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

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)。因为它们生存期的勘嘿皇俏 私 ⑽桓鲈谛畔⑽行 凫 P 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 TEREDO。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、TEREDO 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
```

3 实例设计

3.1 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。

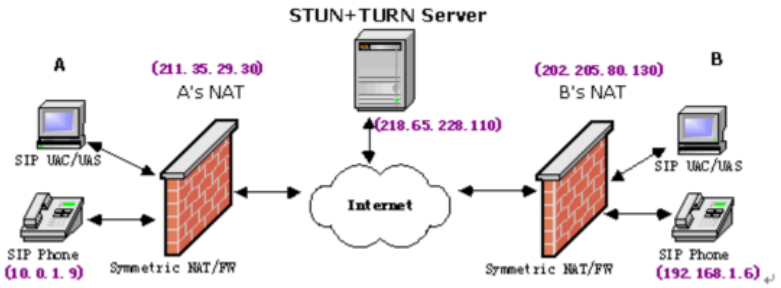


图 1 Symmetric NAT/FW 网络拓扑图

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。

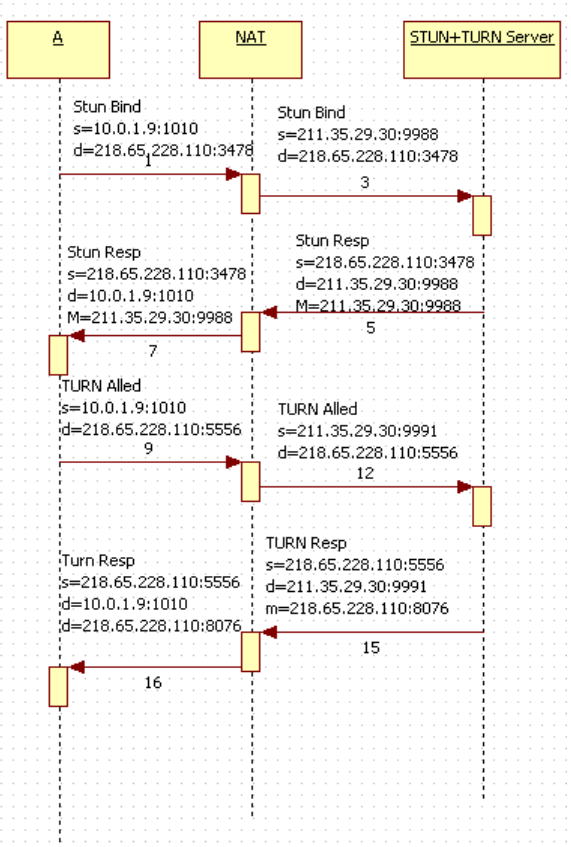


图2：A的地址收集过程时序图

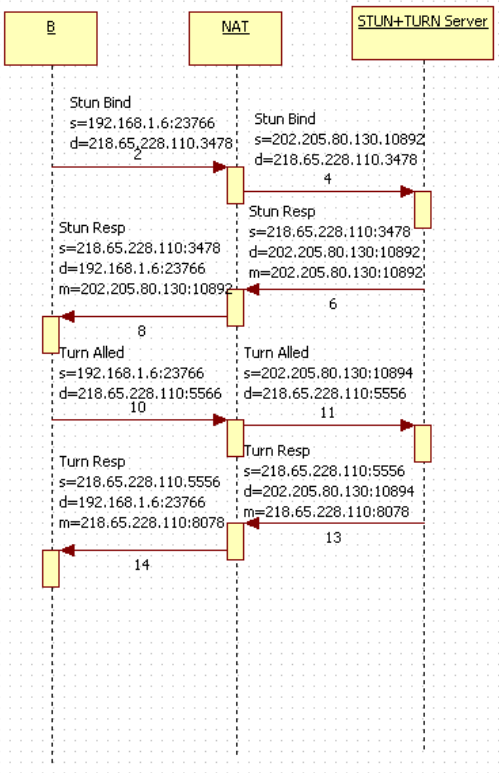


图3：B的地址收集过程时序图

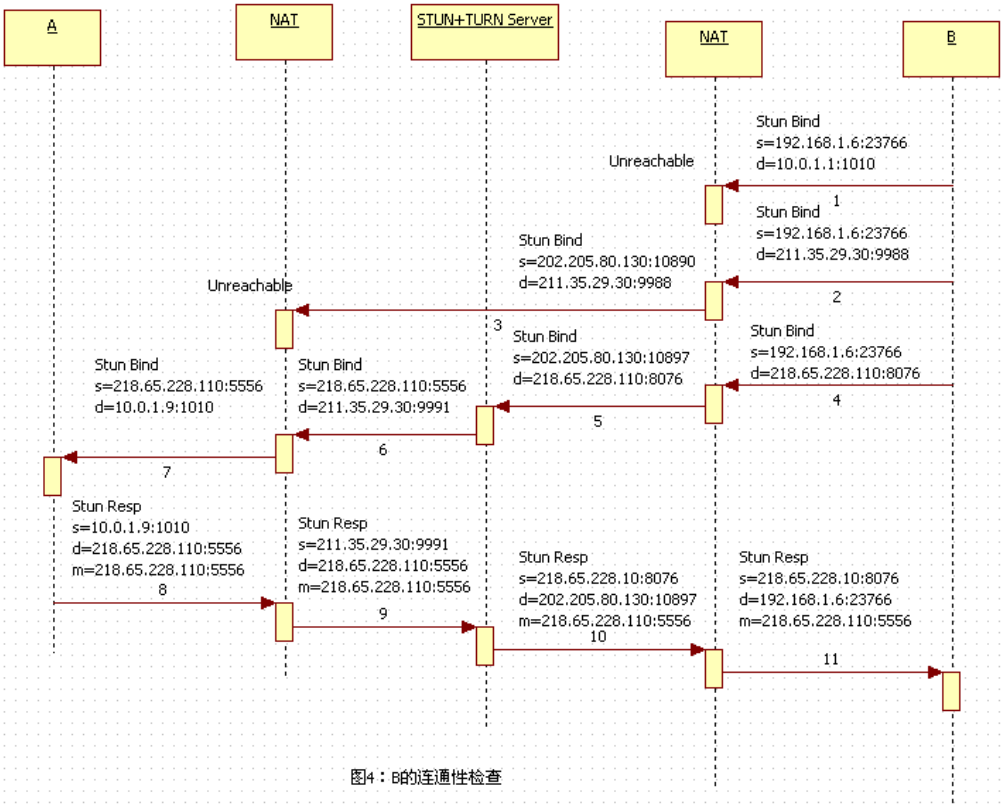


图4：B的连通性检查

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

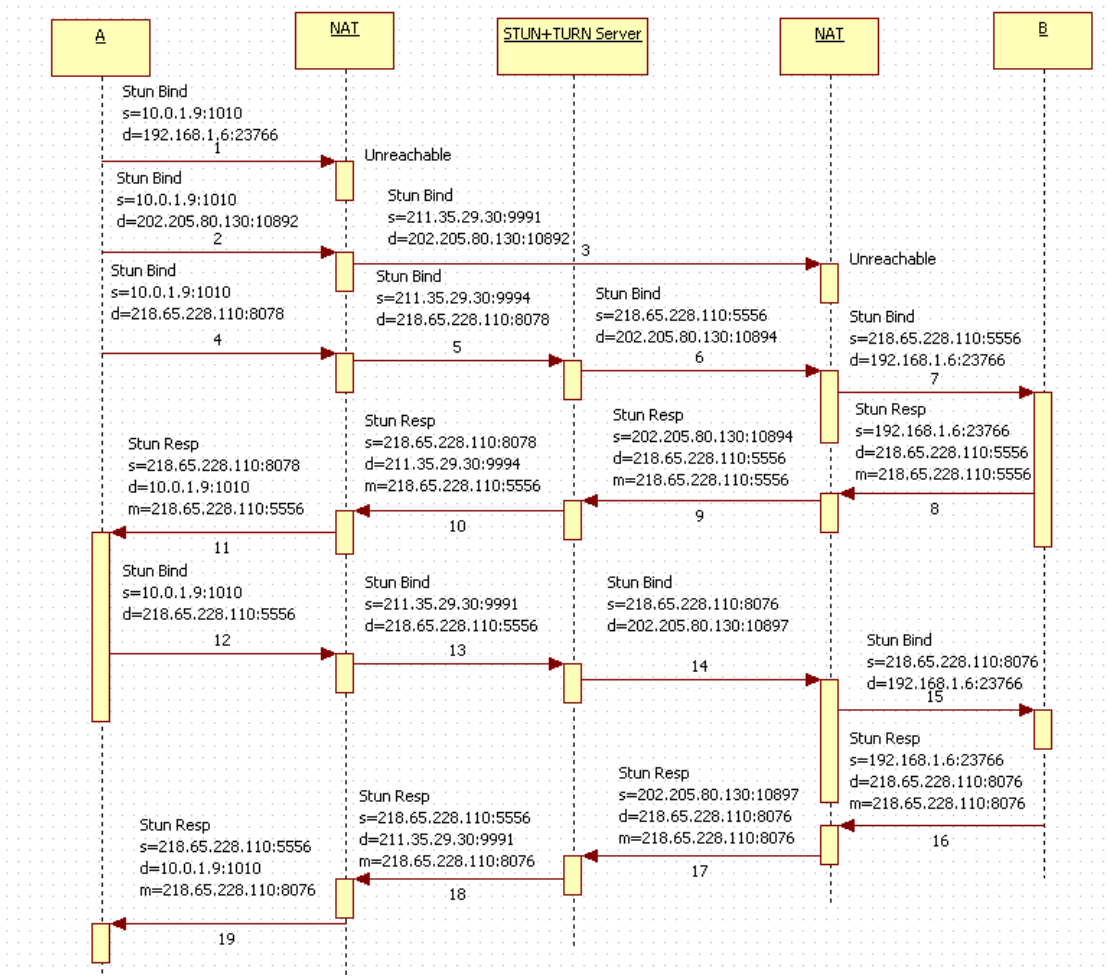
a=alt:4 1.0 : peer as88j1 192.168.1.6 23766

a=alt:5 0.8 : peer1 as88k1 202.205.80.130 10892

a=alt:6 0.4 : peer2 as88l1 218.65.228.110 8078

a=alt:7 0.4 3 peer3 as88m1 218.65.228.110 5556

当 A 收到应答后，它也执行连通性检查，如图所示：



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。