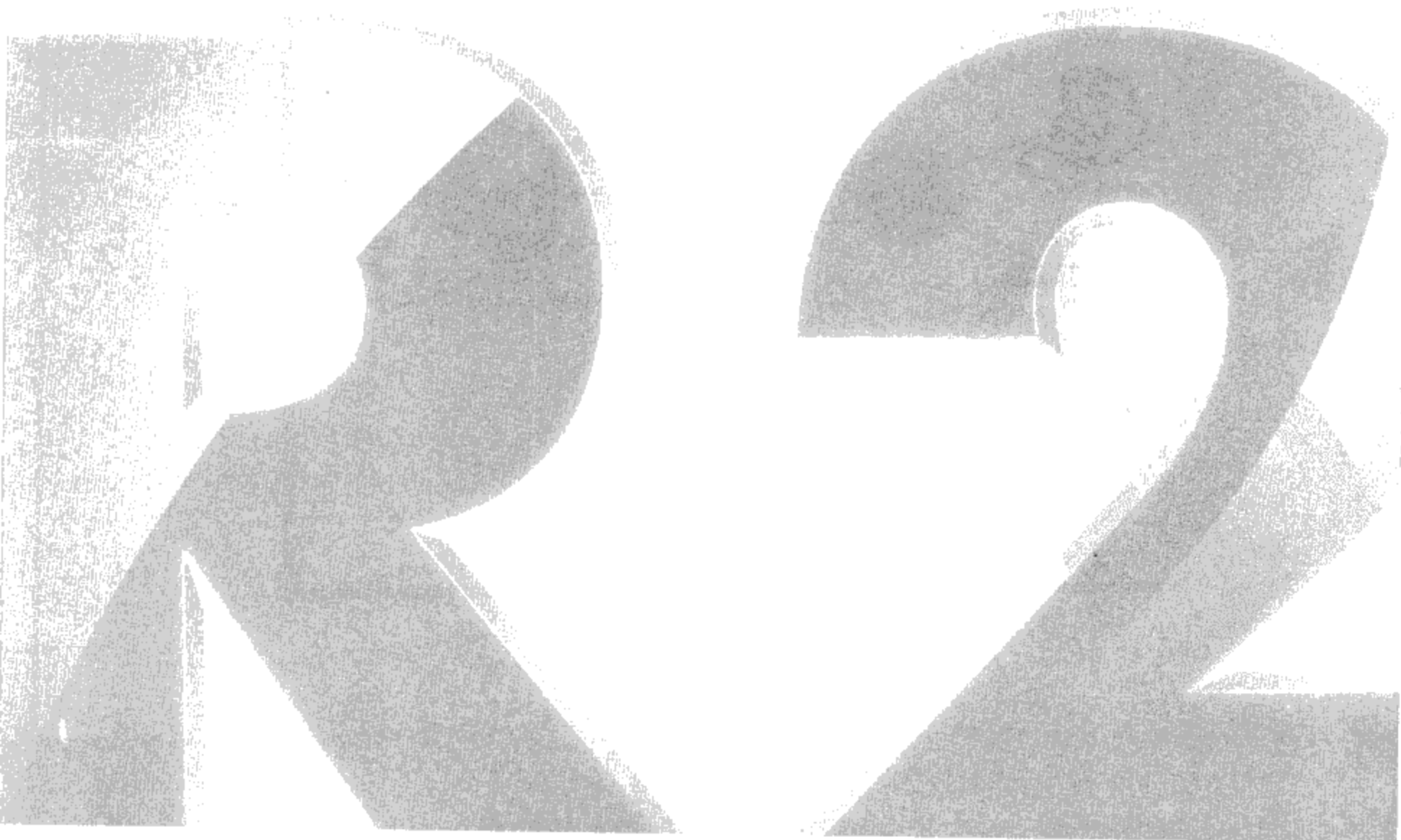


# 第 14 章

## RADIUS服务器的架设

如果网络内有多台远程访问服务器或VPN服务器话，则您可以将这些服务器的验证用户身份工作，转给**RADIUS服务器**或**RADIUS代理服务器**来集中执行。

- RADIUS概述
- 安装网络策略服务器（NPS）
- RADIUS服务器与客户端的设置
- RADIUS代理服务器的设置



## 14-1 RADIUS概述

RADIUS (Remote Authentication Dial-In User Service) 是一种**客户端/服务器** (client/server) 的协议, 它让RADIUS客户端可以将验证用户身份 (authentication)、授权 (authorization) 与记账 (accounting) 等工作, 转给RADIUS服务器来执行; 或转给RADIUS代理服务器 (proxy server), 然后再由它转给RADIUS服务器来执行。

Windows Server 2008 R2通过**网络策略服务器** (Network Policy Server, NPS) 角色来提供RADIUS服务器与RADIUS代理服务器的服务。

### 14-1-1 RADIUS服务器

网络策略服务器 (NPS) 可以让Windows Server 2008 R2计算机扮演RADIUS服务器的角色, 而其RADIUS客户端可以是常规的远程访问服务器 (利用调制解调器连接客户端)、VPN服务器或无线访问接入点 (Access Point, AP) 等访问服务器 (access server), 如图 14-1 所示。

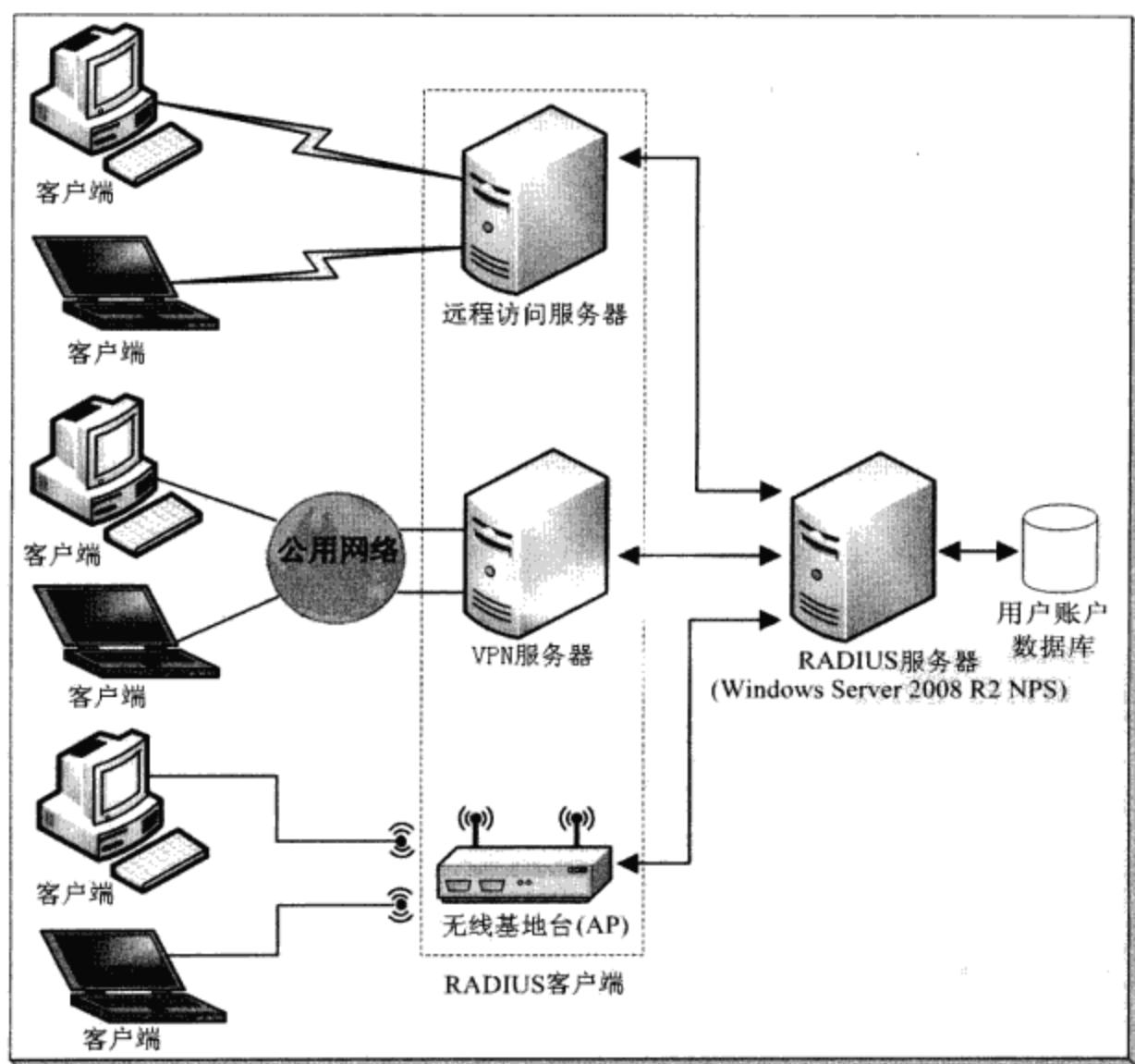


图 14-1

图中RADIUS服务器是由Windows Server 2008 R2的NPS来提供RADIUS的服务，它可以为RADIUS客户端执行验证用户身份、授权与记帐等工作。其工作流程如下：

1. 远程访问服务器、VPN服务器或无线访问接入点等访问服务器接收来自客户端的连接请求。
2. 访问服务器请求RADIUS服务器来执行身份验证、授权与记帐的工作。
3. RADIUS服务器检查用户名称与密码是否正确认证，并且通过用户账户属性（**拨入**标签）与网络策略的设置，决定是否授权用户。

**提示**

**网络策略**在Windows Server 2003内被称为**远程访问策略**。

4. 若用户被允许连接的话，则RADIUS服务器会通知访问服务器，然后访问服务器即可让客户端连接。同时访问服务器也会通知RADIUS服务器将此次的连接请求记录下来。

我们可以开放让用户用RADIUS服务器的本地用户账户或Active Directory用户账户来连接访问服务器，RADIUS服务器在验证用户身份与账户属性时，可以从以下两个用户账户数据库来得到这些数据：

- ✎ RADIUS服务器的本地安全数据库。
- ✎ 域的Active Directory数据库，此时RADIUS服务器需为域成员，而用户账户可以是所属域的账户或有双向信任关系的其他域的账户。

若未将验证、授权与记帐的工作转给RADIUS服务器的话，则每一台远程访问服务器或VPN服务器必须自己执行这些工作，因此每一台远程访问服务器或VPN服务器都需要有自己的网络策略与记录文件，这样将增加维护这些数据的负担。

而在将验证、授权与记帐的工作转给RADIUS服务器后，就只需要维护位于RADIUS服务器内的网络策略与记录文件即可，也就是在远程访问服务器或VPN服务器内都不需要另外创建网络策略与记录文件。

## 14-1-2 RADIUS代理服务器

RADIUS代理服务器（proxy server）可以将从RADIUS客户端（远程访问服务器、VPN服务器或无线访问接入点等访问服务器）所发来的验证身份、授权与记帐等请求转发给其他RADIUS服务器来执行，如图 14-2所示。

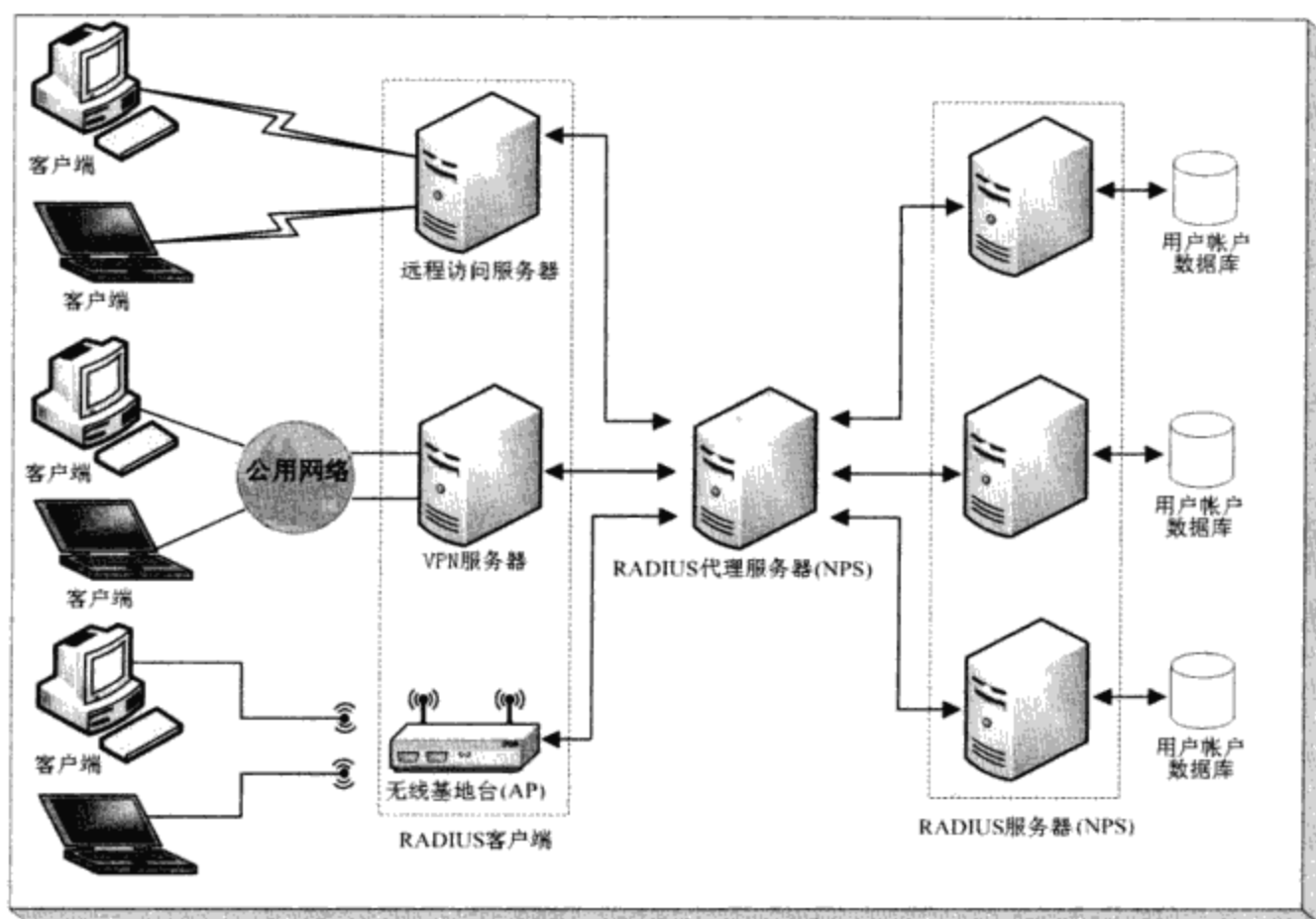


图 14-2

举例来说，在以下两种场合，您可能需要用到RADIUS代理服务器：

- ✎ 以前面图 14-1来说，如果用户帐户并不是RADIUS服务器的本地帐户、也不是RADIUS服务器所属域的Active Directory帐户、也不是有双向信任关系的其他域的Active Directory帐户，例如用户帐户是位于未创建信任关系的域内、或只有单向信任关系的域内、或其他林（forest）内，则RADIUS服务器将无法读取到用户帐户的数据，因而无法验证用户身份，也无法验证用户是否有权限来连接。  
此时我们可以通过图 14-2的RADIUS代理服务器来将验证、授权与记帐工作，转发给可以读取用户帐户数据的RADIUS服务器来执行，这些RADIUS服务器可能分别隶属于不同域、林，甚至是其他非微软系统的RADIUS服务器。
- ✎ 分散RADIUS服务器的负担：如果有大量的客户端连接请求的话，则可以通过RADIUS代理服务器将这些连接请求转发到不同的RADIUS服务器，以便加快处理的效率。

当Windows Server 2008 R2 NPS被当作是RADIUS代理服务器来使用时，它与RADIUS客户端、RADIUS服务器之间的交互如下（参考图 14-2）：

1. 远程访问服务器、VPN服务器或无线访问接入点等访问服务器接收来自客户端的连接请求。
2. 访问服务器请求RADIUS代理服务器来执行验证、授权与记帐的工作。
3. RADIUS代理服务器会转而请求RADIUS服务器来执行验证、授权与记帐的工作。
4. RADIUS服务器验证用户的身份并决定是否允许用户连接。

5. 若用户被允许连接，则RADIUS服务器会通知RADIUS代理服务器，然后再由RADIUS代理服务器转通知访问服务器，访问服务器即可让客户端连接。同时访问服务器也会通知RADIUS代理服务器将这次的连接请求记录下来。

## 14-2 安装RADIUS服务器

我们将利用图 14-3来说明如何安装RADIUS服务器，图中的RADIUS1为Windows Server 2008 R2 RADIUS服务器，而且是域成员服务器，而VPNS1为VPN服务器，它同时也是RADIUS客户端。本章将只着重在RADIUS这部分，至于VPN服务器的部分在第13章已经介绍过了，此处不再说明。

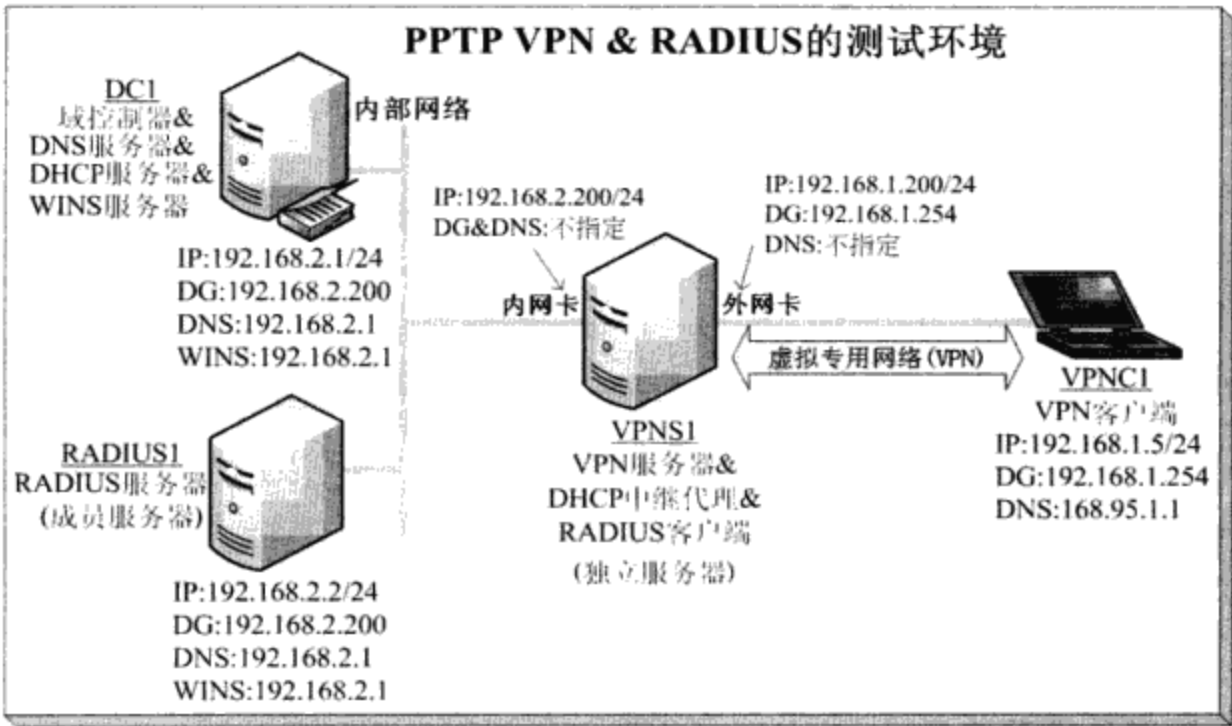



图 14-3

### 14-2-1 安装网络策略服务器（NPS）

我们需要通过安装**网络策略服务器**（Network Policy Server，NPS）角色的方式来创建RADIUS服务器或RADIUS代理服务器。

- STEP 1** 请在RADIUS1上利用域Administrator身份登录，然后选择【单击左下角**服务器管理器**图标单击**角色**右方的**添加角色**】。
- STEP 2** 出现**开始之前**界面时单击**下一步**。
- STEP 3** 在图 14-4中选择**网络策略和访问服务**后单击**下一步**。

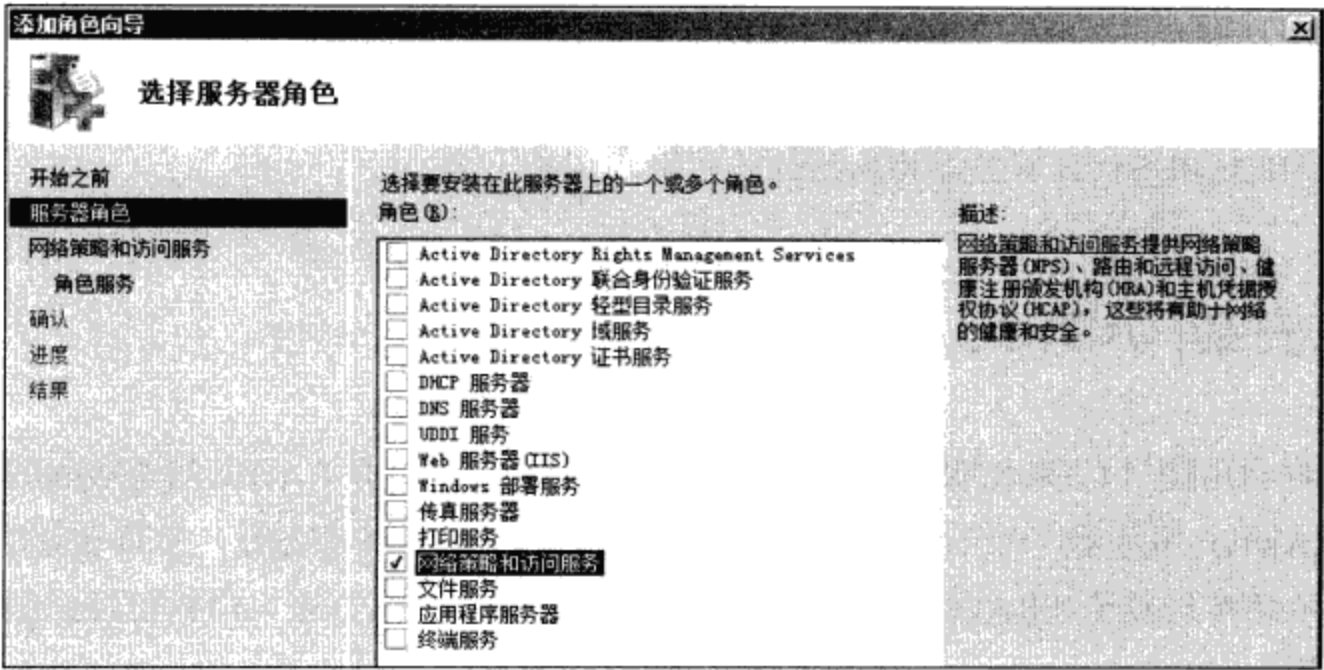


图 14-4

- 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 14-5所示选择网络策略服务器后单击 **下一步**。

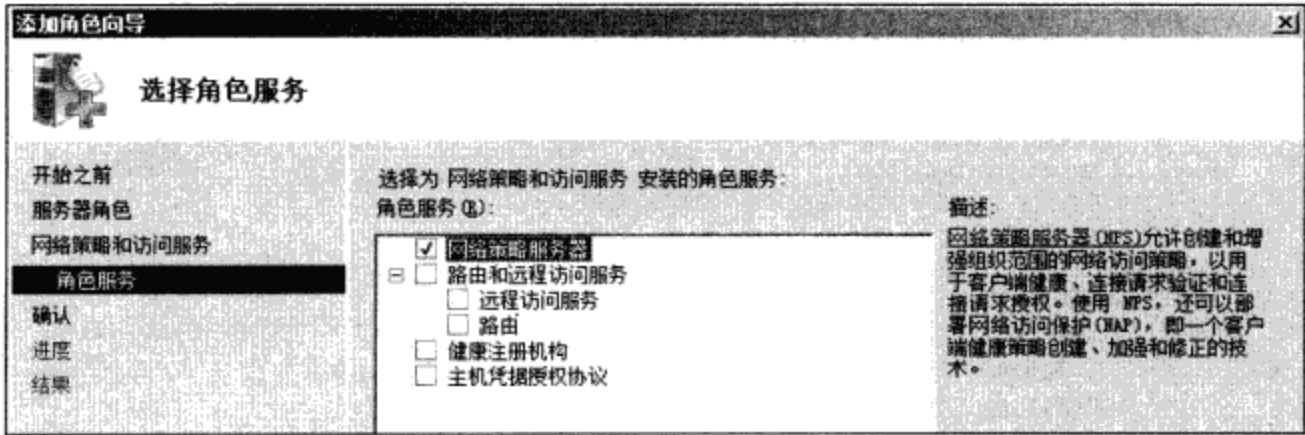


图 14-5

- STEP 6** 出现确认安装选择界面时单击 **安装**。
- STEP 7** 出现安装结果界面时单击 **关闭**。

完成安装后可以通过【开始 ➤ 管理工具 ➤ 网络策略服务器】的途径来管理NPS，如图 14-6 所示。您也可以通过【对着NPS（本地）单击右键 ➤ 停止NPS服务或启动NPS服务】的途径来停止或启动NPS。



**提示**

若要管理其他RADIUS服务器的话：【开始 ➤ 运行 ➤ 输入MMC后按 **Enter** 键 ➤ 文件菜单 ➤ 添加/删除管理单元 ➤ 从列表中选择 **网络策略服务器** ➤ 添加 ➤ 选择另一台计算机、输入计算机名或IP地址 ➤ ……】。

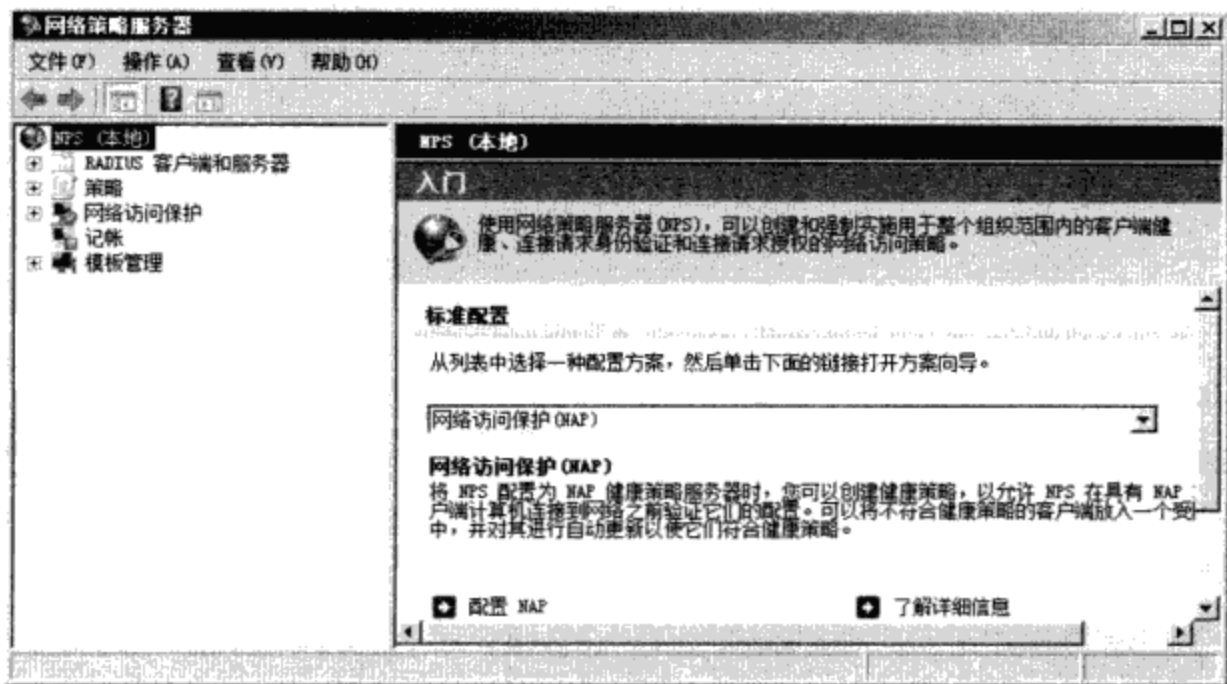


图 14-6

## 14-2-2 注册网络策略服务器

若NPS（网络策略服务器）隶属于Active Directory域的话，则当域用户连接时，NPS必须向域控制器查询用户账户的拨入属性，才能判断用户是否被允许连接，不过您必须事先将NPS注册到Active Directory数据库。您可以利用以下方法中的一种来注册NPS：

- 利用**网络策略服务器控制台**：请在NPS这台计算机上利用域系统管理员的身份登录，然后选择【开始☞管理工具☞网络策略服务器☞如图 14-7所示对着NPS（本地）单击右键☞在Active Directory中注册服务器☞在前图中单击**确定**】。

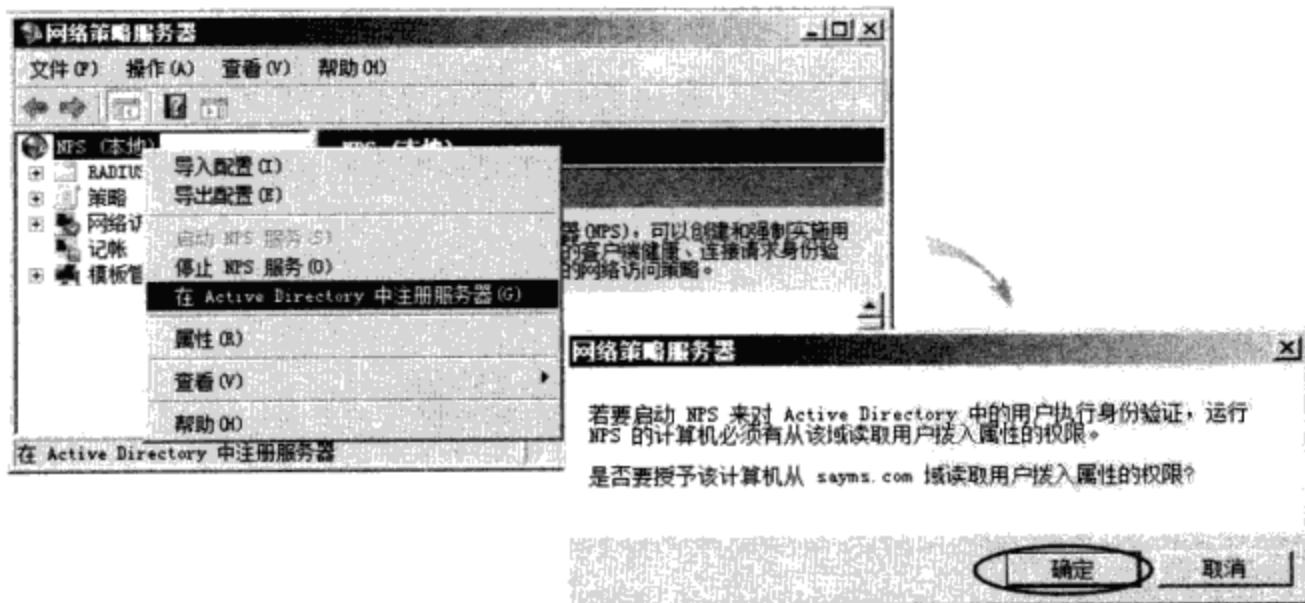


图 14-7

- 在**命令提示符**（或Windows PowerShell）窗口下运行netsh命令：请在NPS这台计算机上用域系统管理员身份登录，然后选择【开始☞命令提示符☞如图 14-8所示运行netsh ras add registeredserver】。



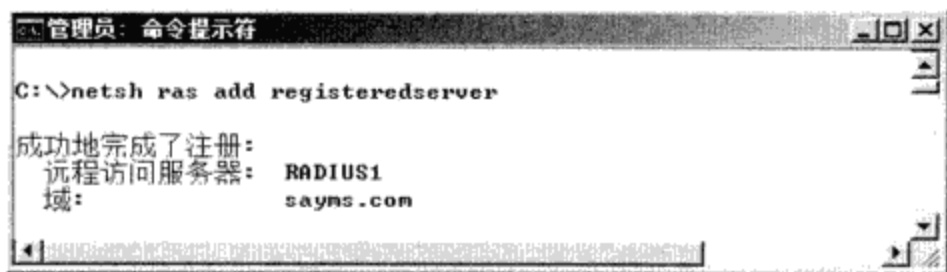


图 14-8

- 直接NPS计算机账户加入到RAS and IAS Servers组：到域控制器上利用域系统管理员身份登录，打开Active Directory用户和计算机或Active Directory管理中心、将NPS计算机（RADIUS1）加入到RAS and IAS Servers组（位于Users容器）内，图 14-9分别为完成后的界面。

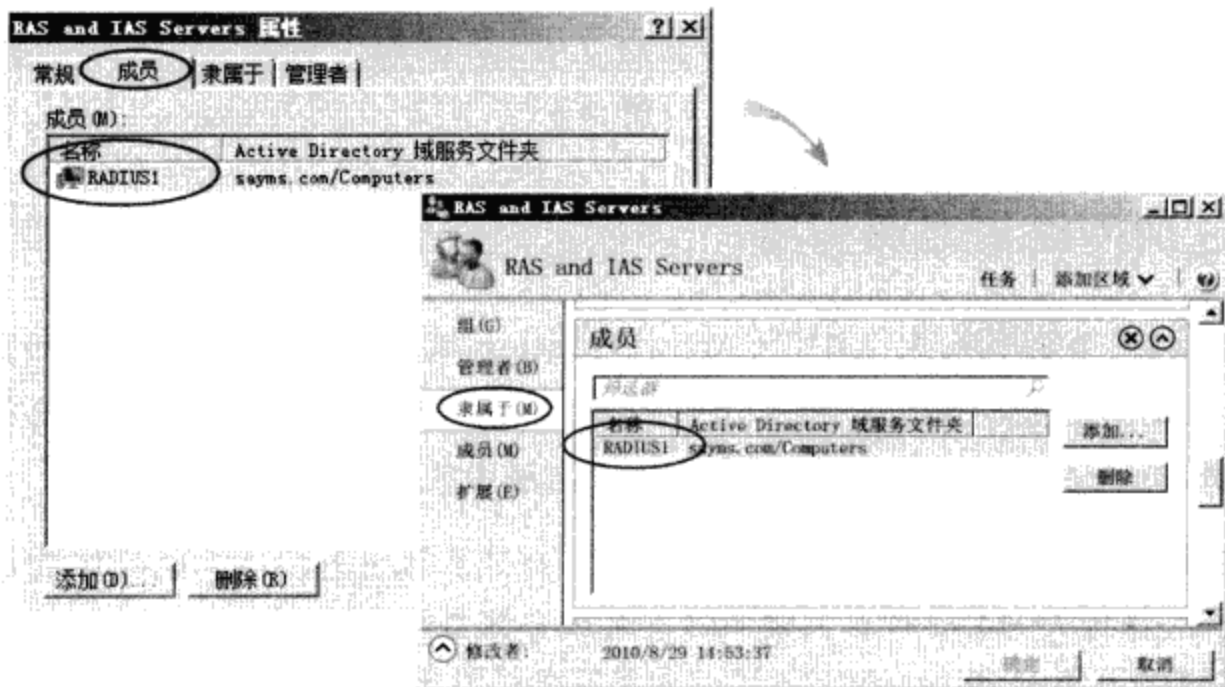


图 14-9

以上方法都可以将NPS注册到NPS所隶属的域。如果要想NPS读取其他域用户账户的拨入属性的话，则需将NPS注册到其他域的Active Directory数据库，也就是将NPS加入到其他域的RAS and IAS Servers组内。

### 14-3 RADIUS服务器与客户端的设置

无论NPS是扮演RADIUS服务器或RADIUS代理服务器的角色，您都必须指定其RADIUS客户端，它们只接受这些指定的RADIUS客户端所传来的连接请求。以下针对图 14-10来说明如何设置 RADIUS服务器与RADIUS客户端，图中RADIUS客户端是由VPN服务器VPNS1所扮演，而RADIUS服务器由域成员服务器RADIUS1来扮演。



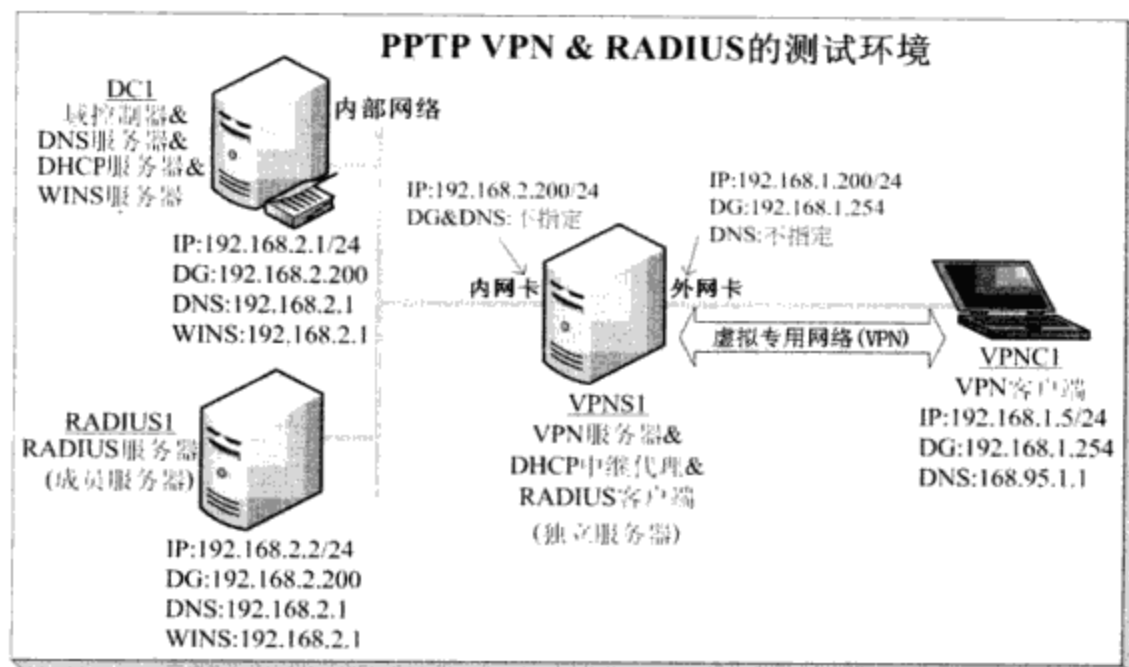


图 14-10

### 14-3-1 RADIUS服务器的设置

NPS安装完成后，系统默认是将它设置为RADIUS服务器，以下步骤用来指定此RADIUS服务器的RADIUS客户端。

**STEP 1** 请到NPS上选择【开始☞管理工具☞网络策略服务器☞如图 14-11所示对着RADIUS客户端单击右键☞新建】。

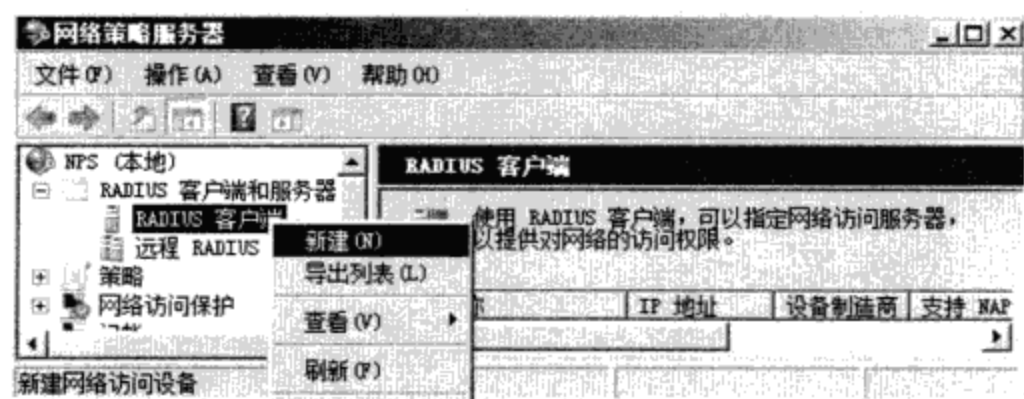


图 14-11

**STEP 2** 在图 14-12中先确认已选择启用此RADIUS客户端，接着设置：

- **友好名称**：为此RADIUS客户端设置一个名称。
- **地址（IP或DNS）**：输入RADIUS客户端的IP地址或主机名。若输入NetBIOS计算机名或DNS主机名的话，请单击**验证**来确认可以解析到此名称的IP地址。



#### 注意

若输入NetBIOS计算机名的话，由于被RADIUS客户端的Windows防火墙阻挡，因此会无法解析到RADIUS客户端的IP地址，除非您将RADIUS客户端的Windows防火墙关闭或例外开放文件和打印机共享。

- **共享机密**：可以选择手动（如图所示）或自动创建密码，需在RADIUS客户端也设置相同密码，只有双方密码相同时，才接受该客户端传来的验证、授权与记帐要求。密码区分大小写。

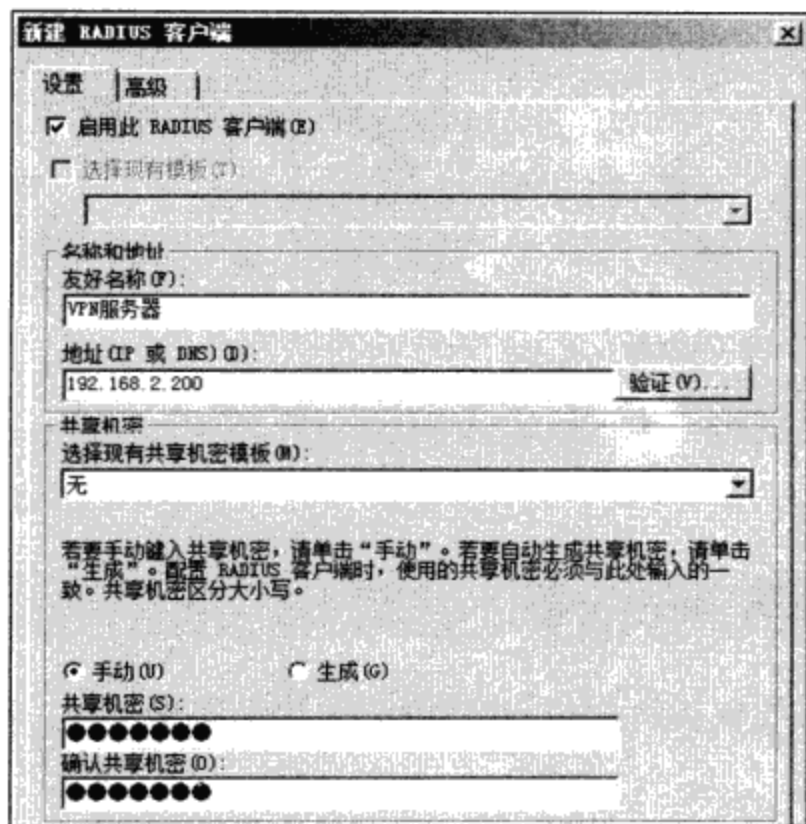


图 14-12

**STEP 3** 单击图 14-13中的高级标签：

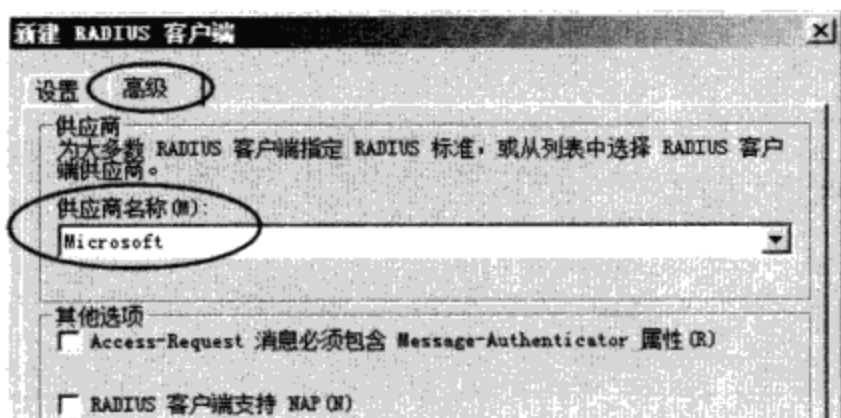


图 14-13

- **供应商名称**：选择提供客户端RADIUS功能的供应商，由于我们的RADIUS客户端为 Microsoft Windows Server 2008 R2 VPN服务器，故此处请选择 **Microsoft**。若列表中找到供应商或不确定供应商的话，可选择标准的 **RADIUS Standard**。
- **Access-Request消息必须包含Message-Authenticator属性**：如果双方所采用的验证方法是PAP、CHAP、MS-CHAP、MS-CHAP v2的话，则您可以要求对方发送消息验证程序属性，以提高安全（可找出假造来源IP地址的RADIUS客户端）。若验证方法是采用EAP的话，它会自动启用此功能，不需要在此另外设置。

- RADIUS客户端支持NAP：第15章会详细介绍NAP。

**STEP 4** 图 14-14为完成后的界面。

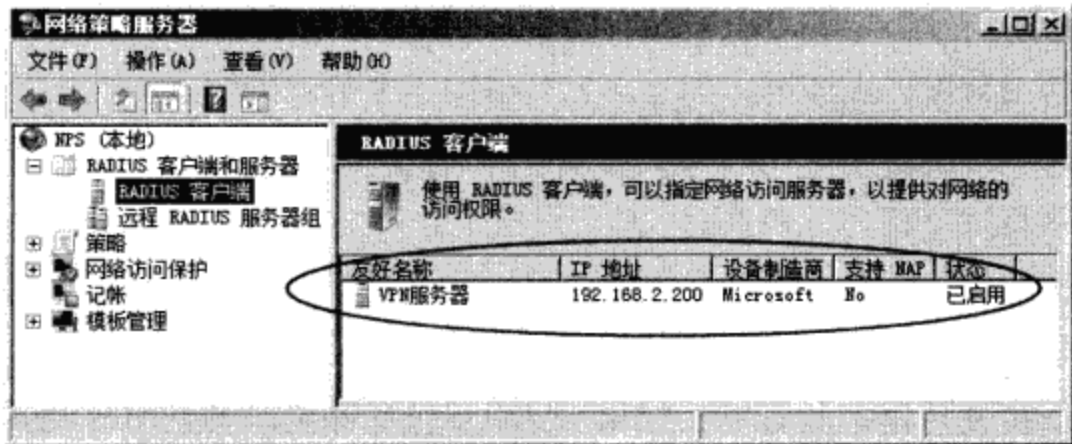


图 14-14

### 14-3-2 RADIUS客户端的设置

所谓的RADIUS客户端是指访问服务器，例如远程访问服务器、VPN服务器或无线访问接入点等，常规的客户端计算机端并不是RADIUS客户端。

您必须在扮演RADIUS客户端角色的服务器上（例如VPN服务器），设置将其客户端（例如VPN客户端）所发来的连接请求转发给RADIUS服务器。

**STEP 1** 请到RADIUS客户端上（远程访问服务器或VPN服务器），选择【开始→管理工具→路由和远程访问→如图 14-15所示单击本地计算机→单击上方属性图标→安全标签→在身份验证提供程序处选择RADIUS身份验证→单击配置】。

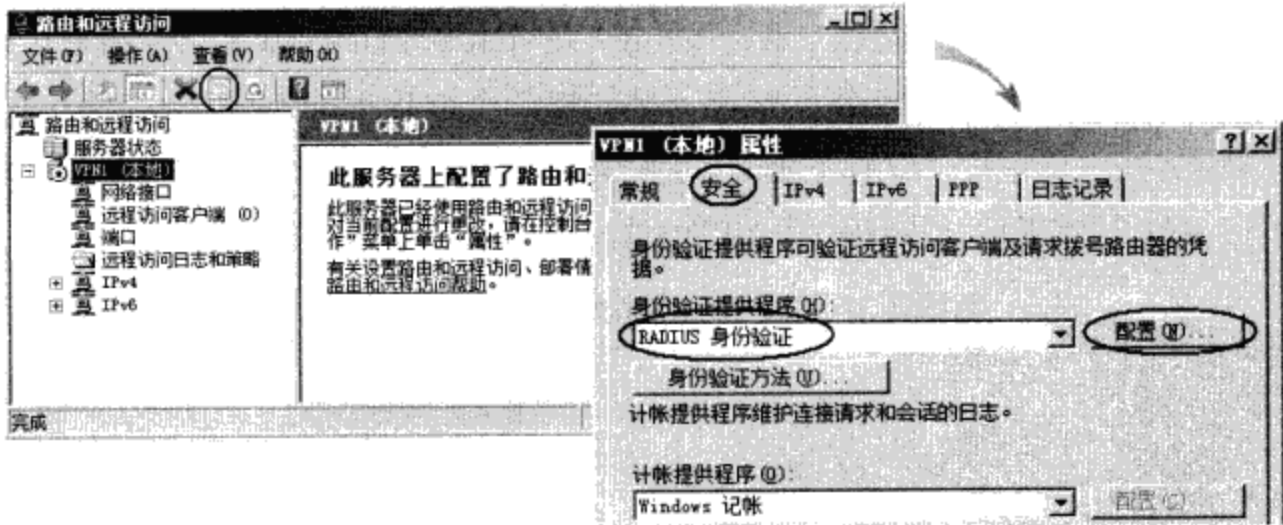


图 14-15

**STEP 2** 在图 14-16中单击**添加**，然后通过前图来设置：

- 服务器名称：请输入RADIUS服务器的主机名或IP地址。
- 共享机密：通过**更改**来设置与RADIUS服务器端相同的密码（见图 14-12中的共享机密）。

- **超时**：若等候时间到达时，仍然没有收到这台RADIUS服务器响应的话，就自动将身份验证请求转发到另外一台RADIUS服务器（若有设置多台RADIUS服务器的话）。
- **初始分数**：若同时设置了多台RADIUS服务器的话，则此处用来设置它们的优先级，系统会先将身份验证请求发到优先级较高的RADIUS服务器。初始分数值越大，优先级越高。
- **端口**：RADIUS服务器的端口号，标准端口号是1812（旧版的RADIUS服务器是1645）。
- **一直使用消息验证者**：如果RADIUS服务器要求传送Message-Authenticator属性的话，则请选择此选项。若是采用EAP验证方法的话，则它会自动启用此功能，不需要另外选择。

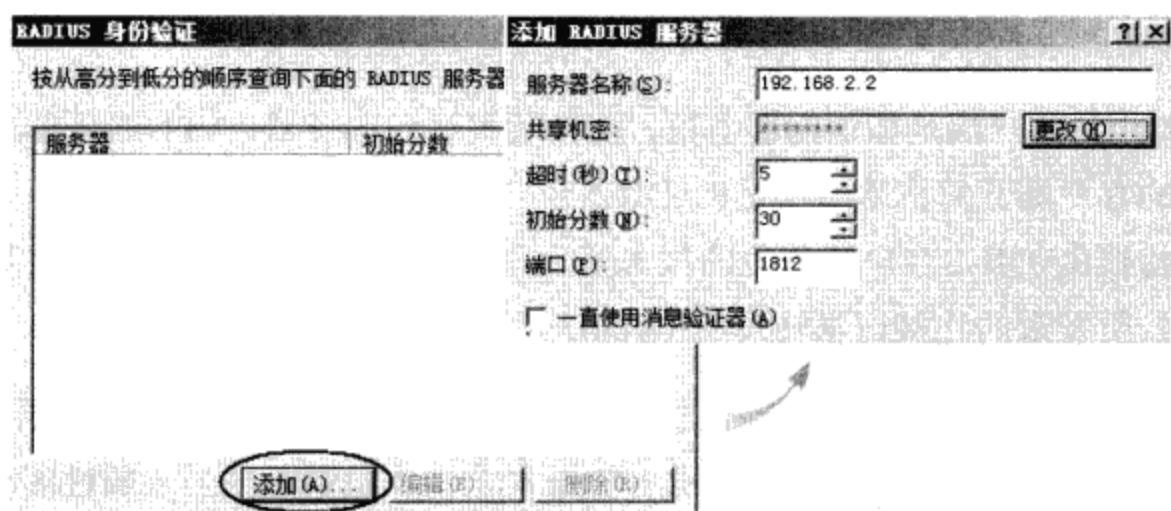


图 14-16

您也可以如图 14-17所示将记帐（accounting）的工作转给RADIUS服务器来执行，也就是让RADIUS服务器来记录每一个连接的情形，例如每一个被接受的连接、被拒绝的连接等验证记录，还有登录/注销等用来记账的记录等。RADIUS记帐的设置方法与前面的RADIUS验证设置类似，不过其端口号是1813（旧版的RADIUS服务器是1646）。

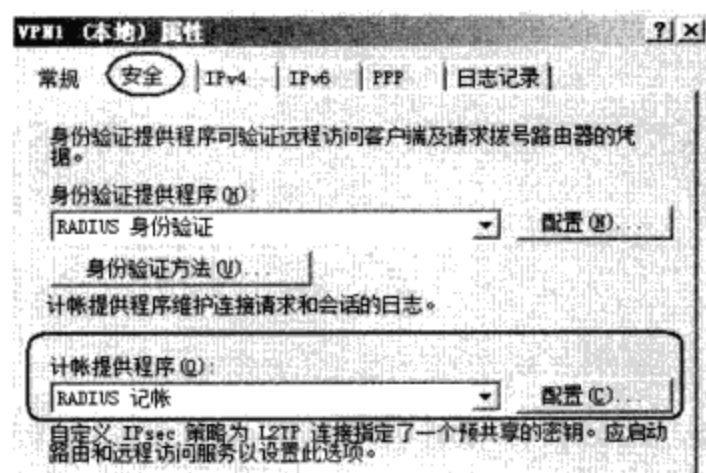


图 14-17

## 14-4 RADIUS代理服务器的设置

当远程访问服务器、VPN服务器或无线访问接入点等RADIUS客户端将用户的连接请求转发给NPS时，NPS是要扮演RADIUS服务器角色自行验证此连接请求，还是扮演RADIUS代理服务器角色来将验证工作传送给另外一台RADIUS服务器执行呢？它是通过**连接请求策略**（connection request policies）来决定的。NPS安装完成后，系统默认是将它设为RADIUS服务器。

### 14-4-1 连接请求策略

**连接请求策略**与**网络策略**有点类似，它也定义了一些条件，只要用户连接请求满足所定义的条件，就会以**连接请求策略**的设置，来决定是要让NPS自行验证此连接请求（此时NPS是RADIUS服务器），还是要将其转发给另外一台RADIUS服务器（此时NPS是 RADIUS 代理服务器）。NPS已经有一个内置的**连接请求策略**，如图 14-18所示。

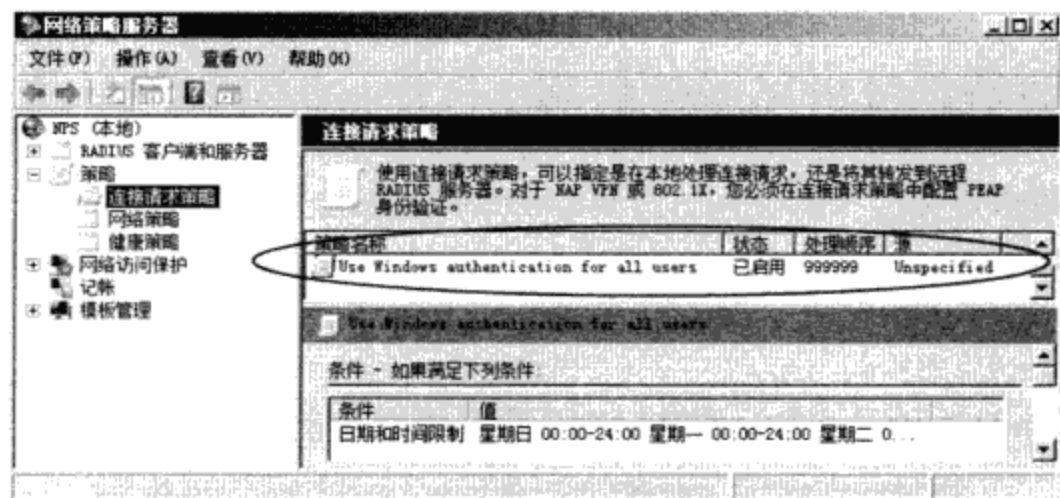


图 14-18

双击此策略，可通过图 14-19中的**条件**标签来看出此策略的条件是“一个星期7天内任何一个时段都可连接”，因此所有连接请求都满足此条件。

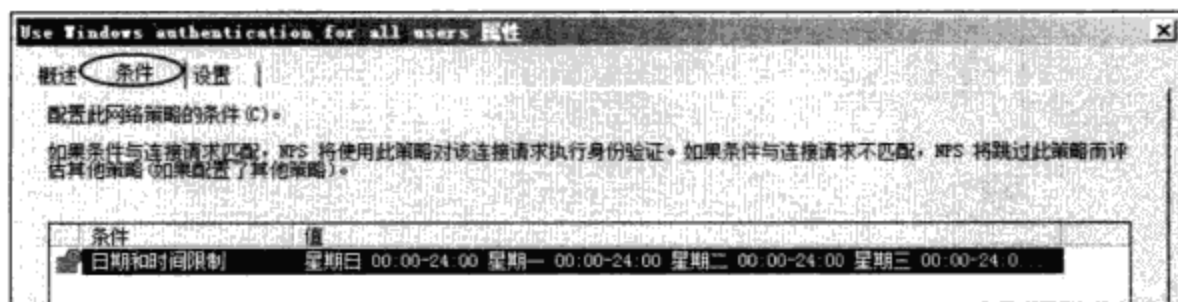


图 14-19

在单击图 14-20**设置**标签下的**验证**后，可看到以下的几个选项：

- 在此服务器上对请求进行身份验证：表示直接通过这台NPS来验证用户的连接请求，也就是将此服务器当作是RADIUS服务器来使用。这是默认值。

- **将请求转发到以下远程RADIUS服务器组进行身份验证：**也就是要让这台NPS来扮演RADIUS代理服务器的角色，它会将验证要求转发到所选择的RADIUS服务器组中的RADIUS服务器。您必须先创建RADIUS服务器组后才可以选择此选项（见下一节）。
- **不验证凭据就接受用户：**表示它既不验证用户身份，也不检查是否允许连接，而一律允许用户的连接请求。

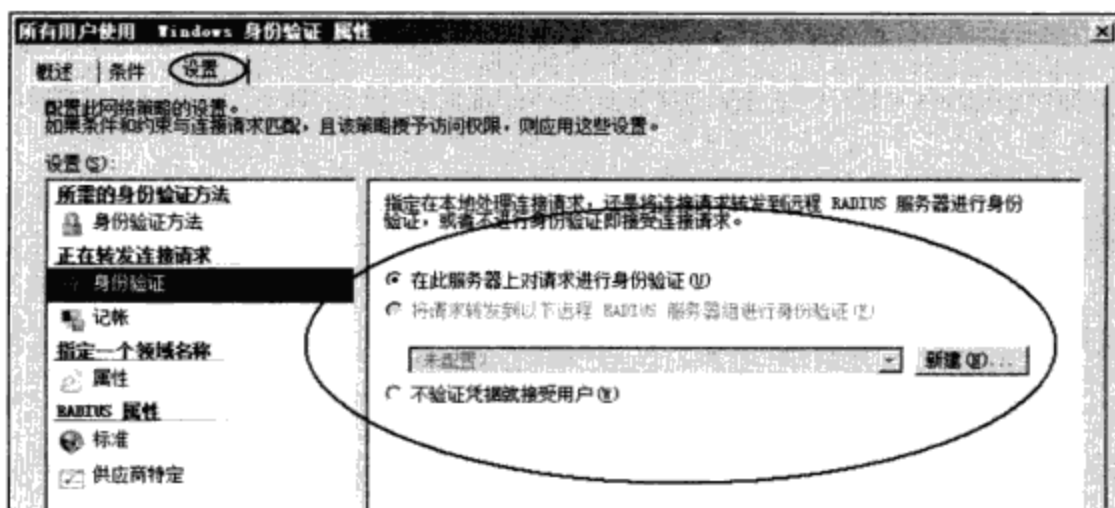


图 14-20

## 14-4-2 创建远程RADIUS服务器组

若要在**连接请求策略**内设置让NPS扮演RADIUS代理服务器角色的话，就需事先创建远程RADIUS服务器组，以便将验证要求转发给组中的RADIUS服务器。创建远程RADIUS服务器组的步骤如下。

**STEP 1** 如图 14-21所示【对着**远程RADIUS服务器组**单击右键➤新建】。

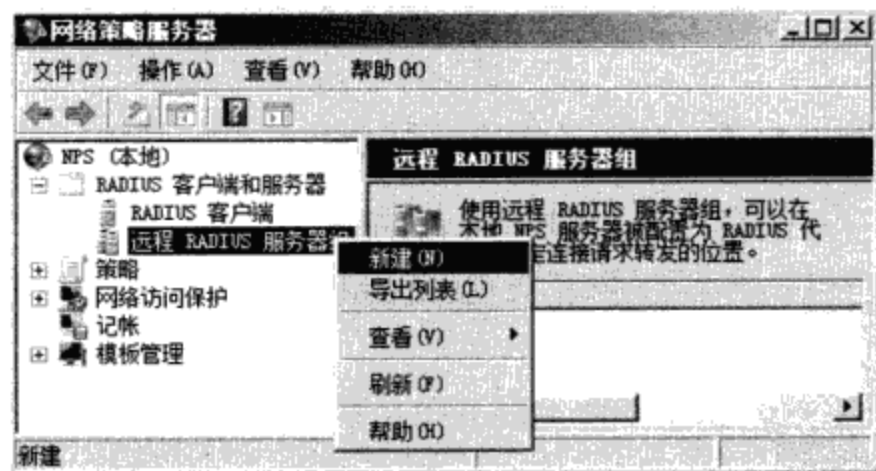


图 14-21

**STEP 2** 在图 14-22中输入一个组名（例如Group1），单击**添加**，然后输入要加入组的RADIUS服务器的主机名或IP地址，单击**确定**。若输入主机名的话，请先单击**验证**来查看是否可解析其IP地址。



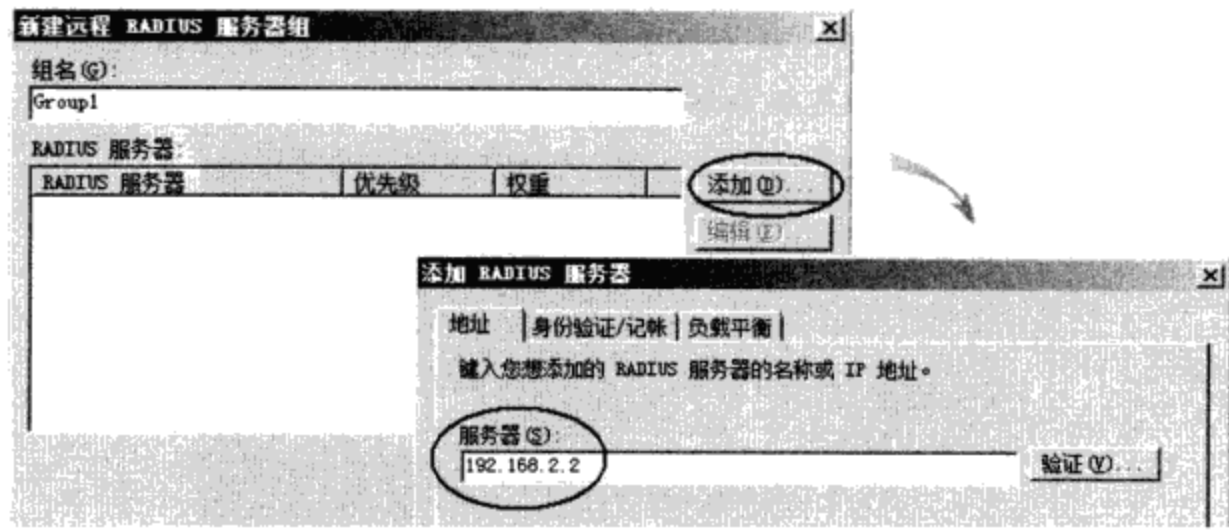


图 14-22

**STEP 3** 您可以继续单击**添加**来将其他RADIUS服务器加入到此组。

### 14-4-3 修改RADIUS服务器组的设置

若要修改RADIUS服务器组内某台RADIUS服务器的设置的话，请【如图 14-23所示双击RADIUS服务器组（例如Group1）➡双击要修改的RADIUS服务器（例如192.168.2.2）】，之后就可以修改此服务器的以下设置值：

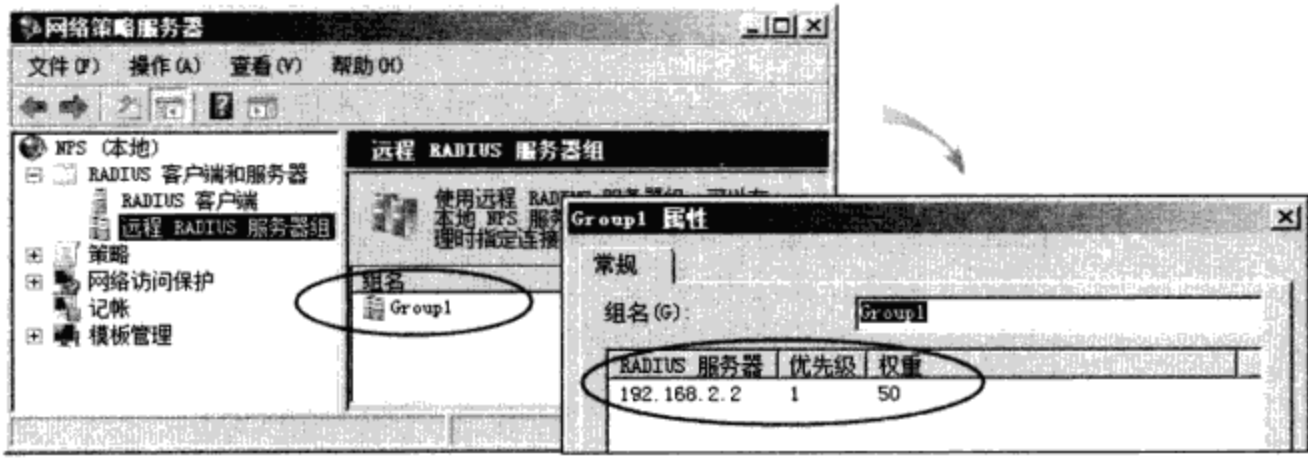


图 14-23

➤ **地址：**如图 14-24所示可更改RADIUS服务器的IP地址。

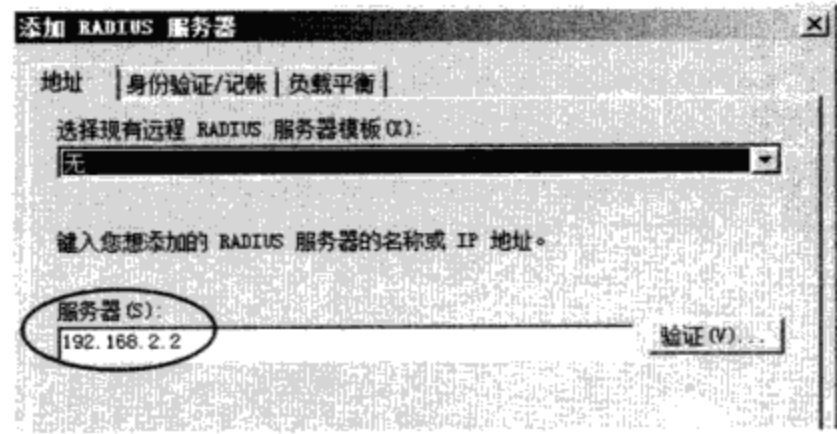


图 14-24



- **身份验证/记帐:** 如图 14-25所示可更改用来连接RADIUS服务器的端口与共享密码, 注意此设置必须与RADIUS服务器端的设置相同。

图 14-25

- **负载均衡:** 如图 14-26所示, 每一台RADIUS服务器都有其优先级, RADIUS代理服务器将连接请求转发给优先级较高的RADIUS服务器的频率, 会比优先级较低的RADIUS服务器来得频繁。优先级的数字为1表示优先级最高。若优先级相同, 则以权重(weight)来决定, 权重越高, 频率越高。

图 14-26