# 实验一

# 中小型企业域网络构建综合实验

本实验以把一个典型的中型企业工作组网络（节点数小于 254）改造为 Windows Server 2003 域网络为例，介绍中型 Windows Server 2003 域网络的组建方法。这是许多初级网管人员进入一个中小型企业上班后首先会遇到的一个实际技能考验。本示例包括这类域网络组建的各个主要方面，按照本实验的配置思路和步骤就可以很轻松地组建一个中小型企业域网络。

# 1.1 实验项目简介

本实验是一个综合的中型 Windows Server 2003 域网络组建与配置实验，贯穿整个域网络的组建与配置过程，包括域控制器、DNS、DHCP 服务器的安装与配置、WLAN 客户端的网络连接配置、客户端的域网络加入配置，OU、域用户和组账户的添加与配置等方面。其目的就是为了让大家熟练掌握域网络构建过程中的配置方法，这对于还没有实际域网络组建经验的广大大学毕业生和准网管来非常有意义。只要跟从本实验中介绍的步骤一步步操作，即可轻松完成一个实际中等规模域网络的构建任务。本实验完全可以在虚拟机网络中进行。

## 1.1.1 实验环境与要求

本实验项目中的网络拓扑结构如图 1-1 所示。具体网络实验环境和部署要求如下所述：

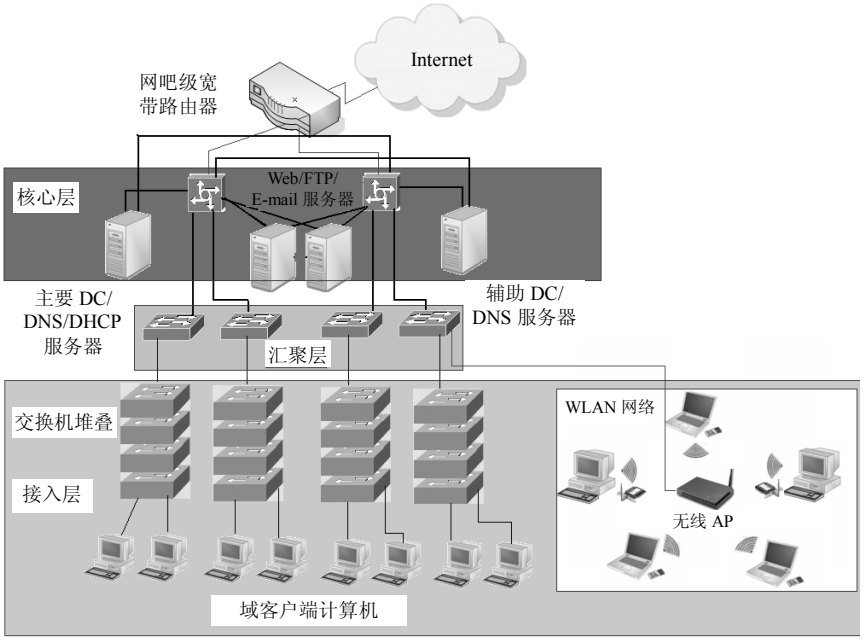



图 1-1 网络实验拓扑结构

- 整个网络结构分为核心层、汇聚层和接入层，共三层。整个域网络通过一个网吧级宽带路由器接入互联网，实现授权用户的互联网访问。
- 两台 Windows Server 2003 SP2（服务器系统另外购置）域控制器（DC），分别担当主域控制器和额外域控制器；两台 DNS 服务器分别集成安装在两台 DC 上，分别担当主要 DNS 服务器和辅助 DNS 服务器；一台 DHCP 服务器安装在主域控制器之上。
- DC（集成 DNS 和 DHCP 服务器）、Web/FTP 服务器、E-mail 服务器与两台核心层交换机采用双线冗余连接。当然这要求在交换机上配置 STP 协议，以防形成环路。接入层采用堆叠式交换机，以实现端口扩展和单交换机性能的提高。有关冗余连接、STP 和交换机堆叠等方面的配置将在中级认证教材中介绍。

- 在域网络中有部分用户是采用带 AP 的基础结构 WLAN 网络连接，并通过有线方式把 AP 与有线以太网连接。各 WLAN 用户采用比较安全的 WPA2-PSK（Wi-Fi Protected Access-2 Preshared Key，Wi-Fi 保护访问 2 预共享密钥）安全认证方式。
- 在域控制器中按部门创建组织单位（OU）和各 OU 下的员工用户账户。本实验中要创建的 OU 包括生产部、工程部、质管部、财务部、市场部、人事部和行政部。为有需要的 OU 配置独自的组策略。
- 客户端系统包括 Windows 2000 Professional、Windows XP Professional、Windows Vista 操作系统。
- 按统一 DNS 名称空间为各域网络客户端计算机和各服务器规划计算机名称和用户账户名称。

【说明】本实验仅介绍域网络构建的相关内容，不涉及到交换机和宽带路由器网络设备配置，以及像 Web、FTP 和 E-mail 应用服务器的配置。交换机的配置将在中级认证教材中介绍；网吧级宽带路由器的配置参见助理级教材《金牌网管师——网吧网管》一书；应用服务器的配置参见本级认证教材《金牌网管师——中小型企业网络组建、配置与管理》一书。

### 1.1.2 实验目的

通过本实验学员要达到以下目的：

- 熟练掌握单域网络中域控制器、额外域控制器、DNS 服务器和 DHCP 服务器的安装方法
- 熟练掌握基于 AP 的基础结构 WLAN 构建配置方法
- 熟练掌握 DNS 服务器正反向主要/辅助查找区域的创建与配置方法
- 熟练掌握 DNS 服务器及查找区域属性配置方法，并深入理解各主 DNS 记录的用途和配置方法
- 熟练掌握 DHCP 服务器作用域的创建，以及 DHCP 服务器的属性配置方法
- 熟练掌握各种主流 Windows 系统客户端域网络的加入配置方法
- 熟练掌握通过 ldifde.exe 命令实现域用户账户批量导入的方法
- 熟练掌握各种类型域组账户的创建与属性配置方法

## 1.2 网络实验项目规划

在正式构建域网络前，建议先对整个域网络的结构、名称空间、服务器类型、数量及安置位置，以及网络 IP 地址等进行细致的规划。

### 1.2.1 实验项目名称规划

本实验所用域名为 test.com。本实验采用的名称规则是根据计算机和用户账户的 NetBIOS 名称进行规划的，完全合格的域名格式只需在 NetBIOS 名称后面加上域名后缀即可。以下是本实验采用的命名规则，但这并不是唯一的，也没有硬性规则，只要自己认为更便于管理就行了。不同公司可以有不同的命名规则，但建议以统一的名称格式进行规

划，以便识别和管理。

- 客户机名称规划

在本实验中，客户端计算机名以“test-w *用户计算机编号*”格式进行统一命名。其中的 test 代表域名的 NetBIOS 名称；用户计算机编号为 3 位编码（因为节点数超过 100）。如 test-w010，代表编号为 10 的用户计算机。

各服务器计算机的命名规则如下：

- 域控制器名称规划

如果是域控制器（DC），则计算机命名规则为以“test-DC *序号*”的格式进行统一命名。其中 DC 代表该服务器为域控制器，“序号”为 1 位编码（因为一般中小型公司不会有超过 10 台 DC 的）。如 test-DC1，代表第一台域控制器，test-DC2 代表第二台域控制器。本实验配置了一台主 DC、一台额外 DC。

- 独立网络服务器名称规则

如果网络服务器是独立的成员服务器，如独立 DNS 服务器、DHCP 服务器，则计算机命名规则为“test-DNS *序号*”、“test-DHCP *序号*”，或者直接以“DNS *序号*”、“DHCP *序号*”格式进行命名，“序号”也为 1 位编码（因为一般中小型公司不会有超过 10 台 DNS 或者 DHCP 服务器的）。本实验配置了两台 DNS 服务器，一台 DHCP 服务器，但 DNS 和 DHCP 服务器都是与 DC 在一起的，所以无需单独命名。

- 应用服务器名称规划

如果是应用服务器，如 Web、FTP 或者 E-mail 服务器，则计算机命名规则为“test-WEB *序号*”、“test-FTP *序号*”、“test-MAIL *序号*”，或者直接以“WEB *序号*”、“FTP *序号*”、“MAIL *序号*”格式进行命名，“序号”也为 1 位编码（因为一般中小型公司不会有超过 10 台这类应用服务器的）。如果公司网络无需独立的应用服务器（如几台应用服务器共同安装在一台成员服务器上），则可以用一个通用名称进行命名，如 AppServer，表示应用服务器（本实验采用这种命名方式），然后在各具体的应用服务器中再配置对应的应用服务器的服务器标识，在 DNS 服务器上添加对应的资源记录即可。

- 用户账户名称规划

出于安全性考虑，网络中各员工的用户账户名称不直接采用中文名称，而采用英文名称，但 OU 名称全部采用中文命名，直接对应部门名。

### 1.2.2 实验项目 IP 地址规划

在本实验的网络中，网络节点数少于 254 个，所以可以直接用一个 C 类 IP 地址段进行 IP 地址分配。本实验采用 192.168.1.0 网段。

在本实验项目中，有两个 DC、两个 DNS 和一个 DHCP 服务器，而且两个 DNS 服务器是分别安装在两台 DC 上的，一个 DHCP 服务器是安装在主域控制器（test-DC1）上面的。另外，网络还将配置专门的一台 Web/FTP 服务器、一台 E-mail 邮件服务器。由此可以推算出本实验项目中所具有的服务器 IP 地址配置：

- 两个 DC、两个 DNS 和一个 DHCP 服务器对应的是两台物理服务器，只需要两个 IP 地址即可。因为网络中通常第一个 IP 地址为网关 IP 地址，所以需要从第二个 IP 地址开始分配。在此为两个 DC 分配的 IP 地址分别为 192.168.1.2 和 192.168.1.3。
- Web、FTP 和 E-mail 服务器各自至少要分配一个 IP 地址，对应的 IP 地址分别为 192.168.1.4、192.168.1.5 和 192.168.1.6。这些应用服务器的具体配置方法将参见

本级认证教材《金牌网管师——中小型企业网络组建、配置与管理》一书。

- 为了方便以后服务器的扩展，在此预留一部分 IP 地址（192.168.1.7～192.168.1.10，192.168.1.10 用于分配给 WLAN AP）不分配给客户端。同时为了减轻管理员的 IP 地址配置负担，网络中采用 DHCP 服务器为客户计算机自动分配 IP 地址。DHCP 服务器 IP 地址池为 192.168.1.11～192.168.1.254。排除规划用于 WLAN 用户的 IP 地址段 192.168.1.30～192.168.1.50。
- 在 WLAN AP 上配置 DHCP 服务器，IP 地址池为 192.168.1.30～192.168.1.50。

至于各服务器和客户机的 IP 地址配置方法相信大家都知道，所以在此不作具体介绍。

# 1.3 安装域控制器

在本实验中，安装了两台域控制器，域的名称为 test.com，主域控制器规划的计算机名称为 test-DC1.test.com，额外域控制器规划的计算机名称为 test-DC2.test.com。主域控制器的安装通常是通过第一台服务器的安装而安装的。这里的“第一台”服务器不仅是指第一台域控制器（主域控制器），会同时安装第一台 DNS 服务器（主要 DNS 服务器）和 DHCP 服务器。第二台 DNS 服务器（辅助 DNS 服务器）安装在额外域控制器（test-DC2.test.com）上。

## 1.3.1 修改域控制器计算机名称

因为在工作组网络中的计算机名称可能没有按照现在域网络的命名规则进行命名，所以在组建域网络前需要首先对域网络中的计算机（包括网络中的所有计算机）名称进行重新修改。尽管包括域控制器在内的所有计算机都可以在配置好域网络后再进行修改，但那样可能会造成 DNS 记录混乱，建议事先进行全面修改。

在此以用于担当 Windows Server 2003 域控制器的计算机名称修改为例进行介绍。具体步骤如下：

（1）在 Windows Server 2003 成员服务器上执行【开始】→【控制面板】→【系统】菜单操作，或者在“开始”菜单→“我的电脑”菜单项上右击，在弹出的菜单中选择“属性”选项，然后再在打开的对话框中选择“计算机名”选项卡，如图 1-2 所示。从中可以看出，一开始的计算机名称并不规范。同时可以在“计算机描述”文本框中输入对计算机的描述，如“此为主域控制器”之类的文字。当然也可以不输入描述。

（2）单击“更改”按钮，打开如图 1-3 所示对话框。在“计算机名”文本框中输入域控制器的 NetBIOS 名称，如主域控制器的计算机名为 test-DC1，如果是修改额外域控制器的计算机名，则要填入 test-DC2。

（3）单击“其他”按钮，打开如图 1-4 所示对话框。在这里可以先为域控制器计算机名称配置完全域名格式的域名后缀（DNS 后缀），如本实验中的域名为 test.com。“在域成员身份变化时，更改主 DNS 后缀”复选项对于域控制器来说则随便了，但最好选上，因为这样以后如果发生域名更改后，计算机名称的 DNS 后缀会自动更改。

（4）两次单击“确定”按钮，返回到图 1-2 所示对话框中。此时会弹出如图 1-5 所示的提示框，提示说要使设置更改生效，必须重启计算机。

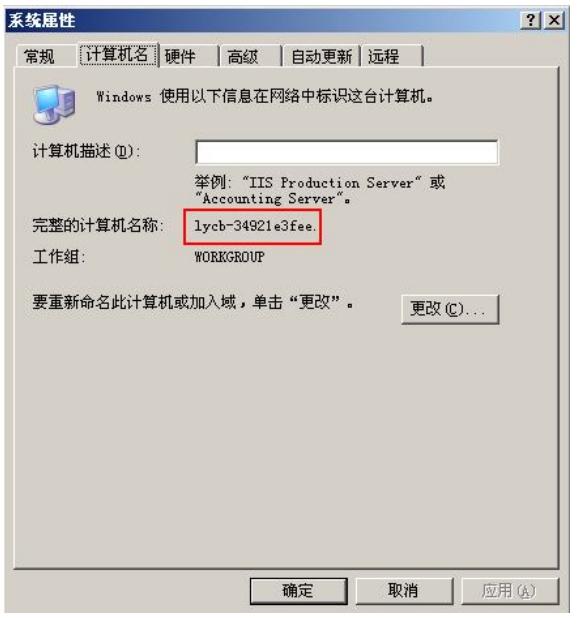



图 1-2　用于担当主域控制器的计算机的“系统属性”对话框之“计算机名”选项卡

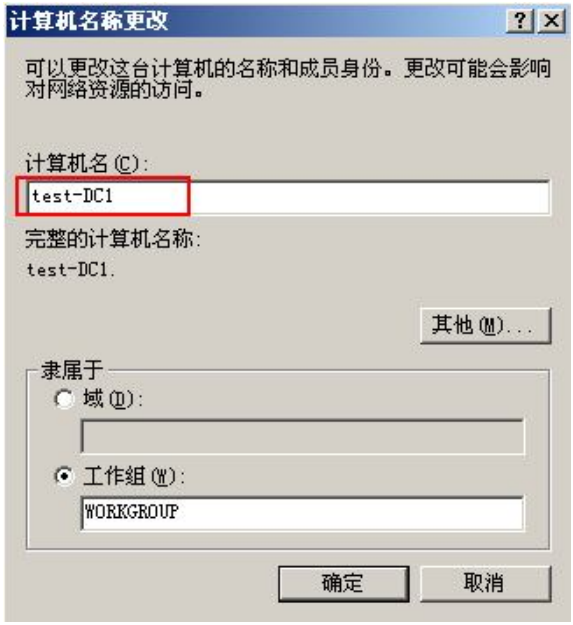



图 1-3　“计算机名称更改”对话框


图 1-4　“DNS 后缀和 NetBIOS 计算机名”对话框


图 1-5 “计算机名更改”对话框

（5）单击图 1-5 所示提示框中的“确定”按钮，再次返回到图 1-2 所示对话框。再单击图 1-2 所示对话框中的“确定”按钮，系统又弹出如图 1-6 所示对话框。再次提示要使设置生效，需要重启计算机，并询问是否现在重启计算机。单击“是”按钮后即自动重启计算机。

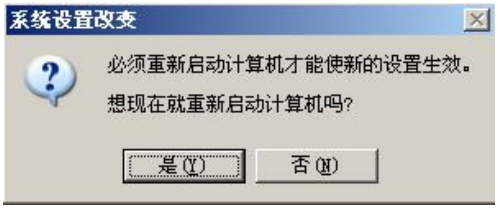



图 1-6 “系统设置改变”对话框

（6）重启计算机后，再打开如图 1-2 所示对话框就可以发现计算机名已按要求更改了，如图 1-7 所示。用于担当主域控制器计算机的完全合格 DNS 域名格式为 test-DC1.test.com，对应的 NetBIOS 名称为 test-DC1。

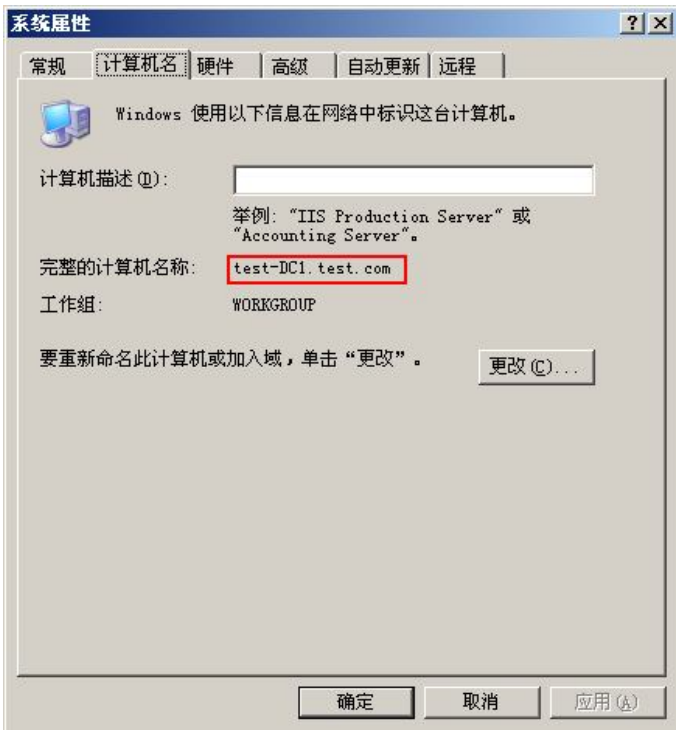



图 1-7 更改用于担当主域控制器的计算机名后的“计算机名”选项卡

用以上介绍的相同方法修改用于担当额外域控制器的 Windows Server 2003 服务器的计算机名称为 test-DC2.test.com，如图 1-8 所示。用于担当额外域控制器的完全合格 DNS 域名格式为 test-DC2.test.com，对应的 NetBIOS 名称为 test-DC2。

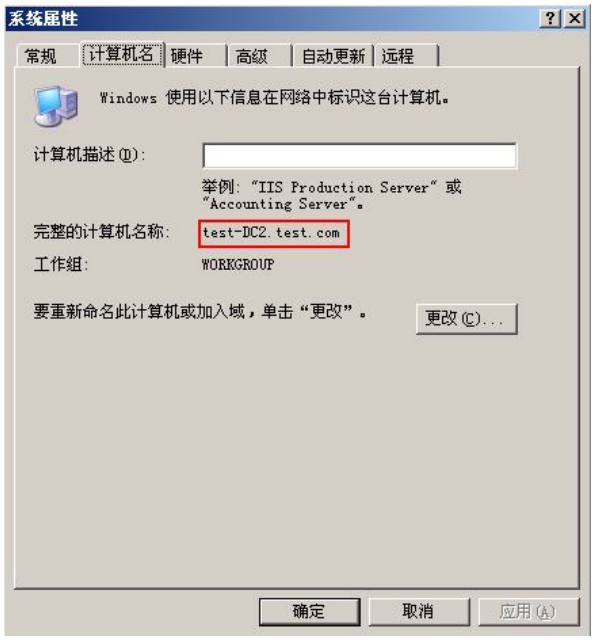



图 1-8　更改用于担当额外域控制器的计算机名后的“计算机名”选项卡

## 1.3.2　安装第一台服务器

第一台域控制器通常选择以第一台服务器方式进行安装，这样做的好处就是会在安装第一台域控制器（主域控制器）的同时自动在主域控制器上集成安装第一台 DNS 和 DHCP 服务器，而无需另外再额外安装第一台 DNS 服务器和 DHCP 服务器，这特别适用于中小型企业网络，因为这类企业中，网络规模不大，用户不多，应用也不会很复杂，所以一般不会单独用一台成员服务器来安装像 DNS 或者 DHCP 这样的网络服务器。

下面是第一台服务器的具体安装步骤（在 test-DC1 服务器上进行操作）。

（1）执行【开始】→【管理工具】→【管理您的服务器】菜单操作，打开如图 1-9 所示窗口。因为该服务器是新安装的 Windows Server 2003 独立服务器，没有配置任何服务器角色，所以在窗口中显示没有添加角色到此服务器。


图 1-9　“管理您的服务器”窗口

（2）单击右上角的“添加或删除角色”按钮，或者执行【开始】→【管理工具】→【配置您的服务器向导】菜单操作，在打开的向导首页对话框中单击“下一步”按钮，都会打开如图 1-10 所示对话框。

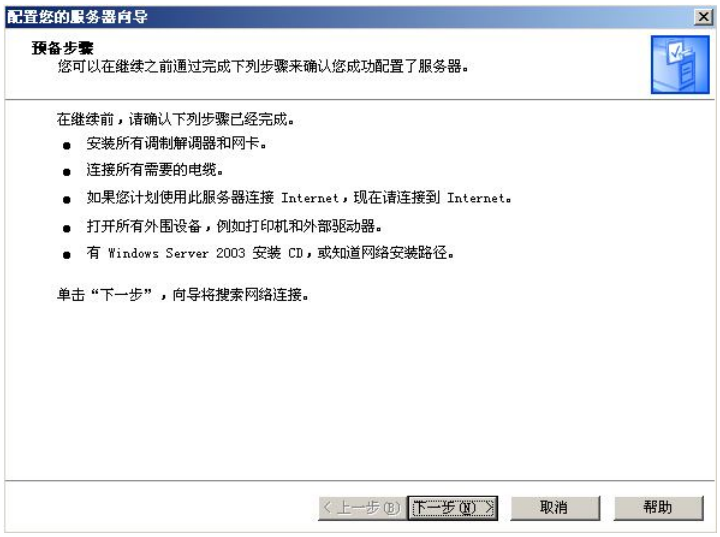



图 1-10　“预备步骤”对话框

（3）单击“下一步”按钮，系统首先检测服务器当前网络设置（主要是检查网络连接设置）是否满足向导运行的条件。检测完成，符合第一台服务器安装的条件时，会打开如图 1-11 所示对话框。在其中有“第一台服务器的典型配置”选项，专门用于运行第一台服务器安装向导，这样就可以一次性安装第一台域控制器、第一台 DNS 服务器和第一台 DHCP 服务器。至于运行第一台服务器安装向导的条件参见本级认证教程的《金牌网管师——中小型企业网络组建、配置与管理》一书。

在此选择“第一台服务器的典型配置”单选项。

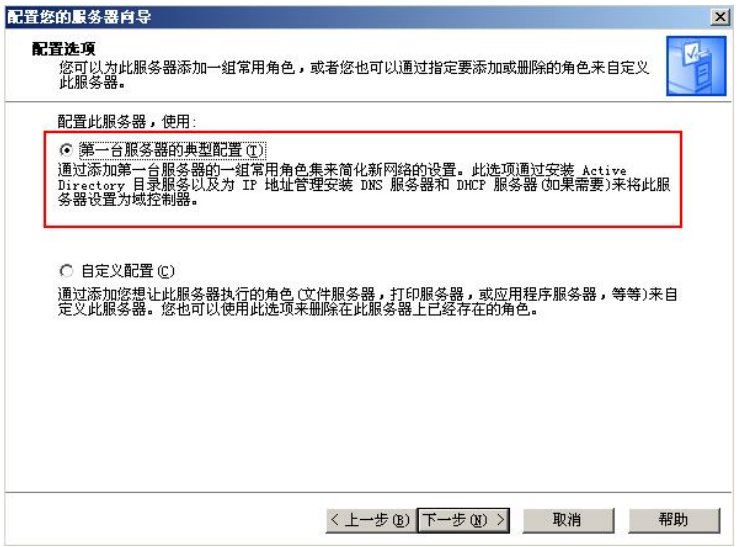



图 1-11　“配置选项”对话框

【说明】如果选择了“自定义配置”单选项，则可以打开直接选择安装单一服务器角色的对话框。这时就可以单独安装域控制器（DC）、DNS 服务器、DHCP 服务器等，而不会一次性安装第一台域控制器、第一台 DNS 服务器和第一台 DHCP 服务器这三种服务器角色。

（4）单击“下一步”按钮，打开如图 1-12 所示对话框。在“Active Directory 域名”（也就是 DNS 域名）文本框中输入本实验中域网络的域名 test.com。

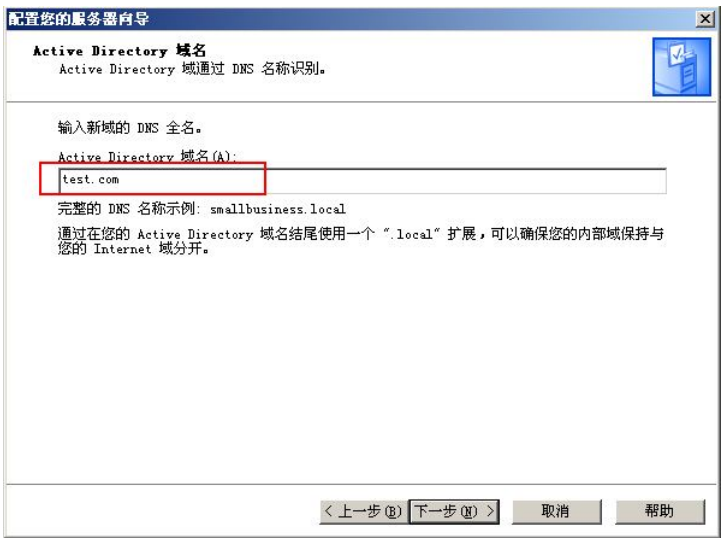



图 1-12 “Active Directory 域名”对话框

（5）单击“下一步”按钮，打开如图 1-13 所示对话框。在这里系统会自动在“NetBIOS 域名”文本框中显示上步配置的 DNS 域名对应的 NetBIOS 域名。默认是取 DNS 域名第一个小圆点前面部分的名称大写（本实验中为 TEST）。当然这里的 NetBIOS 域名也可以不按默认设置，改为与 DNS 域名完全不一样的名称。但一般不建议这么设置，直接按系统的自动配置即可。有关 DNS 域名和 NetBIOS 的区别请参见本级认证教程的《金牌网管师——中小型企业网络组建、配置与管理》一书。

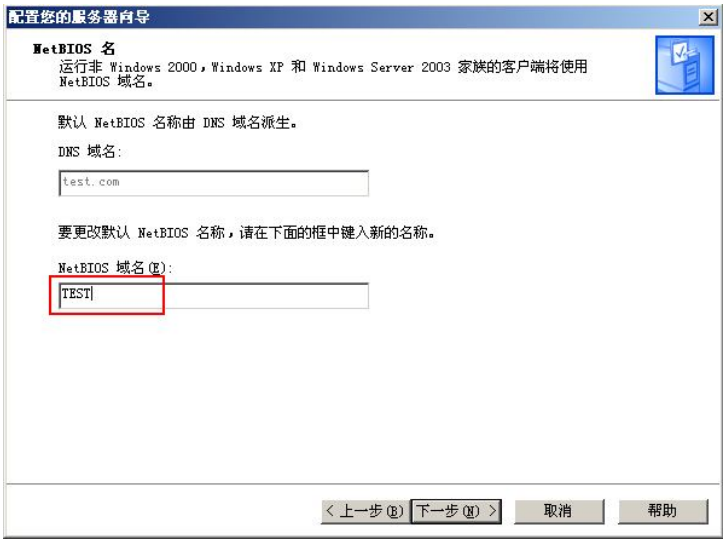



图 1-13 “NetBIOS 名”对话框

（6）单击“下一步”按钮，打开如图 1-14 所示对话框。在这个对话框中可以设置当在安装第一台服务器过程中自动安装的 DNS 服务器接收到不能解析的域名解析请求时，允许把请求转发到指定的 DNS 服务器上进行解析。这主要是考虑到域网络用户还要进行互联网访问或者外网连接的情形。这时就可以把 ISP 提供的 DNS 服务器地址填在“是，将查询转发到 IP 地址如下的 DNS 服务器”单选项下的文本框中。这样一来，局域网中的用户，

无论是内部查询请求还是外部互联网应用查询请求都可以得到支持，不会出现访问不了互联网，打不开网页的故障。

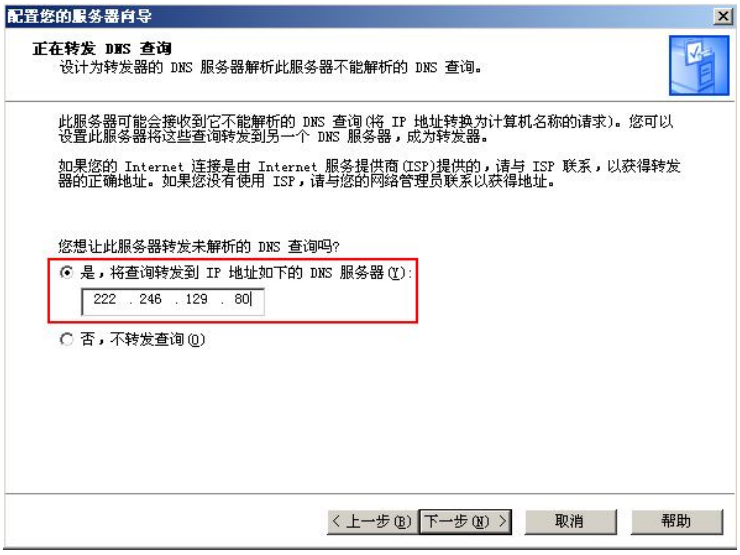



图 1-14　“正在转发 DNS 查询”对话框

（7）单击“下一步”按钮，打开如图 1-15 所示对话框。在其中的“总结”列表框中显示了以上各步的配置选择。这也是本次安装第一台服务器的基本配置任务。

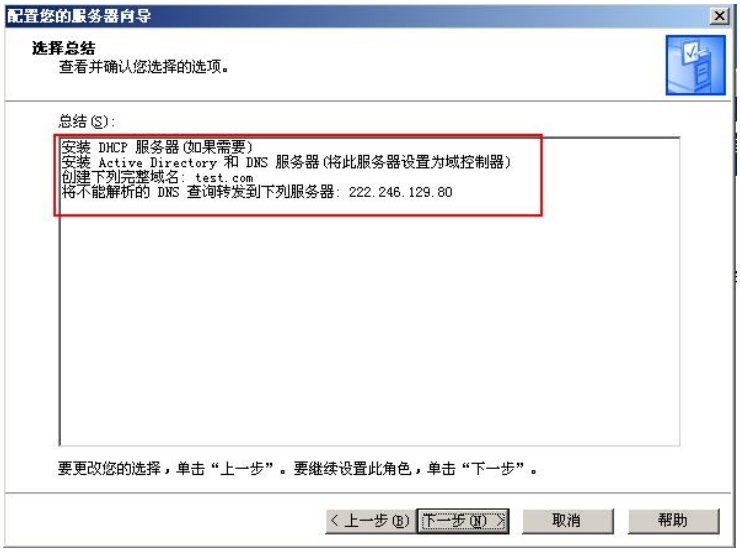



图 1-15　“选择总结”对话框

（8）确认上述配置任务无误后，单击“下一步”按钮，系统首先弹出打开如图 1-16 所示提示框。提示在安装第一台服务器的过程中会自动重启计算机，所以在正式进行配置前最好关闭所有应用程序，以免数据丢失。


图 1-16　安装过程需要重启动计算机的提示框

（9）确认可以正式进行第一台服务器安装后，单击“确定”按钮，即开始安装所需的组件。然后进行活动目录安装，如图 1-17 所示。在安装过程中可能会提示打开 Windows Server 2003 SP2 第一张 CD 中的 i386 目录选择需要复制的文件，如图 1-18 所示。


图 1-17　安装活动目录进程对话框

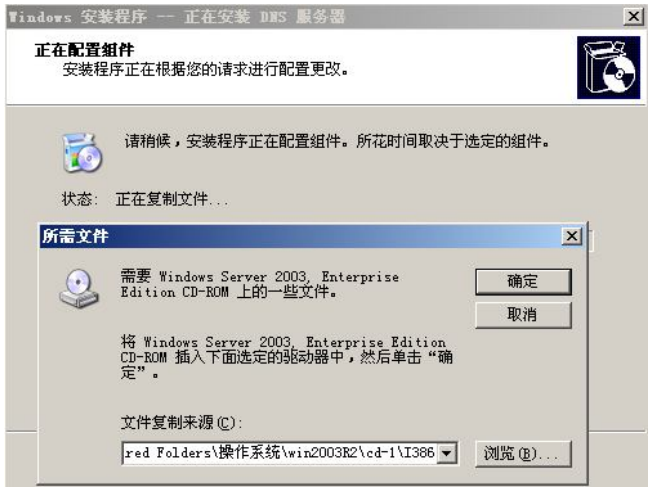



图 1-18　选择需复制的文件位置对话框

（10）选择好后系统会继续安装，复制所需的组件文件，进程对话框如图 1-19 所示。复制完成后，系统会自动重新启动。


图 1-19　“正在配置组件”对话框

重启计算机后，系统会继续进行后面的安装、配置，完成后显示如图 1-20 所示对话框。最上面的“指派静态 IP 地址”项之所以显示的是红色的“-”号，而不是绿色的“√”，是因为这台服务器在正式运行第一台服务器安装向导之前已指定了静态 IP 地址。也可以在运行向导前不为服务器指定静态 IP 地址，但这时它直接指派的是 192.168.0.1 这个 IP 地址，可能与网络的 IP 规划不一致。

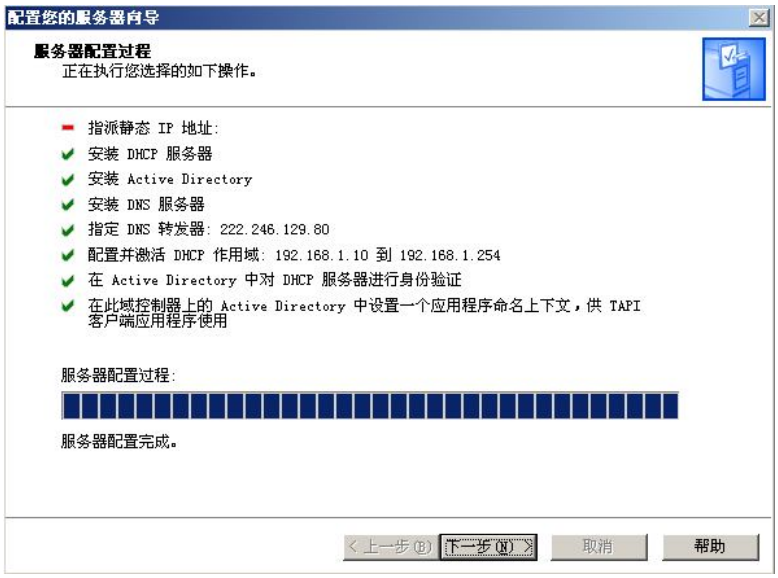



图 1-20　第一台服务器配置过程对话框

（11）在图 1-20 所示对话框中单击“下一步”按钮，打开如图 1-21 所示向导完成对话框，提示这台服务器已配置好。单击“完成”按钮，打开如图 1-22 所示“管理您的服务器”窗口，从中可以见到，此时服务器已具有三重角色了：域控制器、DNS 服务器、DHCP 服务器。


图 1-21　“此服务器现在已配置好”对话框

同时，会在“管理工具”菜单中自动生成对应的管理控制台快捷菜单，如图 1-23 所示。这些管理控制台的具体配置与使用将在本实验后面依次介绍。


图 1-22　运行第一台服务器安装向导后安装的三种服务器角色

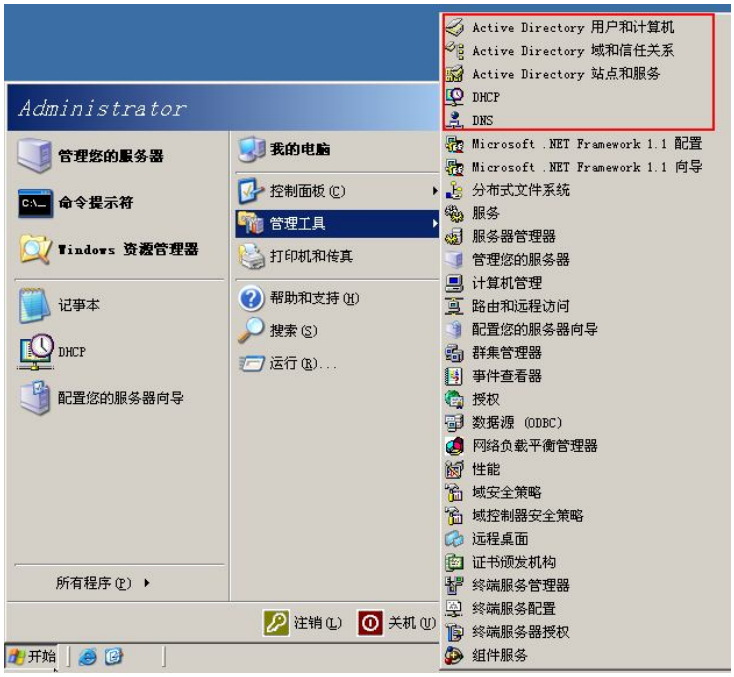



图 1-23　安装第一台服务器后自动生成的管理控制台快捷菜单

### 1.3.3　安装额外域控制器

在安装了第一台域控制器、第一台 DNS 服务器和 DHCP 服务器（这 3 种服务器角色如果是采用上节介绍的第一台服务器安装向导进行安装的，则它们都是集成在一台服务器上的）后，如果公司网络出于安全或者性能要求需要安装另外一台 Windows Server 2003 SP2 额外域控制器时，就需要利用 Windows Server 2003 SP2 独立服务器进行额外域控制器安装了。本实验是在前面配置的 test-DC2 独立服务器上进行额外域控制器安装的。又因为本实验与主域控制器位于相同的本地局域网中，不需要同时安装 DHCP 服务器，所以采用常规的额外域控制器安装方法（不能采用上节介绍的安装第一台服务器的方法）。具体步骤如下：

（1）在 test-DC2 独立服务器上配置好 IP 地址和 DNS 服务器地址。IP 地址按照前面的规划设置为 192.168.1.3，首选 DNS 服务器 IP 地址为上节安装的第一台 DNS 服务器地址。因为它是与第一台域控制器安装在同一台计算机中，所以首选 DNS 服务器的 IP 地址就是第一台域控制器的 IP 地址——192.168.1.2。具体配置如图 1-24 所示。

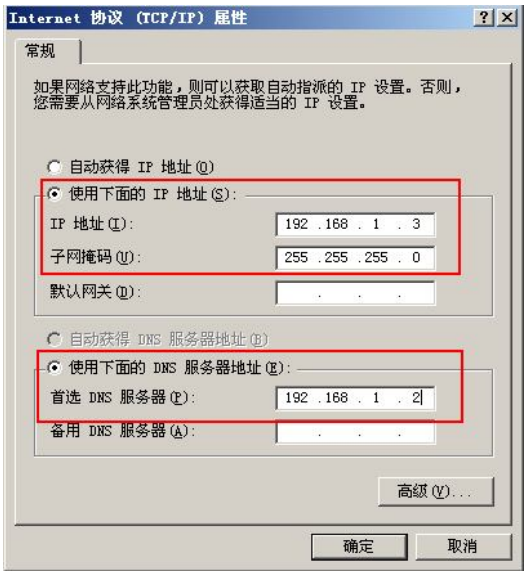



图 1-24　额外域控制器的 IP 地址和首选 DNS 服务器地址的配置

【注意】额外域控制器以及其他服务器和客户机的 IP 地址必须与第一台域控制器的 IP 地址在同一网段，额外域控制器的首选 DNS 服务器地址也必须指向网络中上节安装的第一台 DNS 服务器的 IP 地址，因为在安装额外域控制器时需要 DNS 服务器进行域名解析，否则就联系不上第一台域控制器，造成额外域控制器安装不了。在其他服务器和客户机加入域网络时也要注意这一点，当然这时选择的 DNS 服务器还可以是当前域中的其他 DNS 服务器。

从下步开始，其实也就是在图 1-11 中选择了“自定义配置”单选项后所进行的步骤。

（2）执行【开始】→【管理工具】→【配置您的服务器向导】菜单操作，打开如图 1-25 所示向导首页对话框。


图 1-25　“欢迎使用‘配置您的服务器向导’”对话框

（3）单击“下一步”按钮，打开如图 1-26 所示对话框。在这里列出了在运行该向导前先要做好的准备工作。

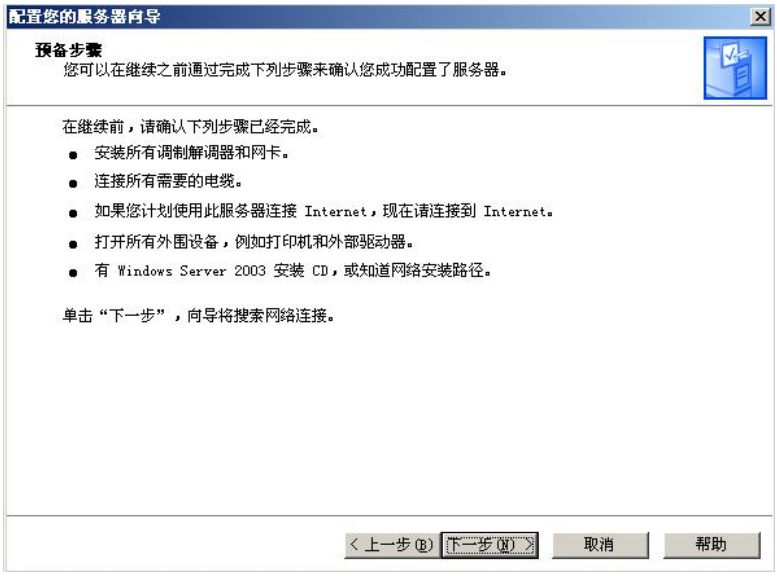



图 1-26 “预备步骤”对话框

（4）确认所有准备工作都做好后，单击“下一步”按钮，打开如图 1-27 所示对话框。在这里列出了当前 Windows Server 2003 系统中可以安装或者删除的所有服务器角色（服务器着色的安装与删除操作都可以通过这个向导进行），如文件服务器、域控制器、DNS 服务器、DHCP 服务器、WINS 服务器、IIS 应用服务器、流媒体服务器、POP3 服务器等。本节要安装的是额外域控制器，所以选择“域控制器（Active Directory）”选项，当然必须是当前服务器没有安装相应的服务器，否则执行向导就成了删除所选角色的服务器操作了。

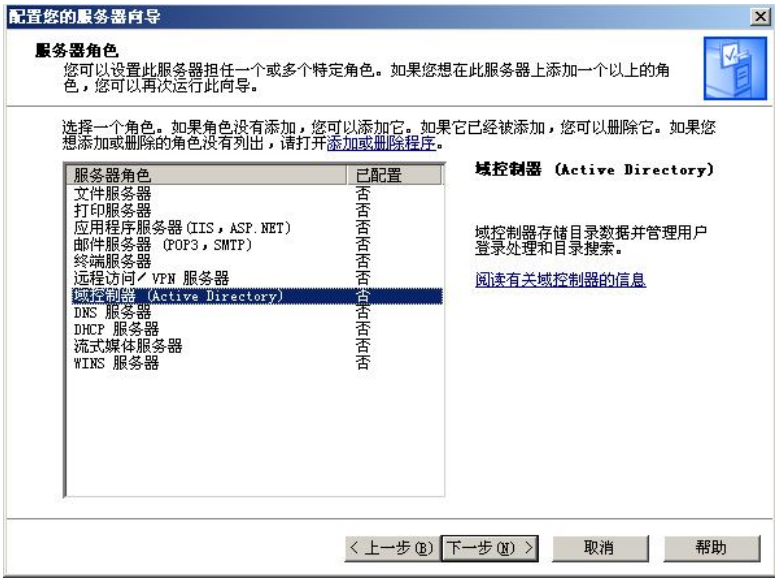



图 1-27 “服务器角色”对话框

（5）单击“下一步”按钮，打开如图 1-28 所示对话框。在这里列出了本次向导操作的任务摘要。如本次操作是把当前服务器通过运行 Active Directory 向导配置成域控制器。

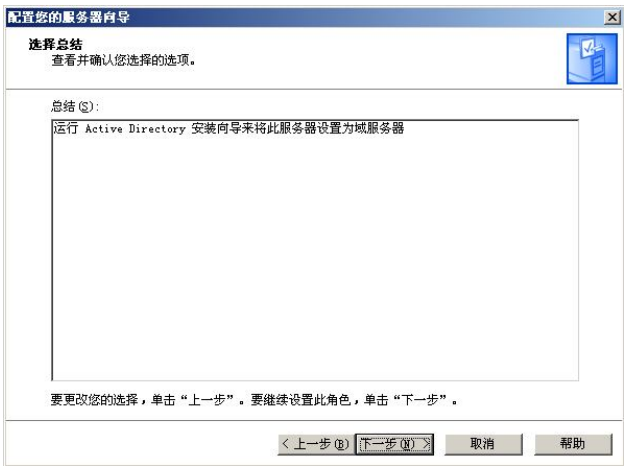



图 1-28　“选择总结”对话框

（6）单击“下一步”按钮，打开执行本次域控制器角色安装任务所需的 Active Directory 向导首页对话框，如图 1-29 所示。


图 1-29　“欢迎使用 Active Directory 安装向导”对话框

（7）单击“下一步”按钮，打开如图 1-30 所示对话框。在这里提示用户，由于 Windows Server 2003 系统改进的安全设置，所以最早期的 Windows 系统，如 Windows 95 和 Windows NT 4.0 不能再成为 Windows Server 2003 域成员了。但 Windows 98 系统可以。


图 1-30　“操作系统兼容性”对话框

（8）单击“下一步”按钮，打开如图 1-31 所示对话框，在这里要选择安装的域控制器类型。本节安装的是现有域 test.com 的额外域控制器，所以选择“现有域的额外域控制器”单选项。要注意这里的警告提示了，把这台服务器转换成额外域控制器后，本地的用户和组账户都将删除，这样所有加密的密钥（如 EFS 密钥）都将被删除，所以需要事先对加密文件用原有密钥进行解密，否则加密文件将永远打不开了。这一点要特别引起重视。

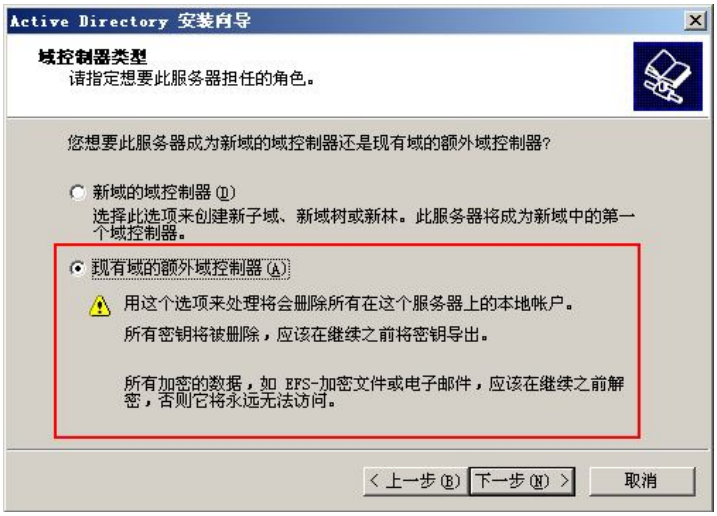



图 1-31 “域控制器类型”对话框

（9）单击“下一步”按钮，打开如图 1-32 所示对话框。在这里要输入有权把该台服务器转换成额外域控制器的用户账户信息。通常只需要使用现有域的域管理员账户 Administrator 即可。本实验的域名为 test.com。


图 1-32 “网络凭据”对话框

（10）单击“下一步”按钮，打开如图 1-33 所示对话框。在这里要输入把该服务器转换成额外域控制器所对应的域名。本实验为 test.com。

（11）单击“下一步”按钮，打开如图 1-34 所示对话框。在这里要指定 Active Directory 数据库和日志文件的存放位置，默认保存在系统文件夹下的 NTDS 文件夹下，而且一般按默认设置即可。如果要更改默认的存放位置，则一定要保证所选位置必须是 NTFS 文件格式的，而且文件夹名一定要是 NTDS，只是路径可以更改。

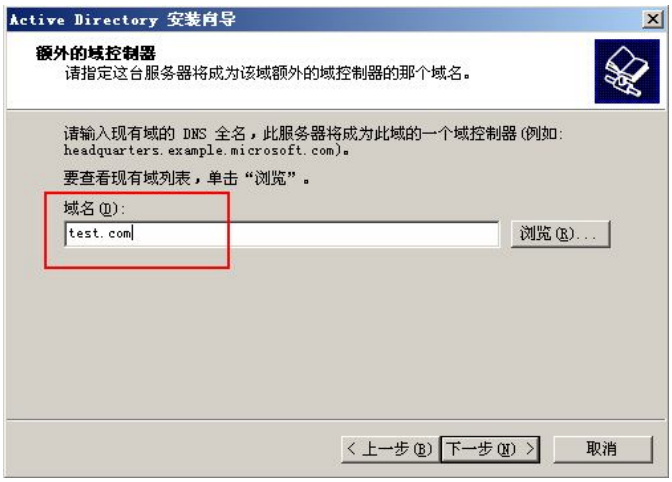



图 1-33　“额外的域控制器”对话框


图 1-34　“数据库和日志文件文件夹”对话框

（12）单击“下一步”按钮，打开如图 1-35 所示对话框。在这里要设置 Active Directory 公用文件夹 SYSVOL 的存储位置。这个文件夹也必须是在 NTFS 文件格式的卷中，而且在安装了域控制器后会自动设置为共享的，供域网络中其他域控制器相互复制 AD 数据。

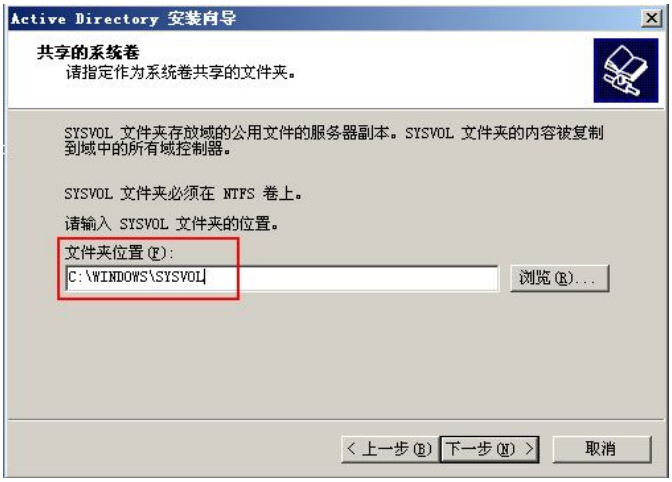



图 1-35　“共享的系统卷”对话框

（13）单击“下一步”按钮，打开如图 1-36 所示对话框。在这里为设置安装域控制器后以目录还原方式登录时的管理员密码。目录还原模式的管理员密码可以与域管理员密码不一样，而且是建议不一样。当然是出于对域管理员密码的安全保护角度考虑的。


图 1-36 “目录服务还原模式的管理员密码”对话框

只有安装了域控制器的服务器系统才有“目录还原方式”，是一种可用来还原域控制器活动目录的还原方式。在目录还原方式下，相当于把域控制器的活动目录功能去掉了，重新恢复为成员服务器状态，这样活动目录数据库就不会运行，进而达到恢复活动目录的目的。

**【说明】**如何使用目录还原方式恢复域控制器中的活动目录，请参见本级认证教材《金牌网管师——中小型企业网络组建、配置与管理》一书第 10 章。

（14）单击“下一步”按钮，打开如图 1-37 所示对话框。在这里显示了本次活动目录安装任务的配置摘要。

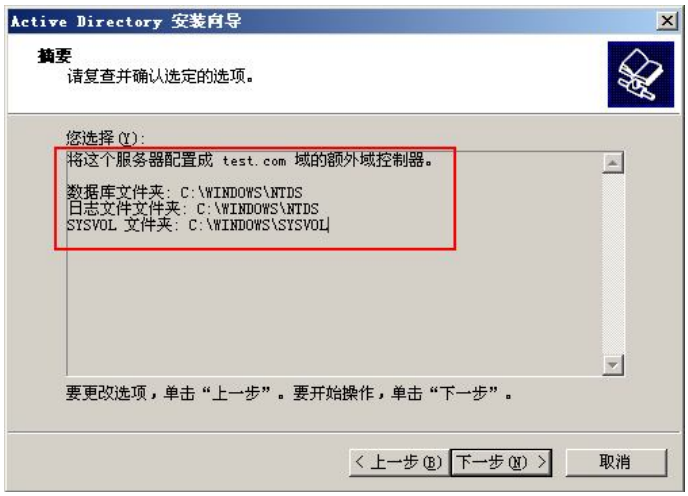



图 1-37 “摘要”对话框

（15）在确认以上配置无误后，单击“下一步”按钮，系统即开始进行活动目录的安装，进程对话框如图 1-38 所示。完成后自动显示如图 1-39 所示活动目录安装向导完成对话框。单击“完成”按钮，系统会弹出询问是否要立即重启系统的提示框。按要求重启系统，然后会弹出如图 1-40 所示的配置您的服务器向导完成对话框，提示此服务器已是域控制器角色。


图 1-38　活动目录安装进程对话框


图 1-39　“正在完成 Active Directory 安装向导”对话框


图 1-40　“此服务器现在是域控制器”对话框

至此，额外域控制器的安装也完成了。接下来要在额外域控制器上安装另外一台 DNS 服务器，然后再配置两台域控制器的 DNS 服务器和一台 DHCP 服务器。

# 1.4 安装与配置 DNS 服务器

在域网络中，DNS 服务器是必需的。尽管在运行第一台服务器安装向导中已随主域控制器的安装集成安装了第一台主要 DNS 服务器，但是在安装第一台主要 DNS 服务器时只默认创建了主要正向查找区域，并没有创建反向查找区域。这对于小型域网络没什么影响，但对于有像 Web 网站、FTP 站点和 E-mail 等应用服务器的域网络来说，通常需要由 IP 地址解析出对应的域名，所以最好同时创建反向查找区域。另外，对于有一定规模的域网络来说，通常还需要配置一台，甚至多台用于提高域网络 DNS 解析能力和 DNS 服务器容错的辅助 DNS 服务器。本节介绍反向查找区域的创建和辅助 DNS 服务器的安装与配置。

## 1.4.1 在主要 DNS 服务器上创建反向查找区域

在上节进行的第一台服务器安装过程中，主要 DNS 服务器上默认是没有创建反向查找区域的。如有需要，则需要另外手动创建。为了提高解析效率，在中等规模的域网络中往往需要同时配置反向查找区域，以便通过 IP 地址来解析出对应的 DNS 域名。本节以在主要 DNS 服务器上创建反向查找区域为例介绍反向查找区域的创建方法。

（1）在如图 1-41 所示的主要 DNS 服务器（在本实验中是在主域控制器上）管理控制台的“反向查找区域”容器上右击，在弹出菜单中选择“新建区域”选项，打开如图 1-42 所示区域创建向导首页对话框。


图 1-41 主要 DNS 服务器管理控制台

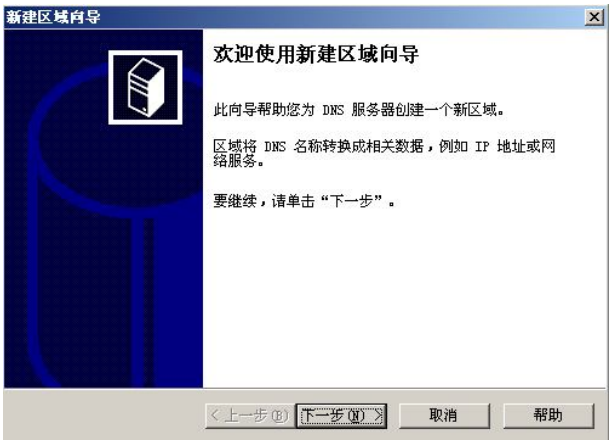



图 1-42 “欢迎使用新建区域向导”对话框

（2）单击“下一步”按钮，打开如图 1-43 所示对话框。在这里选择所创建的 DNS 区域类型。因为此处是在主要 DNS 服务器上创建反向查找区域的，所以要选择“主要区域”单选项，创建一个主要反向查找区域。

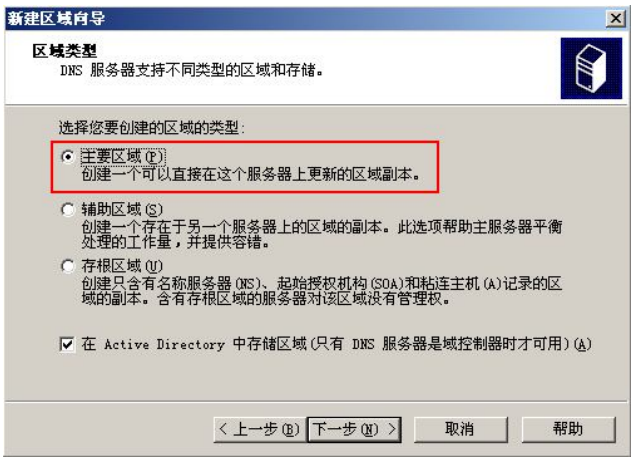



图 1-43　“区域类型”对话框

（3）如果在图 1-43 所示对话框中选择了“在 Active Directory 中存储区域”复选项（只有当该 DNS 服务器位于域控制器上该选项才可选），则在单击“下一步”按钮后打开如图 1-44 所示对话框。在这里要选择该 DNS 区域中的数据将复制到哪个范围。本实验是单级域网络，且两台服务器都是在域控制器上，所以可以任意选择一个复制作用域。在此以选择“至 Active Directory 域 test.com 中的所有 DNS 服务器”单选项为例进行介绍。

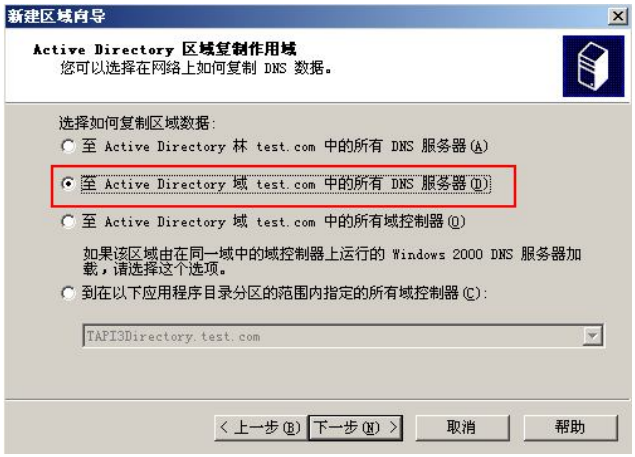



图 1-44　“Active Directory 区域复制作用域”对话框

（4）单击“下一步”按钮，打开如图 1-45 所示对话框。在这里要设置反向查找区域网络 ID 或者区域名称。通常是选择以网络 ID 进行区域标识。选择“网络 ID”单选项，然后在下面正向输入对应域网络的网络 ID 部分，如本实验中，域网络所在子网的网络 ID 为 192.168.1.0，255.255.255.0，输入前面网络 ID 部分的 192.168.1 即可。输入好后在下面的“反向查找区域名称”文本框中会自动显示对应的反向查找区域名称。其格式为：*反向的网络 ID*.in-addr.arpa。

（5）单击“下一步”按钮，打开如图 1-46 所示对话框。在这里可以选择是否允许动态更新。只有安装在域控制器上的 DNS 主要区域才能动态更新，辅助区域不能动态更新，只能通过从主要 DNS 服务器上复制进行记录更新。本实验中的主要 DNS 服务器是安装在

主域控制器上的，所以可以选择安全更新单选项——“只允许安全的动态更新”。

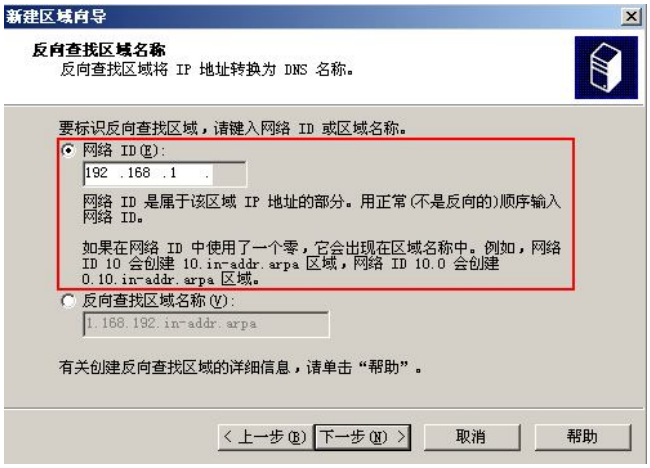



图 1-45 “反向查找区域名称”对话框

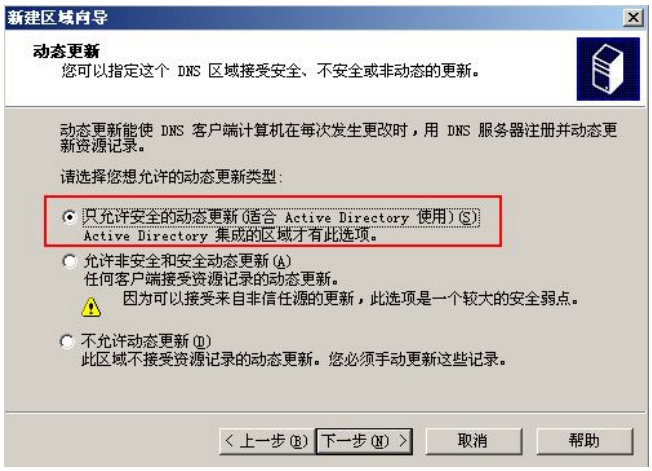



图 1-46 “动态更新”对话框

（6）单击“下一步”按钮，打开如图 1-47 所示向导完成对话框。在其中提示了本次任务所进行的配置摘要。单击“完成”按钮即开始反向查找区域的创建与配置。完成后的主要 DNS 服务器管理控制台如图 1-48 所示。此时可见到新建的主要反向查找区域了。


图 1-47 “正在完成新建区域向导”对话框

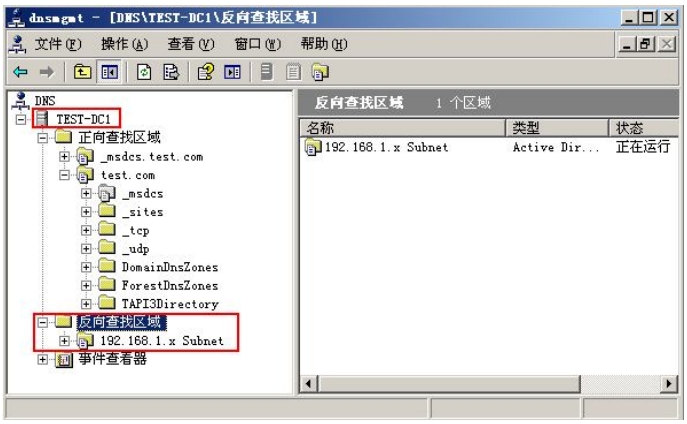



图 1-48　在主要 DNS 服务器上新建的主要反向查找区域

## 1.4.2　安装辅助 DNS 服务器

通过 1.2.2 节的第一台服务器安装，已在第一台域控制器 test-DC1 上集成安装了第一台 DNS 服务器（主要 DNS 服务器）和第一台 DHCP 服务器。根据网络实验要求，还要求在额外域控制器上安装第二台 DNS 服务器（辅助 DNS 服务器），然后再对两台 DNS 服务器和一台 DHCP 服务器进行配置。之所经配置两台 DNS 服务器，一是为了提高域网络中 DNS 解析能力，二是可以实现 DNS 服务器容错，在一台 DNS 服务器出现故障时另外一台 DNS 服务器可以接替全部的 DNS 解析工作，就像安装主域控制器与额外域控制器的目的一样。

因为实验中要求辅助 DNS 服务器是安装在额外域控制器上的，而额外域控制器在安装时不能采用第一台服务器那样的安装方式，所以额外域控制器和辅助 DNS 服务器需要单独安装。下面是在域控制器 test-DC2 上安装辅助 DNS 服务器的具体步骤。

（1）在 test-DC2 Windows Server 2003 SP2 额外域控制器上执行【开始】→【管理工具】→【配置您的服务器向导】菜单操作，打开如图 1-49 所示向导首页对话框。


图 1-49　“欢迎使用‘配置您的服务器向导’”对话框

（2）单击“下一步”按钮，打开如图 1-50 所示对话框。在这里显示在进行向导前要做好的准备工作。

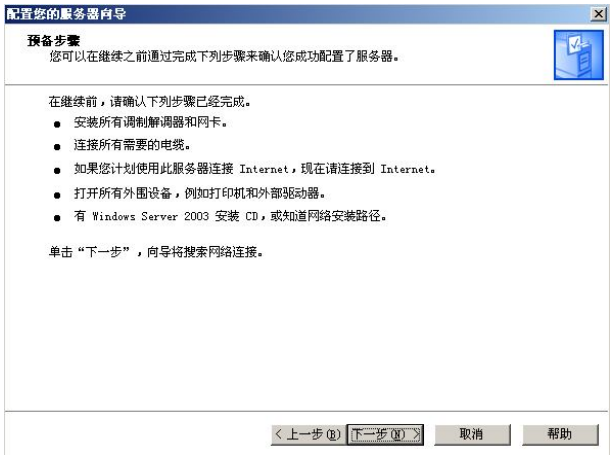



图 1-50 “预备步骤”对话框

（3）准备工作都确认做好后，单击“下一步”按钮，打开如图 1-51 所示对话框。在这里要选择添加或者删除的服务器角色（添加、删除服务器角色都是通过“配置您的服务器向导”进行的）。在此选择“DNS 服务器”选项。

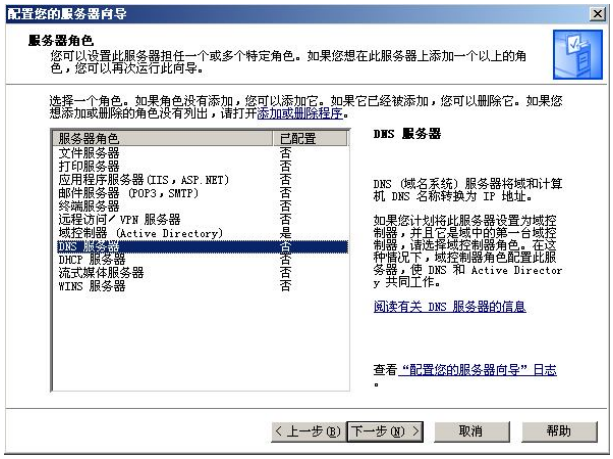



图 1-51 “服务器角色”对话框

（4）单击“下一步”按钮，打开如图 1-52 所示对话框。在这里显示了本次服务器配置任务摘要。本次为 DNS 服务器安装与配置。


图 1-52 “选择总结”对话框

（5）单击“下一步”按钮，系统开始复制 DNS 服务器组件文件。在复制过程中可能会弹出提示框，要求插入 Windows Server 2003 安装光盘，如图 1-53 所示，在第一张光盘的 i386 目录下。选择好后，继续复制 DNS 服务器组件文件，完成后打开如图 1-54 所示的 DNS 服务器配置向导首页对话框。


图 1-53　插入安装光盘提示框

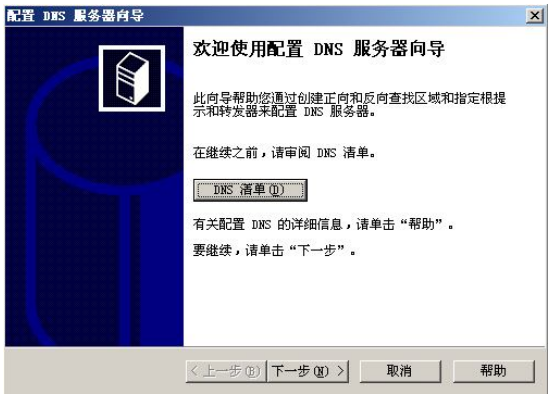



图 1-54　“欢迎使用配置 DNS 服务器向导”对话框

（6）单击“下一步”按钮，打开如图 1-55 所示对话框。在这里要选择配置的 DNS 区域类型。正向查找区域是将对象的 DNS 名称解析为对应对象的 IP 地址，而反向区域则相反，是用对象的 IP 地址解析为对应对象的 DNS 名称。本实验是根据典型中企业网络规模进行配置的，所以选择“创建正向和反向查找区域”单选项，同时创建正向和反向查找区域。

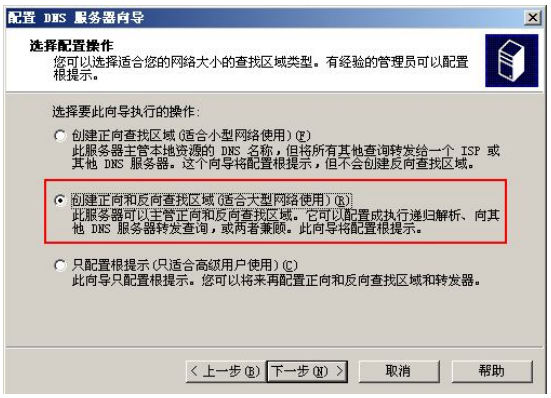



图 1-55　“选择配置操作”对话框

（7）单击“下一步”按钮，打开如图 1-56 所示对话框。在这里系统询问是否要立即创建 DNS 服务器的正向查找区域。本实验选择“是，创建正向查找区域”单选项。

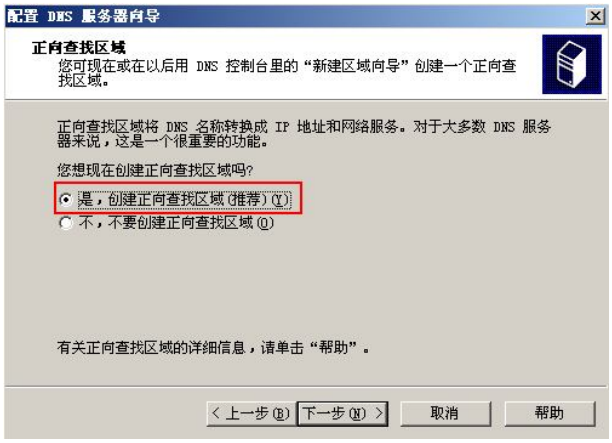



图 1-56 “正向查找区域”对话框

（8）单击“下一步”按钮，打开如图 1-57 所示对话框。在这里要选择创建的正向查找区域类型，有“主要区域”、“辅助区域”和“存根区域”三种。有关这种区域的区别与联系，请参见本级教材《金牌网管师——中小型企业网络组建、配置与管理》一书。在此因为要把额外域控制器上的 DNS 服务器配置为辅助 DNS 服务器，所以选择“辅助区域”单选项。当然也可以把两台 DNS 服务器都配置为主要 DNS 服务器，但这样一来网络中各 DNS 服务器的 DNS 记录信息可能就不一样了，造成混乱。而辅助区域类型的 DNS 服务器上的记录全是从主要 DNS 服务器上复制过来的，所以可以保证网络中各 DNS 服务器的 DNS 记录信息一致。

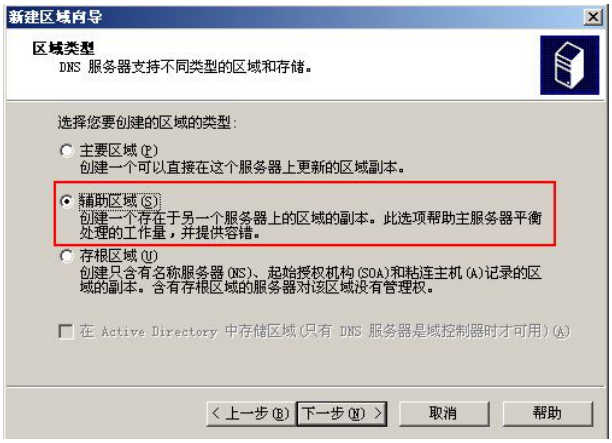



图 1-57 “区域类型”对话框

（9）单击“下一步”按钮，打开如图 1-58 所示对话框。在这里要正向配置辅助区域名称（其实也就是 DNS 域名），记得要与主 DNS 服务器上的主要区域名称一致。本示例仍为 test.com。

（10）单击“下一步”按钮，打开如图 1-59 所示对话框。在其中要指定该辅助 DNS 服务器复制 DNS 记录的主要 DNS 服务器 IP 地址。本实验中主要 DNS 服务器就是主域控制器，IP 地址为 192.168.1.2。

（11）单击“下一步”按钮，打开如图 1-60 所示对话框。这里询问是否要立即创建反向查找区域。选择“是，现在创建反向查找区域”单选项，进行反向查找区域创建。

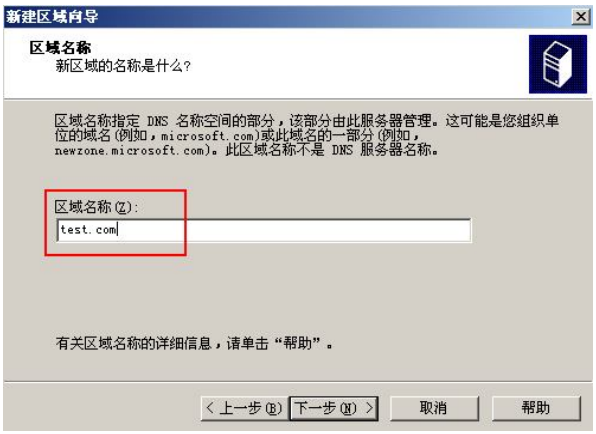



图 1-58　“区域名称”对话框

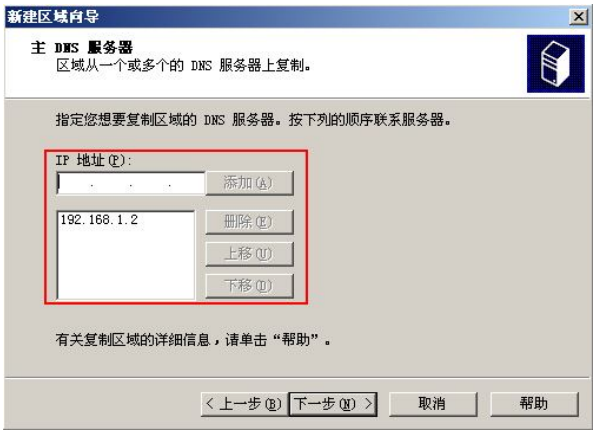



图 1-59　“主 DNS 服务器”对话框

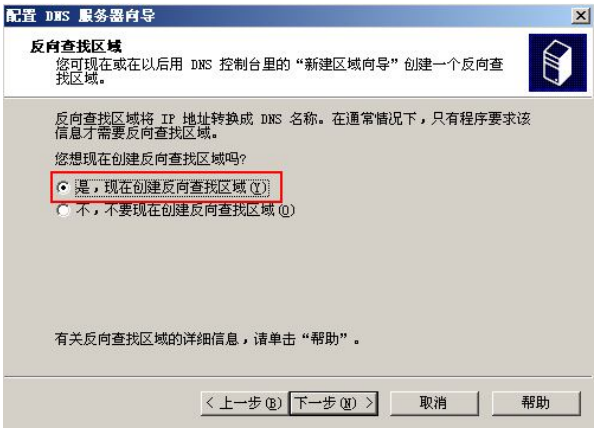



图 1-60　“反向查找区域”对话框

（12）单击“下一步”按钮，打开如图 1-61 所示对话框。在这里同样要选择所创建的反向查找区域类型。在此也以选择“辅助区域”单选项创建辅助区域为例进行介绍。与主要 DNS 服务器的主要反向查找区域一起提供容错机制，同时也可提高反向解析效率。

（13）单击“下一步”按钮，打开如图 1-62 所示对话框。在这里要输入反向查找区域名称或者网络 ID。通常是以网络 ID 来标识反向查找区域的。这里的“网络 ID”是指仅需要输入对应子网的网络 ID 部分，而且输入时要正向输入。如本实验所在子网为 192.168.1.0，255.255.255.0，只需要输入 192.168.1 这个网络 ID 部分。

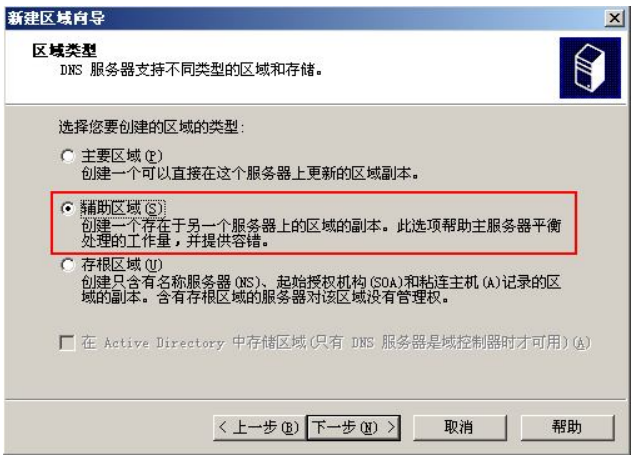



图 1-61 “区域类型”对话框

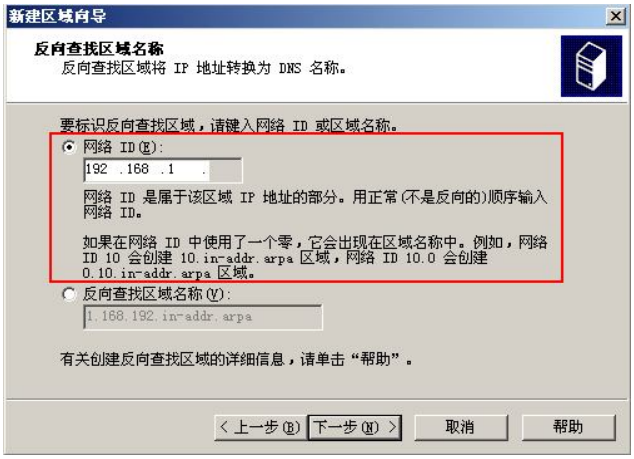



图 1-62 “反向查找区域名称”对话框

输入网络 ID 后，在“反向查找区域名称”栏中会自动显示“逆向网络 ID+in-addr.arpa”格式的对应反向查找区域名称（注意这时的网络 ID 部分是反向显示的）。

（14）单击“下一步”按钮，打开如图 1-63 所示对话框。在这里要输入本辅助反向查找区域所对应的主要 DNS 服务器。本实验辅助查找区域所对应的主要 DNS 服务器是在主域控制器上的，IP 地址为 192.168.1.2。

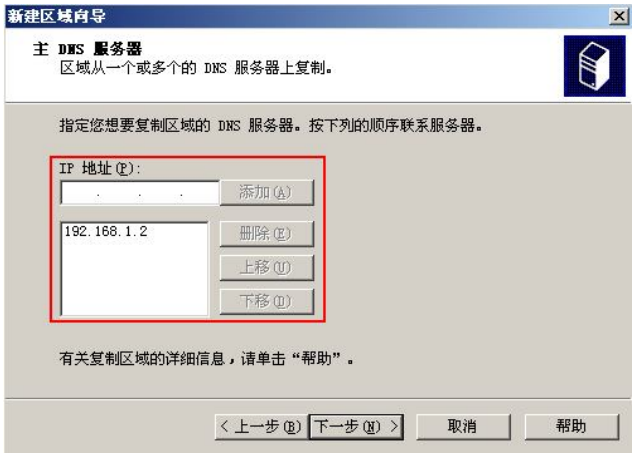



图 1-63 “主 DNS 服务器”对话框

（15）单击“下一步”按钮，打开如图 1-64 所示对话框。在这里可配置是否转发本 DNS 服务器不能解析的 DNS 名称解析请求。如果域网络中的用户要上互联网，则可以在此选择“是，应当将查询转发到有下列地址的 DNS 服务器上”单选项，然后在下面输入 ISP 提供的 DNS 服务器地址。本实验暂时不考虑这种需求，选择“否，不向前转发查询”单选项，不转发 DNS 名称解析请求。

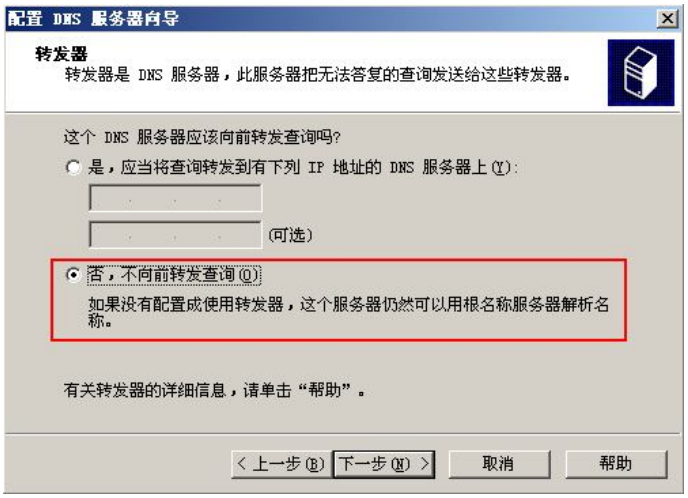



图 1-64　“转发器”对话框

（16）单击“下一步”按钮，打开如图 1-65 所示向导完成对话框。单击“完成”按钮即可完成 DNS 服务器安装与配置向导，同时打开如图 1-66 所示的对话框，提示该服务器已是 DNS 服务器了，这样额外域控制器也就同时成为辅助 DNS 服务器了。

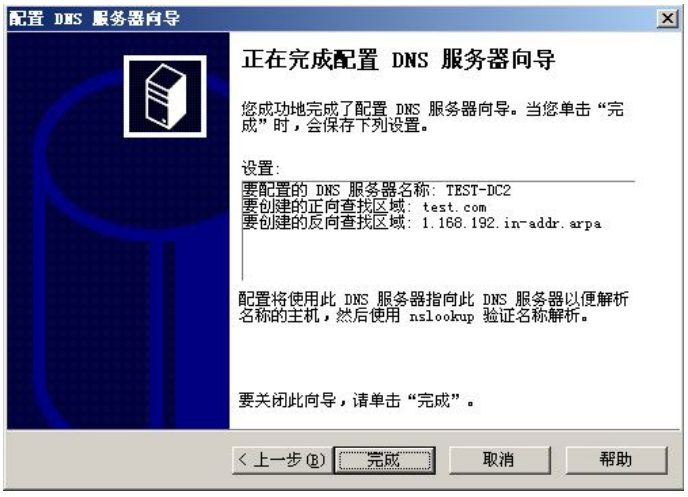



图 1-65　“正在完成配置 DNS 服务器向导”对话框

辅助 DNS 服务器安装好后，系统会自动从以上安装过程中指定的主要 DNS 服务器上复制各个区域中的 DNS 记录，以实现主、辅 DNS 服务器的 DNS 记录信息同步，如图 1-67 所示。但不能在辅助 DNS 服务器上创建新的 DNS 记录。

对比一下主要 DNS 服务器上的记录（如图 1-48 所示），可以发现，辅助 DNS 服务器上各区域中的 DNS 记录与主要 DNS 服务器对应区域中的 DNS 记录是一致的。因为在安装第一台服务器时安装的主要 DNS 服务器默认是不创建反向查找区域的，所以在辅助 DNS 服务器上也没有创建反向查找区域。


图 1-66 “此服务器现在是 DNS 服务器”对话框

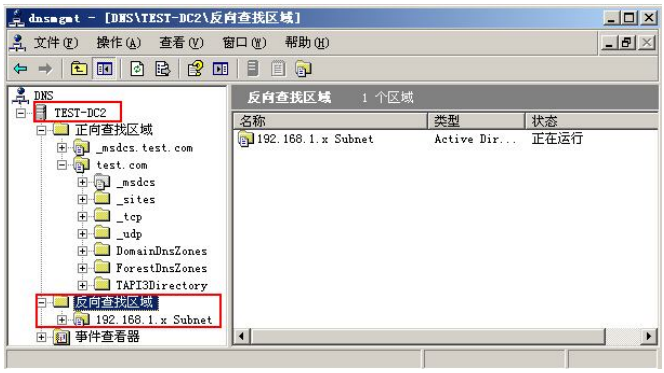



图 1-67 辅助 DNS 服务器上的 DNS 区域记录

## 1.4.3 配置主要/辅助 DNS 服务器属性

为了确保在后面域客户端计算机加入域时不出现因 DNS 服务器配置不当加入不成功的现象，有必要对主要和辅助 DNS 服务器的一些主要属性进行必要的配置确认。

DNS 服务器属性配置包括公共属性配置和查找区域属性配置两个方面。下面介绍一些在中小型域网络组建中常用的属性配置方法。

### 1．公共属性配置

DNS 服务器公共属性配置是在 DNS 服务器管理控制台的 DNS 服务器上进行的。下面以本实验的主要 DNS 服务器 test-DC1 的公共属性配置为例进行介绍。在 test-DC1 的 DNS 管理控制台 DNS 服务器 test-DC1 上右击，在弹出菜单中选择“属性”选项，打开如图 1-68 所示对话框。这里有许多选项，但对于中小型域网络来说，一般只需留意一下“接口”和“转发器”这两个选项卡。

如图 1-68 所示的“接口”选项卡用来指定本服务器中用于侦听 DNS 请求的 IP 地址。这主要适用于一台服务器上配置了多个 IP 地址的情形。如在一些小型网络中，一台服务器担当几种服务器角色，如 DNS 服务器、域控制器、Web 服务器、FTP 服务器，这时为了给每个服务器角色分配一个单独的 IP 地址，就需要在同一块网卡上配置多个 IP 地址了（当然，其实也可以统一用一个 IP 地址）。在这种情况下，需要在图 1-68 所示“接口”选项卡

中指定用于侦听 DNS 请求的 IP 地址。默认是本机上所有配置的 IP 地址都可以侦听 DNS 请求，也就是选择“所有 IP 地址”单选项。如果要指定特定的 IP 地址，则要选择“只在下列 IP 地址”单选项，然后把相应 IP 地址添加到下面的列表中。

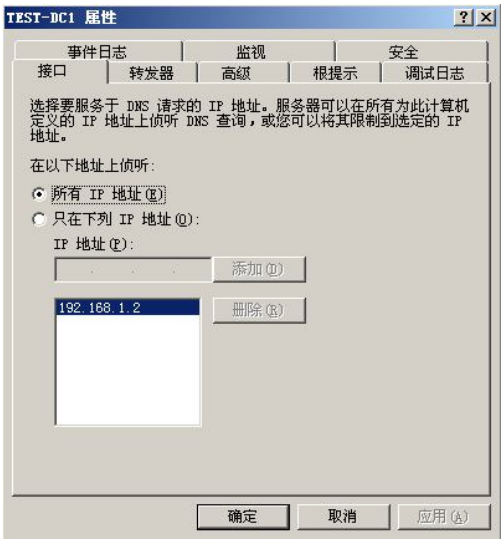



图 1-68　DNS 服务器属性对话框的“接口”选项卡

一般来说，按照默认选择所有 IP 地址也不会有什么太大问题，只是在其他服务器应用比较繁忙时会浪费服务器的一些资源，因为可能其他 IP 地址根本就没有分配给 DNS 服务器。

在如图 1-69 所示的“转发器”选项卡中可以配置在本 DNS 服务器接收到不能解析的 DNS 请求（如访问其他域，或者互联网的请求）时，本 DNS 服务器把该请求转发到哪个对应的 DNS 服务器。

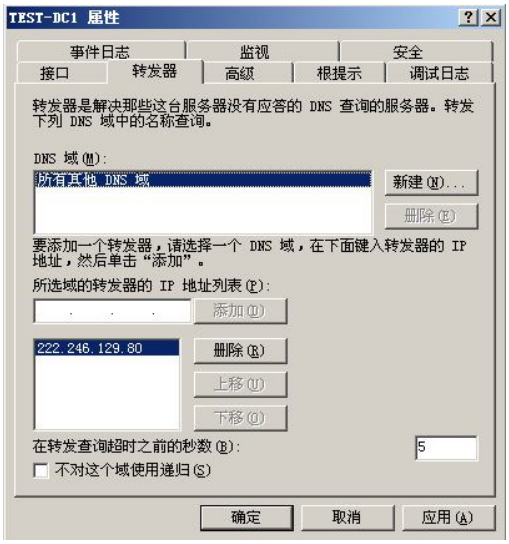



图 1-69　DNS 服务器属性对话框的“转发器”选项卡

要为指定 DNS 域指定转发器，先可在“DNS 域”栏中单击“新建”按钮，然后在打开的如图 1-70 所示对话框中输入要转发 DNS 查询请求的域名（如本示例假设要转发访问另一个域网络 lycb.local 的请求，所以输入该域的域名 lycb.local）。先新建 DNS 域，再在下面的“所选域的转发器的 IP 地址列表”中添加对应 DNS 域的 DNS 服务器 IP 地址即可。

当然要转发这个请求到另一个 DNS 域，必须先确保当前域与另一个域的网络是通的。如通常在域网络中，域用户除了访问域网络外，还要访问互联网，这时就可以把 ISP 提供的 DNS 服务器地址添加到转发器中，这样就可以使域网络用户同时访问互联网。


图 1-70 “新转发器”对话框

以上介绍的是主要 DNS 服务器的公共属性配置，在辅助 DNS 服务器上同样可以配置以上属性，方法完全一样，不再赘述。

### 2．区域属性配置

除了可以配置 DNS 服务器公共属性外，还可以针对各个查找区域配置相关属性。但要注意的是，主要 DNS 服务器与辅助 DNS 服务器上的区域属性配置有些地方是不一样的。下面仅以正向查找区域为例进行介绍（反向查找区域的属性配置方法完全一样）。

在主要 DNS 服务器的一个正向查找区域上右击，在弹出菜单中选择“属性”选项，打开如图 1-71 所示对话框。在这里也有 6 个选项卡，在中小型域网络中，通常只需要配置“常规”、“起始授权机构（SOA）”、“名称服务器”和“区域复制”这四个选项卡。

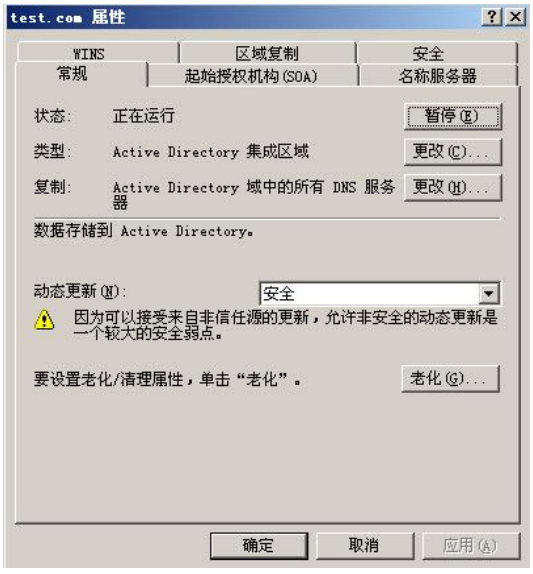



图 1-71 区域属性对话框的“常规”选项卡

在“常规”选项卡中可以配置区域的类型（是主要区域、辅助区域，还是存根区域，以及是否与 Active Directory 集成）、区域复制范围、动态更新方式，以及区域中 DNS 记录老化（也就是指定当记录多少时间没有更新后就认为是过时，过时的记录都将被清理）设置。这些选项在创建 DNS 区域时都配置好了，除非确实要更改，一般无须重新配置。

在如图 1-72 所示的“起始授权机构（SOA）”选项卡中，要手动配置的选项不多，通常按照系统设置即可。在“序列号”文本框中显示的是当前区域更改的次数。每次更改区域时，该序列号按值 1 增加以表明新的版本。在区域刷新请求确定是否更改区域和是否需

要传输来更新区域期间，由服务器检查和比较该序列号。低序列号的 DNS 服务器区域要从高序列号的 DNS 服务器区域上复制。可以使用“增量”按钮来手动地增加该序列号，强制其他 DNS 服务器从该 DNS 服务器进行区域复制。

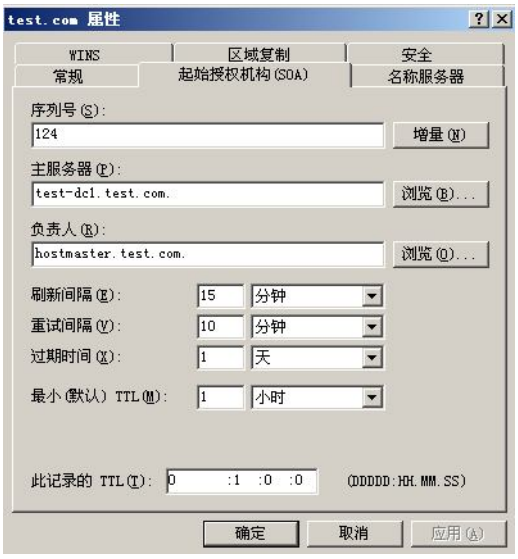



图 1-72　区域属性对话框的“起始授权机构（SOA）”选项卡

在“起始授权机构（SOA）”选项卡中要注意的是，在“主服务器”文本框中，对于主要 DNS 服务器来说，要配置当前 DNS 服务器的 DNS 域名，而对于辅助 DNS 服务器来说，则一定要指向主要 DNS 服务器的 DNS 域名，而不是本辅助 DNS 服务器的 DNS 域名，但系统默认都是显示本地 DNS 服务器的 DNS 域名的。

在如图 1-73 所示“名称服务器”选项卡中，可查看当前域网络中的所有 DNS 服务器（包括所有主要 DNS 服务器和辅助 DNS 服务器）是否都在“名称服务器”列表中，如果没有，则要把未加入的 DNS 服务器添加到列表中，指定该域网络中可用的 DNS 服务器及对应的 IP 地址。如果网络中原来的 DNS 服务器被删除了，则在这里的“名称服务器”列表中也要及时删除。


图 1-73　区域属性对话框的“名称服务器”选项卡

在如图 1-74 所示的“区域复制”选项卡中可以选择是否启用本地 DNS 服务器相应区域的区域复制功能。启用后，本区域的副本将复制到设定的 DNS 服务器（可以是主要 DNS 服务器，也可以是辅助 DNS 服务器）中。但一般只需要在主要 DNS 服务器上启用区域复制功能，因为辅助 DNS 服务器上的 DNS 记录都是从主要 DNS 服务器上复制而来的，它不能保证是最新的，所以建议不要在辅助 DNS 服务器上启用区域复制功能。启用区域复制功能时还可以指定区域副本的复制范围。至于到底以哪个 DNS 服务器上的数据为主进行复制，这就要用到前面在图 1-72 中的“序列号”了，序列号高的为版本新的，以最高序列号的 DNS 服务器上的数据为主对其他指定的 DNS 服务器对应区域进行复制。可以通过人为修改图 1-72 所示对话框中的“序列号”来改变复制关系。

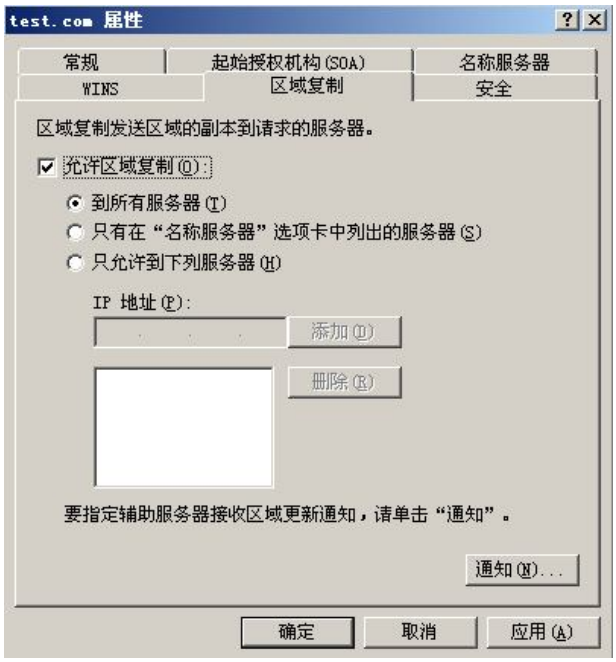



图 1-74　区域属性对话框的“区域复制”选项卡

以上介绍的是正向查找区域的设置，反向查找区域的设置方法一样。

## 1.5　配置 DHCP 服务器

如果打算使域网络中的客户端计算机采用域网络中的 DHCP 服务器来自动分配 IP 地址，则要根据需要对 1.2.2 节随第一台服务器安装而安装的 DHCP 服务器进行选项设置了。

在中小型企业域网络 DHCP 服务器配置中，主要需要配置的是 DHCP 服务器的 IP 地址池（用于为客户端计算机分配 IP 地址的地址范围）、排除的 IP 地址（排除 IP 地址池中），以及 DHCP 服务器选项。

### 1．IP 地址池的配置

在 DHCP 服务器安装过程中，DHCP 服务器的 IP 地址池是已配置好的，如无需更改配置，只需要在 DHCP 控制台中找到对应的作用域（在同一个 DHCP 服务器中不能有地址池交叉的多个作用域）的“地址池”选项，如图 1-75 所示。在右边窗口中可以见到当前的 IP 地址池配置。


图 1-75　DHCP 服务器的 IP 地址池

如果要修改地址池，则要在图 1-75 的 DHCP 控制台对应作用域中右击，在弹出菜单中选择“属性”选项，打开如图 1-76 所示对话框。在“常规”选项卡中可以修改地址池范围，以及客户端 IP 地址的租约期。

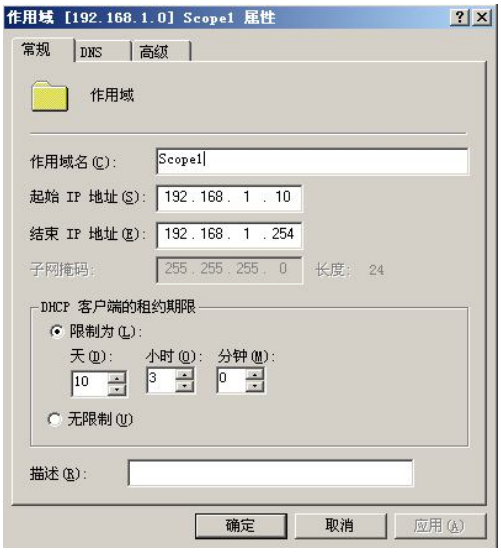



图 1-76　作用域属性对话框的“常规”选项卡

### 2．排除地址

因为本实验在事先已做好了 IP 地址池规划，把各服务器所用的 IP 地址都排除在外了，所以在本实验中不需要另外设置地址排除范围。如果需要添加新的排除范围，可以在图 1-75 所示 DHCP 控制台“地址池”上右击，在弹出菜单中选择“新建排除范围”选项，在打开的如图 1-77 所示对话框中输入要排除的起始和终止 IP 地址（本实验中要排除用于 AP 上 DHCP 服务器分配的 IP 地址段 192.168.1.30～192.168.1.50），然后单击“确定”按钮即可。如果仅需要排除一个 IP 地址，则只需要在“起始 IP 地址”栏输入该地址即可。

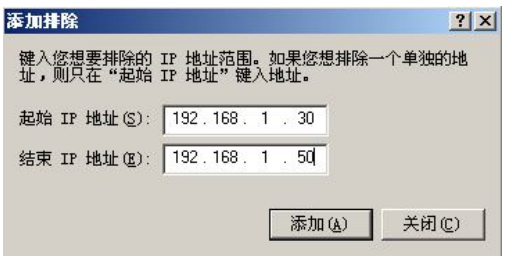



图 1-77　“添加排除”对话框

### 3．DHCP 服务器选项配置

当客户端采用 DHCP 服务器自动分配 IP 地址时，网关甚至 DNS 服务器都可以自动。那么客户端又是如何自动获得网关和 DNS 服务器等相关参数配置呢？答案就是通过 DHCP 服务器上的服务器选项设置获得的。所以，在配置 DHCP 服务器时最好同时对这些主要参数选项进行配置。在 DHCP 服务器中，这些选项的设置既可以在 DHCP 服务器上进行全局设置，也可以在具体的作用域上为各作用域配置不同的这些参数选项。在此仅以在服务器上全局设置为例进行介绍。

在 DHCP 服务器上全局配置服务器选项的方法是在图 1-75 所示 DHCP 控制台窗口的“服务器选项”节点上右击，在弹出菜单中选择“配置选项”选项，打开如图 1-78 所示对话框。在“常规”选项卡的“可用选项”列表中列出了在 DHCP 服务器上可以为客户配置的参数选项。在一般的中小型域网络中，通常只需要设置路由器（也就是默认网关）、DNS 服务器（DNS Servers）、DNS 域名这三个选项。


图 1-78 “路由器”配置选项

- 默认网关配置

在 DHCP 服务器选项中，默认网关的配置选择代码为 003 的“路由器”选项，如图 1-78 所示。选择该选项后，可直接在“IP 地址”文本框中输入网关 IP 地址，然后单击“添加”按钮把该网关 IP 地址（本实验中默认网关为宽带路由器的 LAN IP 地址——192.168.1.1）添加到下面的列表中即可。这样所有 DHCP 客户端（如果是在对应作用域上配置 DHCP 服务器选项，则此处的配置仅作用于对应的作用域，下同）的默认网关就自动设为这个 IP 地址。这样就相当于在 TCP/IP 属性配置对话框中配置默认网关。

可以在这里为 DHCP 客户端配置多个网关地址，此时排在列表中最上面的网关 IP 地址就是默认网关 IP 地址了。

- DNS 服务器配置

在 DHCP 服务器选项中，DNS 服务器的配置选择代码为 006 的 DNS Servers 选项，如图 1-79 所示。配置方法与上面的默认网关配置方法一样，也是在选择该选项后，直接在“IP 地址”文本框中输入 DNS 服务器的 IP 地址，然后单击“添加”按钮，把 DNS 服务器

添加到下面的列表中。本实验中有两个 DNS 服务器，IP 地址分别为 192.168.1.2 和 192.168.1.3。这样就相当于在 TCP/IP 属性配置窗口中配置主要/辅助 DNS 服务器 IP 地址。


图 1-79　DNS Server 配置选项

- DNS 域名配置

在手动分配 IP 地址时，可以为各客户端配置 DNS 域名（在域网络中才需要配置这个选项），在全部采用 DHCP 自动分配时，也可以使用 DHCP 服务器中的选项来配置 DNS 域名，那就是代码为 015 的“DNS 域名”选项，如图 1-80 所示。选择该选项后，在下面的“字符串值”文本框中输入对应域的 DNS 域名，如本实验的域名为 test.com。这样就会在客户端的计算机名后面自动添加 DNS 域名后缀。

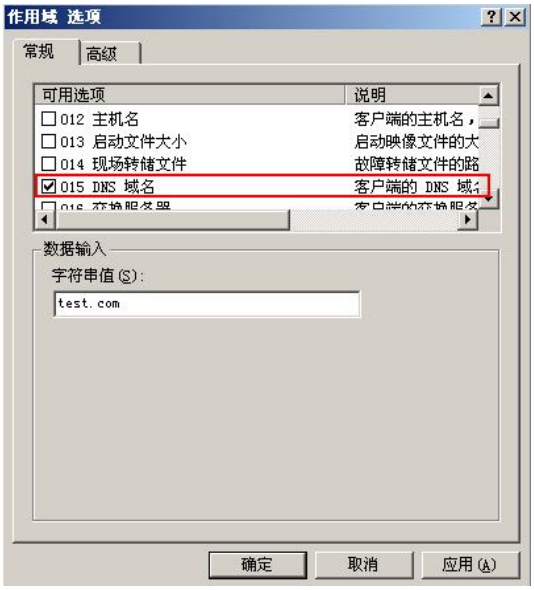



图 1-80　“DNS 域名”配置选项

也可以根据需要设置其他 DHCP 服务器选项，设置好后单击“确定”按钮使设置生效。配置好的 DHCP 服务器选项将在右边窗格中显示，如图 1-81 所示。

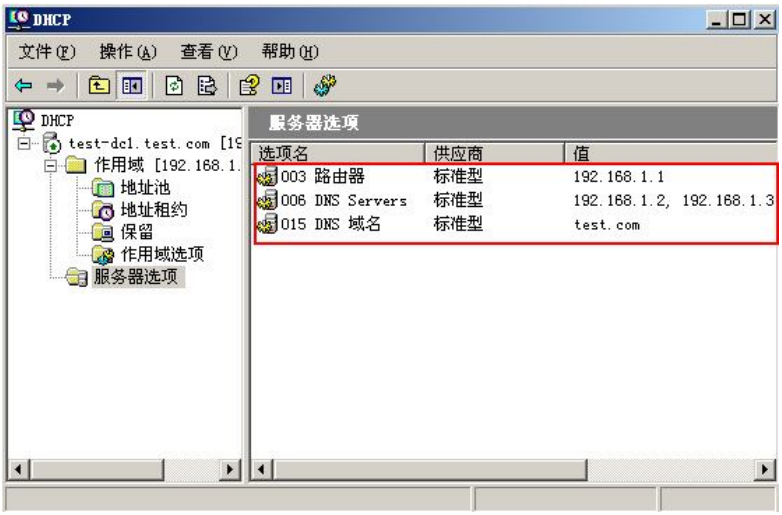



图 1-81　配置好的 DHCP 服务器选项

# 1.6　WLAN 网络连接配置

在域控制器、DNS、DHCP 服务器安装和配置好后，接下来的工作是什么呢？那就是把各用户计算机加入到域网络中。本实验中，多数用户计算机是采用有线方式连接到域网络中的，可以直接通过配置用户计算机的系统属性加入；但也有一些是采用 WLAN 无线连接的，这时就需要先配置 WLAN 网络连接，实现 WLAN 用户计算机的物理和链路级别的网络连接。下面先介绍 WLAN 计算机的网络连接配置（仅以企业网络中使用最广泛的 Infrastrucure 结构 WLAN 网络的连接配置为例进行介绍）。

## 1.6.1　WLAN 用户计算机的网络连接配置

本实验的所用的 WLAN AP 为 DWL-2000AP+，客户端 WLAN 网卡有 TP-LINK TL-WN550G（支持 IEEE 802.11g，向下兼容 IEEE 802.11g 接入标准），以及 IBM ThinkPad R400 笔记本中迅驰二代的 Wi-Fi 5100 网卡（支持 IEEE 802.11n，向下兼容 IEEE 802.11a、IEEE 802.11b、IEEE 802.11g 接入标准）。现假设本实验中所用的 SSID 名为 test，采用 WPA 身份验证。

在配置 Infrastrucure 结构 WLAN 网络中，首先要配置的就是 WLAN AP。AP 的配置是通过 PC 的浏览器打开 Web 配置界面进行的。用一条直通双绞线连接 PC 机网卡（或者交换机）和 AP 中的 LAN 端口。并把 PC 机网卡的 IP 地址设置为 AP 默认 IP 地址所在的同一网段 IP 地址（一般选择自动分配方式即可）。下面是具体步骤。

（1）在连接 AP 的计算机上打开浏览器，在地址栏中输入 DWL-2000AP+默认的 IP 地址——192.168.0.50（不同 AP 默认的 IP 地址不一样，具体要查看说明书），打开如图 1-82 所示身份认证对话框。

（2）在其中输入管理员账户名（默认为 admin）和密码（默认为空），单击“确定”按钮即进入到 DWL-2000AP+的 Web 配置界面，如图 1-83 所示。在首页中显示了“运行向导”按钮，单击它可以打开基本配置向导，这适用于初学用户。在此不以向导方式进行介绍。

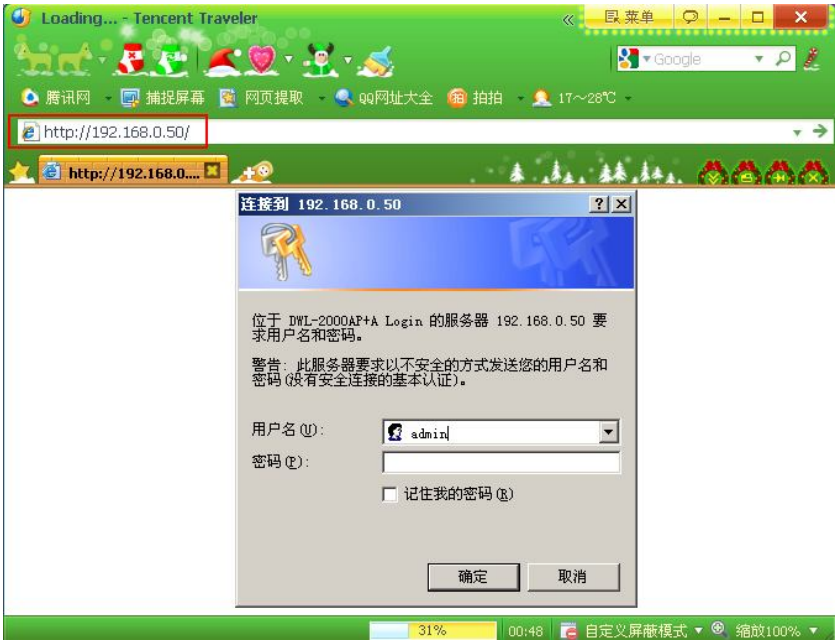



图 1-82　进入 AP Web 配置界面前的身份认证对话框

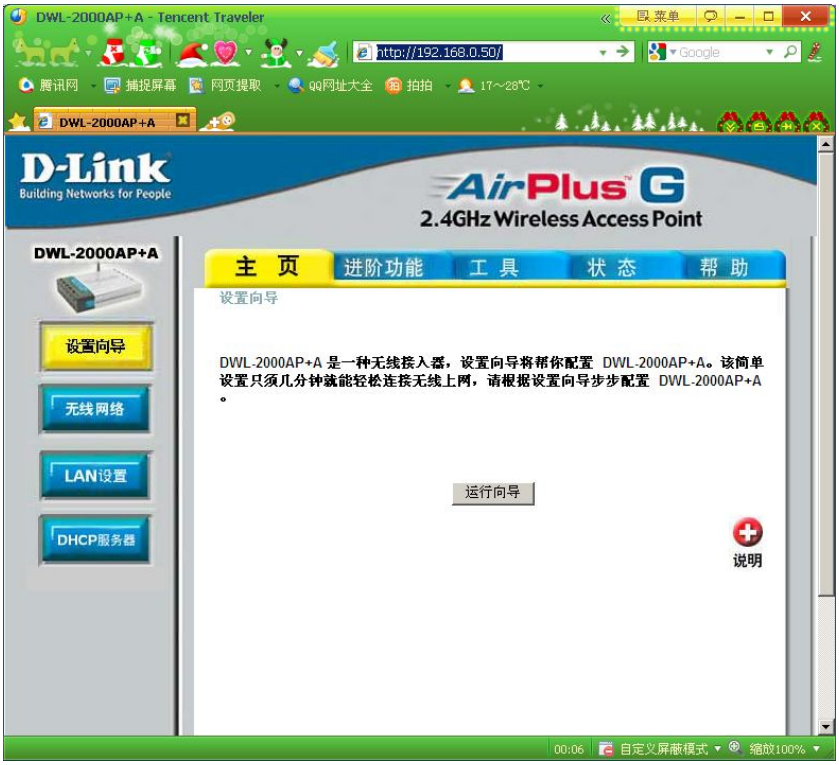



图 1-83　DWL-2000AP+ Web 配置界面首页

（3）因为域网络所用的网段为 192.168.1.0，而 DWL-2000AP+默认的 IP 地址所在网段为 192.168.0.0，所以需要先更改 AP 的 LAN 地址。在图 1-83 所示首页左边导航栏中单击“LAN 设置”按钮，打开如图 1-84 所示对话框。在这里显示了当前的 IP 地址，把原来的 192.168.0.50 更改为 192.168.1.10，然后单击“执行”按钮使设置更改生效。

（4）更改了 IP 地址后需要重新操作上面的第 1 步和第 2 步，进入 Web 配置界面。下面再进行无线网络配置。


图 1-84　DWL-2000AP+的 LAN 设置窗口

（5）在 Web 配置界面左边导航栏中单击“无线网络”按钮，打开如图 1-85 所示对话框。在这里的 SSID 文本框中输入本实验中规划的 SSID 名 test，在“信道”下拉列表中，如果网络中仅一个 AP，则无所谓，随便选择哪个信道都可以（默认为第 6 信道）；如果网络中有多个 AP，则要确保各相邻 AP 所选择的信道不相互干扰。相邻 AP 可以采用 1、6、11，2、7、12，或者 3、8、13 这三个信道组合，否则就会有重叠。


图 1-85　DWL-2000AP+的无线网络设置窗口

在下面的“认证”栏中提供了身份认证方式：

- Open System：开放系统。其实就是不认证，任何人都可以加入进来，当然在企业 WLAN 网络中这是不允许的，所以不要选。
- Shared Key：共享密钥。这是最早在 IEEE 802.11b 标准中沿用的一种认证方式，就是通过设置一个共享密钥来实现身份认证，而且密钥是采用 WEP（有线对等保护）方式加密的。这种密钥不仅有固定位数要求（只能是 5 个或者 13 个 ASCII 字符，或者 10 个或 26 个十六进制数），而且采用的 WEP 加密方式最高仅为 128 位，安全性较差。

- WPA-PSK：WPA（Wi-Fi Protected Access，Wi-Fi 保护接入）预共享密钥，是一种替代 WEP 加密方式的新 WLAN 安全技术，应用于没有专门配置 RADIUS（Remote Authentication Dial In User Service，远程拨入用户身份认证服务）身份认证服务器的情况下，如个人，或者 SOHO 环境。也需要设置共享密钥，但密钥长度可以很灵活，并非固定位数（但至少 8 位）。而且所采用的 TKIP（Temporal Key Integrity Protocol，临时密钥完整性协议）/ MIC（Message Integrity Code，消息完整性编码）加密技术也更先进。
- WPA2-PSK：是 WPA-PSK 的改进版本（也至少 8 位），采用了更先进的 AES-CCMP（Advanced Encryption Standard – Counter mode with Cipher-block chaining Message authentication code Protocol，高级加密标准－计数器模式密码区块链接消息身份验证代码协议）加密技术。同样只适用于没有 RADIUS 服务器的个人或者 SOHO 网络环境中。
- WPA：是应用于有 RADIUS 服务器进行专门身份认证的企业级网络环境中。采用了 TKIP/MIC 加密技术和 IEEE 802.1x 身份认证技术。
- WPA2：是 WPA 的改进版，采用了 AES-CCMP 加密技术和 IEEE 802.1x 安全认证技术。同样适用于有 RADIUS 服务器进行专门身份认证的企业级网络环境中。采用的也是 IEEE 802.1x 身份认证技术。

以上认证技术，不同的设备支持的种类不同，有关这些安全认证技术的详细介绍将在中级教材中介绍。在此以选择比较安全的 WPA2-PSK 认证技术为例进行介绍。

**【经验之谈】**至于到底先选哪种安全认证方式，则要充分考虑网络中当前 AP 所有客户端所支持的安全认证技术，在 AP 上要选择所有客户端都支持的安全认证技术。如有些早期的 IEEE 802.11b 标准的 WLAN 网卡并不支持 WPA、WPA2（只支持 WEP 加密方式），有些早期的 IEEE 802.11g WLAN 网卡并不支持 WPA2 安全认证技术。不过对于 IEEE 802.11g 标准的 WLAN 网卡，通过下载最新版本的驱动和配置程序是可以支持 WPA2 的。如本实验中的 TL-WN550G 网卡原版驱动和配置程序 TWCU 只支持 WEP 和 WPA，但下载安装最新的驱动和配置程序后，就可以支持 WPA2 安全认证技术了。所以，在正式配置前，最好把网络中所有 WLAN 网卡到对应的厂商官方网站下载、安装最新的驱动程序和配置程序。

设置好后单击配置窗口下面的“执行”按钮使设置生效。

另外，出于安全性考虑，最好关闭所有 WLAN 设备上的 SSID 广播功能。在 DWL-2000AP+中，SSID 广播功能的设置是在如图 1-86 所示窗口中进行的。选择“禁用”单选项，这样就会在 WLAN 网络中自动广播本 WLAN 的 SSID。在其中还可以在“模式设置”栏中设置 AP 的工作模式，默认是混合模式，也就是可以同时工作在 IEEE 802.b 标准和 IEEE 802.11g 标准。这样就可以兼容网络中不同接入标准的 WLAN 设备。同样最后要单击“执行”按钮使设置更改生效。

（6）本步可选。如果要为 WLAN 客户提供 DHCP 服务，为 WLAN 客户端自动分配 IP 地址，则可以在 AP 上配置 DHCP 服务（一般的 AP 都提供这种功能）。

在图 1-83 所示的 DWL-2000AP+配置主界面左边导航栏中单击“DHCP 服务器”按钮，打开如图 1-87 所示 DHCP 服务器配置窗口。在其中首先要选择“启用”单选项，然后在下面配置 IP 地址池（通常是事先要规划好每个 AP 所负责分配的 IP 地址范围，如本实验中 WLAN 客户端计算机的 IP 地址范围为 192.168.1.30～192.168.1.50），然后单击“执行”按钮保存设置。

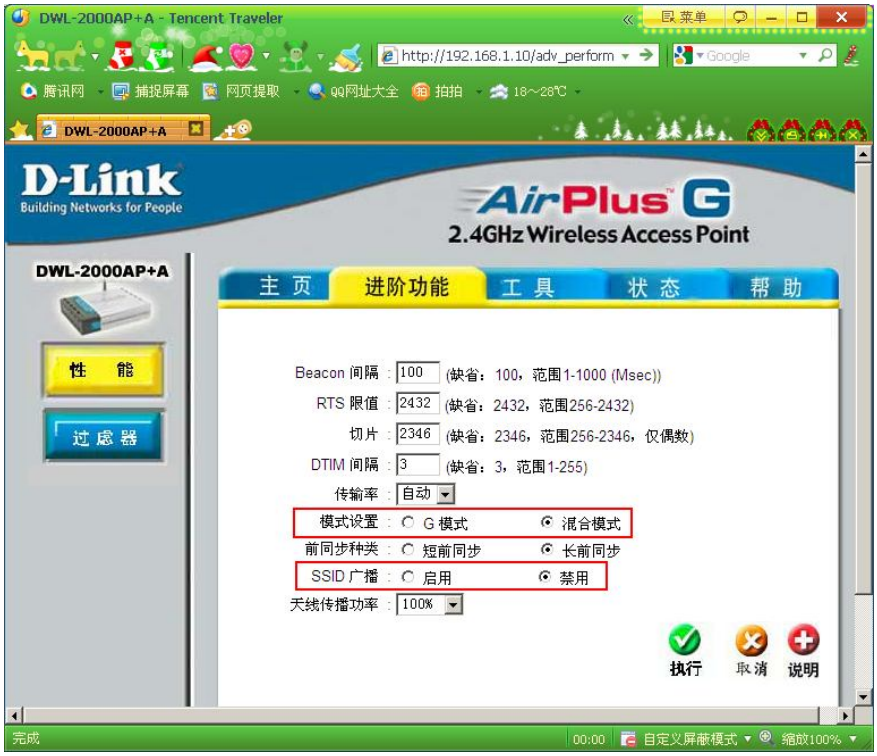



图 1-86　DWL-2000AP+的 SSID 广播和工作模式设置窗口


图 1-87　DWL-2000AP+的 DHCP 服务器配置窗口

（7）本步可选。因为有些 WLAN 网卡没有信道选择，而是通过指定首选 AP 的 MAC 地址来指定连接的 AP，也就是对应的信道。这时就先要记下各 AP 的 MAC 地址。DWL-2000AP+的 MAC 地址是在主配置界面的“状态”选项卡的“装置情况”窗口中查看的，如图 1-88 所示。记下这个 AP 的 MAC 地址，本实验后面在配置 TL-WN550G 无线网卡时要用到。在其中还可以查看 AP 的 IP 地址和 SSID 配置情况。

AP 设置好后，接下来就是要设置 WLAN 客户端计算机的无线网络连接。但要记住 AP 中设置的 SSID 的预共享密钥，因为在客户端计算机中也要做同样的设置。


图 1-88　DWL-2000AP+的配置状态查看窗口

## 1.6.2　迅驰二代笔记本的 WLAN 网络连接配置

下面以 IBM ThinkPad R400 集成的 WiFi Link 5100 无线网卡为例介绍迅驰二代笔记本 WLAN 网络连接配置方法。

首先要在操作系统中安装 WiFi Link 5100 无线网卡的驱动程序（本实验中以应用比较广泛的 Windows XP SP2 系统为例进行介绍，当然也可以是 SP3 版本，或者 Vista 系统），可以在“设备管理器”中查看到该网卡的高级属性，如图 1-89 所示。从中可以看出它是支持最新的 IEEE 802.11n WLAN 接入标准的，同时向下兼容 IEEE 802.11a、IEEE 802.11b、IEEE 802.11g 接入标准。


图 1-89　WiFi Link 5100 无线网卡属性对话框的“高级”选项卡

一般来说，最好还是采用无线网卡自身所带的驱动和管理程序，所以还需要安装好网卡厂商所提供的无线网络连接程序。因为即使像目前主流的 Windows XP 系统，也只有更新到 SP3，才能对 WLAN 新技术，如 WPA2 安全认证技术提供支持。SP2 版本都只能支持

到 WPA 技术。下面是正式的配置步骤。

（1）在状态栏的无线网络连接图标上右击，在弹出菜单中选择“配置 WiFi”选项，或者双击无线网络图标，打开如图 1-90 所示英特尔 PROSet/无线 WiFi 连接实用程序主界面。一打开，就会发现自动搜索到附近环境中多个 WLAN 网络，其中包括上节配置的 DWL-2000AP+无线接入点网络，上面显示“SSID 未广播”的就是（在上节专门配置了 AP 禁止 SSID 广播功能）。


图 1-90　英特尔 PROSet/无线 WiFi 连接实用程序主界面

（2）这时可以选择这个 WLAN 网络选项，单击“属性”按钮，打开如图 1-91 所示对话框。在其中可以查看到该 WLAN 网络的基本配置，如支持的频带、安全认证方式、数据加密技术等。但仍不能查看到 SSID。


图 1-91　WLAN 网络连接属性对话框

（3）在图 1-90 所示界面中选择上节 AP 创建的 WLAN 网络，然后单击“连接”按钮，打开如图 1-92 所示 WiFi 设置向导对话框。在这里要设置该 WLAN 网络的配置式名称（也就是 WLAN 连接名称）、SSID。SSID 一定要与上节 AP 中配置的 SSID 一样，本实验为 test。


图 1-92　“一般设置”对话框

（4）单击“下一步”按钮，打开如图 1-93 所示对话框。在“网络验证”下拉列表中选择“WPA2-个人”（相当于上节 AP 配置中的 WPA2-PSK）选项，在“数据加密”下拉列表中选择 WPA2 加密技术，也就是 AES-CCMP 选项。然后在下面的“无线安全性密码”文本框中配置 WPA2-PSK 预共享密钥，也要与上节 AP 中配置的 WPA2-PSK 预共享密钥一致。


图 1-93　“安全性设置”对话框

（5）单击“下一步”按钮，打开如图 1-94 所示向导完成对话框，提示此 WLAN 网络连接已配置好。此时单击“确定”按钮即开始与 AP 上 SSID 为 test 的 WLAN 网络进行连接。成功后会显示“已连接”状态，并显示连接状态、信号强度，以及该 WLAN 网络

SSID 名称等，如图 1-95 所示。在状态栏中对应的无线网络连接图标为，全为绿色（没有成功连接时为橙色），表示已成功连接。


图 1-94 “已配置”对话框


图 1-95 成功连接后的 WLAN 连接状态

【说明】如果在图 1-90 所示英特尔 PROSet/无线 WiFi 连接实用程序主界面中没有搜索到上节 AP 所配置的 WLAN 网络，可以在这里新建一个 WLAN 连接。方法是在图 1-90 所示界面中单击“配置式”按钮，打开如图 1-96 所示对话框。单击“添加”按钮，打开如图 1-97 所示配置窗口。在这里要为新建 WLAN 网络连接指定配置式名称和 SSID，以及 WLAN 网络工作模式（有 AP 的 WLAN 网络是基础结构模式）。配置式名称可以自定，但 SSID 必须与上节 AP 中配置的 SSID 一样，为 test。


图 1-96　“配置式”对话框

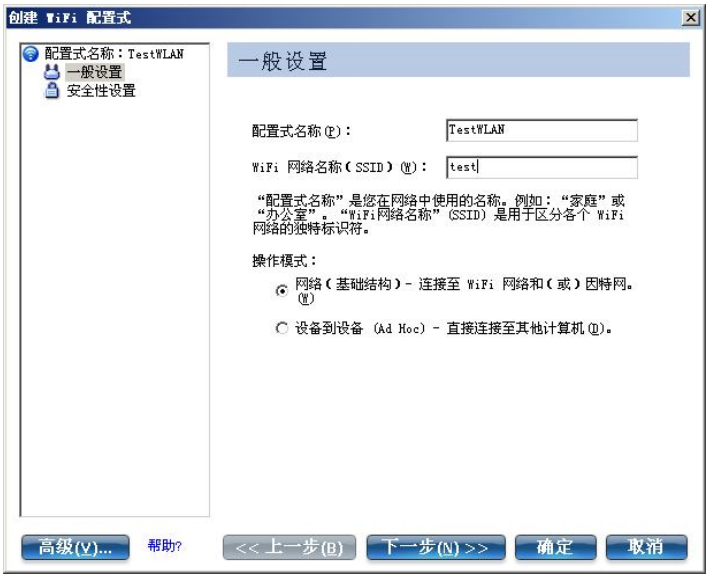



图 1-97　“一般配置”配置窗口

单击“下一步”按钮，打开如图 1-98 所示配置窗口。在这里要为该 WLAN 连接指定安全认证类型和所使用的技术标准。这里的配置也要与上节 AP 中配置的安全认证方式完全一样。在这里选择“个人安全性”（没有专门配置 RADIUS 服务器的情况下），然后在“安全性设置”下拉列表中选择“WPA2-个人（AES-CCMP）”（相当于上节 AP 上配置的 WPA2-PSK）选项，这时会在窗口下新增一个用于配置 WPA2-个人身份认证的预共享密钥的文本框，如图 1-99 所示，也要与上节 AP 配置的一样（至少 8 位）。

单击“确定”按钮，即新添加了一个 WLAN 网络连接，并在图 1-96 所示的配置式窗口列出，如图 1-100 所示。这时再选择这个新建的 WLAN 连接项，单击“连接”按钮即可与 AP 的 WLAN 网络进行连接。同时，这个 WLAN 连接就可以由管理员来管理了。可以在需要时连接/断开该 WLAN 网络，也可以删除该 WLAN 网络，当然还可以查看、编辑该 WLAN 网络属性。

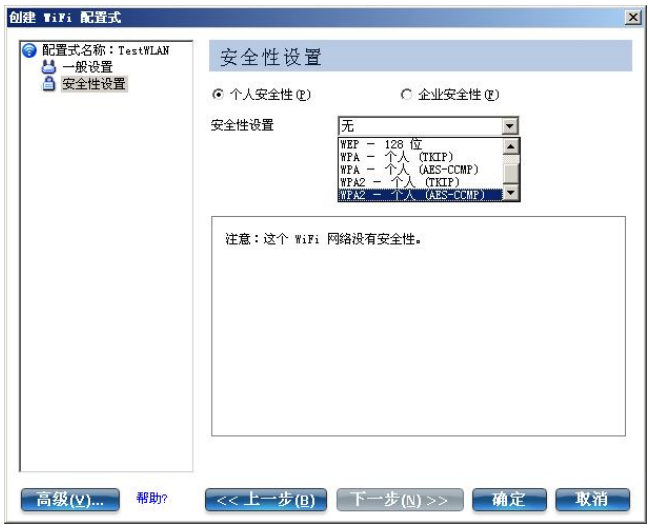



图 1-98 “安全性设置”配置窗口

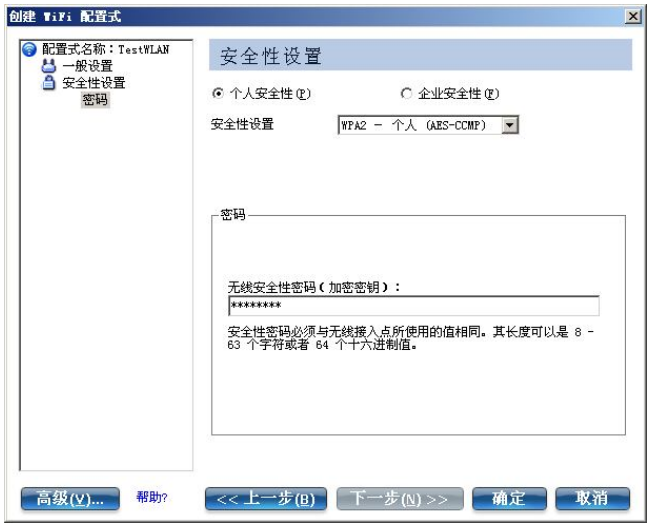



图 1-99 “密码”配置窗口


图 1-100 新建的 WLAN 网络连接项

### 1.6.3 TL-WN550G 无线网卡客户端的 WLAN 网络连接配置

TP-LINK TL-WN550G WLAN 网卡也自带有驱动程序和实用配置程序 TWCU，安装后，会自动搜索当前环境中的 WLAN 网络，但只显示信号最强的一个 WLAN 网络，如图 1-101 所示。


图 1-101 安装驱动程序后自动搜索到的 WLAN 网络

下面来新建一个与 AP WLAN 网络的无线连接。

（1）在图 1-101 所示的 TWCU 配置界面中单击“用户文件管理”选项卡，打开如图 1-102 所示对话框。


图 1-102 TWCU 配置程序界面的“用户文件管理”选项卡

（2）单击“新建”按钮，打开如图 1-103 所示对话框，为连接到 AP 创建一个 WLAN 网络连接。在“常规”选项卡中配置新连接的配置文件名称（也就是上面在 Intel Link 5100 无线网卡配置中所说的“配置式名称”）、本客户端计算机的名称（会自动显示当前计算机的计算机名配置），及 SSID（一定要与 AP 上配置的 SSID 一致，还可配置多个 SSID，本实验 AP 中配置的 SSID 为 test）。

（3）单击“安全”选项卡，打开如图 1-104 所示配置窗口。在这里要配置该 WLAN 网络连接所用的安全认证选项。这时经过下载安装最新的驱动程序和配置实用程序后可以支持 WPA2 了。因为在 AP 中配置的是 WPA2-PSK，所以在这里也要选择这种安全认证方式。但这里显示的名称为“WPA/WPA2 密码短语”，就相当于上节 Intel Link 5100 WLAN 网卡配置程序中的“WPA-个人”或者“WPA2-个人”一样。

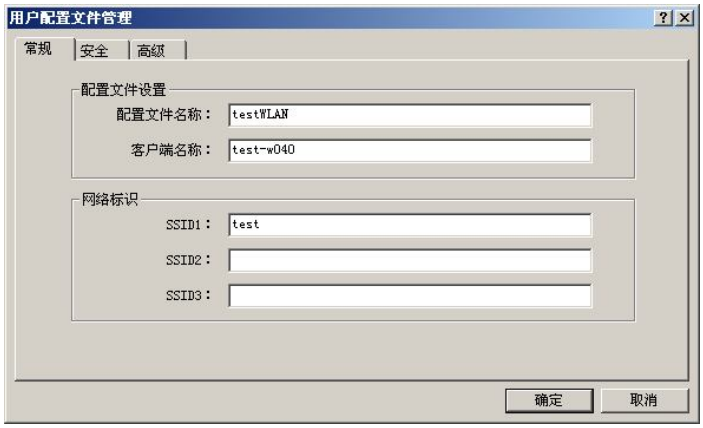



图 1-103　“用户配置文件管理”对话框的“常规”选项卡

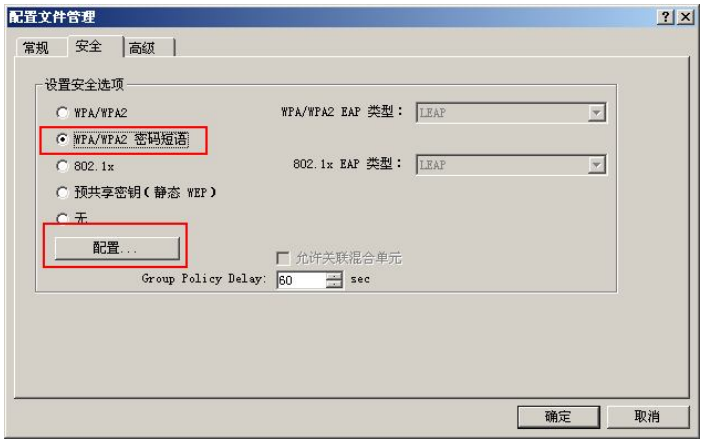



图 1-104　“用户配置文件管理”对话框的“安全”选项卡

（4）选择了“WPA/WPA2 密码短语”单选项后，单击“配置”按钮，打开如图 1-105 所示对话框。在这里要为 WPA2-PSK 配置一个预共享密钥（最少 8 位），当然也必须与 AP 上配置的预共享密钥一致。但这里是明文显示的，所以在配置时一定要做好保密工作，以防密钥泄漏。配置好后单击“确定”按钮返回到图 1-104 所示对话框。


图 1-105　预共享密钥配置对话框

（5）在图 1-104 所示对话框中选择“高级”选项卡，打开如图 1-106 所示对话框。在这里主要可以配置网卡的无线工作模式，以及网络类型（也就是 WLAN 网络拓扑结构）。在工作模式方面，主要要考虑到该 WLAN 中其他用户 WLAN 网卡所支持的接入标准，通常是选择可以支持多种接入标准的混合模式，以实现与其他标准 WLAN 设备的兼容支持。在网络类型方面要选择“基础结构”选项。

（6）在图 1-106 所示对话框中单击“首选 AP”按钮，打开如图 1-107 所示对话框。在这里可以通过指定 AP 的 MAC 地址确定该 WLAN 网卡优先连接的 AP。最多可以指定 4

个 AP。在这里要注意的是，在输入 MAC 地址时一定不要包括图 1-88 所示 AP 配置窗口中显示的 AP MAC 地址中的“:”，也不能包括通常所见的连接符“-”，直接输入 12 位十六进制字符即可。而且字母全部是以大写显示，即使输入时是以小写输入。如本实验中输入的是 001346271b8e，结果显示的是 001346271B8E。指定首选 AP 后，单击“确定”按钮返回到图 1-106 所示对话框。此时再回到图 1-102 所示“用户文件管理”选项卡，即可见到新添加的 WLAN 网络连接项。选择新创建的 WLAN 网络连接项，然后单击“激活”按钮使网卡当前连接所选定的 WLAN 网络连接项。此时会在连接项旁边有一个状态图标，相当于指定了 WLAN 网卡的当前默认连接，如图 1-108 所示。

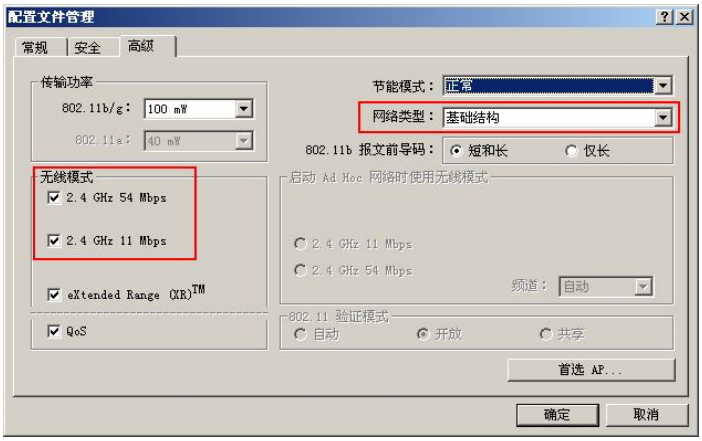



图 1-106　“用户配置文件管理”对话框的“高级”选项卡


图 1-107　“首选接入点”对话框


图 1-108　添加并激活新的 WLAN 连接项后的“配置文件管理”选项卡

单击选择“当前状态”选项卡，此时可见到所选择的 WLAN 连接基本状态、信号强度，如图 1-109 所示。可以看出，信号非常强，并且处于连接状态。此时在状态栏图标中也可以见到此时 WLAN 无线网络连接状态是极好的，显示满格信号。


图 1-109　当前 WLAN 连接状态图示

如果想要查看当前 WLAN 的详细配置状态，可以在图 1-109 所示对话框中单击“高级”按钮，在打开的如图 1-110 所示对话框中就可以见到当前 WLAN 网络连接的详细参数配置。

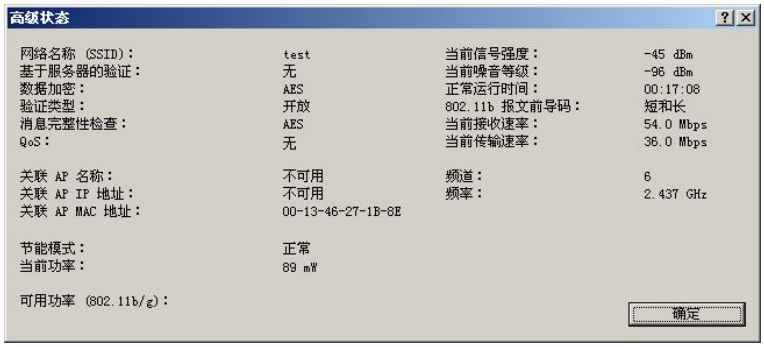



图 1-110　WLAN 连接的详细配置状态对话框

# 1.7　在域网络中添加工作站

采用有线连接方式的客户端计算机可以直接在其操作系统下配置加入域网络，采用 WLAN 无线连接方式的客户端在前面配置了 WLAN 网络连接后，也可以在其操作系统下通过配置加入域网络。无论是有线网络连接还是 WLAN 无线网络连接，加入域的配置方法是完全一样的。

下面把域网络中 Windows 2000 Professional、Windows XP Professional 和 Windows Vista 工作站加入到前面创建和配置的 test.com 域中。

## 1.7.1　把 Windows 2000 Professional 工作站加入域网络

如果网络中有 Windows 2000 Professional 工作站，则在 Windows Server 2003 域网络中

的域功能级别一定要是 Windows 2000 混合模式，不能是纯 Windows Server 2003 模式。

要查看 Windows Server 2003 域的功能可以在 ADUC（Active Directory 用户和计算机）的域名上右击，在弹出菜单中选择“属性”选项，在打开的如图 1-111 所示的“常规”选项卡中就可以看到当前域的域功能级别（默认为“Windows 2000 混合模式”）。

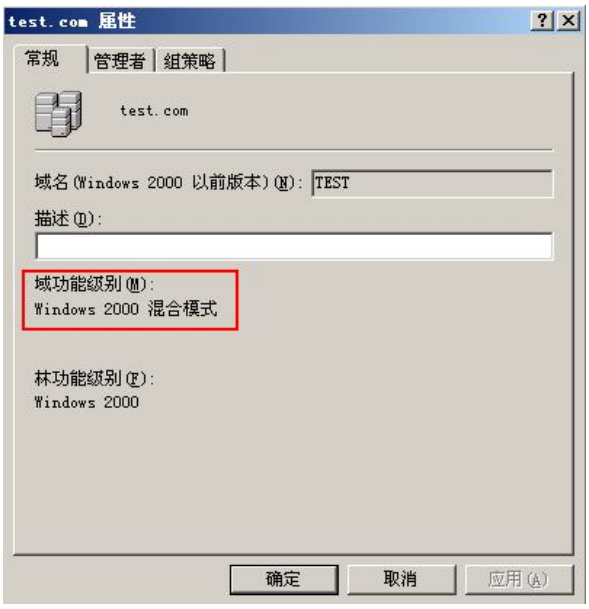



图 1-111　域属性对话框的“常规”选项卡

如果以前是 Windows Server 2003 模式，则要先把域控制器降级为 Windows 2000 混合模式。要更改域功能级别，则需要在 ADUC 的域上右击，在弹出菜单中选择“提升域功能级别”选项，在打开的如图 1-112 所示对话框的“选择一个可用的域功能级别”下拉列表中选择“Windows 2000 混合模式”选项，然后单击“确定”按钮完成域功能级别配置。

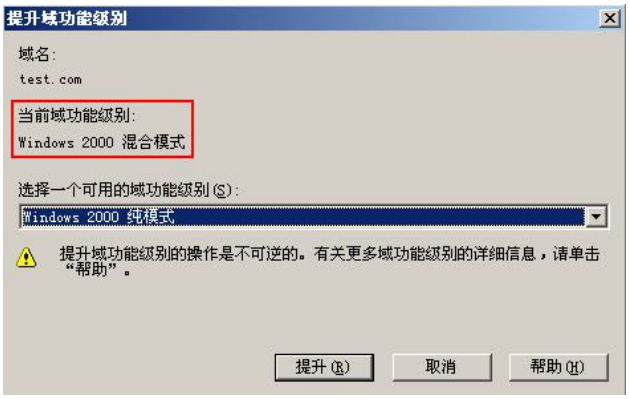



图 1-112　“提升域功能级别”对话框

另外，对 Windows 2000 Professional 工作站计算机也要按照本实验前面的计算机名称规划（工作站计算机名称格式统一为 test-w+ID）更改计算机名称。同时在工作站的 TCP/IP 协议配置窗口配置首要 DNS 服务器地址为域网络中的一台 DNS 服务器 IP 地址（192.168.1.2 或者 192.168.1.3）。

下面正式介绍 Windows 2000 Professional 工作站加入域网络的配置方法。

（1）在 Windows 2000 Professional 工作站计算机上执行【开始】→【设备】→【控制面板】命令，打开如图 1-113 所示的“控制面板”窗口。


图 1-113 “控制面板”窗口中的“系统”选项

（2）双击“系统”选项，在打开的对话框中选择“网络标识”选项卡，如图 1-114 所示。

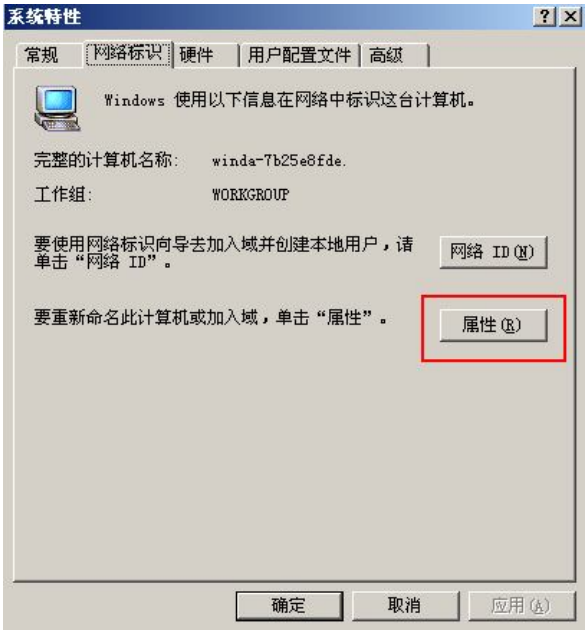



图 1-114 “系统属性”对话框的“网络标识”选项卡

（3）单击“属性”按钮，打开如图 1-115 所示对话框。在这里可以同时修改计算机名（在此以修改为 test-w011 为例）和加入域配置。在“计算机名”文本框中输入该计算机亲手分配的计算机名 test-w011，然后选择“域”单选项，在下面的文本框中输入域名 test.com（也可以只输入域名的 NetBIOS 名称）。

（4）单击“确定”按钮，打开如图 1-116 所示对话框。要求输入有权把工作站加入域的用户账户信息。管理员组成员默认具有这种权限，管理员也可以在域控制器上为普通用户或组账户委派这一添加工作站到域网络的权限。在此直接输入域管理员账户 administrator 和对应的密码。

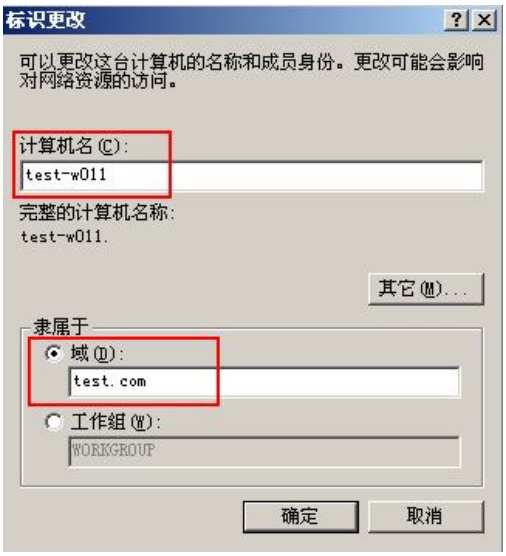



图 1-115　“标识更改”对话框


图 1-116　“域用户名和密码”对话框

（5）输入好相应账户信息后，单击“确定”按钮，如果成功加入域的话，就会弹出如图 1-117 所示欢迎加入域的提示。


图 1-117 欢迎加入域网络提示框

（6）单击“确定”按钮，系统再弹出如图 1-118 所示提示框，要求重启计算机使配置生效。单击“确定”按钮，返回到图 1-114 所示对话框。单击“确定”按钮，系统弹出如图 1-119 所示提示框，询问是否立即重启计算机。单击“是”按钮，系统自动重新启动。


图 1-118　重新启动计算机提示框

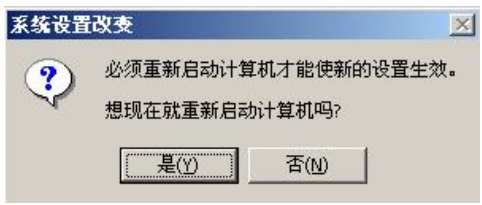



图 1-119　询问现在是否立即重启计算机提示框

这样就一次性修改了计算机名和加入了域网络。

通过以上简单的步骤就把一台 Windows 2000 Professional 工作站计算机加入到 Windows Server 2003 域网络中了。用同样的方法把其他 Windows 2000 Professional 工作站计算机加入到域网络中。

如果在加入域网络时出现各种故障，请参见本级认证教材《金牌网管师——中小型企业网络组建、配置与管理》一书中介绍的排除方法。下面再介绍其他 Windows 系统域网络的加入方法。

### 1.7.2 把 Windows XP Professional 工作站加入域网络

在这里要注意，Windows XP HOME 版本是不能加入域网络的。下面是 Windows XP Professional 工作站加入域网络的具体步骤，总体上与 Windows 2000 Professional 系统计算机加入域网络的步骤类似。同样也需要先在该计算机的 TCP/IP 配置中把首要 DNS 服务器地址指向域网络中的一台 DNS 服务器（192.168.1.2 或者 192.168.1.3）。

（1）在 Windows XP Professional 工作站的“开始”菜单→“我的电脑”菜单项上右击，在弹出菜单中选择“属性”选项，在打开的对话框中选择“计算机名”选项卡，如图 1-120 所示。

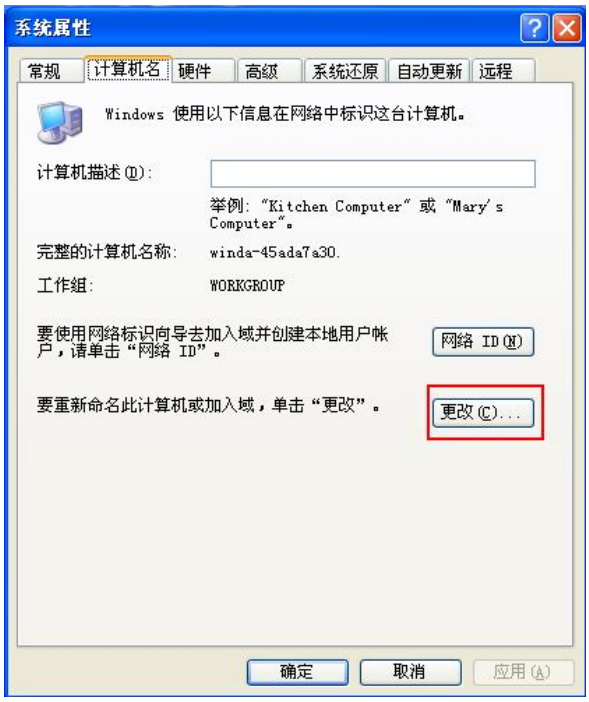



图 1-120 “系统属性”对话框的“计算机名”选项卡

（2）单击“更改”按钮，打开如图 1-121 所示对话框。在“计算机名”文本框中修改本计算机的计算机名为 test-w021，选择“域”单选项，然后在下面的文本框中输入本域网络的 DNS 域名 test.com。

（3）单击“确定”按钮，打开如图 1-122 所示对话框。在这里输入有权把工作站加入域网络的用户账户信息。默认为域管理员组成员，也可以是委派了相应权限的普通用户。在此直接输入域管理员账户 administrator 和对应的密码。

（4）单击“确定”按钮，如果成功加入域网络，则系统会弹出如图 1-123 所示的欢迎加入域网络的提示框。


图 1-121　“计算机名称更改”对话框


图 1-122　“计算机名更改”对话框


图 1-123　欢迎加入域网络提示框

（5）单击“确定”按钮，系统弹出如图 1-124 所示提示框。提示要求重启计算机使更改的设置生效。

（6）单击“确定”按钮，返回到如图 1-120 所示对话框。单击“确定”按钮，系统弹出如图 1-125 所示提示框，询问是否立即重启计算机。单击“是”按钮，系统自动重启计算机。

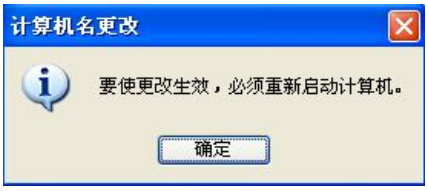



图 1-124　重新启动计算机提示框

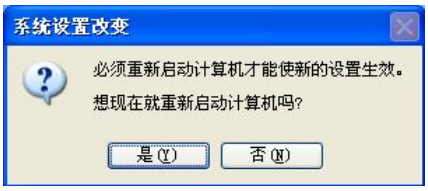



图 1-125　询问现在是否立即重启计算机提示框

通过以上简单的步骤就把一台 Windows XP Professional 工作站计算机成功加入到域网络 test.com 中了。用同样的方法把其他 Windows XP Professional 工作站计算机加入到域网络中。下面介绍 Windows Vista 工作站计算机加入到 Windows Server 2003 域网络的方法。

### 1.7.3　把 Windows Vista 工作站加入域网络

自 Windows Vista 操作系统开始，微软的 Windows 系统在操作方法上发生了一系列本

质性的改变。在加入域网络方面，操作方法也与 Windows 2000 和 Windows XP 系统有些不同，但也需要选择本计算机的 TCP/IP 配置中的首选 DNS 服务器指向域网络中的一台 DNS 服务器（192.168.1.2 或者 192.168.1.3）。下面是具体的配置方法。

（1）在 Windows Vista 工作站的“开始”菜单→“计算机”菜单选项上右击，在弹出菜单中选择“属性”选项，打开如图 1-126 所示窗口。


图 1-126　系统属性窗口

（2）单击“改变设置”按钮，打开如图 1-127 所示对话框。

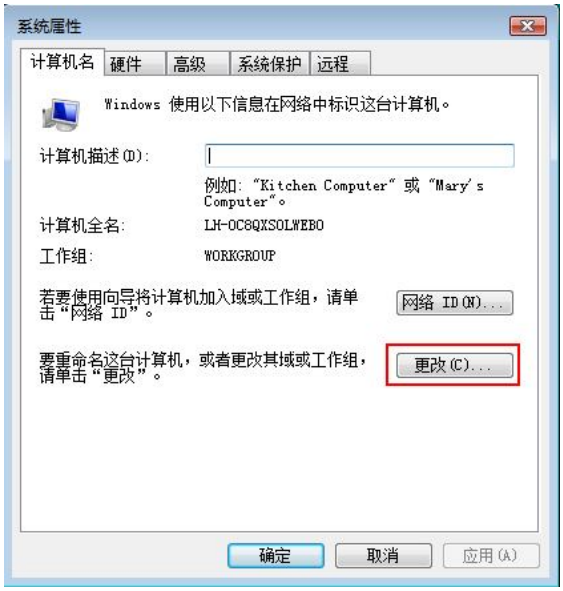



图 1-127　“系统属性”对话框的“计算机名”选项卡

（3）单击“更改”按钮，打开如图 1-128 所示对话框。在这里的“计算机名”文本框中输入为该计算机分配的计算机名 test-w041，选择“域”单选项，然后在下面的文本框中输入本域网络的 DNS 域名 test.com。


图 1-128　“计算机名/域更改”对话框

（4）单击“确定”按钮，打开如图 1-129 所示对话框。在这里同样要输入有权把该计算机加入域网络的用户账户信息。直接输入域管理员账户和密码即可。

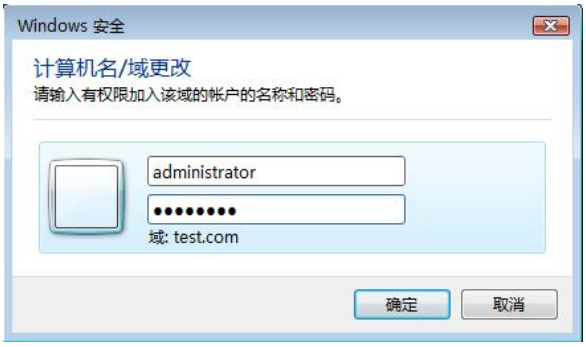



图 1-129　“Windows 安全”对话框

（5）单击“确定”按钮，加入成功后系统会弹出如图 1-130 所示欢迎加入域的提示框。单击“确定”按钮，系统又弹出如图 1-131 所示要求重新启动计算机的提示框。


图 1-130　欢迎加入域提示框

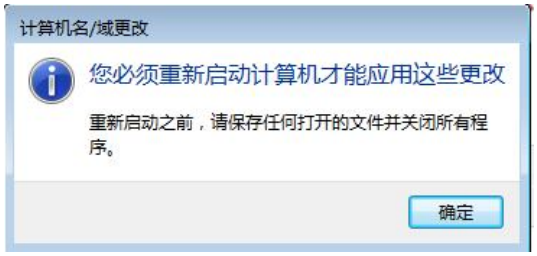



图 1-131　重启计算机提示框

（6）单击“确定”按钮，返回到如图 1-127 所示对话框。单击“确定”按钮，系统弹出询问是否立即重新启动计算机的提示框，如图 1-132 所示。单击“立即重新启动”按钮，系统自动重新启动计算机。这样就成功把一台 Windows Vista 工作站加入到域网络 test.com 中。用同样的方法把其他 Windows Vista 工作站加入到域网络 test.com 中即可。

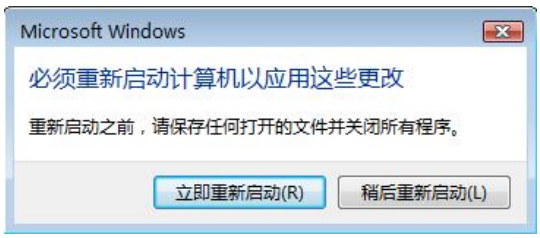



图 1-132　询问现在是否立即重启计算机提示框

以上分别介绍了 Windows 2000 Professional、Windows XP Professional 和 Windows Vista 操作系统计算机加入 Windows Server 2003 域网络 test.com 的方法。无论是有线网络连接还是 WLAN 无线网络连接，配置方法都是一样的。

下面介绍域网络中的组织单位、组和用户账户的创建方法。

# 1.8　添加、配置组织单位、域用户和组

首先是为各部门创建对应的组织单位（OU，要创建的包括工程部、生产部、质管部、人事部、财务部、市场部、行政部，共 7 个部门的 OU），然后在各 OU 下创建对应的用户账户。但要注意，只需要在主域控制器上进行配置即可，额外域控制器通过自动更新可以实现与主域控制器的 AD 数据同步。下面介绍在主域控制器上创建组织单位和域用户账户的方法。

## 1.8.1　创建组织单位

组织单位（OU）是域网络中最小的安全边界，所以在域网络中，组策略的最小部署单位就是组织单位。域控制器也是一个组织单位，所以域控制器也有自己专门的组策略，应用于本地域网络中的所有域控制器。

在企业域网络中，组织单位的划分通常是根据部门进行的，把各部门的用户、组和计算机对象分别移到对应部门的组织单位中，就可以对不同部门的对象进行分别管理和策略应用。但是用户账户属性（如密码策略、Kerberos 策略等）的配置必须是在域级别进行的，不能基于组织单位下的用户账户属性配置。

在本实验中，只是按部门创建一级的 OU，分别是工程部、生产部、质管部、财务部、人事部、行政部、市场部。因为本实验中的网络环境并不复杂，只是单域，单级 OU，所以采用手动创建方式就行了。

OU 的创建很简单，只需要在主域控制器的“Active Diretory 用户和计算机”管理单元控制台的域名（本实验的域名为 test.com）上右击，在弹出菜单中选择“新建”→“组织单位”选项，打开如图 1-133 所示对话框。在“名称”文本框中输入组织单位的名称（如“工程部”），单击“确定”按钮即可。

用同样的方法在域下面创建其他一级组织单位。如果要在现有组织单位下面创建二级甚至三级组织单位，只需在对应的组织单位上右击，同样在弹出菜单中选择“新建”→“组织单位”选项，同样会打开如图 1-133 所示对话框。输入下级组织单位名称后，单击“确定”按钮即可完成新的 OU 创建。


图 1-133 “新建对象－组织单位”对话框

创建好 OU 后，管理员就可以把位于 ADUC 其他容器（如 users、computers）中的用户、组和计算机对象移到对应的 OU 中，实现分部门管理。移动方法是在对应的对象上右击，在弹出菜单中选择“移动”选项，在打开的如图 1-134 所示对话框中选择要把该对象移到 ADUC 的目标容器中，同时也可以更好地应用 OU 中的个性化组策略。


图 1-134 “移动”对话框

在域级别创建好全部 OU 后的 ADUC 管理单元如图 1-135 所示。创建好后，过 15 分钟左右，额外域控制器会自动从主域控制器上复制这些新建的组织单位数据，以实现 AD 数据同步。

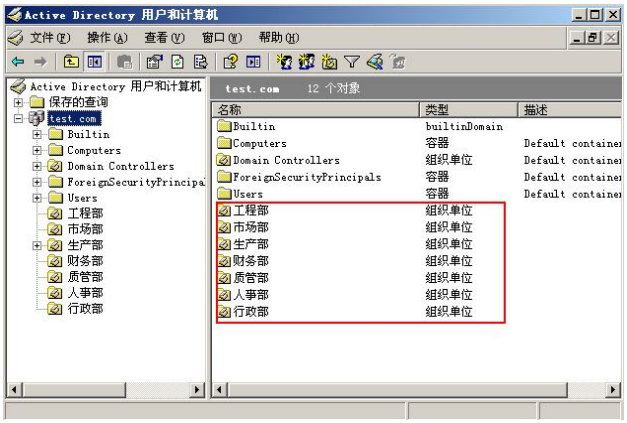



图 1-135 新创建的组织单位

### 1.8.2 批量创建域用户账户

单个用户账户的创建方法很简单，但对于新建、升级或者迁移的域网络来说，通常不是采用一个个用户账户创建的方法，而是采用批量导入的方法进行的。

在本级认证教材中的《金牌网管师——中小型企业网络组建、配置与管理》一书中介绍了 ldifde.exe 和 csvde.exe 两种域用户账户批量导入的方法，但相比而言，csvde.exe 命令更适合于大批量用户账户的导入，因为它使用的导入文件可以是 Excel 表格格式的，更容易编制。本实验项目将采用 csvde.exe 命令批量导入域用户账户。

现以在 test.com 域主域控制器中的“工程部”组织单位中添加 alice、winda、sally、cindy、shelly、hellen、lycb、russy、cathy 和 bob 这 10 个域用户账户为例，一次性批量导入这 10 个域用户账户。至于账户属性只需要配置常见的 DN（域名称）、objectClasss（对象类型）、sAMAccountName（登录账户名）、displayName（显示名）。这些属性的详细说明参见本系列丛书的《金牌网管师——中小型企业网络组建、配置与管理》的第 8 章。

在导入前，无论是 ldifde.exe 命令还是 csvde.exe 命令，在导入用户账户时默认是不能配置用户账户密码的（可以通过添加属性实现密码的导入，但比较复杂，在此不作介绍），所以先要在域级别中暂时禁用账户密码策略，否则导入时因为没有配置密码而出现错误，不能成功导入。

在主域控制器的“组策略编辑器”（GPMC）中，在域默认组策略中按【计算机配置】→【Windows 设置】→【安全设置】→【账户策略】顺序找到“密码策略”项。现对右边窗格的各策略项进行如下设置（配置图如图 1-136 所示）：

- 密码必须符合复杂性要求：禁用（这样就不进行密码复杂性检查）。
- 密码长度最小值：0（这样可以使用空密码）。
- 密码最长使用期限：2 天（配置了下面的最短使用期限后必须配置一个比最短使用期限更长的最长使用期限，不宜设置期限过长，以免出现安全问题）。
- 密码最短使用期限：1 天（以便有足够的时间完成后续配置）。
- 强制密码历史：0（不记住历史密码）。
- 用可还原的加密来储存密码：没有定义。

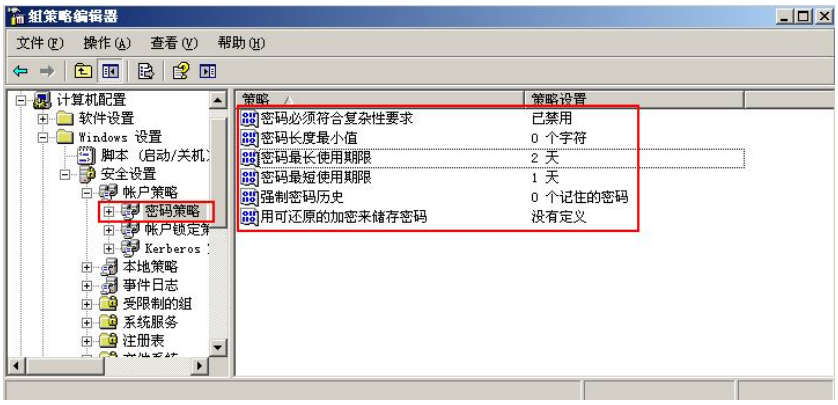
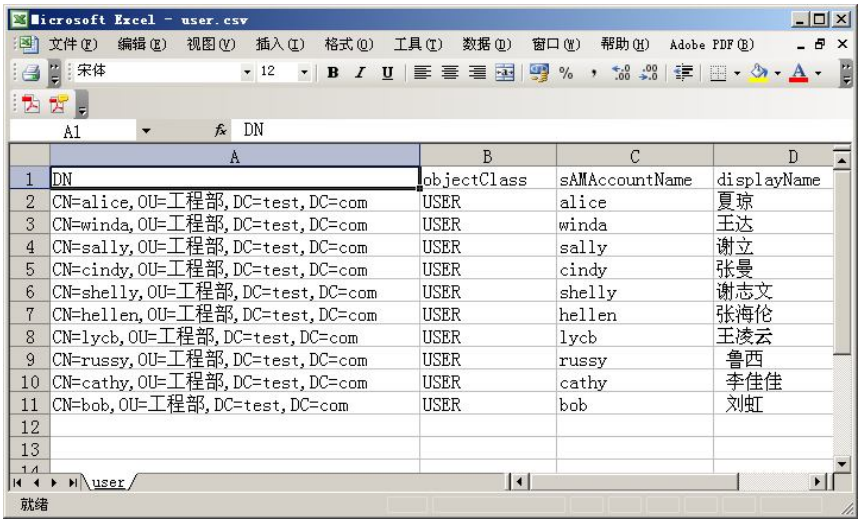



图 1-136 导入空密码账户前的域策略设置

以下是向 test.com 域的主域控制器的“工程部”组织单位中添加以上 10 个域用户的 csv 格式的文本内容（标识符号要用半角西文格式输入）。把它放进记事程序中，以 user.csv（文件名可以随意，文件扩展名可以是.txt 格式，建议为.csv 格式）文件名保存后，就成了

Excel 表格文档，用 Excel 程序就可以查看了，如图 1-137 所示。

```
DN,objectClass,sAMAccountName,displayName
"CN=alice,OU=工程部,DC=test,DC=com",USER,alice,夏琼
"CN=winda,OU=工程部,DC=test,DC=com",USER,winda,王达
"CN=sally,OU=工程部,DC=test,DC=com",USER,sally,谢立
"CN=cindy,OU=工程部,DC=test,DC=com",USER,cindy,张曼
"CN=shelly,OU=工程部,DC=test,DC=com",USER,shelly,谢志文
"CN=hellen,OU=工程部,DC=test,DC=com",USER,hellen,张海伦
"CN=lycb,OU=工程部,DC=test,DC=com",USER,lycb,王凌云
"CN=russy,OU=工程部,DC=test,DC=com",USER,russy, 鲁西
"CN=cathy,OU=工程部,DC=test,DC=com",USER,cathy, 李佳佳
"CN=bob,OU=工程部,DC=test,DC=com",USER,bob, 刘虹
```




| | A | B | C | D |
|---|---|---|---|---|
| 1 | DN | objectClass | sAMAccountName | displayName |
| 2 | CN=alice,OU=工程部,DC=test,DC=com | USER | alice | 夏琼 |
| 3 | CN=winda,OU=工程部,DC=test,DC=com | USER | winda | 王达 |
| 4 | CN=sally,OU=工程部,DC=test,DC=com | USER | sally | 谢立 |
| 5 | CN=cindy,OU=工程部,DC=test,DC=com | USER | cindy | 张曼 |
| 6 | CN=shelly,OU=工程部,DC=test,DC=com | USER | shelly | 谢志文 |
| 7 | CN=hellen,OU=工程部,DC=test,DC=com | USER | hellen | 张海伦 |
| 8 | CN=lycb,OU=工程部,DC=test,DC=com | USER | lycb | 王凌云 |
| 9 | CN=russy,OU=工程部,DC=test,DC=com | USER | russy | 鲁西 |
| 10 | CN=cathy,OU=工程部,DC=test,DC=com | USER | cathy | 李佳佳 |
| 11 | CN=bob,OU=工程部,DC=test,DC=com | USER | bob | 刘虹 |
| 12 | | | | |
| 13 | | | | |
| 14 | | | | |

图 1-137　在 Excel 程序中显示的用户账户导入内容

在主域控制器的命令提示符下输入（假设账户导入文件 user.csv 是保存在 c:\根目录下）：

```
csvde -i -f c:\user.csv
```

最终出现 10 个用户账户导入成功的提示，如图 1-138 所示。有关 csvde.exe 命令的详细使用方法参见本级别认证教材《金牌网管师——中小型企业网络组建、配置与管理》一书。此时可以在主域控制器上的“Active Directory 用户和计算机”管理单元控制台“工程部”组织单位下见到刚导入的 10 个域用户账户，如图 1-139 所示。


图 1-138　域用户账户导入成功的提示框

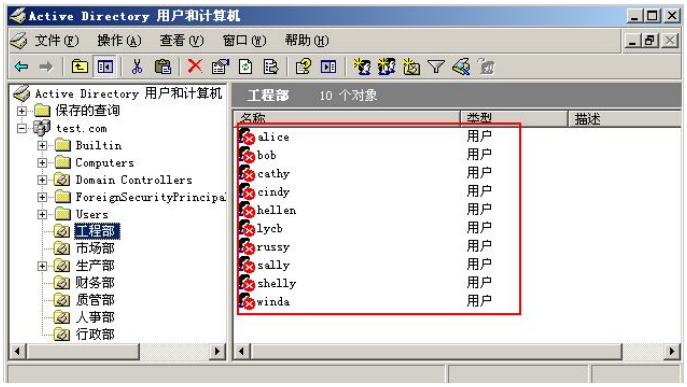



图 1-139　新导入的 10 个域用户账户

此时 10 个用户账户都是默认没有启用（可以在导入时通过添加 userAccountControl 属性来实现导入后即启用的目的，但对于空密码用户账户的导入，这样做比较危险，可能被一些非法人员趁机入侵），在各用户账户上右击，在弹出菜单中选择“启用账户”选项（如图 1-140 所示）启用账户，然后通知用户可以使用账户了。这时在用户第一次使用该账户时密码为空，同时因为域用户账户属性选项中默认选择了“用户下次登录时须更改密码”选项（如图 1-141 所示），所以在用户使用这些新创建的域账户登录域网络时会自动提示用户必须修改密码（这时要求按密码复杂性策略要求配置新密码）。然后管理员在主域控制器上修改上面提到的密码策略，启用密码复杂性策略。

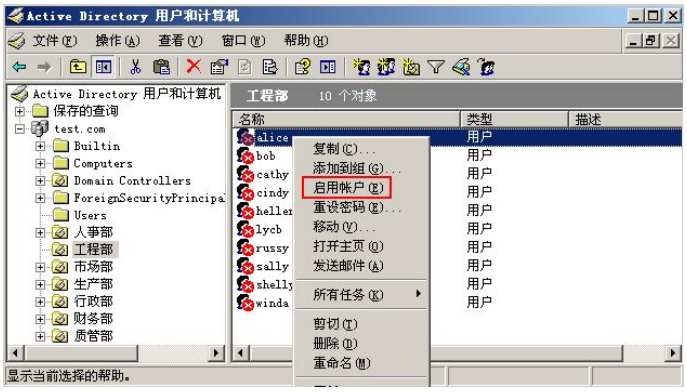



图 1-140　“启用账户”快捷菜单

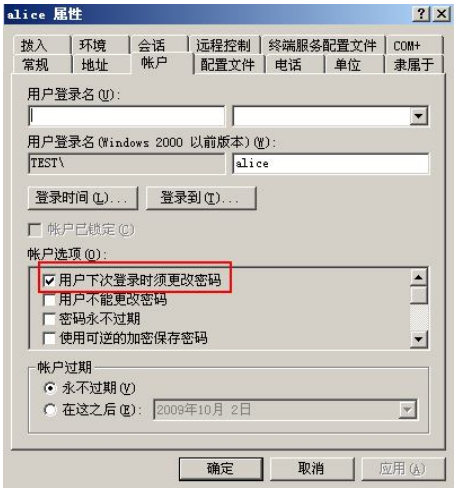



图 1-141　用户账户选项配置对话框

这样就实现了域用户账户的批量创建与配置了。下面介绍域组账户的创建。

### 1.8.3 创建和配置域组账户

为了方便用户权限设置以及对用户的管理，有时需要创建一系列的域组账户，然后再把具有某种相同权限需求的用户加入到相应的域组中。这样在为这些用户配置权限时就不需要一个个地配置，只需要把对应的组再加入到系统内置组中，或者为对应的域组账户委派相应的权限，就可以使组中所有成员账户都具有相应的权限。

如在配置组策略时，往往是仅允许某个部门或者某个管理角色的用户或组账户具有或者不具有某种权限（如网络访问某类工作站的权限），这时只需要把这个组账户添加到许可或者禁止的用户列表中就可以了，而不必一一添加具体的用户账户。这对于一个有着几百、几千用户的域网络来说，其意义更显得特别重大。

在 1.7.1 节中为各部门创建了单独的 OU，并为各 OU 新建或者移动了所需的用户和计算机账户。为了便于以后组策略的配置，在此为各 OU 创建一个域用户组。在此仅以 “工程部”OU 为例进行介绍，其他 OU 中的域用户组创建方法完全一样。

（1）在主域控制器 ADUC 控制台的“工程部”OU 上右击，在弹出菜单中选择“新建”→“组”选项，打开如图 1-142 所示对话框。在这里有两方面的选择：一是组作用域的选择，一是组类型的选择。


图 1-142 新建域组账户对话框

域组作用域（也就是组的作用范围）有以下三类：

- 通用组（Universal Group）：可以配置在整个域树或林范围内使用，其成员任一。但只有在 Windows Server 2003 域功能级别时才可以创建，因为这是 Windows Server 2003 域新的组账户类型。Windows 2000 混合模式不能创建通用组。
- 全局组（Global Group）：可以配置在本地域和信任域中使用，成员只能是本地域用户或者全局组账户。
- 本地域组（Domain Local Group）：可以配置在本地域中使用，成员可以是任何信任域的用户、全局组或者通用组。

对于中小型企业单域网络来说，具体创建哪种作用域组账户（只有在 Windows Server 2003 域功能级别才能选择“通用组”作用域类型）都没什么大的关系，因为是单域，以上三种作用域组账户类型的区别不能体现出来。但对这种只需要在本地域中使用的组来说，最合适的组账户类型就是本地域组。

至于组类型方面，可以分为“安全组”和“通讯组”两大类。安全组是指可以配置安全属性的组，通讯组是专用于像电子邮件通信的组。对于要配置权限的组账户来说，一定是安全组，这也是默认的组类型。

（2）在“组名”文本框中输入组账户名称，单击“确定”按钮即可完成一个本地域安全组账户的创建。创建好的本地域安全组如图 1-143 所示。

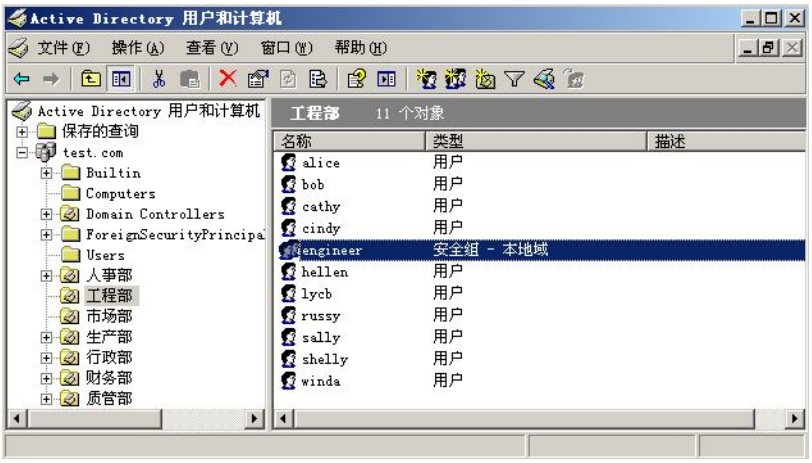



图 1-143　新创建的本地域安全组

（3）创建好域组账户后，还需要向其中添加成员，只有这样，这个组才有意义。添加成员的方法是在组上右击，在弹出菜单中选择“属性”选项，在打开的对话框中选择“成员”选项卡。新创建的组一开始是没有任何成员的，如图 1-144 所示。

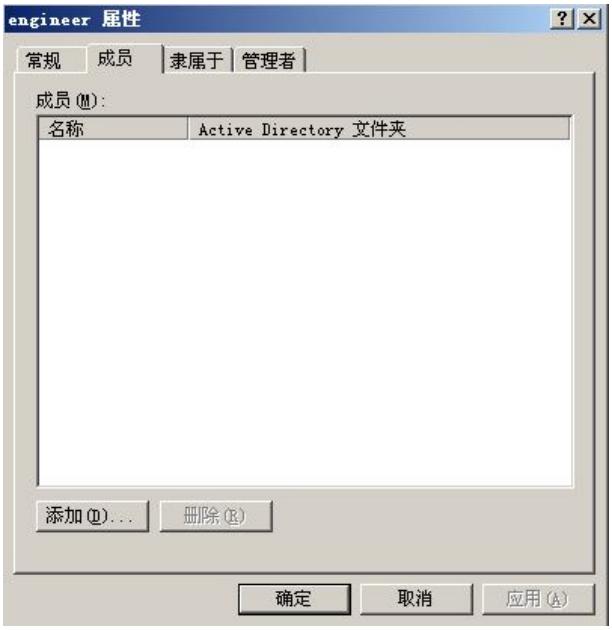



图 1-144　组属性对话框的“成员”选项卡

（4）单击“添加”按钮，打开如图 1-145 所示对话框。单击“对象类型”按钮，打开如图 1-146 所示对话框。从中可以看出，在安全组中不仅可以添加用户账户、其他组账户，还可以添加计算机账户和联系人，只是默认情况下只选择“组”和“用户”两个复选项，所以只能添加用户和组成员。实际上还是可以添加计算机和联系人账户的。可以根据需要选择所需的对象类型复选项。


图 1-145 选择用户、联系人、计算机或组对象对话框


图 1-146 “对象类型”对话框

（5）选择好对象类型选项后单击“确定”按钮，返回到图 1-145 所示对话框中。在这里输入要添加的成员账户（其实只需要输入账户前面几个字母，单击“检查名称”按钮，会自动把匹配已输入字母的对象账户全部列出来，在其中选择要添加的对象账户即可），然后单击“确定”按钮即可把一个对象添加到组成员中。用同样的方法可以添加其他对象到组中，使它们成为该组的成员。

（6）添加好成员后，如果想要为组中成员配置统一权限，可在图 1-144 所示对话框中单击打开“隶属于”选项卡，如图 1-147 所示。


图 1-147 组属性对话框的“隶属于”选项卡

（7）单击“添加”按钮，打开如图 1-148 所示对话框。这个对话框与前面的图 1-145 非常类似，但这里的图 1-148 所示对话框中只能选择组账户对象，不能选择用户、计算机或者联系人对象。输入要隶属的组账户（通常是隶属于自带特定管理权限的内置组）后，单击“确定”按钮，就使当前新建组成为隶属于的组成员。这样做的目的是可以使当前新建组中的所有成员具有现有组的权限，避免了大量的单个用户、计算机或者组对象的权限配置工作。

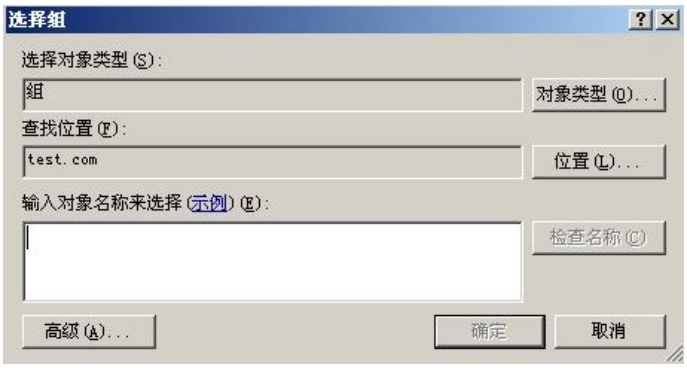



图 1-148　选择组对象对话框

当然，可以不把安全组隶属于其他组中，创建安全组的目的可以只是以一个账户代表组成员的所有账户，以方便在组策略中的各种权限配置。

在主域控制器上创建好 OU、用户和组账户后，开启额外域控制器，过 15 分钟就会自动从主域控制器上复制这些 AD 数据，完成 AD 数据的同步了。

OU、用户和组账户创建好后，一个基本的域网络就组建、配置完成了，本实验也就最终完成了。至于域网络管理方面参见本书的另一个实验——中小型企业域网络管理综合实验。