北京科海培训中心

MCSE考试胜经

Microsoft Certified System Engineer

考试70-216：实现和管理 Microsoft Windows 2000网络基础设施

(Exam70-216)

北京科海集团公司 出品

北京科海培训中心

MCSE 考试胜经——

Windows 2000 Network Administration (Exam 70-216)

博雅工作室　编著

北京科海集团公司　出品

2001.9

内 容 提 要

本书是针对微软认证系统工程师（MCSE）核心考试课程“实现和管理 Microsoft Windows 2000 网络基础设施”（考试号 70-216）的参考书。内容涵盖了这门考试的所有知识要点，尽可能详细地讲授了 MCSE 应试者所应该掌握的所有技能。针对每个考试目标，在各章中提供了大量的模拟试题，可以使您在快速复习考试内容的同时，进一步巩固所学知识。

本书由具有丰富 MCSE 考试培训经验的认证教师（MCT）编写，是参加 MCSE 考试人员的必备考试辅导教材。

书　　名：MCSE 考试胜经——Windows 2000 Network Administration (Exam 70-216)
作　　者：博雅工作室
责任编辑：张律
出　　品：北京科海集团公司
印 刷 者：北京门头沟胶印厂
发　　行：新华书店总店北京科技发行所
开　　本：800×1000　1/16　印张：16.75　字数：368 千字
版　　次：2001 年 9 月第 1 版　2001 年 9 月第 1 次印刷
印　　数：0001-5000

前　言

计算机国际认证考试，作为世界各大著名的计算机厂商推出的一套旨在测量和评估专业技术人员技术水平的认证体系，可以证明应试者具有精通公司某项产品，具备安装、维护和支持计算机系统工作的能力。通过认证，就意味着能够在迅猛发展的计算机行业中抓住更多的机会，获取最新的技术，完成新旧技能更新的挑战，在业界处于领先地位。同时，通过了认证考试，在您个人的奋斗史上也就相应地增加了一枚很有份量的砝码。

微软认证系统工程师（MCSE）证书在众多的计算机国际认证考试中显得最炙手可热。该认证是为从事网络工作的专业人员而设立的，用以证明您有能力利用微软相关产品如 Windows 2000 和 BackOffice 家族的集成服务器产品构建计算机网络环境，以及对信息系统进行有效的规划、实现、维护和支持。

Windows 2000 MCSE 认证考试，包含 4 门核心考试课程。本书是专门针对其中的“实现和管理 Microsoft Windows 2000 网络基础设施”（考试号 70-216）考试而设计，内容包括如何管理 DNS 服务、配置 DHCP 服务、配置 WINS 服务、管理 Windows 2000 网络结构中的远程访问、管理 Windows 2000 网络结构中的网络协议、配置 IP 路由、管理 NAT 以及管理认证服务等考试要点，并为每章内容精心挑选了大量的模拟试题，使您可以充分了解这门考试的要求和题型。模拟试题的标准答案和详尽解释，更可以使您打开思路，触类旁通。

通过本书，您可以进行最有效地模拟测试，对考试内容进行快速复习，以便在认证考试中获得优异成绩。

本书由博雅工作室策划并组织编写，杨军、段洪涛、李超、郝艳芬等人参加了本书的写作工作，在此，表示深深的感谢。由于本书涉及的内容丰富，加之篇幅、时间所限，书中不足之处，敬请读者批评指正。

博雅工作室

2001 年 9 月

目 录

第 1 章　Windows 2000 网络结构中 DNS 的管理

1.1　知识要点

DNS（Domain Name System，域名系统）的应用与 Internet 息息相关。然而，私有网络也可以使用 DNS 来解析计算机名称和寻找局域网络内部和 Internet 上的计算机。DNS 的一项优点是使用容易被记住的 DNS 名称而不是 IP 地址来解析计算机的名称。另一个好处是允许用户使用和 Internet 相同的命名方式与自己网络内的服务器连接。

域名称方式是为 DNS 数据库提供层次结构的 naming scheme（命名方式）。DNS 数据库以名称作为索引，所以每个域（节点）都需要有一个名称。域名称的层次结构是由 root domain（根域）、top-level domain（顶级域）、second-level domain（二级域）和主机名称所组成。主机名称是 Internet 或是私有网络上的一部特定计算机的名称。主机名称是 FQDN（Fully Qualified Domain Name，完全限定域名）最左边的部分，它说明了这部计算机在域层次结构中的实际地址。

本章将介绍关于管理和监控 DNS 的基本技能和知识。

1.1.1　DNS 简介

很多时候，我们提到 DNS 总会与 Internet 网络有关。然而，私有专用网络也可以在自己的网络区域中创建 DNS 来解析计算机名称，以便找出计算机在网络中的位置。DNS 具有以下好处：

- DNS 名称更接近于人类的自然语言，这意味着它比 IP 地址更容易记住。
- DNS 名称比起 IP 地址更能保持不变。
- DNS 允许使用者使用与 Internet 网络一样的命名规则来与网络中的服务器相连接。

DNS 定义

DNS 是一种组织成域层次结构的计算机和网络服务命名系统。DNS 命名用于 TCP/IP 网络，如 Internet，用来通过用户友好的名称定位计算机和服务。当用户在应用程序中输入 DNS 名称时，DNS 服务可以将此名称解析为与此名称相关的其他信息，如 IP 地址。

多数用户喜欢使用友好的名称（例如 example.microsoft.com）来定位诸如网络上的邮件服务器或 Web 服务器这样的计算机。友好的名称更容易被记住，但是，计算机使用数字地址在网络上通讯。为了更方便地使用网络资源，DNS 的名称服务提供了一种方法，将用户友好的计算机或服务名称映射为数字地址。你如果使用过 Web 浏览器，则应该也使用过 DNS 服务。

图 1-1 显示了 DNS 的基本原理，如何根据计算机名称查询其 IP 地址。

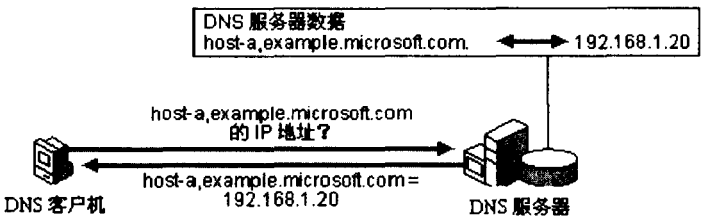

图 1-1 DNS 查询示例

在本例中，客户机查询服务器，请求 DNS 域名为 host-a.example.microsoft.com 的计算机的 IP 地址。由于服务器能够根据其本地数据库应答查询，因此服务器将已包含所请求信息的应答回复给客户机，即包含 host-a.example.microsoft.com 的 IP 地址的信息 A（主机）资源记录。

此例显示了单个客户机和服务器之间的简单 DNS 查询。

域名称空间

DNS 数据库以名称作为索引的依据。因此，每个域都必须要有一个名称。当向层次结构中加入一个域时，上一层域的名称就会附加到下一层子域名称后面，因而，能区分出各个域在层次结构中的关系。例如，在 sales.Microsoft.com 域名称中，sales 域是 microsoft.com 域的子域，而 microsoft 为 com 的子域。

域名称空间的层次结构是由根域、顶级域、第二层域和其他子域以及主机名称组成的。

根域

根域是这个层次结构的最高层，用点号“.”表示。Internet 的根域由许多组织管理，包括 Network Solutions.Inc 等民营企业。

顶级域

顶级域有两个或三个特性名称代码。顶级域依据组织类别或是地理区域来划分，顶级域内可以包含第一层域和主机名称。表 1-1 提供了一些顶级域名称的例子。

表 1-1 顶级域名称

顶级域名称	说明
Gov	政府部门
Com	民间企业
Edu	学术单位
Org	非商业组织
Au	澳洲的国家域代码

第二层域

企业或组织，如 Network Solutions.Inc，可以在 Internet 上为个人或是团体指定和登录第二层域。第二层域名称包括两个部分：上一层域名称和独立的下一层域名称。表 1-2 提供了一些第二层域名称的范例。

表 1-2　第二层域名称的范例

第二层域名称	说明
eu.gov	美国的教育部
microsoft.com	微软公司
sanford.edu	史丹佛大学
www.org	World Wide Web 组织
Pgov.ou	澳洲总理的网站

子域

组织团体内也可以依内部的部门、事业群和地区的分别而建立子域。子域名称是由 3 部分所组成：顶级域名称、独一无二的第二层域名称和独一无二用来标识部门、事业群的名称，如：sales.Microsoft.com。

主机名称

主机名称是 Internet 上或私有网络上特定的计算机名词。例如，在 Computer1.sales.Microsoft.com 中，Computer1 是一部计算机的主机名称。主机名称包含在一个 FQDN 的最左边，说明一部计算机在域层次架构中总的确实地址。

DNS 使用这个 FQDN 将主机名称在数据库内转换为 IP 地址之后，所有的连接才可以直接进行。

Zone（区域）概念

区域代表一个区段的域名称结构。它提供了一种通过分割域名称结构以方便管理各个区段的方法。

- 在域名称结构中分割多个区域，最主要的目地是将管理工作分散到不同的群组中。例如 microsoft.com 域名称被分割为两个区域：sales.Microsoft.com 和 development.Microsoft.com。这两个区域使得 microsoft 和 sales 这两个域各由一位管理员来管理，而 development 域则由第三位管理员来管理。
- 区域必须包含在一段相连的域名称结构内。无法建立一个仅由 sales.Microsoft.com 和 development.Microsoft.com 两个域所组成的区域，因为这两个域并不相连。

名称服务器

DNS 名称服务器中储存了区域的数据库内容。名称服务器内可以储存一个或是多个区域

的数据库，名称服务器对于该区域范围内的域名称有管理的权限。

1 台名称服务器中包含了主要的区域数据库记录，称为 primary zone database file（主要区域数据库记录）。所以，每个区域至少要有 1 台名称服务器。对于某个区域所做的改变，例如，添加域或是主机，就需要改变服务器上的主要区域数据库记录。

安装多台名称服务器的目的在于提供对主要区域数据库记录备份的功能。多台名称服务器能够提供以下功能：

- 执行区域传输：第 2 台名称服务器借助于第 1 台名称服务器内的主要区域数据库记录取得区域数据库文件的备份，我们称为区域传输。这些备份的名称服务器每隔一段固定的时间会查询含有主要区域数据库文件的第 1 台名称服务器，来更新区域的信息。
- 提供备用：假如包含主要区域数据库文件的第 1 台名称服务器无法使用，其他的名称服务器将自动处理查询的服务。
- 改善远程的访问速度：假如有许多使用者在远程需要使用到 DNS 服务时，可以为远程的网络增加 1 台备份名称服务器，来减少跨越低速的广域网的查询信息流量。
- 减少含有主要区域数据库文件的主名称服务器的查询负担。

区域传输

区域传输是指将区域的信息传输到多台名称服务器的过程，由 master server（上层的名称服务器）将区域的信息复制到 secondary server（下层的名称服务器）。上层的名称服务器提供了区域信息的来源，可以是 primary server（主名称服务器）或是 secondary server（次要名称服务器）的。

区域的复制传输主要有两种方式：

- AXFR（Full Zone Transfer，全部区域的传输）：复制整个的区域信息。大部分的 DNS 系统都可以提供 AXFR 的区域更新方式。当下层名称服务器达到自动更新间隔时间时，它会对上层名称服务器发出 AXFR 的询问要求。下层名称服务器会比较它的区域信息序号是否与上层名称服务器的区域信息相同，如果下层名称服务器发现它的区域信息序号不是最新的，它会将上层名称服务器的区域信息 Pull（拉）到它的数据库中。
- IXFR（Incremental Zone Transfer，增量区域的传输）：只复制区域信息中变更的部分。IXFR 是 Windows 2000 DNS 服务器新增服务的功能，可以避免因更新全部区域的信息而产生的信息流量。IXFR 只会传输变更或新增的记录而不是整个区域的信息。变更或新增的信息会存放在主要的名称服务器中的 Cache（缓存区），并且只会传输到要求复制的尚未更新信息的下层名称服务器中。区域内的复制是由区域信息的序号来控制的。

DNS 允许将 DNS 名称空间分成几个区域，它存储着有关的一个或多个 DNS 域的名称信息。对于包括在区域中的每个 DNS 域名，该区域成为该域的有关信息的权威性信息源。

了解区域和域之间的差异

对于单个 DNS 域名，区域作为存储数据库启动。如果其他的域被添加到用于创建该区域的域下面，则这些域可作为相同区域的一部分，或属于另一个区域。一旦添加了子域，则它可以：

- 作为源区域记录的一部分被管理和包含。
- 被委派到为支持子域而创建的另一区域。

例如，图 1-2 显示了 microsoft.com 域，它包括 Microsoft 的域名。在单个服务器上首次创建 microsoft.com 域时，对于所有的 Microsoft DNS 名称空间，该域配置为单区域。然而，如果这个 microsoft.com 域需要使用子域，那么这些子域必须包含在该区域中或被委派到另一个区域。

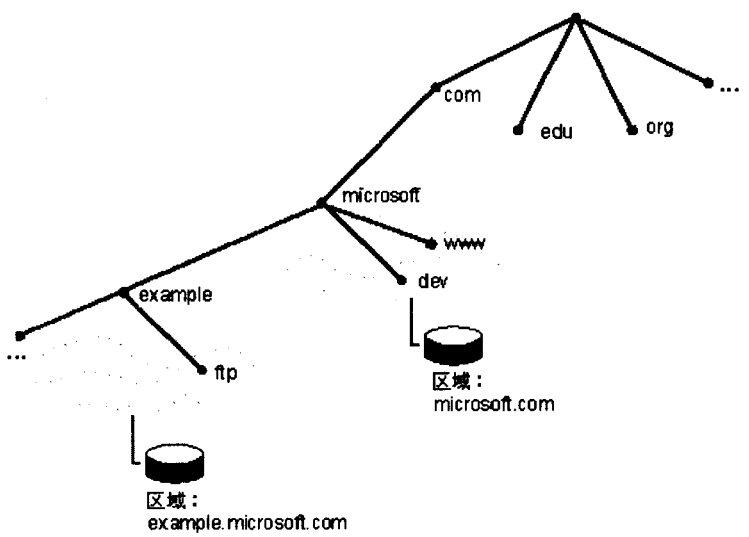

图 1-2　区域和域的差异

在此范例中，example.microsoft.com 域显示了新的子域，example.microsoft.com 由 microsoft.com 域委派并在它自己的区域中内管理。但是，microsoft.com 区域需要包含几个资源记录以提供委派信息，该信息参考了对于委派的 example.microsoft.com 子域具有绝对权威的 DNS 服务器。

如果 microsoft.com 区域不对子域使用委派方式，那么子域的任何数据都保留为 microsoft.com 区域的一部分。例如，虽然没有委派子域 dev.microsoft.com，但是它由 microsoft.com 区

域管理。

为什么需要区域复制和区域传送

由于区域在 DNS 中发挥着重要的作用，因此希望在网络上的多个 DNS 服务器中提供区域，以提供解析名称查询时的可用性和容错。否则，如果使用单个服务器而该服务器没有响应，则该区域中的名称查询会失败。对于提供区域的其他服务器，要求进行区域传送来复制和同步每个服务器上使用的所有区域副本。

当新的 DNS 服务器被添加到网络中，并且配置为现有区域的辅助服务器时，它执行该区域的完全初始传送，以获得和复制该区域的一份完整的资源记录。对于大多数较早版本的 DNS 服务器在实现区域更改后如果区域请求更新，则还将使用相同的完全区域传送方法。对于 Windows 2000 Server，DNS 服务支持递增区域传送，用于为中间的改变修订 DNS 区域传送过程。

递增区域传送

在 RFC 1995 中，递增区域传送被描述为复制 DNS 区域的附加 DNS 标准。当作为区域源的 DNS 服务器和从其中复制区域的任何服务器都支持递增传送时，它提供了公布区域变化和更新的更有效方法。

在较早的 DNS 实现中，更新区域数据的任何请求，都通过使用 AXFR 查询来完全传送整个区域数据库。它允许辅助服务器仅找出一些区域的变化，这些变化将用于区域副本与源区域（可以是另一个 DNS 服务器维护的区域主要副本或次要副本）之间的同步。

通过 IXFR 区域传送时，区域的复制版本和源区域之间的差异必须首先确定。如果该区域识别为与每个区域的 SOA（Start of Authority，启动授权机构）资源记录中序列号字段所指示的版本相同，则不进行任何传送。

如果源区域中区域的序列号比申请辅助服务器中的大，则传送的内容仅由区域中每个递增版本的资源记录的改动组成。为了使 IXFR 查询成功并发送更改的内容，此区域的源 DNS 服务器必须保留递增区域变化的历史记录，以便在应答这些查询时使用。实际上，递增传送过程在网络上需要更少的通信量，而且区域传送完成得更快。

区域传送可能会发生在以下任何情况中：

- 当区域的刷新间隔时间到期时。
- 当主服务器向辅助服务器通知区域更改时。
- 当 DNS 服务器服务在区域的辅助服务器上启动时。
- 在区域的辅助服务器使用 DNS 控制台，以便手动启动来自主服务器的传送时。

区域传送始终在区域的辅助服务器上开始，并且发送到作为区域源的配置主服务器中。主服务器可以是加载区域的任何其他 DNS 服务器，如区域的主服务器或另一辅助服务器。当主服务器接收区域的请求时，它可以通过区域的部分或全部传送来应答辅助服务器。

如图 1-3 所示，服务器之间的区域传送按顺序进行。该过程取决于区域在以前是否复制

过或者是否在执行新区域的初次复制。

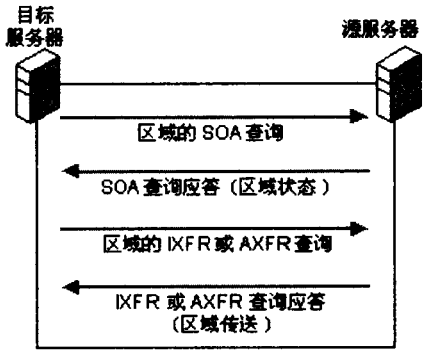

图 1-3　区域传送示例

在该示例中，请求辅助服务器（区域的目标服务器）及其源服务器（提供区域的另一 DNS 服务器）按以下顺序执行。

（1）在进行新的配置期间，目标服务器向主 DNS 服务器（配置为区域源）发送初始“所有区域”传送请求。

（2）主（源）服务器响应辅助（目标）服务器并将此区域完全传送到该服务器。该区域将发送给请求传送的目标服务器，通过启动授权机构 SOA 资源记录（RR）的属性中的“序列号”字段建立的版本一起传送。SOARR 也包含一个以秒计的状态刷新间隔（默认是 900 秒或 15 分钟），以指出目标服务器下一次应在何时请求使用源服务器来续订该区域。

（3）刷新间隔时间到期时，目标服务器使用 SOA 查询来请求从源服务器续订此区域。

（4）源服务器应答其 SOA 记录的查询。在源服务器，该响应包括当前状态的区域序列号。

（5）目标服务器检查响应中的 SOA 记录的序列号，并确定怎样续订该区域。如果 SOA 响应中的序列号值等于其当前的本地序列号，则它做出结论区域在两个服务器中都相同并且不需要区域传送。然后，目标服务器根据来自源服务器的 SOA 响应中的该字段值重新设置其刷新间隔，来续订该区域。如果 SOA 响应中的序列号值比其当前本地序列号要高，则可以确定此区域已更新并需要传送。

（6）如果这个目标服务器推断此区域已经更改，它会把 IXFR 查询发送至源服务器，包括此区域的 SOA 记录中序列号的当前本地值。

（7）源服务器通过区域的递增传送或完全传送做出响应。如果源服务器通过对已修改的资源记录维护最新递增区域变化的历史记录来支持递增传送，则它可通过此区域的 IXFR 做出应答。如果源服务器不支持递增传送或没有区域变化的历史记录，则它

可通过 AXFR 做出应答。

动态更新

动态更新允许 DNS 客户机在发生更改的任何时候，使用 DNS 服务器注册和动态地更新其资源记录。它减少了对区域记录进行手动管理的需要，特别是对于频繁移动或改变位置，并使用 DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）获得 IP 地址的客户机更是如此。

如 RFC 2136 中所述，Windows 2000 对动态更新的使用提供客户和服务器支持。对于 DNS 服务器，DNS 服务允许在配置使用加载标准主机或目录集成区域的每台服务器上，在每个区域基础上启用或禁用动态更新。在默认情况下，对 TCP/IP 进行配置时，在 Windows 2000 任何版本下运行的客户机动态地更新 DNS 中的 A（主机）资源记录。

Windows 2000 计算机如何更新其 DNS 名称

在默认情况下，运行 Windows 2000 而且静态配置 TCP/IP 的计算机尝试为由其安装的网络连接所配置和使用的 IP 地址动态注册 A（主机）和 PTR（Pointer Record，指针记录）资源记录。在默认情况下，所有计算机都在其“完整计算机名”的基础上注册记录。

对于 Windows 2000 计算机，主要的完整计算机名，即 FQDN 基于以下系统设置：

附加到“计算机名”的“该计算机的主 DNS 后缀”。

这两个设置都在 System Properties（系统属性）中的 NetWork（网络标识）选项卡中显示和配置。下列任何原因或事件都可导致发送动态更新内容：

- 在 TCP/IP 属性配置中，为任何一个已安装的网络连接添加、删除或修改 IP 地址。
- IP 地址租用，通过 DHCP 服务器更改或续订任何一个已安装的网络连接。例如，当启动计算机时或在使用 Ipconfig/renew 命令时。
- 用 Ipconfig/registerdns 命令手动执行 DNS 中客户机名称注册的刷新。
- 在启动计算机时。

当上述的其中一个事件触发动态更新操作时，DHCP 客户服务（非 DNS 客户服务）发送更新内容。它是这样设计的，如果由于 DHCP 的原因而使 IP 地址信息发生变化，则会在 DNS 中进行相应的更新，为该计算机同步名称到地址的映射。DHCP 客户机服务为在系统上使用的所有网络连接执行该功能，包括未配置使用 DHCP 的连接。

1.1.2 管理和监控 DNS

建立正向查找区

Forward Lookup Zones（正向查询区域）能够传输正向查询。在名称服务器上，为了让 DNS 服务能够运作，必须至少设定一个正向查询区域。

建立一个新的正向查询区域，先在正向查询区域文件夹上单击鼠标右键，然后会出现一个安装向导引导完成整个步骤。这个向导会展示下列的设定选项：Zone Type（区域类型）、

Zone Name（区域名称）及 Zone File（区域数据库文件名称），如图 1-4 所示。

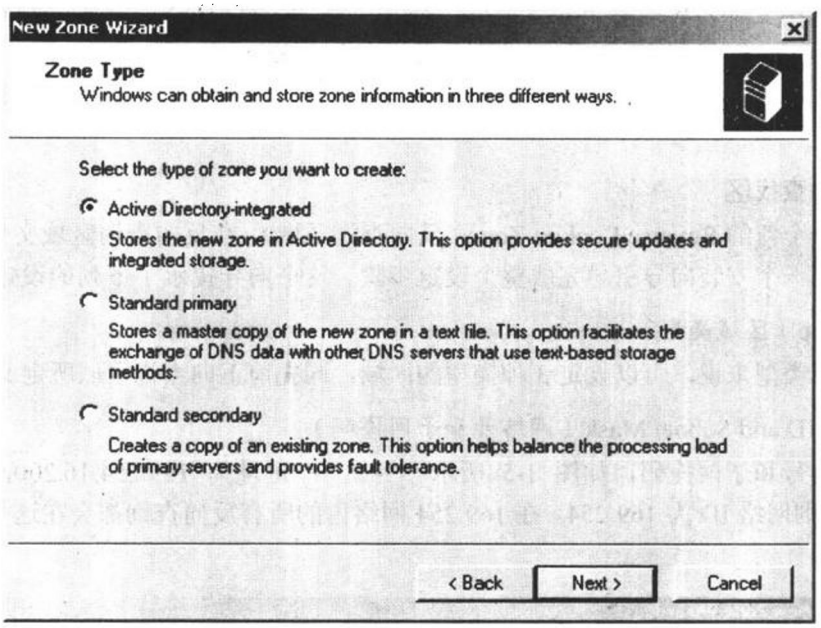

图 1-4　区域类型

Zone Type（区域类型）

可以设定 3 种类型的区域：

- Standard Primary（标准主区域）：标准主区域包含了新区域的主要备份信息，而且是以标准的文本文件格式来存储的。标准主区域区域的维护与管理是在建立该区域的电脑上执行的。
- Standard Secondary（标准二级区域）：标准的二级区域是既有主区域的备份复制。二级区域是只读的，并且以标准的文字文件格式来存储。必须先设定好标准主区域区域，才能够设定二级区域。建立二级区域的时候，必须指定一台称为主服务器的 DNS 服务器，这台服务器会将区域信息传输到含有标准二级区域的名称服务器上。标准的二级区域主要是作为备份以及降低主名称服务器中区域数据库文件的负担。
- Active Directory Integrated（活动目录集成区）：Active Directory 集成目录区域是一个新区域的主要复制信息。该区域使用活动目录的技术来存储和复制区域文件。

Zone Name（区域名称）

一般而言，区域以其层次结构中的顶级域之后的名称来命名，也就是该区域的根域。例如一个区域包含 microsoft.com 和 sales.microsoft.com，区域名称就是 microsoft.com。

Zone File（区域数据库文件名称）

区域数据库文件名称缺省下是区域的名称加上附加名称 DNS。例如，假如区域名称是 microsoft.com，预设的区域数据库名称就是 microsoft.com.dns。

在建立区域之前，必须将现有的文件放在目的计算机的 Systemroot\System32\DNS 文件夹中。

建立反向查找区

要建立一个新的 Reverse Lookup Zone（反向查询区域），在反向查询区域文件夹上单击右键，即会出现一个安装向导引导完成整个设定步骤。这个向导提示了下列的设定选项。

Zone Type（区域类型）

对于区域类型来说，可以设定 3 种类型的区域，同先前正向查询区域所定义的一样。

Network ID and Subnet Mask（网络号和子网掩码）

输入网络号和子网掩码，如图 1-5 所示。例如 IP 地址为 169.254.16.200，子网掩码为 255.255.0.0，则网络 ID 为 169.254。在 169.254 网络内的所有反向查询都会在这个新区域内被解析。

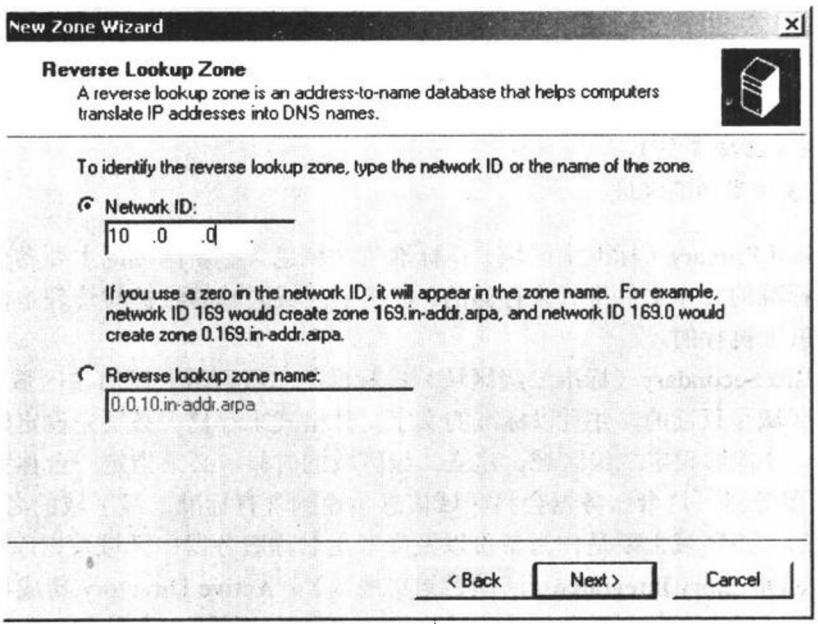

图 1-5 输入反向查询区网络号

Zone File（区域文件名称）

网络 ID 和子网掩码决定了缺省的区域文件名称。DNS 将 IP 的 8 个位反向并加上了 in-addr.arpa 字尾。例如，169.254 网络的反向搜寻区域，就变成了 254.169.in-addr.arpa.dns。当由其他

服务器移植某个区域时，可以存入已有的区域文件。但是必须在建立这个新区域之前，先将此文件放在目的计算机的 systemroot\Sys-tem32\DNS 目录下。

增加记录

区域建立后，就可以继续使用 DNS Snap-in 来添加资源记录。资源记录是区域数据库文件中的记录。如果要加入一笔资源记录，请在要加入记录的区域上单击右键，选择 New（新建），然后选择要加入的记录类别。

资源记录有许多不同的类别。当区域建立时，DNS 会自动的加入两笔资源记录：SOA 和 NS（Name Server，命名服务器）资源记录。

设定动态 DNS

动态更新

可以设定数台授权的服务器启动动态更新，如图 1-6 所示。这些服务器，可以包括次要名称服务器、域控制器，以及其他为用户端执行网络登录的服务器（如执行 DHCP 服务或是 WINS 的服务器）。

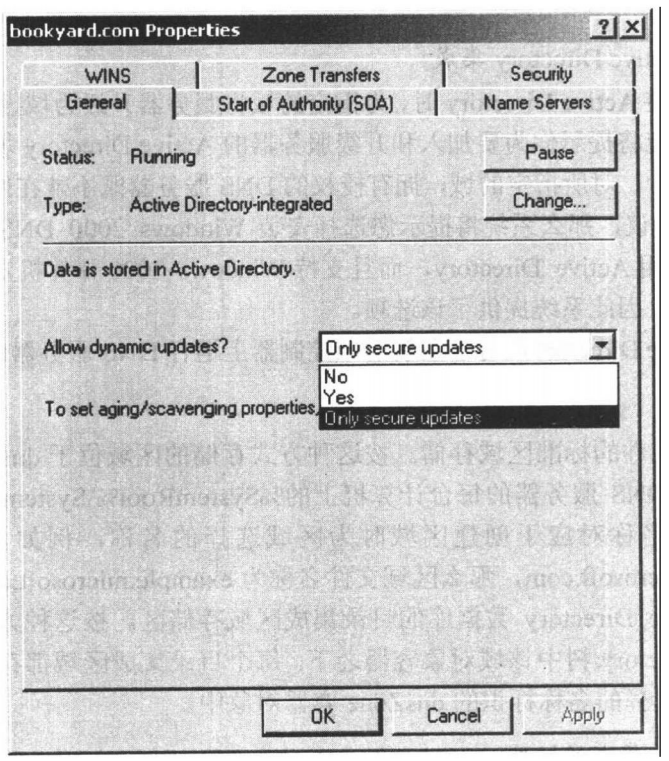

图 1-6　设置动态更新