第十二部分　NAT的安装与配置

实验四十二　安装和配置NAT服务器

实验四十三　让外网用户通过NAT服务器访问内部服务

知识背景

NAT是Network Address Translation(网络地址转换)的英文缩写。网络地址转换工作在网络层和传输层，主要用于内部网络共享Internet连接。

网络地址转换有两方面的作用：一是共享IP地址和网络连接。它使内部网络使用私有的IP地址，共用一个或少量的Internet公用地址，从而节省IP地址资源，弥补IP地址的不足；二是保护网络安全，通过隐藏内部网络的IP地址，防止黑客攻击。

在Windows Server 2003“路由和远程访问”服务中包括NAT路由协议。服务器上只要安装和配置了NAT路由协议，此服务器就成为NAT服务器。将Windows Server 2003作为NAT服务器时，它就相当于一台路由器，但它是利用软件来实现网络地址转换的。

NAT分为源地址翻译(SNAT，Source Network Address Translation)和目的地址翻译(DNAT，Destination Network Address Translation)。源地址翻译让一个局域网里的计算机共享一个或少量IP上Internet(外网)。目的地址翻译就是端口映射，允许外网的计算机(Internet上的客户机)访问局域网内的机器，例如，在局域网内建了个Web服务器，要想让外网的用户来访问它，就用DNAT。

NAT服务器必须安装两个网卡，其中一个网卡连接到Internet或校园网，即外网；另一个网卡连接到局域网，即内网。NAT服务器作为局域网和互联网之间的一个网关。局域网中的每一个PC通过NAT服务器的内网网卡相连，并向这台NAT服务器发送HTTP请求，NAT服务器充当路由器，将这些请求转发到外网网卡上，并代表客户机在互联网上或校园网上转发这个请求，因此从外网看，所有的请求看上去都像是来自NAT服务器的外部IP地址。当此请求有回应时，这个回应将发送到NAT服务器上，NAT服务器又充当路由器的角色，再把这个回应转发给原来提出这个申请的客户机上，其结果总是使客户机不必直接与互联网联系。

网络地址转换(NAT)能够在转发数据包时转换内部的IP地址和TCP/UDP端口号。对于由内网传出的数据包，源IP地址和TCP/UDP端口号被映射到一个公共源IP地址和一个可能被改变的TCP/IP端口号上。而对从外网传入的数据包，也必须经过网络地址转换(NAT)。在NAT转换表中存在一种特定的映射，使目标IP地址和TCP/UDP端口号被映射到专用IP地址和缺省的TCP/IP端口号上，从而把来自Internet的数据转发到特定网络或特定的计算机上。

例如，在专用网络上安装了一个Web服务器，该专用网络以一个NAT服务器作为边界，假定已在一个ISP供应商中创建了一个域名(DNS)记录，将所申请到的公网域名如www.example.com映射到ISP供应商处申请的公共IP地址202.121.20.1上。当外部某个Internet客户端访问专用网络上的Web服务器时，将按以下步骤完成：

(1) Internet上的一个Web客户端计算机(使用公共IP地址121.117.0.1)上的用户在他们的Web浏览器中键入http://www.example.com。

(2) Internet Web客户端使用DNS将名称www.example.com解析为地址202.121.20.1。

(3) Internet Web客户端计算机从121.117.0.1/TCP端口2000向202.121.20.1/TCP端口80发送一个传输控制协议(TCP)同步(SYN)段。

(4) 当NAT服务器接收到该TCP SYN段时，检查自己的NAT转换表。

(5) 如果在NAT转换表中不存在针对目标202.121.20.1/TCP端口80的条目，该TCP SYN段将自动被丢弃。

(6) Internet Web客户端计算机一直重试，直至最终显示一条出错消息为止。

NAT服务器为解决此问题，必须进行手动静态配置。通常有两种静态配置，一种是将某个特定公共IP地址的所有流量映射到某个特定的专用地址上(地址映射，不分端口)。其特点是内网中特定的专用地址的计算机对外开放，配置容易，但易受攻击，但不能对外开放多种资源服务(如Web服务、FTP服务、邮件服务等)，若需要这些服务都对外开放，需多个公共外网IP地址。另一种是将一个特定的公共IP地址/端口号映射到一个特定的专用IP地址/端口号(地址/端口映射)。其特点是要额外配置，不易受到攻击，但对不同的资源服务(如Web服务、FTP服务、邮件服务等)可使用一个公共IP地址。我们这里将介绍第二种静态配置。

实验四十二 安装和配置NAT服务器

【实验条件】

(1) 在Windows Server 2003上安装两块网卡，一块网卡与外网(校园网或Internet)相连，一块网卡与内网(Windows 2000 Professional客户端和Windows XP客户端)相连。

(2) 在Windows Server 2003上能访问外网。

(3) Windows Server 2003、Windows 2000 Professional和Windows XP三台计算机网络连通。

【实验说明】

本实验详细介绍安装和配置NAT服务器的步骤。

【实验任务】

(1) 网络环境的配置说明。

(2) 安装和配置NAT服务器。

(3) 客户端通过NAT服务器访问外网。

【实验目的】

(1) 掌握NAT服务器的安装和配置方法。

(2) 掌握NAT的使用。

【实验内容】

一、配置NAT服务器所需的环境

将Windows Server 2003作NAT服务器，其上的两个网卡设置如下：

- 8139网卡(外网网卡，与校园网或Internet连接)：

IP地址：219.220.237.服务器的机器号

子网掩码：255.255.255.0

默认网关：219.220.237.254

首选DNS：202.121.241.8

202.96.209.5

- D-LINK网卡(内网网卡，与另两台工作站连接)：

IP：192.168.1.服务器的机器号

子网掩码：255.255.255.0

网关：

DNS：202.121.241.8

202.96.209.5

二、安装NAT服务器(以01小组为例)

(1) 在“管理工具”菜单中选择“路由和远程访问”菜单，出现“路由和远程访问”控制台窗口，展开服务器名称win2003s-01(此时服务器的左边有一个大的红点，表明这台服务器目前还没有作为路由使用)，用鼠标右键点击此服务器，从快捷菜单中选择“配置并启用路由和远程访问”菜单，Windows将启动“路由和远程访问服务器安装向导”。单击“下一步”按钮，出现如图12-1-1所示对话框。

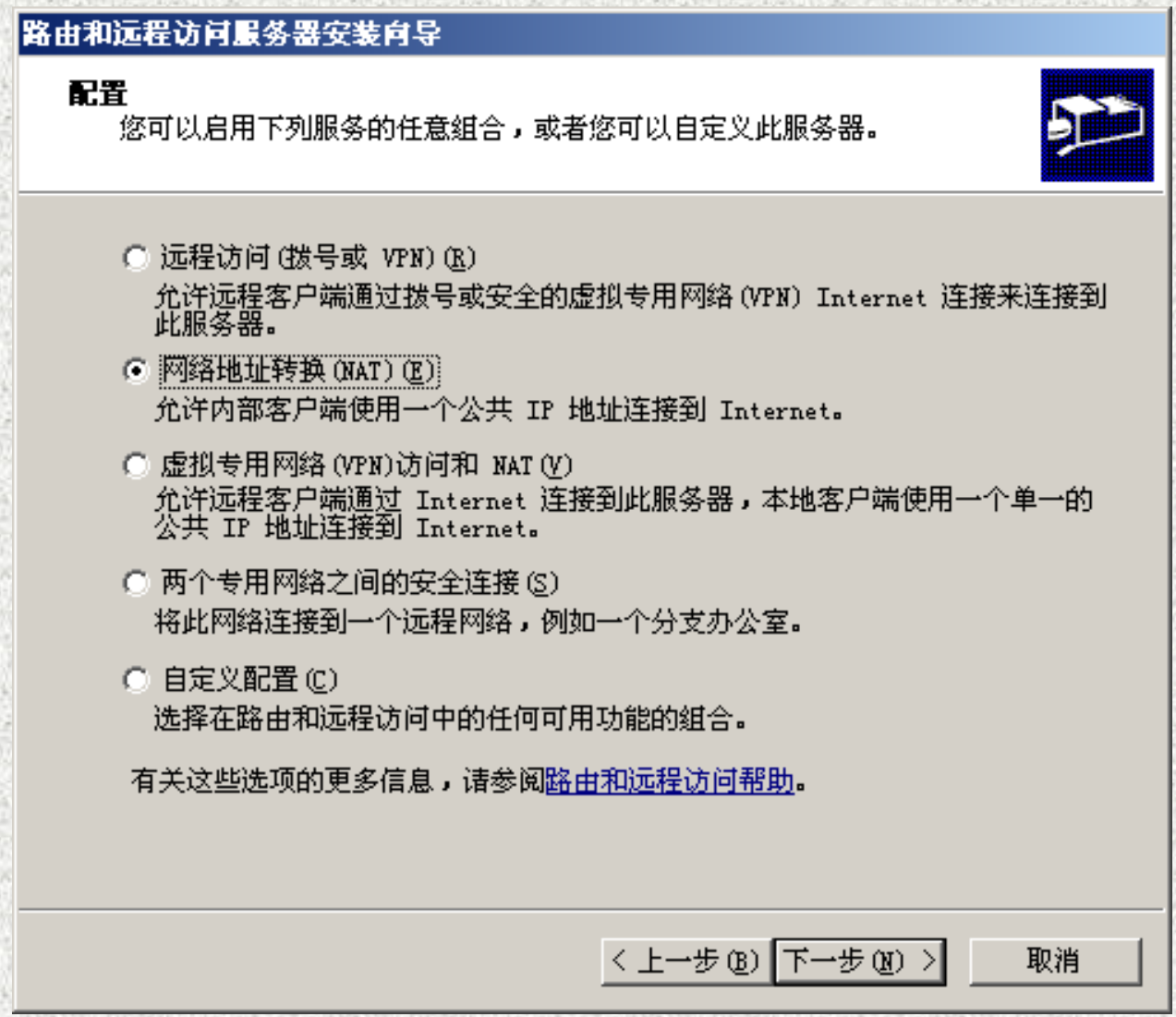
路由和远程访问服务器安装向导
配置
您可以启用下列服务的任意组合，或者您可以自定义此服务器。
远程访问(拨号或 VPN)(R)
允许远程客户端通过拨号或安全的虚拟专用网络(VPN) Internet 连接来连接到此服务器。
网络地址转换(NAT)(E)
允许内部客户端使用一个公共 IP 地址连接到 Internet。
虚拟专用网络(VPN)访问和 NAT(V)
允许远程客户端通过 Internet 连接到此服务器，本地客户端使用一个单一的公共 IP 地址连接到 Internet。
两个专用网络之间的安全连接(S)
将此网络连接到一个远程网络，例如一个分支办公室。
自定义配置(C)
选择在路由和远程访问中的任何可用功能的组合。
有关这些选项的更多信息，请参阅路由和远程访问帮助。
< 上一步(B)
下一步(N) >
取消

图12-1-1

(2) 选中“网络地址转换(NAT)”，单击“下一步”按钮，出现两行以上的连接说明，显示各网卡所对应的连接名及IP地址，其中一个是连接到外网(这里是校园网)的网络接口的选项(这里是RealTek 8139，IP地址是219.220.237.服务器的机器号)，并选中“通过设置基本防火墙来对选择的接口进行保护”，如图12-1-2所示，然后单击“下一步”按钮。


路由和远程访问服务器安装向导
NAT Internet 连接
您可以选择一个现存的接口，或者为客户端计算机创建一个新的请求拨号接口来连接到 Internet。
使用此公共接口连接到 Internet(U):
名称
描述
IP 地址
内网
D-Link
192.168.1.1
外网
Realtek RTL8139/...
219.220.237.1
创建一个新的到 Internet 的请求拨号接口(D)
当客户端使用 Internet 时激活请求拨号接口。如果此服务器连接到一个调制解调器或使用通过以太网的点对点协议，则选择此选项。请求拨号接口向导将在此向导结束后启动。
通过设置基本防火墙来对选择的接口进行保护(E)
基本防火墙防止未授权的用户通过 Internet 访问此服务器。
有关网络接口的更多信息，请参阅路由和远程访问帮助。
< 上一步(B)
下一步(N) >
取消

图12-1-2

(3) 出现如图12-1-3所示对话框，询问是否开启并配置DNS和DHCP服务，因局域网内采用静态IP，且Windows Server 2003系统中已启用了DNS服务，这里选“我将稍后设置名称和地址服务”。单击“下一步”按钮，开始启动路由和远程访问，从而完成NAT服务器的基本设置。

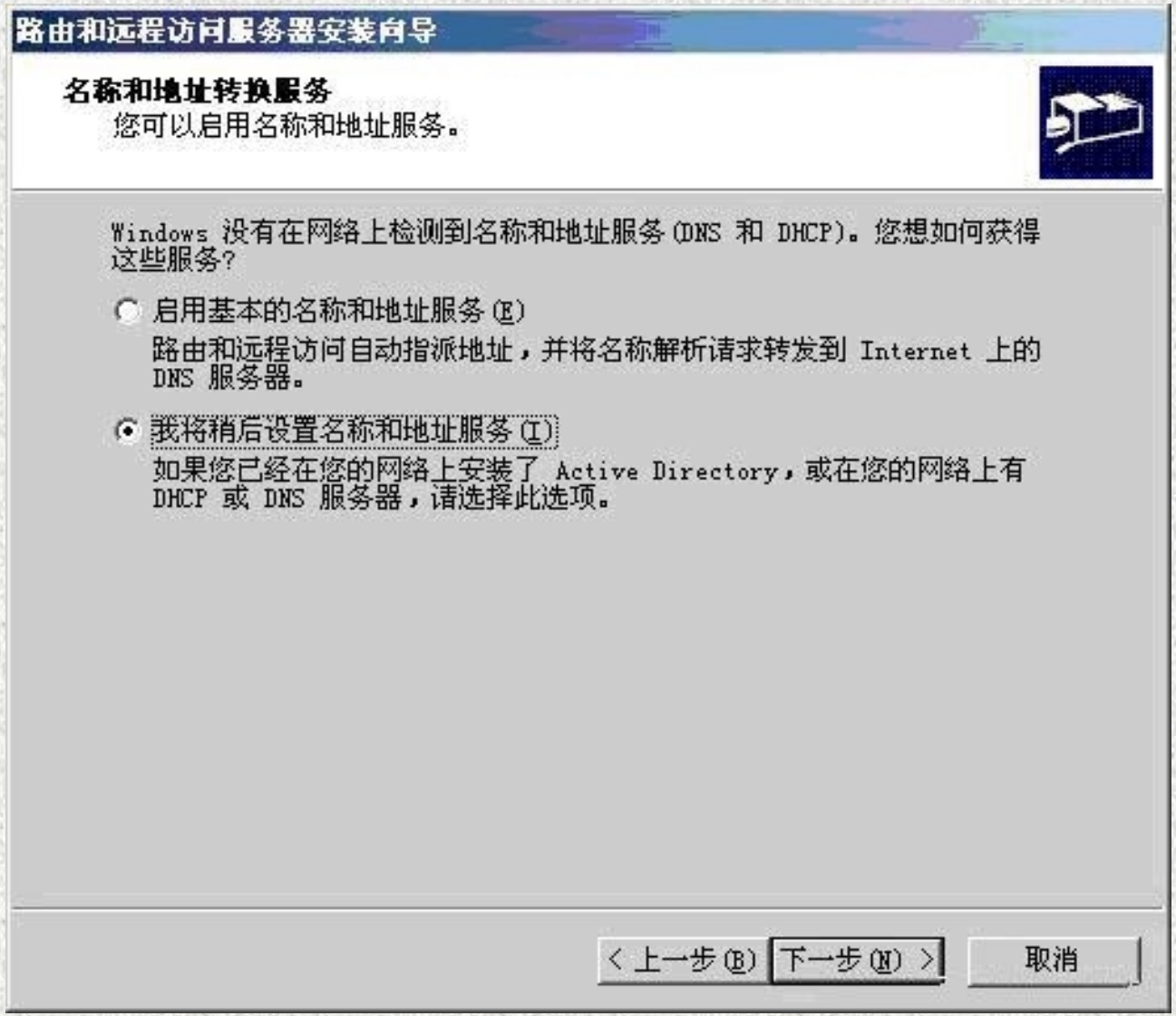
路由和远程访问服务器安装向导
名称和地址转换服务
您可以启用名称和地址服务。
Windows 没有在网络上检测到名称和地址服务(DNS 和 DHCP)。您想如何获得这些服务?
启用基本的名称和地址服务(E)
路由和远程访问自动指派地址,并将名称解析请求转发到 Internet 上的 DNS 服务器。
我将稍后设置名称和地址服务(I)
如果您已经在您的网络上安装了 Active Directory,或在您的网络上有 DHCP 或 DNS 服务器,请选择此选项。
< 上一步(B)
下一步(N) >
取消

图12-1-3

三、在NAT服务器中启动DHCP服务的配置(这里可省略，因为客户端采用的是静态IP地址)

配置路由和远程访问NAT服务器，使其为客户端分配IP地址。当客户端需要自动获得IP地址时，NAT服务器可以自动为内部网络客户端分配IP地址。如果没有DHCP服务器(虽安装了但没有使用)，可使用此功能。

NAT服务器分配IP地址的操作步骤如下：

(1) 在“路由和远程访问”控制台窗口中，右击“IP路由选择”的“NAT/基本防火墙”，然后单击“属性”按钮。

(2) 单击“地址分配”选项卡，选中“使用DHCP自动分配IP地址”复选框，在“IP地址”框中键入网络ID，在掩码框中键入子网掩码。这些都是将自动分配给客户端的网络号和子网掩码。

四、在NAT服务器中启动DNS服务的配置(这里可省略，因为Windows Server 2003上已启动了DNS服务)

NAT服务器还可以代表NAT客户端执行域名系统(DNS)查询。“路由和远程访问”NAT服务器对包括在客户请求中的Internet主机名进行解析，然后将该IP地址转发给该客户端。由于此Windows Server 2003系统中已安装并使用了DNS服务，因而这里不需要在NAT服务器中执行域名系统(DNS)查询。

如果需要DNS解析，则在“路由和远程访问”控制台窗口中，右击“IP路由选择”的“NAT/基本防火墙”，然后单击“属性”按钮。切换到“名称解析”选项卡，选中“使用域名系统(DNS)的客户”复选框，并选中“当名称需要解析时连接到公共网络”复选框，然后在网络接口中选中连接外网的连接名称。

五、配置内部网络客户端使用NAT服务器

在客户端的“Internet协议(TCP/IP)”配置中，在“默认网关”框中，键入NAT服务器的内部IP地址。

在两个客户机上启动D-LINK网卡，设置如下：

IP地址：192.168.1.客户机的机器号

子网掩码：255.255.255.0

默认网关：192.168.1.服务器的机器号

首选DNS：192.168.1.服务器的机器号

202.121.241.8