(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 1825828 B
(45)授权公告日 2011.04.27

(21)申请号 200510008871.9

(22)申请日 2005.02.24

(73)专利权人 北京风行在线技术有限公司
地址 100088 北京市海淀区知春路6号锦秋知春家园4号楼1单元601

(72)发明人 唐柯

(74)专利代理机构 北京市金杜律师事务所 11256
代理人 罗朋

(51)Int.Cl.
H04L 12/56(2006.01)
H04L 12/46(2006.01)

(56)对比文件
WO 2004/063843 A2,2004.07.29,摘要、说明书第27页第12行至第28页第5行,附图7A-7C.
CN 1514584 A,2004.07.21,摘要,说明书第8页第20行至第9页第21行、第7页第24-26行.

审查员 胡锐先

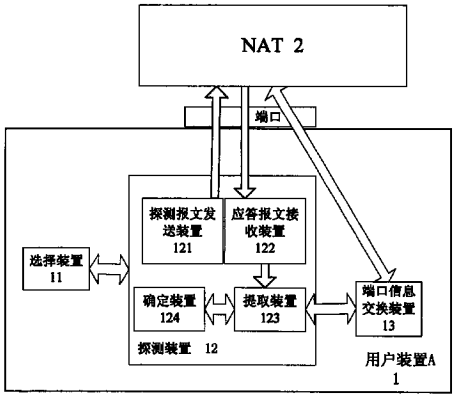
权利要求书 2 页 说明书 11 页 附图 5 页

(54)发明名称

一种两端均处于不同NAT下直接穿透通信的控制方法和设备

(57)摘要

本发明公开了用于使得处于NAT下与在不同NAT下用户装置进行直接穿透通信的用户装置及其通信,通过由一个选择的本地端口向外网辅助探测装置发送探测报文,并接收来自所述辅助探测装置的应答报文获取该探测报文被NAT转换的NAT源端口,并通过比较多次探测报文的NAT源端口来确定所选择的本地端口是否为穿透端口,然后将其对应的NAT源地址和NAT穿透端口通过外网设备通知在不同NAT下的另一个用户装置(同样也通过外网设备来接收所述另一个用户装置所确定的NAT穿透端口和NAT源地址),从而可以经由所确定的本地穿透端口将对方的NAT源地址和NAT穿透端口作为目的地址和目的端口进行直接穿透通信。



CN 1825828 B

1. 一种在NAT下的用户装置中与在不同NAT下的用户装置进行直接穿透通信的通信方法，包括以下步骤：

a) 选择一个本地源端口，用以发送和接收报文；

b) 通过所述本地源端口经由 NAT 向外网辅助探测装置上的多个目标端口或向外网的多个辅助探测装置发出多次探测报文；

c) 接收来自所述外网辅助探测装置的多个探测应答报文，其中所述探测应答报文的内容包括该探测应答报文对应的探测报文被 NAT 转换后的 NAT 源地址和 NAT 源端口；

d) 从所述应答报文中提取所述探测报文被 NAT 转换后的 NAT 源地址和 NAT 源端口；

e) 如果所述多次探测报文的 NAT 源端口都相同，则判断所述本地源端口为与其他设备的端口没有冲突的本地穿透端口，并以所述 NAT 源地址和 NAT 源端口作为最后选择的 NAT 外网地址和 NAT 端口；

f) 否则，重新选择一个不同的本地源端口，重复以上步骤，直到找到合适的本地穿透端口为止；

g) 通过一个外网的通知装置将本用户装置的所述NAT外网地址和NAT端口通知另一个NAT下的用户装置，并通过外网的通知装置获知来自所述另一个NAT下的用户装置的NAT外网地址和 NAT 端口；

i) 通过所述合适的本地穿透端口，所述的用户装置和对端的用户装置分别使用所接收的对方的 NAT 外网地址和 NAT 端口作为目标地址进行直接通信。

2. 根据权利要求 1 所述的方法，其特征在于：所述用户装置可同时选择多个本地源端口，并对于每个选择的本地源端口，同时执行所述步骤 a)-f)，以更快地确定一个可以实现通信的本地源端口。

3. 根据权利要求 1 或 2 所述的方法，其特征在于，所述合适的本地穿透端口为端口限制的本地穿透端口，在所述步骤 g) 之后且在所述步骤 i) 之前，还包括：

- 通过所述合适的本地穿透端口，所述的用户装置使用对端的用户装置的 NAT 外网地址和 NAT 端口作为目的地址和目的端口发送握手包；

- 接收所述对端的用户装置以所述用户装置的 NAT 外网地址和 NAT 端口作为目的地址和目的端口发来的握手包；

所述步骤 i) 包括：

- 在握手建立完成后，所述用户装置和对端的用户装置通过所述合适的本地穿透端口进行直接通信。

4. 一种在 NAT 下的用户装置中用于检测所选择的本地源端口是否为本地穿透端口的方法，包括以下步骤：

选择一个本地源端口；

通过所述本地源端口经由 NAT 向外网辅助探测装置上的多个目标端口或向外网的多个辅助探测装置发出多次探测报文；

接收来自所述外网辅助探测装置的探测应答报文，其中所述探测应答报文的内容包括所述探测报文被 NAT 转换后的 NAT 源地址和 NAT 源端口；

获取所述探测报文被 NAT 转换后的 NAT 源地址和 NAT 源端口；

如果多次探测报文的 NAT 源端口都相同，则判断所述本地源端口为与其他设备的端口

没有冲突的本地穿透端口；

否则，再选择一个不同的本地源端口，重复以上步骤，直到找到合适的本地穿透端口为止。

5. 根据权利要求 4 所述的方法，其特征在于：所述用户装置同时选择多个本地源端口发起探测，对于每个本地源端口，都执行权利要求 4 中所述的各个步骤，来检测该本地源端口是否为合适的本地穿透端口。

6. 一种在 NAT 下的用户装置，其用于通过一个特定的本地端口与另一个 NAT 下的用户装置直接穿透通信，该用户装置有多个网络端口，还包括：

选择装置，用于选择一个本地源端口，用以发送和接收报文；

探测装置，其中包括：

探测报文发送装置，用于通过所述本地源端口经由 NAT 向外网辅助探测装置上的多个目标端口或向外网的多个辅助探测装置发出多次探测报文；

应答报文接收装置，接收来自所述外网辅助探测装置的多个探测应答报文，其中所述探测应答报文的内容包括该探测应答报文对应的探测报文被 NAT 转换后的 NAT 源地址和 NAT 源端口；

提取装置，用于从所述探测应答报文中提取出所述探测报文被 NAT 转换后的 NAT 源地址和 NAT 源端口；

确定装置，如果所述多次探测报文的 NAT 源端口都相同，则确定所述本地源端口为与其他设备的端口没有冲突的本地穿透端口，并以所述 NAT 源地址和 NAT 源端口作为最后选择的 NAT 外网地址和 NAT 端口；

端口信息交换装置，用于通过一个外网的通知装置将所述最后选择的 NAT 外网地址和 NAT 端口通知另一个 NAT 下的用户装置，并通过外网的通知装置来获知来自所述另一个 NAT 下的用户装置的 NAT 外网地址和 NAT 端口；

其中，通过所述本地源端口，所述用户装置和对端的用户装置分别使用所接收的对方 NAT 外网地址和 NAT 端口作为目标地址进行直接通信。

7. 根据权利要求 6 所述的用户装置，其特征在于：

所述选择装置还用于同时选择多个本地源端口；

所述探测装置中的各个装置还用于同时为所述多个本地源端口分别执行相应的操作。

8. 根据权利要求 6 或 7 所述的用户装置，其特征在于，所述合适的本地穿透端口为端口限制的本地穿透端口，其中，在所述用户装置通过所述合适的本地穿透端口，使用对端的用户装置的 NAT 外网地址和 NAT 端口作为目的地址和目的端口发送握手包；

并且，所述用户装置还接收所述对端的用户装置以所述用户装置的 NAT 外网地址和 NAT 端口作为目的地址和目的端口发来的握手包；

其中，在握手建立完成后，所述用户装置和对端的用户装置通过所述合适的本地穿透端口进行直接通信。

一种两端均处于不同 NAT 下直接穿透通信的控制方法和设备

技术领域

[0001] 本发明涉及数据通信领域，尤其涉及 IP 通信协议中非常普遍的 NAT 内的用户互相通信的控制方法和设备，比如 :P2P(Peer to Peer) 通信应用领域。

背景技术

[0002] 在数据通信领域包括 :互联网、GPRS 和 CDMA 1x 以及公司内部各组织中，广泛使用 IP 通信协议进行通信。IP 通信协议以其开放性、简单性、成本低廉等因素得到了大量通信设备和主机设备的支持，成为最广泛使用的数据通信协议。

[0003] 当前的 IP 通信方式，是依据 IETF 国际组织所制定的 IPv4 通信协议，IPv4 定义了 IP 地址以 4 个 Byte 为标识。由于 IP 通信协议的在商业领域内得到广泛使用，导致了 IP 地址严重短缺。因此，IETF 组织制定了 NAT 技术规范，规定可以在组织和企业内部，使用保留的地址，作为内部私有地址，当这些地址的用户需要访问互联网上的其他用户时，在组织和企业出口，使用 NAT 设备，进行地址转换功能，将私有地址转换为公有 IP 地址，在转换中，可以一对一进行转换，也可以多对一进行转换（但依据端口号进行区分），当进行多对一或多对多（但内部地址多于公有地址）转换时（有些时候也称为 PAT 或 NAPT，这里都简称 NAT，因为一对一的 NAT 基本上没有应用领域），就可以达到节省公有 IP 地址的目的。现在，基本上所有的组织和企业，都使用 NAT 技术，在内部使用私有地址，在公司到互联网的出口部署 NAT 设备，进行地址转换。

[0004] 另外一个使用 NAT 技术的目的是对内部设备和主机进行保护，由于 NAT 屏蔽了外部主机对内部主机的访问（除非是 NAT 上进行了内部主机到 NAT 外部地址的固定端口映射，这种情况只可能是内部主机希望对外提供服务），所以对于组织和企业的内部用户，就会比较安全，不容易被外部恶意者所攻击。这种 NAT 技术广泛用于公司的防火墙策略。

[0005] 因此，在 IPv4 领域，NAT 的存在节省了 IP 地址和带来安全性，在 IPv6 领域，由于 IP 地址扩展到 6 个 Byte 为标识，节省地址不再必要，但从安全性上考虑，防火墙仍然会使用 NAT 技术以保护内部用户。

[0006] 按照 IETF 对 NAT 的定义，NAT 主要分为两大类 :基础 NAT(一对一地址转换)，NAPT(多对一或多数对少数地址转换)。

[0007] 其中，IETF RFC3489 STUN-Simple Traversal of User DatagramProtocol(UDP) Through Network Address Translators(NATs) 中，NAPT 主要分为两大类 :Cone NAT 和 Symmetric NAT，Cone NAT 的特点是当内部主机通过同一个源端口无论访问外部任何地址，NAT 设备在转换后都使用一个端口号，一直到这个会话结束才解除端口绑定；SymmetricNAT 的特点是内部主机访问任何外部地址和端口，NAT 设备在转换后都要使用一个新的端口号。

[0008] Cone NAT还有分类，就是全双工Cone NAT，受限制的Cone NAT，端口受限制的Cone NAT。

[0009] 全双工 Cone NAT，当内部主机发出一个“外出”的连接会话，就会创建了一个公网/私网地址，一旦这个地址对被创建，全双工 Cone NAT 会接收随后任何外部端口传入这个公共端口地址的通信。

[0010] 受限制的 Cone NAT，对传入的数据包进行筛选，当内部主机发出“外出”的会话时，NAT 会记录这个外部主机的 IP 地址信息，所以，也只有这些有记录的外部 IP 地址，能够将信息传入到 NAT 内部，受限制的 ConeNAT 有效的给防火墙提炼了筛选包的原则——即限定只给那些已知的外部地址“传入”信息到 NAT 内部。

[0011] 端口受限制的 Cone NAT，与受限制的 Cone NAT 不同的是：它同时记录了外部主机的 IP 地址和端口信息，所以，也只有有记录的 IP 地址和端口信息，能够将信息传入到 NAT 内部。

[0012] 出于安全性考虑，全双工 Cone NAT 和受限制的 Cone NAT 很少被采用。仅当内部服务器希望对外提供服务时，使用全双工 Cone NAT 建立内部服务器到 NAT 公网地址和某个特定端口的一一映射。

[0013] 由于在使用中的 NAT 出于种种安全性考虑，屏蔽了外部主机对内部用户的访问，因此，内部用户可以自由的通过 NAT 对外部主机进行访问，但相反，外部主机不能自由地通过 NAT 访问内部用户。同样地，一个 NAT 下的内部用户一般不可能直接访问另一个 NAT 下的内部用户。

[0014] 在目前以 BS 和 CS 架构下的应用环境下，这种方式是完全可行的，但是在 P2P 应用环境下，由于每一个用户都有可能为其他用户提供服务，而不仅仅是拥有公网地址的服务器。

[0015] 在现在技术中，解决以上两个问题的技术方案有两个：

[0016] 第一，解决外部的用户访问内部用户的问题。使用某种方法通知内部用户主动访问外部用户，就能使得该外部用户的 IP 地址和端口号被 NAT 记录，从而使得外部用户可以通过 NAT 访问内部用户，实际上是一种反联的方式，上述通知的过程一般是通过一个第三方设备来进行，因而所有的外部/内部用户都预先与第三方设备建立联系，由第三方设备进行通知过程。

[0017] 第二，解决一个 NAT 下的内部用户与另一 NAT 下的内部用户的互访问题。采用一个位于公网上的第三方设备，所有的内部用户都可以自由访问该第三方设备，由该第三方设备充当代理 (proxy)，用于转发在任何两个内部用户之间的所有数据报文。

[0018] 以上第二种方案缺陷比较明显，需要公网上的第三方设备进行所有流量的转发，这将消耗大量的网络资源。

[0019] 公知地，Cone NAT（以下除非特殊注明，下述 NAT 一般指端口限制的 Cone NAT）具有一个特性，当用户在一次会话中，使用同一个源 IP 地址和源端口，向外网任何地址的主机进行访问时，Cone NAT 都会使用同一个 NAT 的外网出口地址和源端口，向外网的主机进行访问。本发明认识到，可以利用 Cone NAT 这一特性来实现一个 NAT 下的内部用户与另一 NAT 下的内部用户的直接互访，而无需通过一个外部的第三方代理。

[0020] 一个重要问题出现了，绝大部分 NAT 设备，例如 Cisco 路由器、WinXP、Linux IPTABLE、Wingate、Sysgate 等等，通常都表现为 SymmetricNAT，而是在一些特定条件下才表现出 Cone NAT 的特性。

[0021] 名词解释：

[0022] NAT：用于内部地址与外部地址转换的设备。定义在 IETF RFC1631，RFC3022。

[0023] Cone NAT：在一次回话中，使用同一端口号向不同目标地址和端口发送的连接报文，NAT 都会转换为同一源端口的报文。

[0024] Symmetric NAT：使用同一端口号向不同目标地址和端口发送的连接报文，NAT 都会转换为不同源端口的报文。

[0025] 用户装置：完成对 NAT 的探测和与另一方 NAT 下用户装置进行通信。

[0026] 通知装置：转发 NAT 下的用户装置的通知报文。

[0027] 辅助探测装置：应答用户装置发送的探测报文，获取 NAT 外网地址和被 NAT 所转换的源端口信息，发送给相应的用户装置。

[0028] NAT 穿透端口：NAT 上被用户装置所探测出，并用于 NAT 穿透通信的端口，与内网用户装置的本地穿透端口一一映射。

[0029] 本地穿透端口：用户装置所探测出可以用于 NAT 穿透通信的本地源端口，在 NAT 上与 NAT 穿透端口一一映射。

发明内容

[0030] 本发明的目的是提供一种位于 NAT 下与在不同 NAT 下的其他设备进行直接穿透通信的设备及其方法。

[0031] 根据本发明的第一方面，提供一种在 NAT 下的用户装置中与在不同 NAT 下的用户装置进行直接穿透通信的通信方法，包括以下步骤：

[0032] - 选择一个本地源端口，用以发送和接收报文；

[0033] - 获取所述本地源端口在 NAT 上的对应的 NAT 外网地址和 NAT 端口；

[0034] - 通过一个外网的通知装置将自己的所述 NAT 外网地址和 NAT 端口通知另一个 NAT 下的用户装置，并通过外网的通知装置获知来自所述另一个 NAT 下的用户装置的 NAT 外网地址和 NAT 端口；

[0035] - 通过所述本地源端口，所述的用户装置和对端的用户装置分别使用所接收的对方 NAT 的外网地址和 NAT 端口作为目标地址进行直接通信。

[0036] 根据本发明的第二方面，提供了一种在 NAT 下的用户装置中用于检测所选择的本地源端口是否为穿透端口的方法，包括以下步骤：

[0037] —选择一个本地源端口；

[0038] —通过所述源端口经由 NAT 向外网辅助探测装置上的多个目标端口或向外网的多个辅助探测装置发出多次探测报文；

[0039] —接收来自所述外网辅助探测装置的探测应答报文，其中所述探测应答报文的内容包括所述探测报文在 NAT 上对应的 NAT 源地址和 NAT 端口；

[0040] —获取所述探测报文被 NAT 上转换后的 NAT 源地址和 NAT 源端口；

[0041] —如果多次探测报文的 NAT 源端口都相同，则判断所述本地端口为与其他设备的端口没有冲突的本地穿透端口；

[0042] —否则，再选择一个不同的本地源端口，重复以上步骤，直到找到合适的端口为止。

[0043] 根据本发明的第三方面，提供了一种在 NAT 下的用户装置，其用于通过一个特定的本地端口与另一个 NAT 下的用户装置直接穿透通信，该用户装置有多个网络端口，还包括：

[0044] 选择装置，用于选择一个本地源端口，用以发送和接收报文；

[0045] 探测装置，用于获取所述本地源端口在 NAT 上的对应的 NAT 源地址和 NAT 端口；

[0046] 端口信息交换装置，用于通过一个外网的通知装置将所述 NAT 源地址和 NAT 端口通知其他 NAT 下的另一个用户装置，并通过外网的通知装置来获知来自所述另一个 NAT 下的用户装置的 NAT 源地址和 NAT 端口，

[0047] 其中，通过所述本地源端口，所述用户装置和对端的用户装置分别使用所接收的对方 NAT 源地址和 NAT 端口作为目标地址进行直接通信。

[0048] 根据本发明的第四方面，提供了一种在外网辅助探测装置中用于辅助 NAT 下的用户装置获取其本地源端口所对应的 NAT 端口的方法，包括：

[0049] 接收来自所述用户装置的探测报文；

[0050] 由所接收的探测报文中解析出报文源地址和源端口信息；

[0051] 通过应答报文将所解析出的报文源地址和源端口信息发送给所述用户装置。

[0052] 根据本发明的第五方面，提供了一种在外网中用于辅助 NAT 下的用户装置获取其本地源端口所对应的 NAT 端口的辅助探测装置，包括：

[0053] 报文解析装置，用于由所接收的探测报文中解析出报文源地址和源端口信息；

[0054] 发送装置，通过应答报文将所解析出的报文源地址和源端口信息发送给所述用户装置。

[0055] 与现有技术不同，根据本发明的技术方案，解决不同 NAT 下的用户装置直接相互通信的问题，不需要所有的报文都通过外部代理来转发

附图说明

[0056] 下面参照附图来对本发明进行详细描述，其中相同的附图标记表示相同或相似的部件：

[0057] 图 1 为根据本发明的一个优选实施例的支持分别处于不同 NAT 下的用户装置进行直接穿透通信的拓扑结构图；

[0058] 图 2 为所选择的用户装置源端口不可以穿透通信的情形的示意图；

[0059] 图 3 为所选择的用户装置源端口可以穿透通信的情形的示意图；

[0060] 图 4 为根据本发明一个优选实施例的在不同 NAT 下的用户装置进行直接穿透通信方案中通知阶段的示意图；

[0061] 图 5 为根据本发明一个优选实施例的在不同 NAT 下的用户装置进行直接穿透通信方案中通信建立阶段的示意图；

[0062] 图 6 为根据本发明一个优选实施方式的用于支持在不同 NAT 下的用户装置进行直接穿透通信的通信方法的流程图；

[0063] 图 7 为根据本发明的一个优选实施例的在一个 NAT 下用于与在不同 NAT 下的其他用户装置进行直接穿透通信的用户装置的框图；

[0064] 图 8 为根据本发明一个优选实施例的辅助探测装置的框图。

具体实施方式

[0065] 下面参考附图，并结合具体实施例对本发明作详细描述。应当理解，本发明并不限于具体实施例。

[0066] 图 1 为根据本发明的一个优选实施例的支持分别处于不同 NAT 下的用户装置进行直接穿透通信的拓扑结构图。图中示出四种不同设备：用户装置 A 1 和用户装置 B（为简明起见，仅给出用户装置 A 的附图标记），NAT A 2 和 NAT B（为简明起见，仅给出 NAT A 的附图标记），通知装置 3，辅助探测装置 4。

[0067] NAT2 在内网和外网之间，完成地址转换功能。

[0068] 用户装置 A 和 B 分别处于 NAT A 和 NAT B 之下，运行在内网环境下，由于通知装置 3 和辅助探测装置 4 运行在外网环境下，所以用户装置 A 和 B 都可以自由访问通知装置 3 和辅助探测装置 4。

[0069] 根据本发明的用于在不同 NAT 下进行直接穿透通信的技术方案包括通知建立阶段、通知建立阶段、通知阶段和通信建立阶段等四个阶段。下面结合图 1 并参照图 2-5 来对这四个阶段进行详细描述。

[0070] 通知建立阶段：

[0071] 通知装置 3 是一个信令代理和信令处理装置，可以完成用户装置之间的信息共享。通知装置 3 可以通过两种方式来实现信息共享，一种方式是同步方式，另一种方式是异步方式。

[0072] 同步方式时，通知装置 3 的功能包括：注册功能、握手功能、信令转发功能，这三种功能具体如下所述：

[0073] 注册功能：用户装置 A 和 B 使用预设唯一的识别号 ID，访问通知装置，在通知装置上完成注册。

[0074] 握手功能：用户装置 A 和 B 需要维持与通知装置的连接，以便通知装置 3 及时与用户装置进行通信。因为，长时间不通信，NATA 和 NATB 上的通信端口会被 NAT 所老化掉，老化时间可配置（一般为 1 分钟）。所以用户装置需要定时（一般为 30 秒）向通知装置发送握手报文，该握手报文没有实际意义，通知装置 3 也可以不响应，仅用于维持 NAT 端口不被老化，保持用户装置 A 和 B 分别经由 NAT A 和 NAT B 的与通知装置 3 的长连接。长连接的意义就在于不仅仅用户装置可以向通知装置 3 发送报文，通知装置 3 也可以向用户装置 A 和 B 发送报文。

[0075] 在异步方式中，用户装置不一定要与通知装置 3 建立一个长连接，而是用户装置定时（例如几分钟）到通知装置 3 上提取自己所要（其他装置发送给自己）的信息。其中，通知装置 3 可以预先为每个用户装置分配一个存储区域。

[0076] 用户装置 A 1 通过发送信息到通知装置 3，并标明该信息是要实际发送给用户装置 B 的，则通知装置 3 将该信息放到用户装置 B 可以访问的存储区域，而不需要主动告诉用户装置 B。当用户装置 B 定时来访问通知装置 3 上预设的存储区域时，就可以获取用户装置 A 发送给自己的信息。

[0077] 异步方式下的通知装置 3 也可以采用电子邮件服务器，就可以达到同样的功能。

[0078] 探测阶段：

[0079] NAT 在以下特定情况下表现为 Cone NAT 特性，也就是同一个内网内的通信主机和设备（用户装置），经由 NAT 在对外访问时，使用的 NAT 源端口不能与其他内部主机和设备所使用的 NAT 源端口一致。当用户装置使用这样的特殊端口访问不同的外部地址和端口时，NAT 就采用一个端口与之相对应，而不需要打开多个端口。这表现为 Cone NAT 特性。

[0080] 由于用户装置无法获知同一个 NAT 下的其他用户采用哪些 NAT 源端口，也就无法获知自己所用端口是否与同一内网下的其他用户装置所用端口相冲突，而如果出现冲突，则不能获得 Cone NAT 的应用环境。

[0081] 所以，用户装置可以，通过不断（在端口号为 2000 以上的端口中，因为一般地，端口号为 1024 以下的端口大部分为系统所占用）选择一个源端口（用户装置的源端口）直至通过一个源端口能够进行正常通信的方式，来判断是否找到一个具有 Cone Nat 特性（也即，不与在同一 NAT 下的其他用户装置所用端口相冲突）的源端口。另外，所以用户装置也可通过一个外部的辅助探测装置 4 来探测所选择的源端口是否与与在同一 NAT 下的其他用户装置所用端口相冲突，具体的，用户装置以该选择的源端口发送探测报文给辅助探测装置 4，并接收来自辅助探测装置 4 的探测应答报文，然后通过所接收的探测应答报文来判断该源端口是否与其他用户装置所用端口相冲突。

[0082] 下面表 1-2 为探测报文和探测应答报文的数据结构的示例：

[0083] 表 1：探测报文：

		发起探测报文	NAT 转换后的发起探测报文
报文头	目标地址	辅助探测装置 IP 地址	辅助探测装置 IP 地址
	目标端口	辅助探测装置端口号	辅助探测装置端口号
	源地址	本地主机内网地址	NAT 外网地址
	源端口	本地选择端口	NAT 按照预定规则选择的端口
报文内容		本地端口	本地端口

[0084] 表 2：探测应答报文

		探测应答报文	NAT转换后的探测应答报文
报文头	目标地址	NAT 外网地址	本地主机内网地址
	目标端口	NAT 按照预定规则选择的端口	本地选择端口
	源地址	辅助探测装置 IP 地址	辅助探测装置 IP 地址
	源端口	辅助探测装置端口号	辅助探测装置端口号
报文内容		本地端口 NAT 外网地址 NAT 按照预定规则选择的端口	本地端口 NAT 外网地址 NAT 按照预定规则选择的端口

[0085] 图 2 示出了所选择的用户装置本地源端口不可以穿透通信的情形。其中，同一用户装置 1 的源端口、源地址的报文因为目标地址、端口不同，被 NAT 转换为经由多个 NAT 源端口（图中示出三个不同端口）发送的报文。

[0086] 而图 3 示出了所选择的本地源端口可以穿透通信的情形。其中，同一用户装置的源端口、源地址的报文被 NAT 2 转换为经由 NAT 的同一个 NAT 源端口发送的报文。

[0087] 通过探测过程，用户装置 1 就能获取到每一次发送报文被 NAT 转换后的 NAT 源端口号。重复探测过程，当用户装置 1 发现通过一个特定的用户源端口发送报文时，无论发送给辅助探测装置 4 的任何一个端口或发送给多个辅助探测装置 A 和 B 时，NAT 都使用同一个 NAT 端口进行转发。就发现该用户端口体现出 Cone NAT 特性，可以使用该用户端口作为本地穿透端口，而对应的 NAT 端口被称为 NAT 穿透端口。

[0088] 通知阶段：

[0089] 图 4 为根据本发明一个优选实施例的在不同 NAT 下的用户装置进行直接穿透通信方案中通知阶段的示意图；

[0090] 信令转发：当用户装置 A 1 需要告知用户装置 B 自己的 NAT 穿透端口时，用户装置 A 通过发送信息到通知装置 3，并标明内容是要实际发送给用户装置 B 的，通知装置将该信息重新封装新的 IP 地址和端口号以后，通过在上述同步方式中与用户装置 B 预先建立的长连接端口，发送该信息给用户装置。用户装置 B 收到该报文后，从中提取出用户装置 A 的 NAT 穿透端口。

[0091] 用户装置 B 重复以上步骤，使得用户装置 A 也获得用户装置 B 的 NAT 穿透端口。

[0092] 通信建立阶段：

[0093] 图5为根据本发明一个优选实施例的在不同NAT下的用户装置进行直接穿透通信方案中通信建立阶段的示意图；

[0094] 其中，用户装置A 1向用户装置B发送通信握手报文，如下表3所示。

[0095] 表3

		用户装置A握手报文	用户装置B握手报文
报文头	目标地址	NAT B外网地址	NAT A外网地址
	目标端口	用户装置B的NAT穿透端口	用户装置A的NAT穿透端口
	源地址	用户装置A的本地内网地址	用户装置B的本地内网地址
	源端口	用户装置A的穿透端口	用户装置B的穿透端口
报文内容		ACK	ACK

[0096] 报文内容表示收到报文，没有实际意义。

[0097] 用户装置互相成功收到报文后，就表明NAT A已经成功将用户装置A的穿透端口与用户装置B的NAT穿透端口建立绑定关系，NAT B已经成功将用户装置B的穿透端口与用户装置A的NAT穿透端口建立绑定关系（此为端口受限制的NAT的特性，为现有技术）。

[0098] 用户装置A和B使用根据探测过程选定的穿透源端口，将对方的NAT外网地址和NAT源端口，作为目的地址和目的端口，发送握手包。由于NAT A和NAT B会分别记录下其内网用户装置A和B向哪一个外部地址和端口发起过报文，以此来判断外部地址和端口号的报文，是否是对方的合法应答报文，如果某个来临报文的目标地址是NAT地址，目标端口是NAT已经分配给内网用户装置（例如内部主机和设备）的NAT穿透端口号，但如果该报文的源地址和源端口号，在预定时间内没有被由该NAT穿透端口号发出的报文访问过，NAT就会认为是该报文是非法报文而将其丢弃。但是，通过NAT下的主机和设备在一定时间内重复地相互对发探测报文，就可以让两端的NAT确认对方发出的报文是本方所发出报文的应答报文，从而，这些报文就可以有效地传送到对方的用户装置上。

[0099] 通信阶段：

[0100] 在通信建立过程之后，在NAT A和NAT B之下的两个用户装置A和B就可以进行直接穿透通信，也即进入通信阶段。图5示出了根据本发明一个优选实施例的用于在不同NAT下进行直接穿透通信方案中的通信阶段的示意图

[0101] 用户装置A发送通信报文给用户装置B的NAT穿透端口和NAT外网地址，用户装置B通过本地穿透端口接收用户装置A发送的报文。

[0102] 用户装置B发送通信报文给用户装置A的NAT穿透端口和NAT外网地址，用户装置A通过本地穿透端口接收用户装置B发送的报文。

[0103] 用户装置 A 和 B 所发送的报文的具体内容如下表 4 所示：

[0104] 表 4

		用户装置 A 发送报文	用户装置 B 发送报文
报文头	目标地址	NAT B 外网地址	NAT A 外网地址
	目标端口	用户装置 B 的 NAT 穿透端口	用户装置 A 的 NAT 穿透端口
	源地址	用户装置 A 的本地内网地址	用户装置 B 的本地内网地址
	源端口	用户装置 A 的穿透端口	用户装置 B 的穿透端口
报文内容		有效载荷	有效载荷

[0105] 其中，报文内容为有效数据载荷。

[0106] 图 6 为根据本发明的用于支持在不同 NAT 下的用户装置进行直接穿透通信的通信方法的流程图，下面参照图 6 对该方法进行详细说明：

[0107] 在步骤 S1 中，NAT 下的用户装置首先向外网的通知装置进行注册，每个用户装置有一个特定的 ID 识别号，通知装置将这个识别号与相应的信令端口和信令 IP 地址进行绑定，随后进到步骤 S2；

[0108] 在步骤 S2 中，NAT 下的用户装置与外网的通知装置进行定时握手，以防止 NAT 上的端口不被老化（这一步骤是可选的，因为 NAT 上的端口可以保持一定时间不被老化），随后进到步骤 S3；

[0109] 在步骤 S3 中，NAT 外部的辅助探测装置打开多个端口，NAT 下的用户装置选择 1 个本地源端口（其中，端口号高于 2000 成功率较高，因为 2000 以下的端口大部分为系统占用），同时向多个辅助探测装置或一个辅助探测装置上的多个目标端口发出探测报文，探测报文中填写本地源端口号，NAT 将该报文的源地址转换为 NAT 的外网地址，将本地源端口转换为按照预定规则选择的 NAT 源端口，辅助探测装置根据收到的被 NAT 转换后的探测报文的源 IP 地址和源端口号，将该源 IP 地址和源端口号填写在应答报文的数据域中，将应答报文发送回发起探测的用户装置，填写的目标 IP 地址和目标端口号应是 NAT 的外网地址和发起探测的用户装置相对应的 NAT 端口号；

[0110] 在步骤 S4 中，NAT 下的用户装置接收的探测应答报文，获取到自己上次发送的探测报文在 NAT 上的相应的 NAT 端口号。

[0111] 在步骤 S5 中，用户装置检测并判断选择某个源端口发出多个探测报文时在 NAT 上是否被映射为同一个 NAT 源端口号，如果是，则进到步骤 S6，否则，重复上述步骤 S3 和 S4。

[0112] 在步骤 S6 中，用户装置就会选择这一特定的本地源端口作为发送和接收之用的本地穿透端口号，而将 NAT 上相应的 NAT 穿透端口通知其他用户装置；

[0113] 并且，优选的，用户装置可定时通过该本地穿透端口发送握手报文给外部装置，以维持该端口不被 NAT 老化。

[0114] 在随后的步骤 S7 中，NAT 下的用户装置向 NAT 外部的通知装置发送通知报文，报文内容至少包含：发送方 ID，接收方 ID，发送方的 NAT 地址和穿透端口。

[0115] 在步骤 S8 中，通知装置接收到通知报文后，解析报文内容，根据接收方 ID，查询相应的信令端口和信令 IP 地址，将报文重新封装后发送给相应的接收方用户装置。

[0116] 在步骤 S9 中，接收的用户装置收到通知报文后，获取到对方的 NAT 地址和 NAT 穿透端口。

[0117] 在步骤 S10 中，接收的主机也向对方发送通知报文，重复上述步骤 S7-S9 步骤，直到双方都获取到对方的 NAT 地址和穿透端口。

[0118] 在步骤 S11 中，两个 NAT 下的用户装置就可以通过预定的本地穿透端口，将对方的 NAT 外网地址和端口，作为目的地址和目的端口，向对方发送握手包。

[0119] 在随后的步骤 S12 中，用户装置判断是否收到握手包后，如果收到即表明可以使用该穿透端口进行通信，如果不能收到，重复发送步骤 S11。（这是由于握手包在实际网络环境中可能丢失，不是必要技术特征）

[0120] 在步骤 S13 中，一旦该握手建立完成，两个不同 NAT 下的用户装置就可以通过既定的源端口进行自由通信，当然限制条件是必须使用该既定端口才可以互相通信。

[0121] 图 7 示出了根据本发明的一个优选实施例的在一个 NAT 下用于与在不同 NAT 下的其他用户装置进行直接穿透通信的用户装置的框图。

[0122] 其中，所述用户装置 1 包括：

[0123] 一个选择装置 11，用于选择一个本地源端口，用以发送和接收报文；

[0124] 一个探测装置 12，用于获取所述本地源端口在 NAT 上的对应的 NAT 源地址和 NAT 端口；

[0125] 一个端口信息交换装置 13，用于通过一个外网的通知装置将所述 NAT 源地址和 NAT 端口通知其他 NAT 下的另一个用户装置，并通过外网的通知装置来获知来自所述另一个 NAT 下的用户装置的 NAT 源地址和 NAT 端口，

[0126] 其中，通过所述本地源端口，所述用户装置和对端的用户装置分别使用所接收的对方 NAT 源地址和 NAT 端口作为目标地址进行直接通信。

[0127] 在一个优选实施例中，所述探测装置 12 包括：

[0128] 一个探测报文发送装置 121，用于通过所述本地源端口经由 NAT 向外网的辅助探测装置发送探测报文；

[0129] 一个应答报文接收装置 122，用于接收来自所述外网的辅助探测装置的应答报文，在所述应答报文中包括所述探测报文的被 NAT 转换后的 NAT 源地址和 NAT 源端口；和

[0130] 一个提取装置 123，用于从所述应答报文中提取出所述探测报文被 NAT 转换后的 NAT 源地址和 NAT 源端口。

[0131] 优选的，如果在所述用户装置在限定时间不能实现正常通信时，则所述选择装置就重新选择一个不同的本地源端口；而所述探测装置也用于重新获取所述重新选择的本地源端口在 NAT 上的对应的 NAT 源地址和 NAT 端口。

[0132] 在另一个优选实施例中，所述探测装置 12 包括：

[0133] 一个探测报文发送装置 121，用于通过所选择的本地源端口经由 NAT 向外网辅助探测装置上的多个目标端口或向外网的多个辅助探测装置发出多次探测报文；

[0134] 一个应答报文接收装置 122，用于接收来自所述外网辅助探测装置的多个应答报文，其中所述每个应答报文的内容包括其对应的探测报文被 NAT 转换后的 NAT 源地址和 NAT 端口；

[0135] 一个提取装置 123，用于从所述应答报文中提取出所述探测报文被 NAT 转换后的 NAT 源地址和 NAT 源端口；

[0136] 一个确定装置 124，如果所述多次探测报文的 NAT 源端口都相同，则确定所述本地端口为与其他设备的端口没有冲突的本地穿透端口，并以所述 NAT 源地址和 NAT 端口作为最后选择的 NAT 外网地址和 NAT 端口。否则，选择装置 11 重新选择一个不同的本地源端口，在由探测装置 12 来通过发送多次探测报文来确定该本地源端口是否为与其他设备的端口没有冲突的本地穿透端口。

[0137] 端口信息交换装置 14 将最后确定的 NAT 穿透端口信息经由外网的通知装置告知在不同 NAT 下的另一个用户装置，并获知所述另一个用户装置的的 NAT 源地址和 NAT 穿透端口，从而可以通过本地穿透端口将对方的 NAT 源地址和 NAT 穿透端口作为目的地址和目的端口进行通信。

[0138] 图 8 还示出了根据本发明一个优选实施例的辅助探测装置的框图，所述辅助探测装置位于外网，用于辅助 NAT 下的用户装置获取其本地源端口所对应的 NAT 端口，其中辅助探测装置 4 包括：

[0139] 报文解析装置 41，用于由所接收的探测报文中解析出报文的源地址和源端口信。

[0140] 发送装置 42，通过应答报文将所解析出的报文源地址和源端口信息发送给所述用户装置。

[0141] 为简明起见，在上下文中引用了内网和公网，内部地址和公有地址等术语，但本发明不仅仅应用于内网和公网领域，而是适用于任何 NAT 应用领域下，例如：在企业内部可能有多级 NAT，两个组织下的用户装置分别处于不同 NAT 下。

[0142] 本发明优选地适用于通过 UDP 的通信。

[0143] 对于完全的 Symmetric NAT，本发明并不适用。但是大部分商用的 NAT 都是采用一种混合模式，大部分情况下表现为 Symmetric NAT，特殊情况下表现为 Cone NAT。

[0144] 以上对本发明的具体实施例进行了描述。需要理解对是，本发明并不局限于上述特定对实施方式，本领域技术人员可以在所附权利要求的范围内做出各种变形或修改。

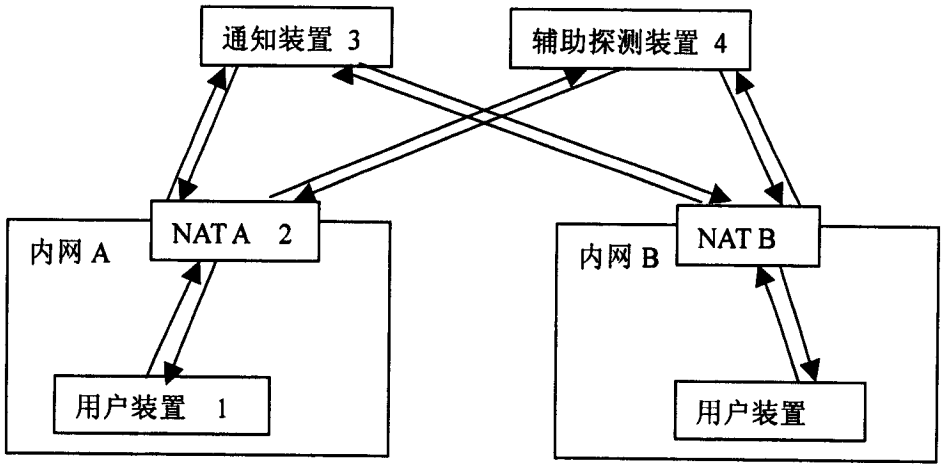

通知装置 3
辅助探测装置 4
NAT A 2
NAT B
内网 A
内网 B
用户装置 1
用户装置

图 1

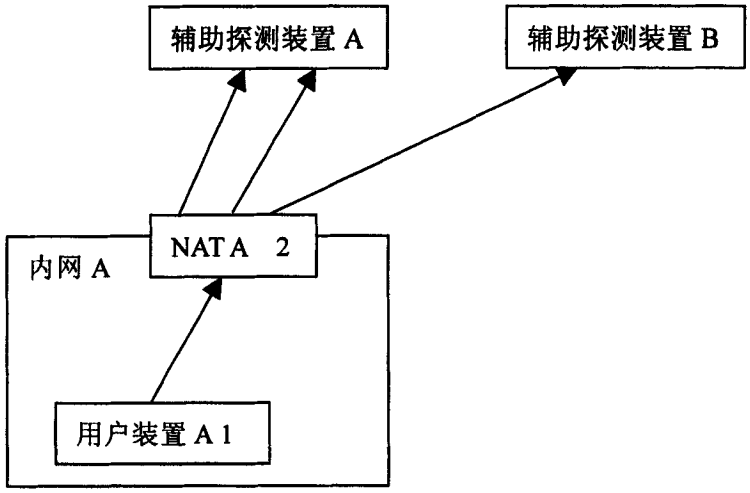

辅助探测装置 A
辅助探测装置 B
NAT A 2
内网 A
用户装置 A 1

图 2

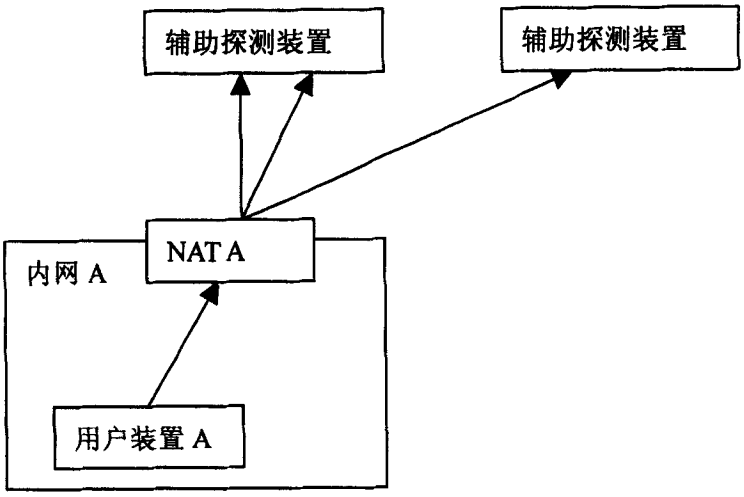

辅助探测装置
辅助探测装置
NAT A
内网 A
用户装置 A

图 3

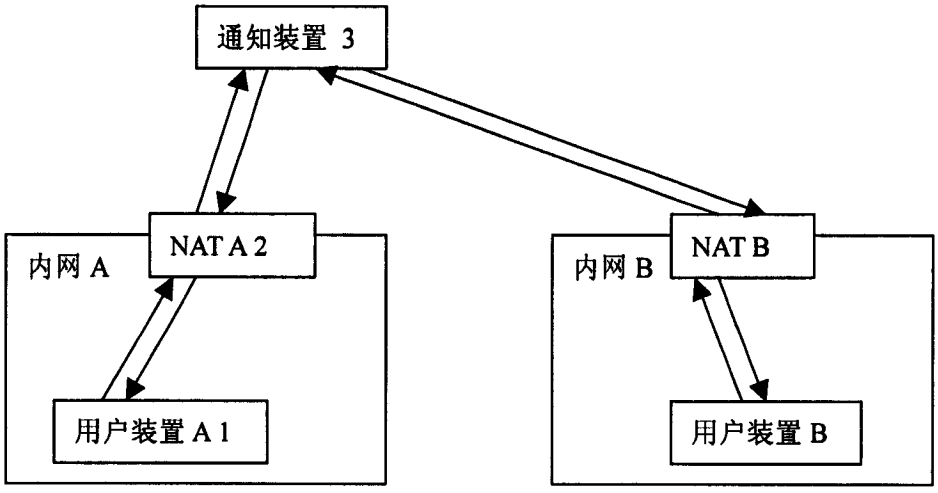

通知装置 3
NAT A 2
内网 A
NAT B
内网 B
用户装置 A 1
用户装置 B

图 4

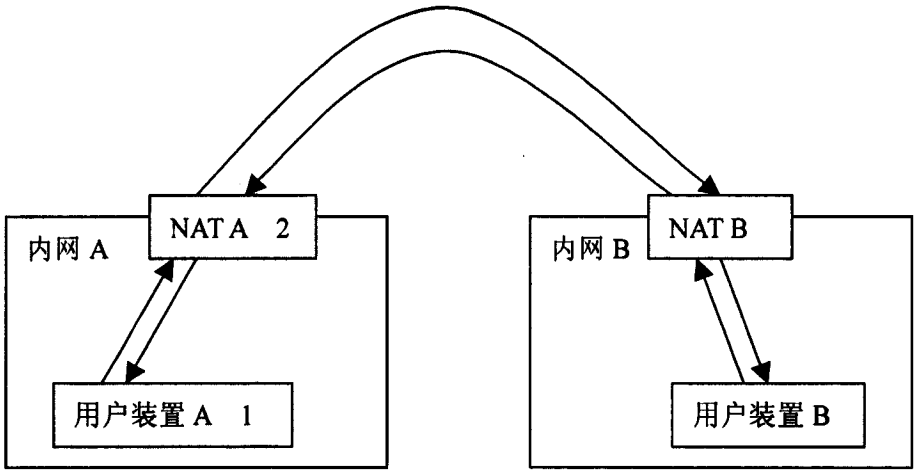


图 5

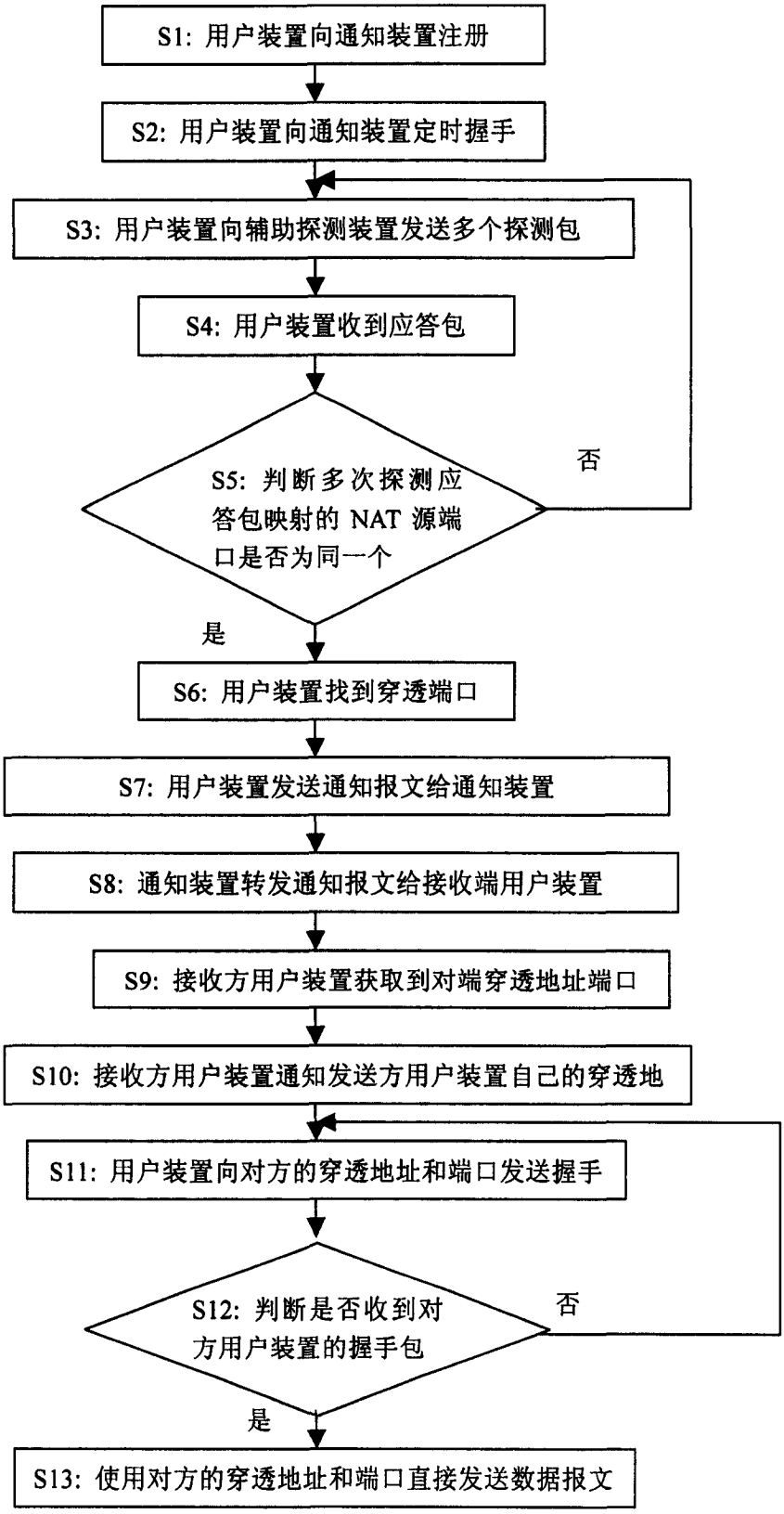

S1: 用户装置向通知装置注册
S2: 用户装置向通知装置定时握手
S3: 用户装置向辅助探测装置发送多个探测包
S4: 用户装置收到应答包
S5: 判断多次探测应答包映射的 NAT 源端口是否为同一个
否
是
S6: 用户装置找到穿透端口
S7: 用户装置发送通知报文给通知装置
S8: 通知装置转发通知报文给接收端用户装置
S9: 接收方用户装置获取到对端穿透地址端口
S10: 接收方用户装置通知发送方用户装置自己的穿透地
S11: 用户装置向对方的穿透地址和端口发送握手
S12: 判断是否收到对方用户装置的握手包
否
是
S13: 使用对方的穿透地址和端口直接发送数据报文

图 6

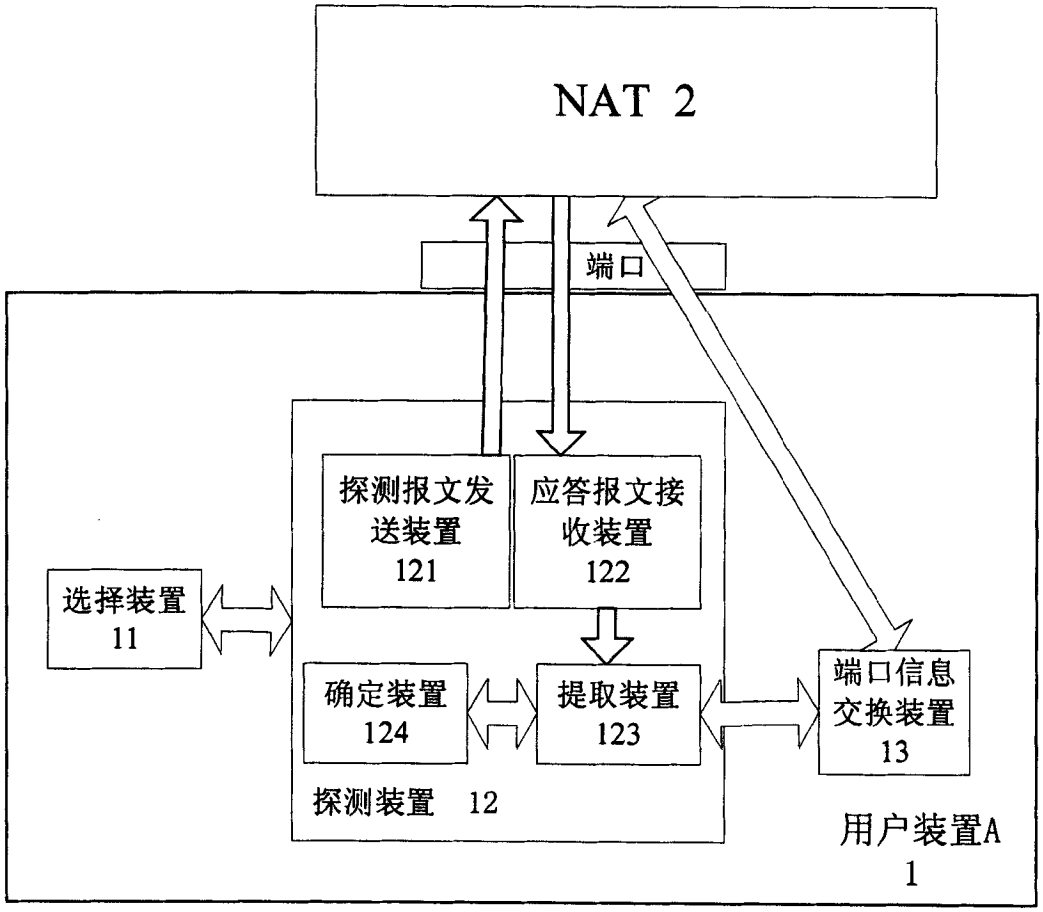

NAT 2
端口
探测报文发送装置 121
应答报文接收装置 122
选择装置 11
确定装置 124
提取装置 123
端口信息交换装置 13
探测装置 12
用户装置A 1

图 7

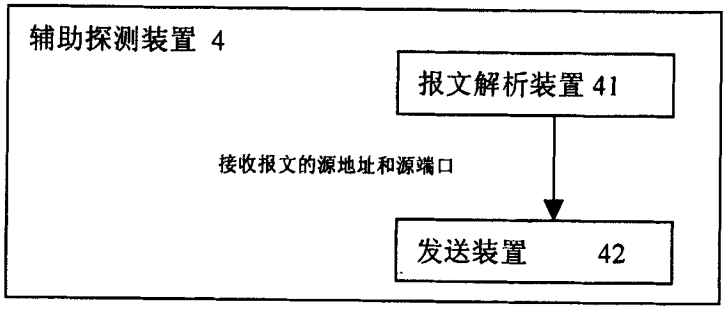

辅助探测装置 4
报文解析装置 41
接收报文的源地址和源端口
发送装置 42

图 8