**NAT的四种类型**

简述

基于UDP的P2P应用需要考虑NAT的类型，因为不同的NAT组合的穿透的方式并不一致，有的能通， 有的不能通。

一般来讲， NAT可以分为四种类型，分别是:

1, 全锥型(Full Cone)

2,  受限锥型(Restricted Cone)， 或者说是IP受限锥型

3,  端口受限锥型(Port Restricted Cone), 或者说是IP + PORT受限锥型

4,  对称型(Symmetric)

其中1,2,3属于同一种类型，都是锥型，区别只是路由器的不同的安全策略。

还有些NAT不属于这四种中的任何一种，就不在本文的讨论范围了。

为什么有四种类型的NAT

NAT缓解了IPV4地址不够用的问题，同时也也带了限制，那就是NAT外部的主机无法主动跟位于NAT内部的主机通信，NAT内部主机想要通信，必须主动和公网的一个IP通信，路由器负责建立一个映射关系，从而实现数据的转发， 这就是NAT的工作原理。

假定

公网server1 ip是1.1.1.1， 监听端口是1111

公网server2 ip是2.2.2.2， 监听端口是2222

NAT router ip是8.8.8.8

NAT内部client是192.168.0.3

client发送数据的时候，不管是tcp还是udp必须本地绑定一个端口，一般来讲，这个过程都是自动的。

假定client(192.168.0.3, 100)给 server(1.1.1.1, 1111)发送报文，报文到达路由器，路由器在自己的公网ip上开辟一个端口800，从而建立了一个隐射关系(8.8.8.8, 800)<--->(192.168.0.3, 100),  建立映射关系后，所以(192.168.0.3, 100)和(1.1.1.1, 1111)之间的报文都通过这个映射关系进行转发。

NAT之间主要的区别分两种情况讨论

1:

client(192.168.0.3, 100)和server(1.1.1.1, 1111)在路由器上建立好映射关系后，如果client(192.168.0.3, 100)又给(2.2.2.2, 2222)发送数据，路由器该怎么处理呢?

1,  复用旧的映射关系(8.8.8.8, 800)<--->(192.168.0.3, 100)和(2.2.2.2, 2222)通信, 这就是锥型(Cone) NAT

2,  创建新的映射关系(8.8.8.8, 801)<--->(192.168.0.3, 100)和(2.2.2.2, 2222)通信, 这就是对称型NAT

注:  (8.8.8.8, 801)只是举例，到底用什么端口取决于路由器的端口管理策略，总之是另外的一个端口，有的路由器有多个公网IP，不同的IP也会参与到这个映射关系中。

2:

client(192.168.0.3, 100)和server(1.1.1.1, 1111)在路由器上建立好映射关系后，如果这个时候路由器(8.8.8.8)在800端口上收到从另外一台server(2.2.2.2, 2222)发来的数据，是不是应该转发给(192.168.0.3, 100)呢？

有四种情况:

1, 无条件转发给(192.168.0.3, 100)， 这就是全锥型(Full Cone)NAT。

2, 如果(192.168.0.3, 100)之前给(2.2.2.2)发送过数据，则转发， 这就是受限锥型(Restricted Cone)。

3, 如果(192.168.0.3, 100)之前给(2.2.2.2, 2222)发送过数据，则转发， 这就是端口受限锥型(Port Restricted Cone)。

4, 丢弃报文，拒绝转发, 这就是对称型NAT。

从上面也描述也可以看出，安全性系数,  对称型 > 端口受限锥型 > 受限锥型 > 全锥型

不同NAT的穿透性

NAT有10种组合

|  |  |  |
| --- | --- | --- |
| 全锥型 | 全锥型 | **✓** |
| 全锥型 | 受限锥型 | **✓** |
| 全锥型 | 端口受限锥型 | **✓** |
| 全锥型 | 对称型 | **✓** |
| 受限锥型 | 受限锥型 | **✓** |
| 受限锥型 | 端口受限锥型 | **✓** |
| 受限锥型 | 对称型 | **✓** |
| 端口受限锥型 | 端口受限锥型 | **✓** |
| 端口受限锥型 | 对称型 | **✘, 无法打通** |
| 对称型 | 对称型 | **✘, 无法打通** |



