指导教师评定成绩 (五级制)： 指导教师签字：

附件 C：译文

传统 IP 网络地址转换（传统 NAT）

摘要

基本网络地址转换 NAT 是 IP 地址从一个组映射到另一种方法，对终端用户是透明的。网络地址端口转换或 NAPT 是很多网络地址和它们的 TCP/UDP 端口转换成一个唯一的网络地址和它的 TCP/UDP 端口。总之，这两个操作，被称为传统 NAT，提供了一种机制，就可以与全球唯一一个与私人地址领域到外部境界注册地址。

1 介绍

IP 地址转换的提出是因为一个网络的 IP 内部地址不能用在外部网，不论是因为隐私的原因还是因为它们在外部网不合法。

一个局域网的网络拓补可以用很多方式改变，顾客可以改变他们的提供商，公司骨干可能重组或则提供商可能合并或分裂。客户可能会改变供应商，公司骨干可能要重组，或供应商可能合并或分裂。每当外部拓扑结构随时间的变化，对节点分配地址在本地域中也必须改变，以反映外部的变化。这种类型的变化可以隐藏在域名被集中到一个单一的改变路由器用户的地址转换。

基本地址转换将（在很多情况下，除了[NAT-TERM]和这个文档第 6 部分所有指的）允许在局域网中的主机可以透明的连接外部网和可以连接外部网中可选的主机。网络组织的建立首先是为了局域网内部的应用，还有和广域网的连接需要是这个规划的很好候补。

许多小公司，家庭办公室用户和电信员工在它们的办公室有多个网络节点运行 TCP/UDP 应用程序，但是服务提供商只有给他们在远程连通路由提供唯一的 IP 地址。这个远程连接用户渐增的社区将从 NAPT 中获得好处，NAPT 将允许在局域网中有多个节点同时用路由器附以的唯一 IP 地址连接远程网络。

用这种方式有许多局限性。属于一个会议的所有请求和应答强制路游通过相同的 NAT 路由器。一种确认的方式将是有一个基于唯一残缺网段路由的 NAT，在那所有的 IP 包或者从那个起始或者以那个为目的地。还有其他方法用多 NAT 设备来确保这个规则。例如，一个单一能够拥有两个不同的出口到不同的提供者和局部网络的主机之间的会议能够穿过 NAT 设备到达外部主机的最好途径。当一个 NAT 路由器不正常 ，其他的路由器能够路由所有连接。但是在这中方法下有可能有一个警告，因为再次路由的流量可能在新的 NAT 路由交换时间里交换失败。一种解决这个问题的方法是路由器共享相同的 NAT 配置和交换状态信息保证互相失

败备份。

地址转换是独立的应用，经常伴随特殊应用网关（ALOGS）执行有效负荷检测和变换。FTP 是 NAT 设备里最常用 ALG 功能。要求 ALG 干涉的应用一定不能有他们自己的有效负荷编码，因为那样可能影响到使 ALG 失笑，直到 ALG 有解密有效负荷的主键。

这个方法有个缺陷是取消了 IP 地址点对点的意义，和在网络中用增加的状态来补偿。总之，通过 IPSec 保证的点对点 IP 网络层安全不能适用于终端主机，如果有 NAT 设备路由。但是，这个方法的优点是它在不需要变换主机和路由器的情况下安装。在这篇文章里一些概念的定义例如“地址域”,“透明路由”,“TV 端口”,“ALG”和其它概念可以在 NAT-TERM 里找到。

2 传统 NAT 概述

在这个文档里描述的地址转换操作是根据“传统 NAT”。其它的 NAT 在这个文档里没有给以描述。在大部分情况下，传统 NAT 允许在局域网的主机透明的和外部主机连接。在传统 NAT 中，从局域网到广域网方式是单一方向的。相反方向的两个任务可能允许预选择主机状态地址影射的异常。基本 NAT 和 NAPT 是不同的两种传统 NAT，因为基本 NAT 地址转换只是限于 IP 地址，然而 NAPT 的地址转换包括 IP 地址转换和传输认证（例如 TCP/UDP 端口或 ICMP 询问 ID）。

除了提到的那些外，贯穿这篇文章的地址转换或 NAT 属于传统 NAT，也就是基本 NAT 和 NAPT。只有如底下图一中所描述的残段网可能配置成执行地址转换。

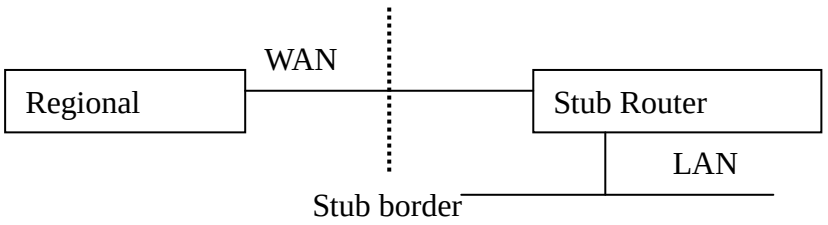

图 1：传统 NAT 设置

2.1 基本 NAT 的概述

基本 NAT 的操作如下。拥有一系列 IP 地址的残域能够和外部网络通讯，通过映射本地地址成全球统一地址。如果本地节点数量等于或小于有效通用地址的数量，每个本地地址都能保证映射到。另外，能够多个出口到广域网的节点数受通用地址的数量限制。单一本地地址应该映射成一个专门的全球通用地址来保证连通外部或者通过一个公共地址来与外部连接。多路同时任务可以从一个本地节点

进行初始化，用相同的地址映射。

在一个残域里的地址只是在本地有效而在此域外却是无效的。但是，在一个残域里的地址可以被任何其他的残域从新使用。例如，一个单一类 A 地址能够被许多残域地址所使用。在每一个残域和主干网的出口点安装 NAT。如果有多个出口，每个出口应该有相同的转换表。

例如，如图 2，残域 A 和 B 内部都用类 A 地址段 10.0.0.0/8[RFC1918]。残域 A 的 NAT 附议 C 类地址段 198.76.29.0/24，而残域 B 的 NAT 附议 C 类地址段 198.76.28.0/24。C 类地址是全球通用的唯一地址，其他 NAT 都不能用它们。

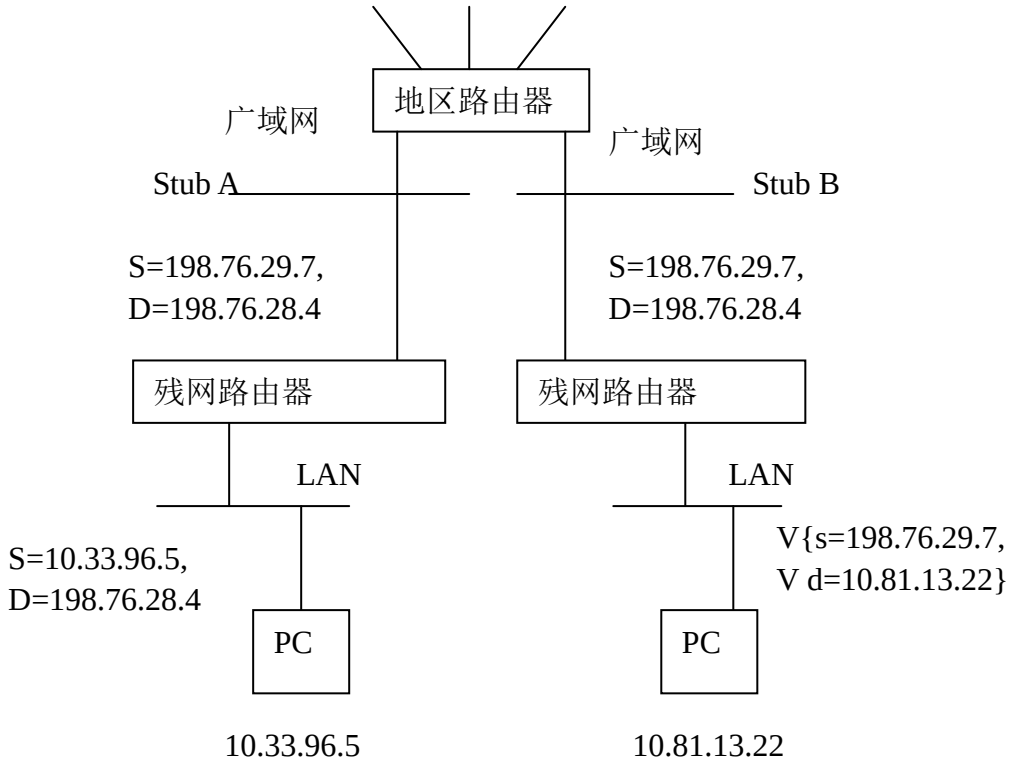

图 2 基本 NAT 操作

当残域 A 主机 10.33.96.5 试图发送一个包到残域 B 主机 10.81.13.22 时，用全球通用地址 198.76.28.4 作为目标主机地址，然后送包到第一个路由器。残域路由器对网络 198.76.28.4 有一个静态所以包可以继续往前到广域网路由器。但是，NAT 在包被继续向前送之前转换源地址 10.33.96.5 成 198.76.29.7。相应的，IP 包往回传时依据相同的地址转换。

需要注意的是主机或路由器不要改变。例如，针对残域 A 主机，198.76.28.4 是残域 B 中的地址。在绝大多数情况下，地址转换对目标主机是通明的。当然，这个只是一个简单的例子。还有很多问题待解决。

2.2 NAPT 概述

有一种说法，一个组织有一个局域网和一个广域网连接到服务提供商。局域网络的残域路由器附议在广域网连接中的有效地址而此组织中剩余的节点拥有只是在本地有效的 IP 地址。在这种情况下，局域网的多个节点允许多个连接到广域网，在 NAPT 的帮助下用登记的唯一 IP 地址。NAPT 允许映射两个类型（登记 IP 地址，TV 端口数）到两个类型（ 登记 IP 地址，TV 端口数）。这种模型符合大部分小公司家庭公司（SOHO）团体用服务提供商提供的登记 IP 地址连接广域网的要求。这个模型能够扩展趁允许内部连接通过映射登记 IP 地址的每一个服务 TV 端口的本地节点。

在下面的图 3 中，残域 A 内部用 A 类地址段 10.0.0.0/8。残域路由器接口被服务提供商附以 IP 地址 138.76.28.4。

当残域 A 主机 10.0.0.10 发送一个远程登陆包到主机 138.76.29.7,用全球通用地址 138.76.29.7 作为目标地址，然后送包到第一个路由器。残域路由器有一个子网 138.76.0.0/16 静态路由，所以包可以继续往前传送到广域网。但是，在包被网前传之前,NAPT 转换 IP 和 TCP 包头里源地址 10.0.0.10 和源 TCP 端口 3017 成通用唯一地址 138.76.28.4 和唯一 TCP 端口。在往回传的包经过同样的地址和 TCP 端口转换。和上边一样，我们必修注意，这个转换不需要改变主机或路由器。这个转换是完全透明的。

在这个设置中，只有 TCP/UDP 任务允许且必须从本地局域网中初始化。但是，有些服务例如 DNS 要求内部访问。还有其它服务一个组织想允许内部任务访问。在路由器上，静态配置一个残域网众所周知的端口是可能的[RFC 1700]，可以直接连向专门的局域网节点。

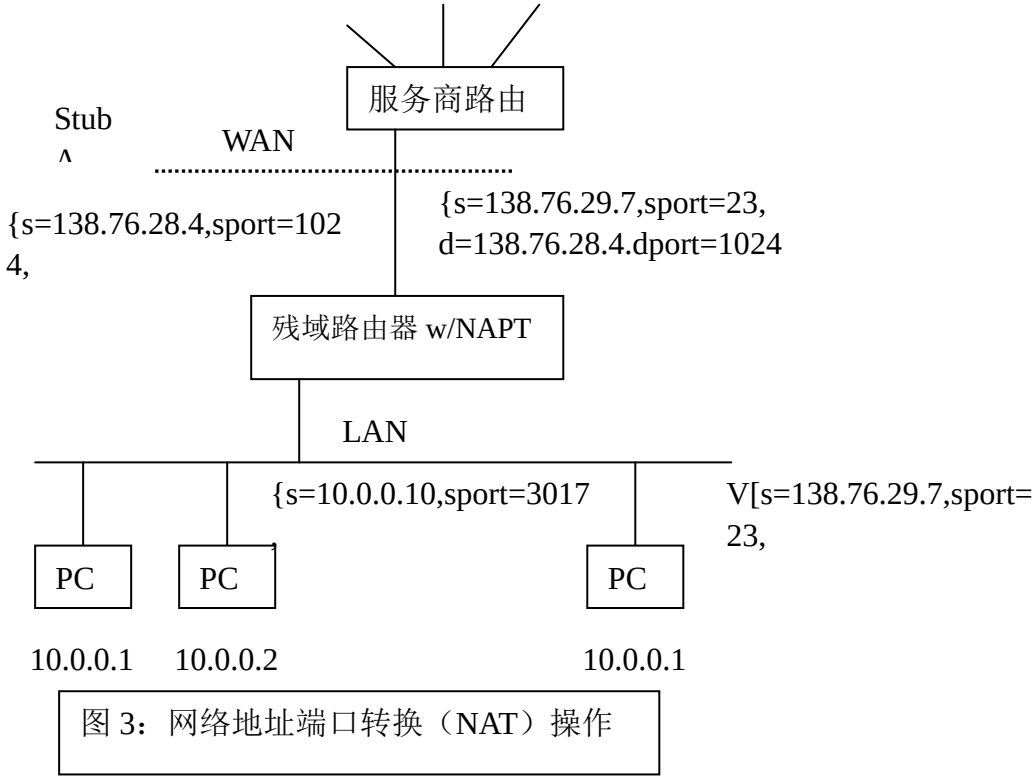

图 3：网络地址端口转换（NAT）操作

除了重定向信息类型，TCP/UDP 任务和 ICMP 信息都可以通过 NAPT 路由器来控制。ICMP 查询类型包和 TCP/UDP 包的转换类型一样，在于 ICMP 包头的标志域一对一地和登记 IP 地址的查询标志对应。在 ICMP 查询信息中的标志域由发送者设置并且从查询问答端毫无改变的反馈。所以，一对地址（本地 IP 地址，本地 ICMP 查询标志）通过 NAPT 路由器映射成一对（登记 IP 地址，附议的 ICMP 查询标志），这个过程保证从任何本地主机来的任何类型有唯一的标志。ICMP 错误信息的更改在以后的章节中给以讨论，包括 ICMP 有效负荷的改变和 IP 和 ICMP 报头。

在 NAPT 设置中，任何登记 IP 地址和残域网路由器的广域网接口的 IP 地址一样的地方，路由器必须保证区分发生于自己的 TCP，UDP 或 ICMP 查询任务 和那些发生于局域网节点的任务。所有内部任务（包括 TCP，UDP 和 ICMP 查询任务）被假设为直接到 NAT 路由器作为终节点，除非目标服务端口静态映射于局域网中的不同节点。

除了 TCP,UDP 和 ICMP 查询类型的任务不允许从本地节点由 NAPT 路由器传输。

3 任务传输过程

传统 NAT 的传输过程和[NAT-TERM]中描述的一样。下面的部分说明和传统 NAT 的特殊的内容。

3.1 地址绑定

用基本 NAT，当第一个外传任务从私有主机初始化时，一个内部私有地址绑定一个外部地址。后来，所有其它的外传任务从相同的私有地址初始化将用相同的地址绑定来传输包数据。

对 NAPT 而言，在许多私有地址映射一个全球唯一地址时，绑定是从成对地址（私有 IP 地址，私有 TV 端口）到另外一对地址（指派地址，指派 TV 端口）。和基本 NAT 一样，绑定是在第一个外传任务有一对地址（私有 IP 地址，私有 TV 端口）发动时决定的。由于不是一个普通实践，有可能同时多个任务初始化一对相同地址（私有地址，私有端口）在一个私有主机中建立是可能的。在这种情况下，一对地址（私有地址，私有 TV 端口）的一个唯一绑定可能用于所有从相同地址主机中的任务传送的包。

3.2 地址查询和转换

在一个地址绑定或地址对绑定（假设 NAPT 以建立），一个软状态将用绑定来维持任何连接。属于相同任务的包将服从转换目的的任务查询。转换的确切属性将在接下去的章节中进行讨论。

解开地址

当基于单个地址或成对地址绑定的最后一个任务终止时，绑定自己将终止。

4 包传输

属于 NAT 管理任务的包经历任何方向的转换。对立包数据任务在接下去进行详细的描述。

4.1 IP，TCP，UDP 和 ICMP 报头操作

在基本 NAT 模型，每个包的 IP 头必须改变，包括 IP 地址（外传包的源 IP 地址，往里传的目的 IP 地址）和 IP 校验和。

对 TCP 和 UDP 任务，改变包括 TCP 和 UDP 报头的校验和的更正。这是因为 TCP/UDP 校验和同时有一个假头包含源和目的 IP 地址。有一个例外，校验和为 0 的 UDP 报头不需要改变。至于 ICMP 查询包，由于在 ICMP 报头中不包含 IP 地址，所以不需要额外的变化。

在 NAPT 模型中，IP 头的变化和基本 NAT 中的相同。对 TCP/UDP 任务，在报头中变化必须扩展成包含转换 TV 端口(外传数据的源 TV 端口和内传的目的 TV 端口）的转换。在 ICMP 查询包中 ICMP 报头必须改变来代替查询 ID 和 ICMP 报头校验和。私有主机查询 ID 必须转换成外传的指派 ID 和内传的相信转换。ICMP 报头校验和

必须更正来说明查询 ID 转换。

校验和调整

NAT 修正以每个包为准的，能够准确计算，因为除了简单域转换外，它们包括一个或多个校验和修正。幸运的是，我们有一个算法，它能简单有效地调整 IP，TCP，UDP 和 ICMP 报头校验和。因为所有这些报头用一个辅助校验和在转换时计算差距和把它加到校验和是足够的。下面的算法只有对偶偏移有效（如：下面 optr 是从报头开始必须是偶偏移）和偶数长度（如，下面的 olen 和 nlen)。样本代码如下：

```
Void checksumadjust(unsigned char *chksum, unsigned char *optr, int olen,
unsigned char *nptr, int nlen)
/assuming:unsigned char is 8 bits, long is 32 bits.
chksum points to the chksum in the packet
optr points to the old data in the packet
nptr points to the new data in the packet */
{
   long x,old,new;
x=chksum[0]*256+chksum[1];
x=x&0xFFFF;
while(olen)
{
   old = optr[0]*256+optr[1];
optr+=2;
x-=old&oxffff;
if(x<=0 ){ x--; x&=0xffff;}
olen-=2;
}
while(nlen)
{
    new=nptr[0]*256+nptr[1];
    nptr+=2;
    x+= new& 0xffff;
    if(x & 0x10000){ x++; x&=0xffff;}
    nlen-=2;
```

```
}
x=x& 0xffff;
chksum[0]=x/256;
chksum[1]=x&0xff;
}
```

4.3 ICMP 包错误修正

ICMP 错误信息的变化包括在外层的 IP 和 ICMP 报头的变化和嵌入在 ICMP 错误信息有效负荷报头的改变。

为了使 NAT 对目的主机是透明的，嵌入在 ICMP 错误信息里的 IP 报头里的 IP 地址必须改变，嵌入 IP 报头的校验和域也必须改变，最后 ICMP 报头校验和也必须随着有效负荷的变化而变化。

在 NAPT 设置中，如果嵌入在 ICMP 里的 IP 信息和 TCP，UDP 或 ICMP 查询包同时发生，你必须改变在 TCP/UDP 报头里的相应的 TV 端口数或 ICMP 查询报头里的查询标志域。

最后，传输 ICMP 包的 IP 头必须改变。

4.4 FTP 支持

作为最通用的一种应用之一，FTP 要求一个 ALG 来管理控制任务有效负荷来决定保证数据传输参数。FTP ALG 是大部分 NAT 执行的一个整数部分。

FTP ALG 表需要一个一个专门的表来纠正 TCP 系列和确认源 FTP 或目的 FTP 端口数。这个表里头应该有源地址，目的地址，源端口，目的端口，系列号和时间戳。新的内容只是在 FTP 端口命令或 PASV 反馈时才增加。对每一个 FTP 端口命令或 PASV 反馈系列数有可能增加或减少。系列数在外传时增加和确认数随往内传时减少。

对任何 NAT，FTP 有效负荷局限于私有地址和它们指派的外部地址（编码成 ASCII 码 8 进制）。但是对 NAPT 设置，这个转换必须同时包括 TCP 端口（ASCII）。

4.5 DNS 支持

考虑传统 NAT 任务主要是从本地外传数据，DNS ALG 可能避免和下面的传统 NAT 相关使用。在局域网内部的 DNS 服务器维持内部主机地址或有可能外部主机地址和名字的映射。外部 DNS 服务器只是维持外部主机地址和名字的映射，而不对内部主机进行映射。如果一个局域网没有内部 DNS 服务器，所有 DNS 请求直接到外部 DNS 服务器去找外部主机的映射。

4.6 IP 选项处理

一个含有任何 IP 选项记录路由，严格源路由或松散源路由的 IP 数据包括记录和使用中间路由器的 IP 地址。NAT 中间路由器可能不支持这些选项或者处理这些选项时不对地址进行转换。不对地址进行转换的结果将是在源路由中私有地址一直暴露出来。这个不会危害报文的传输路径，因为每个路由器只看下一跳的路由器。

5 混杂的问题

5.1 本地和通用地址的划分

在这个文档里描述的 NAT 操作，有必要划分 IP 地址空间为两部分—在内部残域里使用的私有地址和通用唯一的地址。不论是私有地址还是全球通用地址给定的话，都不能重叠。

交迭的问题为如下。假设在残域 A 的一个主机试图传送数据报到残域 B 中的主机，但是残域 B 中的全球地址和残域 A 的私有地址交迭。在这种情况下，在残域 A 中的路由器不能够从分辨它自己的私有地址和残域 B 的全球通用地址。

5.2 推荐的私有地址空间

[RFC1918]已经对地址空间的分配作了推荐。因特网授权数量权威（IANA）有 3 个 IP 地址空间块，相应的为：10.0.0.0/8,172.16.0.0/12,和 192.168.0.0/16。在 pre-CIDR 符号中，第一个为唯一的 A 类网络块，第二块为有 16 个相邻的 B 类网络块，第三块为有 256 个 C 类网络的网络块。一个组织内部需要用如上的 IP 地址不需要和 IANA 或因特网注册机构有任何调和。这些地址空间能够同时被许多对立组织使用，用边界路由器来执行 NAT 操作。

5.3 NAT 上路由

路由器运行 NAT 不应该用局域网影响到主干网。只有有通用地址的网络才能在残域网外被识别。但是，NAT 从残域边界路由器获得的全球信息能够进入残域。特别的是，NAT 残域路由器有一个静态路由配置来通过广域网连接传送外部流量到服务商路由器，和服务商路由器有一个静态路由配置在广域网连接来传输 NAT 报文（如，目标 IP 地址在 NAT 管理通用地址范围列表里）到 NAT 路由器。

5.4 从基本 NAT 到 NAPT 的交换

在基本 NAT 设置里，当私有节点比通用地址数量多时（也就是说，一个 B 类

私有网络映射一个 C 类地址网络块），外面网络连接本地节点有可能突然中断在最后一个通用地址用完之后。这个是非常不方便和受限制的。这样的情况能够安全的避免通过有选择地允许基本 NAT 路由器为在地址表最后一个通用地址交换成 NAPT 设置。这能保证局域网里主机能够和外部节点和服务能够在大部分应用中连续的连接。但是记住，如果一些基于基本 NAT 的应用由于交换到 NAPT 突然中断有可能引起混乱。

6 NAT 局限性

广泛的说，[NAT-TERM]包括所有 NAT 类型的局限性。下面的部分说明传统 NAT 的局限性。

6.1 私有和安全

传统 NAT 被认为提供一种私有机制，因为任务是从主机出发的单向连接和私有主机地址的确切地址对外部网络是不可见的。增强私有性的相同特性使调试问题更加困难（包括安全问题）。如果私有网络里的一个主机用某种方式乱用因特网（例如试图攻击另外一台机器或甚至发送大的垃圾数据报），那么更加困难追击确实的原因因为主机隐藏在 NAT 服务器中）。

6.2 在局域网中根据映射通用地址 NAT 的 ARP 接口

NAT 必须只能在边缘路由器或残域中。在这个文档中提供的例子寿命了基本 NAT 和 NAPT 可以从 NAT 路由器维持一个广域网连接到外部路由器中。（如，服务提供商路由器）。

但是，如果广域网连接由局域网连接代替和如果所有 NAT 映射的通用地址属于局域网段有相同的 IP 子网，NAT 路由器将提供属于相同子网的地址范围 ARP 支持。根据 ARP 要求 NAT 映射通用地址用它自己的 MAC 地址 在基本 NAT 中是必须的设置。如果一个 NAT 路由器不适应这些要求，在网络中没有其它节点拥有这些地址然后没有反映。

这些设想不可能用 NAPT 设置除了当在 NAPT 映射中的单个地址不是 NAT 路由器的接口地址。（例如，在上面 5。4 中谈到的从基本 NAT 到 NAPT 的交换一样）。用 NAT 地址映射直接连接的子网范围内的一个地址可以避免在服务提供商路由器的静态路由设置。

作者的意见是一个局域网连接到服务提供商路由器不是非常普通的。但是，销售商在这种情况下对支持代理 ARP 比较感兴趣。

6.3 在 NAPT 设置中外发 TCP/UDP 数据报的转换

在 NAPT 设置中外发 TCP/UDP 数据报的转换（如，那些从私有主机发出的地址）注定要失败。它的原因如下：只有第一个数据片包含 TCP/UDP 报头，而这个数据报头对数据报的发送又是必须的。接下去的片段不包含 TCP/UDP 端口信息，但是包含其它第一个数据报中包含的一些标志信息。也就是说，两个私有主机发送 TCP/UDP 数据报到相同的目的主机。和，它们用相同的片标志。当目的主机收到这两个没有相关的数据报，它们有相同的片标志，和相同的指派主机地址，所以不可能决定数据报是属于哪个发送任务。相应的，两个任务同时崩溃。

7 当前实现

很多行业应用商业应用，这些商业应用和这个文档中描述的 NAT 紧密关联。LINUX 公众软件在 IP 伪装下有 NAT。FreeBSD 公众软件用 NAPT 来运行用作邮件收发的后台程序。但是必须注意，LINUX 源程序包含 GNU 声明，而 FreeBSD 软件包含 UC Berkeley 声明。

8 安全考虑

在{NAT-TERM}描述中的对任何 NAT 的安全考虑对传统 NAT 也是适用的。

参考文献

[NAT-TERM] Srisuresh, P。 and M。 Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999。

[RFC 1918] Rekhter, Y。, Moskowitz, B。, Karrenberg, D。, de Groot, G。 and E。 Lear, "Address Allocation for Private Internets",BCP 5, RFC 1918, February 1996。

[RFC 1700] Reynolds, J。 and J。 Postel, "Assigned Numbers", STD 2, RFC 1700, October 1994。

[RFC 1122] Braden, R。, "Requirements for Internet Hosts -- Communication Layers", STD 3, RFC 1122, October 1989。

[RFC 1123] Braden, R。, "Requirements for Internet Hosts -- Application and Support", STD 3, RFC 1123, October 1989。

[RFC 1812] Baker, F。, "Requirements for IP Version 4 Routers",RFC 1812, June 1995。

[FTP] Postel, J。 and J。 Reynolds, "FILE TRANSFER PROTOCOL (FTP)", STD 9, RFC 959, October 1985。

[TCP] Defense Advanced Research Projects Agency Information Processing Techniques Office, "TRANSMISSION CONTROL PROTOCOL (TCP) SPECIFICATION", STD 7, RFC 793, September 1981。

[ICMP] Postel, J。, "INTERNET CONTROL MESSAGE (ICMP) SPECIFICATION",STD 5, RFC 792, September 1981。

[UDP] Postel, J。, "User Datagram Protocol (UDP)", STD 6, RFC 768, August 1980。

[RFC 2101] Carpenter, B。, Crowcroft, J。 and Y。 Rekhter, "IPv4 Address Behaviour Today", RFC 2101, February 1997。

译文原文出处： RFC 3022 Traditional IP Network Address Translator (Traditional NAT)