(19)中华人民共和国国家知识产权局

(12)发明专利

(10)授权公告号 CN 101217536 B
(45)授权公告日 2011.11.09

(21)申请号 200710306339.4

(22)申请日 2007.12.28

(73)专利权人 腾讯科技(深圳)有限公司
地址 518044 广东省深圳市福田区振兴路赛格科技园2栋东410室

(72)发明人 王志华

(74)专利代理机构 北京德琦知识产权代理有限公司 11018
代理人 谢安昆 宋志强

(51)Int.Cl.
H04L 29/06(2006.01)

(56)对比文件
CN 1917512 A,2007.02.21,说明书第5页第11行-第6页第10行,图5,6.
CN 1805388 A,2006.07.19,全文.
WO 2007/041417 A1,2007.04.12,全文.
US 2006/0182100 A1,2006.08.17,全文.
US 2006/0072569 A1,2006.04.06,全文.

审查员 蔡茹辛

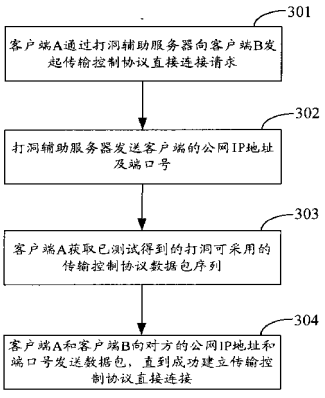
权利要求书 6 页 说明书 11 页 附图 5 页

(54)发明名称

穿越网络地址转换设备/防火墙的方法、系统及客户端

(57)摘要

本发明公开了一种穿越网络地址转换设备/防火墙的方法,该方法包括:第一客户端通过打洞辅助服务器向第二客户端发起传输控制协议直接连接请求;打洞辅助服务器将第一客户端的公网IP地址及端口号发送给第二客户端,并将第二客户端的公网IP地址及端口号发送给第一客户端;第一客户端获取已测试得到的打洞可采用的传输控制协议数据包序列;第一客户端和第二客户端在打洞辅助服务器的协助下,按照所述打洞可采用的传输控制协议包序列,向对方的公网IP地址和端口号发送数据包,直到成功建立传输控制协议直接连接。本发明还相应的公开了与所述方法对应的系统及客户端。本发明实施例提供的技术方案提高了穿越网络转换设备的成功率。



CN 101217536 B

1. 一种穿越网络地址转换设备 / 防火墙的方法，其特征在于，包括：

第一客户端和第二客户端利用测试服务器测试网络地址转换设备的类型；

若第一客户端判断得到用户数据报协议包无法通过或者业务层要求使用传输控制协议打洞，则第一客户端获取已存的打洞环境测试结果，使用传输控制协议打洞；

否则，第一客户端判断能否进行打洞，若能，则第一客户端根据网络地址转换设备的类型，使用用户数据报协议打洞，否则，触发超级节点中转数据；

所述使用传输控制协议进行打洞具体包括：

第一客户端通过打洞辅助服务器向第二客户端发起传输控制协议直接连接请求；

打洞辅助服务器将第一客户端的公网 IP 地址及端口号发送给第二客户端，并将第二客户端的公网 IP 地址及端口号发送给第一客户端；

第一客户端获取已测试得到的打洞可采用的传输控制协议数据包序列；

第一客户端和第二客户端在打洞辅助服务器的协助下，按照所述打洞可采用的传输控制协议包序列，向对方的公网 IP 地址和端口号发送数据包，直到成功建立传输控制协议直接连接。

2. 如权利要求 1 所述的方法，其特征在于，进一步包括：

第一客户端向测试服务器发送第一同步数据包，

若第一客户端接收到测试服务器返回的第二同步数据包，则由所述第一同步数据包和第二同步数据包构成的序列为可用于打洞的第一传输控制协议包序列；

若第一客户端接收到测试服务器返回的互联网控制消息协议包和第二同步数据包，则由所述第一同步数据包，互联网控制消息协议包，及第二同步数据包构成的序列为可用于打洞的第二传输控制协议包序列；

若第一客户端接收到测试服务器返回的互联网控制消息协议包和同步数据包确认消息，则由所述第一同步数据包，互联网控制消息协议包，及同步数据包确认消息构成的序列为可用于打洞的第三传输控制协议包序列；

若第一客户端接收到测试服务器返回的复位消息以及第二同步数据包，则由所述第一同步数据包，复位消息以及第二同步数据包构成的序列为可用于打洞的第四传输控制协议包序列；

若第一客户端接收到测试服务器返回的复位消息和同步数据包确认消息，则由所述第一同步数据包，复位消息和同步数据包确认消息构成的序列为可用于打洞的第五传输控制协议包序列。

3. 如权利要求 2 所述的方法，其特征在于，若打洞可采用的传输控制协议包序列为所述第一传输控制协议包序列，则第一客户端获取已测试得到的打洞可采用的传输控制协议数据包序列之后进一步包括：

第一客户端获取已存的环境测试结果，若测试结果为操作系统版本符合预置的版本条件，则所述第一客户端和第二客户端向对方发送数据包；

其中，所述第一客户端和第二客户端向对方发送数据包具体包括：

第一客户端通过打洞辅助服务器向第二客户端发送通知消息；

第一客户端向第二客户端的公网 IP 地址和端口号，发送第一同步数据包；

第二客户端在收到所述通知消息后，向第一客户端的公网 IP 地址和端口号，发送第二

同步数据包；

第一客户端和第二客户端在收到所述同步数据包后，向对方的公网 IP 地址和端口号返回同步数据包确认消息，至此第一和第二客户端成功建立传输控制协议直接连接。

4. 如权利要求 2 所述的方法，其特征在于，若打洞可采用的传输控制协议包序列为所述第二传输控制协议包序列，则第一客户端获取已测试得到的打洞可采用的传输控制协议数据包序列之后进一步包括：

第一客户端获取已存的环境测试结果，若测试结果为能够使用操作系统接口设置公网 IP 地址的 TTL 值，则所述第一客户端和第二客户端向对方发送数据包；

其中，所述第一客户端和第二客户端向对方发送数据包具体包括：

第一客户端通过打洞辅助服务器向第二客户端发送第一同步数据包，所述第一同步数据包携带第二客户端的公网 IP 地址的 TTL 值被设置为低；

打洞辅助服务器向第一客户端返回互联网控制消息协议包，所述协议包携带第一客户端的公网 IP 地址的 TTL 值被设置为过期；

打洞辅助服务器向第二客户端发送通知消息；

第二客户端在收到所述通知消息后，向第一客户端的公网 IP 地址和端口号发送第二同步数据包；

第一客户端收到所述第二同步数据包后，向第二客户端发送第二同步数据包确认消息，至此第一和第二客户端成功建立传输控制协议直接连接。

5. 如权利要求 2 所述的方法，其特征在于，若打洞可采用的传输控制协议包序列为所述第三传输控制协议包序列，则第一客户端获取已测试得到的打洞可采用的传输控制协议数据包序列之后进一步包括：

第一客户端获取已存的环境测试结果，若测试结果为操作系统版本符合预置的版本条件，能够使用操作系统接口设置公网 IP 地址的 TTL 值，并且用户具有超级用户权限，则所述第一客户端和第二客户端向对方发送数据包；

其中，所述第一客户端和第二客户端向对方发送数据包具体包括：

第一客户端和第二客户端通过打洞辅助服务器向对方发送同步数据包，所述同步数据包携带的公网 IP 地址的 TTL 值被设置为低；

打洞辅助服务器向第一客户端和第二客户端发送互联网控制消息协议包，所述协议包携带的公网 IP 地址的 TTL 值被设置为过期；

第一客户端和第二客户端通过打洞辅助服务器向对方发送传输控制协议序列号；

第一客户端和第二客户端在收到所述传输控制协议序列号后，向对方发送同步数据包确认消息，至此第一和第二客户端成功建立传输控制协议直接连接。

6. 如权利要求 2 所述的方法，其特征在于，若打洞可采用的传输控制协议包序列为所述第四传输控制协议包序列，则所述第一客户端和第二客户端向对方发送数据包具体包括：

第一客户端向第二客户端的公网 IP 地址和端口号对应的网络地址转换设备发送第一同步数据包；

所述网络地址转换设备向第一客户端的公网 IP 地址和端口号返回复位消息；

第一客户端通过打洞辅助服务器向第二客户端发送通知消息；

第二客户端在收到所述消息后，向第一客户端发送第二同步数据包；

第一客户端收到所述第二同步数据包后，向第二客户端返回同步数据包确认消息，至此第一和第二客户端成功建立传输控制协议直接连接。

7. 如权利要求 2 所述的方法，其特征在于，若打洞可采用的传输控制协议包序列为所述第五传输控制协议包序列，则第一客户端获取已测试得到的打洞可采用的传输控制协议数据包序列之后进一步包括：

第一客户端获取已存的环境测试结果，若测试结果为系统版本符合预置的版本条件，并且用户具有超级用户权限，则第一客户端和第二客户端向对方发送数据包；

其中，所述第一客户端和第二客户端向对方发送数据包具体包括：

第一客户端和第二客户端向对方的公网 IP 地址和端口号对应的网络地址转换设备发送同步数据包；

网络地址转换设备在收到所述同步数据包后，向对方的客户端返回复位消息；

第一客户端和第二客户端向对方的公网 IP 地址和端口号发送传输控制协议序列号；

第一客户端和第二客户端在收到对方的传输控制协议序列号后，向对方返回同步数据包确认消息，至此第一和第二客户端成功建立传输控制协议直接连接。

8. 一种第一客户端，其特征在于，包括：

网络地址转换设备类型测试单元，用于利用测试服务器测试网络地址转换设备的类型；

打洞方法选择单元，若判断得到用户数据报协议包无法通过或者业务层要求使用传输控制协议打洞，则触发直连请求发送单元，否则，判断能否进行打洞，若能，则触发用户数据包直连建立单元，否则，触发超级节点中转数据；

用户数据包直连建立单元，用于根据网络地址转换设备的类型，使用用户数据报协议打洞；

直连请求发送单元，用于通过打洞辅助服务器向第二客户端发起传输控制协议直接连接请求；

公网 IP 地址接收单元，用于接收打洞辅助服务器返回的第二客户端的公网 IP 地址及端口号；

包序列获取单元，用于获取已测试得到的打洞可采用的传输控制协议包序列；

直连建立单元，用于在打洞辅助服务器的协助下，按照所述打洞可采用的传输控制协议包序列，向第二客户端的公网 IP 地址和端口号发送数据包，直到成功建立传输控制协议直接连接。

9. 如权利要求 8 所述的客户端，其特征在于，所述客户端进一步包括：测试数据包发送单元，测试数据包接收单元，序列记录单元；

测试数据包发送单元，用于向测试服务器发送第一同步数据包，

测试数据包接收单元，用于接收测试服务器返回的数据包；

若测试数据包接收单元接收到的数据包是第二同步数据包，则序列记录单元，用于记录由所述第一同步数据包和第二同步数据包构成的序列为可用于打洞的第一传输控制协议包序列；

若测试数据包接收单元接收到数据包是互联网控制消息协议包和第二同步数据包，则

序列记录单元，用于记录由所述第一同步数据包，互联网控制消息协议包，及第二同步数据包构成的序列为可用于打洞的第二传输控制协议包序列；

若测试数据包接收单元接收到数据包是互联网控制消息协议包和同步数据包确认消息，则序列记录单元，用于记录由所述第一同步数据包，互联网控制消息协议包，及同步数据包确认消息构成的序列为可用于打洞的第三传输控制协议包序列；

若测试数据包接收单元接收到数据包是复位消息以及第二同步数据包，则序列记录单元，用于记录由所述第一同步数据包，复位消息以及第二同步数据包构成的序列为可用于打洞的第四传输控制协议包序列；

若测试数据包接收单元接收到数据包是复位消息和同步数据包确认消息，则序列记录单元，用于记录由所述第一同步数据包，复位消息和同步数据包确认消息构成的序列为可用于打洞的第五传输控制协议包序列。

10. 如权利要求 9 所述的客户端，其特征在于，若打洞可采用的传输控制协议包序列为所述第一传输控制协议包序列，则所述客户端进一步包括：

测试结果获取单元，用于获取已存的环境测试结果，若测试结果为操作系统版本符合预置的版本条件，则触发所述直连建立单元；

其中，所述直连建立单元具体包括：

同步数据包发送单元，用于向第二客户端的公网 IP 地址和端口号，发送第一同步数据包；

通知消息发送单元，用于通过打洞辅助服务器向第二客户端发送通知消息；

同步数据包接收单元，用于接收第二客户端在收到所述通知消息后，发送的第二同步数据包；

确认消息发送单元，用于在收到所述第二同步数据包后，向第二客户端发送同步数据包确认消息；

确认消息接收单元，用于接收第二客户端在收到第一同步数据包后，返回的同步数据包确认消息。

11. 如权利要求 9 所述的客户端，其特征在于，若打洞可采用的传输控制协议包序列为所述第二传输控制协议包序列，则所述客户端进一步包括：

测试结果获取单元，用于获取已存的环境测试结果，若测试结果为能够使用操作系统接口设置公网 IP 地址的 TTL 值，则触发所述直连建立单元；

其中，所述直连建立单元具体包括：

同步数据包发送单元，用于通过打洞辅助服务器向第二客户端发送第一同步数据包，所述第一同步数据包携带第二客户端的公网 IP 地址的 TTL 值被设置为低；

协议包接收单元，用于接收打洞辅助服务器返回的互联网控制消息协议包，所述协议包携带第一客户端的公网 IP 地址的 TTL 值被设置为过期；

通知消息发送单元，用于通过打洞辅助服务器向第二客户端发送通知消息；

同步数据包接收单元，用于接收第二客户端在收到所述通知消息后，发送的第二同步数据包；

确认消息发送单元，用于在收到所述第二同步数据包后，向第二客户端发送第二同步数据包确认消息。

12. 如权利要求 9 所述的客户端，其特征在于，若打洞可采用的传输控制协议包序列为所述第三传输控制协议包序列，则所述客户端进一步包括：

测试结果获取单元，用于获取已存的环境测试结果，若测试结果为操作系统版本符合预置的版本条件，能够使用操作系统接口设置公网 IP 地址的 TTL 值，并且用户具有超级用户权限，则触发所述直连建立单元；

其中，所述直连建立单元具体包括：

同步数据包发送单元，用于通过打洞辅助服务器向第二客户端发送同步数据包，所述同步数据包携带第二客户端的公网 IP 地址的 TTL 值被设置为低；

协议包接收单元，用于接收打洞辅助服务器返回的互联网控制消息协议包，所述协议包携带第一客户端的公网 IP 地址的 TTL 值被设置为过期；

序列号发送单元，用于通过打洞辅助服务器向第二客户端发送第一传输控制协议序列号；

序列号接收单元，用于接收打洞服务器发送来的第二客户端的第二传输控制协议序列号；

确认消息发送单元，用于在收到第二传输控制协议序列号后，向第二客户端发送同步数据包确认消息；

确认消息接收单元，用于接收第二客户端在收到第一传输控制协议序列号后，返回的同步数据包确认消息。

13. 如权利要求 9 所述的客户端，其特征在于，若打洞可采用的传输控制协议包序列为所述第四传输控制协议包序列，则所述直连建立单元具体包括：

同步数据包发送单元，用于向第二客户端的公网 IP 地址和端口号对应的网络地址转换设备发送第一同步数据包；

复位消息接收单元，用于接收所述网络地址转换设备返回的复位消息；

通知消息发送单元，用于通过打洞辅助服务器向第二客户端发送通知消息；

同步数据包接收单元，用于接收第二客户端在收到所述通知消息后，发送的第二同步数据包；

确认消息发送单元，用于在收到所述第二同步数据包后，向第二客户端返回同步数据包确认消息。

14. 如权利要求 9 所述的客户端，其特征在于，若打洞可采用的传输控制协议包序列为所述第五传输控制协议包序列，则所述客户端进一步包括：

测试结果获取单元，用于获取已存的环境的测试结果，若测试结果为操作系统版本符合预置的版本条件，并且用户具有超级用户权限，则触发所述直连建立单元；

其中，所述直连建立单元具体包括：

同步数据包发送单元，用于向第二客户端的公网 IP 地址和端口号对应的网络地址转换设备发送第一同步数据包；

复位消息接收单元，用于接收所述网络地址转换设备返回的复位消息；

序列号发送单元，用于向第二客户端的公网 IP 地址和端口号发送第一传输控制协议序列号；

序列号接收单元，用于接收第二客户端发送的第二传输控制协议序列号；

确认消息发送单元，用于在收到第二传输控制协议序列号后，向第二客户端返回同步数据包确认消息；

确认消息接收单元，用于接收第二客户端在收到第一传输控制协议序列号后，返回的同步数据包确认消息。

15. 一种穿越网络地址转换设备 / 防火墙的系统，其特征在于，包括：第一客户端，第二客户端，打洞辅助服务器；

测试服务器，用于测试网络地址转换设备的类型；

第一客户端，用于在测试服务器判断能进行打洞时，根据网络地址转换设备的类型，使用用户数据报协议打洞；

在测试服务器判断得到用户数据报协议包无法通过或者业务层要求使用传输控制协议打洞时，获取已存的打洞环境测试结果，通过打洞辅助服务器向第二客户端发起传输控制协议直接连接请求，并获取已测试得到的打洞可采用的传输控制协议包序列；

打洞辅助服务器，用于将第一客户端的公网 IP 地址及端口号发送给第二客户端，并将第二客户端的公网 IP 地址及端口号发送给第一客户端；

第一客户端和第二客户端在打洞辅助服务器的协助下，按照所述打洞可采用的传输控制协议包序列，向对方的公网 IP 地址和端口号发送数据包，直到成功建立传输控制协议直接连接。

16. 如权利要求 15 所述的系统，其特征在于，所述系统进一步包括：第一测试服务器和第二测试服务器；

第一测试服务器，用于协助第一客户端测试打洞可采用的传输控制协议包序列；

第二测试服务器，用于协助第二客户端测试打洞可采用的传输控制协议包序列。

穿越网络地址转换设备／防火墙的方法、系统及客户端

技术领域

[0001] 本发明涉及网络技术领域，尤其涉及一种穿越网络地址转换设备／防火墙的方法、系统及客户端。

[0002] 背景技术

[0003] 目前，互联网中存在大量的网络地址转换 (Network Address Translation，NAT) 设备。网络地址转换设备解决了 IPV4 地址不足的问题，但同时也给 P2P(Peer to Peer) 网络中客户端的直接连接设置了障碍。因此，在 P2P 网络中，需要克服网络地址转换设备产生的障碍，建立通信连接，。

[0004] 为实现上述目的，现有技术提出了一种 TCP 穿越网络地址转换设备的方法。请参见图 1，两个私网分别通过 NAT-A 设备 101 和 NAT-B 设备 102 连接到公网，NAT-A 设备 101 后面有一台客户端 A103，NAT-B 设备 102 后面有一台客户端 B104，打洞辅助服务器 105 用于协助客户端 A 和客户端 B 建立直接的 TCP 连接，即由客户端 B 向客户端 A 打一个洞，让客户端 A 可以沿这个洞直接连接到客户端 B，如同 NAT-B 设备不存在。现有的 TCP 穿越 NAT 设备的过程如下：

[0005] 1) 打洞辅助服务器启动两个端口侦听，一个为主连接侦听，一个为协助打洞侦听；

[0006] 2) 客户端 A 和客户端 B 分别与打洞辅助服务器的主连接保持联系；

[0007] 3) 当客户端 A 需要和客户端 B 建立直接的 TCP 连接时，客户端 A 首先连接打洞辅助服务器的协助打洞端口，并发送协助连接请求，同时在该端口启动侦听；

[0008] 4) 打洞辅助服务器收到客户端 A 的协助连接请求后，通过主连接向客户端 B 发送连接通知，并将客户端 A 经过 NAT-A 设备转换后的公网 IP 地址和端口号发送客户端 B；

[0009] 5) 客户端 B 收到连接通知后，首先与打洞辅助服务器的协助打洞端口连接，随便发送一些数据后立即断开，这样做的目的是让打洞辅助服务器记录客户端 B 经过 NAT-B 设备转换后的公网 IP 地址和端口号；

[0010] 6) 客户端 B 尝试与客户端 A 的公网 IP 地址和端口进行连接，目的是为了 NAT-B 设备记录客户端 A 的公网 IP 地址和端口号，为接下来真正的连接 做准备，这就是所谓的打洞，即客户端 B 为客户端 A 在 NAT-B 设备上打了一个洞；

[0011] 7) 客户端 B 在一切准备就绪以后通过主连接向打洞辅助服务器回复“已经准备好消息”；

[0012] 8) 打洞辅助服务器在收到上述回复消息后，将客户端 B 的公网 IP 地址和端口号发送给客户端 A；

[0013] 9) 客户端 A 在收到客户端 B 的公网 IP 地址和端口号等信息后，开始连接客户端 B 的公网 IP 地址和端口号，由于在步骤 6 中客户端 B 曾经尝试连接过客户端 A 的公网 IP 地址和端口号，因此，NAT-B 设备记录了此次连接的信息，所以当客户端 A 主动连接客户端 B 时，NAT-B 设备会认为客户端 A 发送来的同步数据包 (synchronize，SYN) 是合法数据，允许通过，从而建立直接的 TCP 连接。

[0014] 在对现有技术的研究和实践过程中，发明人发现现有技术的缺点是：穿越 NAT 设备的成功率很低，只有在特定的环境下才能成功。这是因为步骤 6 客户端 B 尝试与客户端 A 的公网 IP 地址和端口号进行连接时，有些 NAT 设备会认为这是一个非法的连接请求，此时，NAT-A 设备会向客户端 B 发送一个复位消息 (Reset the connection，RST)，要求客户端 B 和 NAT-B 设备复位，这会导致 NAT-B 设备清除其记录的客户端 A 的公网 IP 地址和端口号，当步骤 9 客户端 A 主动连接客户端 B 时，由于 NAT-B 设备上没有客户端 A 的记录，因此，NAT-B 设备认为客户端 A 的连接请求是非法的，从而拒绝客户端 A 的连接请求，TCP 直接连接失败。

[0015] 发明内容

[0016] 本发明实施例要解决的技术问题是提供一种穿越网络地址转换设备 / 防火墙的方法、系统及客户端，能够保证很高的穿越网络转换设备的成功率。

[0017] 为解决上述技术问题，本发明所提供的实施例是通过以下技术方案实现的：

[0018] 本发明实施例提供了一种穿越网络地址转换设备 / 防火墙的方法，包括：

[0019] 第一客户端和第二客户端利用测试服务器测试网络地址转换设备的类型；

[0020] 若第一客户端判断得到用户数据报协议包无法通过或者业务层要求使用传输控制协议打洞，则第一客户端获取已存的打洞环境测试结果，使用传输 控制协议打洞；

[0021] 否则，第一客户端判断能否进行打洞，若能，则第一客户端根据网络地址转换设备的类型，使用用户数据报协议打洞，否则，触发超级节点中转数据；

[0022] 所述使用传输控制协议进行打洞具体包括：

[0023] 第一客户端通过打洞辅助服务器向第二客户端发起传输控制协议直接连接请求；

[0024] 打洞辅助服务器将第一客户端的公网 IP 地址及端口号发送给第二客户端，并将第二客户端的公网 IP 地址及端口号发送给第一客户端；

[0025] 第一客户端获取已测试得到的打洞可采用的传输控制协议数据包序列；

[0026] 第一客户端和第二客户端在打洞辅助服务器的协助下，按照所述打洞可采用的传输控制协议包序列，向对方的公网 IP 地址和端口号发送数据包，直到成功建立传输控制协议直接连接。

[0027] 本发明实施例还提供了一种第一客户端，包括：

[0028] 网络地址转换设备类型测试单元，用于利用测试服务器测试网络地址转换设备的类型；

[0029] 打洞方法选择单元，若判断得到用户数据报协议包无法通过或者业务层要求使用传输控制协议打洞，则触发直连请求发送单元，否则，判断能否进行打洞，若能，则触发用户数据包直连建立单元，否则，触发超级节点中转数据；

[0030] 用户数据包直连建立单元，用于根据网络地址转换设备的类型，使用用户数据报协议打洞；

[0031] 直连请求发送单元，用于通过打洞辅助服务器向第二客户端发起传输控制协议直接连接请求；

[0032] 公网 IP 地址接收单元，用于接收打洞辅助服务器返回的第二客户端的公网 IP 地址及端口号；

[0033] 包序列获取单元，用于获取已测试得到的打洞可采用的传输控制协议包序列；

[0034] 附图说明

[0035] 直连建立单元，用于在打洞辅助服务器的协助下，按照所述打洞可采用的传输控制协议包序列，向第二客户端的公网 IP 地址和端口号发送数据包，直到成功建立传输控制协议直接连接。

[0036] 本发明实施例还提供了一种穿越网络地址转换设备 / 防火墙的系统，包括：第一客户端，第二客户端，打洞辅助服务器；

[0037] 测试服务器，用于测试网络地址转换设备的类型；

[0038] 第一客户端，用于在测试服务器判断能进行打洞时，根据网络地址转换设备的类型，使用用户数据报协议打洞；

[0039] 在测试服务器判断得到用户数据报协议包无法通过或者业务层要求使用传输控制协议打洞时，获取已存的打洞环境测试结果，通过打洞辅助服务器向第二客户端发起传输控制协议直接连接请求，并获取已测试得到的打洞可采用的传输控制协议包序列；

[0040] 打洞辅助服务器，用于将第一客户端的公网 IP 地址及端口号发送给第二客户端，并将第二客户端的公网 IP 地址及端口号发送给第一客户端；

[0041] 第一客户端和第二客户端在打洞辅助服务器的协助下，按照所述打洞可采用的传输控制协议包序列，向对方的公网 IP 地址和端口号发送数据包，直到成功建立传输控制协议直接连接。

[0042] 上述技术方案具有如下有益效果：

[0043] 本发明实施例中，由于第一客户端保存了预先测试的打洞环境测试结果，第一客户端可以根据测试结果，向第二客户端的公网 IP 地址和端口号发送数据包，避免了现有技术只能在特定的环境下穿越 NAT 设备的缺陷，提高了穿越网络转换设备的成功率。

[0044] 具体实施方式

[0045] 图 1 为现有技术提供的 TCP 穿越网络地址转换设备的组网图；

[0046] 图 2 为本发明实施例提供的穿越网络地址转换设备的系统组成示意图

[0047] 图 3 为本发明实施例提供的穿越网络地址转换设备的方法流程图；

[0048] 图 4 为本发明第一实施例提供的穿越网络地址转换设备的方法流程图；

[0049] 图 5 为本发明第二实施例提供的穿越网络地址转换设备的方法流程图；

[0050] 图 6 为本发明第三实施例提供的穿越网络地址转换设备的方法流程图；

[0051] 图 7 为本发明第四实施例提供的穿越网络地址转换设备的方法流程图；

[0052] 图 8 为本发明第五实施例提供的穿越网络地址转换设备的方法流程图；

[0053] 图 9 为本发明第六实施例提供的穿越网络地址转换设备的方法流程图。

[0054] 本发明实施例提供的穿越网络地址转换设备 / 防火墙的方法、系统及客户 端，用于在 P2P 网络中需要可靠数据传输的场合，建立 TCP 直接连接 (TCP 直连)，本发明实施例提供的方法也可以简称为 TCP 打洞方法。

[0055] 为使本发明实施例的目的、技术方案、及优点更加清楚明白，以下结合附图对本发明实施例进行详细说明。

[0056] 以下以穿越网络地址转换设备的方法为例说明本发明实施例提供的方法，该方法也能够用于穿越防火墙。

[0057] 请参见图 2，为本发明实施例提供的穿越网络地址转换设备的系统组成示意图，该系统包括：客户端 A（第一客户端）201，客户端 B（第二客户端）202，打洞辅助服务器 203；

[0058] 其中，打洞辅助服务器 203，用于协助客户端 A201 和客户端 B202 穿越 NAT 设备建立图 2 中虚线所示的 TCP 直连，打洞辅助服务器 203 在协助客户端 A201 和客户端 B202 建立 TCP 直连以后，不会介入数据传输过程，数据传输由客户端 A201 和客户端 B202 独立完成。

[0059] 在本发明实施例中，在穿越 NAT 设备，建立 TCP 直连前，客户端需要测试打洞环境，并保存测试结果，打洞环境测试包括：测试操作系统版本是否符合打洞要求、测试用户是否有超级用户权限（一般 Windows 用户都具有超级用户权限）、测试是否可以使用操作系统接口设置公网 IP 地址的 TTL 值，以及测试表 1 所示的 TCP 包序列是否为可用于打洞的 TCP 包序列，其中，可用于打洞的 TCP 包序列是指未被 NAT 设备过滤的 TCP 包序列。

[0060] 其中，操作系统版本是否符合打洞要求、用户是否有超级用户权限、以及是否可以使用操作系统接口设置 IP 地址的 TTL 值的测试由客户端使用操作系统提供的接口独立完成。并且，在本发明实施例中，客户端的操作系统版本为 WinXP SP2 及以上的版本，则符合打洞要求。

[0061] 为了完成对表 1 所示 TCP 包序列过滤情况的测试，图 2 所示的系统中进一步包括：测试服务器 A204，测试服务器 B205；

[0062] 其中，测试服务器 A204，用于协助客户端 A201 测试客户端 A 的 NAT 设备 (NAT-A) 对表 1 所示 TCP 包序列的过滤情况，即测试客户端 A 可用表 1 中的哪些 TCP 包序列打洞；测试服务器 B205，用于协助客户端 B202 测试客户端 B 的 NAT 设备 (NAT-B) 对表 1 所示 TCP 包序列的过滤情况，即测试客户端 B 可用表 1 中的哪些 TCP 包序列打洞。

[0063] 值得注意的是，为了节约网络资源，在本发明实施例中，如果打洞环境 没有改变，则客户端可以直接获取已保存的测试结果，并按照该结果进行打洞，并不影响本发明实施例的实现。

[0064] 以下对表 1 所示的 TCP 包序列进行介绍。表 1 每一行表示一个 TCP 包序列，其中，第一个包表示客户端向测试服务器发送的数据包，第二个包和第三个包表示测试服务器在收到第一个包后，向客户端返回的数据包。

[0065]

序号	第一个包	第二个包	第三个包
1	SYN_{out}	SYN_{in}	无
2	SYN_{out}	$ICMP_{in}$	SYN_{in}
3	SYN_{out}	$ICMP_{in}$	$SYNACK_{in}$
4	SYN_{out}	RST_{in}	SYN_{in}
5	SYN_{out}	RST_{in}	$SYNACK_{in}$

[0066] 表 1

[0067] 以下结合图 2 所示的系统对本发明实施例提供的方法进行详细介绍。

[0068] 请参见图 3，为本发明实施例提供的穿越网络地址转换设备的方法，该方法包括：

[0069] 步骤 301：客户端 A 通过打洞辅助服务器向客户端 B 发起 TCP 直接连接请求；

[0070] 步骤 302：打洞辅助服务器将客户端 A 的公网 IP 地址及端口号发送给客户端 B，并将客户端 B 的公网 IP 地址及端口号发送给客户端 A；

[0071] 步骤 303：客户端 A 获取已测试得到的打洞可采用的 TCP 包序列；

[0072] 步骤 304：客户端 A 和客户端 B 在打洞辅助服务器的协助下，按照步骤 303 获得的

打洞可采用的 TCP 包序列，向对方的公网 IP 地址和端口号发送数据包，直到成功建立 TCP 直接连接。

[0073] 若客户端是第一次进行 TCP 打洞，则上述方法进一步包括如下步骤：

[0074] 客户端 A 和客户端 B 在测试服务器的协助下，测试打洞环境；

[0075] 客户端 A 保存自身的打洞环境测试结果及客户端 B 通过打洞辅助服务器向其返回的打洞环境测试结果。

[0076] 举例说明客户端和测试服务器如何测试哪些 TCP 包序列是可以用于打洞的 TCP 序列。比如，客户端 A 向测试服务器 A 发送第一个包 SYNout 后，客户端收到了测试服务器返回的第二个包 ICMPin 和第三个包 SYNin，这说明序号为 2 的 TCP 包序列未被 NAT 设备过滤，则客户端 A 记录序号为 2 的 TCP 包序列为可用打洞的 TCP 包序列，反之，若客户端 A 未收到测试服务器返回的数据包，说明 TCP 包序列被 NAT 设备过滤，则该序列不能用于打洞。

[0077] 以上介绍了本发明实施例提供的穿越 NAT 设备的方法，在本发明其他实施例中，客户端可以在步骤 304 之前的任意一个位置执行步骤 303，并不影响本发明实施例的实现。

[0078] 具体实现时，会存在多种不同的打洞环境测试结果，以下针对不同的打洞环境测试结果对本发明实施例的具体实现过程进行详细介绍。

[0079] 请参见图 4，为本发明第一实施例提供的穿越 NAT 设备的方法流程图，该方法包括：

[0080] 步骤 401：客户端 A 连接打洞辅助服务器的协助打洞端口，并发送 TCP 直接连接请求；

[0081] 步骤 402：打洞辅助服务器收到所述请求后，通过主连接向客户端 B 发送 TCP 连接通知，并将客户端 A 经过 NAT-A 设备转换的公网 IP 地址和端口号通过主连接发送给客户端 B；

[0082] 客户端 B 在收到 TCP 连接通知后，与打洞辅助服务器的协助打洞端口连接，随便发送一些数据至打洞辅助服务器后立即断开，以使得打洞辅助服务器记录客户端 B 经 NAT-B 设备转换后的公网 IP 地址和端口号；

[0083] 步骤 403：打洞辅助服务器通过主连接将客户端 B 的公网 IP 地址和端口号发送给客户端 A；

[0084] 此时，客户端 A 知道了客户端 B 的公网 IP 地址和端口号，客户端 B 也知道了客户端 A 的公网 IP 地址和端口号；

[0085] 步骤 404：客户端 A 获取已测试得到的打洞可采用的 TCP 包序列，若所述 TCP 序列是表 1 中序号为 1 的 TCP 包序列，则客户端 A 获取已存的环境测试结果，若环境测试结果为系统版本为 WinXP SP2 及以上，则进入步骤 405；

[0086] 步骤 405：客户端 A 通过打洞辅助服务器向客户端 B 发送通知消息，该通知消息用于通知客户端 B 向客户端 A 的公网 IP 地址和端口号发送 SYN 包；

[0087] 步骤 406：客户端 A 和客户端 B 向对方的公网 IP 地址和端口号，发送 SYN 包；

[0088] 步骤 407：客户端 A 和客户端 B 在收到 SYN 包后，返回同步数据包确认消息 (SYNACK) 至对方；

[0089] 至此 TCP 直连已建立，按照 TCP 协议的规定，上述方法进一步包括：

[0090] 步骤 408：客户端 A 和客户端 B 在收到 SYNACK 后，向对方返回确认消息 (ACK)。

[0091] 请参见图 5，为本发明第二实施例提供的穿越网络地址转换设备的方法流程图，该方法与第一实施例的区别在于：

[0092] 步骤 504：客户端 A 获取已测试得到的打洞可采用的 TCP 包序列，若所述 TCP 序列是表 1 中序号为 2 的 TCP 包序列，则客户端 A 获取已存的环境测试结果，若环境测试结果为系统版本为能够使用操作系统接口设置公网 IP 地址的 TTL 值，则进入步骤 505；

[0093] 步骤 505：客户端 A 通过打洞辅助服务器向客户端 B 发送第一 SYN 包，第一 SYN 包携带客户端 B 的公网 IP 地址的 TTL 值被设置为低；

[0094] 其中，低 TTL 值的要求是：TTL 值可以使第一 SYN 包穿过 NAT-A 设备，但是不能到达客户端 B；

[0095] 并且，第一 SYN 包由客户端 A 利用底层网络函数自己构造。

[0096] 步骤 506：打洞辅助服务器向客户端 A 返回 Internet 控制消息协议包 (Internet Control Message Protocol，ICMP)，ICMP 包携带客户端 A 的公网 IP 地址的 TTL 值设置为过期；

[0097] 步骤 507：打洞辅助服务器向客户端 B 发送通知消息；

[0098] 步骤 508：客户端 B 在收到所述通知消息后，向客户端 A 的公网 IP 地址和端口号发送第二 SYN 包；

[0099] 步骤 509：客户端 A 在收到客户端 B 发送来的第二 SYN 包后，向客户端 B 发送 SYNACK 包，至此 TCP 直连已建立。

[0100] 请参见图 6，为本发明第三实施例提供的穿越 NAT 设备的方法流程图，该方法与前文已述实施例的区别在于：

[0101] 步骤 604：客户端 A 获取已测试得到的打洞可采用的 TCP 包序列，若所述 TCP 序列是表 1 中序号为 3 的 TCP 包序列，则客户端 A 获取已存的环境测试结果，若环境测试结果为系统版本为操作系统版本为 Win XP SP2 及以上，用户具有超级用户权限，并且，能够使用操作系统接口设置公网 IP 地址的 TTL 值，则进入步骤 605；

[0102] 步骤 605：客户端 A 和客户端 B 通过打洞辅助服务器向对方发送 SYN 包，该 SYN 包携带公网 IP 地址的 TTL 值被设置为低 TTL 值；

[0103] 具体的，客户端 A 向客户端 B 发送的第一 SYN 包携带客户端 B 的公网 IP 地址，该公网 IP 地址的 TTL 值被设置为低 TTL 值，同理，客户端 B 向客户端 A 发送的第二 SYN 包携带客户端 A 的公网 IP 地址，该公网 IP 地址的 TTL 值被设置为低 TTL 值；

[0104] 并且，低 TTL 值的要求请参见第二实施例相关部分，此处不再赘述。

[0105] 步骤 606：打洞辅助服务器向客户端 A 和客户端 B 分别发送 ICMP 包；

[0106] 其中，发给客户端 A 的 ICMP 包携带客户端 A 的公网 IP 地址，该公网 IP 地址的 TTL 被设置为过期，同理，发给客户端 B 的 ICMP 携带客户端 B 的公网 IP 地址，该公网 IP 地址的 TTL 值被设置为过期；

[0107] 步骤 607：客户端 A 和客户端 B 在收到 ICMP 包后，通过打洞辅助服务器向对方发送自己的 TCP 序列号；

[0108] 其中，TCP 序列号是客户端 A 和客户端 B 在向对方发送 SYN 包的同时自己监听到的；

[0109] 步骤 608：客户端 A 和客户端 B 在收到对方的 TCP 序列号后，向对方发送 SYNACK

包，至此 TCP 直连已建立。

[0110] 以上介绍了本发明第三实施例，该实施例中所有数据包均是由客户端 A 和客户端 B 利用底层网络函数自己构造的。

[0111] 请参见图 7，为本发明第四实施例提供的穿越 NAT 设备的方法流程图，该方法与前文已述方法的区别在于：

[0112] 步骤 704：客户端 A 获取已测试得到的打洞可采用的 TCP 包序列，若所述 TCP 序列是表 1 中序号为 4 的 TCP 包序列，则进入步骤 705；

[0113] 步骤 705：客户端 A 向客户端 B 的公网 IP 地址和端口号对应的 NAT-B 设备发送第一 SYN 包；

[0114] 其中，第一 SYN 包是客户端 A 利用底层网络函数自己构造的数据包；

[0115] 步骤 706：NAT-B 设备向客户端 A 返回 RST 消息，RST 消息是 NAT-B 设备自动生成的；

[0116] 其中，客户端 A 发送第一 SYN 包到 NAT-B 时，由于 NAT-B 设备上没有客户端 A 的记录，所以 NAT-B 设备会自动生成一个 RST 消息，并返回给客户端 A，要求客户端 A 和 NAT-A 设备复位。

[0117] 步骤 707：客户端 A 通过打洞辅助服务器向客户端 B 发送通知消息；

[0118] 步骤 708：客户端 B 接收倒所述通知消息后，向客户端 A 的公网 IP 地址和端口号发送第二 SYN 包；

[0119] 步骤 709：客户端 A 在收到第二 SYN 包后，向客户端 B 返回 SYNACK 包，至此 TCP 直连已建立。

[0120] 请参见图 8，为本发明第五实施例提供的穿越 NAT 设备的方法流程图，该方法与前文已述实施例的区别在于：

[0121] 步骤 804：客户端 A 获取已测试得到的打洞可采用的 TCP 包序列，若所述 TCP 序列是表 1 中序号为 5 的 TCP 包序列，则客户端 A 获取已存的环境测试结果，若环境测试结果为操作系统版本为 WinXP SP2 及以上，用户具有超级用户权限，则进入步骤 805；

[0122] 步骤 805：客户端 A 和客户端 B 的分别向对方的公网 IP 地址和端口号对应的 NAT 设备发送 SYN 包；

[0123] 步骤 806：NAT-A 设备和 NAT-B 设备在收到 SYN 包后，返回 RST 消息至客户端 A 和客户端 B；

[0124] 步骤 807：客户端 A 和客户端 B 通过打洞辅助服务器将自己的 TCP 序列发送给对方；

[0125] 步骤 808：客户端 A 和客户端 B 在收到对方的 TCP 序列号后，分别向对方返回 SYNACK 包，至此 TCP 直连已建立。

[0126] 以上为本发明第五实施例提供的方法，该方法中除 RST 消息外，其他的数据包均是由客户端 A 和客户端 B 分别利用底层网络函数自己构造的。

[0127] 以上针对不同的打洞环境对本发明实施例进行了介绍。

[0128] 进一步，在本发明实施例中，上述五个实施例提供的方法可以运行在同一个客户端上，在开始打洞前，获取 TCP 包序列的测试结果，如果表 1 中序号为 N(N = 1,2,,5) 的 TCP 包序列未被 NAT 设备过滤，则选择第 N 实施例提供的方法，然后，测试表 2 所列信息的测试

结果是否满足第 N 实施例的要求，如果满足，则使用第 N 实施例提供的方法开始打洞，如果不满足，则不能进行 TCP 打洞。表 2 所示是前文已述 5 个实施例各自需要测试及不需要测试的信息，其中，“√”表示需要测试的信息，“×”表示不需要测试的信息。

[0129] 通常情况下，客户端 B 需要将自己打洞环境测试结果通过打洞辅助服务器发送给客户端 A，客户端 A 通过已保存自己的打洞环境测试结果和客户端 B 的打洞环境测试结果，选择打洞方法。

[0130]

TCP 打洞方法	操作系统版本	设置 TTL 值	超级用户权限
实施例一	√	×	×
实施例二	×	√	×
实施例三	√	√	√
实施例四	×	×	×
实施例五	√	×	√

[0131] 表 2

[0132] 以上介绍了本发明实施例提供的穿越 NAT 设备的方法，为了保证更高的成功率，可以将本发明实施例提供的方法和现有的 UDP 打洞方法，以及超级节点中转数据的方法相融合。

[0133] 请参见图 9，为本发明实施例提供的融合了多种打洞方式的穿越 NAT 设备的方法流程图，该方法包括：

[0134] 步骤 901：客户端 A 和客户端 B 利用测试服务器 A 和测试服务器 B 使用 STUN 协议测试自己的 NAT 类型；

[0135] NAT 类型有四种：全双工锥型 NAT，IP 受限型 NAT，端口受限型 NAT 及对称型 NAT。

[0136] 步骤 902：若客户端 A 判断得到 UDP 不通或者业务层要求必须使用 TCP 打洞，则进入步骤 903，否则，进入步骤 904；

[0137] 步骤 903：客户端 A 获取已存的打洞环境测试结果，根据所述测试结果，使用本发明实施例提供的 TCP 打洞方法进行 TCP 打洞；

[0138] 步骤 904：客户端 A 判断是否可以进行打洞，如果可以，则进入步骤 905，否则，进入步骤 906；

[0139] 步骤 905：客户端 A 根据 NAT 设备的类型，使用 UDP 打洞；

[0140] 步骤 906：客户端 A 触发超级节点中转数据。

[0141] 本发明实施例还提供了一种第一客户端，该客户端包括：

[0142] 直连请求发送单元，用于通过打洞辅助服务器向客户端 B 发起 TCP 直接连接请求；

[0143] 公网 IP 地址接收单元，用于接收打洞辅助服务器返回的客户端 B 的公网 IP 地址及端口号；

[0144] 包序列获取单元，用于获取已测试得到的打洞可采用的传输控制协议包序列；

[0145] 直连建立单元，用于在打洞辅助服务器的协助下，按照所述打洞可采用的传输控制协议包序列，向客户端 B 的公网 IP 地址和端口号发送数据包，直到成功建立 TCP 直接连接。

[0146] 若第一客户端是第一次进行 TCP 打洞，则上述第一客户端进一步包括：

[0147] 环境测试单元，用于测试打洞环境，并保存第一客户端保存自身的打洞环境测试

结果及客户端 B 通过打洞辅助服务器向其返回的打洞环境测试结果。

[0148] 本发明实施例针对不同的打洞环境测试结果，提供了几种第一客户端的具体实现方式，以下进行详细介绍。

[0149] 1、若表 1 中序号为 1 的 TCP 包序列是可用于打洞的 TCP 序列，则所述客户端进一步包括：

[0150] 测试结果获取单元，用于获取已存的环境测试结果，若测试结果为操作系统版本符合预置的版本条件，则触发所述直连建立单元；

[0151] 在具体实现时，直连建立单元包括：同步数据包发送单元，同步数据包接收单元，确认消息发送单元；

[0152] 同步数据包发送单元，用于向客户端 B 的公网 IP 地址和端口号，发送第一同步数据包；

[0153] 通知消息发送单元，用于通过打洞辅助服务器向客户端 B 发送通知消息，该通知消息用于通知客户端 B 向客户端 A 的公网 IP 地址和端口号发送 SYN 包；

[0154] 同步数据包接收单元，用于接收客户端 B 在收到所述通知消息后，发送的第二同步数据包；

[0155] 确认消息发送单元，用于在收到所述第二同步数据包后，向客户端 B 发送同步数据包确认消息；

[0156] 确认消息接收单元，用于接收客户端 B 在收到第一同步数据包后，返回的同步数据包确认消息。

[0157] 2、若表 1 中序号为 2 的 TCP 包序列是可用于打洞的 TCP 序列，则所述客户端进一步包括：

[0158] 测试结果获取单元，用于获取已存的环境测试结果，若测试结果为能够使用操作系统接口设置公网 IP 地址的 TTL 值，则触发所述直连建立单元；

[0159] 在具体实现时，直连建立单元包括：

[0160] 同步数据包发送单元，用于通过打洞辅助服务器向客户端 B 发送第一同步数据包，所述第一同步数据包携带客户端 B 的公网 IP 地址的 TTL 值被设置为低；

[0161] 协议包接收单元，用于接收打洞辅助服务器返回的互联网控制消息协议包，所述协议包携带第一客户端的公网 IP 地址的 TTL 值被设置为过期；

[0162] 同步数据包接收单元，用于接收客户端 B 发送的第二同步数据包；

[0163] 确认消息发送单元，用于在同步数据包接收单元收到所述第二同步数据包后，向客户端 B 发送同步数据包确认消息。

[0164] 3、若表 1 中序号为 3 的 TCP 包序列是可用于打洞的 TCP 序列，则所述客户端进一步包括：

[0165] 测试结果获取单元，用于获取已存的环境测试结果，若测试结果为操作系统版本为 WinXP SP2 及以上，能够使用操作系统接口设置公网 IP 地址的 TTL 值，并且用户具有超级用户权限，则触发所述直连建立单元；

[0166] 在具体实现时，直连建立单元包括：

[0167] 同步数据包发送单元，用于通过打洞辅助服务器向客户端 B 发送同步数据包，所述同步数据包携带客户端 B 的公网 IP 地址的 TTL 值被设置为低；

[0168] 协议包接收单元，用于接收打洞辅助服务器返回的互联网控制消息协议包，所述协议包携带第一客户端的公网 IP 地址的 TTL 值被设置为过期；

[0169] 序列号发送单元，用于通过打洞辅助服务器向客户端 B 发送第一传输控制协议序列号；

[0170] 序列号接收单元，用于接收打洞服务器发送来的客户端 B 的第二传输控制协议序列号；

[0171] 确认消息发送单元，用于在收到第二传输控制协议序列号后，向客户端 B 发送同步数据包确认消息；

[0172] 确认消息接收单元，用于接收客户端 B 在收到第一传输控制协议序列号后，返回的同步数据包确认消息。

[0173] 4、若表 1 中序号为 4 的 TCP 包序列是可用于打洞的 TCP 序列，则在具体实现时，直连建立单元包括：

[0174] 同步数据包发送单元，用于向客户端 B 的公网 IP 地址和端口号对应的网络地址转换设备发送第一同步数据包；

[0175] 复位消息接收单元，用于接收所述网络地址转换设备返回的复位消息；

[0176] 通知消息发送单元，用于通过打洞辅助服务器向客户端 B 发送通知消息；

[0177] 同步数据包接收单元，用于接收客户端 B 在收到通知消息后，发送的第二同步数据包；

[0178] 确认消息发送单元，用于在收到所述第二同步数据包后，向客户端 B 返回同步数据包确认消息。

[0179] 5、若表 1 中序号为 5 的 TCP 包序列是可用于打洞的 TCP 序列，则所述客户端进一步包括

[0180] 测试结果获取单元，用于获取已存的环境测试结果，若测试结果为操作系统版本为 WinXP SP2，并且用户具有超级用户权限，则触发所述直连建立单元；

[0181] 在具体实现时，直连建立单元包括：

[0182] 同步数据包发送单元，用于向客户端 B 的公网 IP 地址和端口号对应的网络地址转换设备发送第一同步数据包；

[0183] 复位消息接收单元，用于接收所述网络地址转换设备返回的复位消息；

[0184] 序列号发送单元，用于向客户端 B 的公网 IP 地址和端口号发送第一传输控制协议序列号；

[0185] 序列号接收单元，用于接收客户端 B 发送的第二传输控制协议序列号；

[0186] 确认消息发送单元，用于在收到第二传输控制协议序列号后，向客户端 B 返回同步数据包确认消息；

[0187] 确认消息接收单元，用于接收客户端 B 在收到第一传输控制协议序列号后，返回的同步数据包确认消息。

[0188] 按照 TCP 协议的要求，在上述五种直连建立单元都进一步包括：

[0189] 响应消息发送单元，用于在收到第二客户端返回的同步数据包确认消息后，向第二客户端发送响应消息 (ACK)；

[0190] 响应消息接收单元，用于接收第二客户端在收到第一客户端发送的同步数据包确

认消息后，返回的响应消息。

[0191] 在本发明实施例提供的第一客户端中，进一步包括：测试数据包发送单元，测试数据包接收单元，序列记录单元；

[0192] 测试数据包发送单元，用于向测试服务器发送第一同步数据包，

[0193] 测试数据包接收单元，用于接收测试服务器返回的数据包；

[0194] 若测试数据包接收单元接收到的数据包是第二同步数据包，则序列记录单元，用于记录由所述第一同步数据包和第二同步数据包构成的序列为可用于打洞的传输控制协议包序列；

[0195] 若测试数据包接收单元接收到数据包是互联网控制消息协议包和第二同步数据包，则序列记录单元，用于记录由所述第一同步数据包，互联网控制消息协议包，及第二同步数据包构成的序列为可用于打洞的传输控制协议包序列；

[0196] 若测试数据包接收单元接收到数据包是互联网控制消息协议包和同步数据包确认消息，则序列记录单元，用于记录由所述第一同步数据包，互联网 控制消息协议包，及同步数据包确认消息构成的序列为可用于打洞的传输控制协议包序列；

[0197] 若测试数据包接收单元接收到数据包是复位消息以及第二同步数据包，则序列记录单元，用于记录由所述第一同步数据包，复位消息以及第二同步数据包构成的序列为可用于打洞的传输控制协议包序列；

[0198] 若测试数据包接收单元接收到数据包是复位消息和同步数据包确认消息，则序列记录单元，用于记录由所述第一同步数据包，复位消息和同步数据包确认消息构成的序列为可用于打洞的传输控制协议包序列。

[0199] 为了保证更高的穿越 NAT 设备的成功率，本发明实施例提供的第一客户端进一步包括：

[0200] 网络地址转换设备类型测试单元，用于利用测试服务器测试网络地址转换设备的类型；

[0201] 打洞方法选择单元，若判断得到用户数据报协议包无法通过或者业务层要求使用传输控制协议打洞，则触发测试结果获取单元，否则，判断是否能够进行打洞，若能，则触发用户数据报直连建立单元，否则，触发超级节点中转数据；

[0202] 用户数据报直连建立单元，用于根据网络地址转换设备的类型，使用用户数据报协议打洞。

[0203] 以上对本发明所提供的一种穿越网络地址转换设备 / 防火墙的方法、系统及客户端进行了详细介绍，对于本领域的一般技术人员，依据本发明实施例的思想，在具体实施方式及应用范围上均会有改变之处，综上所述，本说明书内容不应理解为对本发明的限制。

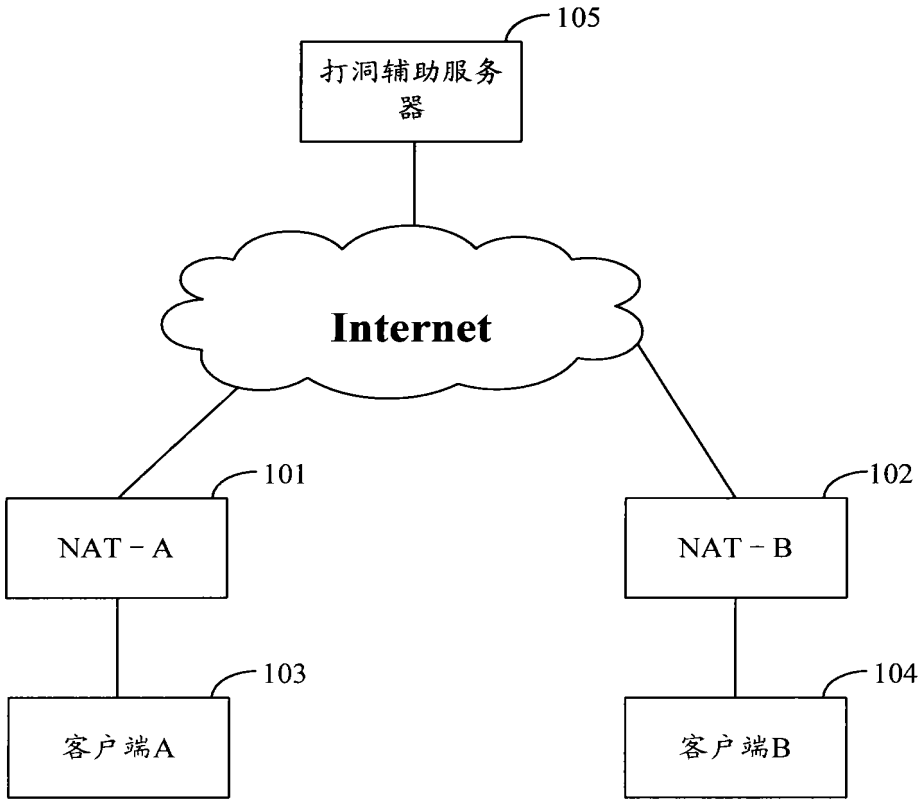

105
打洞辅助服务器
Internet
101
NAT－A
102
NAT－B
103
客户端A
104
客户端B

图 1

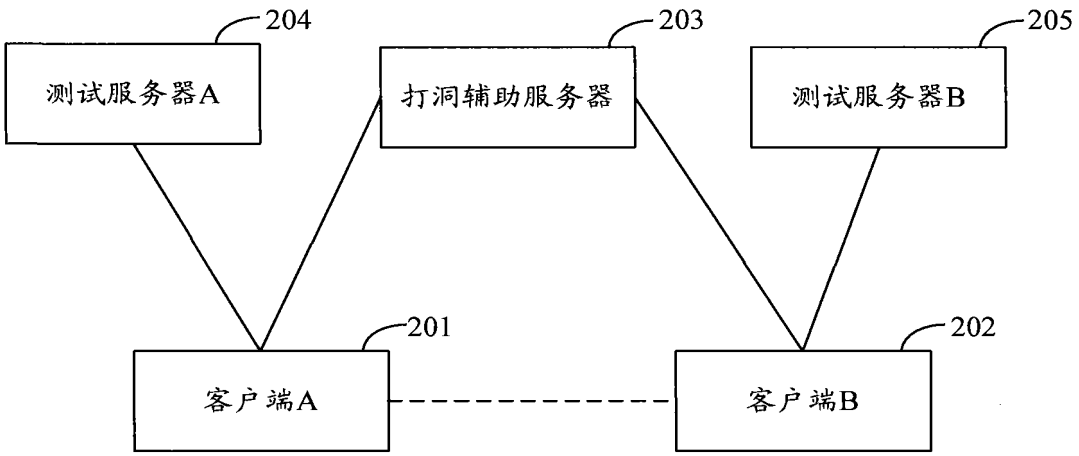

204
测试服务器A
203
打洞辅助服务器
205
测试服务器B
201
客户端A
202
客户端B

图 2

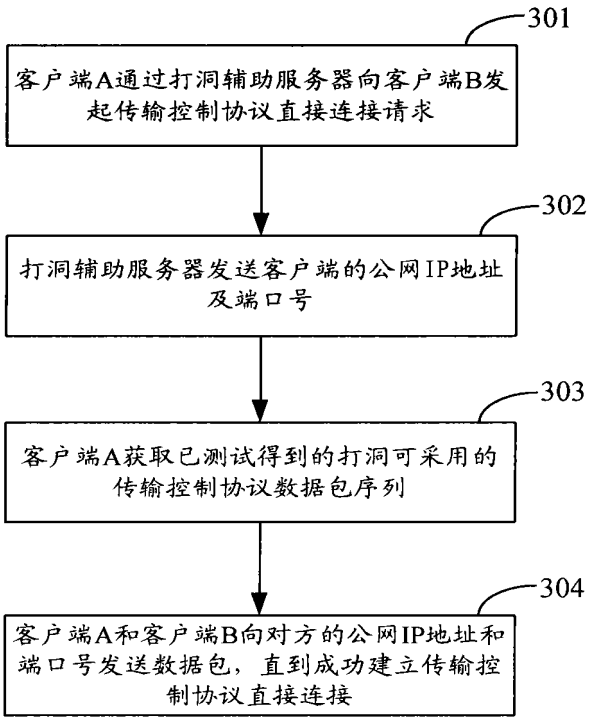

301
客户端A通过打洞辅助服务器向客户端B发起传输控制协议直接连接请求
302
打洞辅助服务器发送客户端的公网IP地址及端口号
303
客户端A获取已测试得到的打洞可采用的传输控制协议数据包序列
304
客户端A和客户端B向对方的公网IP地址和端口号发送数据包，直到成功建立传输控制协议直接连接

图 3

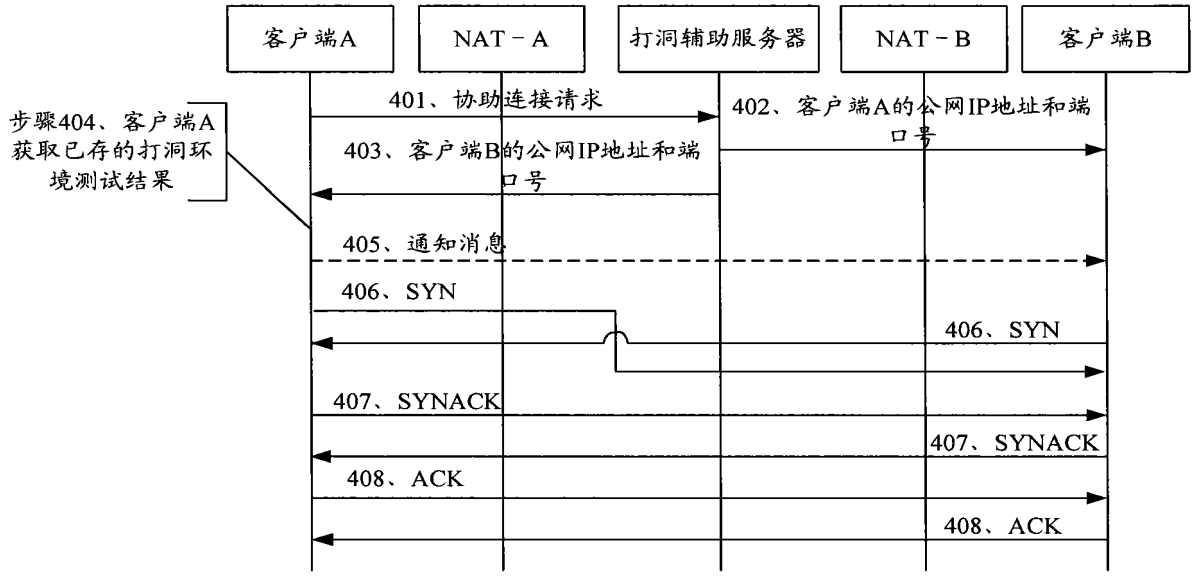

客户端A
NAT－A
打洞辅助服务器
NAT－B
客户端B
步骤404、客户端A获取已存的打洞环境测试结果
401、协助连接请求
402、客户端A的公网IP地址和端口号
403、客户端B的公网IP地址和端口号
405、通知消息
406、SYN
406、SYN
407、SYNACK
407、SYNACK
408、ACK
408、ACK

图 4

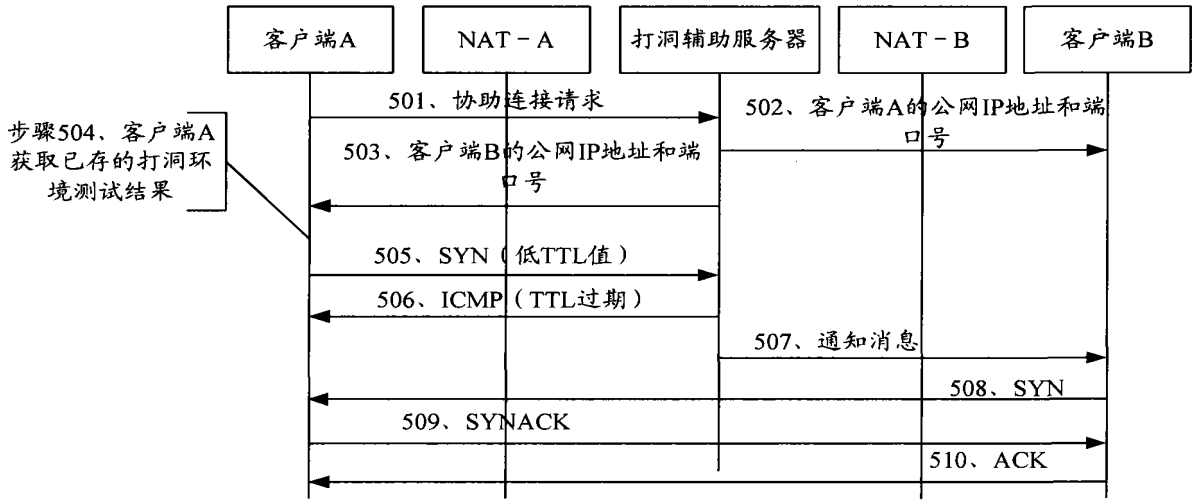

客户端A
NAT－A
打洞辅助服务器
NAT－B
客户端B
501、协助连接请求
502、客户端A的公网IP地址和端口号
步骤504、客户端A获取已存的打洞环境测试结果
503、客户端B的公网IP地址和端口号
505、SYN（低TTL值）
506、ICMP（TTL过期）
507、通知消息
508、SYN
509、SYNACK
510、ACK

图 5

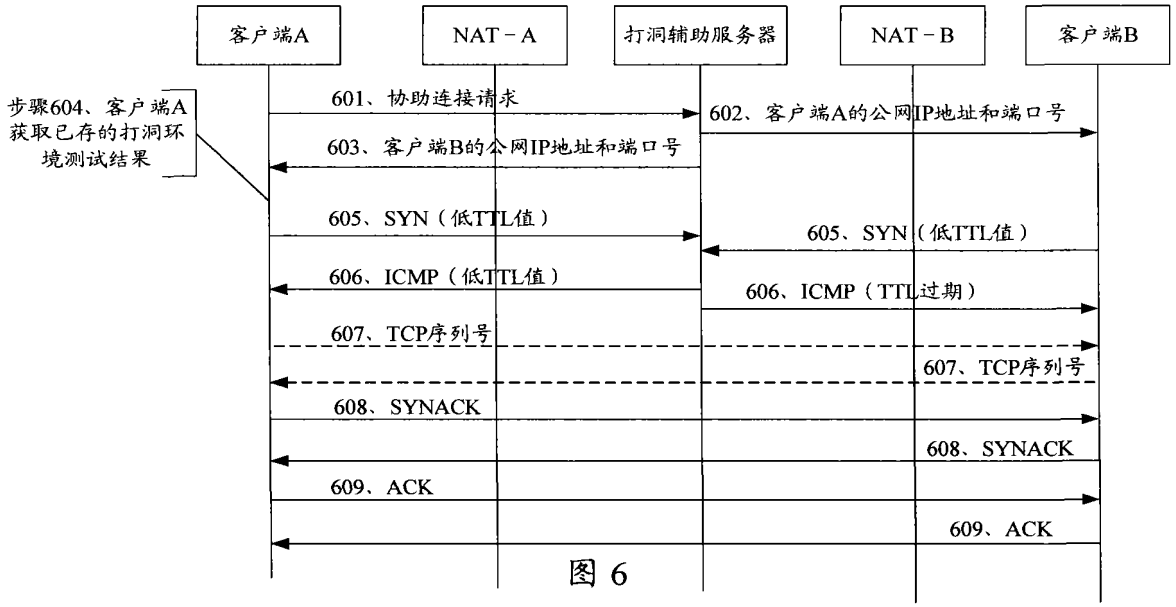

客户端A
NAT－A
打洞辅助服务器
NAT－B
客户端B
601、协助连接请求
602、客户端A的公网IP地址和端口号
步骤604、客户端A获取已存的打洞环境测试结果
603、客户端B的公网IP地址和端口号
605、SYN（低TTL值）
605、SYN（低TTL值）
606、ICMP（低TTL值）
606、ICMP（TTL过期）
607、TCP序列号
607、TCP序列号
608、SYNACK
608、SYNACK
609、ACK
609、ACK

图 6

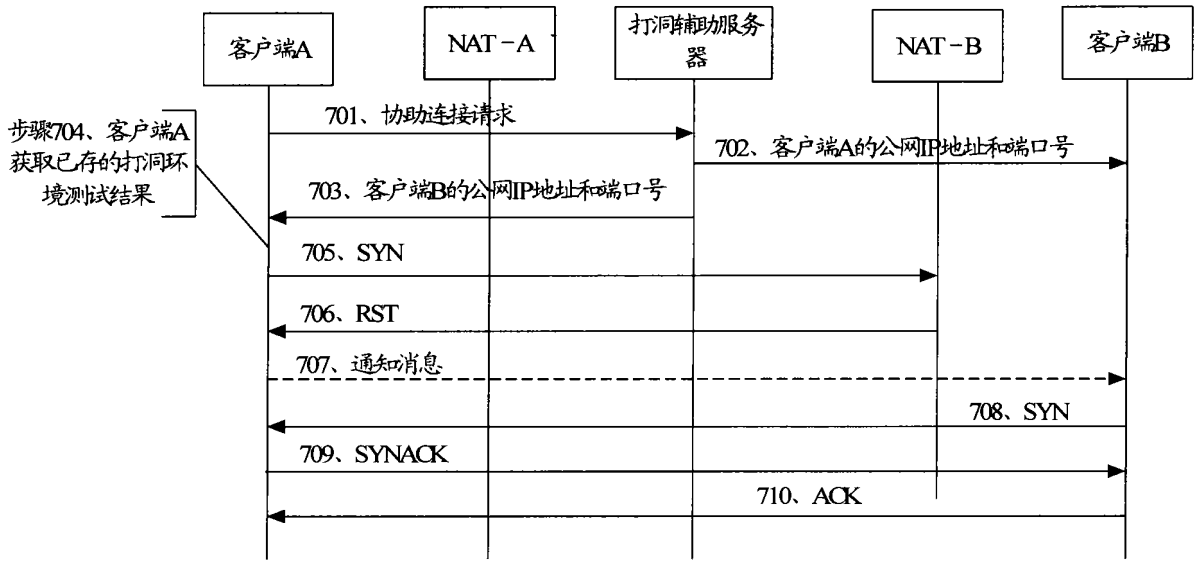

客户端A
NAT－A
打洞辅助服务器
NAT－B
客户端B
步骤704、客户端A获取已存的打洞环境测试结果
701、协助连接请求
702、客户端A的公网IP地址和端口号
703、客户端B的公网IP地址和端口号
705、SYN
706、RST
707、通知消息
708、SYN
709、SYNACK
710、ACK

图 7

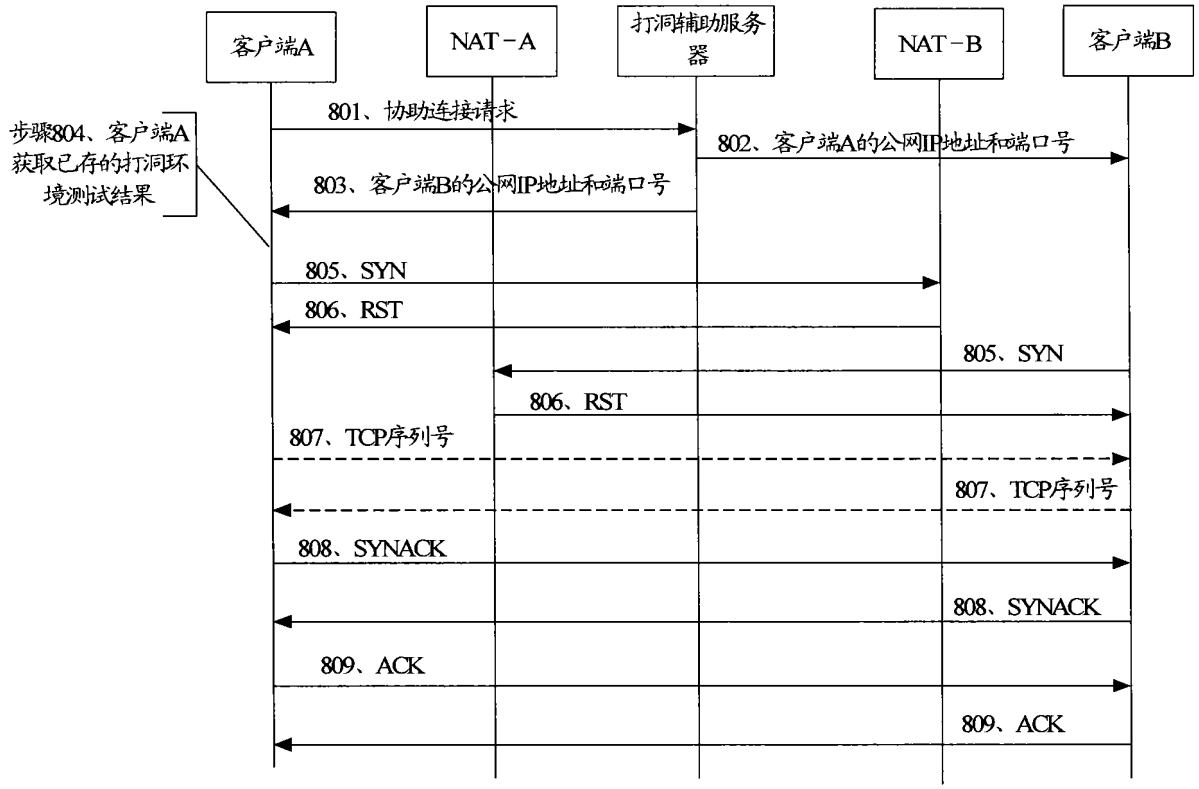

客户端A
NAT－A
打洞辅助服务器
NAT－B
客户端B
步骤804、客户端A获取已存的打洞环境测试结果
801、协助连接请求
802、客户端A的公网IP地址和端口号
803、客户端B的公网IP地址和端口号
805、SYN
806、RST
805、SYN
806、RST
807、TCP序列号
807、TCP序列号
808、SYNACK
808、SYNACK
809、ACK
809、ACK

图 8

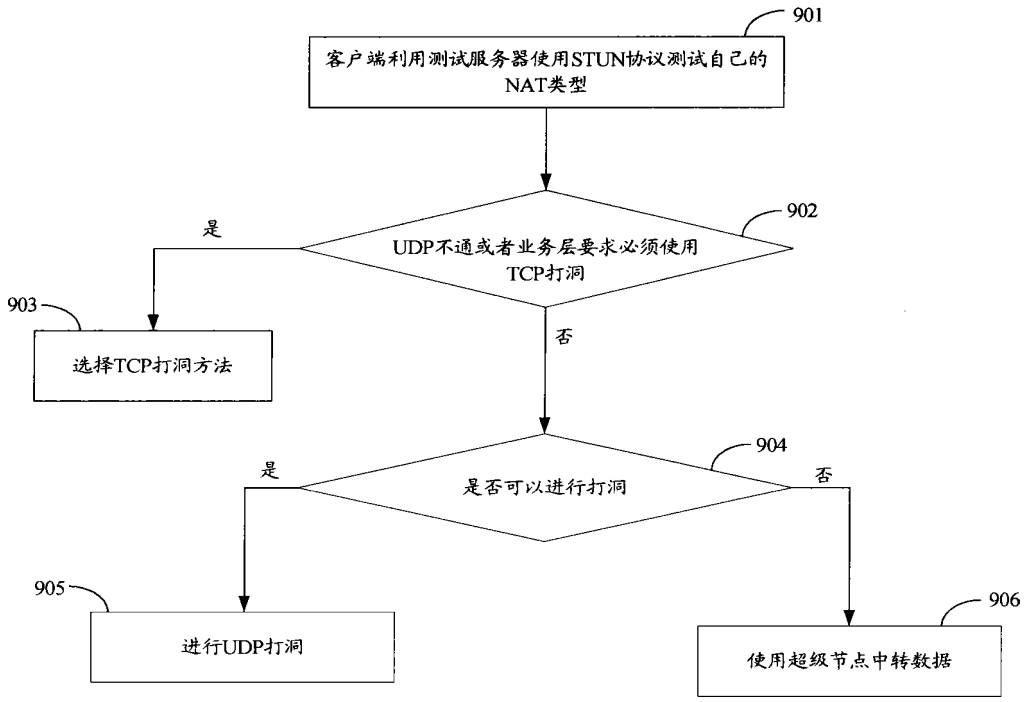

901
客户端利用测试服务器使用STUN协议测试自己的NAT类型
902
UDP不通或者业务层要求必须使用TCP打洞
是
否
903
选择TCP打洞方法
904
是否可以进行打洞
是
否
905
进行UDP打洞
906
使用超级节点中转数据

图 9