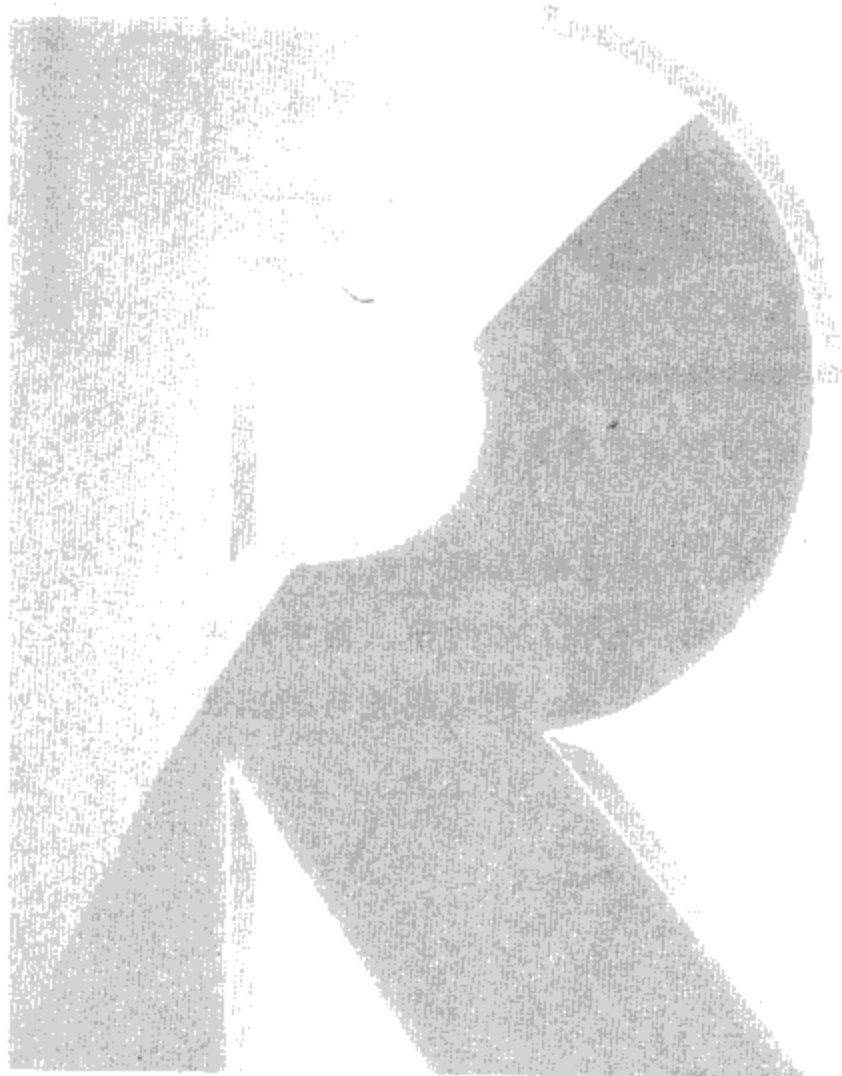


第 12 章

网络地址转换（NAT）

使用Windows Server 2008 R2的**网络地址转换**（Network Address Translation, NAT）功能，位于内部网络的多台计算机只需要共享一个public IP地址，就可以同时连接因特网、浏览网页与收发电子邮件。

- NAT的特色与原理
- NAT服务器架设实例演练
- DHCP分配器与DNS中继代理
- 开放因特网用户来连接内部服务器
- 因特网连接共享（ICS）



12-1 NAT的特色与原理

您可以将Windows Server 2008 R2设置为NAT服务器，它拥有以下的特色：

- ✎ 支持内部多个局域网内多人同时通过NAT服务器连接因特网，而且只需要使用一个public IP地址。
- ✎ 支持DHCP功能，可自动分配IP地址给内部网络的计算机。
- ✎ 支持DNS中继代理功能，可为内部局域网的计算机查询外部主机IP地址。
- ✎ 支持TCP/UDP端口映射功能，让因特网用户可以访问内部网站、电子邮件服务器等。
- ✎ NAT服务器的外部网络接口可使用多个public IP地址，然后搭配地址映射功能，让因特网的应用程序可以通过NAT服务器来与内部网络的应用程序通信。

12-1-1 NAT的网络架构实例图

Windows Server 2008 R2 NAT服务器至少需要有两个网络接口，一个用来连接因特网，一个用来连接内部网络。以下列举几种常见的NAT架构：

✎ 通过路由器连接因特网的NAT架构

如图 12-1 所示，NAT服务器至少需要两块网卡，一块连接内部网络，一块连接路由器，并通过路由器来连接因特网，其中的外网卡应该要手动输入IP地址、默认网关与DNS服务器等。

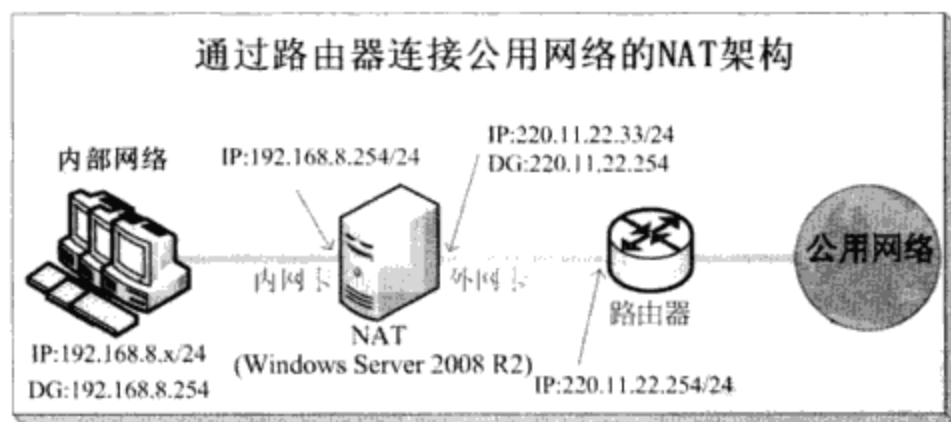


图 12-1

✎ 通过固接式xDSL连接因特网的NAT架构

同样NAT服务器至少需要两块网卡，一块连接内部网络，一块连接xDSL（例如ADSL、VDSL）调制解调器，并通过xDSL调制解调器连接因特网，如图12-2所示，其中外网卡请输入由ISP（因特网服务提供商，例如HiNet）分配的IP地址、默认网关与DNS服务器等。

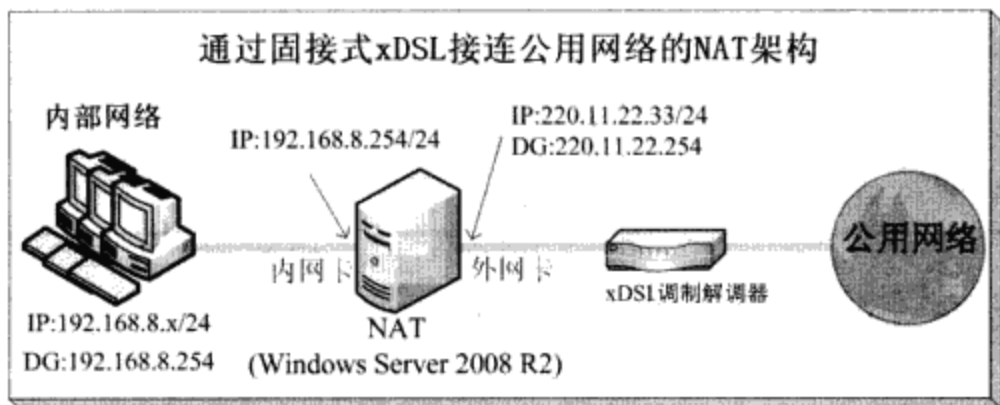


图 12-2

通过非固接式xDSL连接因特网的NAT架构

如图 12-3所示, 此处您需要在NAT服务器上新建**PPPoE请求拨号连接**, 此PPPoE请求拨号连接是通过连接ADSL调制解调器的外网卡来发送数据。通过PPPoE请求拨号连接来拨接到ISP成功后, ISP会自动分配IP地址、默认网关与DNS服务器等设置给此PPPoE请求拨号连接。

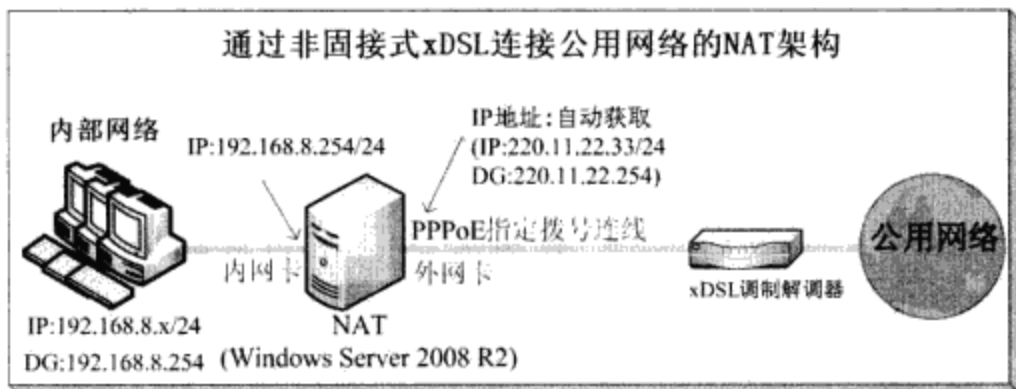


图 12-3

提示

只有一块网卡也可以扮演NAT服务器角色, PPPoE请求拨号连接是新建在这块网卡上, 也就是说NAT服务器对内通信的网卡接口与对外通信的PPPoE接口, 实际上都是通过同一块网卡在发送数据, 也因此安全与效率比较差, 故不建议采用这种架构。

通过电缆调制解调器 (cable modem) 连接因特网的NAT架构

如图 12-4所示, NAT服务器至少需要两块网卡, 一块连接内部网络, 一块连接电缆调制解调器。当通过电缆调制解调器成功连上ISP后, ISP会自动分配IP地址、默认网关与DNS服务器等给NAT服务器的外网卡。

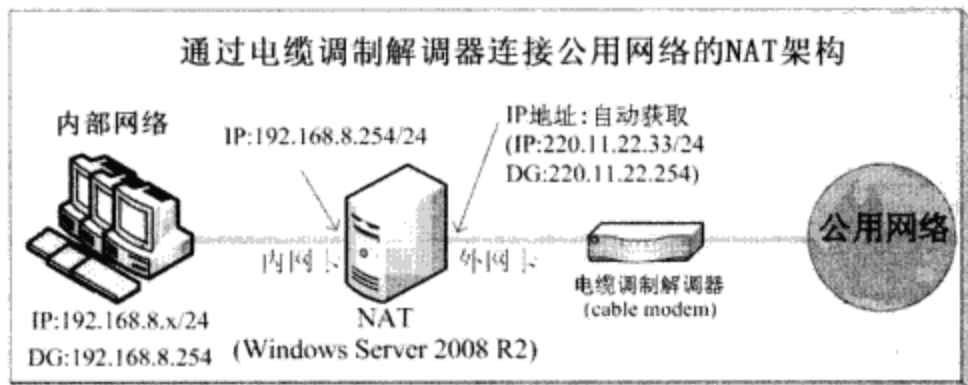


图 12-4



提示

NAT服务器也可以利用一般调制解调器与电话网络来连接ISP与因特网，不过因为它的速度太慢（56 Kbps），故较少人使用。

12-1-2 NAT的IP地址

NAT服务器的每一个网络接口（PPPoE请求拨号连接或网卡的本地连接）都必须要有有一个IP地址，且不同接口的IP地址有着不同的设置：

- 若是连接到因特网的公用网络接口，则其IP地址必须是public IP地址
若是通过路由器或固接式xDSL连接因特网的话，则此IP地址是由ISP事先分配，此时您需要自行将此IP地址输入到网卡的TCP/IP设置处；若是通过非固接式xDSL或电缆调制解调器连接因特网的话，则IP地址是由ISP动态分配的，不需要手动设置。
- 若是连接内部网络的专用网接口，则其IP地址可使用private IP地址
Private IP地址可使用的范围如表 12-1所示。我们在前面几个示例图中所采用的private IP地址的网络标识符为192.168.0.0、子网掩码为255.255.255.0。

表 12-1

网络标识符	默认子网掩码	Private IP地址范围
10.0.0.0	255.0.0.0	10.0.0.1~10.255.255.254
172.16.0.0	255.240.0.0	172.16.0.1~172.31.255.254
192.168.0.0	255.255.0.0	192.168.0.1~192.168.255.254

12-1-3 NAT的工作原理

支持TCP或UDP协议的服务，都有一或多个用来代表此服务的端口号（port number），表 12-2中列出一些最常用的服务器服务与端口号。而客户端应用程序（例如网页浏览器）的端口号是由系统动态产生的，例如当用户在浏览器 Internet Explorer 内输入类似 <http://www.microsoft.com/> 的URL路径上网时，系统就会为Internet Explorer新建端口号。



提示

如果您已经上网的话，可以利用**netstat -n**命令来查看浏览器与网站所使用的端口号。

表 12-2

服务名称	TCP端口号
HTTP	80
HTTPS	443
FTP控制通道	21

(续表)

服务名称	TCP端口号
FTP数据信道	20
SMTP	25
POP3	110
NNTP	119

在介绍NAT原理之前，我们先简单说明一般浏览网页的过程。两台计算机内支持TCP或UDP的应用程序是通过IP地址与端口号来相互通信的，例如图 12-5中右方的服务器A兼具网站（80）、FTP站点（21）与邮件服务器（25、110）的角色，如果计算机A的用户利用浏览器来连接图中网站的话，则计算机A与服务器A之间的互动如下所示（假设浏览器的端口号为2222）：

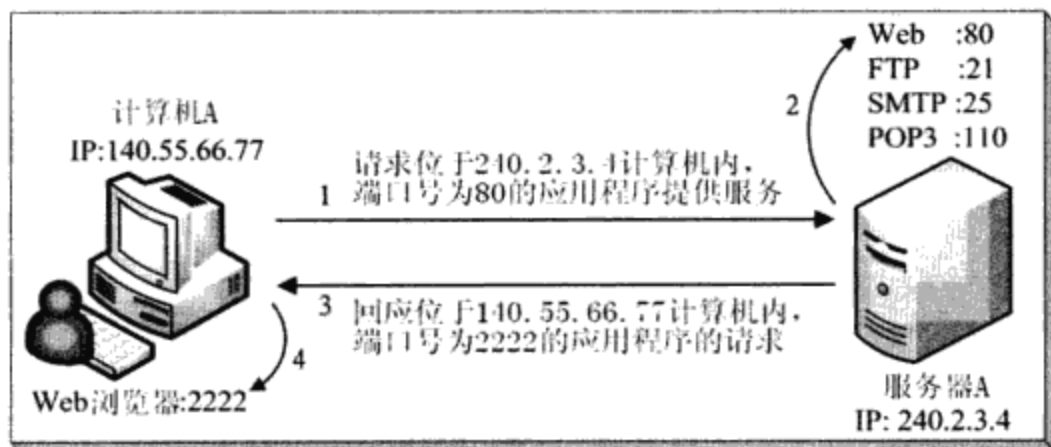


图 12-5

1. 由端口号为2222的浏览器提出浏览网页的请求后，计算机A会将此请求发送给IP地址为240.2.3.4的服务器A，并指定要交给支持端口号为80的应用程序（网站）。
2. 服务器A收到此请求后，会由支持端口号为80的应用程序（网站）来负责处理此请求。
3. 服务器A的网站将网页发送给IP地址为140.55.66.77的计算机A，并指定要交给支持端口号为2222的应用程序（浏览器）。
4. 计算机A收到网页后，会由支持端口号2222的浏览器来负责显示网页内容。

NAT (Network Address Translation) 运作的基本程序，就是执行IP地址与端口号的转换工作。NAT服务器至少要有两个网络接口，其中连接因特网的网络接口需要使用public IP地址，而连接内部网络的网络接口采用private IP地址即可，例如图 12-6中NAT服务器的外网卡与内网卡的IP地址分别是public IP 220.11.22.33与private IP 192.168.8.254。

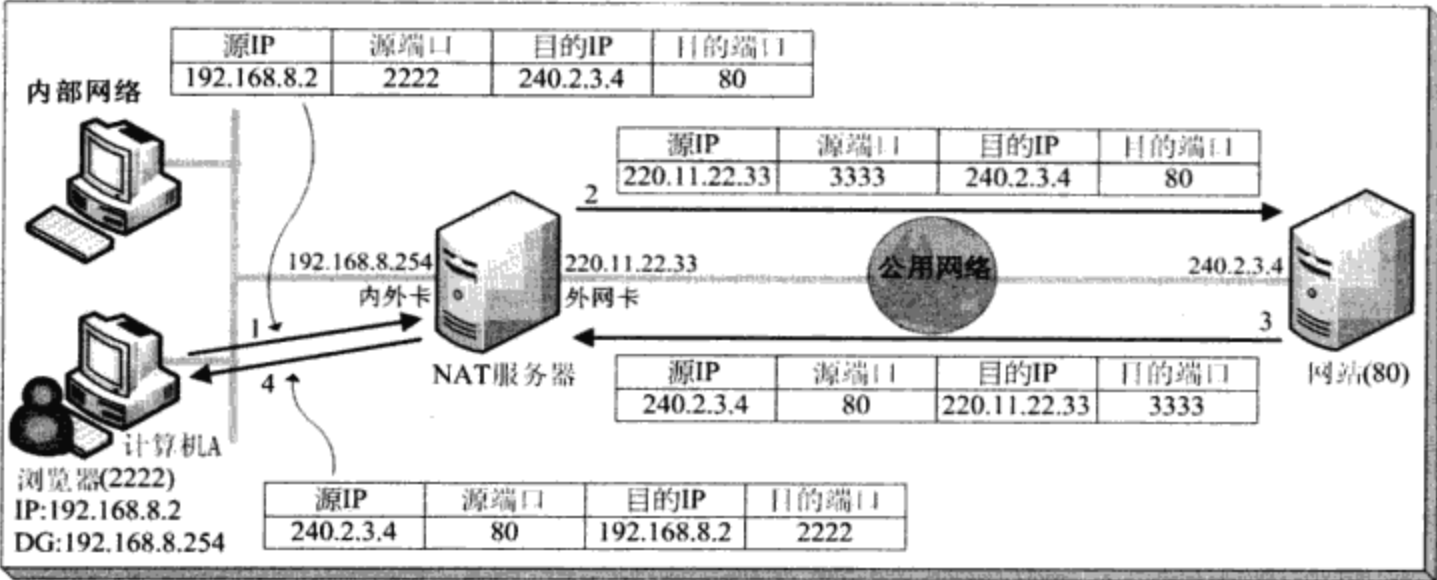


图 12-6

我们以图中内部网络的计算机A的用户要通过NAT服务器连接外部网站为例，来解说NAT的转换运作过程。假设计算机A的浏览器端口号为2222，而网站的端口号为默认的80。

1. 计算机A将上网数据包发送给NAT服务器。此数据包header内的源IP地址为192.168.8.2、端口为2222，目的IP地址为240.2.3.4、端口号为80。

源IP地址	源端口	目的IP地址	目的端口
192.168.8.2	2222	240.2.3.4	80

2. NAT服务器收到数据包后，会将数据包header内的源IP地址与端口号替换成NAT服务器外网卡的IP地址与端口号，IP地址就是public IP 220.11.22.33，而端口号是动态产生的，假设是3333。NAT服务器不会改变此数据包的目的IP地址与端口号。

源IP地址	源端口	目的IP地址	目的端口
220.11.22.33	3333	240.2.3.4	80

同时NAT服务器会建立一个如下所示的对照表，以便之后按照对照表，将从网站得到的网页内容回传给计算机A（此对照表被称为NAT Table）。

源IP地址	源端口	更改后的源IP地址	更改后的源端口
192.168.8.2	2222	220.11.22.33	3333

3. 网站收到浏览网页的数据包后，会根据数据包内的源IP地址与端口号将网页发送给NAT服务器，此网页数据包中的源IP地址为240.2.3.4、端口号为80，目的IP地址为220.11.22.33、端口号为3333。

源IP地址	源端口	目的IP地址	目的端口
240.2.3.4	80	220.11.22.33	3333

4. NAT服务器收到网页数据包后，会根据对照表（NAT Table），将数据包中的目的IP地址更改为192.168.8.2、端口号更改为2222，但是不会更改源IP地址与端口号，然后将网页

数据包发送给计算机A的浏览器来处理。

源IP地址	源端口	目的IP地址	目的端口
240.2.3.4	80	192.168.8.2	2222

NAT服务器通过IP地址与端口的转换，让位于内部网络的计算机只需要使用private IP地址就可以上网。由以上介绍可知，NAT服务器会隐藏内部计算机的IP地址，外界计算机只能够接触到NAT服务器的public IP地址，无法直接与内部使用private IP地址的计算机通信，因此可以增加内部计算机的安全性。

12-2 实例演练——NAT服务器架设

以下将列举两个示例来说明如何设置NAT服务器与客户端计算机。

12-2-1 路由器、固接式xDSL或电缆调制解调器环境的NAT设置

我们以图 12-7的路由器、固接式xDSL或电缆调制解调器为例，来说明如何设置图中的NAT服务器，此服务器为Windows Server 2008 R2计算机。



提示

只要NAT服务器可以上网，则不论NAT服务器的外网卡是连接到路由器或其他NAT设备，您都可以让连接在内网卡的内部网络客户通过这台NAT服务器上网。



图 12-7

图中NAT服务器内安装了2块网卡，一块连接路由器、xDSL调制解调器或电缆调制解调器，一块连接内部网络，其相应的网络连接名称默认是本地连接与本地连接2，建议您将其更改为易于识别的名称，例如在图 12-8中我们分别将其重命名为内网卡与外网卡，重命名的方法为【开始➡对着网络单击右键➡属性➡单击更改适配器设置➡对着所选网络连接单击右键➡重命名】。

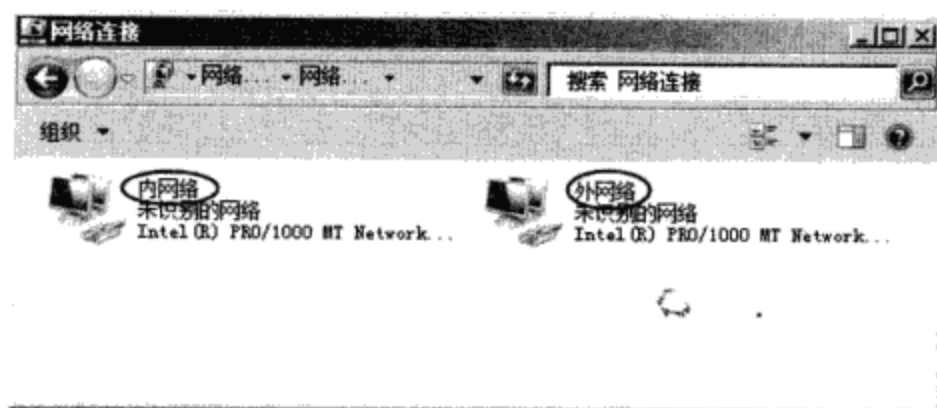




图 12-8

STEP 1 单击左下角服务器管理器图示  角色  单击添加角色。

STEP 2 出现开始之前界面时单击 **下一步**。

STEP 3 在图 12-9 中选择网络策略和访问服务后 **下一步**。

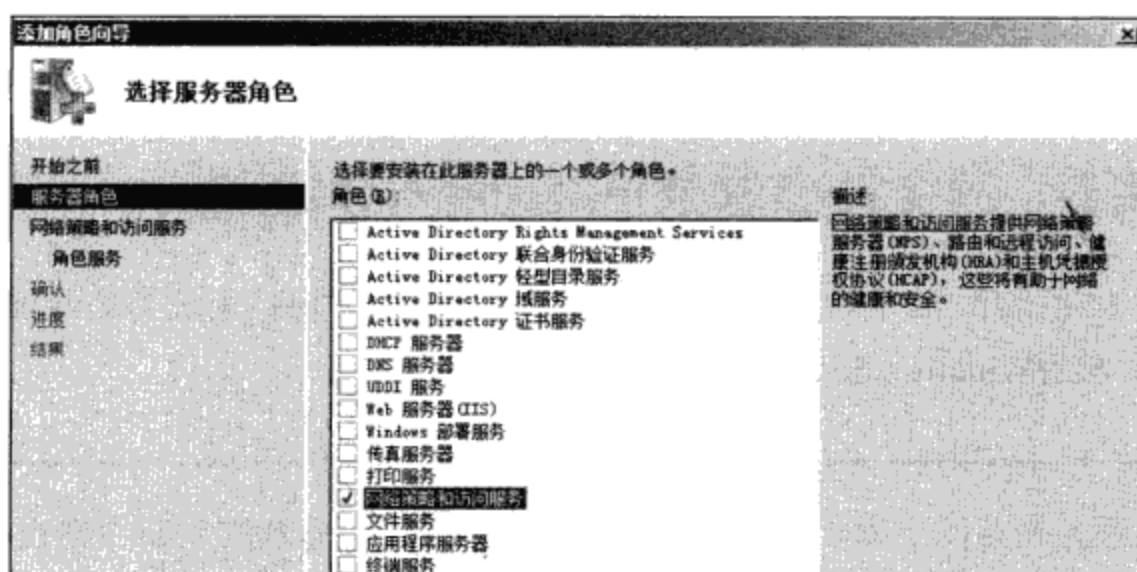


图 12-9

STEP 4 出现网络策略和访问服务界面时单击 **下一步**。

STEP 5 如图 12-10 所示选择路由和远程访问服务后单击 **下一步**。

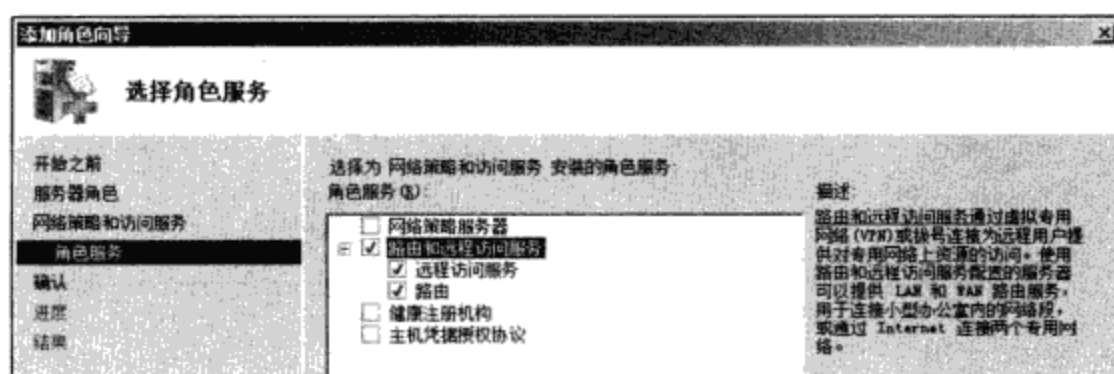


图 12-10

STEP 6 在确认安装选择界面中单击 **安装**，之后单击 **关闭**。

STEP 7 选用【开始  管理工具  路由和远程访问  如图 12-11 所示对着本机计算机单击右键  配置并启用路由和远程访问】。

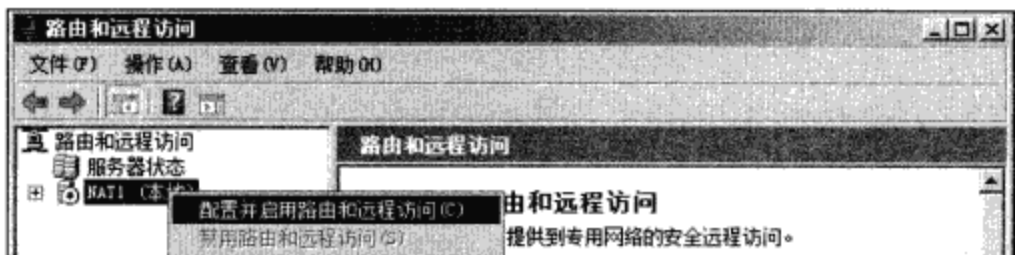


图 12-11

- STEP 8** 在欢迎使用路由和远程访问服务器安装向导界面中单击 **下一步**。
- STEP 9** 如图 12-12 所示 **【选择网络地址转换 (NAT) 后单击 下一步】** 选择用来连接因特网的网络接口 (外网卡)，然后单击 **下一步**。

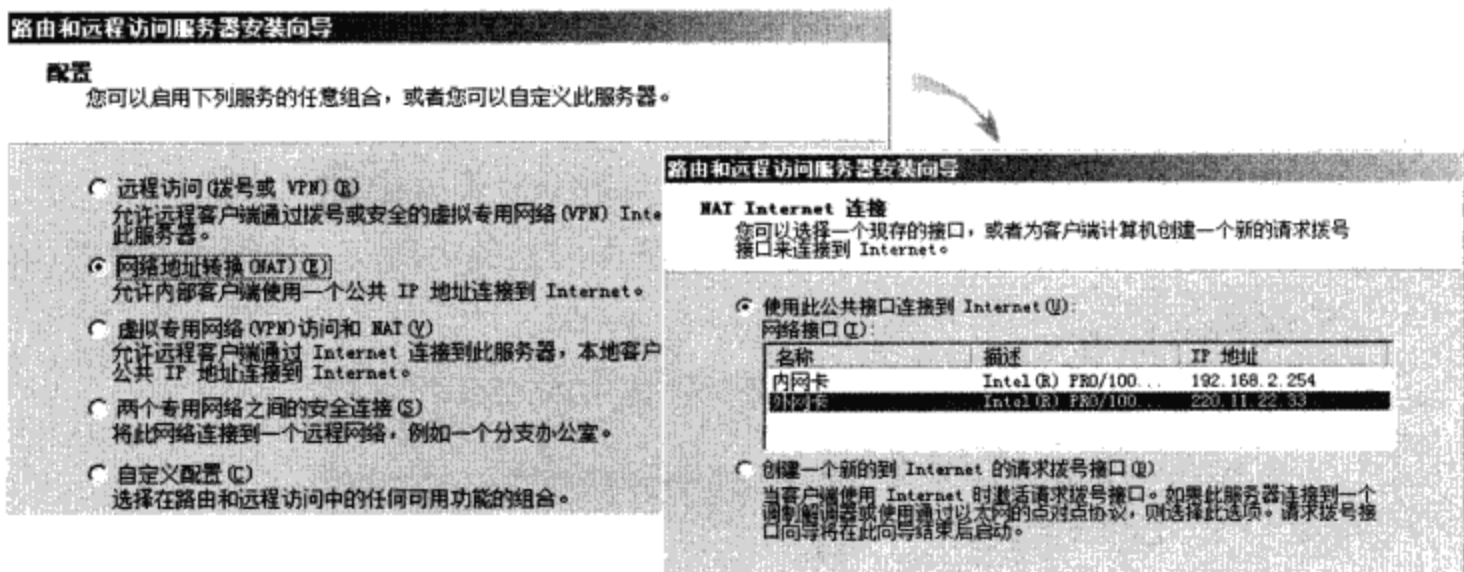


图 12-12



提示

除了连接因特网的公用网络接口外，如果NAT服务器还拥有两个（含）以上专用网接口的话，则系统会要求您从中选择一个可通过NAT服务器来连接因特网的专用网。如果要开放多个专用网可以通过NAT服务器来连接因特网的话，请在完成NAT服务器的架设后再来增加。

- STEP 10** 如果安装向导检测不到网络中有提供DHCP与DNS服务的话，就会出现图 12-13 的界面，此时您可以如图所示选择让这台NAT服务器来提供DHCP与DNS服务，然后单击 **下一步**，内部网络客户的IP地址设置为自动获取即可。

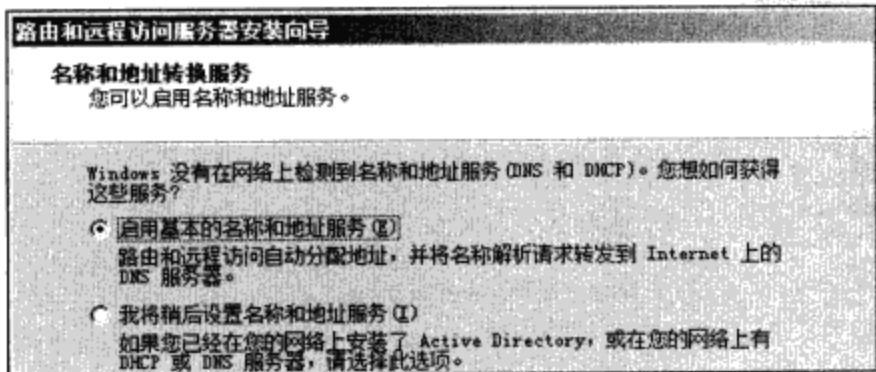


图 12-13

STEP 11 由图 12-14 可看出 NAT 服务器会分配网络标识符为 192.168.8.0 的 IP 地址给内部网络的客户端，它是依据图 12-7 内网卡的 IP 地址（192.168.8.254）来决定此网络标识符，您可以事后修改此设置。

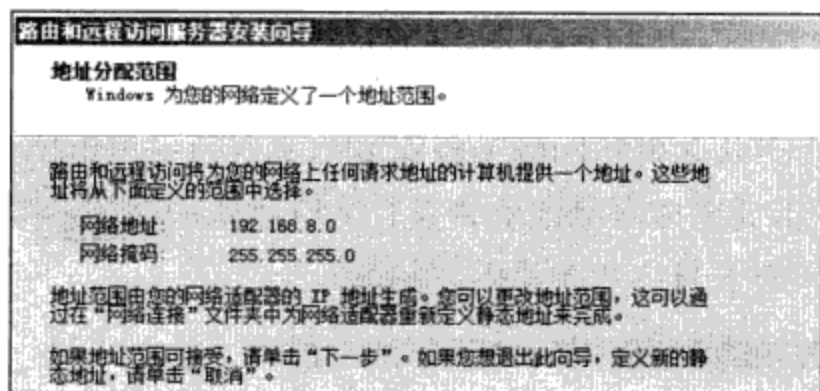


图 12-14

STEP 12 出现完成路由和远程访问服务器安装向导界面时单击 **完成**。

STEP 13 图 12-15 为完成后的界面。您可以双击界面右边的内网卡、外网卡来更改内外网卡的设置。

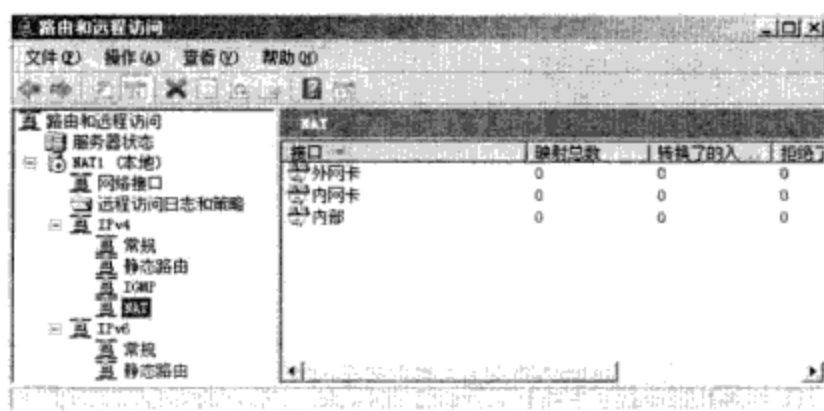


图 12-15

STEP 14 虽然 NAT 服务器具备 DNS 中继代理功能，它可以代替内部客户端来查询 DNS 主机名，不过您需要在 NAT 服务器的 Windows 防火墙来开放 DNS 流量（端口号为 UDP 53），以便允许接受客户端传来的 DNS 查询流量：【开始 高级安全 Windows 防火墙 选择端口后单击 **下一步** 】。



图 12-16

完成以上设置后，如果NAT服务器目前已经连上因特网的话，则当内部网络客户的连接因特网请求（例如上网、收发电子邮件等）被发送到NAT服务器后，NAT服务器就会代替客户端来连接因特网。

12-2-2 非固接式xDSL环境的NAT设置

我们以图 12-17的非固接式xDSL为例，来说明如何设置图中的NAT服务器，此服务器为Windows Server 2008 R2计算机。

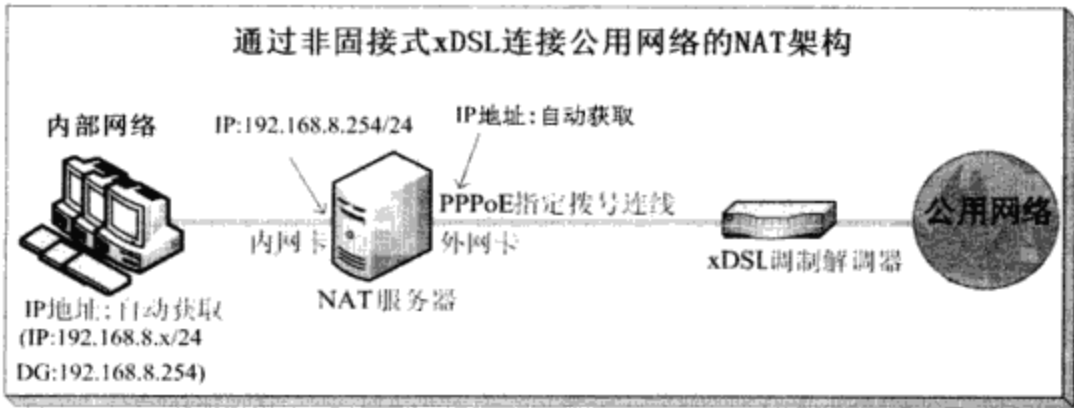


图 12-17

图中NAT服务器内安装了两块网卡，一块连接xDSL调制解调器，一块连接内部网络，其相应的网络连接名称默认是本地连接与本地连接2，建议您将其更改为易于识别的名称，例如在图 12-18中我们分别将其改名为内网卡与外网卡，改名的方法为【开始⌵对着网络单击右键⌵属性⌵单击更改适配器设置⌵对着所选网络连接单击右键⌵重命名】。

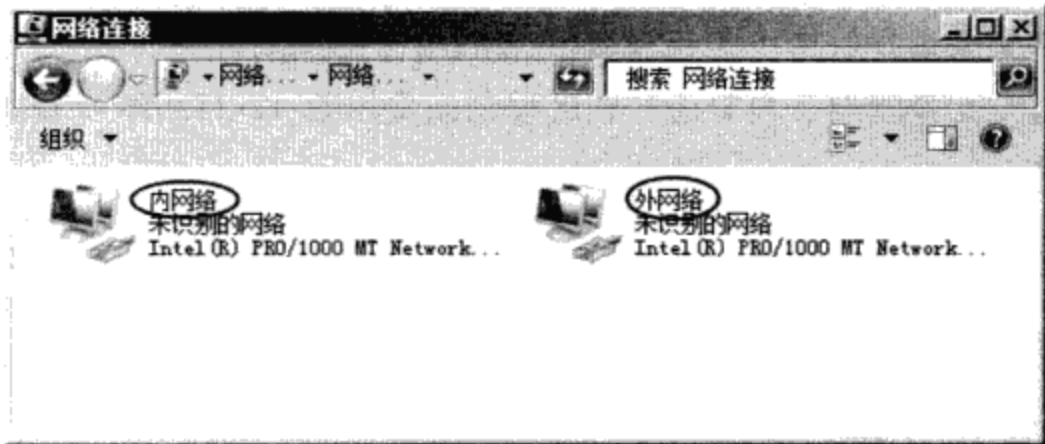


图 12-18

- STEP 1 单击左下角服务器管理器图示⌵角色⌵单击添加角色。
- STEP 2 出现开始之前界面时单击下一步。
- STEP 3 在图 12-19中选择网络策略和访问服务后下一步。

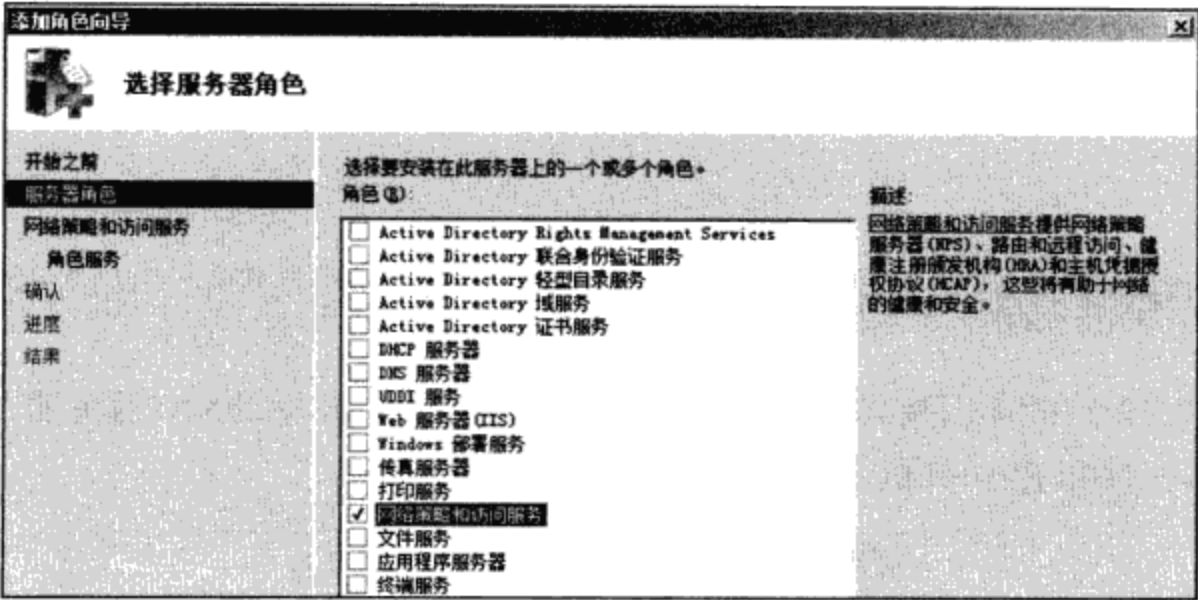


图 12-19

- STEP 4** 出现网络策略和访问服务界面时单击 **下一步**。
- STEP 5** 如图 12-20所示选择路由和远程访问服务后单击 **下一步**。

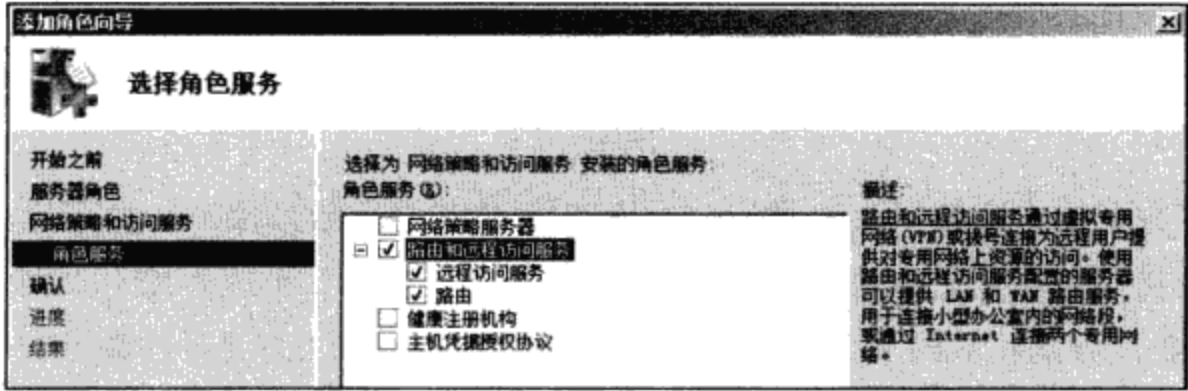


图 12-20

- STEP 6** 在确认安装选择界面中单击 **安装**，之后单击 **关闭**。
- STEP 7** 选用【开始 ➤ 管理工具 ➤ 路由和远程访问 ➤ 如图 12-21所示对本机计算机单击右键 ➤ 配置和启用路由和远程访问】。

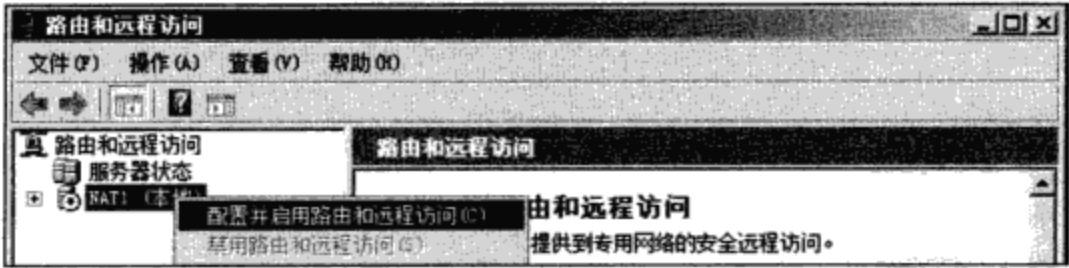


图 12-21

- STEP 8** 在欢迎使用路由和远程访问服务器安装向导界面中单击 **下一步**。
- STEP 9** 如图 12-22所示【选择网络地址转换 (NAT) 后单击 **下一步** ➤ 选择创建一个新的到 Internet 的请求拨号接口后单击 **下一步**】。

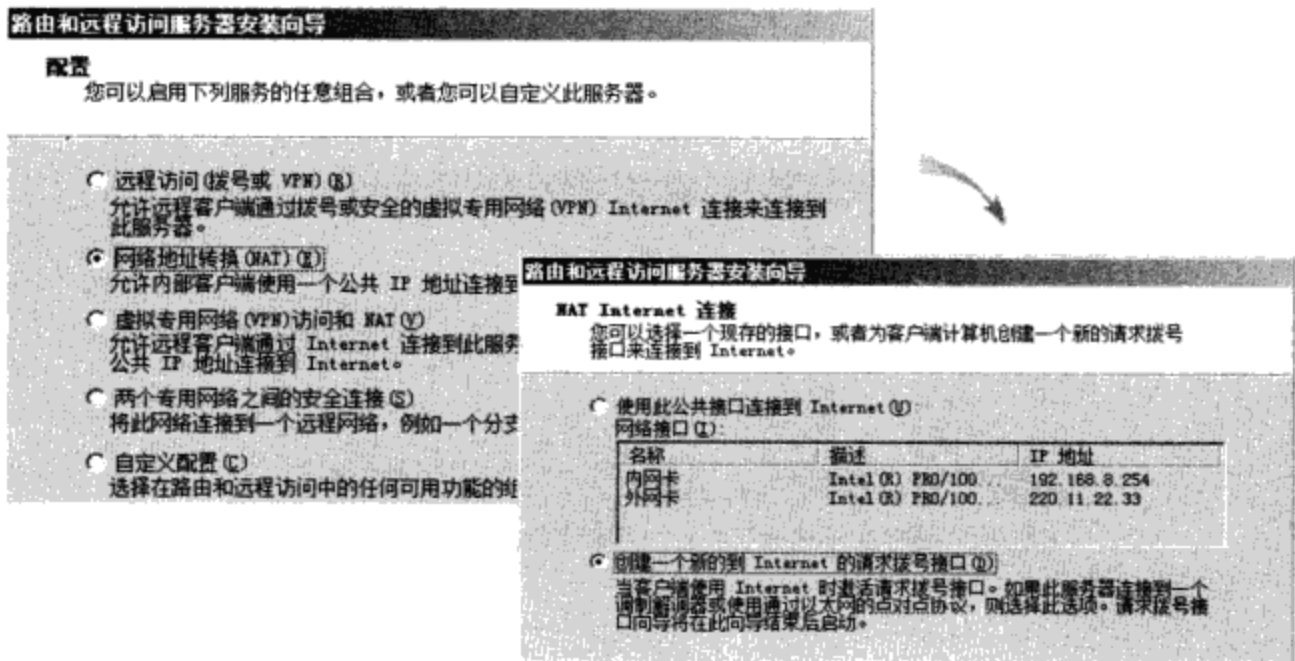


图 12-22

STEP 10 在图 12-23 中选择被允许通过 NAT 服务器来连接因特网的内部网络，例如图中选择连接在 NAT 服务器内网卡的网络。

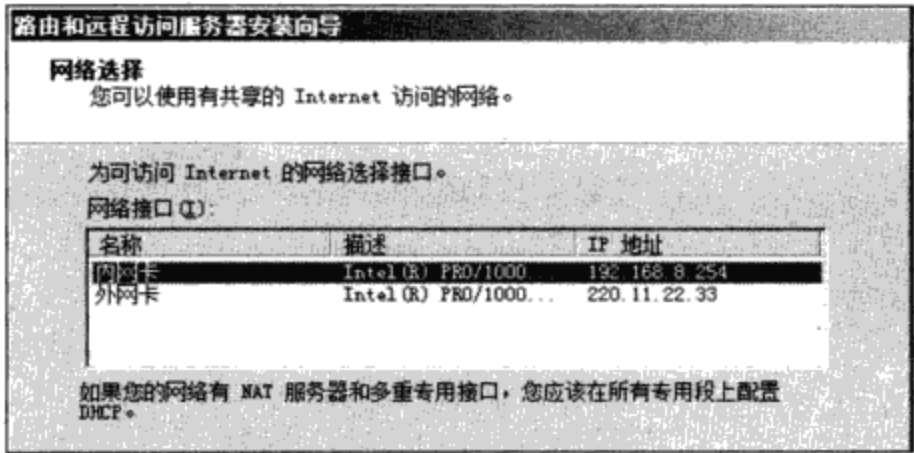


图 12-23

STEP 11 如果安装向导检测不到网络中有提供 DHCP 与 DNS 服务的话，就会出现图 12-24 的界面，此时您可以如图所示选择让这台 NAT 服务器来提供 DHCP 与 DNS 服务之后，单击 **下一步**，因此内部网络客户的 IP 地址设置为自动获得即可。

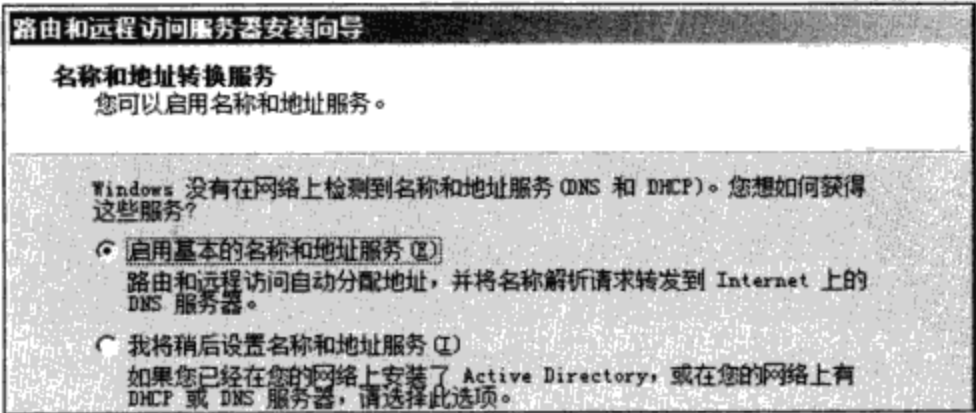


图 12-24

STEP 12 由图 12-25 可看出 NAT 服务器会分配网络标识符 192.168.8.0 的 IP 地址给内部网络的

客户端，它是依据图 12-17 内网卡的 IP 地址（192.168.8.254）来决定此网络标识符，您可以事后修改此设置。

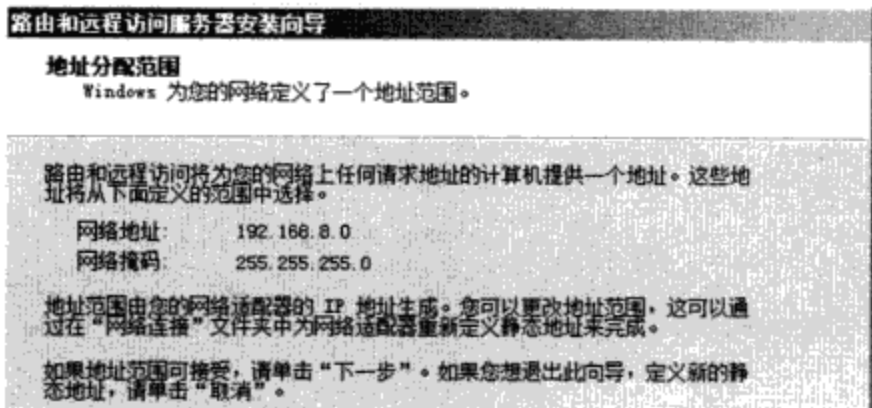


图 12-25

STEP 13 出现准备应用选择界面时单击 **下一步**。

STEP 14 出现欢迎使用请求拨号接口向导界面时单击 **下一步**，

STEP 15 在图 12-26 中为此连接设置名称，例如 **PPPoE 请求拨号**，然后选择利用 PPPoE 协议来连接因特网。

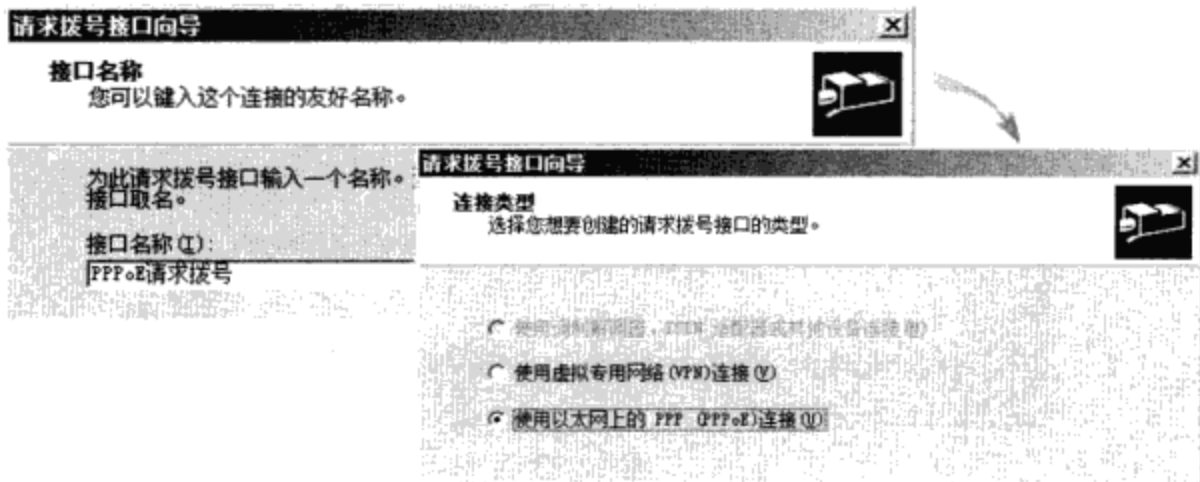


图 12-26

STEP 16 在图 12-27 中单击 **下一步**。服务名称保留空白或按照 ISP（因特网服务提供供应商）指示来设置，请勿随意设置，否则可能无法连接。

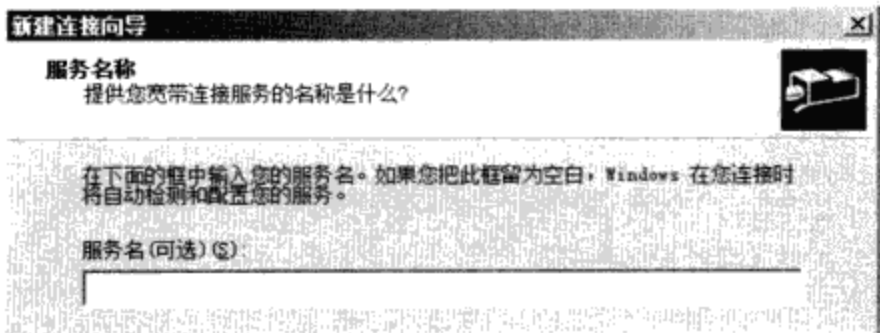


图 12-27

STEP 17 如果 ISP 没有支持密码加密功能的话，请在图 12-28 中增加选择 **如果这是唯一连接的方式的话**，请发送纯文本密码后单击 **下一步**。

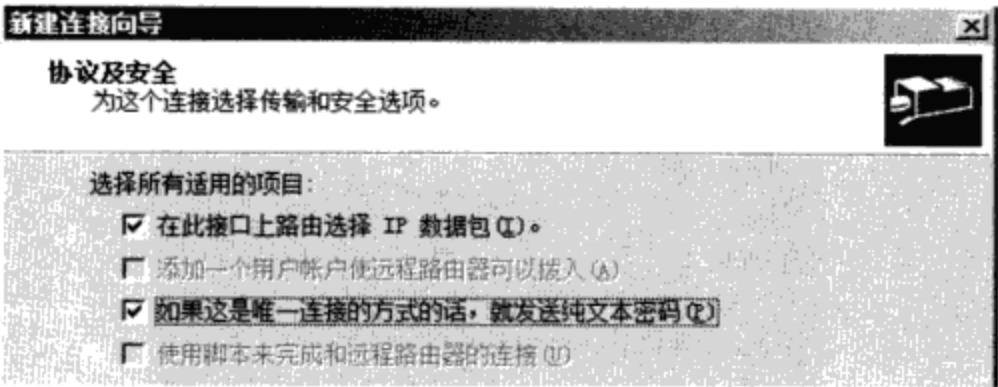


图 12-28

STEP 18 在图 12-29中输入用来连接到ISP的用户名与密码后单击**下一步**。

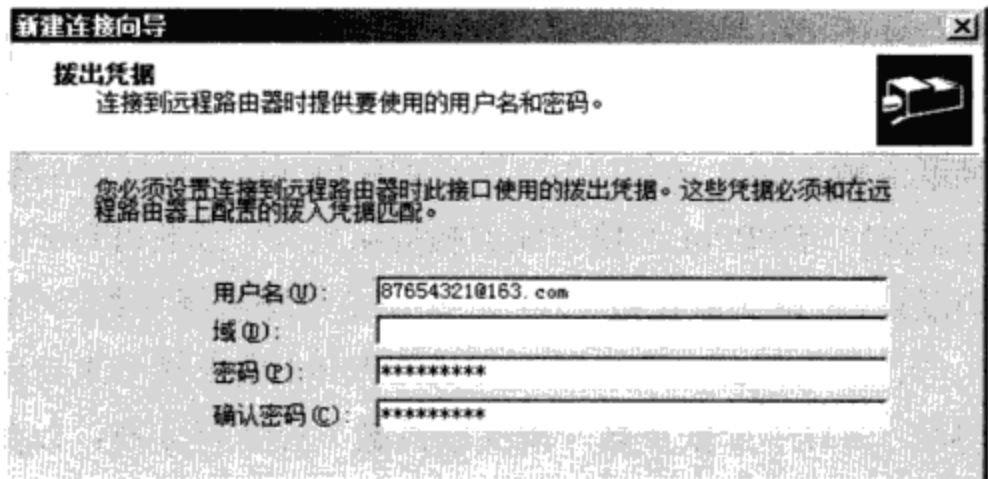


图 12-29

STEP 19 出现完成请求拨号接口向导界面时单击**完成**。

STEP 20 出现完成路由和远程访问服务器安装向导界面时单击**完成**。

STEP 21 如图 12-30所示【展开到IPv4➤对着静态路由单击右键➤新建静态路由】。

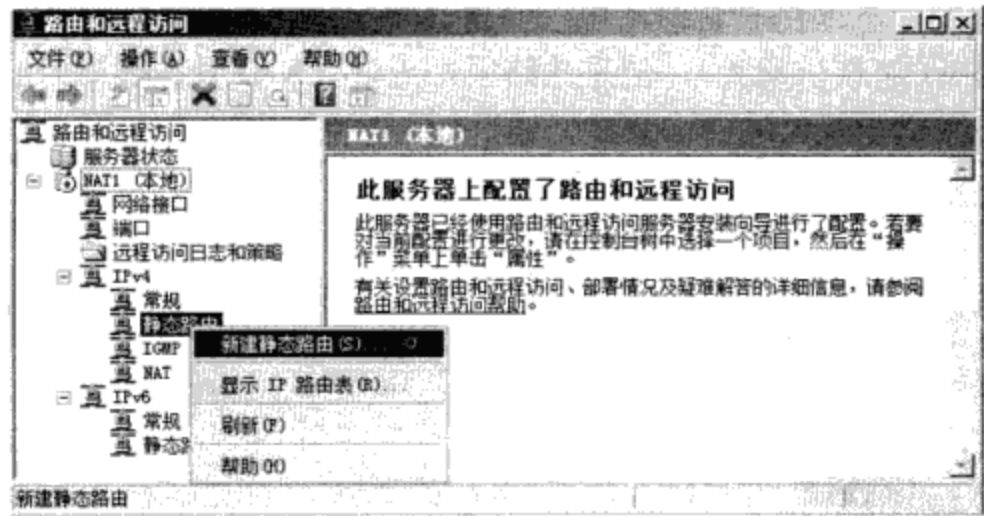


图 12-30

STEP 22 如图 12-31所示为NAT服务器新建一个默认网关（目标与默认网关为0.0.0.0），以便让NAT服务器要连接因特网时，可以通过PPPoE请求拨号接口来连接ISP与因特网。

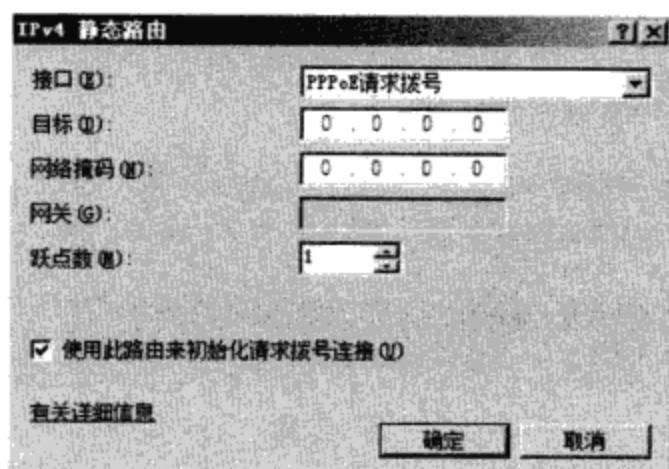


图 12-31

我们在第11章中说过若有多个路径可供选择的话，则系统会挑选**路径跃点数**较低的路径。若NAT服务器的网络适配器指定有**默认网关**的话，以1 Gbps网络来说，其默认的路径跃点数为266，在图 12-31中我们将PPPoE请求拨号的**跃点数**（它是**网关跃点数**）设置为1、而PPPoE的**接口跃点数**默认为50，故此PPPoE请求拨号的路径跃点数为**接口跃点数+网关跃点数=51**，它比网卡的路径跃点数266低，故当NAT服务器接收到内部计算机的上网要求时，会挑选PPPoE请求拨号来自动连接因特网。请不要将图 12-31中的**跃点数（网关跃点数）**设置得太高，以免此PPPoE请求拨号的路径跃点数超过网卡的路径跃点数，造成NAT服务器不通过PPPoE请求拨号而自动连接因特网的后果。

STEP 23 图 12-32为完成后的界面。

**注意**

虽然从图右边的静态路由表看似系统已经自动针对PPPoE请求拨号新建了路径（目标处为::，看似为IPv6的默认网关），但是该路径却无法让NAT服务器与内部网络的计算机连接因特网，故我们需要另外自行新建上述目标为0.0.0.0的路径。

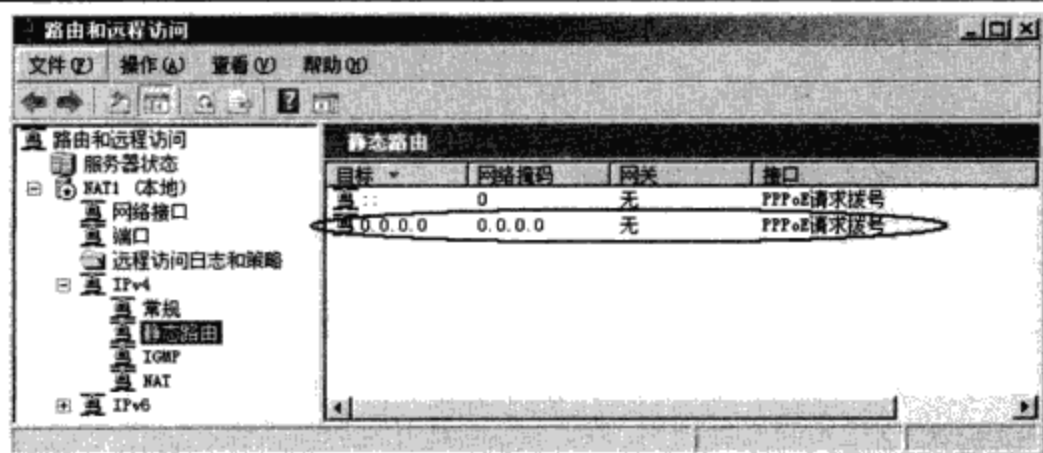


图 12-32

STEP 24 虽然NAT服务器具备DNS中继代理功能，它可以代替内部客户端来查询DNS主机名，不过您需要在NAT服务器的Windows防火墙来开放DNS流量（端口号为UDP 53），以便允许接受客户端传来的DNS查询流量：【开始 ➤ 管理工具 ➤ 高级安全

Windows防火墙➡单击入站规则右方的新建规则…➡选择端口后单击**下一步**➡如图 12-33所示将端口号设置为UDP 53➡…】。

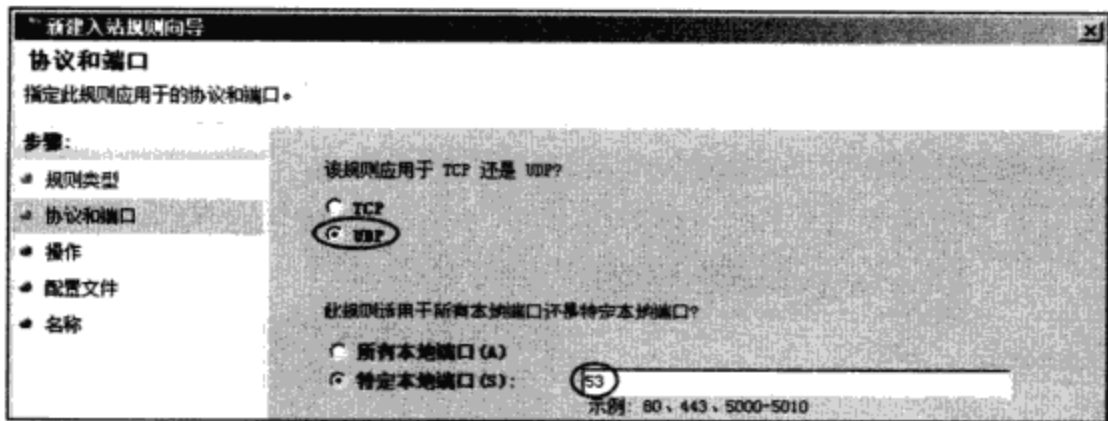


图 12-33

完成设置后，当内部客户端用户的连接因特网请求（例如上网、收发电子邮件等）被发送到NAT服务器后，NAT服务器就会自动通过PPPoE请求拨号来连接ISP与因特网。

12-2-3 内部网络包含多个子网

如果内部网络包含多个子网区段的话，则请确认各个子网的上网请求会被发送到NAT服务器，例如图 12-34中内部网络包含子网1、子网2与子网3，则请确认当路由器2收到子网3来的上网请求时，它会将此请求发送给路由器1（必要时可能需在路由表内手动新建路径），再由路由器1发送给NAT服务器，否则子网3内的计算机无法通过NAT服务器上网。

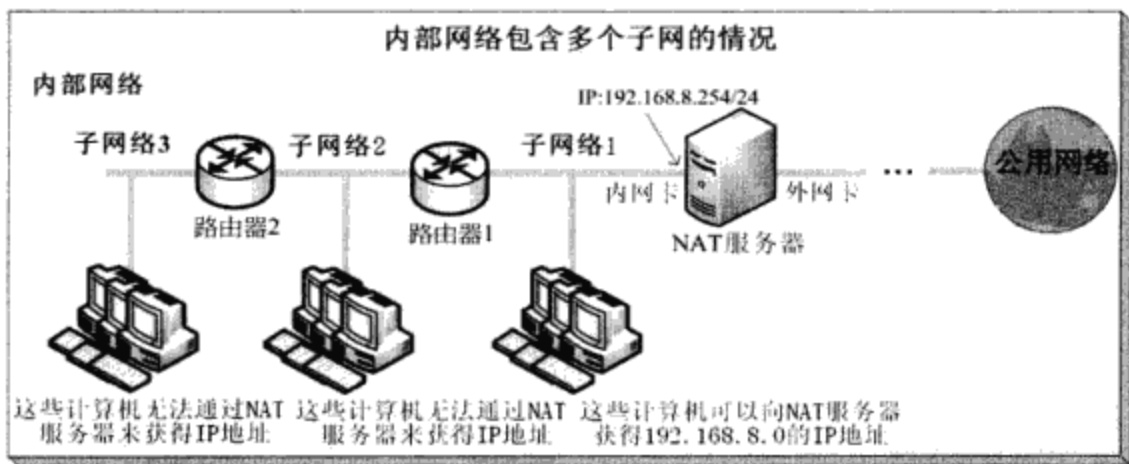


图 12-34

还有因为NAT服务器只会分配IP地址给一个网段，例如图 12-34它只会分配192.168.8.0的IP地址给子网1内的计算机，无法分配IP地址给子网2与子网3内的计算机，因此这两个子网内的计算机，其IP地址需手动设置或另外通过其他DHCP服务器来分配。

12-2-4 新增NAT网络接口

如果NAT服务器拥有多个网络接口（例如多块网卡），这些网络接口分别连接到不同的网

络，其中连接因特网的接口被称为**公用接口**，而连接内部网络的接口被称为**专用接口**。系统默认仅开放一个内部网络的计算机可以通过NAT服务器来连接因特网，若要开放其他内部网络的话，请通过【如图 12-35所示展开到IPv4对着NAT单击右键新增接口选择连接该网络的专用接口（假设是内网卡2）选择专用接口连接到专用网络…】的方法。

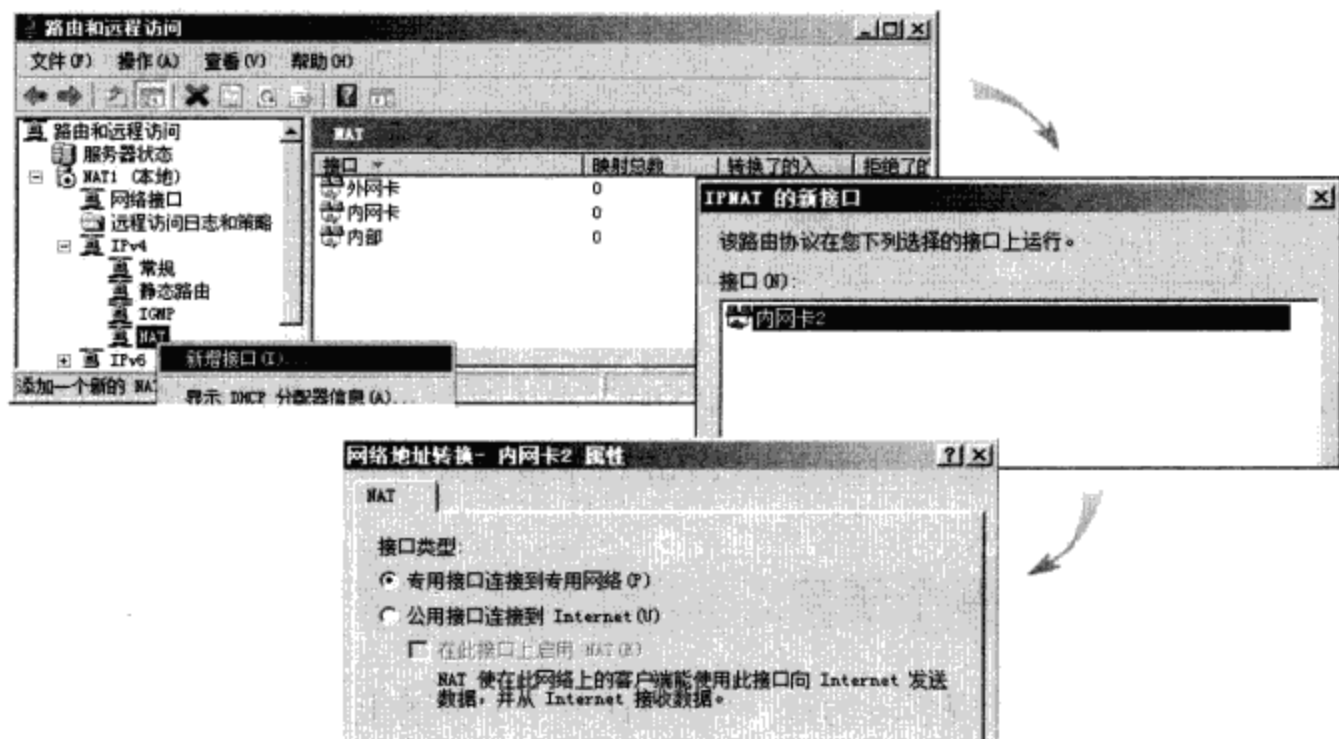


图 12-35

若NAT服务器有多个**专用网接口**的话，例如图 12-36的内部网络有3个**专用网接口**，由于NAT服务器只会分配IP地址给其中一个网络，因此只有一个网络内的计算机可以向NAT服务器自动索取IP地址，其他网络内的计算机的IP地址需手动设置或另外通过其他DHCP服务器来分配。

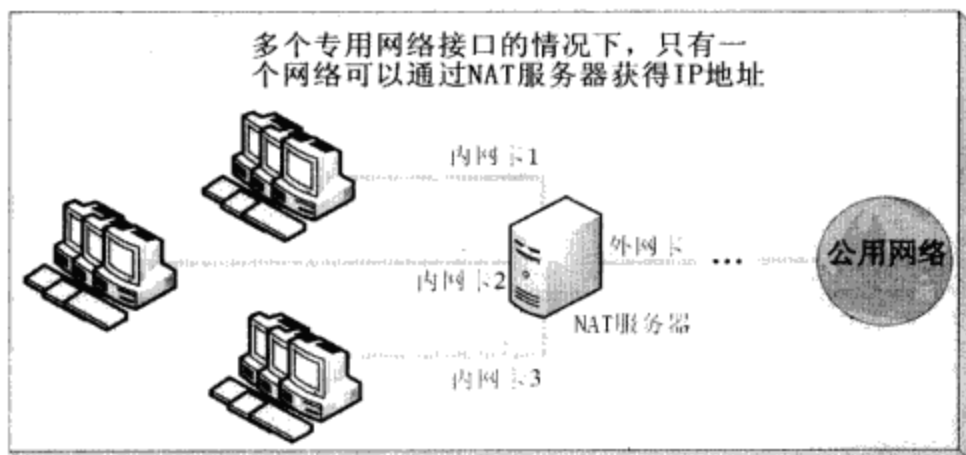


图 12-36

12-2-5 内部网络的客户端设置

内部网络客户（参见前面图 12-17）的IP地址设置必须正确，才能够通过NAT服务器来连接因特网，以Windows 7为例，其设置方法为【开始控制面网络和网络和Internet网络和网络和共享

中心 单击本地连接 单击属性 单击Internet协议版本4(TCP/IPv4) 单击属性 然后选择

自动获得IP地址: 如图 12-37所示, 此时客户端会自动向NAT服务器或其他DHCP服务器来索取IP地址、默认网关与DNS服务器等设置。若是向NAT服务器索取IP地址的话, 由于NAT服务器只会发放与内网卡相同网络标识符的IP地址, 故这些客户端需位于此网卡所连接的网络内。

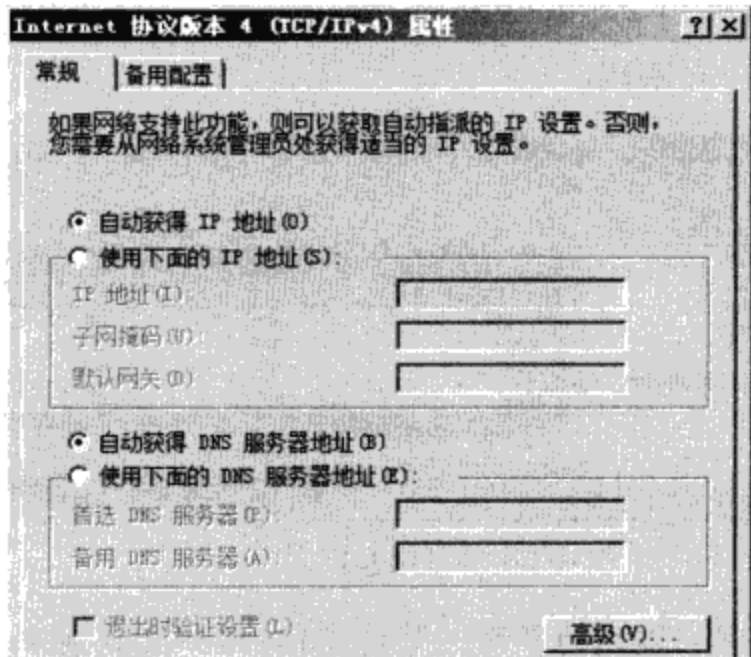


图 12-37

使用下列的IP地址: 如图 12-38所示, 图中客户端IP地址的网络标识符与NAT服务器内网卡的IP地址相同、默认网关为NAT服务器内网卡的IP地址、首选DNS服务器可以被指定到NAT服务器内网卡的IP地址（因它具备DNS中继代理功能）或其他正常运行的DNS服务器的IP地址。

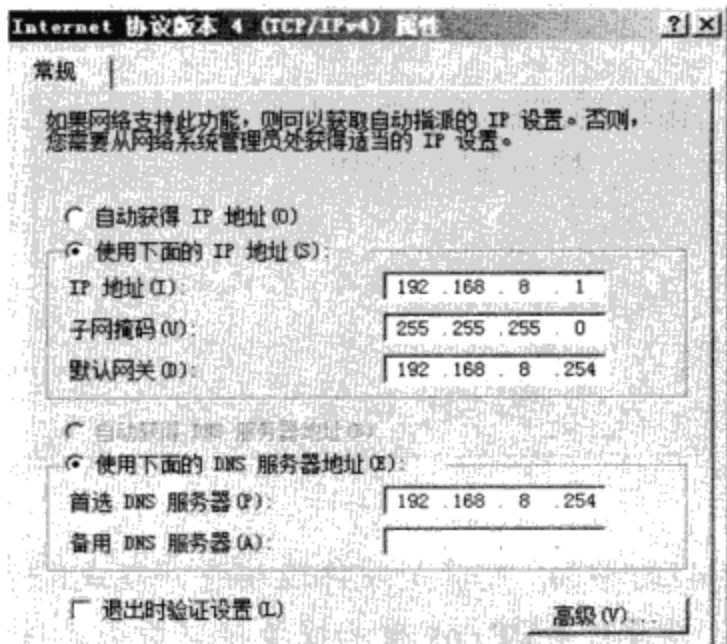





图 12-38

如果内部网络包含多个子网或NAT服务器拥有多个专用网接口的话, 由于NAT服务器只会分配IP地址给一个网段, 因此其他网络内的计算机的IP地址需手动设置或另外通过其他DHCP

服务器来分配。

12-2-6 连接错误排除

如果PPPoE请求拨号无法成功连接ISP的话，请利用手动拨号的方式来查找可能的原因：
【如图 12-39所示单击网络接口对着PPPoE请求拨号接口单击右键连接】。您也可以通过图中设置认证选项来更改账户与密码。

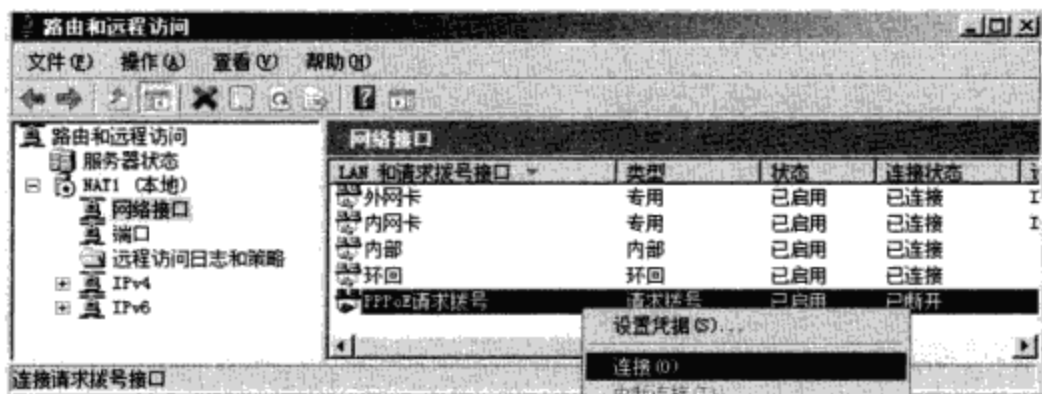




图 12-39

- 若连接时出现类似图 12-40的界面：可能是ISP端不支持密码加密功能，此时请【对着PPPoE请求拨号接口单击右键属性如图 12-41所示选择允许没有加密的密码】。

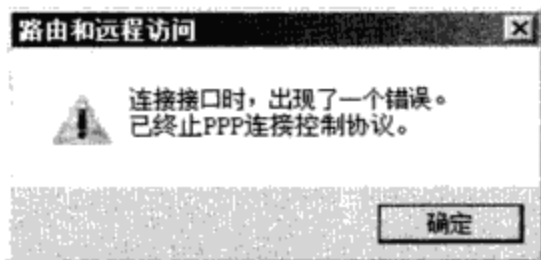


图 12-40

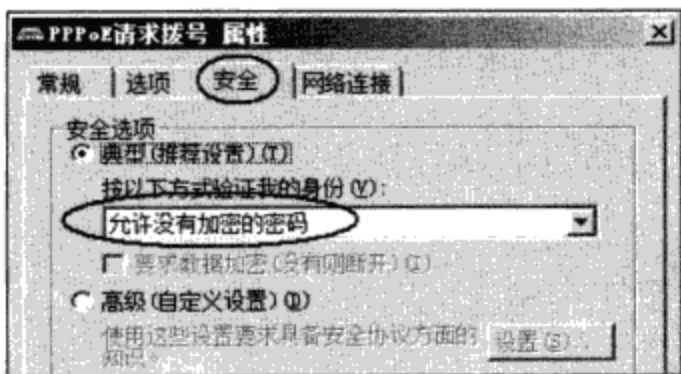




图 12-41

- 若连接时出现图 12-42的界面：可能是硬件连接有问题或PPPoE请求拨号的服务名称有误，若为后者的话，请【对着PPPoE请求拨号接口单击右键属性在图 12-43中将服务名称清除或按ISP的提示来输入】。

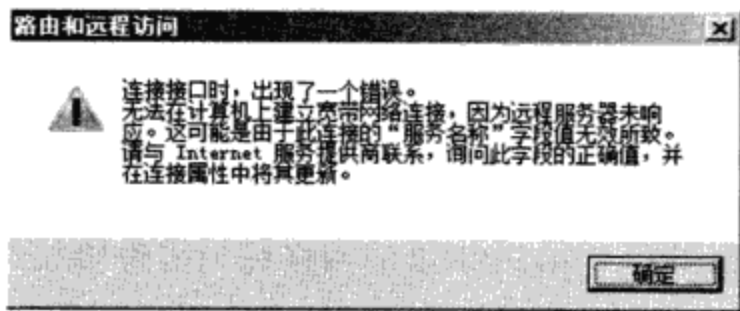


图 12-42

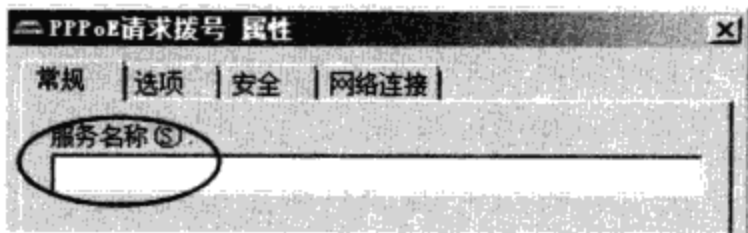


图 12-43

- PPPoE 请求拨号连接 ISP 成功，但是 NAT 服务器与客户端却无法连接因特网：请检查前面的图 12-32 中是否有另外新建正确的静态路由。

12-3 DHCP 分配器与 DNS 中继代理

Windows Server 2008 R2 NAT 服务器还具备着以下的两个功能：

- **DHCP 分配器**：用来分配 IP 地址给内部网络的客户端计算机。
- **DNS 中继代理**：可代替内部计算机向 DNS 服务器查询 DNS 主机的 IP 地址。

12-3-1 DHCP 分配器

DHCP 分配器 (DHCP Allocator) 扮演着类似 DHCP 服务器的角色，用来分配 IP 地址给内部网络的客户端。要查看或更改 DHCP 分配器设置的话，请【如图 12-44 所示展开到 IPv4 单击 NAT 单击上方的属性图示 单击前图中的地址分配标签】。

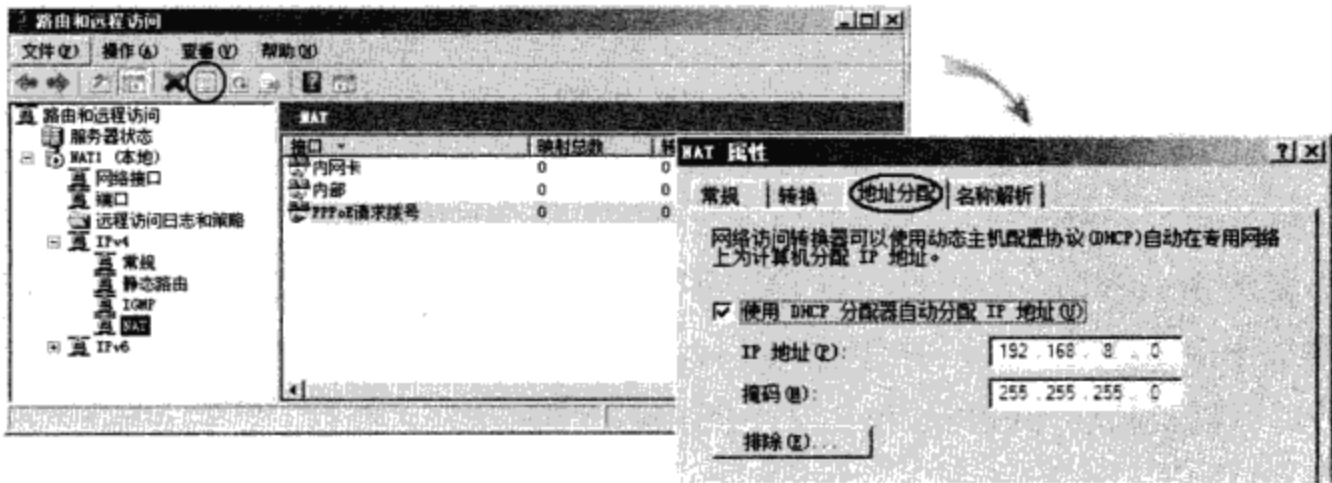


图 12-44



提示

在架设NAT服务器时，如果系统检测到内部网络上有DHCP服务器的话，它就不会自动启动DHCP分配器。

图中DHCP分配器分配给客户端的IP地址的网络标识符为192.168.8.0，这个默认值是根据NAT服务器内网卡的IP地址（192.168.8.254）来产生的。您可以自行修改这个默认值，不过必须与NAT服务器内网卡IP地址一致，也就是网络标识符需相同。

若内部网络内某些计算机的IP地址是自行输入的，且这些IP地址是位于上述IP地址范围内的话，则请通过界面中的**排除**来将这些IP地址排除，以免这些IP地址被发放给其他客户端计算机。

若内部网络包含多个子网或NAT服务器拥有多个专用网接口的话，由于NAT服务器的DHCP分配器只能够分配一个网段的IP地址，因此其他网络内的计算机的IP地址需手动设置或另外通过其他DHCP服务器来分配。

12-3-2 DNS中继代理

当内部计算机需要连接网站、FTP站点或电子邮件服务器等时，它们可以将查询这些服务器IP地址的请求发到NAT服务器，然后由NAT服务器的**DNS中继代理**（DNS proxy）来替它们查询这些服务器的IP地址。

您可以通过图 12-45 中**名称解析**标签来启动或更改DNS中继代理的设置，选择**使用域名系统(DNS)的客户端**，即表示要启用DNS中继代理的功能，以后只要客户端要上网、发送电子邮件等，NAT服务器都可以代替这些客户端来向DNS服务器查询网站、邮件服务器等主机的IP地址（这些主机可能位于因特网或内部网络）。

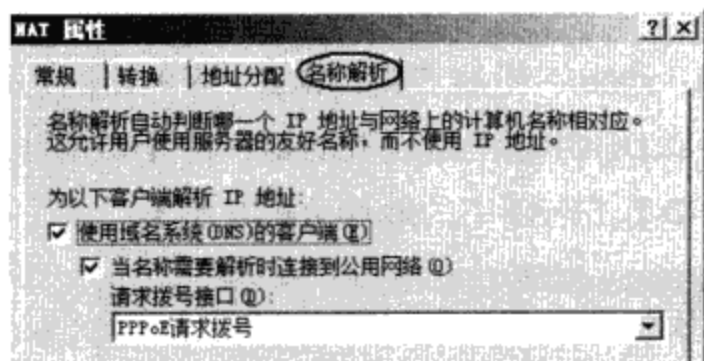


图 12-45

NAT服务器会向哪一台DNS服务器来查询呢？它会向TCP/IP设置处的**首选DNS服务器**或**备用DNS服务器**来查询。如果这台DNS服务器是位于因特网，而且NAT服务器是通过**PPPoE请求拨号**来连接因特网的话，则请选择图 12-45 中**当名称需要解析时连接到公用网络**，以便让NAT服务器可以自动利用PPPoE请求拨号来连接因特网。

12-4 开放因特网用户来连接内部服务器

NAT服务器让内部用户可以连接因特网，不过因为内部计算机使用private IP地址，这种IP地址不可以暴露在因特网上，外部用户只能够接触到NAT服务器的外网卡的public IP地址，因此若要让外部用户来连接内部服务器的话（例如内部网站、SMTP服务器等），就需要通过NAT服务器来转发。

12-4-1 端口映射

通过TCP/UDP端口映射功能（port mapping），可以让因特网用户来连接内部使用private IP的服务器。以图 12-46为例来说，内部网站的IP地址为192.168.8.1、端口号为默认的80，SMTP服务器的IP地址为192.168.8.2、端口号为默认的25。若要让外部用户可以访问此网站与SMTP服务器的话，请对外宣称网站与SMTP服务器的IP地址是NAT服务器的外网卡的IP地址220.11.22.33，也就是将此IP地址注册到DNS服务器内：

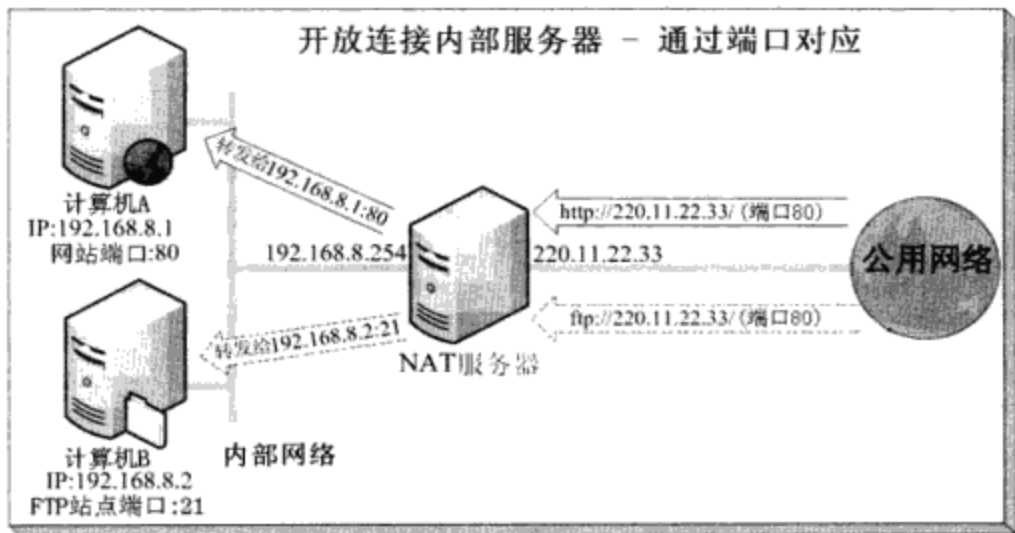


图 12-46

- 当因特网用户通过类似http://220.11.22.33/路径来连接网站时，NAT服务器会将此请求转发到内部计算机A的网站、网站将所需网页发送给NAT服务器、再由NAT服务器将其发送给因特网用户。
- 当因特网用户通过IP地址 220.11.22.33来连接SMTP服务器时，NAT服务器会将此请求转发到内部计算机B的SMTP服务器。

以图 12-46为例，要将从因特网来的上网请求转发到内部计算机A，设置方法为【如图 12-47所示展开到IPv4☞单击NAT☞对着外网卡单击右键☞属性】。

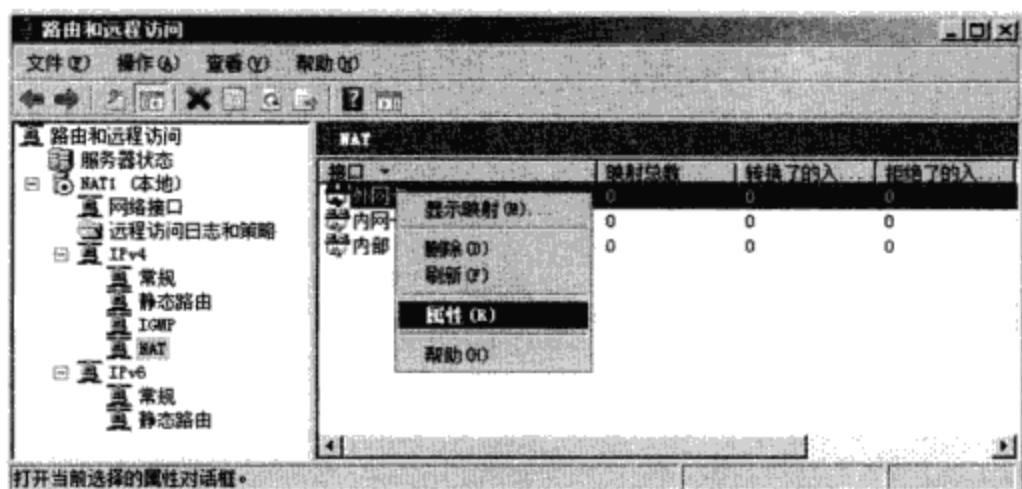


图 12-47

然后【在图 12-48 中单击服务和端口标签选择 Web 服务器 (HTTP) 在前图的专用地址处输入内部网站的 IP 地址 192.168.8.1...】，图中公用地址 (public address) 处默认为在此接口上，它代表 NAT 服务器外网卡的 IP 地址，以图 12-46 为例，就是 220.11.22.33。图中完整的意思为：从因特网发送给 IP 地址 220.11.22.33 (公用地址)、端口号 80 (传入端口) 的 TCP 数据包 (协议)，NAT 服务器会将其转发给 IP 地址为 192.168.8.1 (专用地址)、端口号为 80 (传出端口) 的应用程序来负责。

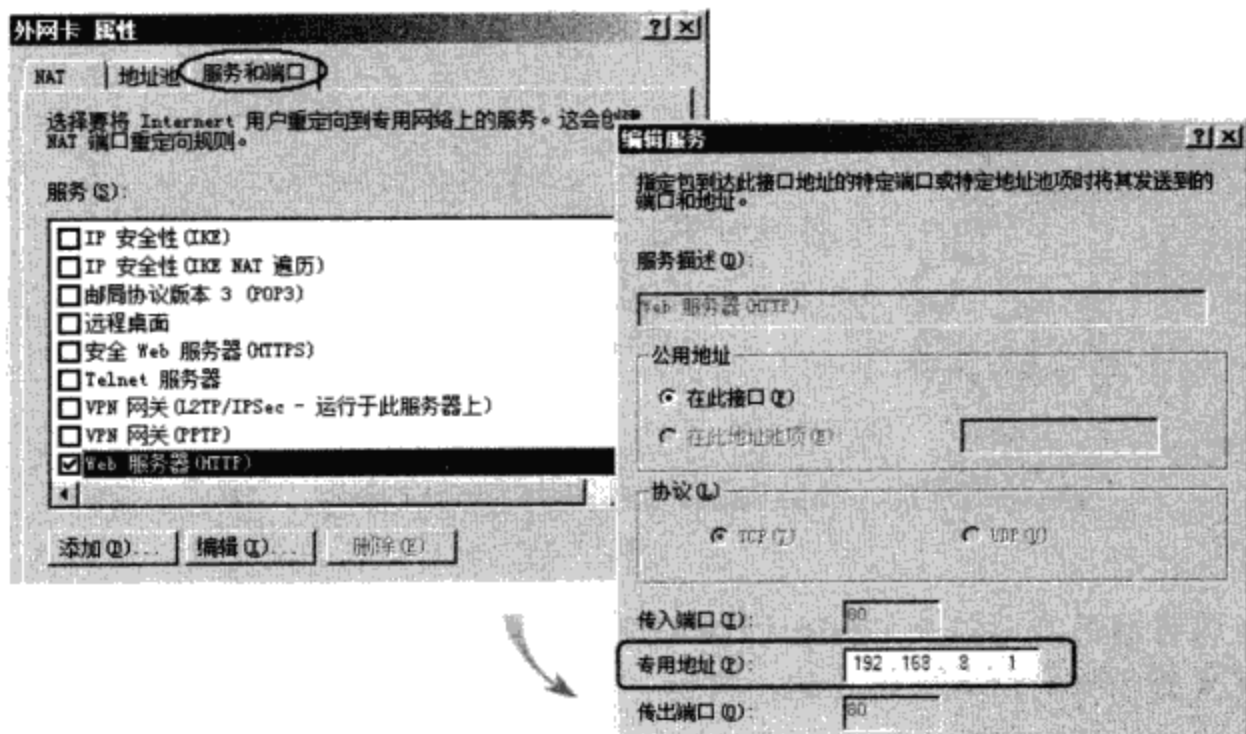


图 12-48

**注意**

您无法更改图中默认服务的标准输入与输出端口号，若您的输入或输出端口非标准号码的话，请通过后图添加来自行新建新服务。

如果 NAT 服务器的外网卡拥有多个 public IP 地址的话，则您还可以从在此地址池项来选择其他的 public IP 地址（后述）。

12-4-2 地址映射

前一小节的端口映射功能，可以让从因特网送到NAT服务器外网卡（IP地址220.11.22.33）的不同类型的请求转交给不同的计算机来处理，例如将HTTP请求转给计算机A、将SMTP请求转给计算机B。

如果NAT服务器外网卡拥有多个IP地址的话，则您可以利用**地址映射**（address mapping）方式来保留特定IP地址给内部特定的计算机，例如图 12-49中NAT服务器外网卡拥有两个public IP地址（220.11.22.33与220.11.22.34），此时我们可以将第1个IP地址220.11.22.33保留给计算机A、将第2个IP地址220.11.22.34保留给计算机B，因此所有送到第1个IP地址220.11.22.33的流量都会转给计算机A、所有送到第2个IP地址220.11.22.34的流量都会转发给计算机B。

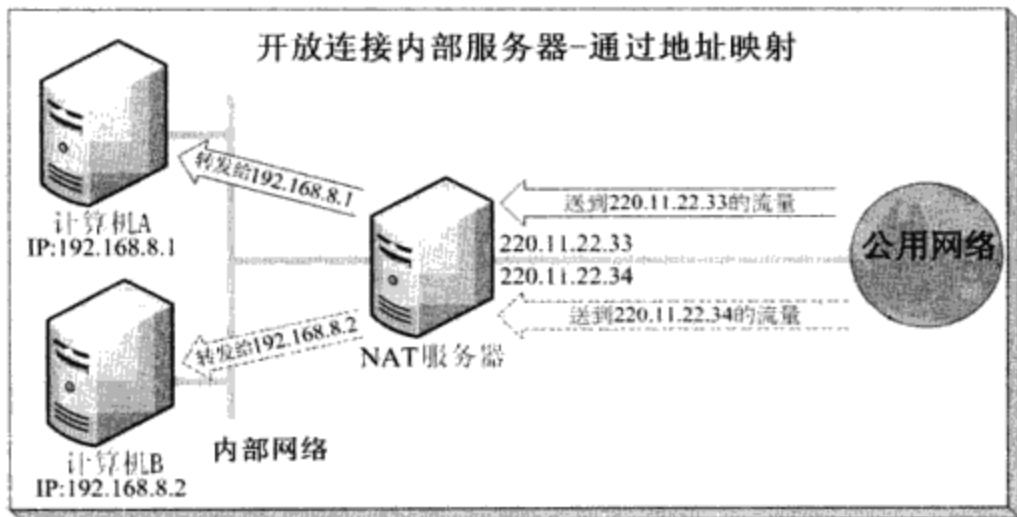


图 12-49

同时所有从计算机A发出的外送流量会通过第1个IP地址220.11.22.33发出、从计算机B发出的外送流量会通过第2个IP地址220.11.22.34发出。

地址池的设置

NAT服务器需要多个public IP地址，才可以享有地址映射的功能。假设NAT服务器外网卡除了原有的IP地址220.11.22.33之外，还需要另外一个IP地址220.11.22.34。请完成以下两项工作：

- 请在外网卡的TCP/IP设置处添加两个IP地址【开始☞对着网络单击右键☞属性☞单击更改适配器设置☞对着代表外网卡的连接单击右键☞属性☞单击Internet协议版本4(TCP/IPv4)☞单击属性☞单击高级☞单击IP地址处的添加☞...】，如图 12-50所示为完成后的界面。

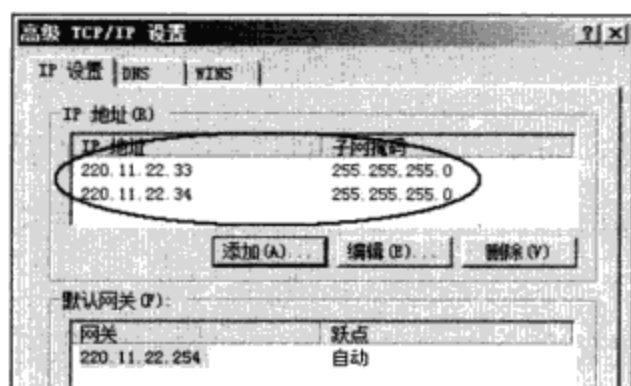


图 12-50

- **添加地址池:**【打开路由和远程访问控制台☞展开到IPv4☞单击NAT☞对着外网卡单击右键☞属性☞如图 12-51所示单击地址池标签下的**添加**☞输入NAT服务器外网卡的IP地址范围与子网掩码☞...】。

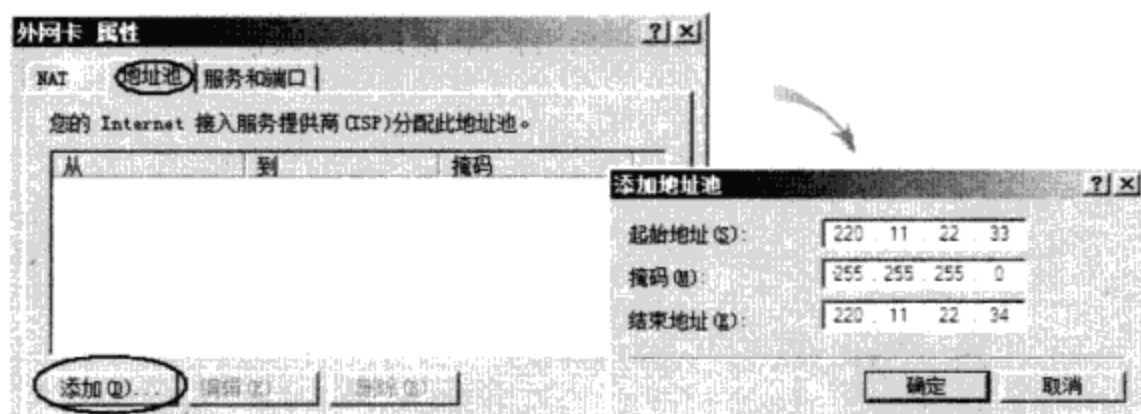


图 12-51

地址映射的设置

请单击前面图 12-51中后图右下方的**保留**，然后如图 12-52所示来设置，图中我们将地址池中的public IP地址220.11.22.33保留给内部使用private IP地址 192.168.8.1的计算机A（参考前面图 12-49）。

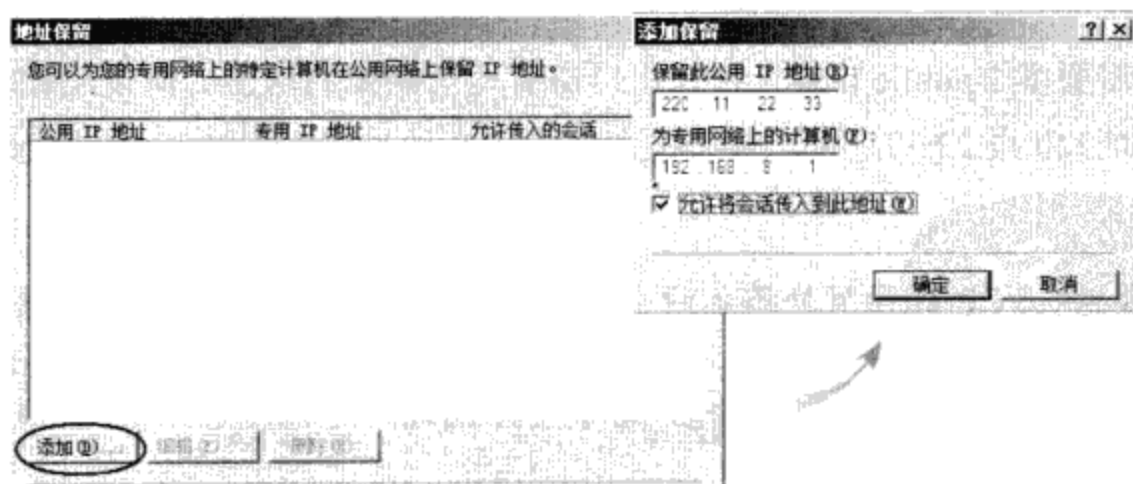


图 12-52

完成以上设置后，所有由计算机A（192.168.8.1）发出的外送流量都会从NAT服务器的IP地址220.11.22.33发出；同时因为我们还选择了**允许将会话传入到此地址**，因此所有从因特网发送给NAT服务器IP地址220.11.22.33的数据包，都会被NAT服务器转发给内部网络IP地址为

192.168.8.1的计算机A。

12-5 因特网连接共享 (ICS)

因特网连接共享 (Internet Connection Sharing, ICS) 是一个功能较简易的NAT, 它一样可以让内部网络多人同时通过ICS计算机来连接因特网、只需要使用一个public IP地址、可以通过路由器/电缆调制解调器/固接式或非固接式xDSL等来连接因特网。不过ICS在使用上比较缺乏弹性, 例如:

- ✎ 只支持一个专用网接口, 也就是只有该接口所连接的网络内的计算机可以通过ICS来连接因特网。
- ✎ DHCP分配器只能够分配网络标识符为192.168.137.0/24的IP地址 (前版Windows系统的DHCP分配器为192.168.0.0/24)。
- ✎ 无法将DHCP分配器停用, 也无法更改其设置, 因此若内部网络已经有DHCP服务器在服务的话, 请小心设置或将其停用, 以免DHCP分配器与DHCP服务器所分配的IP地址相冲突。
- ✎ 只支持一个public IP地址, 因此无**地址映射**的功能。

由于ICS与**路由和远程访问**不可以同时启用, 故要启用ICS前请先将**路由和远程访问**停用。启用ICS的步骤为: 【开始 ➤ 对着**网络**单击右键 ➤ 属性 ➤ 单击**更改适配器设置** ➤ 如图 12-53 所示对着连接因特网的连接 (例如外网卡或xDSL连接) 单击右键 ➤ 属性 ➤ 选择**共享**标签下的**允许其他网络用户通过此计算机的Internet连接来连接** ➤ 单击**确定**】。



提示

由于ICS计算机只允许从一个专用网接口来的用户可以通过ICS计算机连接因特网, 因此若ICS计算机拥有两个以上专用网接口的话, 则图 12-53中的前图会要求您从中选择一个专用网接口, 只有从这个接口来的请求可以通过ICS计算机连接因特网。

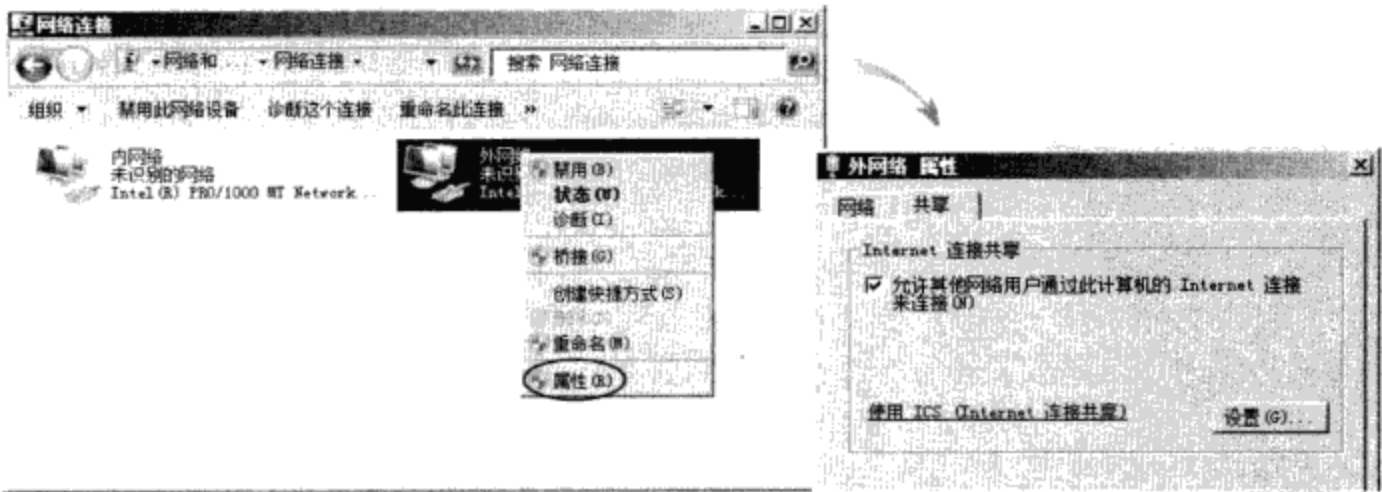


图 12-53

之后将出现图 12-54 的界面，表示一旦您启用ICS后，系统会将内部专用网接口（例如内网卡）的IP地址改为192.168.137.1/24，因此该网络接口所连接网络内的计算机的IP地址，其网络标识符也必须是192.168.137.0/24，否则无法通过ICS计算机来连接因特网。

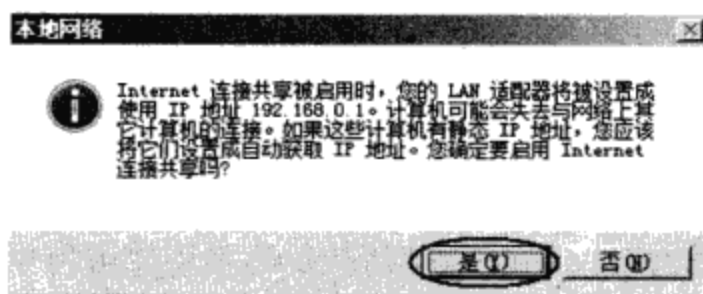


图 12-54

ICS客户端的TCP/IP设置方法与NAT客户端相同。一般来说，客户端的IP地址设置成自动取得即可，此时它们会自动向ICS计算机来索取IP地址、默认网关与首选DNS服务器等设置。它们所取得的IP地址将是192.168.137.x的格式，而默认网关与首选DNS服务器都是ICS计算机内网卡的IP地址192.168.137.1。

如果您希望客户端使用非192.168.137.x格式的IP地址的话，则ICS计算机的内网卡与客户端计算机的IP地址都必须自行手动输入（网络标识符必须相同），同时客户端的默认网关必须指定到ICS计算机内网卡的IP地址，首选DNS服务器可以指定到ICS内网卡的IP地址或任何一台正常运行的DNS服务器。

如果专用网接口所连接的网络内，包含着多个子网的话，则请确认各个子网的上网请求会被发送到ICS计算机，也就是各子网的上网数据包能够通过路由器来发送到ICS计算机（必要时可能需在路由器的路由表内手动新建路径）。