audio		传真组 2/3

注 1: 本表中G.711编解码器只是一个例子, 也可能用其他的编解码器。

注 2: CLEARMODE尚未标准化, 对其的使用有待进一步研究。

5.2.3.6 叫用户号码

表 5 汇总了 SIP INVITE 头字段映射到 ISUP CLI 参数的情况。表 6 给出了当主叫用户号码参数置成“网络提供”时的详细信息。表 7 给出了其他情况下主叫用户号码映射的详细信息。表 8 给出了映射到通用号码时 (如果有可能) 的详细信息。

Privacy 头字段见 RFC 3323 和附录 A.9, P-Asserted-Identity 头字段和 P-Preferred-Identity 头字段见附录 A。

对于 Profile C:

在应用了本节所述的映射程序之后, 主叫用户号码或通用号码参数内的地址如果和封装在 ISUP 中的地址分别相等, 则无需额外的互通。对于不等的情况, 则采用和 Profile A 和 Profile B 相同的方式处理。

表 5 SIP From/P-Asserted-Identity/Privacy 头字段到 ISUP CLI 参数的映射

接收到“P-Asserted-Identity”头字段, 其中包含的 URI (注 2) 带有格式为“+” CC+NDC+SN 的标识?	接收到“From”头字段, 其中包含的 URI 带有格式为“+” CC+NDC+SN 的标识?	主叫用户号码参数地址信号	主叫用户号码参数 APRI	通用号码 (附加的主叫号码) 地址信号	通用号码参数 APRI
否	否	网络选项, 或者包含一个网络提供的 E.164 号码 (见表 6) 或者省略该地址信号	如果收到 Privacy 头字段, 则根据表 7 设置 APRI, 否则网络选项, 将 APRI 或者设置为“提供限制”或者设为“提供允许”	不包含	不适用
否	是	网络选项, 或者包含一个网络提供的 E.164 号码 (见表 6) 或者省略该地址信号	如果收到 Privacy 头字段, 则根据表 7 设置 APRI, 否则网络选项, 将 APRI 或者设置为“提供限制”或者设为“提供允许”	网络选项, 或者省略该参数 (如果 CgPN 已经省略) 或者从“From”头字段导出 (见表 8) (注 1)	APRI = “提供限制”或“提供允许”, 这取决于 SIP Privacy 头字段 (见表 8)
是	否	从 P-Asserted-Identity 导出 (见表 7)	APRI = “提供限制”或“提供允许”, 这取决于 SIP Privacy 头字段 (见表 7)	不包含	不适用
是	是	从 P-Asserted-Identity 导出 (见表 7)	APRI = “提供限制”或“提供允许”, 这取决于 SIP Privacy 头字段 (见表 7)	网络选项, 或者省略该参数, 或者从 From 头字段导出 (注 1) (见表 8)	APRI = “提供限制”或“提供允许”, 这取决于 SIP Privacy 头字段 (见表 8)

注 1: 这种映射有效地为所有的 SIP UAC 提供接入到 I-IWU 的 Special Arrangement 的等价参数。
 注 2: P-Asserted-Identity 头字段有可能同时包含一个 tel URI 和一个 sip URI。对这种情况的处理有待进一步研究。
 注 3: “From”头字段可能包含一个“Anonymous URI”。“Anonymous URI”包含不指向主叫用户的信息。建议 Anonymous URI 自身的值为“anonymous@anonymous.invalid”。

表6 网络提供的带 CLI (网络选项) 的 ISUP 主叫用户号码参数的设置

ISUP CgPN 参数字段	值
过滤指示语	“网络提供”
号码不全指示语	根据实际情况设置
编号计划指示语	“ISDN/电话 (E.164)”
地址提供限制指示语	“提供允许/提供限制” (见表 5)
地址性质指示语	如果下一个 ISUP 节点位于同一个国家, 则置成“国内 (有效) 号码”, 否则置成“国际号码”
地址信号	如果地址性质指示语是“国内 (有效) 号码”, 则不应包含国家码。如果 NOA 是“国际号码”, 则应包含网络提供号码中的国家码

表7 P-Asserted-Identity 和 Privacy Headers 到 ISUP 主叫用户号码参数的映射

SIP 头字段和成分	成分值	ISUP 主叫用户号码 参数/字段	映射值
-	-	号码不完整指示语	“完整”
-	-	编号计划指示语	“ISDN/电话编号计划 (E.164)”
P-Asserted-Identity 头字段, URI 的部分号码, 假定格式为: “+” CC+NDC+SN (注 1)	CC	地址性质指示语	地质性质指示语的设置, 遵从 YD/T 1157.2-2003 网间主叫号码的传送 (补充件 2)
Privacy 头字段, priv-value 成分 (注 2)	Privacy 头字段不存在	限制地址提供指示语 (APRI)	允许提供
	“none”		允许提供
	“header”		限制提供
	“user”		限制提供
	“id”		限制提供
-	-	过滤指示语	网络提供
P-Asserted-Identity 头字段, URI 的部分号码 (注 1)	注 3	地址信号	遵从 YD/T 1157-2001、YD/T 1157.2-2003、YD/T 1157.3-2005 的要求

注 1: P-Asserted-Identity 头字段有可能同时包含一个 tel URI 和一个或多个 sip URI。对这种情况的处理有待进一步研究。
注 2: 有时可能同时收到两个 priv-value, 一个是“none”, 另一个是“id”, 在这种情况下, APRI 应该设成“限制提供”。
注 3: 本部分不考虑国际局的情况

5.2.3.7 通用号码

表8 SIP From 头字段到 ISUP 通用号码 (附加的主叫用户号码) 参数 (网络选项) 的映射

SIP 头字段和成分	成分值	ISUP 通用号码参数/字段	映射值
-	-	号码限定词指示语	“附加主叫用户号码”
From 头字段, URI 的 userinfo 成分	CC	地址性质指示语	地质性质指示语的设置, 遵从 YD/T 1157.2-2003 网间主叫号码的传送 (补充件 2)
-	-	号码不完整指示语	“完整”
-	-	编号计划指示语	“ISDN/电话编号方案 (E.164)”
-	-	限制地址提供指示语 (APRI)	使用与主叫用户号码相同的设置
-	-	过滤指示语	“用户提供, 未核实”
From 头字段, Userinfo 成分	注	地址信号	遵从 YD/T 1157-2001、YD/T 1157.2-2003、YD/T 1157.3-2005 的要求

注: 本部分不考虑国际局的情况。

5.2.3.8 用户业务信息 (可选)

见 5.2.3.5 节。

5.2.3.9 跳计数器 (可选)

对于 Profile C, I-IWU 应使用从封装的 IAM 中提取的跳计数器来执行正常的 ISUP 跳计数器程序。如果封装的 IAM 消息中没有跳计数器参数可用, I-IWU 也可以使用应用于 Profile A 和 Profile B 的处理程序。

对于 Profile A 和 B, I-IWU 应执行本节的下述互通程序。

在 I-IWU 中, 应使用 Max-Forwards SIP 头字段来导出跳计数器参数。I-IWU 通过使用一个因数来将 Max Forwards 适配到跳计数器, 如表 9 所示。该因数根据下列原则构造:

1) 给定消息的跳计数器应在每访问过一个 IWU 后单调递减, 中间的互通不记入其中。SIP 域内的 Max-Forwards 亦是如此。

2) 跳计数器的初始值及其后的映射值应该足够大, 使之能满足一个呼叫有效选路所预期的最大跳数目。

表9给出了映射的原则。

表9 Max-Forwards 到跳计数器的映射

Max-Forwards 值	跳计数器值
X	$Y = (X/\text{因数})$ 的整数部分

注: Max-Forward到跳计数器的映射需要考虑呼叫所经过的网络的拓扑结构。既然呼叫的选路和跳数依赖与呼叫的始发地和目的地, 映射因数同样也依赖于呼叫的始发地和目的地。而且当呼叫路由经过一个管理边界时, I-IWU运营者会和紧邻的网络管理者进行协调, 提供与紧邻网络所使用的初始设置或映射因数保持一致的映射方式。

总之, 映射因数依赖于呼叫的始发地和目的地, 而且 I-IWU 需要根据网络拓扑结构、信任域规则和双边协定来提供该因数。

5.3 后续 INVITE 的接收

当 I-IWU 支持重叠信令时适用本节内容。

如果 I-IWU 收到一个 INVITE, 这个 INVITE 的 Call-ID 和 From tag 与之前收到的 INVITE 消息相同, 且这个之前的 INVITE 已经在 ISUP 侧触发了一个呼叫, 则:

1) 如果 Request-URI 中的号码的数量大于已经收集到的号码的数量, I-IWU 将产生一个 SAM, 并把它交给出局 ISUP 程序处理。SAM 消息中的后续号码参数应当只包含附加的号码, 不应包含之前收集到的号码。对于 Profile C (SIP-I), 任何封装在 INVITE 里的 IAM 在这个处理过程中不予使用。对于之前的任何一个 INVITE 消息, 都以 484 (地址不全) 给予响应。

2) 如果 Request-URI 中的号码的数量少于已经收集到的号码的数量, 则 I-IWU 应立即对这个 INVITE 消息给出 484 地址不全响应。在这种情况下, 将不发出 SAM 消息。

5.3.1 独立于会话协商和地址信息的接收

作为一般性原则, 重叠信令程序考虑到会话协商 (特别地, 预置条件的协商和确认), 程序继续执行而与地址信息的接收无关。当发送 484 地址不全响应时, I-IWU 会认为由 INVITE 发起的 offer-answer 交互已经结束。新的 INVITE 发起新的 offer-answer 交互。然而, 如果资源已经预留且它们在新的 offer-answer 的交互中可以重新使用, 则预置条件的信令应当反映受影响的预置条件的当前状态。

5.3.2 不支持重叠信令

若 I-IWU 不支持重叠信令,在收到 INVITE 后,如果 I-IWU 能够判定 INVITE 中包含太少的数字位,而不能向 PSTN/ISDN 发送成组信令时, I-IWU 应该立即产生一个 484 地址不全响应。

5.4 COT 的发送

当 I-IWU 确定已满足入局 SIP 侧的所有预置条件且在出局 ISUP 侧的导通测试已成功完成时, I-IWU 应发送导通指示语应置为“导通检验成功”的 COT 消息。

5.5 连接消息 (CON) 的接收

如果收到 CON,则发送 200 OK (INVITE),见表 10。

表10 接收到 CON 后给 SIP 发送的 Method

←发送给 SIP 的消息	←从 ISUP 接收到的消息
200 OK (INVITE)	CON

对于 Profile C (SIP-I), CON 封装在 200 OK 消息里,作为 INVITE 的最终响应。

5.6 ACM 的接收

表 11 给出了 I-IWU 中 ACM 消息到 SIP 侧的映射。

接收到 ACM 后, I-IWU 的入局侧回送的 SIP 响应取决于 ACM 消息的“后向呼叫指示语——被叫用户状态指示语”参数的值。

1) BCI (被叫用户状态指示语) = “用户空闲”:

——如果是 Profile A 和 Profile B,则 I-IWU 发送 180 Ringing SIP 响应;

——如果是 Profile C,则 I-IWU 发送封装了 ACM 消息的 180 Ringing SIP 响应。

2) BCI (被叫用户状态指示语) = “无指示”或除“用户空闲”外的其他任何值:

——如果是 Profile A 和 Profile B,则 ACM 不参与互通,带有“带内信息或适当码型目前可用”信息的 ACM 除外(注 1);

——如果是 Profile C (SIP-I),则 I-IWU 发送封装了 ACM 的 183 Session Progress 响应(见表 11)。

注 1:对于 Profile A 和 Profile B,如果 I-IWU 收到在任选后向呼叫表示语中带有“带内信息或适当码型目前可用”信息的 ACM,则在 SIP 侧发送带有 SDP 的 183 Session Progress。

如果 T9 定时器超时,则释放 ISUP 连接并发送 480 Temporarily Unavailable。

表11 接收到 ACM 后发送给 SIP 的 Method

←发送给 SIP 的消息	←ACM	
	后向呼叫指示语参数	任选后向呼叫指示语
	被叫用户状态指示语	比特 A
183 Session Progress (仅用于 Profile C)	00 无指示	-
183 Session Progress, 且携带相关的 SDP (用于 Profile A 和 B)	-	带内信息或适当码型目前可用
180 Ringing	01 用户空闲	-

5.7 CPG 的接收

对于 Profile A 和 Profile B,如果 CPG 的事件指示语是“进展”和,则 CPG 不参与互通。如果事件指示语是“带内信息或适当码型目前可用”,则映射成带有 SDP 的 183 Session Progress。如果事件指示语是“振铃”,则 CPG 映射成 180 Ringing,见表 12。

对于 Profile C, 收到 CPG 消息后, I-IWU 的 SIP 侧应该发送 180 Ringing 或者 183 Session Progress SIP 响应 (见表 12), 且 CPG 消息封装在响应中。

表12 I-IWU 接收到 CPG

←发送给 SIP 的消息	←CPG
	事件信息参数 事件指示语
180 Ringing	000 0001 (振铃)
183 Session Progress (仅用于 Profile C)	000 0010 (进展)
183 Session Progress 且携带相关的 SDP (用于 Profile A 和 B)	000 0011 (带内信息或适当码型现在可用)

5.8 应答消息 (ANM) 的接收

接收到 ISUP ANM 后, I-IWU 应向 UAC 发送 200 OK (INVITE)。如果初始的 INVITE 消息没有携带 SDP offer, 且不支持可靠的临时性响应, 则 200 OK 应该包含 SDP offer, 该 SDP 应该与 ISUP 侧所使用到 TMR/USI 保持一致。

对于 Profile C (SIP-I), ANM 封装在 200 OK 消息里, 作为 INVITE 的最终响应。

5.9 承载通道的直通连接

对于 Profile A 和 Profile B 的情况, I-IWU 在发出初始地址消息之后, 立即建立传输通道的后向直通连接; 当收到 CON 或 ANM, 则建立传输通道的前向直通连接, 除非出局电路有限制。

如果呼叫连接类型是“语音”或“3.1kHz 音频”, 且出局电路没有特别的限制, 则在发出 IAM 消息之后也可以立即建立双向的直通连接。

对于 Profile C (SIP-I) 的情况, 如果出局电路没有特别的限制, 则 I-IWU 在发出 IAM 消息之后立即建立承载通道双向的直通连接。

5.10 网络发起的暂停消息 (SUS) 的接收

ISUP 侧接收到暂停消息 (SUS) 后的动作见 YDN 038-1997 的 7.4.1 节中描述。

SUS 在 Profile A 和 Profile B 中不参与互通。

对于 Profile C, SUS 被封装在 INFO 请求的 MIME 消息体中。

表13 接收到 SUS 后发送给 SIP 的 INFO (仅用于 Profile C)

←发送给 SIP 的消息	←从 ISUP 接收到的消息
INFO	SUS

5.11 网络发起的恢复消息 (RES) 的接收

ISUP 侧接收到恢复消息 (RES) 后的动作见 YDN 038-1997 的 7.4.2 节。

RES 在 Profile A 和 Profile B 中不参与互通。

对于 Profile C, RES 被封装在 INFO 中。

表14 网络发起的恢复消息 (RES) 的接收 (仅用于 Profile C)

←发送给 SIP 的消息	←从 ISUP 接收到的消息
INFO	RES

5.12 I-IWU 的释放程序

5.12.1 BYE/CANCEL 的接收

接收到 BYE 或 CANCEL 后, I-IWU 向 ISUP 侧发送 ISUP REL。

对于 Profile C, 封装在 BYE 内的 REL 无需修改直接传送给 ISUP 程序。至于收到的 CANCEL 消息, 处理程序同下面描述的 Profile A 和 Profile B 的处理程序。

对于 Profile A 和 Profile B:

如果 BYE 或 CANCEL 包含带有 Q.850 原因值的 Reason 头字段, 则原因值将依据本地策略映射成 REL 的原因值。表 15 描述了 SIP Reason 头字段到 ISUP 原因指示语参数的映射。表 16 给出了当 SIP Reason 头字段未给出原因值时, REL 中的原因值的编码。在这两种情况下, ISUP 的位置域 (Location) 置为“超出互通点的网络”。Reason 头字段见 RFC 3326。

表15 SIP Reason 头字段到 ISUP 原因指示语参数的映射

SIP Reason 头字段的成分	成分值	ISUP 参数/域	值
protocol	“Q.850”	原因指示语参数	-
Protocol-cause	“cause = x x” (注)	原因值	“x x” (注)
-	-	位置	“超出互通点的网络”

注: “x x”是 Q.850 中定义的原因值。

表16 当不能从 Reason 头字段中获得原因值时 REL 原因值的编码 (收到封装的 REL 的情况除外)

SIP 消息 →	REL →
	原因指示语参数
BYE	原因值 16 (正常拆线 normal clearing)
CANCEL	原因值 31 (正常 - 未指定 normal unspecified)

5.12.2 REL 的接收

接收到 ISUP REL 后, I-IWU 立即请求释放内部承载通道。当这条 ISUP 电路可供重选时, 向 ISUP 侧发送一个 ISUP RLC。

表 17 给出了 ISUP 原因指示语参数到 SIP Reason 头字段的映射。

表17 ISUP 原因指示语参数到 SIP Reason 头字段的映射

ISUP 原因指示语参数/域	参数/域值	SIP Reason 头字段的成分	成分值
-	-	protocol	“Q.850”
原因值	“x x” (注 1)	Protocol-cause	“cause = x x” (注 1)
-	-	reason-text	应当填满 Q.850 中声明的定义正文。(注 2)

注 1: “x x”是 Q.850 中定义的原因值。
注 2: 由于原因指示语参数不包含 Q.850 的 Table 1 中定义的定义正文, 这就得依据 O-IWU 的规定。

如果在接收到 ANM 或 CON 之前接收到 REL, I-IWU 应该发送适当的状态码作为最终响应。表 18 给出了 ISUP 原因值到 SIP 状态码的映射。在表 18 中未出现的原因值应该与 Q.850 中定义的类默认值有相同的映射。

如果在接收到 ANM 或 CON 之后接收到 REL, I-IWU 应发送 BYE。

对于 Profile C, 封装 REL 消息的状态码应当与表 18 中的默认映射一样。

如果在接收到 REL 消息之前, I-IWU 的人局侧已经发送最终响应 (如 200 OK (INVITE)) (但还没有接收到 ACK), 则 I-IWU 不应发送 487 Request terminated, 而是等到接收到 ACK 之后再发送 BYE 消息。

表18 释放消息 (REL) 的接收

←SIP 消息	← REL
	原因指示语参数
404 Not Found	原因值 1 (未分配的号码)
500 Server Internal Error	原因值 2 (无路由到指定的网络)
500 Server Internal Error	原因值 3 (无路由到目的地)
500 Server Internal Error	原因值 4 (发送专用信息音)
404 Not Found	原因值 5 (误拨长途字冠)
500 Server Internal Error (Profile-C only)	原因值 8 (抢占)
500 Server Internal Error (Profile-C only)	原因值 9 (抢占—电路留作再用)
486 Busy Here	原因值 17 (用户忙)
480 Temporarily unavailable	原因值 18 (用户未响应)
480 Temporarily unavailable	原因值 19 (用户未应答)
480 Temporarily unavailable	原因值 20 (用户缺席)
480 Temporarily unavailable	原因值 21 (呼叫拒绝)
410 Gone	原因值 22 (号码改变)
无映射	原因值 23 (改发到新目的地)
480 Temporarily unavailable	原因值 25 (交换机选路错误)
502 Bad Gateway	原因值 27 (目的地不可达)
484 Address Incomplete	原因值 28 (无效的号码格式 (地址不全))
500 Server Internal Error	原因值 29 (性能拒绝)
480 Temporarily unavailable	原因值 31 (正常, 未指定) (此为 000 和 001 类默认值)
如果诊断指示语包含 (CCBS 指示语 = CCBS 可能), 则状态码为 486 Busy here, 否则为 480 Temporarily unavailable	010 类的原因值 (资源不可用类, 原因值 34 无电路/通路可用)
500 Server Internal Error	010 类的原因值 (资源不可用类, 原因值 38 - 47) (47 为 010 类默认值)
500 Server Internal Error	原因值 50 (所请求的性能未预订)
500 Server Internal Error (SIP-I only)	原因值 55 (CUG 中限制去呼叫)
500 Server Internal Error	原因值 57 (承载能力无权)
500 Server Internal Error	原因值 58 (承载能力目前不可用)
500 Server Internal Error	原因值 63 (业务选项不可用, 未指定) (此类默认值)
500 Server Internal Error	100 类的原因值 (业务或选项未实现类 原因值 65 - 79) (79 为 100 类默认值)
500 Server Internal Error (SIP-I only)	原因值 87 (被叫用户不是 CUG 的成员)
500 Server Internal Error	原因值 88 (不兼容的目的地)
500 Server Internal Error (SIP-I only)	原因值 90 (不存在的 CUG)
404 Not Found	原因值 91 (无效的转接网选择)
500 Server Internal Error	原因值 95 (无效的消息, 未指定) (此为 101 类默认值)
500 Server Internal Error	原因值 97 (消息类型不存在或未实现)

表 18 (续)

←SIP 消息	← REL
	原因指示语参数
500 Server Internal Error	原因值 99 (信息单元/参数不存在或未实现)
480 Temporarily unavailable	原因值 102 (定时器超时恢复)
500 Server Internal Error	原因值 103 (参数不存在或未实现,传递)
500 Server Internal Error	原因值 110 (消息带有未被识别的参数,舍弃)
500 Server Internal Error	原因值 111 (协议错误,未指定) (此为 110 类默认值)
480 Temporarily unavailable	原因值 127 (互通,未指定) (此为 111 类默认值)

5.12.3 I-IWU 中的自行释放

表 19 给出了当呼叫从 SIP 穿越到 ISUP 时发生在 I-IWU 内的触发事件以及由 I-IWU 发起的释放。

如果 I-IWU 发起的自动重复试呼不成功 (因为呼叫无法选路), I-IWU 应向 SIP 侧发送 480 Temporarily Unavailable 响应。ISUP 侧无需动作。

在应答后, 如果 IWU 中 ISUP 程序的结果为自行 REL, 则应在 SIP 侧发送 BYE。

如果 I-IWU 接收到不可识别的后向 ISUP 信令信息, 并根据编码判定需要释放该呼叫, 则 I-IWU 应在 SIP 侧发送 500 ServerInternal Error 响应。根据本地策略, Reason 头字段应该加入到 I-IWU 发出的 SIP 消息 (BYE 或最终响应) 中, 它所带的原因值与 I-IWU 在 ISUP 侧发出的 REL 的原因值应该一样。

对于 Profile C, 基于触发事件, 封装 REL 的 BYE 或 SIP 状态码应当与表 18 所给出的默认映射一致。

表 19 I-IWU 中的自行释放

← SIP	触发事件	REL→ 原因指示语参数
484Address Incomplete	确认没有收到足够的位数, 见 5.2 节的注。 在重叠发送程序内接收到后续的 INVITE, 见 5.3 节	不发送
480 Temporarily Unavailable	IWU 中拥塞。	不发送。
BYE	ISUP 程序导致应答后释放	遵从 ISUP 程序
500 Server Internal Error	ISUP 兼容性程序导致呼叫释放 (注)	遵从 ISUP 程序
484 Address Incomplete	在 ISUP 程序内由于 T7 超时导致呼叫释放	遵从 ISUP 程序
480 Temporarily Unavailable	在 ISUP 程序内由于 T9 超时导致呼叫释放	遵从 ISUP 程序
480 Temporarily Unavailable	应答前由于其他 ISUP 程序导致呼叫释放	遵从 ISUP 程序

注: I-IWU 接收到不可识别的 ISUP 信令信息, 并根据兼容性指示语的编码判定需要释放该呼叫, 见 YDN 038 - 1997

5.12.4 RSC、GRS 或 CGB (ISUP) 的接收

表 20 给出了在已经接收到至少一个与呼叫相关的后向 ISUP 消息后, 接收到 ISUP RSC 消息、GRS 消息或带有编码为“面向硬件故障”的电路群监视消息类别指示语的 CGB 消息时 I-IWU 所发送的消息。

- 1) 如果 I-IWU 已经接收到 200 OK (INVITE) 的 ACK, 则发送 BYE。
- 2) 如果 I-IWU 已发送 200 OK (INVITE) 但还未收到 200 OK (INVITE) 的 ACK, 则应等到接收到 200 OK (INVITE) 的 ACK 之后再发送 BYE。
- 3) 其他的情况, I-IWU 发送 500 Server Internal Error。

接收到 GRS 或 CGB 消息后,应给每个相关呼叫发送一个 SIP 消息。所以,接收到一个 GRS 或 CGB 消息后可能发送多个 SIP 消息。

在使用 Profile C 的情况下, SIP BYE 或 500 Server Internal Error 响应封装的应该是 ISUP 程序产生的 REL,而不是 RSC、GRS 或 CGB 消息。

表20 RSC、GRS 或 CGB 消息的接收

← SIP	← 从 ISUP 接收到的消息
500 Server Internal Error 或 BYE	复原电路消息 (RSC)
500 Server Internal Error 或 BYE	电路群复原消息 (GRS)
500 Server Internal Error 或 BYE	电路群闭塞消息 (CGB) 带有编码为“面向硬件故障”的电路群监视消息类别指示语

6 O-IWU 中从 ISUP 到 SIP 的出局呼叫的互通

本章规定在出局 IWU 中对基本呼叫的信令互通要求。本章按照 O-IWU 的出局 SIP 侧收到或发送的消息划分成各个子节。本章只考虑作为 ISUP 和 SIP 互通的结果而产生的消息,不描述作为本地协议状态机的结果而产生的消息。

对于 Profile C, ISUP 消息的分段如 4.2.3.3 节所述。

6.1 第一个 INVITE 的发送

O-IWU 从 ISUP 网络接收地址消息 (IAM, 其后还可能跟着 SAM) 后,执行正常的 ISUP 处理并将该呼叫选路到 SIP 网络域。O-IWU 根据配置确定是否在 SIP 侧使用成组寻址方式。

1) 如果使用成组寻址方式, O-IWU 应根据以下 a) 到 d) 判据来确定地址信令的结尾,然后调用本节所描述的适当的出局 SIP 信令程序。地址信令的结尾由以下判据来确定:

- 接收到 end-of-pulsing (ST) 信号;
- 接收到国内编号计划中使用的上限位数;
- 通过分析被叫用户号码,发现已接收到足够的位数来将呼叫选路到被叫用户;
- 观察到定时器 T_{Orw1} 已超时。

如果符合上面的判据 a), b) 和 c), 地址信令的结尾已被确定,则在发送 INVITE 时应启动定时器 T_{Orw2} 。

注: 最好选择成组方式, Profile A 要求使用成组方式。

2) 如果在 SIP 网络侧使用重叠地址发送,则 O-IWU 在接收到为这个呼叫选路所需的最少的位数之后应:

- 启动定时器 T_{Orw2} , 并调用本节所描述的适当的出局 SIP 信令程序。
- 按照 6.2.1 节所述准备处理 SAM。

O-IWU 将根据以下情形之一调用出局 SIP 信令程序,使用哪种情形取决于 SIP 网络中是否使用预置条件:

- 1) 接收到 ISUP IAM/SAM 后发送不带预置条件的 INVITE;
- 2) 接收到 ISUP IAM/SAM 后发送带预置条件的 INVITE。

详细的流程将会在本节中进行描述,而 O-IWU 接收到的 IAM 编码和发送的 INVITE 将在后面的章节中进行描述。

对于 Profile C, IAM 就会被封装在出局的 INVITE 消息中。

如果定时器 (T_{OIRW2}) 超时, 则向 ISUP 网络发送一个 early ACM, 见 6.4 节。

(A) 接收到 ISUP IAM/SAM 后发送不带预置条件的 INVITE

出局的 SIP 流程的应用将会考虑以下的一些关于何时发送 INVITE 的说明和特例情况。

当接收到 ISUP IAM (可能还有 SAM), 且 IAM 消息的连接性质指示语参数中的导通检验指示语被设为“不要求导通检验”, 则发送 INVITE。

如果 IAM 的连接性质指示语参数中的导通检验指示语被设为“在本电路上要求导通检验”或“在前一电路上执行导通检验”, 则延迟发送 INVITE。在接收到导通指示语参数置为“导通检验成功”的导通消息之后, 才发送 INVITE。如果接收到导通指示语参数置为“导通检验失败”的导通消息或 ISUP 定时器 T8 超时, 则不应发送 INVITE。

(B) 接收到 ISUP IAM/SAM 后发送带预置条件的 INVITE

接收到 ISUP IAM (可能还有 SAM) 后发送带预置条件的 INVITE。入局的 SIP 流程的应用将会考虑以下一些关于何时发送已满足预置条件确认的说明和特例情况。

注: 配置的程序可能延迟发送 INVITE, 直到在出局承载通道上预留好本地资源。

O-IWU 应使用 INVITE 中的 SDP Offer 来发起预置条件信令程序。当满足下述两个条件时, 发送带有表示预置条件已满足的确认的 SDP offer 或 answer。(在一个 SDP offer-answer 交换内) 发送表示预置条件已满足的确认后, 预置条件信令结束。

1) 如果 IAM 的连接性质指示语参数中的导通检验指示语被设为“在本电路上要求导通检验”或“在前一电路上执行导通检验”, 且接收到导通指示语参数设为“导通检验成功”的导通消息。

2) SIP 网络满足所要求的预置条件。

注: 对于 Profile A, “预置条件已满足”的信令总是产生在 UPDATE 消息的 SDP offer 中。

如果接收到导通指示参数被设为“导通检验失败”的导通消息或 ISUP 定时器 T8 超时, 则应发送 CANCEL 或 BYE (依据 6.7.1 的规则)。

如果内部资源预留不成功, 则在 O-IWU 的 ISUP 侧发送原因值为 47 (资源不可用, 未指定) 的 REL, 在 SIP 侧发送 CANCEL 或 BYE (依据 6.7.1 的规则)。更多细节见 6.7.3 节。

对于以上两种发送 INVITE 的情况 ((A) 和 (B)), 表 21 对出局 INVITE 消息的头字段作了汇总。

表 21 INVITE 消息的互通内容

IAM→	INVITE→
被叫用户号码	Request-URI (见 6.1.2 和 6.2 节)
	To (见 6.1.2 节)
主叫用户号码	P-Asserted-Identity (见 6.1.3 节)
	Privacy (见 6.1.3 节)
	From (见 6.1.3 节)
通用号码 (附加的主叫用户号码)	From (见 6.1.3 节)
跳计数器	Max-Forwards (见 6.1.4 节)
TMR/USI	Message Body (application/SDP) (见 6.1.1 节)
ISUP 消息	Message Body (application/ISUP) (注)

注: 只适用于 Profile C, 见 4.2.1.2

6.1.1 来自 TMR/USI 的 SDP 媒体描述行的编码

O-IWU 接收到的 IAM 中带有 TMR 参数和可选的用户业务信息参数,这两个参数表明了用户所请求的承载业务特性。它们的编码应映射成 SDP 信息。YDN 038-1997 给出了 TMR 和 USI 参数中可用编码的完整列表。原则上,只要有转换代码,这些编码的任意组合能映射成任意的 SDP 信息。

对于 Profile-A, O-IWU 应能够对 AMR 编解码器进行 SDP 编码,这在 RFC 3267 “用于 AMR、AMR-WB 音频编解码器的 RTP 净荷格式和文件存储格式”中有描述。

表 22 给出了 O-IWU 不带编解码器时从 TMR/USI 编码到 SDP 媒体描述行的映射关系。

表22 由 TMR/USI 导出的 SDP 媒体描述行的编码: 从 ISUP 到 SIP

TMR 参数	USI 参数		ATP 中的 HLC IE		m=行		b=行	a=行
TMR 编码	信息传送能力	用户信息 1 层协议指示	高层特性识别	<media>	<transport>	<fmt-list>	<modifier>: <bandwidth-value>	rtpmap: <dynamic-PT> <encoding name>/<clock rate>[/encoding parameters]
speech	Speech	G.711A-law	忽略	audio	RTP/AVP	8	AS: 64	rtpmap: 8 PCMA/8000
speech	Speech	G.711A-law	忽略	audio	RTP/AVP	Dynamic PT	AS: 64	rtpmap: <dynamic-PT> PCMA/8000
3.1 kHz audio	USI Absent		忽略	audio	RTP/AVP	0 和/或 8, 注 1	AS: 64	rtpmap: 0 PCMU/8000 和/或 rtpmap: 8 PCMA/8000, 注 1
3.1 kHz audio	3.1kHz audio	G.711A-law	Telephony or HLC absent	audio	RTP/AVP	8	AS: 64	rtpmap: 8 PCMA/8000
3.1 kHz audio	3.1kHz audio		Facsimile Group 2/3	image	udptl	t38	AS: 64	Based on T.38
3.1 kHz audio	3.1kHz audio		Facsimile Group 2/3	image	tcptl	t38	AS: 64	Based on T.38
64 kbit/s unrestricted	Unrestricted digital inf. W/tone/ann	不适用	忽略	audio	RTP/AVP	9	AS: 64	Rtpmap: 9 G.722/8000
64 kbit/s unrestricted	Unrestricted digital information	不适用	忽略	audio	RTP/AVP	Dynamic PT	AS: 64	rtpmap: <dynamic-PT> CLEARMODE/8000,注 1
2 64 kbit/s unrestricted	Unrestricted digital information	不适用	忽略	待定	待定	待定	待定	待定
384 kbit/s unrestricted	Unrestricted digital information	不适用	忽略	待定	待定	待定	待定	待定
1536 kbit/s unrestricted	Unrestricted digital information	不适用	忽略	待定	待定	待定	待定	待定
1920 kbit/s unrestricted	Unrestricted digital information	不适用	忽略	待定	待定	待定	待定	待定
N×64 kbit/s unrestricted, N from 3 to 29	Unrestricted digital information	不适用	忽略	待定	待定	待定	待定	待定

注 1: CLEARMODE 尚未标准化, 其用途待定

6.1.2 Request-URI 和 To 头字段

IAM 消息的被叫用户号码参数（可能还有 SAM 消息的后续号码参数的地址信号指示语）包含了用来导出 INVITE Request-URI 的 userinfo 成分的前向地址信息。

注：O-IWU 应依据现有 ISUP 处理程序来选择出局路由。如果产生一个新的被叫用户号码用于出局路由，则应将新产生的被叫用户号码映射到 INVITE Request URI 的 userinfo 成分中。

对于基本呼叫，包含在被叫用户号码参数和后续号码参数（如果有）中的地址信息也被视为被叫用户的标识。该信息映射成 Request-URI 的 userinfo 成分和 To 头字段的 addr-spec 成分。

如果 Request-URI 或 To 头字段包含 SIP: URI，则它应该包含“user = phone” URI 参数。

6.1.3 P-Asserted-Identity 和 privacy 头字段

表 23 给出了从主叫用户号码和通用号码到 INVITE 中的 SIP P-Asserted-Identity、From 和 Privacy 头字段的映射。表 24 给出了从通用号码到 From 头字段的详细映射。表 25 给出了从主叫用户号码到 P-Asserted-Identity 头字段的详细映射。表 26 给出了从主叫用户号码到 From 头字段的详细映射。表 27 给出了从主叫用户号码和通用号码的 APRI 子参数到 Privacy 头字段的详细映射。

表23 ISUP CLI 参数到 SIP 头字段的映射

是否接收到一个带有完整 E.164 号码的主叫用户号码，其带有的鉴别指示语=UPVP 或 NP(见注 1)，APRI=“提供允许”或“提供限制”？	是否接收到一个带有完整 E.164 号码的通用号码（附加的主叫用户号码），其带有的鉴别指示语=UPVP，APRI=“提供允许”？	P-Asserted-Identity 头字段	From 头字段： display-name（可选）和 addr-spec	Privacy 头字段
否	否	不包含该头字段	Unavailable@Hostportion	不包含该头字段
否 (注 4)	是	不包含该头字段	如果可能，display-name 从通用号码（ACgPN）中导出。 addr-spec 从通用号码（AcgPN）的地址信号中导出或使用网络提供的值	不包含该头字段
是 (注 1)	否	从主叫用户号码参数地址信号中导出（见表 25）	如果 APRI=“允许”，若可能 display-name 从主叫用户号码（CgPN）中导出。 如果 APRI=“限制”，则 display-name 为“Anonymous” 如果 APRI=“允许”，则 addr-spec 从主叫用户号码参数地址信号（见表 26）中导出或使用网络提供的值。 如果 APRI=“限制”，则 addr-spec 置为“Anonymous URI”（注 3）	如果主叫用户号码参数 APRI=“限制”，则 priv-value=“id”。对于其他的 APRI 设置，则不包含 Privacy 头字段，或者如果包含 Privacy 头字段，则不包含“id”（见表 27）
是	是	从主叫用户号码参数地址信号中导出（见表 25）	display-name 从通用号码（ACgPN）中导出（注 2） addr-spec 从通用号码（ACgPN）地址信号（见表 24）导出	如果主叫用户号码参数 APRI=“限制”，则 priv-value =;“id”。对于其他的 APRI 设置，则不包含 Privacy 头字段，或者如果包含 Privacy 头字段，则不包含“id”（见表 27）

注 1: CgPN参数中网络提供的CLI可能出现在来自模拟接入线的呼叫中。为了使该网络提供的CLI显示在SIP UAS中, 该网络提供的CLI必须映射成SIP From头字段。由于这是一个与特定主叫线对应的完全可信的CLI, 它也可以映射成 P-Asserted-Identity头字段。

注 2: IWU是否可能从通用号码参数导出Display name尚有待进一步研究。

注 3: “From”头字段可包含一个“Anonymous URI”。“Anonymous URI”包含不指向主叫用户的信息。建议display-name成分包含“Anonymous”。Anonymous URI自身应具有“anonymous@anonymous.invalid”值。

注 4: CgPN和ACgPN的这种组合是一种错误的情况, 在这里把它列出来是为了在不同的实现过程中确保映射完整性。

表24 通用号码 (附加的主叫用户号码) 到 SIP From 头字段的映射

ISUP 参数/字段	值	SIP 成分	值
通用号码 Number Qualifier Indicator	“附加的主叫用户号码”	From 头字段	display-name (可选) 和 addr-spec
地址信号	CC (如果存在), NDC (如果存在), SN 或 CC (如果存在), IC, SN	Display-name	如果可能且网络策略允许, Display-name 可以从地址信号映射
		Addr-spec	地址信号映射成所使用的 URI 编号方案的 user 部分 (注)

注: 如果被叫用户不是本地用户, 且 ISUP 信令中的主叫用户号码采用区号编号方式, 但未提供 NDC, 则应加上 NDC 再映射成 URI 编号方案的 user 部分。

表25 主叫用户号码参数到 SIP P-Asserted-Identity 头字段的映射

ISUP 参数/字段	值	SIP 成分	值
主叫用户号码		P-Asserted-Identity 头字段	display-name (可选) 和 addr-spec
地址信号	CC (如果存在), NDC (如果存在), SN 或 CC (如果存在), IC, SN	display-name	如果可能且网络策略允许, 可以将地址信号映射成 Display-name
		addr-spec	地址信号映射成所使用的 URI 方案的号码部分 (注)

注: 如果被叫用户不是本地用户, 且 ISUP 信令中的主叫用户号码采用区号编号方式, 但未提供 NDC, 则应加上 NDC 再映射成 URI 编号方案的 user 部分。

表26 ISUP 主叫用户号码参数到 SIP From 头字段的映射

ISUP 参数/字段	值	SIP 成分	值
主叫用户号码		From 头字段	display-name (可选) 和 addr-spec
地址信号	如果 NOA 是“国内 (有效) 号码”, 则地址信号的格式为 NDC+SN 如果 NOA 是“国际号码”, 则地址信号的格式为 CC+NDC+SN	display-name	如果可能且网络策略允许, 可以将地址信号映射成 Display-name
		addr-spec	“+” CC NDC SN 映射成所使用的 URI 方案的 userinfo 部分

表27 ISUP APRI 到 SIP Privacy 头字段的映射

ISUP 参数/字段	值	SIP 成分	值
主叫用户号码		Privacy 头字段	priv-value
APRI (使用哪个 APRI 来进行映射, 见表 23)	“提供限制”	Priv-value	“id” (仅当 SIP INVITE 中包含了 P-Asserted-Identity 头字段时才包含 “id”)
	“提供允许”	Priv-value	忽略 Privacy 头字段 或者如果需要其他的 privacy 业务, 则 Privacy 头字段不带 “id”
注: 如果主叫用户号码参数存在, 则 P-Asserted-Identity 头字段总是由此导出, 如表 23 所示			

6.1.4 Max Forwards 头字段 (任选)

对于 Profile C (SIP-I), 如果有可用的跳计数器参数, 则当 O-IWU 构造出局的被封装的 IAM 时应执行正常 ISUP 跳计数器程序; 对于 Profile A 和 B, O-IWU 应执行本节的下述互通程序。

O-IWU 中应利用跳计数器参数来导出 Max-Forwards SIP 头字段。O-IWU 应使用一个因数来将跳计数器适配到 Max Forwards, 如表 28 所示。该因数根据下列原则构造:

a) 给定消息的 Max-Forwards 应在每访问过一个 IWU 后单调递减, 中间的互通不计入其中。ISUP 域内的跳计数器亦是如此。

b) Max-Forwards 的初始值及其后的映射值应该足够大, 使之能满足为一个呼叫有效选路所预期的最大跳数目。

表 28 给出了映射的原则。

表28 跳计数器到 Max-Forwards 的映射

跳计数器值	Max-Forwards 值
X	$Y = (X * \text{因数})$ 的整数部分

注: 跳计数器到Max-Forward的映射需要考虑呼叫所经过的网络的拓扑结构。既然呼叫的选路和跳数依赖与呼叫的始发地和目的地, 映射因数同样也依赖于呼叫的始发地和目的地。而且当呼叫路由经过一个管理边界时, O-IWU 运营者会和紧邻的网络管理者进行协调, 提供与紧邻网络所使用的初始设置或映射因数保持一致的映射方式。

总之, 映射因数依赖于呼叫的始发地和目的地。而且 O-IWU 需要根据网络拓扑结构、信任域规则和双边协定来提供该因数。

6.1.5 被封装的 IAM 的参数编码 (仅适用于 Profile C)

本小节规定了特定的被封装的 ISUP 信息的编码, 该编码基于适当的 ISUP 程序。特定参数/指示值的计算基于 O-IWU 是一个 ISDN/PSTN 交换机的假定。

6.1.5.1 连接性质参数

O-IWU 应在连接性质参数中将卫星指示语的值加 1。

6.1.5.2 传播时延计数器参数

O-IWU 应基于表征 IP 网络时延的可用网络配置数据, 将传播时延计数器增加一个适当值。

6.2 发出 INVITE 之后的 SAM 的接收

6.2.1 采用成组方式时接收到 SAM 后的程序

如果对 SIP 网络使用成组寻址, 则应忽略在 O-IWU 发送 INVITE 之后所接收到的后续 SAM 消息。

6.2.2 采用重叠方式时接收到 SAM 后的程序

在 O-IWU 入局侧运行的 ISUP 程序接收到 SAM 消息后，O-IWU 应：

1) 停止定时器 T_{Oiw3} (如果正在运行)。

2) O-IWU 应重启定时器 T_{Oiw2} ，调用 6.1 节所描述的适当的 SIP 出局信令程序 (A) 或 (B)，并附带以下程序：

a) 新 INVITE 的 Request-URI 和 To 头字段应包含迄今为止对该呼叫所接收到的所有位数。

b) 发送一个与前一 INVITE 具有相同 call-ID 和 From 头字段(包括 tag)的新 INVITE。对于 Profile C，封装在初始的 INVITE 中的 IAM 也要封装在新的 INVITE 中。

c) 新 INVITE 应包含一个新的 SDP offer。O-IWU 可以重新使用已经为该呼叫预留的任何资源。这种对现有预留资源的使用应在相应 SDP 参数的预置条件属性中反映出来。

d) 新 INVITE 的其余内容从始发 IAM 的参数中互通得到，具体互通程序见 6.1 节。

如果定时器 T_{Oiw2} 超时，则应忽略在 O-IWU 发送 INVITE 之后接收到的后续 SAM 消息。

6.3 18X 响应的接收

表 29 给出了 18X 消息到 ISUP 消息的映射。

表29 18X 响应的接收

←ISUP 消息	←18X 响应
ACM 或 CPG (注 1)	180 Ringing
ACM 或 CPG (注 2)(只适用语 Profile C)	183 Session Progress, 封装着 ACM 或 CPG
注1: 见 6.3.1 节。	
注2: 见 6.3.2 节	

注：基于定时器超时，本地ISUP程序可产生后向的早期ACM（无指示）。这些程序的运作独立于与SIP的互通。

6.3.1 180 Ringing 的接收

接收到 180 Ringing 消息后，停止定时器 T_{Oiw2} (如果正在运行)。如果接收到一个未封装任何 ISUP 消息的 180 Ringing, O-IWU 应发送 ACM 消息或 CPG 消息, 这由有关在此之前是否为该呼叫发送过 ACM 的 ISUP 程序确定。如果要发送 ACM 消息，则后向呼叫指示参数中的被叫用户状态指示语编码为“用户空闲”。如果要发送 CPG，则事件指示语应置为“提醒”。

对于 Profile C，如果收到的 180 Ringing 封装了 ACM 或 CPG 消息，O-IWU 应当根据封装的 ISUP 消息和现有的 ISUP 信令状态确定适当的后向 ISUP 消息和参数, 应当停止定时器 T_{Oiw2} (如果正在运行)。

6.3.1.1 ACM 后向呼叫指示语的设置 (仅适用于 Profile A 和 Profile B)

本节的表中给出了当发送 ACM 时，O-IWU 所设置的后向呼叫指示语参数的缺省值。其他的后向呼叫指示语参数根据 ISUP 程序来设置。

IWU 所设置的 BCI 参数的指示语如下：

比 特	BCI 参数中的指示语
DC	被叫用户的状态指示语
I	互通指示
K	ISDN 用户部分指示
M	ISDN 接入指示

对 Profile A 和 Profile B，被叫用户状态指示语（比特 DC）置为“用户空闲”。

对于 Profile A, 缺省设置见表 30。

表30 Profile A 的后向呼叫指示语的默认设置

参 数	比 特	编 码	含 义
互通指示	I	1	遇到互通
ISDN 用户部分指示	K	0	ISDN 用户部分非全程使用
ISDN 接入指示	M	0	终端接入非 ISDN

对于 Profile-B, O-IWU 应基于对各种信息的分析, 如信令、内部状态和/或本地策略来设置 (被叫用户状态指示语之外的) BCI 参数的其他指示语的适当值。

6.3.1.2 CPG 消息的事件信息参数的设置 (只适用于 Profile A 和 Profile B)

本节的表中给出了在当发送 CPG 时, O-IWU 所设置的事件信息参数的缺省值。事件信息参数中的其他指示语根据 ISUP 程序来设置。

比 特	事件信息参数中的指示语
GFEDCBA	事件指示语

接收到 180 Ringing 后, O-IWU 应在事件信息参数字段中设置以下编码:

比 特	编 码	含 义
GFEDCBA: =	0000001	提醒

6.3.2 183 Session Progress 的接收

如果接收到未封装任何 ISUP 消息的 183 Session Progress, 则不发送任何后向 ISUP 消息, 并继续 ISUP 程序。

对于 Profile C (SIP-I), 如果接收到封装有 ISUP 消息的 183 Session Progress, O-IWU 应基于所封装的 ISUP 消息和当前 ISUP 信令的状态来确定适当的后向 ISUP 消息。在这种情况下应停止定时器 T_{Orw2} 。

6.4 定时器超时及 Early ACM 的发送

如果定时器 T_{Orw1} (对于在出局 SIP 接口中转换成成组呼叫的情况) 或 T_{Orw2} 超时, O-IWU 应返回 ACM。在执行导通检验的情况下, O-IWU 应暂不发送 ACM, 直到接收到成功的导通指示。

对于 Profile A 和 Profile B, O-IWU 应向主叫用户返回等待应答指示 (如振铃音或适当的进展提示音)。

BCI 参数的被叫用户状态指示语 (比特 DC) 置为“无指示”。其他 BCI 指示语应按 6.3.1.1 节所述进行设置。

6.5 200 OK (INVITE) 的接收

O-IWU 接收到对该呼叫的一个 200 OK (INVITE) 后, 应停止定时器 T_{Orw2} (如果正在运行)。

对于 Profile A 和 Profile B, O-IWU 应:

- 1) 按 ISUP 程序的规定发送 ANM 或 CON;
- 2) 停止任何现有的“等待应答指示” (如振铃音)。

对于 Profile C, 如果收到的 200 OK 响应封装了 ANM 或 CON, O-IWU 应基于所封装的 ISUP 消息和当前 ISUP 信令的状态来确定适当的后向 ISUP 消息。

6.5.1 CON 消息中的后向呼叫指示语的设置 (只适用于 Profile A 和 Profile B)

BCI 参数的被叫用户状态指示语 (比特 DC) 置为“无指示”。其他 BCI 指示语应按 6.3.1.1 节所述进行设置。

6.6 ISUP 承载通道的直通连接

对于 Profile A 和 B, 如果 ASN 不支持直通连接功能, O-IWU 应遵从 YDN 038-1997 中描述的目的交换机的直通连接程序。如果 ASN 支持关于目的交换机的直通连接程序, O-IWU 应当遵从 Profile C 的有关程序。

对于 Profile C (SIP-I), 应用下述程序。

承载通道的直通连接的完成应取决于在呼叫的 SIP 侧是否使用预置条件。

在 SIP 侧完成承载建立后就应建立起承载通道的双向直通连接。SIP 侧承载的建立完成通过下述情况来指示: 可被 O-IWU 接受的 SDP Answer 的接收, 以及一个指明所有必选的预置条件 (如果有) 已被满足的指示。

前向承载通道应在接收到 200 OK (INVITE) 之前完成连接。

6.6.1 信号音和语音通知 (后向)

对于 Profile A 和 Profile B, 以下情况将导致从 O-IWU 处播放振铃音:

- 1) 接收到 180 Ringing; 且
- 2) ISUP 程序指明可以使用振铃音; 且
- 3) 本地设置指配 O-IWU 而不是相关的 SIP 实体, 作为目的交换机。

注 1: 也可能由于 T_{Orw1} 或 T_{Orw2} 超时导致播放振铃音或进展提示音, 见 6.4 节。

注 2: 在相关 SIP 实体作为目的交换机的情况下, 可能从 SIP 网络接收到其他信号音或语音通知。

6.7 O-IWU 的释放程序

6.7.1 前向 REL 的接收

接收到 ISUP REL 后:

1) 在发送出 INVITE 之前收到 REL: 在 SIP 侧不需要任何动作。如果有本地程序在进展中, 则终止该程序。

2) 在收到 INVITE 的任何响应之前接收到 REL 消息: O-IWU 应保持 REL 消息, 直到接收到 SIP 响应。这时, O-IWU 应适当执行 (3) 或 (4) 所述的动作。

3) 在接收到建立确认的对话或早期的对话的响应之前, O-IWU 接收到 REL 消息: O-IWU 应发送 CANCEL 请求。如果 O-IWU 后来接收到一个 200 OK (INVITE), 则它应对该 200 OK (INVITE) 发送 ACK, 在发送 ACK 之后再发送 BYE 请求。

4) 在接收到建立确认的对话或早期的对话响应之后, O-IWU 接收到 REL 消息, O-IWU 应发送 BYE 请求。对于 Profile A 和 Profile B, 对于早期的对话, O-IWU 可用 CANCEL 取代 BYE。

对于 Profile C, 当发送 BYE 消息时, 应当把收到的 REL 封装于其中。

根据本地策略, 如果 O-IWU 支持 Reason 头字段, 则在 CANCEL 或 BYE 中应增加包含所接收到的 REL 原因值的 Reason 头字段。原因指示语参数到 Reason 头字段的映射见表 17 (5.12.2 节)。

6.7.2 后向 BYE 的接收

接收到 SIP BYE 后, O-IWU 应向 ISUP 侧发送 ISUP REL。

对于 Profile C, 被封装的 REL 无需修改直接传送给 ISUP 程序。

如果在 BYE 中包含有带 Q.850 原因值的 Reason 头字段, 则应将该原因值映射到 ISUP REL 的 ISUP 原因值字段中。Reason 头字段到原因指示语参数的映射见表 15 (5.12.1 节)。表 31 给出了在 Reason 头字段没有可用的原因值的情况下 REL 中原因值的编码。

表31 从 O-IWU 的 SIP 侧释放

←REL	←SIP 消息
原因指示语参数	
原因值 16 (normal clearing)	BYE

6.7.3 O-IWU 的自行释放

表 32 给出了在呼叫从 ISUP 穿越到 SIP 时在 O-IWU 处产生的触发事件以及 O-IWU 发起的释放。

如果在应答之后, ISUP 程序导致 O-IWU 的自行 REL, 则在 SIP 侧发送 BYE。

依据本地策略, 带有 REL 的原因值 (Q.850) 的 Reason 头字段可加进 SIP 消息 (BYE 或 CANCEL) 中, 之后 O-IWU 在 SIP 侧将消息发送出去。

表32 O-IWU 的自行释放

REL ←	触发事件	→ SIP
原因指示语参数		
由 ISUP 程序确定	收到导通指示语参数为“导通检验失败”COT 消息, 或 ISUP T8 超时	根据 6.7.1 节描述的规则发送 CANCEL 或 BYE
REL 原因值 47 (资源不可用, 未指定)	内部资源预留不成功	由 SIP 程序确定
由 ISUP 程序确定	ISUP 程序导致 ISUP 侧产生自行 REL	根据 6.7.1 节描述的规则 CANCEL 或 BYE
取决于 SIP 释放原因	SIP 程序导致决定释放该呼叫	由 SIP 程序确定

6.7.4 RSC、GRS 或 CGB (ISUP) 的接收

表 33 给出了在 IWU 接收到 ISUP RSC 消息、GRS 消息或带有编码为“面向硬件故障”的电路群监视消息类型指示语的 CGB 消息后, O-IWU 所发送的消息。

当收到 GRS 或 CGB 时, 将为每一个相关的呼叫发送一个 SIP 消息, 因此, 收到单个 GRS 或 CGB 消息却可能发送多个 SIP 消息。

O-IWU 应当根据 6.7.1 节所描述的规则发送 CANCEL 或 BYE 消息。

依据本地策略, 带有 REL 的原因值 (Q.850) 的 Reason 头字段可加进 SIP 消息 (BYE 或 CANCEL) 中, 然后, O-IWU 在 SIP 侧将该消息发送出去。

在使用 ISUP 封装的情况下, RSC、GRS 或 CGB ISUP 消息不应封装在 SIP BYE 或 CANCEL 中。

表33 O-IWU 中 RSC、GRS 或 CGB 消息 (ISUP) 的接收

从 ISUP 接收到的消息 →	SIP →
复原电路消息 (RSC)	CANCEL 或 BYE
电路群复原消息 (GRS)	CANCEL 或 BYE
电路群闭塞消息 (CGB) 带有编码为“面向硬件故障”的电路群监视消息类型	CANCEL 或 BYE

6.7.5 INVITE 的响应 4XX、5XX、6XX 的接收

如果在 4XX、5XX、6XX 中包含有 Reason 头字段, 则 Reason 头字段的原因值应映射成 ISUP REL 中的 ISUP 原因值。Reason 头字段到原因指示语参数的映射见表 15 (5.12.1 节)。对于其他情况, 在 SIP 侧接收到对 INVITE 的 4XX、5XX 或 6XX 等最终响应后从状态码到原因码的映射在表 34 中描述。

对于 Profile C, 被封装的 REL 无需修改, 直接发送给 ISUP 程序。除此之外的其他情况, 应用本节

下面所描述的程序。

如果在 SIP 规范中或本章中规定了接收到特定 INVITE 响应后 SIP 侧的相应动作，则应优先遵从这些规定的程序，而不是立即向 ISUP 发送 REL 消息。

如果没有与该响应相对应的 SIP 侧程序，则应立即发送 REL。

注：在某些情况下，对 INVITE 的某些 4xx/5xx/6xx 响应的接收可能不会导致向 ISUP 网络发送 REL 消息，这取决于 O-IWU 中所采用的 SIP 侧程序。例如，如果接收到一个 401 Unauthorized 响应且 O-IWU 成功地发起了一个新的包含正确 credentials 的 INVITE，则呼叫将继续进行。

在表 34 中，如果在“备注”一栏没有给出特别说明，则意味着该 SIP 响应映射成一个 ISUP REL 消息从 O-IWU 的入局 ISUP 侧发送，其原因码如表中所示。如果给出了特别说明，则 O-IWU 的动作在所指定的章节中描述；如果该呼叫的 SIP 侧（为了尝试维持该呼叫）采用的进一步措施失败，从而导致通过发送一个带有表中所示原因码的 REL 来释放 ISUP 这半边的呼叫，对于这种情况，表中给出了 O-IWU 的“最终”动作。

如果 INVITE 的响应导致 O-IWU 发送原因值为 127 “互通”的 ISUP REL，则“位置”域 (Location) 应设成“互通点外的网络”。

表34 O-IWU 中 4XX、5XX 或 6XX 的接收

←REL (原因码)	←4XX/5XX/6XX SIP 消息	备注
127 互通	400 Bad Request	
127 互通	401 Unauthorised	注 1
127 互通	402 Payment Required	
127 互通	403 Forbidden	
1 未分配的号码	404 Not Found	
127 互通	405 Method Not Allowed	
127 互通	406 Not Acceptable	
127 互通	407 Proxy authentication required	注 1
127 互通	408 Request Timeout	
22 号码改变 (未诊断)	410 Gone	
127 互通	413 Request Entity too long	注 1
127 互通	414 Request-uri too long	注 1
127 互通	415 Unsupported Media type	注 1
127 互通	416 Unsupported URI scheme	注 1
127 互通	420 Bad Extension	注 1
127 互通	421 Extension required	注 1
127 互通	423 Interval Too Brief	
20 用户缺席	480 Temporarily Unavailable	
127 互通	481 Call/Transaction does not exist	
127 互通	482 Loop Detected	

表 34 (续)

←REL (原因码)	←4XX/5XX/6XX SIP 消息	备注
127 互通	483 Too many hops	
28 无效的号码格式	484 Address Incomplete	注 1
127 互通	485 Ambiguous	
17 用户忙	486 Busy Here	
127 互通, 或无映射 (注 3)	487 Request terminated	注 2
127 互通	488 Not acceptable here	
无映射	490 Request Updated	
无映射	491 Request Pending	注 2
127 互通	493 Undecipherable	
127 互通	500 Server Internal error	
127 互通	501 Not implemented	
127 互通	502 Bad Gateway	
127 互通	503 Service Unavailable	注 1
127 互通	504 Server timeout	
127 互通	505 Version not supported	注 1
127 互通	513 Message too large	注 1
127 互通	580 Precondition failure	注 1
17 用户忙	600 Busy Everywhere	
21 呼叫拒收	603 Decline	
1 未分配的号码	604 Does not exist anywhere	
127 互通	606 Not acceptable	
注 1: 该响应完全可以在 SIP 侧处理, 如果是这样, 就没有互通。		
注 2: 该响应并没有终结一个 SIP 对话, 而只是终结对话中的一个特定的事务。		
注 3: 如果 O-IWU 之前对 INVITE 发出 CANCEL 请求, 则没有映射		

6.7.5.1 484 Address Incomplete 响应的特别处理

接收到当前 INVITE (即该呼叫没有其他未决的 INVITE 事务) 的 484 Address Incomplete 响应后, 如果 O-IWU 配置成将重叠发送信令传播到 SIP 网络中, 则 O-IWU 不应立即发送 REL 消息, 而是启动定时器 T_{Oiw3} 。在 T_{Oiw3} 超时后, 再发送 REL 消息。如果 O-IWU 未配置成将重叠发送信令传播到 SIP 网络中, 则 O-IWU 不启动定时器, 且立即向 ISUP 网络发送 REL 消息。

6.7.5.2 接收到 INVITE 或 UPDATE 的响应: 580 Precondition failure 的特别处理

580 Precondition failure 响应可以作为对 INVITE 或 UPDATE 请求的响应。

6.7.5.2.1 580 Precondition failure 作为 INVITE 的响应

立即向 ISUP 网络发送释放消息, 其中带有表 34 所示的原因值。

6.7.5.2.2 580 Precondition Failure 作为一个早期对话中的 UPDATE 的响应

立即向 ISUP 网络发送释放,其中的原因值为“127 Interworking”,并向 UPDATE 所对应的那个 INVITE 事务发送 BYE 请求。

6.8 O-IWU 的定时器

表 35 定义了第 6 章所涉及的互通定时器。

表35 互通定时器

定时器名	超时值	启动原因	正常终止	超时后	参 考
T _{Oiw1}	4~6s(缺省值为 4s)	已接收到为该呼叫选路所需要的最少位数,但地址信令的结尾仍未确定,则在收到 IAM 或 SAM 之时启动	接收到新的地址信息	发送初始 INVITE, 返回 ACM。对于 Profile A 和 Profile B, 还应向主叫用户发送等待应答指示(如振铃音)或适当的进展提示音	6.1、6.4 节(注 1)
T _{Oiw2}	4~14s(缺省值为 4s)	发送 INVITE 消息,除非已经回送了 ACM	接收到 484 Address Incomplete 响应(对当前 INVITE)、180 Ringing、封装有 ACM 的 183 Session Progress 或 200 OK (INVITE) 响应时	发送 early ACM。对于 Profile A 和 Profile B, 还应向主叫用户发送等待应答指示(如振铃音)或适当的进展提示音	6.1、6.2.1、6.3.1、6.4、6.5 节(注 2)
T _{Oiw3}	4~6s(缺省值为 4s)	在该呼叫没有其他未决的 INVITE 事务的情况下,接收到关于当前 INVITE 的 484Address Incomplete 响应	接收到新的地址信息	向 ISUP 侧发送原因值为 28 的 REL	6.2.1、6.7.5.1 节(注 3)

注 1: 该定时器用于 ISUP 重叠发送到 SIP 成组发送的转换。
 注 2: 该定时器用于当没能及时接收到从后续的 SIP 网络中产生的响应时,从 O-IWU 发送 early ACM。
 注 3: 该定时器被称作“SIP 对话保护定时器”。该定时器仅用于 O-IWU 配置成将 ISUP 重叠发送信令传播到 SIP 网络中的情况

附录 A (规范性附录)

SIP 头字段 P-Asserted-Identity 扩展

A.1 适用性声明

本附录是对 SIP 的扩展，这些扩展使可信 SIP 服务器的网络能够声明端用户或端系统的标识，并发送端用户请求保密的指示。

这些扩展只适用于《网络声明标识短期要求》[5]中定义的“信任域”。在信任域内的节点公开地声明每一方的标识。当保密被请求时，这些节点将负责在信任域外部抑制标识。网络确定声明标识所采用的方式不属于本附录的范畴（虽然它通常需要某种形式的鉴权）。

[5]要求在一个给定的信任域“T”内，所有节点的行为要遵循一组规范，记为“Spec (T)”。“Spec (T)”必须规定：

- 1) 用户鉴权的方式；
- 2) 在信任域内，为保证节点之间通信所使用的机制；
- 3) 在信任域内，为保证 UAs 和节点之间通信所使用的机制；
- 4) 为决定哪些主机是信任域的一部分而使用的方式；
- 5) 默认的保密处理机制，如当没有 Privacy 头字段可用时；
- 6) 在信任域，节点要遵循 SIP[1]；
- 7) 如 A. 6 里所描述的标识的保密处理。

A.11 给出了一个 Spec (T) 的例子。

本附录不提供通用保密，也不提供适用于在不同的信任域之间或在互联网内使用的标识模型。它关于用户和网络之间的信任关系的假定可能不适用于很多应用。此外，既然这些声明的标识的鉴定并没有经过加密，他们常常会遭到伪造，重用，串改而不满足[5]的要求。

声明标识也没有指明究竟是谁对这个标识进行声明，所以必须假定是信任域在声明这个标识。因此，仅当这个标识信息是从信任域内的一个成员节点处安全地接收时，该信息才会有意义。

尽管有这些局限性，但还是有足够有用的专门的配置满足前面所描述的假定，且这些配置能接受这些局限性，从而保证这个机制的发布。一个配置的例子就是模拟传统电路交换电话网的闭合网络。

A.2 基本规则

本附录中对 proxy 服务器或 proxy 行为的要求同样适用于信任域中其他中间实体（如：B2BUA）。在[5]中定义了本附录的术语“标识”、“网络声明标识”和“信任域”。

A.3 介绍

在 IP 网络上提供电话业务的提供商需要在由他们自己运维的可信网络实体（如 SIP proxy 服务器）上交业务用户的标识，也可以在需要时对不可信的实体抑制该信息。这样的网络假定了提供商以及他们所运维的设备当中存在着某种级别的信任传递性。

这些网络需要支持特定的传统电话业务，满足基本管理和公共安全需求。这包括主叫标识递交业务，主叫标识递交闭塞和追查呼叫发起者的能力。虽然基本的 SIP 能够单独地支持每一个业务，但是如果没

有本附录中所描述的扩展，就不能支持特定的业务组合。例如，如果主叫不想公布个人信息，所以他只在 SIP From 头字段中供有限的信息，这些信息就不能被接收方所识别，除非接收方通过其他途径查到主叫的标识。在发起方 UA 中遮蔽标识信息就会影响到特定的业务，如呼叫追查，使之不能在 PSTN 网内运行，或不能在对用户的鉴权标识不知情的中间实体上运行。

在 SIP 网络中提供保密机制比在 PSTN 网络中提供更为复杂。在 SIP 网络中，一个会话的参与者无需 SIP 业务提供商的参与就能够直接交换 IP 业务量，会话所用的 IP 地址本身就暴露了个人私密信息。在[2]中讨论了关于在 SIP 环境下提供保密的通用用途机制。本附录对网络声明标识问题采用了这种保密机制。

A.4 概述

本附录所提出的机制与一个新的头字段有关，这个头字段是“P-Asserted-Identity”。它包含一个 URI（通常是一个 SIP URI）和一个任选的 display-name。例如：

P-Asserted-Identity: “Cullen Jennings” <sip:fluffy@cisco.com>

处理消息的 Proxy 服务器通过某些途径，例如，整理鉴权（Digest authentication），对发起方用户进行鉴权之后，能够将 P-Asserted-Identity 头字段插入到消息内，并将消息前转到其他可信的 proxy。如果用户请求了保密，则 Proxy 在把消息前转给它不信任的 proxy 服务器或 UA 之前，删除所有的 P-Asserted-Identity 头字段的值。用户可以请求这类保密，见 A.7 节

P-Asserted-Identity 头字段的语法见 A.9 节。

A.5 Proxy行为

在信任域内的 proxy 可以接收来自它所信任或不信任的节点发来的消息。如果 proxy 收到来自它不信任的节点发来的消息，而且它希望在消息中加入 P-Asserted-Identity 头字段，这个 proxy 必须对消息的发起者进行鉴权，利用鉴权产生的标识将 P-Asserted-Identity 头字段插入到消息内。

如果这个 proxy 收到来自它信任的节点发来的消息（请求或者响应），它可以使用 P-Asserted-Identity 头字段所携带的信息（如果有的话），就如同它自己已经对该用户进行过鉴权一样。

如果没有 P-Asserted-Identity 头字段可用，proxy 可以增加该头字段。该头字段至多包含一个 SIP 或 SIPs URI，和至多一个 tel URL。如果这个 proxy 收到它不信任的元件发来的消息，且有一个 P-Asserted-Identity 头字段，该头字段包含一个 SIP 或 SIPs URI，则这个 proxy 必须用一个 SIP 或 SIPs URI 取代原来的那个 SIP 或 SIPs URI，或者将它删除。类似地，如果这个 proxy 收到它不信任的元件发来的消息，且有一个 P-Asserted-Identity 头字段。该头字段包含一个 tel URI，这个 proxy 必须用一个 tel URI 取代原来的 tel URI，或者将它删除。

当一个 proxy 把消息前转给另一个节点时，它必须首先判断是否信任这个节点。如果它信任这个节点，这个 proxy 不会删除任何一个它自己产生的，或是从一个可信的源端接收到的 P-Asserted-Identity 头字段；如果它不信任这个节点，proxy 必须检查 Privacy 头字段（如果有），由此判断用户是否请求对声明标识进行保密。

A.6 多标识提示

如果 Proxy 收到来自它不信任的实体发来的消息，且该消息给出了 P-Preferred-Identity 头字段，proxy

会将该头字段所携带的信息作为一种提示，表示建议对已鉴权用户的多个有效标识中的哪些标识进行声明。如果这个提示并未对应于任何一个 proxy 所认识的该用户的标识，proxy 可以添加一个由它自己构造的 P-Asserted-Identity 头字段，或者拒绝该请求（如，使用 403 禁止）。proxy 必须从它要前转的任何一则消息中删除用户提供的 P-Preferred-Identity 头字段。

UA 只向信任域内的 proxy 服务器发送 P-Preferred-Identity 头字段，不向它不信任的 proxy 发送添加了 P-Preferred-Identity 头字段的消息。若 UA 要向信任域之外的节点发送含有 P-Preferred-Identity 的消息，网络可能不会适当地管理被提示的标识，这可能会对保密带来负面的结果。

A.7 请求保密

如果呼叫方希望在 P-Asserted-Identity 被传送给一个不信任的节点之前请求删除 P-Asserted-Identity，则呼叫方可以在 Privacy 头字段中增加“id”保密令牌。在[6]中定义了 Privacy 头字段。如果给出了这个令牌，proxy 必须在将消息前转给不信任的节点之前删除所有的 P-Asserted-Identity 头字段。如果 Privacy 头字段的值设成“none”，则 proxy 不能删除 P-Asserted-Identity。

如果 proxy 正在把请求前转给不信任的节点，且前转的消息中没有含有 Privacy 头字段，那么 proxy 可以在消息中包含 P-Asserted-Identity 头字段或者将其删除。这个决定是信任域的一个策略问题，必须在 Spec (T) 中规定。建议不删除 P-Asserted-Identity 头字段除非本地保密策略要求删除该头字段，因为删除会造成一些基于 Asserted Identity 业务的失败。

然而，需要注意的是，如果所有的信任域内的用户没有使用适当的保密业务的能力，那么将 P-Asserted-Identity 前转可能会造成信息的泄漏，这一点用户并没有请求也没有能力去阻止。所以，强烈建议所有的用户都能够使用本附录所描述的保密业务。

“id”是 Privacy 头字段的成分 priv-value 的值，对它的正式定义见 A.9.3 节的描述。有关用户应该何时请求保密的基本指导准则会在[2]中给出。

如果在一则消息中给出了多个 P-Asserted-Identity 头字段，而且请求了对 P-Asserted-Identity 头字段的保密，则所有的头字段值的实例必须在把请求前转给不信任的实体之前删除。

A.8 UA服务器行为

通常，UA 将它所收到的 P-Asserted-Identity 头字段的值呈递给它的用户。它认为信任域提供的标识比请求中的 From 头字段更值得信任。本附录没有要求任何 UA 处理恰好在一则消息中出现多个 P-Asserted-Identity 头字段的值，如 SIP URI 与 tel URL 一同出现的情况。

然而，如果 UA 服务器接收到来自它不信任的节点发来的消息，它无论如何都不能使用消息中的 P-Asserted-Identity。

如果 UA 是信任域的一部分，并且从信任域接收到含有 P-Asserted-Identity 头字段的消息，那它可以随意地使用该值。但是它必须确保不会将这个信息前转给信任域之外的任何一个实体。

如果 UA 不是信任域的一部分，但从信任域接收到含有 P-Asserted-Identity 头字段的消息，那它可以假定该信息并不需要保密。

A.9 正式语法

以下的语法规则按照 RFC 2234 [4]中描述的 Backus-Naur Form (BNF)。

A.9.1 P-Asserted-Identity 头字段

P-Asserted-Identity 头字段使用于可信的 SIP 实体之间（通常是中间实体），用于携带发送 SIP 消息的用户的标识，且该用户是通过鉴权机制认证的。

PAssertedID = "P-Asserted-Identity" HCOLON PAssertedID-value
* (COMMA PAssertedID-value)

PAssertedID-value = name-addr / addr-spec

P-Asserted-Identity 头字段的值必须确切地包含一个 name-addr 或 addr-spec。可能有一个或两个 P-Asserted-Identity 值。如果有一个值，那它必须是 sip, sips URI 或 tel URI；如果有两个值，那其中一个必须是 sip 或 sips URI，另外一个必须是 tel URI。

本附录将在[1]的表 2 中增加以下条目。

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG	SUB	NOT	REF	INF	UPD	PRA
P-Asserted-Identity		adr	-	0	-	0	0	-	0	0	0	-	-	-

A.9.2 P-Preferred-Identity 头字段

P-Preferred-Identity 头字段用于在 UA 和可信的 proxy 之间携带发送 SIP 消息的用户的标识。可信实体会把它作为 P-Asserted-Identity 插入到消息中。

PPreferredID = "P-Preferred-Identity" HCOLON PPreferredID-value
* (COMMA PPreferredID -value)

PPreferredID-value = name-addr / addr-spec

P-Preferred-Identity 头字段的值必须确切地包含一个 name-addr 或 addr-spec。可能有一个或两个 P-Preferred-Identity 值。如果有一个值，那它必须是 sip、sips URI 或 tel URI；如果有两个值，那其中一个必须是 sip 或 sips URI，另外一个必须是 tel URI。

本附录将在[1]的表 2 中增加以下条目：

Header field	where	proxy	ACK	BYE	CAN	INV	OPT	REG	SUB	NOT	REF	INF	UPD	PRA
P-Preferred-Identity		adr	-	0	-	0	0	-	0	0	0	-	-	-

A.9.3 “id” 保密类型

本附录为 Privacy 头字段增加一个新的保密类型 (“priv-value”)。Privacy 头字段中的这个保密类型表示已在信任域内鉴权的用户希望网络声明标识对信任域外的 SIP 实体有所保密。如果用户请求多个保密类型，则在 Privacy 头字段的值中必须包含所有的请求的保密类型。

```
priv-value = "id"
```

例如：

```
Privacy: id
```

A.10 范例

A.10.1 将网络声明标识传递给可信网关

在本例中，proxy.cisco.com 利用从 SIP Digest 鉴权机制中发现的标识创建一个 P-Asserted-Identity 头字段。它把这个信息前转给一个可信的 proxy，后者再将信息前转给可信的网关。需要说明的是，这里给出的例子只包含部分 SIP 消息，旨在说明那些与鉴权标识问题相关的头字段。

```
* F1  useragent.cisco.com -> proxy.cisco.com
```

```
INVITE sip:+14085551212@cisco.com SIP/2.0
```

```
Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-123
```

```
To: <sip:+14085551212@cisco.com>
```

```
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
```

```
Call-ID: 245780247857024504
```

```
CSeq: 1 INVITE
```

```
Max-Forwards: 70
```

```
Privacy: id
```

```
* F2  proxy.cisco.com -> useragent.cisco.com
```

```
SIP/2.0 407 Proxy Authorization
```

```
Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-123
```

```
To: <sip:+14085551212@cisco.com>;tag=123456
```

```
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
```

```
Call-ID: 245780247857024504
```

```
CSeq: 1 INVITE
```

```
Proxy-Authenticate: .... realm="sip.cisco.com"
```

```
* F3  useragent.cisco.com -> proxy.cisco.com
```


YD/T 1522.3-2006

INVITE sip:+14085551212@cisco.com SIP/2.0
Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-124
To: <sip:+14085551212@cisco.com>
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
Call-ID: 245780247857024504
CSeq: 2 INVITE
Max-Forwards: 70
Privacy: id
Proxy-Authorization: realm="sip.cisco.com" user="fluffy"

* F4 proxy.cisco.com -> proxy.pstn.net (trusted)

INVITE sip:+14085551212@proxy.pstn.net SIP/2.0
Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-124
Via: SIP/2.0/TCP proxy.cisco.com;branch=z9hG4bK-abc
To: <sip:+14085551212@cisco.com>
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
Call-ID: 245780247857024504
CSeq: 2 INVITE
Max-Forwards: 69
P-Asserted-Identity: "Cullen Jennings" <sip:fluffy@cisco.com>
P-Asserted-Identity: tel:+14085264000
Privacy: id

* F5 proxy.pstn.net -> gw.pstn.net (trusted)

INVITE sip:+14085551212@gw.pstn.net SIP/2.0
Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-124
Via: SIP/2.0/TCP proxy.cisco.com;branch=z9hG4bK-abc
Via: SIP/2.0/TCP proxy.pstn.net;branch=z9hG4bK-a1b2
To: <sip:+14085551212@cisco.com>
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
Call-ID: 245780247857024504
CSeq: 2 INVITE
Max-Forwards: 68
P-Asserted-Identity: "Cullen Jennings" <sip:fluffy@cisco.com>
P-Asserted-Identity: tel:+14085264000

Privacy: id

A.10.2 网络声明标识抑制

在本例中，UA 向第一个 proxy 发送 INVITE 消息。在 INVITE 中指明了它首选的标识 sip:fluffy@cisco.om。proxy 通过 SIP Digest 对标识进行了鉴权。这个 proxy 创建了 P-Asserted-Identity 头字段，并把它前转给可信 proxy(outbound.cisco.com)。第二个 proxy 再把请求前转给它不信任的 biloxi.com 的 proxy，并在前转之前删除了 P-Asserted-Identity 头字段。

* F1 useragent.cisco.com -> proxy.cisco.com

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a111
To: <sip:bob@biloxi.com>
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
Call-ID: 245780247857024504
CSeq: 1 INVITE
Max-Forwards: 70
Privacy: id
P-Preferred-Identity: "Cullen Jennings" <sip:fluffy@cisco.com>
```

* F2 proxy.cisco.com -> useragent.cisco.com

```
SIP/2.0 407 Proxy Authorization
Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a111
To: <sip:bob@biloxi.com>;tag=123456
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
Call-ID: 245780247857024504
CSeq: 1 INVITE
Proxy-Authenticate: .... realm="cisco.com"
```

* F3 useragent.cisco.com -> proxy.cisco.com

```
INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a123
To: <sip:bob@biloxi.com>
From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
Call-ID: 245780247857024504
CSeq: 2 INVITE
Max-Forwards: 70
```

YD/T 1522.3-2006

Privacy: id

P-Preferred-Identity: "Cullen Jennings" <sip:fluffy@cisco.com>

Proxy-Authorization: realm="cisco.com" user="fluffy"

* F4 proxy.cisco.com -> outbound.cisco.com (trusted)

INVITE sip:bob@biloxi SIP/2.0

Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a123

Via: SIP/2.0/TCP proxy.cisco.com;branch=z9hG4bK-b234

To: <sip:bob@biloxi.com>

From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748

Call-ID: 245780247857024504

CSeq: 2 INVITE

Max-Forwards: 69

P-Asserted-Identity: "Cullen Jennings" <sip:fluffy@vovida.org>

Privacy: id

* F5 outbound.cisco.com -> proxy.biloxi.com (not trusted)

INVITE sip:bob@biloxi SIP/2.0

Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a123

Via: SIP/2.0/TCP proxy.cisco.com;branch=z9hG4bK-b234

Via: SIP/2.0/TCP outbound.cisco.com;branch=z9hG4bK-c345

To: <sip:bob@biloxi.com>

From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748

Call-ID: 245780247857024504

CSeq: 2 INVITE

Max-Forwards: 68

Privacy: id

* F6 proxy.biloxi.com -> bobster.biloxi.com

INVITE sip:bob@bobster.biloxi.com SIP/2.0

Via: SIP/2.0/TCP useragent.cisco.com;branch=z9hG4bK-a123

Via: SIP/2.0/TCP proxy.cisco.com;branch=z9hG4bK-b234

Via: SIP/2.0/TCP outbound.cisco.com;branch=z9hG4bK-c345

Via: SIP/2.0/TCP proxy.biloxi.com;branch=z9hG4bK-d456

To: <sip:bob@biloxi.com>
 From: "Anonymous" <sip:anonymous@anonymous.invalid>;tag=9802748
 Call-ID: 245780247857024504
 CSeq: 2 INVITE
 Max-Forwards: 67
 Privacy: id

A.11 Spec (T) 的范例

本附录中描述的机制的完整性依赖于一个节点，该节点（通过配置）知道信任域中的所有节点将工作在预先确定的方式下。预先确定的行为需要被清楚地定义，并且要求信任域内的所有节点都要遵守。信任域内所有的节点必须遵守的规范集被称为“Spec (T)”。

本附录剩余的部分给出了 Spec (T) 的例子，但它不是规范性的。

A.11.1 协议要求

必须支持下列规范：

- 1) SIP[1]
- 2) 本部分。

A.11.2 鉴权要求

用户必须通过使用 SIP Digest 鉴权机制鉴权。

A.11.3 安全要求

在信任域内，节点与节点之间、节点与 UAs 之间的连接必须使用 TLS。TLS 使用的是 RSA_WITH_AES_128_CBC_SHA1 的密码序列。信任域内的节点必须相互鉴权，机密性必须商议。

A.11.4 信任域的范围

本附录所规范的信任域由拥有有效证书的主机组成。该证书是：

- 1) 由 `examplerootca.org` 签发的；
- 2) 证书的 `subjectAltName` 以下列的一个域名结尾：

`trusted.div1.carrier-a.net,`

`trusted.div2.carrier-a.net,`

`sip.carrier-b.com;`

且

- 3) 证书的域名对应于 `subjectAltName` 的主机名。

A.11.5 当无 Privacy 头字段时的隐性处理

信任域的实体必须支持“id”保密业务。因此，当没有 Privacy 头字段时，就假定用户并没有请求保密。如果在一个请求中没有 Privacy 头字段，信任域中实体的工作方式同没有保密请求时一样。

A.12 安全考虑

本附录中提到的机制只是对 SIP 中关于标识和保密的问题给予考虑。例如，终端用户可以通过某种途径在没有可信的业务提供商的情况下，端到端安全地共享标识信息，但是这些机制并没提供这样的途径。被用户标明成“保密”(privacy)的标识信息能够被信任域中任何处于中间的参与者检查。这些信息

通过信任传递性保证安全。但是这种信任传递性的可靠度与这条信任链中的最薄弱的链路相同。

当可信的实体向任何一个目的地发送一则带有 P-Asserted-Identity 头字段中带有用户标识的消息时，该实体必须注意保护标识信息免于遭到窃听和拦截，以保证该标识信息的机密性和完整性。通过使用传输层或网络层的 hop-by-hop 安全机制，如 TLS 或带有适当密码序列的 IPSec，能够满足这个需求。

A.13 IANA考虑

A.13.1 新 SIP 头字段的注册

本附录定义了两个新的私有 SIP 头字段：P-Asserted-Identity 和 P-Preferred-Identity。正如传输领域的策略所推荐的那样，这些头字段应当通过 IANA 在 SIP 头字段注册处注册，并使用本附录中的 RFC 编号作为它的参考引用。

Name of Header:	P-Asserted-Identity
Short form:	none
Registrant:	Cullen Jennings fluffy@cisco.com
规范性描述:	附录 A.9.1

Name of Header:	P-Preferred-Identity
Short form:	none
Registrant:	Cullen Jennings fluffy@cisco.com
规范性描述:	附录 A.9.2

A.13.2 SIP Privacy 头字段的“id”保密类型的注册

Name of privacy type:	id
Short Description:	Privacy requested for Third-Party Asserted Identity
Registrant:	Cullen Jennings fluffy@cisco.com
规范性描述:	附录 A.9.3

规范性参考文献

[1] Rosenberg, J. and H. Schulzrinne, "SIP: Session Initiation Protocol", draft-ietf-sip-rfc2543bis-09 (work in progress), February 2002. Now published as RFC 3261.

[2] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", draft-ietf-sip-privacy-general-00 (work in progress), May 2002. Now published as RFC 3323, November 2002..

[3] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[4] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", RFC 2234, November 1997.

资料性参考文献

[5] Watson, M., "Short term requirements for Network Asserted Identity", draft-ietf-sipping-nai-reqs-01 (work in progress) , May 2002.

[6] Andreasen, F., "SIP Extensions for Network-Asserted Caller Identity and Privacy within Trusted Networks", draft-ietf-sip-privacy-04 (work in progress) , March 2002.

[7] Peterson, J., "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP) ", draft-peterson-sip-identity-00 (work in progress) , April 2002.

附 录 B
(资料性附录)
ISUP 补充业务的互通

附录 B 系列描述了 ISUP 补充业务与 SIP 之间的互通。

Profile C 使用封装的参数，不需要互通，除非有特别的说明。因此本附录所述内容仅适用与 Profile A 和 Profile B。

B.1 CLIP/CLIR 补充业务和 SIP 的互通

CLIP/CLIR 业务只在信任节点之间互通。也就是说，在任何 CLIP/CLIR 信息被传送出 SIP /ISUP 边界时，IWU 必须保证信息所要发往的节点是可信的。

在 CLIP/CLIR 业务中，主叫用户号码与 P-Asserted-Identity 头字段之间的映射见 5.2.3.6 和 6.1.3 节。该映射与基本呼叫类似。不同点仅在于当 CLIR 业务被调用时，地址提供限制指示语 (APRI) (对于 ISUP 到 SIP 的呼叫) 或 Privacy 头字段中的 priv-value (对于 SIP 到 ISUP 的呼叫) 会被设成适当的“限制/保密”。

对于特定的 ISUP 侧发起的呼叫，使用 CLIP 业务还需要一种能力，用于确定号码是否是网络提供或者是由接入信令系统提供。由于 P-Asserted-Identity 的 SIP 指示语的缘故，ISUP 的过滤指示语默认设成“网络提供”。

在 O-IWU 内，“限制提供”指示应被映射成 Privacy 头字段的带有“id”或“header”值的 priv-value 成分。

对于 Profile C：

在 O-IWU 处：封装应当支持该业务。

在 I-IWU 处：如果主叫用户号码参数在应用 5.2.3.6 节描述的互通规则和 ISUP 程序之后得到的地址与被封装的 ISUP 消息中所带有的值相等，就无需作进一步的互通，直接使用封装的信息就可以了。对于相反的情况，则采用和 5.2.3.6 节中与 Profile A 和 Profile B 相同的方式处理。

B.2 呼叫保持补充业务与 SIP 的互通

对于 Profile A 和 Profile B：

呼叫保持是 ISUP 的一个补充业务。

在呼叫被应答之后，或在下面的情况下（作为业务提供商选项）的任何时刻，主叫用户都可将呼叫置成保持状态：

- 1) 振铃开始之后，或
- 2) 在主叫用户已经提供了足够进行呼叫的所有信息之后。

在呼叫被应答之后或在呼叫拆线开始之前的任何时刻，被叫用户都可将呼叫置成保持状态。

在呼叫保持补充业务中，CPG 消息中的通用通知指示语参数用来向远端发送适当的通知。

下面的通知描述会被使用：

- “远端保持”
- “远端恢复”

事件指示语置成“进展”。

在 SIP 网络中也存在同样的业务。如果呼叫中的一方想要另一方处于呼叫保持的状态，也就是说，它临时性地停止发送一个或多个 unicast 媒体流，那么呼叫的这一方就会向另一方提供更新的 SDP。被置成保持的流会被注上下列属性：

“a=sendonly”——如果之前的媒体流是“sendrecv”媒体流；

“a=inactive”——如果之前的媒体流为“recvonly”媒体流。

如果一方想恢复呼叫，被恢复的流会被注上下列属性：

“a=sendrecv”——如果之前的媒体流是“sendonly”媒体流。既然缺省时属性为 sendrecv，所以此处或者缺省。

“a=recvonly”——如果之前的媒体流是“inactive”媒体流。

表 B.1 给出了 ISUP 和 SIP 之间关于呼叫保持补充业务的映射。

表 B.1 ISUP 和 SIP 之间关于呼叫保持补充业务的映射

呼叫状态	ISUP 消息	映射	SIP 消息
应答	CPG “远端保持”	↔	INVITE 消息，给出的媒体流的属性行“a=sendonly”或“a=inactive”（见上文）
应答	CPG “远端恢复”	↔	INVITE 消息，给出的媒体流的属性行“a=sendrecv”，或省略属性行，或“a=recvonly”（见上文）
在应答之前	CPG “远端保持”	↔（注）	UPDATE 消息，给出的媒体流的属性行“a=sendonly”或“a=inactive”（见上文）
在应答之前	CPG “远端恢复”	↔（注）	UPDATE 消息，给出的媒体流的属性行“a=sendrecv”，或省略属性行，或“a=recvonly”（见上文）
映射： ↔：表示双向映射，如 ISUP 到 SIP 或 SIP 到 ISUP。 ⇒：仅表示从 ISUP 映射到 SIP。 注：对于“在应答之前”的情况，映射只用于表示主叫用户向被叫用户发出呼叫保持的请求，因为被叫用户无法在应答之前使主叫用户处于保持状态			

对于 Profile C：

互通得通过封装的 CPG 消息。

表 B.2 给出了 ISUP 和 SIP-I 关于呼叫保持补充业务的映射。

表 B.2 ISUP 和 SIP-I 关于呼叫保持补充业务的映射

呼叫状态	ISUP 消息	映射	SIP 消息
应答	CPG “远端保持” 从 SIP 消息体中解封出来的 CPG 带有“远端保持”信息	⇒	INVITE 消息，给出的媒体流的属性行“a=sendonly”或“a=inactive”（见上文），并封装 ISUP CPG 消息
		⇐	
应答	CPG “远端恢复” 从 SIP 消息体中解封出来的 CPG 带有“远端恢复”信息	⇒	INVITE 消息，给出的媒体流的属性行“a=sendrecv”，或省略属性行，或“a=recvonly”（见上文），并封装 ISUP CPG 消息
		⇐	
在应答之前	CPG “远端保持” 从 SIP 消息体中解封出来的 CPG 带有“远端保持”信息	⇒（注） ⇐	UPDATE 消息，给出的媒体流的属性行为“a=sendonly”或“a=inactive”（见上文），并封装 ISUP CPG 消息

表 B.2 (续)

呼叫状态	ISUP 消息	映射	SIP 消息
在应答之前	CPG “远端恢复” 从 SIP 消息体中解封出来的 CPG 带有 “远端恢复” 信息	⇒ (注) ⇐	UPDATE 消息, 给出的媒体流的属性行为 “a=sendrecv”, 或省略属性行, 或 “a=recvonly” (见上文), 并封装 ISUP CPG 消息
<p>映射:</p> <p>⇒: 表示 ISUP 到 SIP 的映射。</p> <p>⇐: 表示 SIP 到 ISUP 的映射。</p> <p>注: 对于 “在应答之前” 的情况, 映射只用于表示主叫用户向被叫用户发出呼叫保持的请求, 因为被叫用户无法在应答之前使主叫用户处于保持状态</p>			

附 录 C
(资料性附录)
SIP/SIP-I 信令的 Profile

参考依据	Profile A	Profile B	Profile C
RFC 2046 多用途因特网邮件扩展 (MIME) 第 2 部分: 媒体类型	支持	支持	支持
RFC 2327 SDP: Session Description Protocol	支持	支持	支持
RFC 2806 URLs for Telephone Calls	支持	支持	支持
RFC 2976 会话初始协议的 INFO 方法	不支持	不支持	支持
RFC 3204 ISUP 和 QSIG 对象的 MIME 媒体类型	不支持	不支持	支持
RFC 3261 SIP:会话初始协议	支持	支持	支持
RFC 3262 会话初始协议 (SIP) 中临时响应的可靠性	支持	任选	任选
RFC 3264 使用会话描述协议 (SDP) 的 Offer/ Answer 模型	支持	支持	支持
RFC 3311 会话初始协议的 UPDATE 方法	支持	支持	支持
RFC 3312 资源管理的综合和会话初始协议 (SIP)	支持	任选	任选
RFC 3323 会话初始协议 (SIP) 的私密机制	支持	支持	支持
RFC 3325 关于在信任网络内声明标识的 SIP 私有扩展 (注)	支持	支持	支持
RFC 3326 会话初始协议 (SIP) 的 Reason 头字段	支持	支持	支持
注: 附录 A 可以替代 RFC 3325 成为正式标准			