P2P基础--NAT穿透

缩写	全称	说明
STUN(RFC3489)	Simple Traversal of UDP Through NATs	NAT的UDP简单穿越
STUN(RFC5389)	Session Traversal Utilities for NAT	NAT会话穿透工具，与RFC3489除了名称变化外，最大的区别是支持TCP穿透
TURN(RFC5766)	Traversal Using Relays around NAT:Relay Extensions to Session Traversal Utilities for NAT	使用中继穿透NAT：STUN的中继扩展，TURN是通过两方通讯的“中间人”方式实现穿透
ICE(RFC5245)	Interactive Connectivity Establishment	交互式连接建立

一、概述

在现实Internet网络环境中，大多数计算机主机都位于防火墙或NAT之后，只有少部分主机能够直接接入Internet。很多时候，我们希望网络中的两台主机能够直接进行通信，即所谓的P2P通信，而不需要其他公共服务器的中转。由于主机可能位于防火墙或NAT之后，在进行P2P通信之前，我们需要进行检测以确认它们之间能否进行P2P通信以及如何通信。这种技术通常称为NAT穿透（NAT Traversal）。

了解STUN和TURN之前，我们需要了解NAT的种类。NAT传输UDP的实现方式有4种，分别如下：

- Full Cone NAT

  完全锥形NAT，所有从同一个内网IP和端口号发送过来的请求都会被映射成同一个外网IP和端口号，并且任何一个外网主机都可以通过这个映射的外网IP和端口号向这台内网主机发送包。

- Restricted Cone NAT

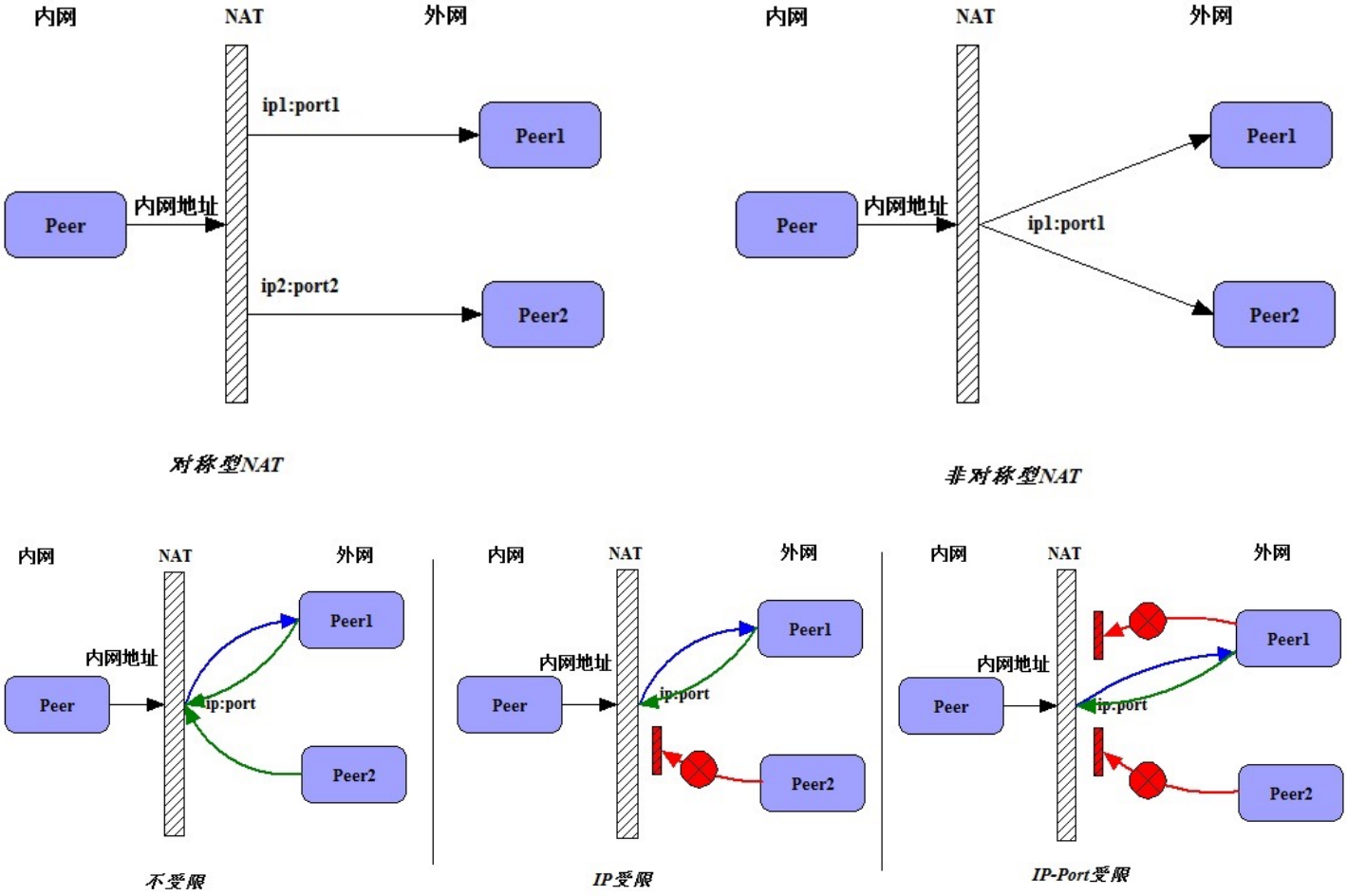
  限制锥形NAT，它也是所有从同一个内网IP和端口号发送过来的请求都会被映射成同一个外网IP和端口号。与完全锥形不同的是，外网主机只能够向先前已经向它发送过数据包的内网主机发送包。

- Port Restricted Cone NAT

  端口限制锥形NAT，与限制锥形NAT很相似，只不过它包括端口号。也就是说，一台IP地址X和端口P的外网主机想给内网主机发送包，必须是这台内网主机先前已经给这个IP地址X和端口P发送过数据包。

- Symmetric NAT

对称NAT，所有从同一个内网IP和端口号发送到一个特定的目的IP和端口号的请求，都会被映射到同一个IP和端口号。如果同一台主机使用相同的源地址和端口号发送包，但是发往不同的目的地，NAT将会使用不同的映射。此外，只有收到数据的外网主机才可以反过来向内网主机发送包。



以上四种是上面两张图的组合类型

二、流程

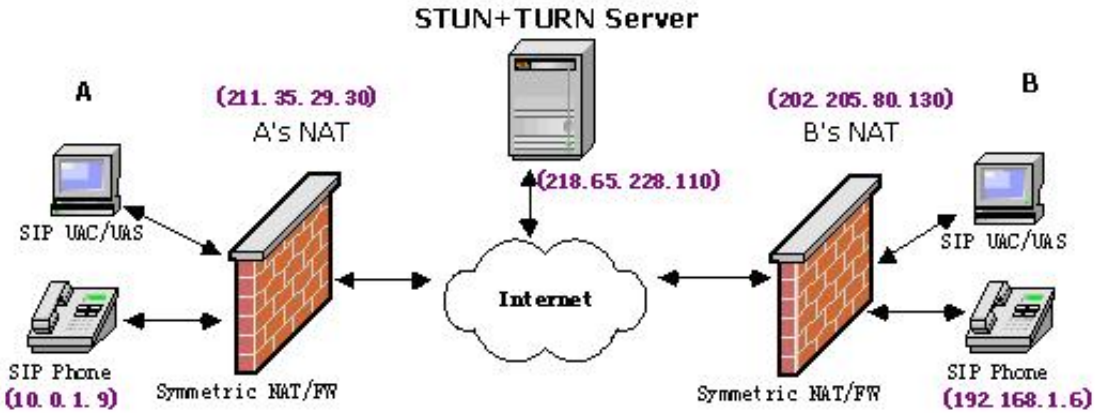


图1 Symmetric NAT/FW网络拓扑图

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。

当A收到应答后，它也执行连通性检查，如图所示：

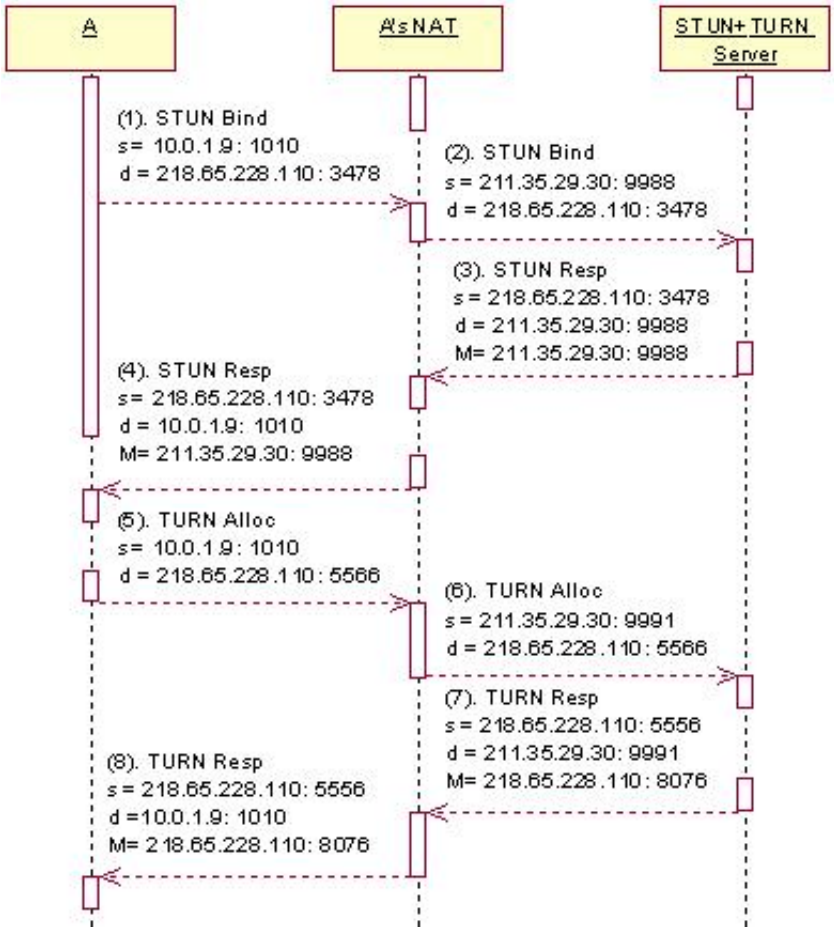


图2： A的地址收集过程时序图

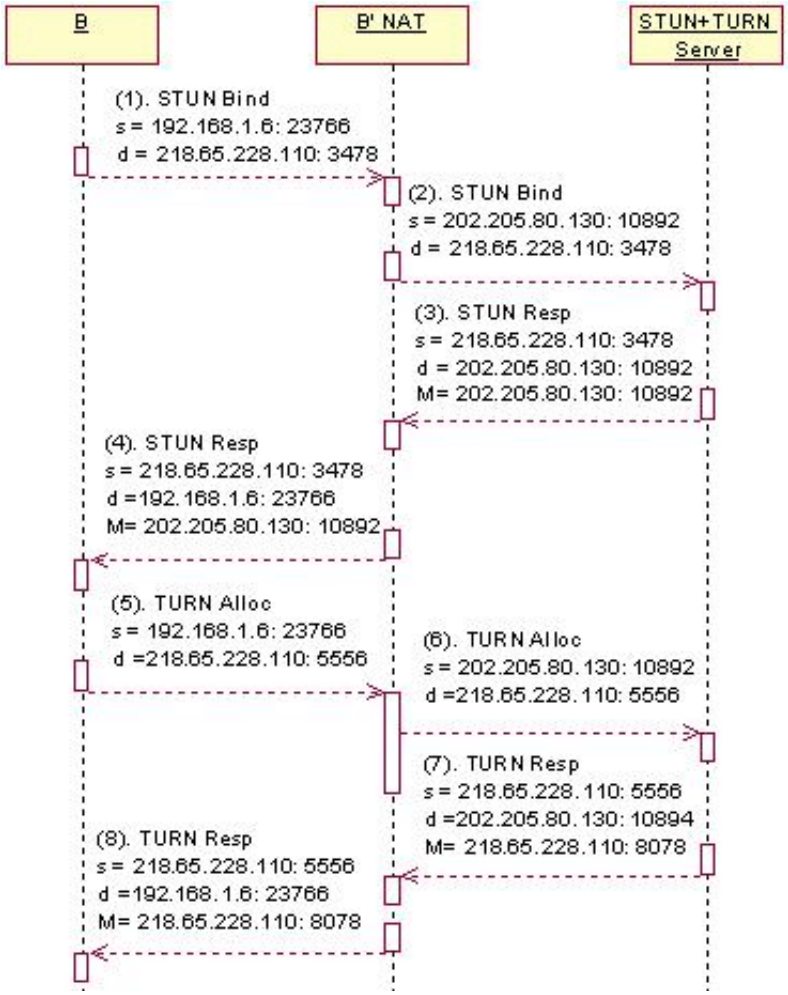


图3： B的地址收集过程时序图

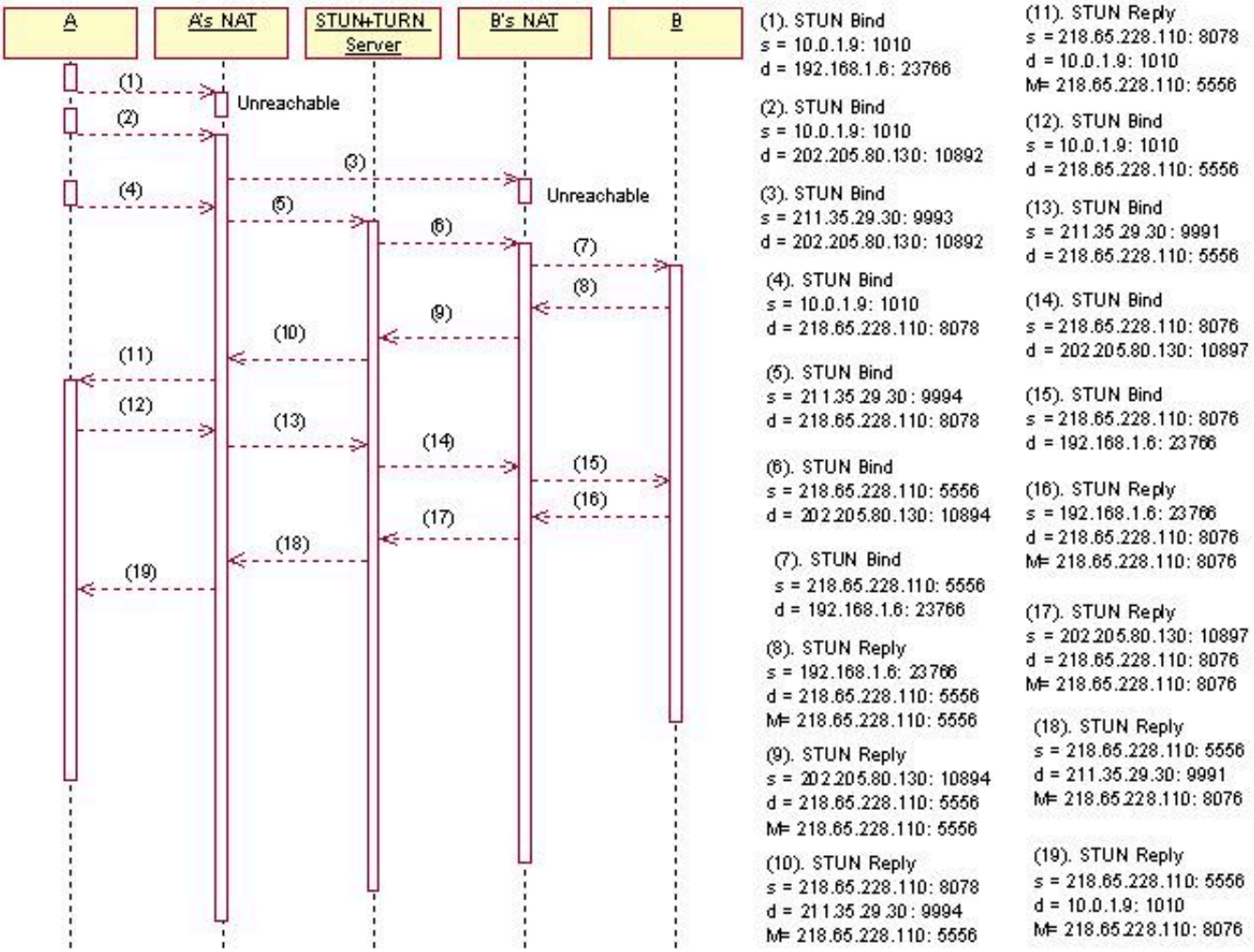


图4： B的连通性检查

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 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
```

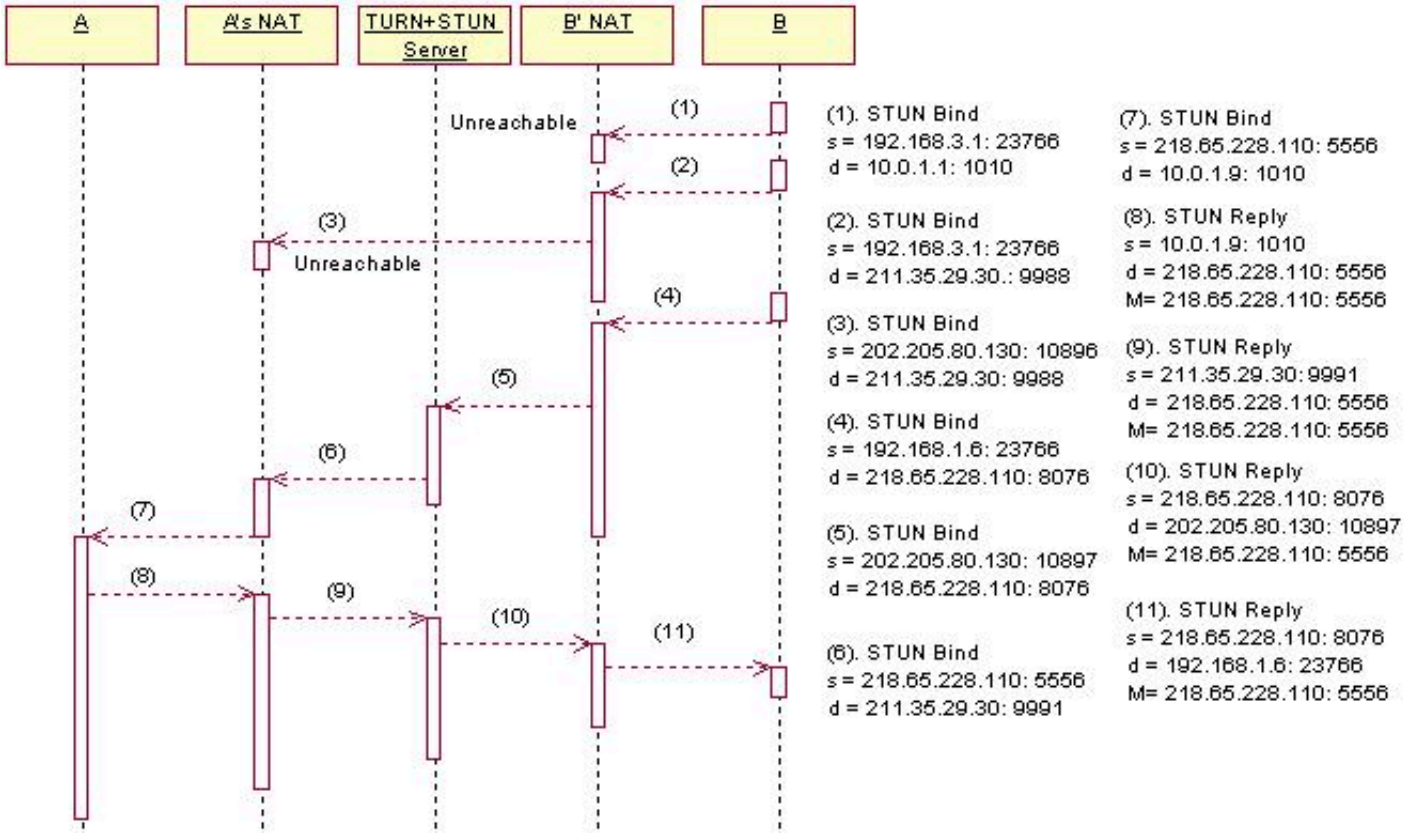


图5： A的连通性检查

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。