一．nat类型介绍

**用语定义**

**1.内部Tuple**：指内部主机的私有地址和端口号所构成的二元组，即内部主机所发送报文的源地址、端口所构成的二元组

**2.外部Tuple**：指内部Tuple经过NAT的源地址/端口转换之后，所获得的外部地址、端口所构成的二元组，即外部主机收到经NAT转换之后的报文时，它所看到的该报文的源地址（通常是NAT设备的地址）和源端口

**3.目标Tuple**：指外部主机的地址、端口所构成的二元组，即内部主机所发送报文的目标地址、端口所构成的二元组

**详细释义**

**1. Full Cone NAT**：所有来自同一 个内部Tuple X的请求均被NAT转换至同一个外部Tuple Y，而不管这些请求是不是属于同一个应用或者是多个应用的。除此之外，当X-Y的转换关系建立之后，任意外部主机均可随时将Y中的地址和端口作为目标地址 和目标端口，向内部主机发送UDP报文，由于对外部请求的来源无任何限制，因此这种方式虽然足够简单，但却不那么安全

**2. Restricted Cone NAT**： 它是Full Cone的受限版本：所有来自同一个内部Tuple X的请求均被NAT转换至同一个外部Tuple Y，这与Full Cone相同，但不同的是，只有当内部主机曾经发送过报文给外部主机（假设其IP地址为Z）后，外部主机才能以Y中的信息作为目标地址和目标端口，向内部 主机发送UDP请求报文，这意味着，NAT设备只向内转发（目标地址/端口转换）那些来自于当前已知的外部主机的UDP报文，从而保障了外部请求来源的安 全性

**3. Port Restricted Cone NAT**：它是Restricted Cone NAT的进一步受限版。只有当内部主机曾经发送过报文给外部主机（假设其IP地址为Z且端口为P）之后，外部主机才能以Y中的信息作为目标地址和目标端 口，向内部主机发送UDP报文，同时，其请求报文的源端口必须为P，这一要求进一步强化了对外部报文请求来源的限制，从而较Restrictd Cone更具安全性

**4. Symmetric NAT**：这是一种比所有Cone NAT都要更为灵活的转换方式：在Cone NAT中，内部主机的内部Tuple与外部Tuple的转换映射关系是独立于内部主机所发出的UDP报文中的目标地址及端口的，即与目标Tuple无关； 在Symmetric NAT中，目标Tuple则成为了NAT设备建立转换关系的一个重要考量：只有来自于同一个内部Tuple 、且针对同一目标Tuple的请求才被NAT转换至同一个外部Tuple，否则的话，NAT将为之分配一个新的外部Tuple；打个比方，当内部主机以相 同的内部Tuple对2个不同的目标Tuple发送UDP报文时，此时NAT将会为内部主机分配两个不同的外部Tuple，并且建立起两个不同的内、外部 Tuple转换关系。与此同时，只有接收到了内部主机所发送的数据包的外部主机才能向内部主机返回UDP报文，这里对外部返回报文来源的限制是与Port Restricted Cone一致的。不难看出，如果说Full Cone是要求最宽松NAT UDP转换方式，那么，Symmetric NAT则是要求最严格的NAT方式，其不仅体现在转换关系的建立上，而且还体现在对外部报文来源的限制方面。

近来公网免费的nat检测，已经越来越不能提供服务了。因此，我们需要搭建一套自己的nat检测服务。

**设计方案：**

需要peer和服务器双方面的修改。设备方面，预计需要2台低配的服务器即可。但是服务器要求有2个公网ip。

检测方案如下：

第一步：检测客户端是否有能力进行UDP通信以及客户端是否位于NAT后？

Peer带上自己的local endpoint 向服务器（ip1，port1）发包，要求返回服务器看到的peer endpoint。同时监听服务器的回报。超时1s，如果3次检测无回包，则客户端无法进行udp通讯。返回nat类型为 TYPE\_ERROR，检测结束

如果peer收到服务器回包，则对比 local endpoint 和 peer endpoint。如果相同，则nat类型为 TYPE\_PUBLIC，检测结束，否则下一步。

第二步：检测客户端NAT是否是Full Cone NAT？

Peer带上自己的local endpoint 向服务器（ip1，port1）发包，要求返回服务器用其他的endpoint（ip2，port2）返回看到的peer endpoint，同时监听服务器回包。如果能收到回包。那么返回nat类型为 TYPE\_FULLCONENAT，检测结束。如果3次超时，继续下一步。

第三步：检测客户端NAT是否是Symmetric NAT？

Peer向服务器的(ip1,port1)和(ip2,port2)发请求，要求返回服务器看到的peer endpoint1和peer endpoint2。这个过程如果网络没有问题，就能收到回应。（如果5次不能收到回应，返回nat类型为type\_error，检测结束）

如果 peer endpoint1 和 peer endpoint2 是不同的，返回nat类型为 TYPE\_SYMNAT，检测结束，否则继续检测。

第四步：检测客户端NAT是否是Restricted Cone NAT还是Port Restricted Cone NAT？

Peer向服务器(ip1,port1)发请求，要求服务用(ip1,port2)进行回应。 如果能收到回复，则nat类型为TYPE\_IP\_RESTRICTEDNAT，如果3次无回复，则nat类型为 TYPE\_IP\_PORT\_RESTRICTEDNAT

检测结束。

第五步：定时重新检测

TYPE\_ERROR 一天重新检测一次，进行了upnp的需要每天检测一次。外网节点可以一周检测一次。