

[19] 中华人民共和国国家知识产权局

[51] Int. Cl⁷

H04L 12/28

H04L 29/06 H04Q 3/00

H04Q 3/545



[12] 发明专利申请公开说明书

[21] 申请号 03158973.1

[43] 公开日 2004 年 9 月 1 日

[11] 公开号 CN 1525699A

[22] 申请日 2003.9.17 [21] 申请号 03158973.1

[71] 申请人 中国科学院计算技术研究所

地址 100080 北京市中关村科学院南路 6 号

[72] 发明人 吴贤国 刘 敏 张天乐 石晶林
李忠诚

[74] 专利代理机构 中科专利商标代理有限责任公
司

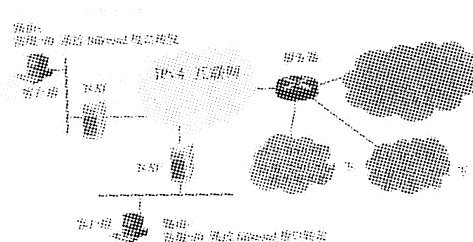
代理人 周国城

权利要求书 8 页 说明书 11 页 附图 5 页

[54] 发明名称 一种可穿越网络地址翻译的自动隧
道的方法

[57] 摘要

本发明涉及互联网技术领域，一种可穿越 NAT (网络地址翻译) 的自动隧道技术，也就是该隧道技术允许隧道主体存在任何类型和任意数量的 NAT，它是一种新的 IPv4 互联网向 IPv6 互联网过渡时期的隧道技术。目的是为了使 NAT 域内的 IPv6/IPv4 双栈节点获得全球端到端 IPv6 连接。利用该隧道技术 NAT 域内的 IPv6/IPv4 双栈节点将通过中间服务器和不在 NAT 域内的 IPv6 节点进行通信，对同为 NAT 域内的 IPv6/IPv4 双栈节点之间。



I S S N 1 0 0 8 - 4 2 7 4

- 1、一种可穿越 NAT 的自动隧道的方法，其特征在于，提出了一种将 IPv6 数据包封装在 UDP 载荷中的隧道技术，称这种隧道为 SilkRoad 隧道，SilkRoad 不受隧道主体上存在任意类型和任意数量的 NAT 的影响，
- 5 可将 IPv6 数据包从隧道首节点传送到隧道尾节点。

2、根据权利要求 1 所述的方法，其特征在于，该隧道技术定义了 3 个通信实体，用于实现上述的方法：

Silkroad 客户端，表示 NAT 域内的 IPv6/IPv4 双栈节点，支持 Silkroad 隧道功能，有一个全球单播聚类 IPv6 地址和一个私有 IPv4 地址；

10 址；

Silkroad 服务器，在 NAT 域外，表示为客户端分配 IPv6 地址并具有路由功能的 IPv6/IPv4 双栈节点，支持 Silkroad 隧道功能，有一个公有 IPv4 地址，它可以有通向 IPv6 骨干网的路由，也可以有通向孤立 IPv6 网络的路由；

15 普通 IPv6 节点，表示除客户端和服务端以外的其他 IPv6 节点。

3、根据权利要求 1 所述的方法，其特征在于，客户端通信时采用的 IPv6 地址是一种规定格式的地址，它包括 64 位的 IPv6 地址前缀和 64 位的接口标识符，接口标识符由伪外部端口字段、NAT 类型标志位字段、Silkroad 地址标志位字段和伪外部地址字段组成，各部分说明如下：

20 ◆ IPv6 前缀：

IANA 正式分配的全球聚类单播地址前缀或“site-local”地址前缀，不可以是“link-local”地址前缀或组播地址前缀；

◆ 伪外部端口：

外部端口，即经 NAT 映射后的端口和 0xFFFF 与或后的 16 位数值，SilkRoad 客户端启动后向服务器发送一个初始化数据包，该包

25 经过 NAT 时其 UDP 端口被映射成一个不同的端口，我们称之为外部端口；服务器从接收到的初始化数据包中获得此端口，考虑到 NAT 会删除过期的映射关系，客户端或服务端，将周期性的向 NAT 发送数据包以维持这种映射关系，所以 NAT 的转换表中始终保留该映射关系，

对外部端口进行与或操作的目的是为了防止某些 NAT 将 UDP 数据包载荷,即 IPv6 头部+IPv6 载荷中的外部端口进行转化;

◆ NAT 类型标志位:

5 长度为 2 位,用来表示客户端所在 NAT 的类型,00 表示客户端位于“cone” NAT 域,10 表示客户端位于“Restricted” NAT 域,11 表示客户端位于“Symmetric” NAT 域;

◆ Silkroad 地址标志位:

10 长度为 14 位,设为 0,表示该地址是一 Silkroad 地址,将该字段放在接口标识符中间的目的在于避免和其他地址冲突,因为目前只要不是随机分配的接口标识符,其中间 16 位都是 FFFE;

◆ 伪外部地址:

15 外部地址,即经 NAT 映射后的地址和 0xFFFFFFFF 与或后的 32 位数值,客户端启动后向服务器发送一个初始化数据包,该包经过 NAT 时其私有 IPv4 地址被映射成一个公有 IPv4 地址,称之为外部地址,服务器从接收到的初始化数据包中获得此地址,考虑到 NAT 会删除过期的映射关系,客户端或服务器,将周期性的向 NAT 发送数据包以维持这种映射关系,所以 NAT 的转换表中始终保留该映射关系,对外部地址进行与或操作的目的是为了防止某些 NAT 将 UDP 数据包载荷,即 IPv6 头部+IPv6 载荷中的外部端口进行转化。

20 4、根据权利要求 1 所述的方法,其特征在于,客户端和其他 IPv6 节点通信时发送或接收的数据包由 IPv4 头部、UDP 头部、IPv6 头部以及 IPv6 载荷组成;

具体说明如下:

● IPv4 头部:

25 源 IPv4 地址为客户端的 IPv4 地址,即私有地址,目的 IPv4 地址为服务器的 IPv4 地址,如果目的地是普通 IPv6 节点或对方客户端经 NAT 映射后的外部地址,如果目的地是另一客户端;

● UDP 头部:

30 源端口为 5188,目的端口为 5188,如果目的地是普通 IPv6 节点或对方客户端经 NAT 映射后的外部端口,如果目的地是另一客户端;

- IPv6 头部:

包含源 IPv6 地址和目的 IPv6 地址, 其中至少有一个是 SilkRoad 地址;

- IPv6 载荷:

5 由 0 或若干个 IPv6 扩展头部, 以及上层协议数据单元, 即 PDU 组成;
 为了维持 NAT 中的映射关系, 如 “cone” NAT 的<源地址, 源端口,
 目的地址, 目的端口>, 客户端需要周期性的向 NAT 发送数据包, 称这种
 数据包为维持包, 在维持包的 IPv6 头部中, 下一跳字段设为 59, 表示
 没有 IPv6 载荷。

10 5. 根据权利要求 1 所述的方法, 其特征在于, 客户端通过 SilkRoad
 隧道接口发送或接收数据包, SilkRoad 隧道接口是一个逻辑接口, 它会
 自动将 IPv6 数据包封装在 UDP 载荷中进行发送, 同样, Silkroad 隧道
 接口接收到的数据包肯定是一个封装了 IPv6 报文的 UDP 数据包, 客户端
 有一个缺省路由 (:::/0), 它将所有 IPv6 地址视为同一链路上的地址并
15 使用 SilkRoad 隧道接口进行转发, 缺省路由的下一跳地址为 IPv6 数据
 包中的目的地址, 下一跳接口为 SilkRoad 隧道接口, 服务器有通向 IPv6
 骨干网以及各孤立 IPv6 网络的路由, 也有通向各客户端的路由, IPv6
 骨干网以及各孤立 IPv6 网络中任何一个 IPv6 节点发送的数据包, 只要
 目的地址前缀是服务器分配给客户端的地址前缀, 都将被路由至服务器,
20 以地址前缀 2001:*/64 为例, 服务器再通过去往客户端的路由将数据包
 转发至客户端; 同样, 客户端可通过服务器和 IPv6 骨干网以及各孤立 IPv6
 网络中的任何一个 IPv6 节点实现互访。

 6. 据权利要求 1 所述的方法, 其特征在于, 客户端每次启动后首先
 向服务器注册以获得一个 SilkRoad 地址, 这样才能和其他 IPv6 节点建
25 立通信, 这个过程我们称之为客户端的初始化配置;

 客户端的初始化配置通过向服务器发送一系列路由请求报文来完成,
 服务器以路由广告报文作为响应, 路由广告报文中含有客户端被 NAT
 映射后的外部地址和外部端口信息, 通过此过程客户端获得一个 SilkRoad
 地址并判断它位于何种 NAT 域内;

30 客户端的初始化配置过程如下:

- 1、户端向首选的服务器，即服务器 1 发送一个路由请求报文，报文的源 IPv6 地址是一个“link-local”地址，其 F 字段值为 00；
 - 2、服务器 1 收到路由请求报文后发送一个路由广告报文作为响应，因为路由请求报文显示客户端位于“cone” NAT 域内，F 字段值为 00，所以它选择一个不同的 IPv4 地址作为源地址发送路由广告报文，如果客户端能收到此报文，表明客户端确实位于“cone” NAT 域内；
 - 3、如果客户端没有收到此路由广告报文，它将再向服务器 1 发送一个路由请求报文，路由请求报文的源 IPv6 地址是另一个“link-local”地址，其 F 字段值为 10；
 - 4、服务器 1 收到路由请求报文后发送一个路由广告报文作为响应，因为路由请求报文显示客户端位于“Restricted” NAT 域内，它将以路由请求报文中的目的 IPv4 地址作为源 IPv4 地址发送路由广告报文，客户端如果收到此报文，表示它位于一个“Restricted” NAT 域内；
 - 5、客户端为了明确是否位于“Symmetric” NAT 域内，将再向另一个服务器，即服务器 2 发送路由请求报文，服务器 2 收到路由请求报文后发送一个路由广告报文作为响应；
 - 6、客户端收到此路由广告报文后和原先收到的路由广告报文作比较，如果报文包含的用来构造 SilkRoad 地址的信息相同，表示 NAT 的地址端口映射关系是一一对应的；如果不同，表示 NAT 将相同的内部地址和端口映射成了不同的外部地址和端口，映射关系是一对多，所以客户端认为它位于“Symmetric” NAT 域；
- 根据第 2、4 或 6 步收到的路由广告报文，客户端按如下构造一个 SilkRoad 地址：
- 地址的前 64 位设置为路由广告报文中的“前缀信息选项”，如 2001:***/64；
 - 接下去的 16 位设为路由广告报文中包含的外部端口；
 - 接下去的 2 位设为 00，如果客户端位于“cone” NAT 后或 10，如果客户端位于“Restricted” NAT 后或 11，如果客户端位于

“Symmetric” NAT 后;

- 接下去的 14 位设为 0;
- 最后 32 位设为路由广告报文包含的外部地址;

7. 根据权利要求 1 所述的方法, 其特征在于, Client 和其他 IPv6
5 节点的通信情况有以下 3 种:

一、 通信对方是同一链路上的客户端;

对于目的地是相同链路上客户端的数据包, SilkRoad 隧道接口采用
SilkRoad 维持包的交换代替邻居发现的地址决议过程, 交换 SilkRoad
维持包是为了获得通信对方在该链路上的 IPv4 地址以便可以直接进行通
10 信;

为了判断目的地址所对应的主机是否位于同一链路, 客户端会检查
它的 SilkRoad 邻居缓存, 每个客户端都会向和它相连的 IPv4 链路发送
SilkRoad 维持包以表明它在该链路上的存在, 所有收到这些 SilkRoad
维持包的客户端将包中的 SilkRoad 地址和 IPv4 地址放入它的 SilkRoad
15 邻居缓存; 因此, 如果某个目的 SilkRoad 地址位于 SilkRoad 邻居缓存,
那么该地址对应的主机肯定位于相同的链路上, 相同链路上客户端之间的
通信过程如下:

1、客户端 1, 即本主机发送一个维持包, 其 IPv4 目的地址为一保
留的 IPv4 多播地址 224.0.0.1, 由 IANA 分配, 维持包的 IPv6 头部的目
20 的 IPv6 地址为客户端 2, 即目的主机的 SilkRoad 地址;

2、客户端 2 收到 SilkRoad 维持包后判断客户端 1 的 IPv4 地址是
否属于同一链路、UDP 端口是否为 5188, 若地址端口都得到确认, 客户
端 2 向客户端 1 发送一个维持包作为响应, 客户端 1 收到该包后获得
客户端 2 的 IPv4 地址, 此地址是 NAT 域内的私有地址;

25 3、接着客户端 1 直接向客户端 2 发送数据, 不需要经过 NAT, 更
不需要经过服务器;

二、 通信对方另一 NAT 域的客户端;

这种情况又可细分为 3 种情况:

1、本主机位于“cone” NAT 域或“Restricted” NAT 域, 目的主
30 机位于“cone” NAT 域

它们之间的通信可以直接进行，因为“cone” NAT 不会对任何源 IPv4 地址加以限制，所以客户端 1 可以直接向客户端 2 发送数据包来创建对方 NAT 转换表中的地址端口映射关系，若客户端 1 位于“Restricted” NAT，因为它向客户端 2 发送数据后 NAT1 已经建立了目的地为 NAT2 的映射关系，所以客户端 2 的数据包可以通过 NAT1；

2、目的主机位于“Restricted” NAT 域

SilkRoad 隧道接口采用维持包的交换来代替邻居发现的地址决议过程，使得对方所在 NAT 创建通信必须的地址端口映射关系，之后两个客户端之间就可以直接交换数据包，具体通信过程如下：

● 客户端 1，即本主机向客户端 2，即目的主机发送一个维持包，目的是为了在“Restricted” NAT1 建立目的地为 NAT2 的映射关系，以便来自 NAT2 的数据可以通过 NAT1，如果 NAT1 是“cone”类型，则可以省略这一步；

● 接着客户端 1 向服务器 1，即客户端 1 注册的服务器发送维持包，目的 IPv4 地址为服务器 1 的公有 IPv4 地址，目的 IPv6 地址为客户端 2 的地址；

● 服务器 1 收到此包后剥去 IPv4 头部和 UDP 头部，新的数据包只有一个 IPv6 头部，通过 IPv6 网将新数据包转发至服务器 2，即客户端 2 注册的服务器，虚线表示该包走的是 IPv6 网络；

● 服务器 2 收到此包后从目的 IPv6 地址中提取出外部地址和外部端口，将此包封装在 UDP 中后发送给客户端 2，UDP 的目的端口为提取的外部端口，源端口为 5188，IPv4 头部的源地址为服务器 2 的 IPv4 地址，目的地址为提取的外部地址；

● 客户端 2 收到来自服务器 2 的数据包后从源 IPv6 地址中提取出客户端 1 的外部地址和外部端口，并从客户端 1 的地址中获知它未位于“Symmetric” NAT 域，然后向客户端 1 发送一个维持包，其中 IPv4 源地址为客户端 2 的私有地址，IPv4 目的地址为提取的外部地址，UDP 源端口为 5188，目的端口为提取的外部端口，即使 NAT1 是“Restricted”类型，因为第一步中 NAT1 已经建立了到 NAT2 的映射关系，所以该包可以通过 NAT1；

接下去客户端 1 就可以直接向客户端 2 发送数据包，不需要中间服务器的转发，发送之前从目的 IPv6 地址也就是客户端 2 的 SilkRoad 地址中提取出外部地址和外部端口，然后将数据包封装在 UDP 中，目的 IPv4 地址为提取的外部地址，源 IPv4 地址为本机的私有 IPv4 地址，目的端口为提取的外部端口，源端口为 5188，客户端 2 收到此包后进行解封装，如果它要向客户端 1 发送数据包，必须执行同客户端 1 一样的封装过程；

3、本主机或目的主机位于“Symmetric” NAT 域

它们之间通信的数据包必须通过服务器转发，具体过程如下：

● 客户端 1，即本主机将要发送的数据包封装在 UDP 中，目的 IPv4 地址为服务器 1 的公有 IPv4 地址，源 IPv4 地址为本机的私有 IPv4 地址，目的端口和源端口均为 5188；

● 服务器 1，即客户端 1 注册的服务器剥去 IPv4 和 UDP 头部，通过 IPv6 网将没有封装的 IPv6 数据包转发至服务器 2，虚线表示该包走的是 IPv6 网络；

● 服务器 2，即客户端 2 注册的服务器收到此包后从目的 IPv6 地址中提取出外部地址和外部端口，将此包封装在 UDP 中然后发送给客户端 2，即目的主机，UDP 的目的端口为提取的外部端口，源端口为 5188，IPv4 头部的源地址为服务器 2 的 IPv4 地址，目的地址为提取的外部地址；

● 客户端 2 收到来自服务器 2 的数据包后如果要向客户端 1 发送数据包，则将该包封装在 UDP 中，目的 IPv4 地址为服务器 2 的公有 IPv4 地址，源 IPv4 地址为本机的私有 IPv4 地址，目的端口和源端口均为 5188；

三、通信对方是普通 IPv6 节点

客户端和普通 IPv6 节点之间通信的数据包必须通过服务器转发，客户端和服务器之间采用“SilkRoad”隧道传送数据流，服务器和普通 IPv6 节点之间的数据流直接利用 IPv6 网络进行传送或通过 IPv6-over-IPv4 隧道利用 IPv4 网络进行传送；

客户端到普通 IPv6 节点的通信过程如下：

● 客户端将要发送的数据包封装在 UDP 中，目的 IPv4 地址为服务器的公有 IPv4 地址，源 IPv4 地址为本机的私有 IPv4 地址，目的端口和源端口均为 5188；

● 服务器剥去 IPv4 和 UDP 头部，通过 IPv6 网将没有封装的 IPv6 数据包转发给 IPv6 节点，虚线表示该包走的是 IPv6 网络；

● IPv6 节点向客户端发回的数据包最终将被路由至服务器，虚线表示该包走的是 IPv6 网络；

- 5 ● 服务器收到此包后从目的 IPv6 地址中提取出外部地址和外部端口，并将该数据包封装在 UDP 中，其 IPv4 头部的源 IPv4 地址为服务器的公有 IPv4 地址，目的地址为提取的外部地址，源端口为 5188，目的端口为提取的外部端口；

普通 IPv6 节点到客户端的通信过程如下：

- 10 ● IPv6 节点向客户端发送数据包，目的 IPv6 地址为客户端的 SilkRoad 地址，虚线表示该包走的是 IPv6 网络；

- 该数据包最终被路由至服务器，服务器从目的 IPv6 地址中提取出外部地址和外部端口，并将该数据包封装在 UDP 中，其 IPv4 头部的源 IPv4 地址为服务器的公有 IPv4 地址，目的地址为提取的外部地址，源
15 端口为 5188，目的端口为提取的外部地址，然后将封装后的数据包发送给客户端；

 ● 客户端将要发送的数据包封装在 UDP 中，目的 IPv4 地址为服务器的公有 IPv4 地址，源 IPv4 地址为本机的私有 IPv4 地址，目的端口和源端口均为 5188；

- 20 ● 服务器剥去 IPv4 和 UDP 头部，通过 IPv6 网将没有封装的 IPv6 数据包转发给 IPv6 节点，虚线表示该包走的是 IPv6 网络。

一种可穿越网络地址翻译的自动隧道的方法

技术领域

本发明涉及互联网技术领域，特别是一种可穿越 NAT（网络地址翻译）
5 的自动隧道方法。该方法利用现有的 IPv4 网络路由体系传输 IPv6 数据包，是一种 IPv4 向 IPv6 过渡时期的隧道技术，用以实现 IPv4 向 IPv6 的过渡。

背景技术

NAT（网络地址翻译）技术是解决 IPv4 地址不足的一种有效方法，它
10 在中国的部署极其广泛。NAT 按映射关系不同可以分为 3 种类型：“cone” NAT、“Restricted” NAT、“Symmetric” NAT。

NAT 收到来自内部网络的数据包时，将数据包的 IPv4 源地址（私有地址）转换成另一地址（公有地址），我们称该地址为外部地址，将 TCP 或 UDP 源端口号转换成另一端口号，我们称该端口号为外部端口，然后
15 向外部网络发送转换后的数据包。并在它维护的转换表中增加源地址、源端口和外部地址、外部端口之间的映射关系。外部网络收到数据包后如果要往回发送数据包，它将外部地址设为数据包的目的地址，将外部端口设为数据包的目的端口。当 NAT 收到来自外部网络的数据包时，根据转换表中的映射关系将数据包的 IPv4 目的地址和 TCP 或 UDP 目的端口
20 （也就是原来的外部地址和外部端口）转换成源地址和源端口后发送给内部网络。

“cone” NAT 中，转换表的映射关系为<源地址，源端口，外部地址，外部端口>。只要来自外部网络的数据包中的<目的地址，目的端口>符合映射关系中的<外部地址，外部端口>，它就将之转化为映射关系中的
25 <源地址，源端口>，然后向内部网络发送该数据包。

“Restricted” NAT 中，转换表的映射关系为<源地址，源端口，

外部地址，外部端口，目的地址，目的端口>或<源地址，源端口，外部地址，外部端口，目的地址>。如果来自外部网络的数据包的<目的地址、目的端口、源地址、源端口>符合映射关系中的<外部地址，外部端口，目的地址，目的端口>或<外部地址，外部端口，目的地址>，它就将数据包5 包的<目的地址，目的端口>转化为映射关系中的<源地址，源端口>，然后向内部网络发送该数据包。

上述两种 NAT，映射关系是一对一，也就是说只要原象<源地址，源端口>不变，映射后的象<外部地址，外部端口>也不变。”Symmetric” NAT 不同，它的映射关系是一对多，对于同一个原象<源地址，源端口>，根据数据包不同的目的地址，会被映射成不同的象<外部地址，外部端口>。10

NAT 在解决 IPv4 地址不足的同时也破坏了 IP 协议端到端的特性，而 IPv4 协议本身在地址分配策略、安全、接入、Qos、移动性等方面存在诸多不足，IPv6 就是为了解决这些问题而设计的。随着政府和企业对 IPv6 互联网研究和运行投入的不断增加，IPv4 互联网向 IPv6 互联网的转变15 势在必行。但这种转变不是一蹴而就的，它需要一个漫长的过程。目前，IETF 已经提出了从 IPv4 过渡到 IPv6 的 3 种主要迁移机制：双栈、协议翻译、隧道。

双栈节点同时实现了 IPv4 和 IPv6 协议，可以和 IPv4 或 IPv6 节点建立通信。节点根据目的 IP 地址决定采用 IPv4 还是 IPv6 协议发送或接收数据包。目前双栈是运行最广泛的迁移机制。但双栈只允许相同 IP 版本20 之间的通信。

协议翻译就是将数据包透明的从一种协议翻译成另一种协议。这样使得纯 IPv6 节点可以和纯 IPv4 节点之间建立通信，而不需要修改任何软件。最有名的协议翻译机制是 NAT-PT。NAT-PT 采用 SIIT (Stateless IP/ICMP T 路由广告 nslator) 进行协议翻译，当 IPv6 节点和 IPv4 节点25 需要建立通信时，NAT-PT 为 IPv6 节点分配一个临时的 IPv4 地址，并在会话期间维护 IPv4 地址和 IPv6 地址的映射关系。同时它还可以提供应用层网关的功能，执行 IPv4 和 IPv6 DNS 请求和应答的翻译。

隧道技术的实质是将 IPv6 (IPv4) 数据包封装在 IPv4 (IPv6) 数据包中，利用已有的 IPv4 (IPv6) 路由体系进行传输，从而解决被不兼容30

的网络分离的采用相同 IP 版本的节点之间相互通信的问题。在过渡前期，IPv4 网络占主导地位，IPv6 网络好比是整个 IPv4 汪洋中的孤立岛屿，这些岛屿之间的通信可采用 IPv6-over-IPv4 隧道来实现。过渡后期，IPv6 网络占统治地位，类似地，各个孤立 IPv4 岛屿之间的通信可采用
5 IPv4-over-IPv6 隧道来实现。

通常隧道由 3 部分组成：隧道首节点，对数据包进行封装；隧道尾节点，对数据包进行解封装；隧道主体，实际上是一条 IPv6 或 IPv4 路径，将封装后的数据包从隧道首节点传送到隧道尾节点。根据各部分实现方式的不同，隧道技术包括 6to4、ISATAP、6over4、Tunnel Broker、
10 DSTM 等。

目前绝大部分隧道技术都采用将 IPv6 数据包封装在 IPv4 载荷中的方式解决被 IPv4 网络分离的两个 IPv6 节点之间通信的问题。但是，这些隧道技术都无法支持 NAT 域内的 IPv6 节点和其他 IPv6 节点之间的通信，也就是说，这些隧道不允许隧道主体上有 NAT 存在。原因是目前的
15 NAT 基本上不允许 IPv6-in-IPv4 数据包（也就是 IPv4 头部的协议类型字段为 41 的数据包）通过。NAT 收到 IPv6-in-IPv4 数据包后，由于不认识而将之丢弃。

发明内容

本发明提出一种可穿越 NAT 的自动隧道的方法，目的是解决 NAT 域
20 内的 IPv6 节点和其他 IPv6 节点（可以在 NAT 域内，也可以不是）之间互相通信的问题。

本发明的技术方案：

因此提出了一种将 IPv6 数据包封装在 UDP 载荷中的隧道技术，我们称之为“SilkRoad”，相应的，我们称这种隧道为 SilkRoad 隧道，SilkRoad
25 不受隧道主体上存在任意类型和任意数量的 NAT 的影响，可将 IPv6 数据包从隧道首节点传送到隧道尾节点。

SilkRoad 隧道定义了 3 个通信实体，用于实现上述的方法：

1. Silkroad 客户端（以下简称客户端），表示 NAT 域内的 IPv6/IPv4 双栈节点，支持 Silkroad 隧道功能，有一个全球单播聚类 IPv6 地址（我

们称之为 SilkRoad 地址) 和一个私有 IPv4 地址。

2. Silkroad 服务器 (以下简称服务器), 在 NAT 域外, 表示为客户端分配 IPv6 地址并具有路由功能的 IPv6/IPv4 双栈节点, 支持 Silkroad 隧道功能, 有一个公有 IPv4 地址, 它可以有通向 IPv6 骨干网的路由, 也可以有通向孤立 IPv6 网络的路由。
3. 普通 IPv6 节点, 表示除客户端和服务端以外的其他 IPv6 节点。

附图说明

- 图 1 为服务器分配给客户端的 SilkRoad 地址格式图。
- 10 图 2 为 SilkRoad 定义的数据包格式图。
- 图 3 为 SilkRoad 定义的维持包格式图。
- 图 4 为 SilkRoad 的路由体系图。
- 图 5 为客户端启动后的初始化配置过程图。
- 图 6 为相同链路上客户端之间的通信过程图。
- 15 图 7 为位于不同 NAT 域客户端之间通信的第一种情况图。
- 图 8 为位于不同 NAT 域客户端之间通信的第二种情况图。
- 图 9 为位于不同 NAT 域客户端之间通信的第三种情况图。
- 图 10 为客户端到普通 IPv6 节点的通信过程图。
- 图 11 为普通 IPv6 节点到客户端的通信过程图。
- 20 客户端通信时采用的 IPv6 地址是一种规定格式的地址, 它包括 64 位的 IPv6 地址前缀和 64 位的接口标识符, 接口标识符由伪外部端口字段、NAT 类型标志位字段、Silkroad 地址标志位字段和伪外部地址字段组成, 如附图 1 所示。各部分说明如下:
- ◆ IPv6 前缀:

25 IANA 正式分配的全球聚类单播地址前缀或 “site-local” 地址前缀, 不可以是 “link-local” 地址前缀或组播地址前缀。
 - ◆ 伪外部端口:

外部端口 (经 NAT 映射后的端口) 和 0xFFFF 与或后的 16 位数值。

SilkRoad 客户端启动后向服务器发送一个初始化数据包, 该包经过

30 NAT 时其 UDP 端口被映射成一个不同的端口, 我们称之为外部端口。

服务器从接收到的初始化数据包中获得此端口。考虑到 NAT 会删除过期的映射关系，客户端（或服务器）将周期性的向 NAT 发送数据包以维持这种映射关系，所以 NAT 的转换表中始终保留该映射关系。对外部端口进行与或操作的目的是为了防止某些“自作聪明”的 NAT 将 UDP 数据包载荷，即 IPv6 头部+IPv6 载荷中的外部端口进行转化。

◆ NAT 类型标志位：

长度为 2 位，用来表示客户端所在 NAT 的类型。00 表示客户端位于“cone” NAT 域，10 表示客户端位于“Restricted” NAT 域，11 表示客户端位于“Symmetric” NAT 域。

◆ Silkroad 地址标志位：

长度为 14 位，设为 0，表示该地址是一 Silkroad 地址。将该字段放在接口标识符中间的目的在于避免和其他地址冲突，因为目前只要不是随机分配的接口标识符，其中间 16 位都是 FFFE。

◆ 伪外部地址：

外部地址即经 NAT 映射后的地址和 0xFFFFFFFF 与或后的 32 位数值。客户端启动后向服务器发送一个初始化数据包，该包经过 NAT 时其私有 IPv4 地址被映射成一个公有 IPv4 地址，我们称之为外部地址。服务器从接收到的初始化数据包中获得此地址。考虑到 NAT 会删除过期的映射关系，客户端（或服务器）将周期性的向 NAT 发送数据包以维持这种映射关系，所以 NAT 的转换表中始终保留该映射关系。对外部地址进行与或操作的目的是为了防止某些“自作聪明”的 NAT 将 UDP 数据包载荷，即 IPv6 头部+IPv6 载荷中的外部端口进行转化。客户端和其他 IPv6 节点通信时发送或接收的数据包我们称之为 Silkroad 数据包，它由 IPv4 头部、UDP 头部、IPv6 头部以及 IPv6 载荷组成，如附图 2 所示。具体说明如下：

● IPv4 头部：

源 IPv4 地址为客户端的 IPv4 地址（私有地址），目的 IPv4 地址为服务器的 IPv4 地址（如果目的地是普通 IPv6 节点）或对方客户端经 NAT 映射后的外部地址（如果目的地是另一客户端）。

● UDP 头部：

源端口为 5188，目的端口为 5188（如果目的地是普通 IPv6 节点）或对方客户端经 NAT 映射后的外部端口（如果目的地是另一客户端）。

- IPv6 头部：

5 包含源 IPv6 地址和目的 IPv6 地址，其中至少有一个是 SilkRoad 地址。

- IPv6 载荷：

由 0 或若干个 IPv6 扩展头部，以及上层协议数据单元（PDU）组成。

为了维持 NAT 中的映射关系，如“cone” NAT 的<源地址，源端口，目的地址，目的端口>。客户端需要周期性的向 NAT 发送数据包，我们称
10 这种数据包为维持包，如附图 3 所示。在维持包的 IPv6 头部中，下一跳字段设为 59，表示没有 IPv6 载荷。

Silkroad 的路由体系如附图 4 所示。客户端通过 SilkRoad 隧道接口发送或接收数据包，SilkRoad 隧道接口是一个逻辑接口，它会自动将 IPv6 数据包封装在 UDP 载荷中进行发送。同样，Silkroad 隧道接口接收到的数据包肯定是一个封装了 IPv6 报文的 UDP 数据包。客户端有一个缺
15 省路由（::/0），它将所有 IPv6 地址视为同一链路上的地址并使用 SilkRoad 隧道接口进行转发。缺省路由的下一跳地址为 IPv6 数据包中的目的地址，下一跳接口为 SilkRoad 隧道接口。服务器有通向 IPv6 骨干网以及各孤立 IPv6 网络的路由，也有通向各客户端的路由。IPv6 骨
20 干网以及各孤立 IPv6 网络中任何一个 IPv6 节点发送的数据包，只要目的地址前缀是服务器分配给客户端的地址前缀，都将被路由至服务器（图中以地址前缀 2001:*/64 为例），服务器再通过去往客户端的路由将数据包转发至客户端。同样，客户端可通过服务器和 IPv6 骨干网以及各孤立 IPv6 网络中的任何一个 IPv6 节点实现互访。

25 客户端每次启动后首先向服务器注册以获得一个 SilkRoad 地址，这样才能和其他 IPv6 节点建立通信，这个过程我们称之为客户端的初始化配置，如附图 5 所示。

客户端的初始化配置通过向服务器发送一系列路由请求报文来完成，服务器以路由广告报文作为响应，路由广告报文中含有客户端被 NAT
30 映射后的外部地址和外部端口信息。通过此过程客户端获得一个 SilkRoad

地址并判断它位于何种 NAT 域内。

客户端的初始化配置过程如下：

- 1、客户端向首选的服务器（图中为服务器 1）发送一个路由请求报文，报文的源 IPv6 地址是一个“link-local”地址，其 F 字段值为 00。
- 5 2、服务器 1 收到路由请求报文后发送一个路由广告报文作为响应，因为路由请求报文显示客户端位于“cone” NAT 域内（F 字段设为 00），所以它选择一个不同的 IPv4 地址作为源地址发送路由广告报文，如果客户端能收到此报文，表明客户端确实位于“cone” NAT 域内。
- 3、如果客户端没有收到此路由广告报文，它将再向服务器 1 发送一个
- 10 路由请求报文，路由请求报文的源 IPv6 地址是另一个“link-local”地址，其 F 字段值为 10。
- 4、服务器 1 收到路由请求报文后发送一个路由广告报文作为响应，因为路由请求报文显示客户端位于“Restricted” NAT 域内，它将以路由请求报文中的目的 IPv4 地址作为源 IPv4 地址发送路由广告报文，
- 15 客户端如果收到此报文，表示它位于一个“Restricted” NAT 域内。
- 5、客户端为了明确是否位于“Symmetric” NAT 域内，将再向另一个服务器（图 5 中为服务器 2）发送路由请求报文，服务器 2 收到路由请求报文后发送一个路由广告报文作为响应。
- 6、客户端收到此路由广告报文后和原先收到的路由广告报文作比较，如
- 20 果报文包含的用来构造 SilkRoad 地址的信息相同，表示 NAT 的地址端口映射关系是一一对应的。如果不同，表示 NAT 将相同的内部地址和端口映射成了不同的外部地址和端口，映射关系是一对多，所以客户端认为它位于“Symmetric” NAT 域。

根据第 2、4 或 6 步收到的路由广告报文，客户端按如下构造一个

25 SilkRoad 地址：

- 地址的前 64 位设置为路由广告报文中的“前缀信息选项”（如 2001:***/64）。
- 接下去的 16 位设为路由广告报文中包含的外部端口。
- 接下去的 2 位设为 00（如果客户端位于“cone” NAT 后）或 10（如
- 30 果客户端位于“Restricted” NAT 后）或 11（如果客户端位于

“Symmetric” NAT 后)。

- 接下去的 14 位设为 0。
- 最后 32 位设为路由广告报文包含的外部地址。

客户端和其他 IPv6 节点之间的通信情况分以下 3 种情况：

5 一、通信对方是同一链路上的客户端；

对于目的地是相同链路上客户端的数据包，SilkRoad 隧道接口采用 SilkRoad 维持包的交换代替邻居发现的地址决议过程，交换 SilkRoad 维持包是为了获得通信对方在该链路上的 IPv4 地址以便可以直接进行通信；

10 为了判断目的地址所对应的主机是否位于同一链路，客户端会检查它的 SilkRoad 邻居缓存，每个客户端都会向和它相连的 IPv4 链路发送 SilkRoad 维持包以表明它在该链路上的存在，所有收到这些 SilkRoad 维持包的客户端将包中的 SilkRoad 地址和 IPv4 地址放入它的 SilkRoad 邻居缓存；因此，如果某个目的 SilkRoad 地址位于 SilkRoad 邻居缓存，
15 那么该地址对应的主机肯定位于相同的链路上，相同链路上客户端之间的通信如附图 6 所示。通信过程如下：

1、客户端 1，本主机发送一个维持包，其 IPv4 目的地址为一保留的 IPv4 多播地址 224.0.0.1（由 IANA 分配）。维持包的 IPv6 头部的目的 IPv6 地址为客户端 2，目的主机的 SilkRoad 地址。

20 2、客户端 2 收到 SilkRoad 维持包后判断客户端 1 的 IPv4 地址是否属于同一链路、UDP 端口是否为 5188。若地址端口都得到确认，客户端 2 向客户端 1 发送一个维持包作为响应，客户端 1 收到该包后获得客户端 2 的 IPv4 地址（此地址是 NAT 域内的私有地址）。

3、接着客户端 1 直接向客户端 2 发送数据，不需要经过 NAT，更
25 不需要经过服务器。

二、通信对方另一 NAT 域的客户端；

这种情况又可细分为 3 种情况：

1. 本主机位于“cone” NAT 域或“Restricted” NAT 域，目的主机位于“cone” NAT 域

30 它们之间的通信可以直接进行，如附图 7 所示。因为“cone” NAT

不会对任何源 IPv4 地址加以限制，所以客户端 1 可以直接向客户端 2 发送数据包来创建对方 NAT 转换表中的地址端口映射关系。若客户端 1 位于“Restricted” NAT，因为它向客户端 2 发送数据后 NAT1 已经建立了目的地为 NAT2 的映射关系，所以客户端 2 的数据包可以通过 NAT1；

5 2. 目的主机位于“Restricted” NAT 域

SilkRoad 隧道接口采用维持包的交换来代替邻居发现的地址决议过程，使得对方所在 NAT 创建通信必须的地址端口映射关系，之后两个客户端之间就可以直接交换数据包，如附图 8 所示。具体通信过程如下：

● 客户端 1（即本主机）向客户端 2（即目的主机）发送一个维持包，目的是为了在“Restricted” NAT1 建立目的地为 NAT2 的映射关系，以便来自 NAT2 的数据可以通过 NAT1。如果 NAT1 是“cone”类型，则可以省略这一步。

● 接着客户端 1 向服务器 1（即客户端 1 注册的服务器）发送维持包，目的 IPv4 地址为服务器 1 的公有 IPv4 地址，目的 IPv6 地址为客户端 2 的地址。

● 服务器 1 收到此包后剥去 IPv4 头部和 UDP 头部，新的数据包只有一个 IPv6 头部。通过 IPv6 网将新数据包转发至服务器 2（即客户端 2 注册的服务器）。图中虚线表示该包走的是 IPv6 网络。

● 服务器 2 收到此包后从目的 IPv6 地址中提取出外部地址和外部端口，将此包封装在 UDP 中后发送给客户端 2。UDP 的目的端口为提取的外部端口，源端口为 5188，IPv4 头部的源地址为服务器 2 的 IPv4 地址，目的地址为提取的外部地址。

● 客户端 2 收到来自服务器 2 的数据包后从源 IPv6 地址中提取出客户端 1 的外部地址和外部端口，并从客户端 1 的地址中获知它不位于“Symmetric” NAT 域。然后向客户端 1 发送一个维持包，其中 IPv4 源地址为客户端 2 的私有地址，IPv4 目的地址为提取的外部地址。UDP 源端口为 5188，目的端口为提取的外部端口。即使 NAT1 是“Restricted”类型，因为第一步中 NAT1 已经建立了到 NAT2 的映射关系，所以该包可以通过 NAT1。

接下去客户端 1 就可以直接向客户端 2 发送数据包，不需要中间服

- 务器的转发。发送之前从目的 IPv6 地址也就是客户端 2 的 SilkRoad 地址中提取出外部地址和外部端口，然后将数据包封装在 UDP 中，目的 IPv4 地址为提取的外部地址，源 IPv4 地址为本机的私有 IPv4 地址，目的端口为提取的外部端口，源端口为 5188。客户端 2 收到此包后进行解封装，
- 5 如果它要向客户端 1 发送数据包，必须执行同客户端 1 一样的封装过程。

3. 本主机或对方位于“Symmetric” NAT 域

它们之间通信的数据包必须通过服务器转发，如附图 9 所示。具体过程如下：

- 客户端 1，本主机将要发送的数据包封装在 UDP 中，目的 IPv4 地址为服务器 1 的公有 IPv4 地址，源 IPv4 地址为本机的私有 IPv4 地址，目的端口和源端口均为 5188。

- 服务器 1（即客户端 1 注册的服务器）剥去 IPv4 和 UDP 头部，通过 IPv6 网将没有封装的 IPv6 数据包转发至服务器 2。图中虚线表示该包走的是 IPv6 网络。

- 15
- 服务器 2（即客户端 2 注册的服务器）收到此包后从目的 IPv6 地址中提取出外部地址和外部端口，将此包封装在 UDP 中然后发送给客户端 2 目的主机。UDP 的目的端口为提取的外部端口，源端口为 5188，IPv4 头部的源地址为服务器 2 的 IPv4 地址，目的地址为提取的外部地址。

- 客户端 2 收到来自服务器 2 的数据包后如果要向客户端 1 发送数据包，则将该包封装在 UDP 中，目的 IPv4 地址为服务器 2 的公有 IPv4 地址，源 IPv4 地址为本机的私有 IPv4 地址，目的端口和源端口均为 5188。

三、通信对方是普通 IPv6 节点

- 客户端和普通 IPv6 节点之间通信的数据包必须通过服务器转发，客户端和服务端之间采用“SilkRoad”隧道传送数据流，服务器和普通 IPv6
- 25 节点之间的数据流直接利用 IPv6 网络进行传送或通过 IPv6-over-IPv4 隧道利用 IPv4 网络进行传送。

客户端到普通 IPv6 节点的通信过程如附图 10 所示，具体描述如下：

- 客户端将要发送的数据包封装在 UDP 中，目的 IPv4 地址为服务器的公有 IPv4 地址，源 IPv4 地址为本机的私有 IPv4 地址，目的端口和源端口均为 5188。
- 30

● 服务器剥去 IPv4 和 UDP 头部，通过 IPv6 网将没有封装的 IPv6 数据包转发给 IPv6 节点。图中虚线表示该包走的是 IPv6 网络。

● IPv6 节点向客户端发回的数据包最终将被路由至服务器。图中虚线表示该包走的是 IPv6 网络。

- 5 ● 服务器收到此包后从目的 IPv6 地址中提取出外部地址和外部端口，并将该数据包封装在 UDP 中，其 IPv4 头部的源 IPv4 地址为服务器的公有 IPv4 地址，目的地址为提取的外部地址，源端口为 5188，目的端口为提取的外部端口。

10 普通 IPv6 节点到客户端的通信过程，如附图 11 所示，具体描述如下：

● IPv6 节点向客户端发送数据包，目的 IPv6 地址为客户端的 SilkRoad 地址。图中虚线表示该包走的是 IPv6 网络。

- 15 ● 该数据包最终被路由至服务器，服务器从目的 IPv6 地址中提取出外部地址和外部端口，并将该数据包封装在 UDP 中，其 IPv4 头部的源 IPv4 地址为服务器的公有 IPv4 地址，目的地址为提取的外部地址，源端口为 5188，目的端口为提取的外部地址。然后将封装后的数据包发送给客户端。

- 20 ● 客户端将要发送的数据包封装在 UDP 中，目的 IPv4 地址为服务器的公有 IPv4 地址，源 IPv4 地址为本机的私有 IPv4 地址，目的端口和源端口均为 5188。

● 服务器剥去 IPv4 和 UDP 头部，通过 IPv6 网将没有封装的 IPv6 数据包转发给 IPv6 节点。图中虚线表示该包走的是 IPv6 网络。

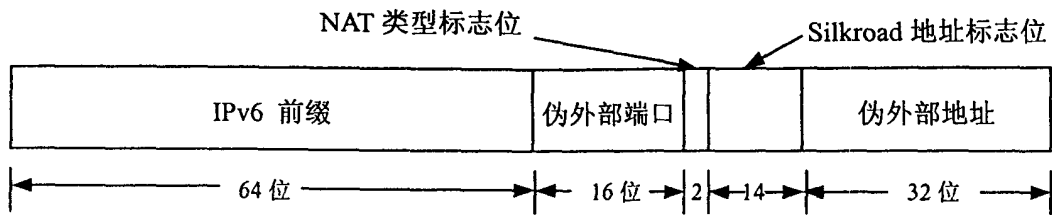


图 1

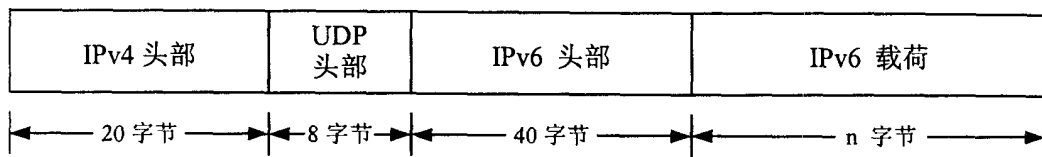


图 2

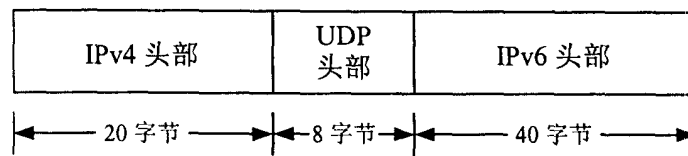


图 3

路由:
前缀::/0 通过 Silkroad 接口转发

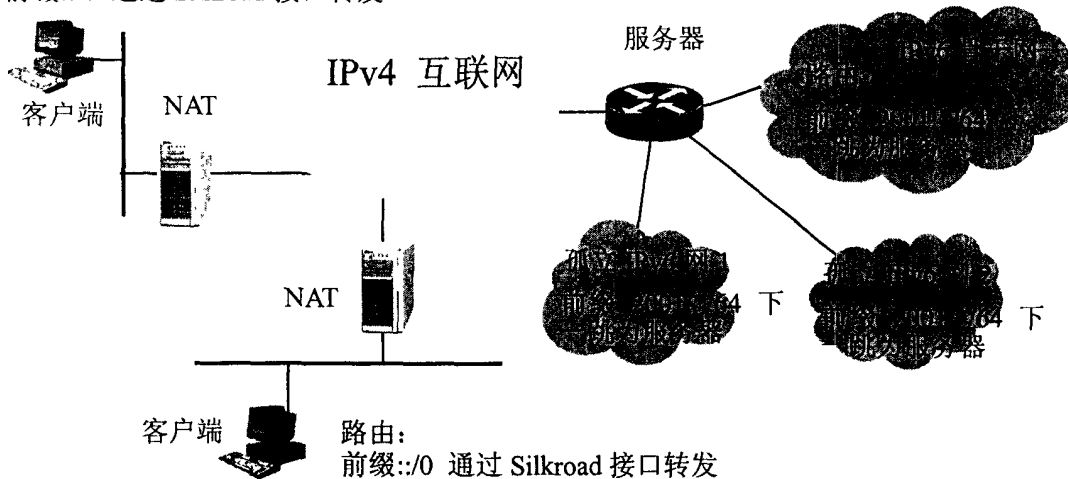


图 4

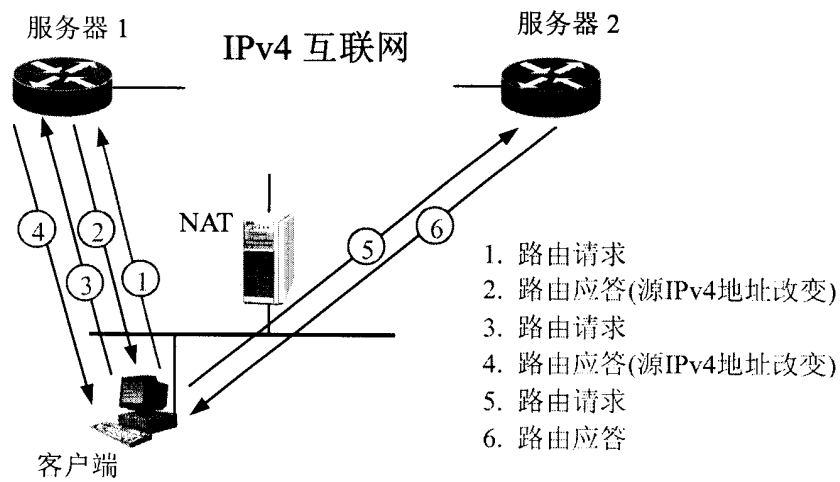


图 5

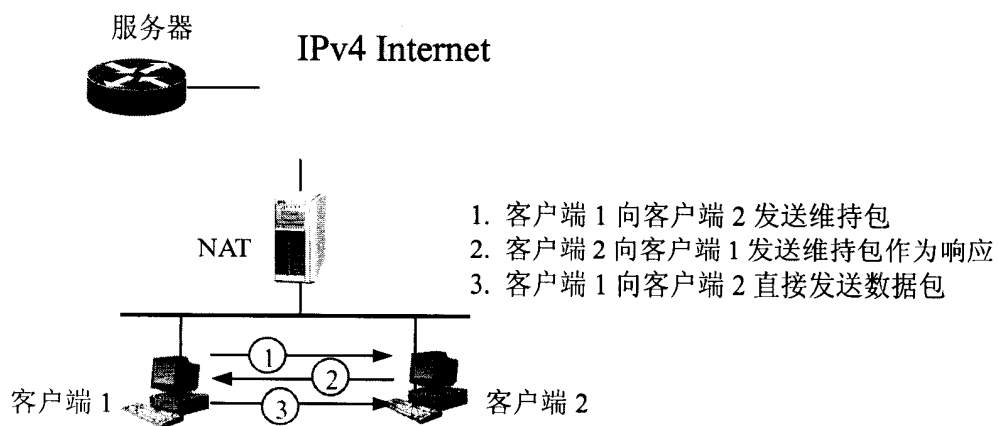


图 6

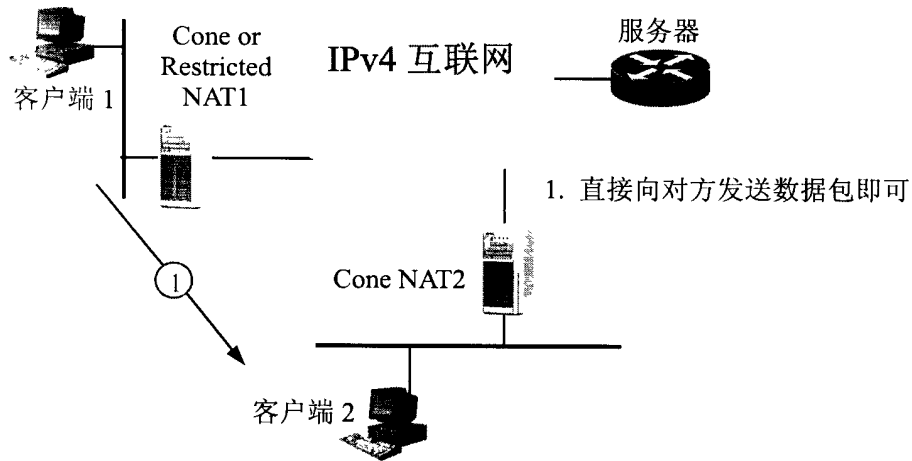


图 7

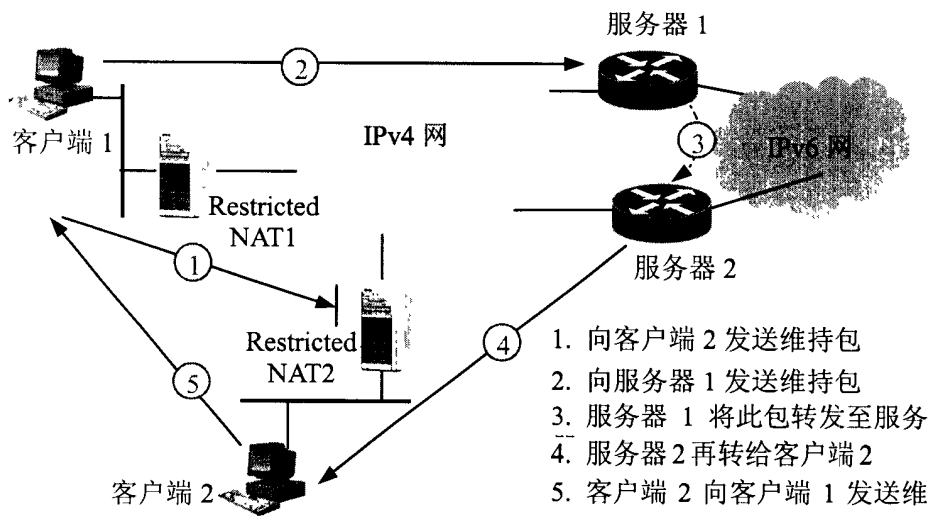


图 8

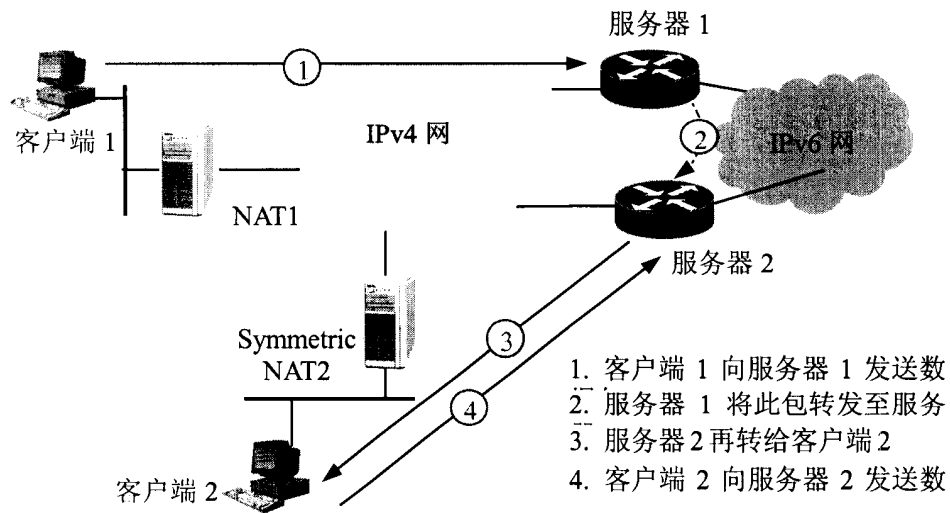


图 9

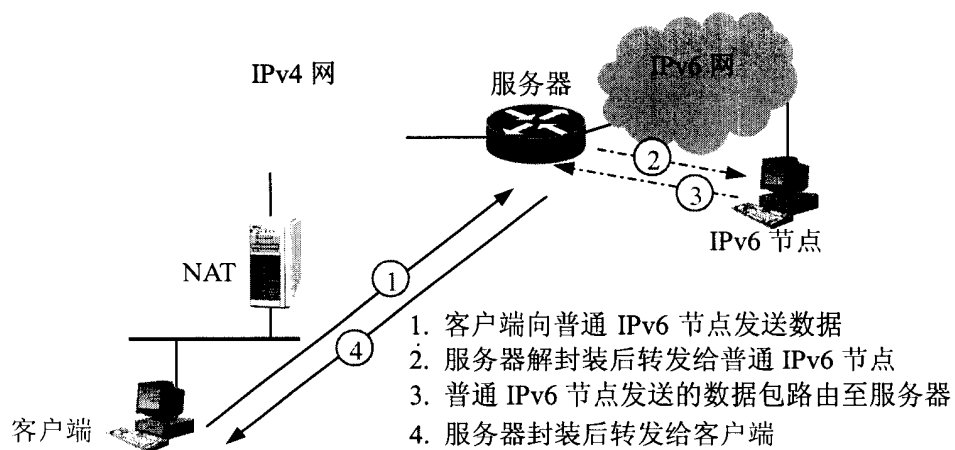


图 10

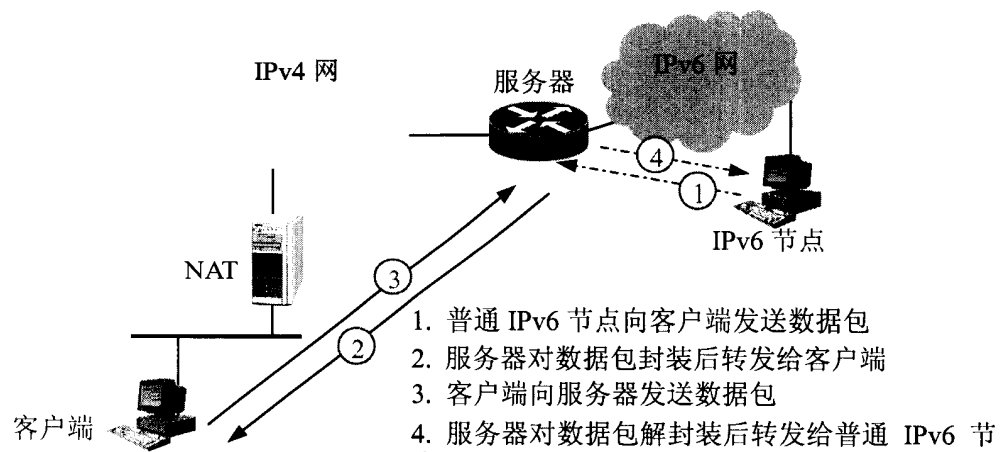


图 11