基于ICE方式SIP信令穿透Symmetric NAT技术研究 [转]

基于ICE方式SIP信令穿透Symmetric NAT技术研究

曾立 吴平 高万林 武文娟

1 (中国农业大学 计算机科学与技术系，北京 100083) 2(中国人民大学信息学院，北京 100872)

摘 要 基于IP的语音、数据、视频等业务在NGN网络中所面临的一个实际困难就是如何有效地穿透各种NAT/FW的问题。对此，会话初始化协议SIP以往的解决方法有ALGs，STUN，TURN等方式。本文探讨了一种新的媒体会话信令穿透NAT/FW的解决方案—交互式连通建立方式(ICE)。它通过综合利用现有协议，以一种更有效的方式来组织会话建立过程，使之在不增加任何延迟同时比STUN等单一协议更具有健壮性、灵活性。本文详细介绍了ICE算法，并设计一个实例针对SIP信令协议穿透Symmetric NAT流程进行了描述，最后总结了ICE的优势及应用前景。

关键词 ICE；Symmetric NAT；STUN；TURN；SIP

1 问题背景

多媒体会话信令协议是在准备建立媒体流传输的代理之间交换信息的协议，例如SIP、RTSP、H.323等。媒体流与信令流截然不同，它们所采用的网络通道也不一致。由于协议自身设计上的原因，使得媒体流无法直接穿透网络地址转换/防火墙(NAT/FW)。因为它们生存期的目标只是为了建立一个在信息中携带IP地址的分组流，这在遇到NAT/FW 时会带来许多问题。而且这些协议的目标是通过建立P2P(Peer to Peer)媒体流以减小时延，而协议本身很多方面却与NAT存在兼容性问题，这也是穿透 NAT/FW的困难所在。

而NAT仍是解决当前公用IP地址紧缺和网络安全问题的最有力手段，它主要有四种类型：完全圆锥型NAT(Full Cone NAT)，地址限制圆锥型NAT (Address Restricted Cone NAT)，端口限制圆锥型NAT (Port Restricted Cone NAT)，对称型NAT (Symmetric NAT)。前三种NAT，映射与目的地址无关，只要源地址相同，映射就相同，而对称型NAT的映射则同时关联源地址和目的地址，所以穿透问题最为复杂。

不少方案已经被应用于解决穿透NAT问题，例如：ALGs(Application Layer Gateways)、Middlebox Control Protocol、STUN (Simple Traversal of UDP through NAT)、TURN (Traversal Using Relay NAT)、RSIP(Realm Specific IP)、symmetric RTP等。然而，当这些技术应用于不同的网络拓扑时都有着显著的利弊，以至于我们只能根据不同的接入方式来应用不同的方案，所以未能很好地解决All-NAT与Efficiency的问题，同时还会给系统引入了许多复杂性和脆弱性因素。所以我们目前需要一种综合的足够灵活的方法，使之能在各种情况下对NAT/FW的信令穿透问题提供最优解。事实上，ICE正是符合这样要求的一种良好的解决方案。

2 ICE技术

2.1 ICE简介

交互式连通建立方式ICE(Interactive Connectivity Establishment)并非一种新的协议，它不需要对STUN、TURN或RSIP进行扩展就可适用于各种NAT。ICE是通过综合运用上面某几种协议，使之在最适合的情况下工作，以弥补单独使用其中任何一种所带来的固有缺陷。对于SIP来说，ICE只需要定义一些SDP(Session Description Protocol)附加属性即可，对于别的多媒体信令协议也需要制定一些相应的机制来实现。本文仅就SIP问题展开讨论。

2.2 多媒体信令

媒体流穿透NAT的过程是独立于某种具体的信令协议的。通信发生在两个客户端－会话发起者和会话响应者。初始化信息(Initiate Message)包含了描述会话发起者媒体流的配置与特征，并经过信令调停者(也叫信令中继)，最后到达会话响应者。假设会话响应者同意通信，接受信息(Accept Message)将产生并反馈至会话初始者，媒体流建立成功。此外，信令协议还对媒体流参数修改以及会话终止消息等提供支持。对于SIP，会话发起者即UAC(User Agent Client)，会话响应者即UAS(User Agent Server)，初始化消息对应SDP请求里面的INVITE，接受消息对应于SDP应答里面的200 OK，终止消息对应于BYE。

2.3 算法流程

2.3.1 收集传输地址

会话发起者需要收集的对象包括本地传输地址(Local Transport Address)和来源传输地址(Derived Transport Address)。本地传输地址通常由主机上一个物理(或虚拟)接口绑定一个端口而获得。会话发起者还将访问提供UNSAF(Unilateral self-address fixing)的服务器，例如STUN、TURN或TERED0。对于每一个本地传输地址，会话者都可以从服务器上获得一组来源传输地址。

显然，实现物理或虚拟连通方式越多，ICE将工作得越好。但为了建立对等通信，ICE通常要求至少有一个来源地址由位于公网上的中继服务器(如TURN)所提供的，而且需要知道具体是哪一个来源传输地址。

2.3.2 启动STUN

会话发起者获得一组传输地址后，将在本地传输地址启动STUN服务器，这意味着发送到来源地址的STUN服务将是可达的。与传统的STUN不同，客户端不需要在任何其它IP或端口上提供STUN服务，也不必支持TLS， ICE用户名和密码已经通过信令协议进行交换。

客户端将在每个本地传输地址上同时接受STUN请求包和媒体包，所以发起者需要消除STUN消息与媒体流协议之间的歧义。在RTP和RTCP中实现这个并不难，因为RTP与RTCP包总是以0b10(v=2)打头，而STUN是0b00。对于每个运行STUN服务器的本地传输地址，客户端都必须选择相应的用户名和密码。用户名要求必须是全局唯一的，用户名和密码将被包含在初始化消息里传至响应者，由响应者对STUN请求进行鉴别。

2.3.3 确定传输地址的优先级

STUN服务器启动后，下一步就是确定传输地址的优先级。优先级反映了UA在该地址上接收媒体流的优先级别，取值范围在0到1之间，通常优先级按照被传输媒体流量来确定。流量小者优先，而且对于相同流量者的Ipv6地址比Ipv4地址具有更高优先级。因此物理接口产生的本地Ipv6传输地址具有最高的优先级，然后是本地Ipv4传输地址，然后是STUN、RSIP、TERED0来源地址，最后是通过VPN接口获得的本地传输地址。

2.3.4 构建初始化信息(Initiate Message)

初始化消息由一系列媒体流组成，每个媒体流都有一个缺省地址和候选地址列表。缺省地址通常被Initiate消息映射到SIP信令消息传递地址上，而候选地址列表用于提供一些额外的地址。对于每个媒体流来说，任意Peer之间实现最大连通可能性的传输地址是由公网上转发服务器(如TURN)提供的地址，通常这也是优先级最低的传输地址。客户端将可用的传输地址编成一个候选地址列表(包括一个缺省地址)，并且为每个候选元素分配一个会话中唯一的标识符。该标识符以及上述的优先级都被编码在候选元素的id属性中。一旦初始化信息生成后即可被发送。

2.3.5 响应处理：连通性检查和地址收集

会话应答方接收到初始化信息Initiate Message后，会同时做几个事情：首先，执行2.3.1中描述的地址收集过程。这些地址可以在呼叫到达前预收集，这样可以避免增加呼叫建立的时间。当获得来源地址以后，应答方会发送STUN Bind请求，该请求要求必须包含Username属性和Password属性，属性值为从 “alt”中得到的用户名和密码。STUN Bind请求还应包括一个Message-Integrity属性，它是由Initiate Message中候选元素的用户名和密码计算得来的。此外，STUN Bind请求不应有Change-Request或Response-Address属性。

当一个客户端收到Initiate Message时，它将通过其中缺省地址和端口发送媒体流。如果STUN Bind请求消息引起错误应答，则需要检查错误代码。如果是401，430，432或500，说明客户端应该重新发送请求。如果错误代码是400，431和600，那么客户端不必重试，直接按超时处理即可。

2.3.6 生成接受信息(Accept Message)

应答者可以决定是接受或拒绝该通信，若拒绝则ICE过程终止，若接受则发送Accept消息。Accept消息的构造过程与Initiate Message类似。

2.3.7 接受信息处理

接受过程有两种可能。如果Initiate Message的接受者不支持ICE，则Accept Message将只包含缺省的地址信息，这样发起方就知道它不用执行连通性检查了。然而如果本地配置信息要求发起者通过TURN服务器发包来进行连通性检查，这将意味着那些直接发给响应者的包会被对方防火墙丢弃。为解决这个问题，发起者需要重新分配一个TURN来源地址，然后使用Send命令。一旦Send命令被接受，发起者将发送所有的媒体包到TURN服务器，由服务器转发至响应者。如果Accept Message包含候选项，则发起方处理Accept Message的过程就与响应方处理Initiate Message很相似了。

2.3.8 附加ICE过程

Initiate或Accept消息交换过程结束后，双方可能仍将继续收集传输地址，这通常是由于某些STUN事务过长而未结束引起，另一种可能是由于Initiate/Accept消息交换时提供了新的地址。

2.3.9 ICE到SIP的映射

使用ICE方式穿透NAT，必须映射ICE定义的参数到SIP消息格式中，同时对其SDP属性进行简单扩展—在SDP的Media块中定义一个新的属性“alt”来支持ICE。它包含一个候选IP地址和端口，SDP的接受端可以用该地址来替换m和c中的地址。Media块中可能会有多个alt属性，这时每个alt应该包括不重复的IP地址和端口。语法属性如下：

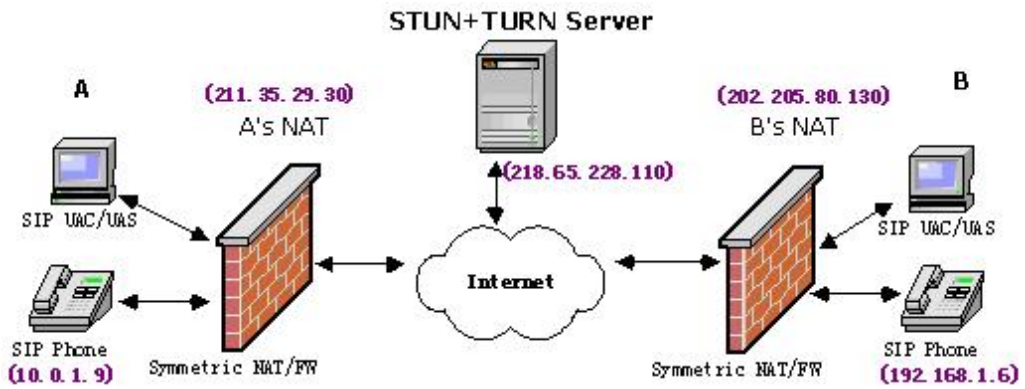
```
alt-attribute = "alt" ":" id SP qvalue SP derived-from SP
                 username SP password SP
                 unicast-address SP port [unicast-address SP port]
                 ;qvalue from RFC 3261
                 ;unicast-address, port from RFC 2327
                 username      = non-ws-string
                 password      = non-ws-string
                 id            = token
                derived-from  = ":" / id
```

Symmetric NAT/FW

下面设计一个简化的基于ICE的对称式网络地址转换/防火墙(Symmetric NAT/FW)的穿透实例，进一步说明ICE的工作流程。

此主题相关图片如下：

图1 Symmetric NAT/FW网络拓扑图



假设通信双方同时处于对称式NAT/FW内部，现在SIP终端A要与B进行VoIP通信。A所在的内部地址是10.0.1.9，外部地址是211.35.29.30；B的内部地址是192.168.1.6，外部地址是202.205.80.130；STUN/TURN服务器的地址是218.65.228.110。

首先A发起请求，进行地址收集，如图所示。生成A的Initiate Message如下：

```
v=0
o=Dodo 2890844730 2890844731 IN IP4 host.example.com
s=
c=IN IP4 218.65.228.110
t=0 0
m=audio 8076 RTP/AVP 0
a=alt:1 1.0 : user 9kksj== 10.0.1.9 1010
```

a=alt:2 0.8 : user1 9kksk== 211.35.29.30 9988

a=alt:3 0.4 : user2 9kksl== 218.65.228.110 8076

其中本地地址的优先级为1.0,STUN地址的优先级为0.8,TURN地址优先级为0.4。

当B收到消息后，也进行地址收集，过程和A类似。然后B开始执行连通性检查，可是我们不难发现，到10.0.1.9:1010的STUN请求和到211.35.29.30:9988的STUN请求都将不可避免地失败。因为前者是一个不可路由的保留地址；而后者由于Symmetric NAT会对于每一个STUN/TURN请求都将分配不同的Binding，当数据包抵达A的NAT时，NAT会发现传输地址211.35.29.30:9988已经映射218.65.228.110:3478了。而此时STUN请求的源地址并非218.65.228.110:3478，所以数据包必然会被A的NAT/FW所丢弃。然而，到218.65.228.110:8076的STUN请求却是成功的，因为TURN服务器用它收集到的原始地址来发送TURN请求。

当A收到应答后，它也执行连通性检查，如图所示：

图2 ： A的地址收集过程时序图
此主题相关图片如下：

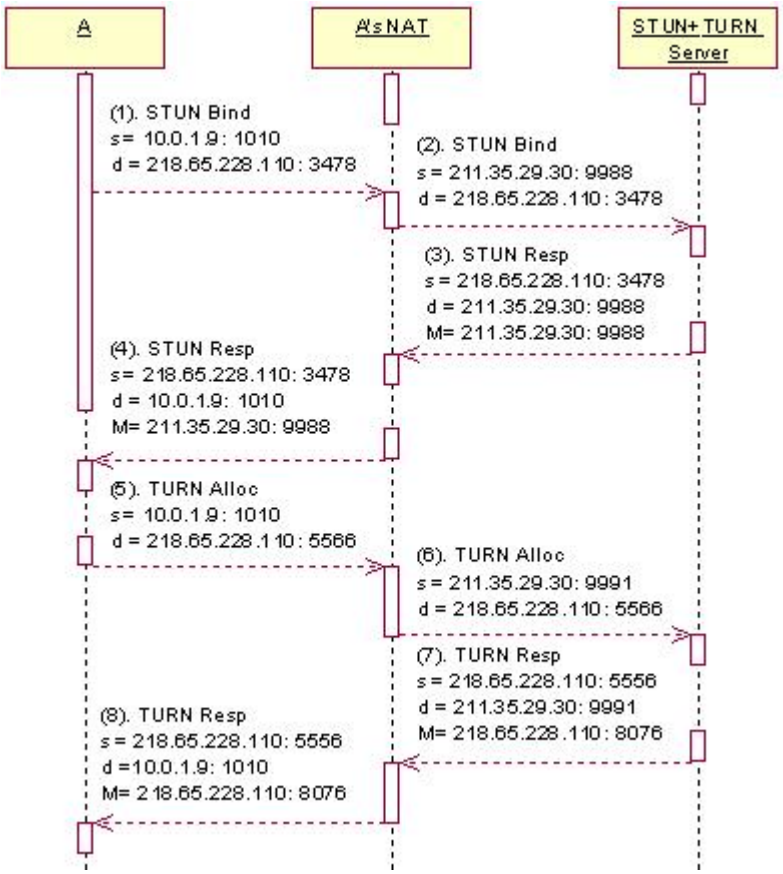


图3 ： B的地址收集过程时序图

此主题相关图片如下：

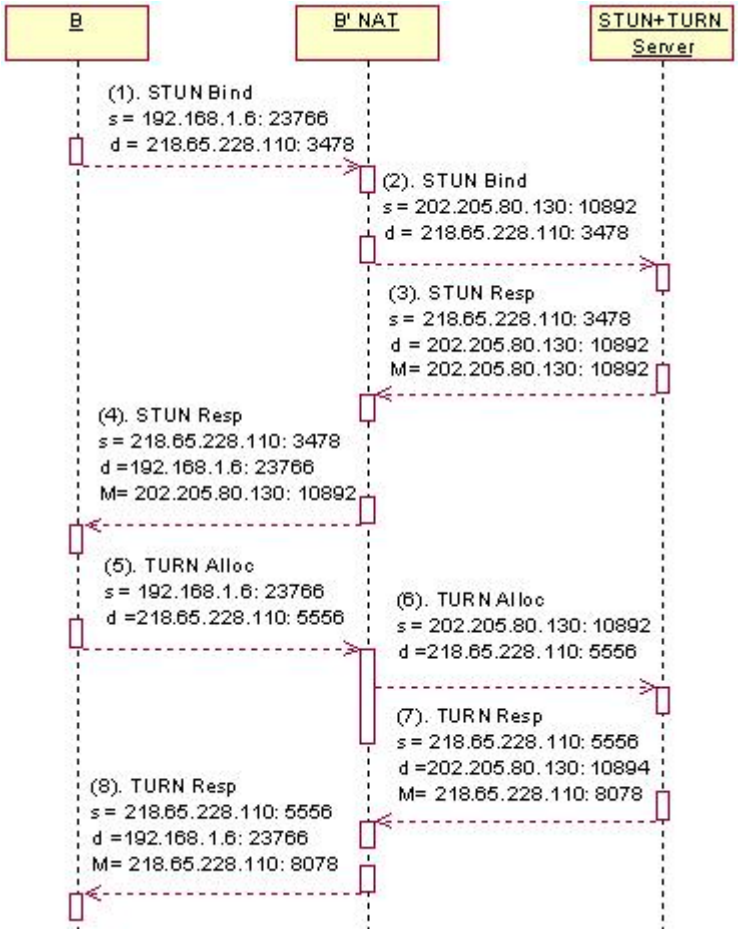
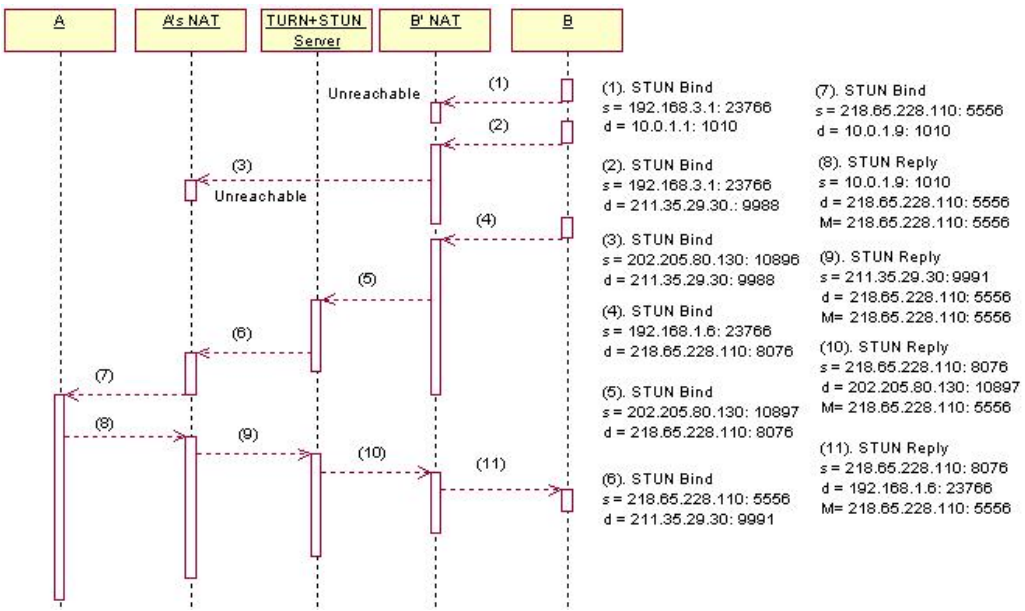


图**4** ： **B**的连通性检查



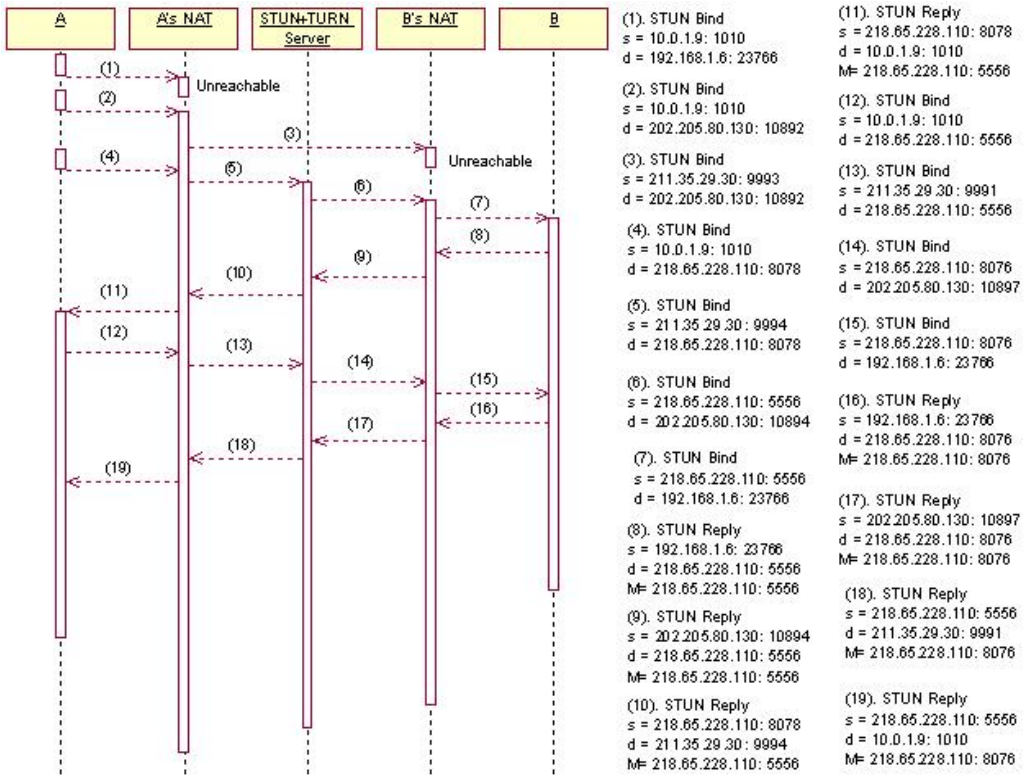
完成连通性检查后，**B**产生的应答消息如下：

v=0

```
o= Vincent 2890844730 289084871 IN IP4 host2.example.com
s=
c=IN IP4 218.65.228.110
t=0 0
m=audio 8078 RTP/AVP 0
a=alt:4 1.0 : peer as88jl 192.168.1.6 23766
a=alt:5 0.8 : peer1 as88kl 202.205.80.130 10892
a=alt:6 0.4 : peer2 as88ll 218.65.228.110 8078
a=alt:7 0.4 3 peer3 as88ml 218.65.228.110 5556
```

此主题相关图片如下：

图5： A的连通性检查



和前面一样，对于B的私有地址和STUN来源地址的连通性检查结果均为失败，而到B的TURN来源地址和到B的peer-derived地址成功(本例中它们都具有相同的优先级0.4)。相同优先级下我们通常采用peer-derived地址，所以A发送到B的媒体流将使用218.65.228.110:5556地址，而B到A的媒体流将发送至218.65.228.110:8076地址。以上为基于ICE方式解决Symmetric NAT/FW穿透问题的一个简化后的典型实例。

3.2 其它类型NAT/FW

基于ICE实现其它类型的NAT/FW穿透问题，其过程比Symmetric NAT还要简单，见参考文献[1] [2] [6]。

4 结束语

ICE方式的优势是显而易见的，它消除了现有的UNSAF机制的许多脆弱性。例如传统的

STUN有几个脆弱点，其中一个就是发现过程需要客户端自己去判断所在NAT类型，这实际上不是一个可取的做法。而应用ICE之后，这个发现过程已经不需要了。另一点脆弱性在于STUN、TURN等机制都完全依赖于一个附加的服务器，而ICE利用服务器分配单边地址的同时，还允许客户端直接相连，因此即使STUN或TRUN服务器中有任何一个失败了，ICE方式仍可让呼叫过程继续下去。此外，传统的STUN最大的缺陷在于它不能保证在所有网络拓扑结构中都正常工作，最典型的问题就是Symmetric NAT。对于TURN或类似转发方式工作的协议来说，由于服务器的负担过重，很容易出现丢包或者延迟情况。而ICE方式正好提供了一种负载均衡的解决方案，它将转发服务作为优先级最低的服务，从而在最大程度上保证了服务的可靠性和灵活性。此外，ICE的优势还在于对Ipv6的支持，目前Cisco等公司正在设计基于ICE方式的NAT/FW解决方案。由于广泛的适应能力以及对未来网络的支持，ICE作为一种综合的解决方案将有着非常广阔的应用前景。