实现 NAT 穿越的 P2P 即时通讯技术研究

袁健　隋树林　张文霞
青岛科技大学　自动化与电子工程学院 山东 青岛 （266042）

E-mail:jyuanjian801209@163.com

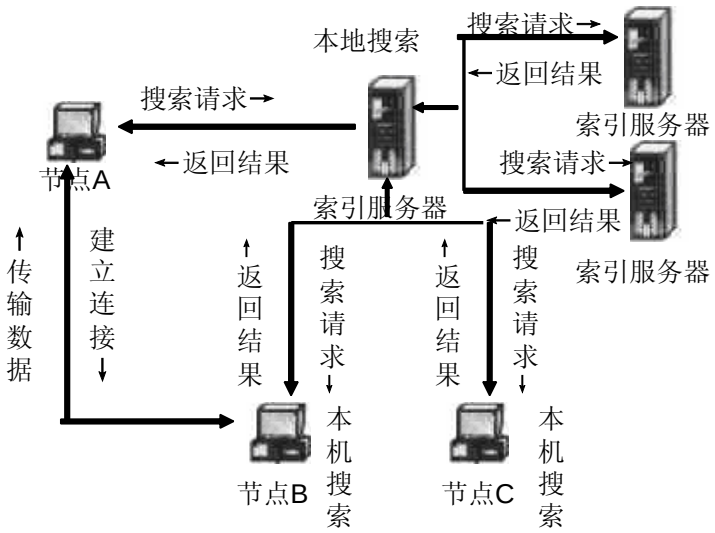
摘　要: 本文介绍了基于 internet 的 P2P 网络技术和 NAT 基本原理，提出了通过一台 internet 注册服务器，利用 UDP 实现 P2P 网络穿越 NAT 的即时通讯技术，并给出一个通讯程序仿真实例。

关键字: P2P, NAT,UDP

1　P2P 网络简介(introduction)

P2P技术[1,2]源于局域网共享，其目标是改变人们通过服务器中转交换文件的传统方式，达到自由交换资源的目的。IBM为P2P下了如下定义：系统由若干互联协作的计算机构成，且至少具有如下特征之一：系统依存于边缘化（非中央式服务器）设备的主动协作，每个成员直接从其他成员而不是从服务器的参与中受益；系统中成员同时扮演服务器与客户端的角色；系统应用的用户能够意识到彼此的存在，构成一个虚拟或实际的群体。P2P网络是互联网整体架构的基础，互联网最基本的 TCP/IP协议并没有客户端和服务器的概念，在通讯过程中，所有的设备都是平等的一端。P2P 技术改变了“内容”所在的位置，使其正在从“中心”走向“边缘”，也就是说不再如C\S模式将内容存于主要的服务器上，而是存在所有用户的 PC 机上。广义的P2P 网络[1,2]将 P2P网络划分为纯分散式 P2P网络(如gnutella模型[9])、超级结点式网络和混合式 P2P网络[7] 等大类。

本文所讨论的通讯技术属于混合式 P2P 网络，各节点之间可以直接建立连接，但网络的构建需要服务器，通过集中认证，建立索引机制。但是这里的服务器仅用于辅助对等节点之间建立连接，对等节点之间直接进行通信，这不同于 C/S 模式中的服务器。如图 1 所示：



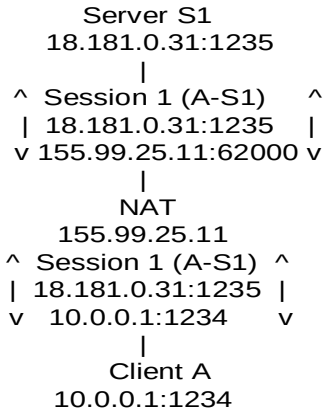
图表 1

Fig. 1 preferred communication model of P2P

2　NAT 基本原理(principle)

NAT的基本功能[3]就是通过一个或几个IP地址,来实现局域网上的所有PC机都可以对

Internet进行访问。NAT技术可以为TCP、UDP以及ICMP的部分信息进行透明中继。NAT技术具体实现方法是通过IP地址映射来实现IP地址的复用。NAT网关充当了路由器的角色,所有外出的网络包都必须路由到NAT网关；同样,所有由外网发往内网的网络包也必须经过NAT网关。NAT网关通过一定的规则,将由内部网向外部网发送的数据包中的源地址映射为一个Internet合法地址,而将由外向内的数据包中的目的地址替换成相应的内网IP地址。NAT网关有内网接口和外网接口,其中外网接口和Internet相连,必须拥有合法IP地址,内网接口则和内网相连,可以分配任意指定的一个内网IP地址,一般情况下,这个IP地址就是内部主机的默认网关。有一个私有网络 10.*.*.*，Client A是其中的一台计算机，这个网络的网关（一个NAT设备）的外网IP是 155.99.25.11(一个内网的IP地址，比如 10.0.0.10)。如果Client A中的某个进程（这个进程创建了一个UDP Socket,这个Socket绑定 1234 端口）想访问外网主机 18.181.0.31 的 1235 端口。 首先NAT会改变这个数据包的原IP地址，改为 155.99.25.11。接着NAT会为这个传输创建一个Session，且给这个Session分配一个端口，比如 62000，然后改变这个数据包的源端口为 62000。所以本来是（10.0.0.1:1234->18.181.0.31:1235）的数据包到了互联网上变为了（155.99.25.11:62000->18.181.0.31:1235）。 一旦NAT创建了一个Session后，NAT会记住 62000 端口对应的是 10.0.0.1 的 1234 端口，以后从 18.181.0.31 发送到 62000 端口的数据会被NAT自动的转发到 10.0.0.1 上。(注意：这里是说18.181.0.31发送到62000端口的数据会被转发,其他的IP发送到这个端口的数据将被NAT抛弃）这样Client A就与Server S1 建立以了一个连接。如图 2 所示：

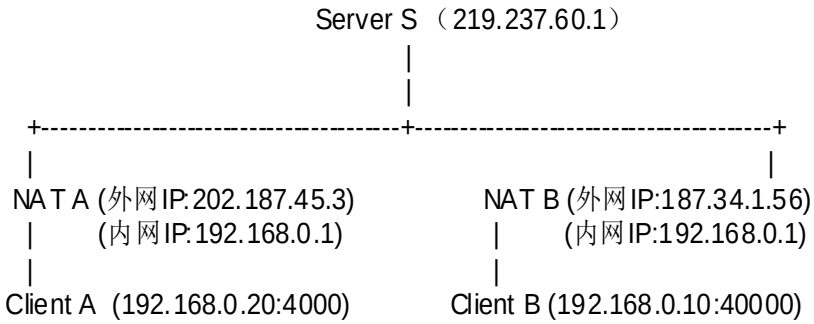


图表 2

Fig. 2 communication principle of NAT

3. 用 UDP 实现 P2P 网络中穿越 NAT 通讯(communication case)

虽然 NAT 的存在禁止外网主动连接内网,但是在 IPv6 没有全面实施之前,NAT 仍然是解 IPv4 地址短缺的主要方法,同时 NAT 也是构建 Internet 防火墙保护网络安全的重要手段。然而,P2P 成千上万的内网中的主机需要对等交换信息和 Internet 资源共享,P2P 穿越 NAT:即外网主主动访问内网主机或位于不同 NAT 之后的不同内网中的主机之间对等连接是 P2P 应用中必须要解的问题。图 3 是一个实例。



图表 3

Fig. 3 sketch map between two communicating users

例如AB两台机器分别处于两个不同的局域网后，由Server做中介，先看连接过程。 A首先连接服务器，采用UDP发包给Server，这个包包括了A的用户信息。Server方，可以用CSocket::GetPeerName()得到A的IP及端口，但得到的IP和端口应该是A的代理网关的公网PublicIP及其映射端口NatPort，该映射端口就是A的代理网关为A的本次UDP通信临时分配的Nat端口。可以断言，得到的端口一定不是A的内网IP和内网UDP端口。后将A的公网IP、映射端口、用户信息等保存到(内存列表或者数据库)，这样标志着A已经上线。服务器马上将其它在线的用户信息发回给A，包括其它用户的代理网关的公网IP及Nat端口。A同样将在线用户的这些信息保存并显示为列表，期待A用户做出选择。对于B，同样有上述过程。当A用户做出选择，要和在线的B用户通信时，A首先发UDP包给B的公网IP及Nat端口，并立即发一个UDP包给服务器，让服务器去通知B，叫B给A也发一个UDP包给A。换句话说：step1.A发包给PublicB. step 2.A发包给Server. step3.Server发包给PublicB. step 4.B发包给PublicA。上面的叙述用到了"Public"字样，它代表代理网关的公网IP及其映射端口。由于A和B各自的网关都保存了各自的端口映射关系，发到网关的数据，网关会按照这个映射关系转发给A和B。当A和B都分别收到对方发来的UDP包以后，连接宣告成功，服务器即可以脱离，AB即可以实现UDP通信。

4 关键程序仿真结果(simulation)

下面是一个P2P通讯程序的关键代码以及仿真结果，P2P Server运行在IP地址为 211.64.212.209 的计算机上，两个P2P Client分别运行在IP地址为 211.64.212.209 和 211.64.212.210 的计算机上；两台计算机通过小型交换机相连。该仿真只是为了验证原理，对异常并没有做过多得处理，后登录的计算机可以获得先登录计算机的用户名，登录的计算机通过send username message的格式来发送消息。如果发送成功，证明已与对方直接连接。此外，两个客户端运行在一个NAT后，程序能否运行正常，取决于NAT是否支持loopback translation，详见[6]。程序现在支持三个命令：send ， getu ， exit。

send 格式：send username message

功能：发送信息给 username

getu 格式：getu

功能：获得当前服务器用户列表

exit 格式：exit

功能：注销与服务器的连接

```
class CClientSocket : public CSocket
{ public: virtual void OnReceive( int nErrCode );
```

```
}void CClientSocket::OnReceive( int nErrCode ) {
int nFlag, *pFlag; //UDP 包标志，位于包头 4 个字节
……
if(lstrcmp(PeerIP,ServerIP)==0)//如果是服务器返回的信息
{switch( nFlag ){
case 0: //标识和服务器连接成功，RecBuf 是服务器返回的其它在线用户的信息(包括对方的公网 IP 及端口)，这里假定是 B 的信息.从 RecBuf 取出 B 的代理网关的 IP 和端口放入 PeerIP 和 PeerPort。接下来，给 B 的代理公网 IP 发一个 UDP 包,填充 RecBuf，并使标志为 0
SendTo( RecBuf, 64, PubPort, PubIP ); //马上叫服务器通知 B，要 B 给 A(本进程)发一个 UDP 包，填充 RecBuf，并使标志为 1
SendTo( RecBuf, 64, ServerPort, ServerIP );
break;
case 1: //标识是来自服务器的通知，叫 B 发一个 UDP 给 A ，RecBuf 里有 A 的代理公网 IP 和端口，取出来，放入 PeerIP 和 PeerPort
……
//给 A 发一个 UDP 包，填充 RecBuf，并使标志为 1
SendTo( RecBuf, 64, PubPort, PubIP );
break;default: break; } }
else //其它对等客户返回的信息
{ switch( nFlag ) {
case 0: //标识直接收到 A 发的 UDP 包
break;
case 1: //标识是 B 发回的 UDP 包，但是靠服务器通知 B 发的。至此，可以判断 AB 互相是否连接成功，就是判断 A 发给 B 的 UDP 包 B 收到，而 B 发给 A 的 UDP 包 A 也收到，那么连接就是成功的。否则重复上面的过程。
break; default: break;
} } }
```

仿真结果(如图 4)

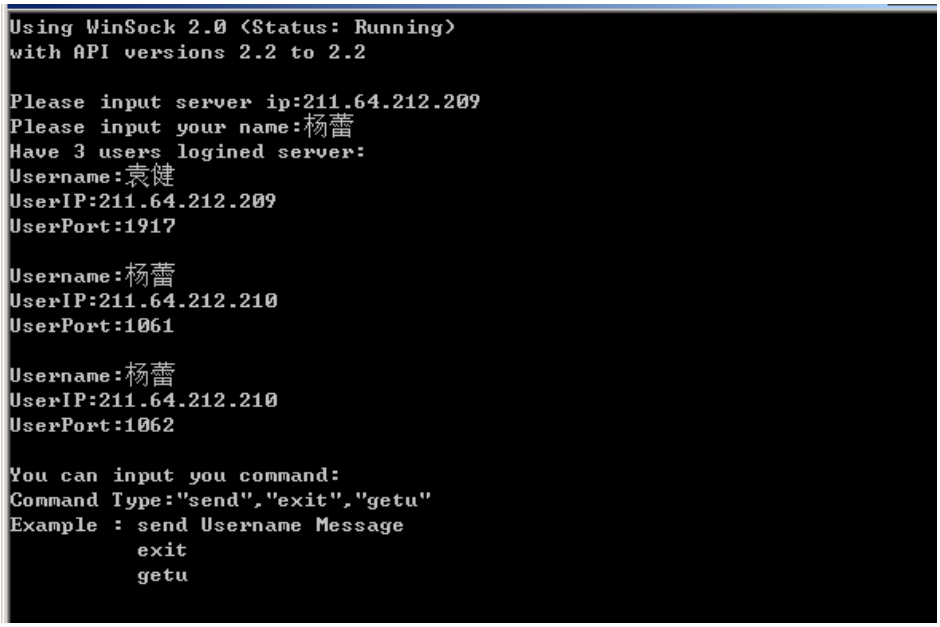
1) 某一用户登陆，输入服务器的 IP 地址，用户的昵称，系统自动识别用户的 IP 地址和端口号

图表 4

Fig .4 logining simulation(1)-one logined user

2)又一用户登陆，登陆操作不变，但后登陆的用户可获得已经登陆用户的信息。

如果同一用户再次登陆系统将自动分配另一个端口号与改用户的进程（如图5)。



图表 5

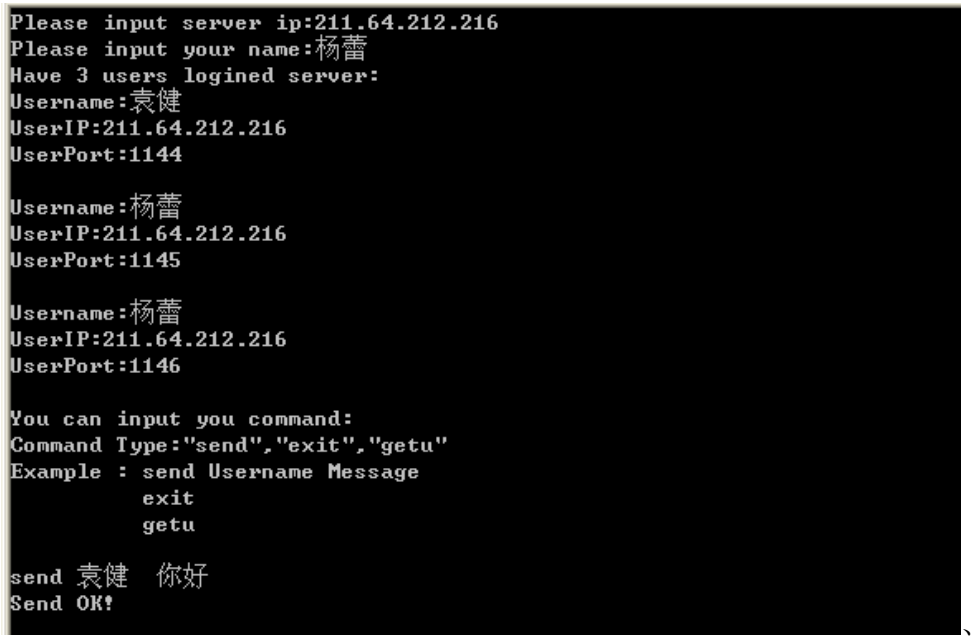
Fig. 5 logining simulation(2)-another logined user

3）服务器显示已经登陆的用户名单（如图6)。

图表 6 服务器显示的信息

Fig 6 logining simulation(3)-display of server

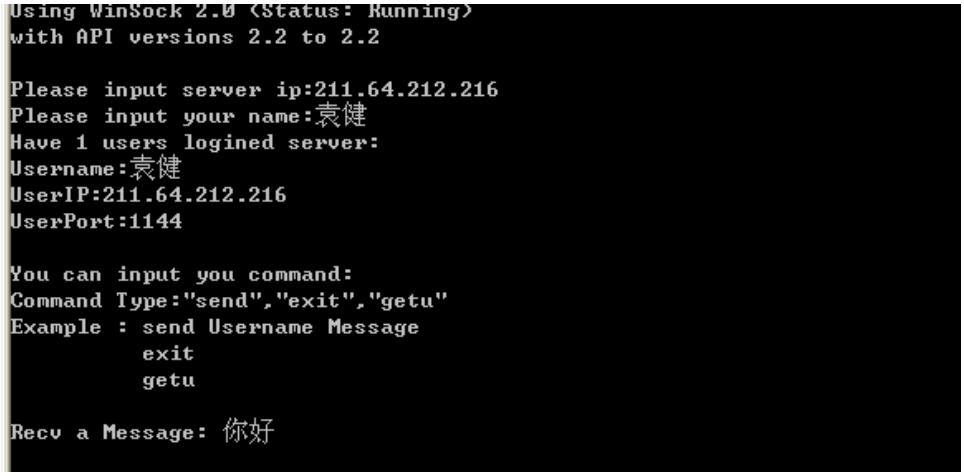
4）用户间进行相互通讯（如图 7 所示）



图表 7 信息发送

Fig.7 send massages

5)接收方收到信息（如图 8 所示）



图表 8 收到信息

Fig.8 receive a message from one user

结束语 (conclusion)

本文实现了通过一台internet注册服务器，利用UDP实现P2P网络穿越NAT的即时聊天技术。由于P2P技术在对等计算、协同工作方面的强大优势，今后肯定会在这两个方面迅猛发展；但由于P2P 技术本身存在不易管理、安全性差等缺陷[2][10]成P2P技术自出现以来，并没有大规模应用，而且这两个问题如果得不到有效解决，将会成为P2P技术在这两个方面发展的的主要瓶颈。目前已有许多人开始从集群技术、人工智能、专家数据库、个人防火墙等方面[2, 4, 5]来试图解决这两个问题。这些都将是我们关注的热点研究领域。

参考文献

[1] 吕向辰 P2P 技术与应用 计算机世界[J] 2002.12

[2] 张联峰,刘乃安 综述：对等网（P2P）技术 计算机工程与应用 2003.12

[3] 李河 ,王树明 P2P 网络中使用 UDP 穿越 NAT 的方法研究 吉林大学学报(信息科学版)

[4]ChunchuanXu Application ofPeer-to-peer[DB/OL].http://netserver.cerc.wvu.edu/classes/cs491h-summer2-2001/Xu-p2papplications/Presentation%20paper.doc,2001.

[5]RyanSit,MikeSemanko.TheFutureoftheDecentralizedModelofP2PFile-Sharing[DB/OL] http://www.cs.ucsd.edu/classes/wi01/cse222/projects/reports/ournet-12.pdf,2001

[6] http://midcom-p2p.sourceforge.net/draft-ford-midcom-p2p-01.txt

[7] 胡放明，李俊兵，贺贵明等 对 P2P 网中发现机制的研究 计算机应用 Vol.24,No.6 June,2004

[8]李祖鹏， 黄道颖，庄雷等 Peer-to-Peer 网络模型研究 计算机工程 Vol.30,No.12, June,2004

[9] 黄道颖，李祖鹏，庄雷等 基于主动网络的分布式 P2P 网络模型 软件学报 Vol.15,No.7,2004

[10] 赵双红，刘寿强 P2P 通信网络安全问题探析 计算机安全[J] 2003，11

Research On Real-time Communication Technology About P2P Achieving Traversion of NAT

Yuan jian Sui shulin Zhang wenxia

(College of automatization and electronic engeering ,Qingdao University Of Science & Technology, Qingdao,Shandong 266042)

Abstract

The network technique of peer-to-peer based on Internet and the keystone of Net-Address-Transfer are introduced,and the real-time communication technique, that is the network of peer-to-peer traverse NAT with User Datagram Protocol through an enrolled server on the internet, is also proposed in this paper.Also we present a simulated instance of communication programme.

Keywords: Peer-to-Peer,Net-Address-Transfer, User Datagram Protocol