目录

[SIP协议 2](#_Toc363475137)

[1. 简介 2](#_Toc363475138)

[2. SIP组件 2](#_Toc363475139)

[2.1. User Agent 2](#_Toc363475140)

[2.2. Proxy Server 2](#_Toc363475141)

[2.3. Redirect Server 2](#_Toc363475142)

[2.4. Registrar Server 3](#_Toc363475143)

[2.5. Location Server 3](#_Toc363475144)

[2.6. Back-to-back user agent (B2BUA) 3](#_Toc363475145)

[2.7. Presence Server 3](#_Toc363475146)

[3. SIP 消息（方法） 3](#_Toc363475147)

[3.1. REGISTER 注册 3](#_Toc363475148)

[3.2. INVITE 发起 3](#_Toc363475149)

[3.3. ACK 回复 3](#_Toc363475150)

[3.4. CANCEL 取消 3](#_Toc363475151)

[3.5. OPTIONS 选项 4](#_Toc363475152)

[3.6. BYE 中断 4](#_Toc363475153)

[3.7. INFO 消息 4](#_Toc363475154)

[3.8. PRACK 4](#_Toc363475155)

[3.9. REFER 4](#_Toc363475156)

[3.10. SUBSCRIBE 4](#_Toc363475157)

[3.11. NOTIFY 4](#_Toc363475158)

[3.12. UPDATE 4](#_Toc363475159)

[4. SIP 应答 5](#_Toc363475160)

[5. SIP 消息例子 7](#_Toc363475161)

[6. SDP 7](#_Toc363475162)

[7. 典型流程 8](#_Toc363475163)

[7.1. 注册流程 8](#_Toc363475164)

[7.2. 注销流程 9](#_Toc363475165)

[7.3. 基本呼叫流程 9](#_Toc363475166)

[7.4. 会话更改流程 10](#_Toc363475167)

[7.5. 正常呼叫结束流程 11](#_Toc363475168)

[7.6. 被叫忙呼叫结束流程 11](#_Toc363475169)

[7.7. 被叫无应答流程一 12](#_Toc363475170)

[7.8. 被叫无应答流程二 13](#_Toc363475171)

[7.9. 遇忙呼叫前转流程 14](#_Toc363475172)

[7.10. 无应答呼叫前转流程 15](#_Toc363475173)

[7.11. 呼叫保持 16](#_Toc363475174)

[7.12. 呼叫等待 18](#_Toc363475175)

[8. 优点及缺点 19](#_Toc363475176)

[8.1. 优点 19](#_Toc363475177)

[8.2. 缺点 19](#_Toc363475178)

# SIP协议

## 简介

* SIP默认使用UDP 5060端口，但也可以使用TCP 5060。
* SIP使用Server-Client模型。
* SIP的四项基本功能：

定位用户，将SIP地址解析为IP地址；

协商Session feature和capability；

在进行呼叫时改变会话参数；负责会话的建立和中断。

* SIP地址形式：sip:1112223344@mycompany.com或sip:1112223344@10.1.1.1 presence概念。用户可为自己设置offline、busy等状态。

## SIP组件

### User Agent

UA是SIP的基本组件，可分为UAC（User Agent Client）和UAS（User Agent Server）。发起呼叫的为UAC，接收呼叫的为UAS。很多设备都可做UA，如IP电话、PC、路由器等。

### Proxy Server

Proxy server起到call routing、authentication、authorization、address resolution、loop detection的功能。

UAC发起呼叫时会先把call setup message发给proxy server，如果proxy server知道UAS的位置，会把call setup message转发给UAS（或者是next hop），否则会找其他的server查询。UAS接收到call setup message后会给proxy server响应，proxy server再把这个响应返回给UAC。当呼叫建立之后，proxy server有2种选择：第一、呼叫建立之后还处于UAC和UAS之间的signaling path之间（Record-Route），以监视call change message或call termination message。第二、退出UAC和UAS之间的signaling path，不再参与会话。

### Redirect Server

UA、Proxy Server可不与Redirect Server通讯，以查找另一个endpoint的位置。这在一个移动网络内尤其有用，Redirect Server可以通知其clients，某一用户是否临时或永久的移动到另一位置。甚至可以通知某一用户移动到了多个位置（例如一个用户同时拥有多部IP电话），如此一来，当其他UAC呼叫这样的UAS时，proxy server会先拦住这样的会话，之后让UAS的多部电话同时振铃或依次振铃，这就是“find me”或“follow me”功能。

### Registrar Server

UA可以向Registrar Server注册自己的位置信息，Registrar Server将位置信息保存在数据库中。

### Location Server

负责维护Location Database。

### Back-to-back user agent (B2BUA)

B2BUA同时扮演UAC和UAS的角色。calling UA发起呼叫至B2BUA，此时B2BUA扮演UAS角色，之后B2BUA在以UAC的角色呼叫called UA。这样做的好处是，B2BUA有更细的控制粒度，甚至是改变呼叫请求的内容。

### Presence Server

负责维护presence信息，并发送status notification。

## SIP 消息（方法）

### REGISTER 注册

UA client使用此message向server注册以标明自己的位置。

### INVITE 发起

UAC发送这个信息用以邀请UAS加入会话（包括一对一通话或conference），其实就是一个call setup message。

### ACK 回复

为INVITE回复一个确认信息。

### CANCEL 取消

用来中止一个还没建立（在建立过程当中）的呼叫。

### OPTIONS 选项

用来查询server的capability。

### BYE 中断

用来中断呼叫。

### INFO 消息

当message body中包含数据时，使用INFO message。

### PRACK

用于回复一个临时性的请求。

### REFER

使用这个REFER指向另一个电话，从而完成call transfer。

### SUBSCRIBE

告诉server一旦发生特定事件时，愿意接收一个通知。

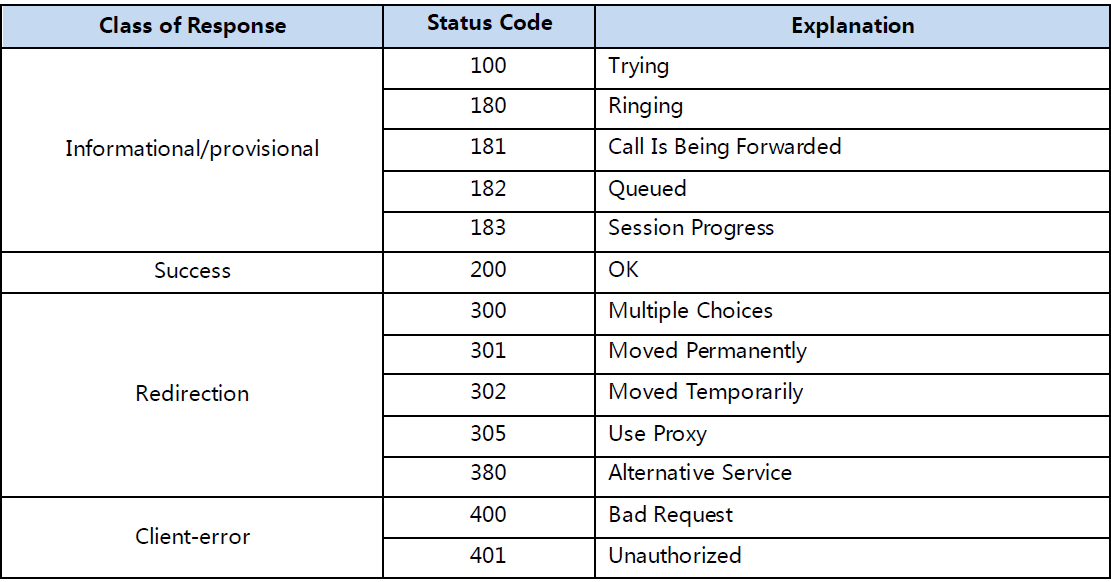
### NOTIFY

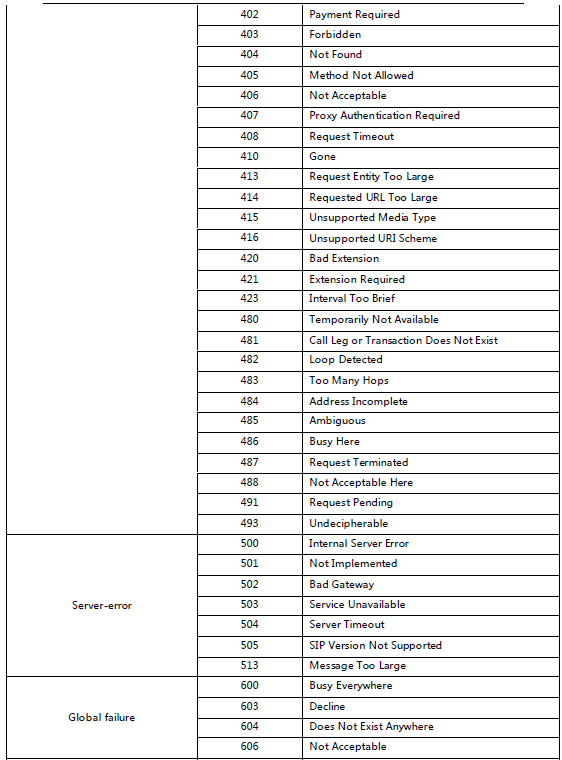
用来通知subscriber发生了特定的事件，也可用于传送DTMF。

### UPDATE

在接到初始INVITE的回复时，UAC用UPDATE修改一个呼叫的参数，例如QoS等。

## SIP 应答



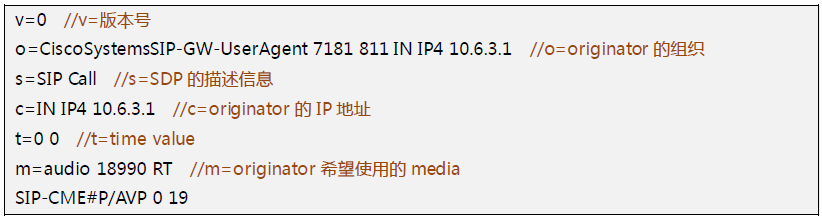


## SIP 消息例子



## SDP

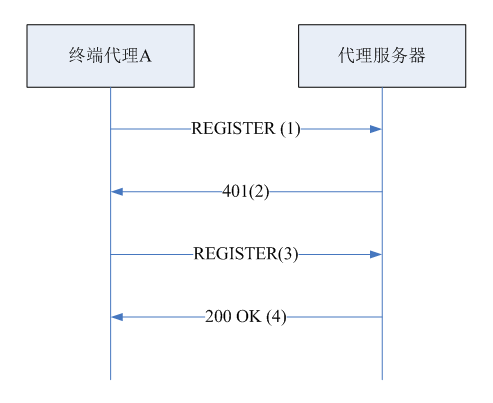
SIP使用SDP（Session Description Protocol）来协商capability和call feature。





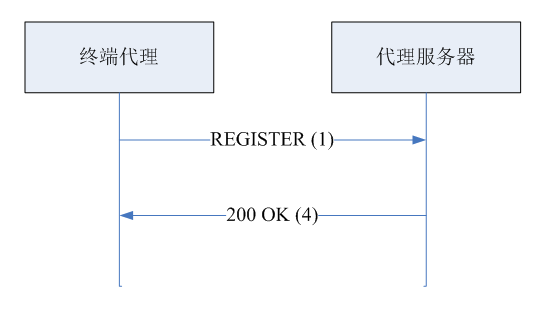
## 典型流程

### 注册流程



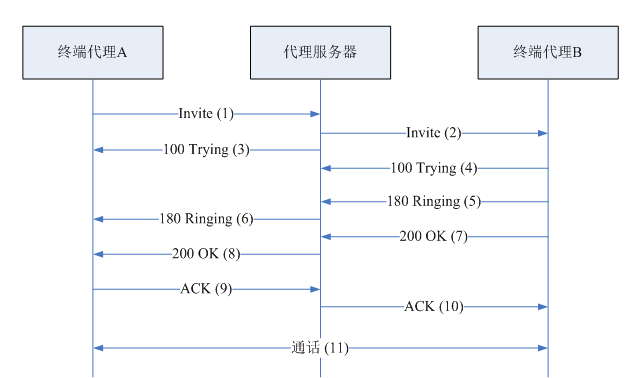
1. 用户首次试呼时，终端代理A向代理服务器发送REGISTER注册请求；
2. 代理服务器通过后端认证/计费中心获知用户信息不在数据库中，便向终端代理回送401 Unauthorized 质询信息，其中包含安全认证所需的令牌；
3. 终端代理提示用户输入其标识和密码后，根据安全认证令牌将其加密后，再次用REGISTER消息报告给代理服务器；
4. 代理服务器将REGISTER消息中的用户信息解密，通过认证/计费中心验证合法后，将该用户信息登记到数据库中，并向终端代理A返回成功相应消息200 OK。

### 注销流程



1. 终端向代理服务器发送REGISTER消息注销，其头中的expire字段置0；
2. 代理服务器收到后回送200 OK响应，并将数据库中的用户有关信息注销。

### 基本呼叫流程

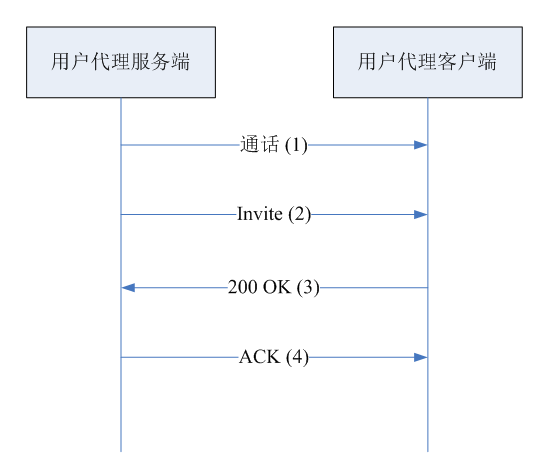


1. 用户摘机发起一路呼叫，终端代理A向该区域的代理服务器发起INVITE请求；
2. 代理服务器通过认证/计费中心确认用户认证已通过后，检查请求消息中的VIA头域中是否包含其地址：

* 若已包含，说明发生环回，返回指示错误的应答；
* 如果没有问题，代理服务器在请求消息的VIA头域中插入自身地址，并向INVITE消息的TO域所指示的被叫终端代理B转送INVITE请求；

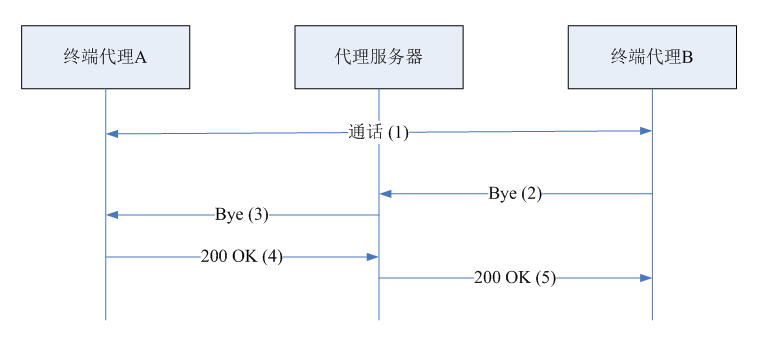
1. 代理服务器向终端代理A送呼叫处理中的应答消息，100 TRYING；
2. 终端代理B向代理服务器送呼叫处理中的应答消息，100 TRYING；
3. 终端代理B只是被叫用户振铃，用户振铃后，向代理服务器发送180 RINGING振铃信息；
4. 代理服务器向终端代理A转发被叫用户的振铃信息；
5. 被叫用户摘机，终端代理B向代理服务器返回表示连接成功的应答200 OK；
6. 代理服务器向终端代理A转发成功指示200 OK；
7. 终端代理A收到消息后，向代理服务器发ACK消息进行确认；
8. 代理服务器将ACK确认消息转发给终端代理B；
9. 主叫用户之间建立通信连接，开始通话。

### 会话更改流程



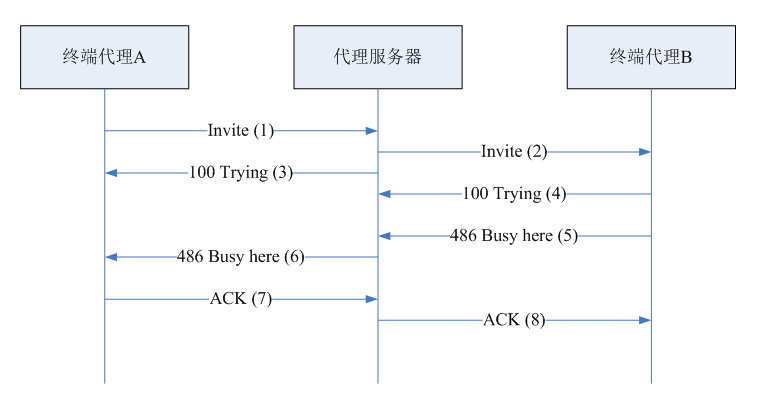
1. 用户代理客户端通过中
2. 用户代理服务端向用户代理客户端发送INVITE消息，带有新的SDP协商消息；
3. 用户代理客户端回复200 OK，并将协商后的SDP信息带回；
4. 用户代理服务端发送ACK给用户代理客户端进行确认。

### 正常呼叫结束流程



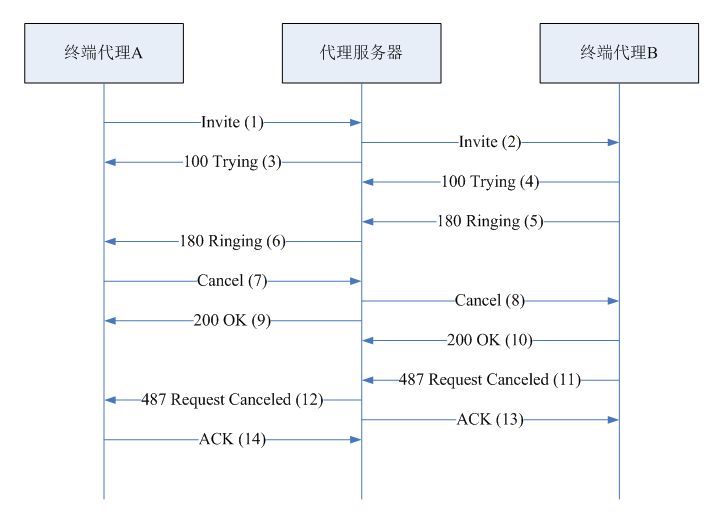
1. 通话中；
2. 用户通话结束后，被叫用户挂机，终端代理B向代理服务器发送BYE消息；
3. 代理服务器转发BYE消息至终端代理A，同时向认证/计费中心传送用户通话的详细信息，请求计费；
4. 主叫用户挂机后，终端代理A向代理服务器发送确认挂断相应消息200 OK；
5. 代理服务器转发响应消息200 OK。

### 被叫忙呼叫结束流程



1. 用户A发起一路呼叫，终端代理A向代理服务器发送INVITE请求；
2. 代理服务器收到呼叫请求后向被叫终端代理转发该INVITE消息；
3. 代理服务器向终端代理A回送100 TRYING，告知终端代理A呼叫正在处理；
4. 终端代理B向代理服务器回送100TRYING，告知代理服务器呼叫正在处理；
5. 呼叫请求送到被叫终端代理B后，被叫忙，终端代理B向代理服务器送486被叫忙响应；
6. 代理服务器向终端代理A转发该响应消息；
7. 终端代理A向代理服务器回送ACK确认消息；
8. 代理服务器向终端代理B送ACK确认消息。

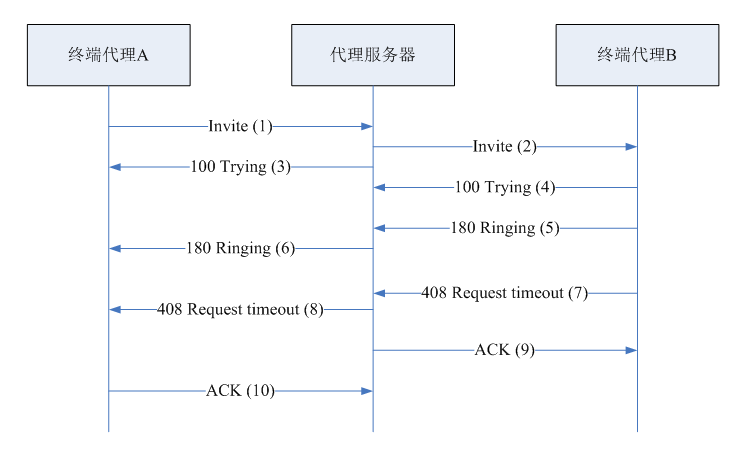
### 被叫无应答流程一



1. 用户A发起一路呼叫，终端代理A向代理服务器发INVITE请求消息；
2. 代理服务器向被叫用户的终端代理B转发该INVITE请求；
3. 代理服务器向终端代理A回送100 TRYING响应，表示呼叫已在处理中；
4. 终端代理B向代理服务器回送100 TRYING，告知代理服务器呼叫正在处理；
5. 被叫用户振铃，终端代理B向代理服务器送180 RING响应；
6. 代理服务器向终端代理A转发该响应消息；
7. 被叫久振铃无应答，终端代理A判断超时后，向代理服务器送CANCEL消息放弃该呼叫；
8. 代理服务器收到CANCEL消息后，向终端代理A回送200 OK响应；
9. 代理服务器将CANCEL消息转发给终端代理B；
10. 终端代理B向代理服务器回送200 OK响应；
11. 终端代理B向代理服务器送487请求已撤销的响应消息；
12. 代理服务器收到后回送ACK确认；
13. 代理服务器向终端代理A送487请求已撤销消息；
14. 终端代理A向代理服务器回送ACK确认。

注：上述步骤中10和12无严格顺序关系。

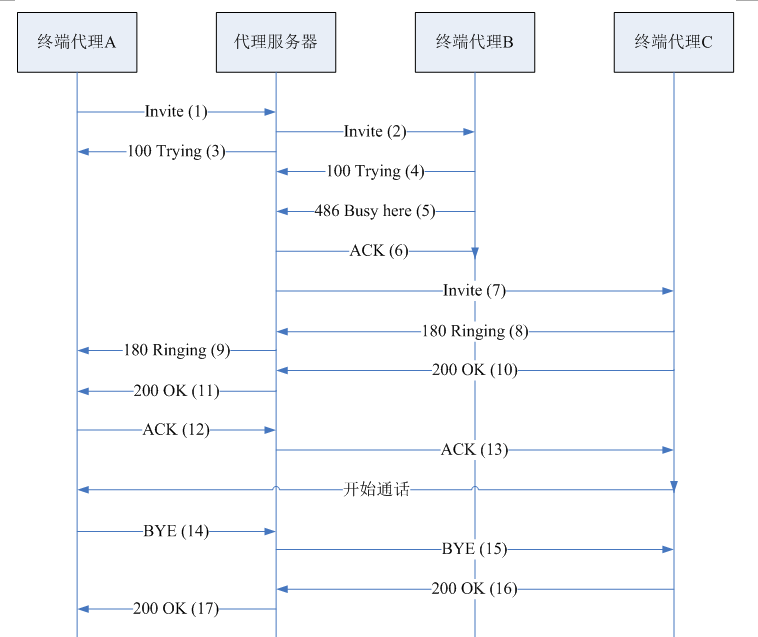
### 被叫无应答流程二



1. 用户A发起一路呼叫，终端代理A向代理服务器发INVITE请求消息；
2. 代理服务器向被叫用户的终端代理B转发该INVITE请求；
3. 代理服务器向终端代理A回送100 TRYING响应，表示呼叫已在处理中；
4. 终端代理B向代理服务器回送100 TRYING，告知代理服务器呼叫正在处理；
5. 被叫用户振铃，终端代理B代理服务器送180 RING响应；
6. 代理服务器向终端代理A转发该响应消息；
7. 被叫久振铃无应答，终端代理B判断超时后，向代理服务器送408 REQUEST TIMEOUT消息放弃该呼叫；
8. 代理服务器收到408 REQUEST TIMEOUT消息后，转发该消息给终端代理A；
9. 代理服务器收到后回送ACK确认给终端代理B；
10. 终端代理A向代理服务器回送ACK确认。

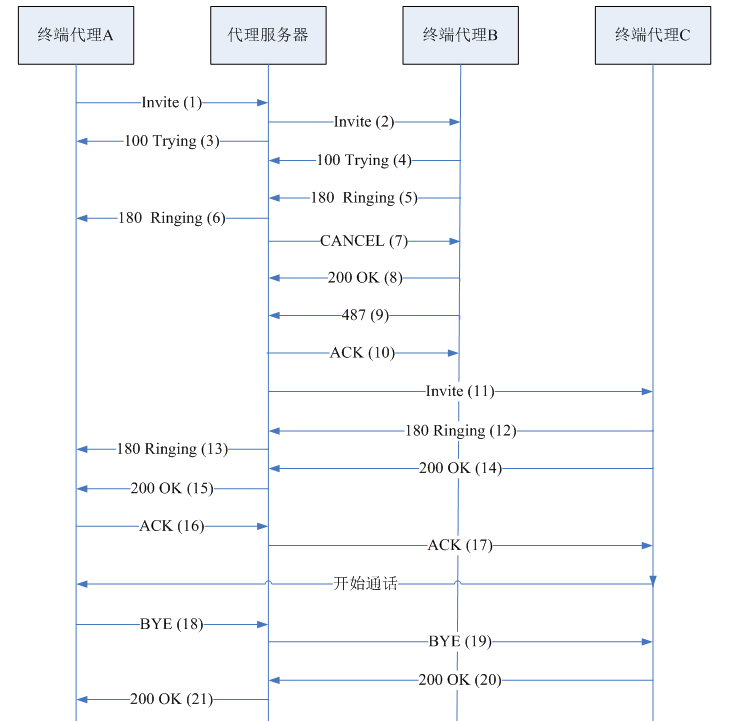
注：上述步骤中9和10无严格的顺序关系。

### 遇忙呼叫前转流程



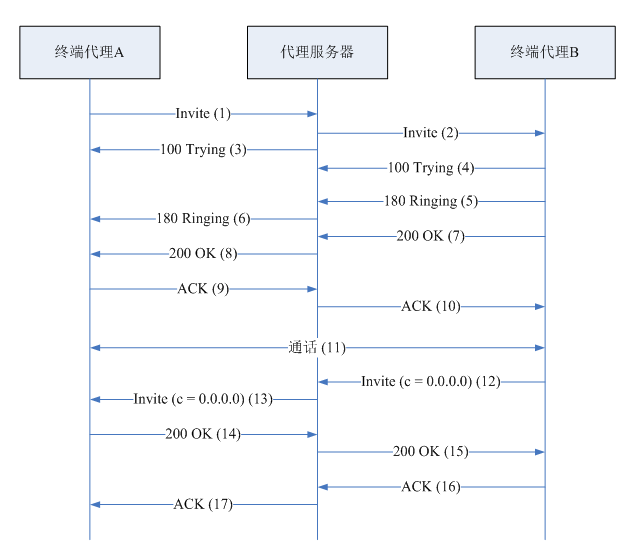
1. 用户A发起一路呼叫，终端代理A向代理服务器发INVITE请求消息；
2. 代理服务器向被叫用户的终端代理B转发该INVITE请求；
3. 代理服务器向终端代理A回送100 TRYING响应，表示呼叫已在处理中；
4. 终端代理B向代理服务器回送100 TRYING，告知代理服务器呼叫正在处理；
5. 终端代理B线路繁忙中，终端代理B向代理服务器送486 BUSY HERE响应；
6. 代理服务器向终端代理B发送ACK响应消息；
7. 代理服务器对此呼叫进行前转，向终端代理C发送INVITE请求消息；
8. 代理终端C收到INVITE请求后，指示用户振铃，同时向代理服务器发送180 RING响应；
9. 代理服务器向代理终端A转发收到的180 RINGING响应；
10. 被叫用户C摘机接听电话，代理终端C向代理服务器发送200 OK响应；
11. 代理服务器向代理终端A转发收到的200 OK响应；
12. 终端代理A向代理服务器回送ACK确认；
13. 代理服务器向代理终端C转发收到的ACK确认，双方开始通话；
14. 主叫挂机，代理终端A向代理服务器发送BYE请求消息，指示用户C挂机；
15. 代理服务器向代理终端C转发收到的BYE请求消息，指示用户C挂机；
16. 用户C播放催促挂断音，同时向代理服务器回应200 OK响应；
17. 代理服务器向代理终端转发收到的200 OK响应。

### 无应答呼叫前转流程



1. 用户A发起一路呼叫，终端代理A向代理服务器发送INVITE请求消息；
2. 代理服务器向被叫用户的代理终端B转发该INVITE请求；
3. 代理服务器向终端代理A回送100 TRYING 响应，表示呼叫已在处理中；
4. 终端代理B向代理服务器回送100 TRYING，告知代理服务器呼叫正在处理；
5. 被叫用户振铃，终端代理B向代理服务器发送180 RINGING响应；
6. 代理服务器向终端代理A转发该响应消息；
7. 被叫振铃无应答，代理服务器判断超时后，向代理终端B发送CANCEL消息放弃该呼叫；
8. 代理终端B收到CANCEL消息后，向代理服务器回送200 OK响应；
9. 终端代理B向代理服务器发送487请求已撤销的响应消息；
10. 代理服务器收到后回送ACK确认；
11. 代理服务器对此呼叫进行前转，向终端代理C发送INVITE请求消息；
12. 代理终端C收到INVITE请求后，指示用户振铃，同时向代理服务器发送180 RINGING响应；
13. 代理服务器向代理终端A转发收到的180 RINGING响应；
14. 被叫用户C摘机接听电话，代理终端C向代理服务器发送200 OK响应；
15. 代理服务器向代理终端A转发收到的200 OK响应；
16. 终端代理A向代理服务器回送ACK确认；
17. 代理服务器向代理终端C转发收到的ACK确认，双方开始通话；
18. 摘机挂机，代理终端A向代理服务器发送BYE请求消息，请求挂机；
19. 代理服务器向代理终端C转发收到的BYE请求消息，指示用户C挂机；
20. 用户C放催促挂机音，同时向代理服务器回应200 OK响应；
21. 代理服务器向代理终端转发收到的200 OK响应。

### 呼叫保持

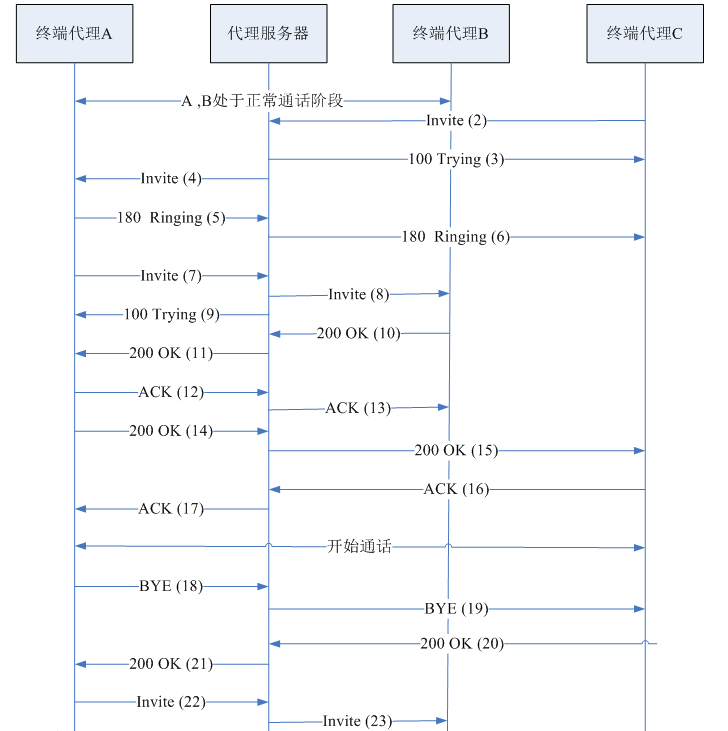


1. 用户摘机发起一路呼叫，终端代理A向该区域的代理服务器发起INVITE请求；
2. 代理服务器通过认证/计费中心确认用户认证已通过后，检查请求消息中的VIA头域中是否已包含其地址：

* 若已包含，说明发生环回，返回指示错误的应答；
* 若没问题，代理服务器在请求消息的VIA头域中插入自身地址，并向INVITE消息的TO域所指示的被叫终端代理B转发INVITE请求。

1. 代理服务器向终端代理A发送呼叫处理中的应答消息，100 TRYING；
2. 终端代理B向代理服务器发送呼叫处理中的应答消息，100 TRYING；
3. 终端代理B指示被叫用户振铃，用户振铃后，向代理服务器发送180 RINGING振铃；
4. 代理服务器向终端代理A转发被叫用户的振铃信息；
5. 被叫用户摘机，终端代理B向代理服务器返回表示连接成功的应答 200 OK；
6. 代理服务器向终端代理A转发成功指示 200 OK；
7. 终端代理A收到消息后，向代理服务器发送ACK消息进行确认；
8. 代理服务器将ACK确认消息转发给终端代理B；
9. 主叫被叫之间建立通信连接，开始通话；
10. 代理终端向代理服务器发送REINVITE请求消息，SDP的C域等于0.0.0.0；
11. 代理服务器转发此消息给代理终端A；
12. 代理终端A收到REINVITE后，回应200 OK响应，表示接受会话更改，同时根据协商结果修改会话方式；
13. 代理服务器转发200 OK给代理终端B；
14. 终端代理B收到消息后，向代理服务器发送ACK消息进行确认；
15. 代理服务器将ACK确认消息转发给终端代理A。

### 呼叫等待



1. 通话中；
2. 用户A，B正处于通话阶段，用户C向A发起呼叫，终端代理C发送INVITE消息给代理服务器；
3. 代理服务器向终端代理C回送100 TRYING响应，表示呼叫已在处理中；
4. 代理服务器把INVITE消息转发给代理终端A；
5. 用户A振铃，终端代理A向代理服务器发送180 RINGING响应；
6. 代理服务器向终端代理C转发该响应消息；
7. 用户A按下呼叫保持键，代理终端A向代理服务器发送INVITE消息，请求与代理终端呼叫保持；
8. 代理服务器转发此消息给终端代理B；
9. 代理服务器向终端代理A回送100 TRYING响应，表示呼叫已在处理中；
10. 终端代理B收到呼叫保持请求后，发送200 OK给代理服务器，表示接受呼叫保持；
11. 代理服务器转发200 OK响应给终端代理A；
12. 终端代理A向代理服务器回送ACK确认；
13. 代理服务器向代理终端B转发收到的ACK确认；
14. 终端代理A发送200 OK给代理服务器，表示接受C的呼叫；
15. 代理服务器转发200 OK响应给终端代理C；
16. 终端代理C向代理服务器回送ACK确认；
17. 代理服务器向代理终端A转发收到的ACK确认，A、C之间开始通话；
18. 用户A挂机，终端代理A向代理服务器发送BYE请求消息；
19. 代理服务器转发BYE消息给代理服务器，表示接受请求；
20. 终端代理C发送200 OK给代理服务器，表示接受请求；
21. 代理服务器转发200 OK响应给终端代理A；
22. 终端代理C重新发送INVITE请求给代理服务器，请求和终端代理B恢复通话；
23. 代理服务器向代理终端B转发收到的INVITE请求。

## 优点及缺点

### 优点

（1）Session和Media间的处理彼此独立，因此SIP更加灵活。

（2）SIP是开放、标准协议。

（3）SIP messages是明文的，利于trouble shooting。

（4）拥有不同capability的用户一样可以通讯。例如：在一个video conference中，video用户和audio用户一样可以通讯，只不过是audio看不到视频而已。

### 缺点

（1）由于SIP messages是明文的，router必须将明文的message翻译为路由器语言，这就导致了router产生更高的负载。

（2）SIP是个较新的协议，懂得人不多。

（3）如果在同一个网络中同时有SIP Phone和SCCP Phone，必须在in-band DTMF和out-band DTMF间进行转换。

（4）SIP仍然是一个处于开发中的协议。