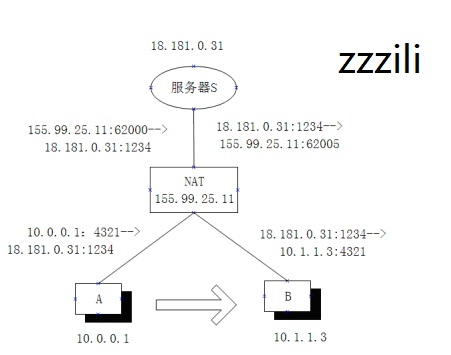
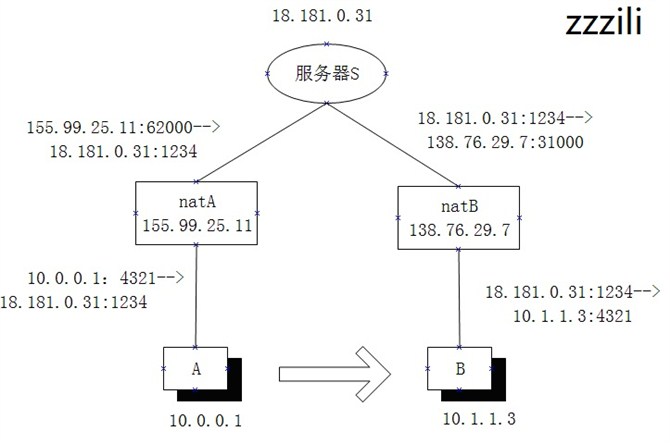
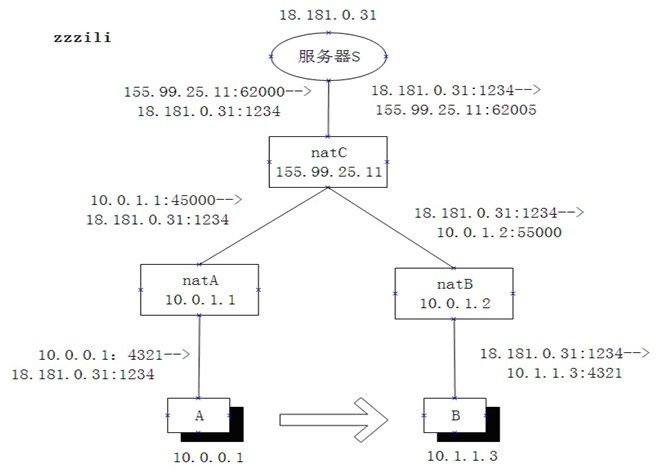
因为当前 IPV4地址的缺乏 ,nat、防火墙的中介设备和不对称寻址建立起来的 p2p通信机制造成了地址访问的问题。   
  
在 internet最初体系结构中，每个节点都有全球唯一的 ip地址，能够直接通信。可是随着节点的增多， ip地址使用紧张，他们需要中介设备如 nat连在一起。   
私有网络中的节点可以直接连接到相同私有网络中的其他节点，也可以连接到全局地址空间中拥有全球唯一 ip地址的节点。。然而 nat通常只允许临时的向外连接申请，对于向内的申请会拒绝。这就造成了在 natA内网中的节点 A连接 natB内网中的节点 B时连接申请报到 natB时就被阻止了。此时我们需要的就是穿越技术。。。   
    
总体来说穿越技术是利用一个公共服务器中转，使节点 A、 B都连接到中转服务器 S之后，通过 S中转 A发送到 B的数据报或者是中转连接申请，，使 A、 B对于 natA和 natB来说都是向外申请。。。   
    
1、         中转数据报： A、 B都先向外与服务器 S建立接连，然后通过 S中转 A、 B之间的数据报。。   
2、         反向连接：当 A、 B都与 S建立了连接，并且只有一个节点在 nat之后（假设 A在 natA之后）。。当 B向 A申请连接时，申请背 natA拒绝。 B可以向 S提出申请要与 A建立连接，然后 S向 A发出指令，通知 A主动向 B申请建立连接。。   
【 UDP打洞】   
1、 A、 B在同一个 nat之后：   
   
  
  
  
  
  
用户 A让 S做介绍人来与 B建立对话   
（1） A向 S发送一个消息请求与 B建立连接   
（2） S使用 B的公共终端（ 155.99.25.11： 62005）和私有终端（ 10.1.1.3）响应 A   
（3） 同时 S也想 B发送 A的公共终端（ 155.99.25.11： 62000）和私有终端（ 10.0.0.1），但是发送到公共终端的消息不一定能达到 B取决于 NAT是否支持“发夹”转化（回环转化）   
（4） 如果 nat支持发夹转化的话，应用程序就可以免除私有和共有终端都要试图连接的复杂性。。   
    
    
2、         不同 NAT后面的节点   
    
（1） 注册， A、 B都想服务器 S注册 natA安排了 62000端口用作 A和 S对话使用， natB安排了 31000端口用作 B和 S对话使用， A向 S的注册消息中报告了自己的私有终端 10.0.0.1： 4321这种情况下 A的公共终端是 155.99.25.11： 62000，同理 B的私有终端 10.1.1.3： 4321和公共终端 136.76.29.7： 31000   
（2） A发送请求消息到 S，请求与 B建立连接，作为响应 S向 A发送了 B的私有终端和公共终端也向 B发送了 A的私有和公共终端。   
（3） 既然 A、 B处在不同的子网中，那么 A、 B的私有终端是不能公共路由的，发送的消息肯能会发到自己子网中的 ip中（应为不同子网中的私有 ip可以相同）   
（4） 当从 A发向 B的第一个消息到达 natA时， natA注意到这是一个新的外出会话， natA看到源地址是子网中地址，而目的地址是外网地址，所以 natA将从私有终端 10.0.0.1： 4321的外出会话转化到对应公共终端 155.99.25.11： 62000，这样 A的第一个到 B的公共终端的外出会话消息就在 natA上“打了一个洞”。新的 UDP会话由 A的私有网络上的终端 10.0.0.1： 4321/138.76.29.7： 31000和 internet上的公共终端 155.99.25.11： 62000/138.76.29.7:31000标识，同理 B也建立了对 A的私有、公共连接标识。   
（5） 如果 A发向 B的公共终端的消息在 B发向 A的第一个消息穿过 B自己的 natB之前到达了 natB的话， natB会认为 A的内入消息是禁止的，丢弃 B的请求消息，但是 B的请求消息在 natB上为 A打了一洞，此时洞双向打开，通信可以进行下去了。。。   
3、         多级 NAT后面的节点：   
    
（ 1） A、 B都建立与 S的向外连接   
（ 2）最终连接目的：   
   Aà B    10.0.0.1à 10.0.1.2:55000   
   Bà A    10.0.0.3à 10.0.1.1:45000   
（ 3）但是在此时 A、 B无法知道伪公众终端 10.0.1.2:55000和 10.0.1.1:45000。 S只看到了 155.99.25.11： 32000和 155.99.25.11： 62005。   
（ 4）此时相应的 A、 B也只知道 155.99.25.11： 32000和 155.99.25.11： 62005   
（ 5）只能依赖 natC的发夹转化。   
     当 A-à B，即 10.0.0.1—>155.99.25.11： 62005时 natA将数据报中源地址 10.0.0.1转化为 10.0.1.1然后发送到 natC，当 natC发现目的地址 ip是 155.99.25.11是自己转化过的 ip后， natC就会转化数据报中的源地址和目的地址，再发送到私有网络中。 155.99.25.11： 62000--à 10.0.1.2： 55000   
（ 6）当数据报到 B私有网络时，同样方法进行转化。。