正确设置 **NAT**

目前国内宽带越来越普及，很大一部分用户是通过 ADSL 连接到 Internet 上的，目前绝大多数的 ADSL Modem 都集成有 NAT 功能，而很多用户对 NAT 功能并不是很熟悉，在许多的具体的应用中（如网上视频聊天、自建 WEB/FTP 站点、内网中的 BT 下载等）都要对 NAT 功能进行正确配置，否则在平常的使用过程中经常遇到一些小麻烦，使我们不能正常、高效地使用宽带网络。因此笔者就针对 ADSL Modem 的 NAT 功能的设置与具体应用，结合本人的实际工作经验作一点说明，希望对在这方面有困难的朋友有所帮助。

笔者使用的是金浪 KN－DSL988E Ethernet ADSL ROUTER Modem，采用 Globespan 的芯片，Web 管理界面，Ethernet 接口，LAN 口通过直通线连接到一个 8 口的交换机，并在其上连接有三台电脑。为例来说明。

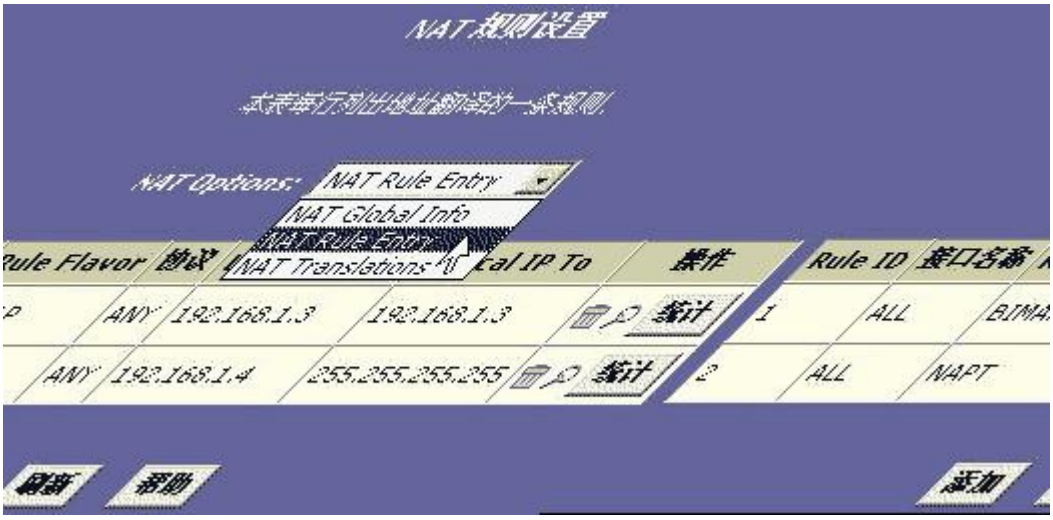
一、NAT 功能的作用

NAT－Network Address Translator 的简称，(又叫网络地址转换)，实现内网 IP 地址与公网 IP 地址之间的相互转换，其作用是让服务器把指定端口的请求转发到指定的 IP 上，让其它的机器来响应这些请求，而内网向外网发送的时候不再是像其它网关服务那样随机分配端口，而是用上面指定的端口。也就是说，NAT 将多个内部地址映射为少数几个甚至一个公网地址，使整个局域网中的机器都能够连上 Internet，同时它还有隐藏内部网络结构的作用，具有一定的安全性。但在 SOHO 应用中，当需要 Internet 上的其他用户能够访问 Intranet 上的服务如 Web 和 FTP 等，这就需要对 NAT 进行端口配置，以实现在 NAT 协议下的各种应用。

二、设置基础：NAT 规则的添加及参数说明

1、添加 **NAT** 规则

在 IE 的地址栏中键入 ADSL Modem 的 IP 地址（默认的为 192.168.1.1），输入用户名和密码（默认的用户名和均是 root），进入配置页面。在"服务"表单单击"NAT"，在"NAT Option"下拉框中选择"NAT Rule Entry"，如下图一所示。



图一

点击"添加"按钮，弹出添加 NAT 规则的页面，在其中填入相应参数，如下图二所示。注意，因为小的规则号的 NAT 规则优先执行。且在这儿 NAT 规则不能修改，要更改一个 NAT 规则的内容只能先删除它再新建一个新的规则。所以在填入 NAT 规则号时最好是选用如 5、10 等 5 的倍数以方便以后在其中插入新的规则。在添加 NAT 规则时各项参数的详细说明如下节所述。

图二

2、添加 **NAT** 规则各项参数说明：

①Rule Flavor: 规则种类，其下有 Basic、Filter 、NAPT、Bimap、RDR 和 Pass 六种不同的规则可供选择。各种规则说明如下：

Basic Rule：提供保留 IP 到 WAN IP 的地址翻译，但是端口不发生变化。这种设置执行 1：1 转换。Basic 方式转换私有（局域网内）IP 地址为公网（广域网内）地址，象 NAPT 规则，然而却不同于 NAPT 规则，Basic 规则不转换数据包头部的端口号，它们是直通不转换的，所以 Basic 规则无法提供象 NAPT 规则一样的安全级别。

Filter Rule：配置有附加标准的 Basic 规则。象 Basic Rule 一样提供保留 IP 到公网 IP 的转换，但是这种翻译只有当本地相应 IP 发出访问特定 IP 和特定服务（Web/FTP）时才发生。如同 Basic 规则方式，这种过滤规则转换公共和私有 IP 地址是在 1：1 基础上的，此过滤规则方式扩大的 Basic 规则的范围。仅当你的局域网计算机开始访问明确目标文件时如果你想让一个地址转换则你可以使用过滤方式，通过它们的 IP 地址可以识别目标文件的服务器类型（如是 FTP 或网站服务器），或者二者都是。

注意：

如果你想让规则适用仅在向外通信时的地址在一个目标地址范围内那么请指定一个目标地址范围。如果你仅输入目标地址的网络 ID 的一部份，那么规则会让外出的通信适用于所有网络上的计算机。

如果你想让规则适用于使用端口号来识别服务器的类型的外出的部份通信，那么在这里指定一个目标端口的范围。

例如如果你不指定一个目标地址，但指定一个目标端口号的开始/结束均为 21，那么这个转换会出现在所有由你的局域网到外部的 FTP 服务器的访问上（即是当你局域网中的一台计算机与外网的 FTP 服务器相连时，在数据包头部的源 IP 地址将会

改为公网 IP 地址而取代原始私有 IP 地址），公共端口号有包括有：21－FTP（文件传输协议）服务器；25－SMTP（简单邮件传送协议）服务器和 80－HTTP（全球广域网站）服务器。

如果想让这个转换规则适用在访问在指定的 IP 地址或网络的指定的服务器类型时那么在目标地址(或范围)和目标端口(或范围）框中指定它们二个的值。

NAPT Rule：系统的出厂缺省设置。转化私有和公网间的 IP 地址。这种设置将局网的保留 IP 地址和端口翻译为公网的单一 IP 地址和在 NAT 全局配置中规定的端口。这种方式提供对 LAN 的最安全的保护。

Bimap Rule：实现二个方向转换。它不同于其它 NAT 方式，Bimap 方式能执行输出和输入二个方向的地址转换。在输入方向上，当设备特定接口接收到一个使用你的公网 IP 地址作为目标地址的数据包时，这个地址将要转换为你局域网计算机上的私有 IP 地址，它看似是访问公网 IP 地址上的计算机，实际它是和一台局域网计算机进行通信。在输出方向上，一个数据包的私有原 IP 地址被转换为你的局域网的公网 IP 地址，在互联网上测试它好像数据包来自那个公网 IP 地址。Bimap 规则可以用来提供外网访问局域网设备，他们不能提供象 RDR 规则那样级别的安全，因为 RDR 规则还能依靠端口号把进入数据包改送，而 Bimap 规则无法依靠端口号，因此它允许外网访问而不管进来的数据包的目标端口。故采用此方式将局网中的某台 PC（IP）完全透明对应到公网的 IP，这样许多复杂的应用如 MSN 话音，网络游戏可以在这台 PC 正常运行。

RDR Rule：通过地址和端口的配置，使 Internet 上的用户可以通过访问路由器的广域网 IP 来访问内部网络提供的诸如 Web Server 或 FTP Server 服务。RDR 方式允许你让你的局域网中的计算机做为如一个网站或 FTP 服务器，互联网上的用户不必向你请求便可以获得这台计算机的公网 IP 地址，在所有进入和输出的数据包中，这些计算机的私有 IP 地址都转换为你的公网 IP 地址。

Pass Rule：直通规则，允许指定地址不经转换直通。尽管很多设定的规则会翻译局域网保留 IP 到公网 IP，但可以通过设置 PASS Rule 将某些固定 IP 不能翻译为 WAN IP。你可以创建一条直通规则允许一个范围的 IP 地址保持不经转换，即使其它规则已经指定要转换它们的 IP 地址也可以保持不经转换。

如果你想让直通规则仅仅执行一个地址，那么在本地 IP 地址开始和本地 IP 地址结尾框中输入同一个 IP 地址。

②Rule ID: 判断地址翻译规则的序号，最小的序号最先执行，如有规则符合，不在向更高的 ID 判断执行。

③IF Name: 请选择相应的广域网接口，如 PPP，1483B 等。常规为 NAT 规则用来在你的局域网和互联网间通信，因为设备使用广域网接口（它可能是 ppp-0, eoa-0 或 ipoa-0）把你的局域网连接到你的 ISP，这是常用的 IF 名的选择。

④协议: 选择相应协议（TCP/UDP/ICMP 等）。这个选项指定哪一类型的互联网通信将会受到这规则的转换，如果这规则应用于所有的数据 你可以选择全部，或者选择 TCP, UDP, ICMP, 或象 IANA－指定协议号码的一个从 1－255 的号码。

⑤Local 地址 From: 使用规则的本地 IP 起始值，输入你想要转换的私有 IP 地址的开始，如果选择全部则填 0.0.0.0。

⑥Local 地址 To: 使用规则的本地 IP 终结值，输入你想要转换的私有 IP 地址的结束，如果是单一 IP，填入 IP 起始值。如果选择全部则填 255.255.255.0。

以上两项可以辨别你想要转换私有地址的范围，或者在二个框中输入同一 IP 地址。如果你指定的一个范围，那么范围内的每个地址都会有次序地转换为在全部公网地址范围（在 Global 地址 From: 和 Global 地址 To:框中指定的）的内的一个相应的地址。

这些地址范围应该符合在你的网络中使用的私有 IP 地址（不管是静态分配到你的 PC 中还是用 DHCP 动态分配的）。

⑦Global 地址 From: 输入你 ISP 分配给你的公网 IP 地址的开始。一般不用修改。

⑧Global 地址 To: 输入你 ISP 分配给你的公网 IP 地址的结束。一般不用修改。

注意：如果你有多个广域网接口，在这二个框中输入规则应用到这个接口的 IP 地址，那么规则不再强迫数据到达其它 PPP 接口。

⑨目的端口起始值和目的端口终止值: 目标 IP 的端口起始值和端口终结值。

⑩Lacal 端口: 本地 IP 端口。

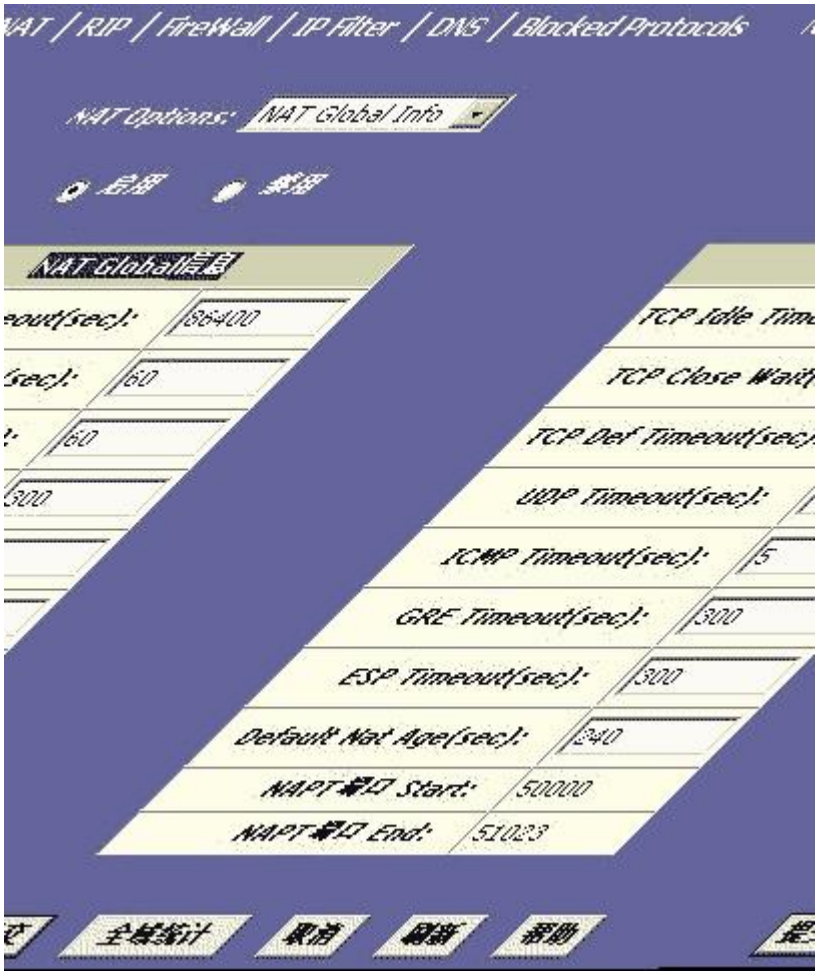
提示：没有使用 *RDR* 规则（或 *Bimap* 规则）的设备可防止外网的计算机试图访问你的局域网计算机。注意：我们不能编辑一个现存的 *NAT* 规则，要改变一个 *NAT* 规则的设定，先删除这个规则，然后建立一个新规则再修改相关参数。

三、查看 NAT 的选项和统计

当我们完成 NAT 规则的设置后，在平常的使用过程中，可能随时要了解 NAT 的工作状态，查看 NAT 端口当前的各项功能应用，监看网络上 NAT 端口的数据流量等，或者当网络出现故障时，我们可能能够从这些统计数据中找到一些原因。这就要使用到"查看 NAT 的选项和统计"，在笔者所使用的 ADSL Modem 中有三种不同的方式可为查看 NAT 的选项和统计，它们分别是：查看 NAT 的全部设置和统计、查看 NAT 规则和规则统计、查处当前 NAT 转换。下面对它们分别加以详述。

1、查看 **NAT** 的全部设置和统计

点击"服务"标签¡ú"NAT"，选择"NAT Global Info"，则弹出的"NAT Global 信息"配置页会显示有以下各项：



图三

NAT Options： NAT 选项列单，它提供可以查用全部信息页（默认显示），NAT 规则配置页和 NAT 转换页，它显示当前的 NAT 地址转换情况。

"启用"/"禁用"单选按钮：它可以打开或关闭 NAT 功能。

NAT Global 信息：NAT 全部信息表，它列举了应用到所有 NAT 规则转换的下列设定：

○TCP Idle Timeout（sec）： TCP 空闲超时时间（秒）；

○TCP Close Wait（sec）：TCP 等待关闭时间（秒）；

○TCP Def Timeout（sec）： TCP Def 暂时停转时间：当二台计算机通过互联网通信时，它们间的数据包交换是建立在 TCP 通信协议上的，依靠 TCP 协议数据包才能被传递，TCP 协议可以看成是以下三种状态之一：建立状态：正在连接时；活动状态：正在使用连接来交换数据；关闭状态：连接已经关闭。

TCP 协议受制于 NAT 规则，在活动状态时如果在规则指定的 TCP 空闲超时时间内还没有数据包交换则 TCP 协议会暂停工作；在关闭状态时如果在规则指定的 TCP 等待关闭时间内还没有数据包交换则 TCP 协议会暂停工作；在建立状态时如果在规则指定的 TCP Def 暂时停转时间内还没有数据包交换则 TCP 协议会暂停工作。

○UDP Timeout（sec）：UDP（User Datagram Protocol, 用户数据报协议）超时（秒），同 TCP 空闲暂时停转时间一样，但它时针对 UDP 通信协议的。

○ICMP Timeout（sec）：ICMP（Internet Control Messages Protocol, 网间控制报文协议）超时，同 TCP 空闲暂时停转时间一样，但它时针对 ICMP 通信协议的。

○GRE Timeout（sec）：GRE 超时，同 TCP 空闲暂时停转时间一样，但它时针对 GRE 通信协议的。

○Default Nat Age（sec）：缺省 NAT 期限（秒），对于所有其它的 NAT 转换协议，如果在这个秒数内没有数据包交换但 NAT 转换仍然有效运行。

○NAPT 端口 Start /NAPT 端口 End： NAPT 端口开启/结束，当建立了一个 NAPT 规则时，源端口将会被转换为有序的数字显示在这里。

如果你已经在这修改了这些值，点击"提交"按钮，然后点击管理标签并提交你的修改到固态存储器中。你可以点击"全域统计"来看有多少 NAT 规则已经调用和有多少数据已经被转换的累积统计数，在出现的"NAT 规则全域统计"页上的表格中提供你已经建立的每条 NAT 规则的基本信息，你可以点击"清除"按钮来清除这些数据，重新从它们的初始值来统计。

2、查看 **NAT** 规则和规则统计

要查看现在在你的系统上的 NAT 规则设定，在"NAT Options"下拉选项菜单中选择"NAT Rule Entry"，则"NAT 规则配置"页上显示有每条规则的基本信息。在"NAT 规则配置"页上你可以点击"添加"按钮来添加新规则，或者使用右边的图标来删除（）规则或查看（）规则的祥细资料。要查看一个特定 NAT 规则的使用频率，可在操作栏中点击"统计"按钮。

图四

在"NAT 规则统计"页上显示有规则已经调用了多长时间及有多少当前活动的协议正在主，调用这规则，你可以点击"清除"按钮来重置统计归零，点击"刷新"按钮来重新显示最新的统计数。

3、查看当前 **NAT** 转换

要查看 NAT 转换列表最近完成转换情况和未完成情况（对一些规则），可从"NAT Options"下拉选项菜单中选择"NAT Translations"，在弹出的"NAT 翻译"页的表格中有以下这些项：

Trans Index：全部号码，由 NAT 转换协议分配连续的号码给 IP 协议使用。

Rule ID：规则 ID，调用 NAT 规则的 ID 号。

接口：NAT 规则被调用的设备接口。

协议：数据包使用 IP 协议时受到转换的方式：TCP，UDP，ICMP。

ALG Type ：Alg（Application Level Gateway 网关使用级别）类型，如果要，它是用来打开 NAT 转换的（当启用 NAT 时，专门设定 ALG 来让某些应用软件来按规定运行）。

NAT Direction ：NAT 方向，转换的方向（引入或输出）每个端口都指定了 NAT 的方向；以太网和 USB 口定义为引入口，广域网口定义为输出口。NAT 方向由调用规则的接口决定的。

Entry Age：使用期限，NAT 转换协议的共用时间（秒）。

你可以在操作栏中点击 来查看有关 NAT 转换协议的其它详细资料，弹出的"NAT 地址翻译－详细"页上主要有以下几项：

Translated In 地址：转换地址，公网 IP 地址，它提供的可转换的 IP 地址。

In 地址：内部地址，被转换的私有 IP 地址。

Out 地址：输出地址，外面目标的 IP 地址（网站，FTP 站点等等）。

In Packets/Out Packets：输入/输出数据包，在这转换协议中已经被转换的引入和输出的 IP 数据包的数。

In 端口 s：引入端口，正在和 LAN 计算机通信的端口。

Out 端口 s：输出端口，连接到目标地址的端口号。

Translated In 端口 s：翻译为端口，局域网计算机真实端口号被转换为的端口号。

图五

四、NAT 功能的具体应用

1、内网机器对外提供 **WEB/FTP** 服务

配置内部网络 IP 192.168.1.2 对外提供 WEB 服务，192.168.1.3 提供 FTP 服务。

图六

在你的 ADSL 收到一个含有请求访问你网站服务器数据包时，这个数据包的头部包含有作为目标 IP 地址的你的局域网的公网 IP 地址，还有目标端口为 80。因为你已经为目标端口为 80 的进入的数据包设置了一个 RDR 规则，ADSL 认为这个数据包是请求访问网站服务器的，它便会转换这个数据包的目标地址为你网站服务器的私有 IP 地址并将数据包传给网站服务器。

你的网站服务器传送回应数据包，在 ADSL 传送数据包到互联网上之前，它把从你的网站服务器私有 IP 地址传来的数据包的源 IP 地址转换为你局域网的公网 IP 地址，对于一个外网用户来说就象你的网站服务器使用你的公网 IP 地址。

（1）、在"Rule Flavor："中选择 RDR 作为规则形式，如果有必要请输入一个规则号。

（2）、选择规则使用的接口。

（3）、选择一个规则适用的协议，或选择全部。

（4）、在本地 IP 地址开始和本地 IP 地址结尾框中输入同一私有 IP 地址，或者最低和最高的地址范围。

如果你在二个框中输入同一个 IP 地址，那么在进入的数据如果符合你在第 5 和 6 步的标准时将要改送到它的地址。

如果你输入的是一个范围地址，那么在进入的数据将要改送到在这个范围可用的任一计算机，这个选项常用在本地网络匹配，凭借它网络通信量可以分散到几个相同的服务器之一以达到保证有效的网络性能。

这些地址应该符合在你的网络中使用的私有 IP 地址（是静态分配到你的 PC 中或是用 DHCP 动态分配的）。

（5）、在公网 IP 地址开始和公网 IP 地址结尾框中，输入你 ISP 分配给你的公网 IP 地址。（动态获取 IP 的不用填）。

如果你有多个广域网(PPP)接口，那么规则不再强迫数据到达其它 PPP 接口。

如果你有多个广域网接口并且你想让规则强制数据到过它们中的不止一个（或全部），那么你要在框中输入开始和结束 IP 地址的范围。

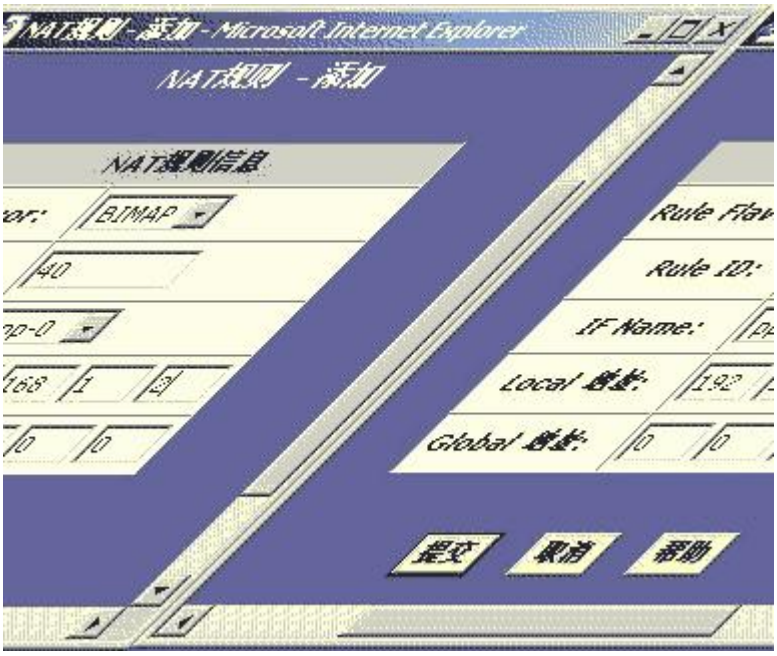
（6）、在目标端口开始和目标端口结尾框中，输入已经创建规则应用到你的局域网计算机中你所想让它获得进入数据包的端口号（或一个范围）。

进入的数据如果符合这规则标准将会改送它到你在下一个框中指定的本地端口号机上。

（7）、然后再提交你的更改。

2、特殊的网络应用

为了更多的网络应用，如内网中的 BT 下载，MSN，网络游戏等，将电脑 192.168.1.2 配置为 Bimap 的透明翻译，注意由于 MSN 语音需要用到特殊的端口，所以该方式不能支持。



图七

（1）、在"Rule Flavor："中选择 Bimap 作为规则形式，输入一个规则号。

（2）、选择规则使用的接口。

（3）、在本地 IP 地址框中输入你同意让外网访问的计算机的私有 IP 地址。

（5）、在公网 IP 地址框中，为你局域网计算机输入你想用作服务器的公开 IP 地址（动态获取 IP 的不用填）。

（6）、然后再提交你的更改。

3、共享上网

通过 NAPT 设置，只允许 30 台 PC 可以共享 ADSL（范围为 192.168.1.2 到 192.168.1.31），具体的设置如下图所示。在小型的局域网中，我们常常要提供多台机器的共享上网，并且内部网络中的机器对外部网络的访问来讲，要有较强的安全性，需要限制外网机器访问局域网中的机器，这就要使用 NAPT 规则。

图八

4、提供非标准端口服务

在局域网的计算机作为一个网站或 FTP 服务器时，可能需要计算机通过特殊的非标准端口来与外网通信，就可以用添加 RDR 规则来实现。以下的举例是使用 RDR 规则以非标准端口来给外网计算机访问内部网站服务器的：

图九

具体的规则添加步骤如例一，这里就不再详述了，但在"Local 端口"中要加以设置。

例如，如果你同意让公众访问你局域网上的网站服务器，那么你要让进入的数据包去往包含端口号为 80 的计算机上，这个设置好像一个过滤器，数据包不包含有这个端口号的将无法访问你的本地计算机。

如果你已经配置你的公用局域网计算机使用一个不标准端口号来接收通信，那么在本地端口框中输入一个不标准端口号。

这个选项转换数据包的标准端口号为你指定的你局域网计算机的不标准端口号，例如，如果你的网站服务器使用（不标准）端口号 2020，但你想接收进入数据包的端口号为（标准）80，那么你要在这输入 2020 和在目标端口框中输入 80，那么进入的数据包头部包含有 80 端口号的将会被修改为端口号 2020，这个数据然后才可以正确传送到网站服务器。