NAT(网络地址转换)是如何工作

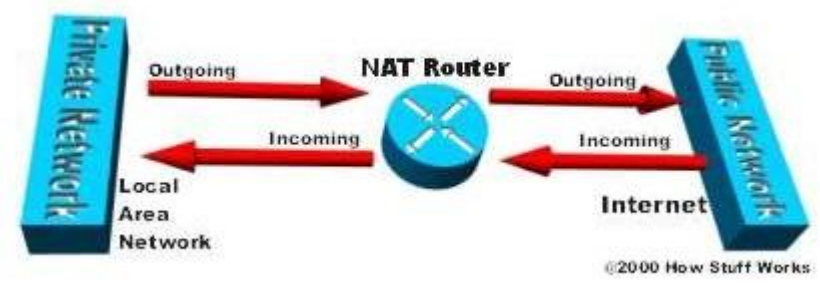
如果你正在阅读本文，那你很有可能已经连上了因特网，这就是你用网络地址转换（Network Address Translation, NAT）的一个很好的机会！因特网已经发展到比人们当初设想时还庞大得多了。尽管其具体规模无法知晓，但现在估计有 1 亿台主机和超过 3.5 亿的用户活跃在因特网上。这比美国所有人口总数还多！（这篇文章发布较早，如今实际数量已经远远超过这个了，译者）事实上，因特网每年都以两倍的速率不断扩大。

那么面对日益庞大的因特网，NAT 该做什么呢？所有的事情！对于一台计算机要想和其他计算机进行通信或应用因特网上的 Web 服务（电子邮件等各种网络服务，译者），那么它必须要有一个 IP 地址。一个 IP 地址是一串唯一的 32 位数字，它标识你的计算机在网络中的位置。它基本上就像你的邮箱地址一样：一种能够正确找到你并把网络信息送给你的地址。

当初 IP 地址问世时，所有人都认为其拥有的地址能够覆盖到每一个人。理论上，互不相同的 IP 地址有 4,294,967,296（232）个。但实际上真正可用的地址数比这要少（在 32 亿到 33 亿之间），因为 IP 地址按类别划分的方法和需要留出一些地址来进行广播，

伴随着因特网的膨胀和家庭网络与公司网络的不断增加，可用的 IP 地址显然已经不够了。最容易想到的解决方案是重新设计地址格式让它拥有更多的地址。这种方案正在开发，但是将花费数年才会实现，因为它需要跟换全球整个因特网的基础设备。

NAT 路由器传送进出私有网络的示意图：



这就是 NAT（RFC 1631）需要拯救的地方。总的来说，网络地址转换（NAT）允许一个单独的设备，比如像路由器，作为因特网（公共网络）和局域网（私有网络）之间的代理。这就意味着对外部网络来说仅仅只需要一个单独的 IP 地址就可以代表一组（内部网络的）计算机。

IP 地址的短缺仅仅是使用 NAT 的一个原因。另外两个原因是：

安全

管理

你将知道跟多关于你如何收益于 NAT 的东西，但是首先，让我们再靠近点看看 NAT 还能做什么 ...

读者所应具备的知识：

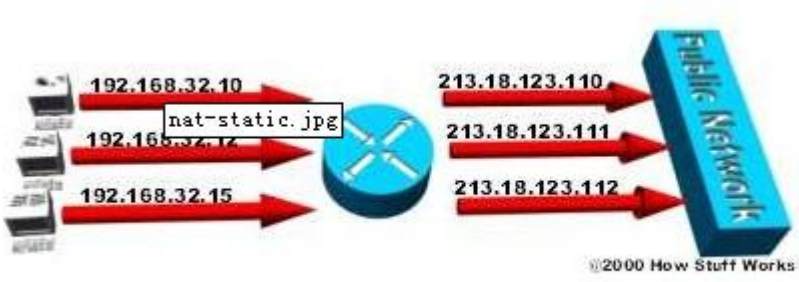
本篇文档的读者应具备以下知识：

IP 地址和路由的概念

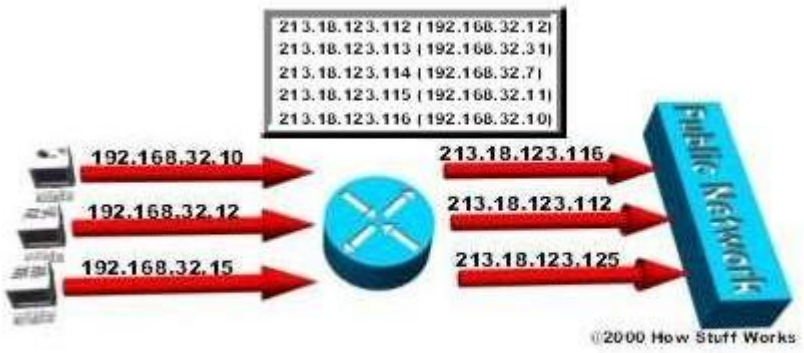
所用到的工具 这篇文档的描述并不受限于任何特定的软件和硬件。

面具之后 NAT 就像一个大办公室里的传达员。我们假设你让传达员拒绝将任何电话接进来给你，除非你要求将其接进来。然后，你给潜在客户打了一个电话，（因为不在）告诉他们回话给你。你告诉传达员你正在等待一个来自这个客户的电话，并允许将他们接进来。

这个客户拨打了主号码（办公室对外的电话号码，译者）到你的办公室，这是客户唯一能查到的号码。当客户告诉传达员他们想找谁的时候，传达员就会查看一张匹配有公司人名和其电话分机的查看表。这个传达员知道你在等待这个电话，因此传达员将这个电话转到了你的分机。 思科开发的网络地址转换 (NAT) 设备是工作在内部网络和外部网络之间的。NAT 的实现有许多种方式，并有许多种工作方法：

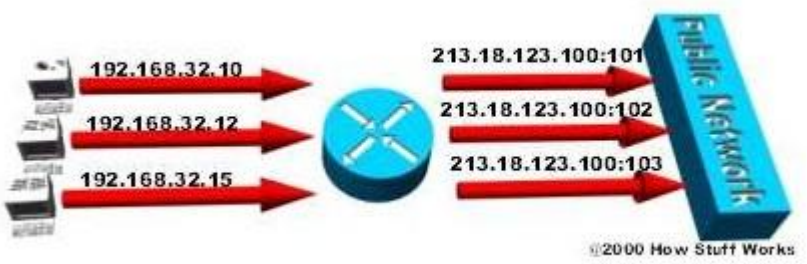


静态 NAT - 用一个一对一设备将一个未注册的 IP 地址映射到一个已注册的 IP 地址。当一台设备需要被外界网络可达时尤其有用。在静态 NAT 中，IP 地址是 192.168.32.10 的计算机总是被转换成 213.18.123.110：

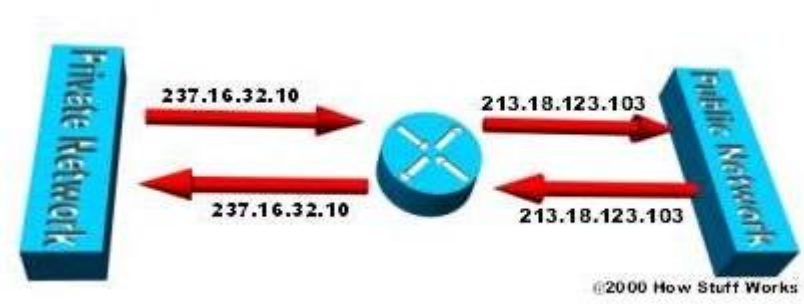


动态 NAT - 映射一个未注册的 IP 地址到一组已注册 IP 地址里的一个。动态 NAT 也是在未注册和已注册 IP 地址之间建立映射关系，但是映射地址的来源是取决于通信时地址池中的可用注册 IP 地址数。在动态 NAT 中，IP 地址是 192.168.32.10 的计算机总是转换成范围在 213.18.123.100 - 213.18.123.150 中第一个可用 IP 地址：

过载 - 映射多个未注册 IP 地址到一个已注册 IP 地址时，动态 NAT 采用不同的端口。也就是所谓的 PAT (Port Address Translation, 端口地址转换)，单地址 NAT 或端口级 NAT 复用。在过载中，私有网络中的每一台计算机都转换到同一个 IP 地址 (213.18.123.100) 但是被分配不同的端口号：



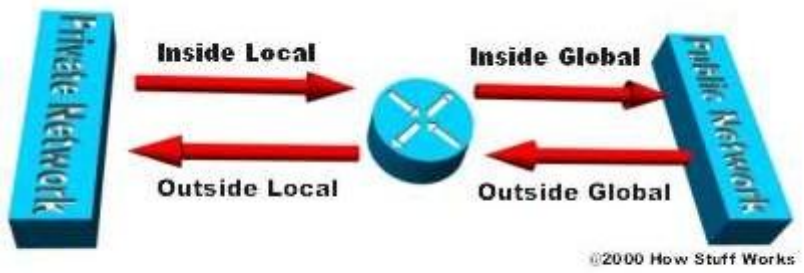
重叠 - 当你在内网使用的 IP 地址已经在另一个网络中被注册并使用了，路由器就会维护一个有这些地址的检查表，这样路由器就可以截断 (内网) 这些地址并将它们替换到唯一已注册 IP 地址。特别注意， NAT 路由器必须将 ”内部“ 已注册地址转换到另一个已注册唯一地址，还必须将 ″外部″ 已注册地址转换到私有网络的唯一地址。这将通过静态 NAT 或是你能用 DNS 并实现动态 NAT 来实现。内部 IP 地址的范围 (237.16.32.XX) 已被另一个网络注册并使用。因此，路由器将进行地址转换来避免和另一个网络的潜在冲突。当信息被送往内部网络时，它还将外部已注册的 IP 地址转换回本地原来的 IP 地址：



内部网络通常是一个局域网（LAN, Local Area Nerwork），通常也被称为存根域。存根域只在内部使用 IP 地址的局域网。存根域中的大多数流量都只在内部传送，不会离开这个内部网络。一个存根域包括注册和未注册的 IP 地址。当然，任何使用未注册 IP 地址的计算机都必须用网络地址转换来和外部网络通信（任何时候存根域内只有一部份主机要与外界通信，甚至还有许多主机可能从不与外界通信，所有整个存根域只需要共享少量的全局 IP 地址，译者注）。

有多种方法能配置 NAT。在下面的例子中，NAT 路由器被配置来将处于私有（内部）网络中的未注册 IP 地址（内部地址）转换成注册 IP 地址。当一台拥有未注册地址的内部设备需要和公共（外部）网络通信时，NAT 将会起作用。

ISP（Internet Server Provider，网络服务提供商)给你的公司分发一定范围的 IP 地址段。分配的这一堆地址是注册唯一的 IP 地址，即所谓的内部全局地址[1]。未被注册的私有 IP 地址被分成两组，数量少的一组（外部本地地址[2]）将被 NAT 使用，而大多数将用于存根域[5]所谓的内部本地地址[3]。外部本地地址用于转换处于公共网络中设备的唯一 IP 地址，即外部全局地址[4]。更多关于本地和全局地址的定义参见 NAT: Local and Global Definitions。NAT 仅仅只是转换在内部和外部网络之间被指定需要被转换的流量。任何不符合流量转换规则或那些仅仅在其他接口（即路由器上的 LAN 口，译者）之间转发的流量并不会被转换，它们只会被转发。根据 IP 地址是私有网络（存根域）还是共有网络（因特网）和流量是输入还是输出，而被分为许多种。



大多数在存根域（网络）中的计算机都用内部本地地址相互通信。

在存根域（网络）中的一些计算机需要经常和外部网络通信。这些计算机就会被分配内部全局地址，这就意味着他们不再需要地址转换。

当一台在存根域（网络）中被分配了内部本地地址的计算机想要和外部网络通信时，数据包就会像通常一样被路由到其默认网关，此时网管充当 NAT 路由器功能。

这个 NAT 路由器检查它的路由表，查看有没有包含这个数据包目的地址的条目。如果其目的地址不在这个路由表里，路由器就将数据包丢弃。如果这条目存在，路由器就验证这个数据包是否是从内部网络到外部网络，并检查其是否满足转换规则。路由器然后查看地址转换表，看有没有一个条目是这个内部本地地址对应的内部全局地址。如果有，路由器就用这个内部全局地址来替代数据包的内部本地地址。如果仅仅是配置了静态 NAT 且没有这样的条目存在，路由器就会不转换地址而直接转发数据包。

通过内部全局地址，路由器将数据包转发至它的目的地址。

共有网络中的一台计算机要发送一个数据包到私有网络。数据包中的源地址是一个外部全局地址。目的地址是一个内部全局地址。

当数据包从外部网络到达路由器时，NAT 路由器查看地址转换表发现其器目的地址有对应的内部本地地址，NAT 路由器就将其映射到这个存根域（网络）的那台计算机上。

NAT 路由器将这个数据包中的内部全局地址（即其目的地址，译者）转换成内部本地地址后再查看路由表。只要在地址转换表中没有发现相应条目，路由器就不会转换，更不会去查看路由表来验证目的地址，它仅仅是将其丢弃而已。

关于用路由器命令执行 NAT 转换的详细信息参见 NAT Order of Operation

NAT 过载运用了 TCP/IP 协议栈的一个功能，多路复用技术，它允许一台计算机用不同的 TCP 或 UDP 端口维持许多当前来自远程计算机的连接。一个 IP 数据包的头部包含以下信息：

源地址——发出数据包的计算机的 IP 地址，例如，201.3.83.132

源端口号——源计算机为 TCP 或 UDP 分配的端口号，例如，1080.

目的地址——接收数据包的计算机的 IP 地址。例如，145.51.18.223.

目的端口号——源计算机请求接收计算机开放的 TCP 或 UDP 端口号，例如，3021.

地址用来标识一个连接两端的两台计算机，而端口号则确保两台计算机之间的连接都有一个唯一的标识符。这四个数字一起确定了一个唯一的 TCP/IP 连接。每一个端口号都是 16 位，这就是说一共有 65536 个（2^16）个端口可供选择。事实上，不同的厂商映射端口的方式略有不同，所以你可能只有大约 4000 个端口是可用的。

动态 NAT 和过载举例

Flash 动画：动态 NAT

这就是动态 NAT 是如何工作的：

点击链接 Dynamic NAT Flash animation ，点击任何一个绿色的按钮是成功发送一个出去或进入存根域（网络）。点击任何一个红色按钮是发送一个带有非法地址而被路由器丢弃的数据包。

左边是一个公司的内部网络（存根域），其中的 IP 地址并不是由 IANA（Internet Assigned Numbers Authority, 互联网编号分配机构，一个掌握所有 IP 地址的全球权威机构 ）分配的。这些地址并不会被路由器转发，因为它们并不是唯一的（其他内部网络也可能有相同的地址，译者）。这些就是所谓的内部本地地址。

这家公司将其路由器配置了 NAT。这个路由器有一段由 IANA 分配给这家公司的唯一 IP 地址。这些地址就是内部全局地址。

然后在这个存根域中的一台计算机试图连接一台处于外部网络的计算机，比如一台网络服务器。

这台路由器收到了来自存根域的这台计算机的数据包。

路由器在检查了路由表之后，转换规则的验证程序就会开始执行，若通过，则路由器会将这台计算机的不可路由的 IP 地址保存到一张地址转换表中。路由器用内部全局地址中第一个可用 IP 地址替换发送计算机的不可路由的 IP 地址。现在，地址转换表就拥有了这台计算的不可路由 IP 地址到一个唯一 IP 地址的匹配映射。

当一个数据包从目的计算机（如网络服务器）发送回来时，路由器检查数据包的目的地址。然后它查看地址转换表确定数据包是属于哪一台存根域中的计算机。路由器将其目的地址换成它保存在地址转换表中的那个，然后将数据包发送到那台计算机。如果它没有在表中找到一条匹配，它就会丢弃这个数据包。

这台计算机收到来自路由器的数据包。只要有计算机想要和外部网络通信，它们将重复这个过程。

这是 NAT 过载如何工作的：

假设一个公司的内部网络（存根域）已经被设置了未被 IANA 专门分配的不可路由的 IP 地址。

这家公司将路由器设置为 NAT 可用的。路由器拥有一个唯一由 IANA 分给这家公司的的 IP 地址。

在存根域中的一台计算机试图连接外部网络中的一台计算机，例如一台网络服务器。

路由器收到来自存根域的这台计算机发送的数据包。

在进行转换之前，路由器查找路由并验证数据包是否合乎规则，然后路由器保存这台计算机的不可路由的 IP 地址和其端口号到一张地址转换表中。路由器将发送计算机的不可路由的 IP 地址替换路由器的 IP 地址，将发送计算机源端口号替换成能够匹配地址转换

表中所存的发送计算机地址信息位置的端口号。现在这张转换表就将这台计算机的不可路由的 IP 地址及其端口号与路由器的 IP 地址绑定起来了。

当一个数据包从目的计算机发送回来时，路由器检查其目的端口号（不用检查其 IP 地址，因为全部内部网络都只用路由器的 IP 地址，路由器用端口号映射不同的计算机，译者）。然后路由器查看地址转换表，找到这个数据包所对应的存根域中的计算机。如果有，则路由器替换其目的地址和目的端口号，然后发送到那台计算机

这台计算机接收来自路由器的数据包， 并且只要这台计算和外部网络通信，此过程就会重复执行。

由于 NAT 路由器现在已经拥有了这台计算机保存在地址转换表中的的源地址和源端口号，它将会在有效期内继续使用同一个端口号进行转换。每当一个新的条目加入到路由器的转换表中时，计数器就会重置。如果在计数器到期之前连接就不可用了，其对应条目就会从表中删除。

下面这张表显示了一台处于存根域的计算机对外部网络将会如何表现：

源计算机	源计算机 IP 地址	源计算机 端口号	NAT 路由器 IP 地址	NAT 路由器分配的端口号
A	192.168.32.10	400	215.37.32.203	1
B	192.168.32.13	50	215.37.32.203	2
C	192.168.32.15	3750	215.37.32.203	3
D	192.168.32.18	206	215.37.32.203	4

就如你说见， NAT 路由器将每一台计算机的 IP 地址和端口号都保存在地址转换表中。然后它用它自己注册的 IP 地址替换发送来的数据包的 IP 地址，并将端口号替换为该数据包的源计算机信息条目在表中的相应位置号。这样任何一台处于外部网络的计算机都会在发送给它的数据包里找到 NAT 的 IP 地址和由路由器分配的端口号。

你也可以给存根域中的一些计算机指定 IP 地址。你可以创建一个 IP 地址列表来告诉路由器网路中的哪些计算机需要 NAT 服务。这样，所有其他 IP 地址的计算机都不会执行转换了。

一台路由器能同时执行地址转换的个数主要取决对于它拥有的 DRAM（动态随机存储器，Dynamic Random Access Memory）。但是由于通常的地址转换条目是 160 字节，而一台有 4MB 大小 DRAM 的路由器理论上可以同时执行 26214 个地址转换！这对大多数应用都已经足已。

IANA 事实上专门给不可路由的网络指定了一段 IP 地址。这些地址是未注册的（关于这些地址的范围定义请参见 RFC 1918：Address Allocation for Private Internets），也就是说没有任何一家公司或机构有权利声称他们拥有这些地址并在公共网络上使用。路由器并不会直接转发数据包到未注册地址，因为它们使用未注册地址就意味着这些网络是私有的，并不想被外界所知道。这就是说一个

数据包从一个未注册地址能够达到一台有注册地址的计算机，但是其响应数据包将会在它到达的第一个路由器就被丢弃（这里说的是不是用 NAT 的情况，译者）。

这是在三类 IP 地址中用于私有网络的地址段：

地址段 1 用于 A 类地址：10.0.0.0 到 10.255.255.255

地址段 2 用于 B 类地址： 172.16.0.0 到 172.31.255.255

地址段 3 用于 C 类地址： 192.168.0 到 192.168.255.255

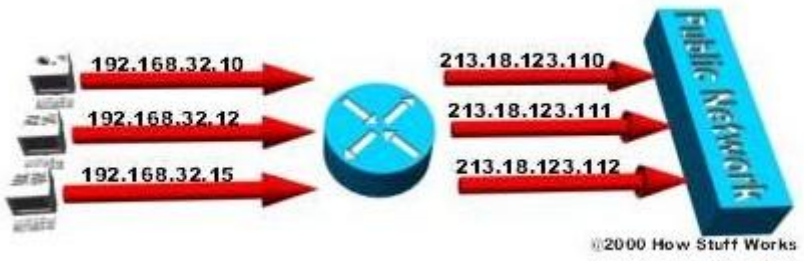
虽然每一段都位于不同类地址中，但是在你的内部网络中你用那一段并没有限制。但它是一个很好的减少 IP 地址冲突的方式。

安全和管理

在你的内部网络和外部网络（或者说因特网）之间使用动态 NAT 相当于自动建立了一个防火墙。动态 NAT 仅仅允许来自内部存根域发起的连接。本质上就是说，一台处于外部网络的计算机将不能连接到你的计算机，除非你的计算机已经建立了连接。所以你可以浏览因特网，连上一个站点，甚至可以下载文件。但是其他人却不能像这样简单的获取到你的 IP 地址并用它连接上你的计算机上的端口。

静态 NAT ，也就是所谓的入站映射，允许在特殊情况下来自外部设备发起的连接到处于存根域中的计算机。例如，你或许希望映射一个内部全局地址到一个指定的内部本地地址，它指向你的网络服务器。

静态 NAT（入站映射）允许当一台在存根域中的计算机与外部网络中的设备通信时维持一个指定的地址：

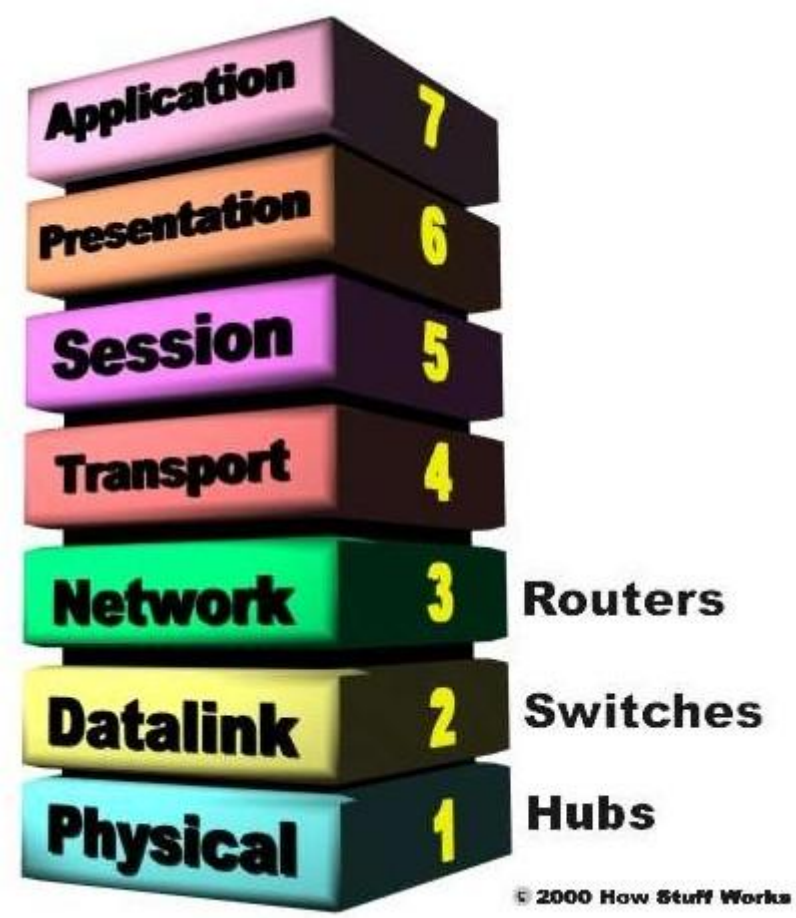


一些 NAT 路由器还提供额外的过滤和流量记录功能。过滤功能让你的公司能控制公司雇员能够访问哪些网站，阻止他们查看可疑的资源。你可以运用流量记录来创建一个记录文件，记录哪些网站被访问了，并根据它生成报告。

网络地址转换常常和代理服务搞混，但是它们之间有明确的不同。NAT 对源和目的计算机都是透明的。没有任何一方会意识到它正在和第三方设备打交道。但是代理服务却不是透明的。源计算机知道它正向代理服务器发起一个请求，而且你还必须进行配置才能这样

做。目的计算机会认为代理服务器就是与它直接通信的源计算机。还有，代理服务通常工作在 OSI 参考模型的第 4 层（传输层）或更高，而 NAT 工作在第 3 层（网络层）。由于代理服务工作在更高层，所以通常它将比 NAT 要慢。

NAT 工作在 OSI 参考模型的网络层（第 3 层）是有道理的，因为路由器就工作在这一层：



NAT 真正的好处是它在网络中是透明的。例如，你可以将你的 Web 服务器或 FTP 服务器移到另一台主机上而不用担心会破坏连接。只需简单地修改入站映射，将路由器映射到你的新内部本地地址就行了。你也可以很容易地改变你的内部网络，因为唯一的外部 IP 地址不是属于路由器就是来自一段分配的全局地址。

NAT 和 DHCP 简直就是天作之合，你可以为你的存根域选择一段未注册 IP 地址然后用 DHCP 服务将它们分发出去。这也使你想扩大网络规模时变得更加容易。你不再需要向 IANA 请求更多的 IP 地址，你只需增加配置在 DHCP 中的可用 IP 地址段，这样你网络中的新增计算机立即就有了地址空间了。

多宿主

由于商业现在正越来越依赖于因特网，拥有多个连接点到因特网正快速成为他们的网络策略中的一部分。多链路，就是所谓的多宿主，当其中一条链路崩溃时，它减少了潜在的灾难性崩溃的可能。

为了维持一条可靠的连接，多宿主允许一家公司通过减少在单条链路上连接到因特网的计算机数量，以此来达到负载平衡。通过多链路而达到分布式负载将会提高性能，并且能够显著地减少等待时间。 多宿主网络通常是连接到不同的 ISP (Internet Service Providers，网络服务供应商)。每一个 ISP 都分配一个（或一段）IP 地址给这家公司。路由器用 BGP (Border Gateway Protocol，边界网关协议)，TCP/IP 协议栈的一部分，在运行不同网络协议的网络之间进行路由。在一个多宿主网络中，路由器在存根域中利用 IBGP (Internal Border Gateway Protocol，内部边界网关协议），在与其他路由器之间通信时利用 EBGP (External Border Gateway Protocol，外部边界网关协议)。当多宿主网络用到 NAT 时，NAT 路由器会被配置来自不同 ISP 分配的多个内部全局地址段。同样的内部本地地址将会被映射到多个不同的来自 NAT 的内部全局地址，这取决于流量将被路由到哪一个目的地址。这就是所谓的目的地的 NAT，查看 NAT - Ability to Use Route Maps with Static Translations 获得跟多信息。

多宿主对于连接到一个 ISP 的链接崩溃时很有效。一旦路由器连接到的那个 ISP 的链接崩溃了，它将马上将所有经过它的流量重定向到其他路由器。

NAT 可用于缓解对于多宿主多用户延伸的可预测路由。

[1] inside global(内部全局地址)：私有主机在非自有网络中使用的地址，通常情况下 inside global 地址是从合法的全球统一可寻址空间中分配的地址，也就是通常所说的共有 IP。inside global 地址的特点是只会出现在非自有网络中并且一定是给私有主机使用的。

[2] outside local(外部本地地址)：非私有主机在自有网络内表现出来的 IP 地址。该地址是自有网络的管理员为本网络以外的设备所准备的用于在自有网络内使用的 IP 地址。outside local 地址的特点是只会出现在自有网络内但是是供给非私有主机使用的。

[3] inside local(内部本地地址)：在自有网络中分配给私有主机的地址，一般情况下该地址是 RFC1918 中定义的私有地址。inside local 地址的特点是只会出现在自有网络中并且一定是给私有主机使用的。

[4] outside global(外部全局地址)：非私有主机在自有网络以外的区域使用的 IP 地址，是非私有主机所在网络的管理员负责管理个分配的。outside global 地址的特点是不会出现在自有网络中而且不是给私有主机使用，不归自有网络的管理员负责。

[5] 存根网络（stub network）:只有一条连接到其邻居网络的网络。