卓越系列

国家示范性高等职业院校重点建设专业教材（计算机类）

Windows 网络环境管理

主 编 边宇枢

天津大学出版社
TIANJIN UNIVERSITY PRESS

卓越系列·国家示范性高等职业院校重点建设专业教材(计算机类)

Windows 网络环境管理

主　编　边宇枢

天津大学出版社
TIANJIN UNIVERSITY PRESS

内 容 简 介

本书全面介绍了管理基于 Windows 的网络环境的各项应用技术，主要包括：创建域、管理域用户账户与组账户、Web 服务、FTP 服务、电子邮件服务、流媒体服务、代理服务等。旨在引导读者掌握使用活动目录对基于 Windows 的网络环境进行高级管理的技术以及若干重要的面向 Internet 的网络应用技术，初步具备为用户提供网页浏览、文件传输、收发电子邮件、流媒体服务以及安全访问 Internet 等功能的能力。

本书突出实用性和可操作性，语言通俗易懂，配有大量演示性图例，内容循序渐进，具有较好的学习参考价值。适合高等院校相关专业学生学习使用，也可作为从事 Internet 工作的科技人员和广大爱好者的学习参考书。

图书在版编目(CIP)数据

Windows 网络环境管理/边宇枢主编. —天津：天津大学出版社，2009.3
(卓越系列)
国家示范性高等职业院校重点建设专业教材. 计算机类
ISBN 978-7-5618-2946-2

Ⅰ. W… Ⅱ. 边… Ⅲ. 窗口软件，Windows－高等学校：技术学校－教材 Ⅳ. TP316.7

中国版本图书馆 CIP 数据核字(2009)第 030712 号

出版发行	天津大学出版社
出 版 人	杨欢
地　　址	天津市卫津路 92 号天津大学内(邮编：300072)
电　　话	发行部：022-27403647　邮购部：022-27402742
网　　址	www.tjup.com
印　　刷	天津泰宇印务有限公司
经　　销	全国各地新华书店
开　　本	169mm×239mm
印　　张	12.75
字　　数	272 千
版　　次	2009 年 3 月第 1 版
印　　次	2009 年 3 月第 1 次
印　　数	1－3 000
定　　价	25.00 元

卓越系列·国家示范性高等职业院校重点建设专业教材(计算机类)

编审委员会

总序

“卓越系列·国家示范性高等职业院校重点建设专业教材(计算机类)”(以下简称“卓越系列教材”)是为适应我国当前的高等职业教育发展形势,配合国家示范性高等职业院校建设计划,以国家首批示范性高等职业院校建设单位之一——天津职业大学为载体而开发的一批与专业人才培养方案捆绑、体现工学结合思想的教材。

为更好地做好“卓越系列教材”的策划、编写等工作,由天津职业大学电子信息工程学院院长丁桂芝教授牵头,专门成立了由高职高专院校的教师和企业、研究院所、行业协会、培训机构的专家共同组成的教材编审委员会。教材编审委员会的核心组成员为丁桂芝、邱钦伦、杨欢、徐孝凯、安志远、高文胜、李韵琴。核心组成员经过反复学习、深刻领会教育部《关于全面提高高等职业教育教学质量的若干意见》(教高[2006]16号)及教育部、财政部《关于实施国家示范性高等职业院校建设计划 加快高等职业教育改革与发展的意见》(教高[2006]14号),就“卓越系列教材”的编写目的、编写思想、编写风格、体系构建方式等方面达成了如下共识。

1. 核心组成员发挥各自优势,物色、推荐“卓越系列教材”编审委员会成员和教材主编,组成工学结合作者团队。作者团队首先要学习、领会教高[2006]16号文件和教高[2006]14号文件精神,转变教育观念,树立高等职业教育必须走工学结合之路的思想。校企合作,共同开发适合国家示范性高等职业院校建设计划的教学资源。

2. “卓越系列教材”与国家示范校专业建设方案捆绑,力争成为专业教学标准体系和课程标准体系的载体。

3. 教材风格按照课程性质分为理论+实验课程教材、职业训练课程教材、顶岗实习课程教材、有技术标准课程教材和课证融合课程教材等类型,不同类型教材反映了对学生不同的培养要求。

4. 教材内容融入成熟的技术标准,既兼顾学生取得相应的职业资格认证,又体现对学生职业素质的培养。

追求卓越是本系列教材的奋斗目标，为我国高等职业教育发展勇于实践、大胆创新是“卓越系列教材”编审委员会努力的方向。在国家教育方针、政策引导下，在各位编审委员会成员和作者团队的协同工作下，在天津大学出版社的大力支持下，向社会奉献一套“示范性”的高质量教材，不仅是我们的美好愿望，也必须变成我们工作的实际行动。通过此举，衷心希望能够为我国职业教育的发展贡献自己的微薄力量。

借“卓越系列教材”出版之际，向长期以来给予“卓越系列教材”编审委员会全体成员帮助、鼓励、支持的前辈、专家、学者、业界朋友以及幕后支持的家人们表示衷心感谢！

“卓越系列教材”编审委员会

2008 年 1 月于天津

前言

在众多的网络操作系统中，Windows 网络操作系统由于具有功能强大、界面友好、易于操作等优点，目前正在各行各业中被广泛使用。因此，为了能够更好地满足企业的各种实际需求，尤其是面向 Internet 的需求，在掌握了 Windows 网络操作系统的基本管理知识与技术的基础上，还需要进一步掌握管理基于 Windows 的网络环境的高端应用技术。

本书是国家示范性高等职业院校重点建设的计算机类专业教材之一，比较全面地介绍了基于 Windows 网络环境的各项重要应用技术，旨在引导读者掌握使用活动目录对基于 Windows 的网络环境进行高级管理的技术以及面向 Internet 的多项网络应用技术，初步具备为用户提供网页浏览、文件传输、收发电子邮件、流媒体服务以及安全访问 Internet 等功能的能力。书中的内容并不片面追求理论深度，而是侧重突出相关技术的应用与实践，做到实用性与可操作性并重。在章节的安排上，强调基本概念的介绍，注重由浅入深、循序渐进，详细介绍了各项管理工作的配置步骤并且配有大量演示性图例。本书语言精练、通俗易懂，非常适合初学者的学习；适合于高等院校相关专业学生学习使用，也可作为从事 Internet 工作的科技人员和广大爱好者的学习参考书。

为了帮助任课教师更好地备课，按照教学计划顺利完成教学任务，我们将对选用本教材的授课教师免费提供一套包括电子教案、教学大纲、教学计划、教学课件，本门课程的电子习题库、电子模拟试卷、实验指导、有关例题源代码等在内的完整的教学解决方案，从而为读者提供全方位的、细致周到的教学资源增值服务（索取教师专用版光盘的联系电话：022－85977234，电子信箱：zhaohongzhi1958@126.com）。

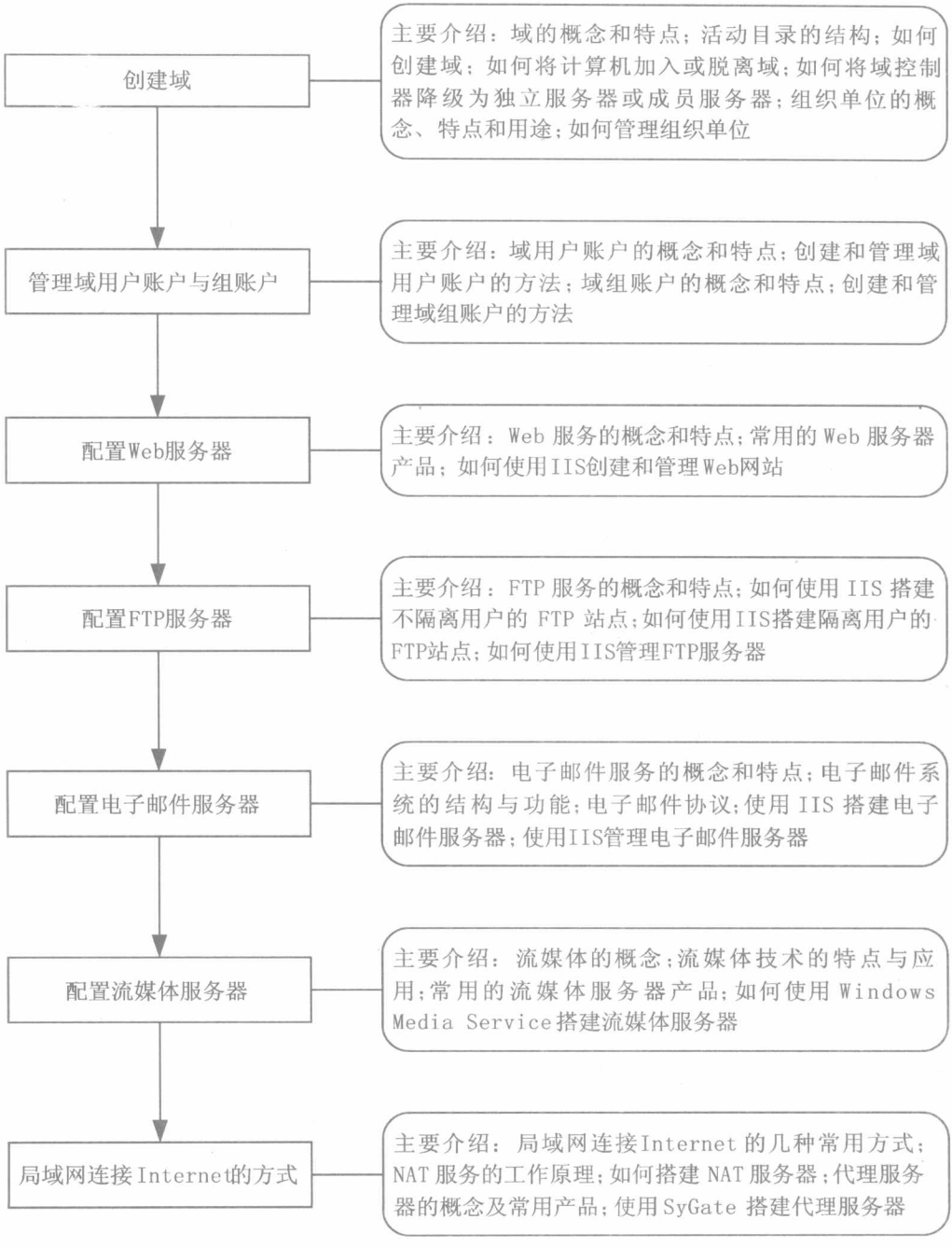
本教材由边宇枢老师负责全书的整体安排、内容选择和编写工作。在编写的过程中，得到邱钦伦老师、高志慧老师等的大力支持，他们为本书提供了大量宝贵的建议。此外，天津大学出版社的编辑也为本书投入了很大的精力，在此一并致谢。

由于编写时间较短，书中错误之处在所难免，希望广大读者给予指正。

作　者

2009 年 2 月

学习引导


创建域
主要介绍：域的概念和特点；活动目录的结构；如何创建域；如何将计算机加入或脱离域；如何将域控制器降级为独立服务器或成员服务器；组织单位的概念、特点和用途；如何管理组织单位
管理域用户账户与组账户
主要介绍：域用户账户的概念和特点；创建和管理域用户账户的方法；域组账户的概念和特点；创建和管理域组账户的方法
配置Web服务器
主要介绍：Web服务的概念和特点；常用的Web服务器产品；如何使用IIS创建和管理Web网站
配置FTP服务器
主要介绍：FTP服务的概念和特点；如何使用IIS搭建不隔离用户的FTP站点；如何使用IIS搭建隔离用户的FTP站点；如何使用IIS管理FTP服务器
配置电子邮件服务器
主要介绍：电子邮件服务的概念和特点；电子邮件系统的结构与功能；电子邮件协议；使用IIS搭建电子邮件服务器；使用IIS管理电子邮件服务器
配置流媒体服务器
主要介绍：流媒体的概念；流媒体技术的特点与应用；常用的流媒体服务器产品；如何使用Windows Media Service搭建流媒体服务器
局域网连接Internet的方式
主要介绍：局域网连接Internet的几种常用方式；NAT服务的工作原理；如何搭建NAT服务器；代理服务器的概念及常用产品；使用SyGate搭建代理服务器

目　录

1 创建域

与工作组相比，域具有便于集中管理、伸缩性强以及安全性高等优点，适用于构建网络较大、需要集中管理的网络环境。

本章主要内容

- ☑ 理解域
- ☑ 活动目录的结构
- ☑ 创建域
- ☑ 将计算机加入或脱离域
- ☑ 将域控制器降级为独立服务器或成员服务器
- ☑ 管理组织单位

本章学习要求

- ☑ 理解域的概念、特点
- ☑ 理解活动目录的结构
- ☑ 掌握创建域的方法
- ☑ 掌握将计算机加入或脱离域的方法
- ☑ 掌握将一台域控制器降级为独立服务器或成员服务器的方法
- ☑ 理解组织单位的概念、特点和用途
- ☑ 掌握管理组织单位的方法

1.1 理解域

Windows Server 2003 支持两种网络管理方式:工作组和域。工作组网络的特点是成本低、安全性低、不能进行集中管理,适合于构建小型网络。与工作组网络相比,域具有便于集中管理、伸缩性强和安全性高等优点,适用于构建网络较大、需要集中管理的网络环境。

1.1.1 域的概念

域是由一组用网络连接在一起的计算机组成的(见图 1.1),它们将计算机内的资源(如文件或打印机)给用户共享访问。与工作组不同的是,域内所有的计算机共享一个集中式的安全数据库,该数据库包含着整个域中所有的用户账户信息、安全信息和资源信息。负责管理与维护这个安全数据库的功能组件被称为“活动目录”(Active Directory),该安全数据库就是活动目录数据库。

在一个 Windows 网络中可以有多个域,每个域都是一个独立的实体,都是一个独立的安全范围,必须具有不同的名称。域管理员可以对本域内的资源和用户账户进行管理。

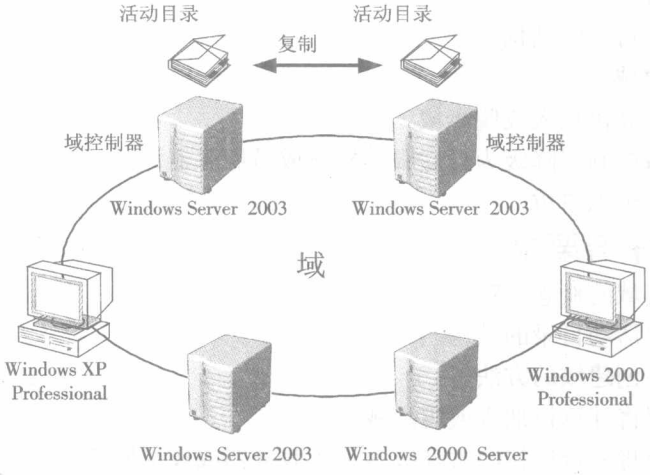


图 1.1 域的结构

1.1.2 域中计算机的角色

在一个域中,可以存在以下几种计算机角色。

1. 域控制器

在域中用来存储活动目录数据库的计算机被称为“域控制器”(Domain Controller),只有服务器级的计算机才能作为域控制器。在 Windows Server 2003 家族中,Windows Server 2003 标准版、企业版和数据中心版的计算机可以作为域控制器,而 Windows Server 2003 Web 版的计算机不能作为域控制器。一个域中至少具有一台域控制器,也可以有多台域控制器。这些域控制器的地位是平等的,它们都存储着一份相同的活动目录数据库。当任何一台域控制器的活动目录做了更改时,该更改内容会自动复制到其他域控制器的活动目录中,从而保证这些域控制器中活动目录数据的一致性。例如,在任何一台域控制器中建立一个用户账户,该账户将被添加到该域控制器的活动目录数据库中,然后该账户的数据会被自动复制到其他域控制器中。当用户在域中的某台计算机上登录该域时,域中的一台域控制器将根据活动目录数据库来审核该用户账户和密码是否正确。当域中有多台域控制器时,这些域控制器可以实现容错。例如,当一台域控制器出现故障时,其他域控制器仍然可以继续提供服务。此外,还可以实现负载平衡。例如,同时有大量用户账户登录同一个域时,由该域中的多台域控制器对这些用户账户和密码进行审核,从而提高了工作效率。

2. 成员服务器

在域中,那些安装了服务器级操作系统但并不存储活动目录的计算机被称为“成员服务器”。例如,Windows Server 2003、Windows 2000 Server 或 Windows NT Server 计算机都可以是成员服务器。在一个域中,成员服务器不是必须的,可有可无。如果在成员服务器上安装了活动目录,它们便会升级为域控制器;如果从域控制器中卸载了活动目录,它们便降级为成员服务器。另外,如果一台服务器级计算机没有加入到域中,即为工作组中的服务器,则此计算机被称为“独立服务器”。

3. 工作站

在域中,那些安装了客户端操作系统的计算机被称为“工作站”,例如 Windows XP Professional、Windows 2000 Professional 或 Windows NT Workstation 计算机。在一个域中,工作站也不是必须的,可有可无。工作站无法存储活动目录,因而不可能升级为域控制器。用户可以通过工作站登录到域,从而访问域中的资源。

因此,在一个域中,至少需要具有一台域控制器,而成员服务器和工作站可有可无。从而可以得知:一个最简单的域将只包含一台计算机,而这台计算机一定是该域的域控制器。

1.1.3 域的特点

域网络结构具有以下 5 个特点。

(1)域中所有计算机共享一个活动目录数据库,该活动目录数据库包含了整个域中所有的资源信息、用户账户信息与安全信息。在域中,域管理员可以通过管理域的活动目录数据库来实现对整个域的资源和用户账户进行统一的管理,因此域为集

中式管理方式。而在工作组中,每台计算机都有一个 SAM 数据库,并由每台计算机的本地管理员分别管理各自计算机内的资源和用户账户,为对等式管理方式。

(2)一个域具有一个活动目录数据库,而且域中所有的安全信息都集中存储在这个活动目录数据库中,因此管理员可以通过制定强有力的安全策略来保证整个域的安全,所以一个域是一个安全范围。与工作组相比,域网络结构具有更高的安全级别。

(3)在域中,域管理员可以在活动目录数据库中为用户创建"域用户账户"。域用户账户都保存在活动目录数据库中,因此,一个用户只要拥有一个域用户账户,便可以在域中的任意一台计算机上登录,访问域中所有计算机上允许访问的资源。而在工作组中,用户使用本台计算机 SAM 数据库中的用户账户只能访问本台计算机中的资源,而不能访问其他计算机中的资源。与工作组相比,域可以大大简化对用户访问资源的管理。例如:假设在一个工作组中有 100 台计算机,用户王某希望访问这 100 台计算机中的资源,这时管理员需要在 100 台计算机中分别为王某建立用户账户;而在域中,域管理员只需为王某建立一个域用户账户,王某便可以使用该域用户账户访问域中所有计算机中允许他访问的资源。

(4)域适用于构建网络较大、需要集中管理的网络环境。如果企业内的计算机数量较多,而且对网络资源的安全级别要求较高,可以通过创建域来管理网络。

(5)域和域的地位是平等的,互不交叉、互不包容。

1.2 活动目录的结构

如果某个企业或公司中具有大量的计算机和网络资源需要进行管理,只建立一个域可能无法满足需求,这时可以考虑建立多个域,并把这些域组建成"域树"。还可以根据需要建立多个域树,并把多个域树组建成"域森林"。

1.2.1 域树

假设某个企业为了对自己内部的资源进行管理,在企业总部建立了第一个域:a.com。后来,随着企业业务的扩展,在另外两个地点建立了企业分部,这时为了便于管理,需要在这两个地点分别建立域。由于这些域中的资源均属于同一个企业,所以希望其中的用户能够互相访问其他域中的资源。然而,从前面的介绍可以看出,每个域的用户账户原则上只能访问本域内的资源,而不能访问其他域的资源。为了解决此问题,在该企业各分部建立域时,需要在新建立的域与第一个域(a.com)之间建立起某种联系,以实现一个域的用户账户能够利用这种联系来访问另一个域的资源,这种联系被称为"信任关系"。在这里,第一个域被称为"父域",而各分部的域被称为父域的"子域"。在给子域命名时,子域的名称中自动包含其父域的域名,以表明它们之间的信任关系。如图 1.2 所示,父域为 a.com,其两个子域分别为 b.a.com 和 c.

a. com。可见,两个子域的名称中都包含父域的名称,因此它们的域名空间是连续的。同理,在域 b. a. com 和域 c. a. com 的下面还可以继续建立子域,如图 1.2 所示。

父域和子域之间的关系为信任关系,在建立子域时自动形成,而且这种信任关系是双向的,即父域中的用户账户具有访问子域资源的能力,子域中的用户账户也具有访问父域资源的能力。此外,这种信任关系是可传递的,即如果域 a. com 与域 b. a. com 存在着信任关系,域 b. a. com 和域 d. b. a. com 存在着信任关系,那么域 a. com 和域 d. b. a. com 也存在着信任关系。也就是说,域 a. com 的用户账户具有访问域 d. b. a. com 中资源的能力,域 d. b. a. com 的用户账户也具有访问域 a. com 中资源的能力。另外,利用信任关系的可传递性,域 d. b. a. com 和域 f. c. a. com 也为信任关系。图 1.2 所示的公用连续名称空间的若干个域就组合成了一个“域树”。

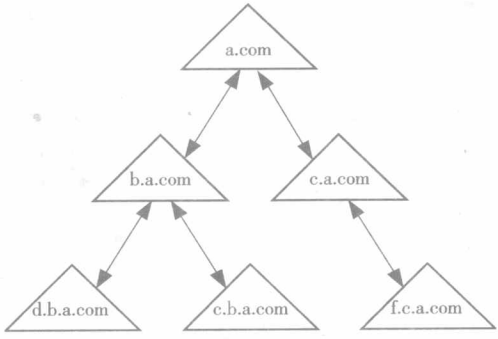


图 1.2 域树

域树具有以下特点。

(1)域树是若干个域的有层次的组合,可以在父域的下面建立子域,还可以在子域的下面再继续建立子域。在一个域树中,第一个域被称为“树根域”。例如在图 1.2 所示的域树中,域 a. com 为该域树的树根域。

(2)在域树中,父域和子域之间的信任关系是自动建立的、双向的、可传递的,因此父域和子域中的用户账户均具有访问对方域中资源的能力。利用这种信任关系的传递性,域树中任何一个域中的用户账户均可以访问域树中所有域中的资源。

(3)域树中的所有域共享了一个连续的域名空间。

(4)在域树中,父域和子域之间的关系不是包含与被包含的关系,而是地位平等的。默认情况下,父域的管理员只能管理父域,而不能管理子域;同样,子域的管理员只能管理子域,也不能管理父域。

(5)域树中的所有域共享了一个活动目录数据库。

(6)最简单的域树中只包含一个域,这个域就是树根域。

1.2.2 域森林

如果一个企业规模非常庞大，这时只建立一个域树往往难以满足管理的需求。可以采用在第一个域树的树根域下，建立第二个域树的树根域。例如图 1.3 中，在第一个域树的树根域 a. com 下建立了第二个域树的树根域 z. net。这两个树根域 a. com 和 z. net 之间也利用双向的、可传递的信任关系联系在一起。然后在第二个域树的树根域 z. net 下面继续建立子域 u. z. net 和 v. z. net，在子域下还可以再继续建立子域。从图 1.3 可以看出，第一个域树和第二个域树都具有自己的连续的名字空间。

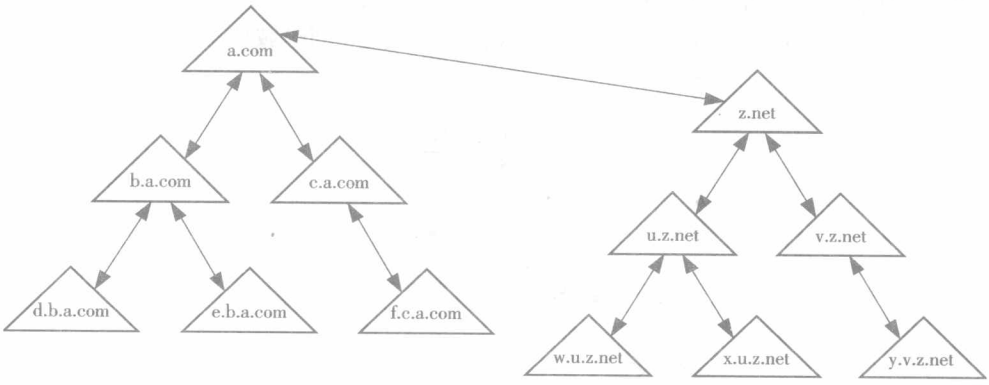


图 1.3 域森林

具有上述特点的若干个域树的组合称为“域森林”。在域森林中，树根域与树根域之间利用双向的、可传递的信任关系联系在一起；而在一个域树中，父域与子域之间也利用双向的、可传递的信任关系联系在一起。所以，利用这种信任关系，域森林中任何一个域的用户账户均可以访问此域森林中任何一个域中的资源。在域森林中，第一个域树的树根域被称为“森林根域”，并且规定森林的名字与森林根域的名字相同。例如在图 1.3 所示的域森林中，森林根域为 a. com，所以该森林的名字便为 a. com。

从活动目录的结构看，一个完整的活动目录应该对应着一个域森林，也就是说，一个域森林共享同一个活动目录数据库。一个域森林可以包含若干个域树，一个域树又可以包含若干个域。因此，域是活动目录中最基本的管理单元。从而可以得知：最简单的域森林将只有一个域树，这个域树中只有一个域，即森林根域，而这个域中只有一台计算机，那就是该域的域控制器。

1.3 创建域

前面已经讲过，一个最简单的域只包含一台计算机，而这台计算机一定是该域的

域控制器。因此为了创建一个域,需要首先创建该域的域控制器。

由于只有服务器级的计算机才能作为域控制器,所以创建域控制器的方法通常是在工作组中的一台独立服务器或者域中的一台成员服务器上,通过安装活动目录,从而把它升级为域控制器,并在安装活动目录的过程中创建新域。

本节主要对创建森林根域的方法进行介绍,即创建域森林中的第一个域,例如创建图 1.3 中的域 a. com。

1.3.1 对域控制器的要求

可以在创建域控制器的过程中创建一个新域。但需要注意的是,并不是任何一台计算机都可以被配置成为域控制器的。作为域控制器的计算机,必须满足以下几个条件。

(1)在 Windows Server 2003 家族中,只有运行 Windows Server 2003 标准版、企业版或数据中心版的服务器才可以被升级为域控制器,而 Windows Server 2003 Web 版的计算机不能成为域控制器。

(2)一台域控制器至少具有 250 MB 的磁盘空间。其中,200 MB 的磁盘空间用于存放活动目录数据库,50 MB 的磁盘空间用于存放活动目录数据库的事务日志文件。

(3)域控制器的磁盘上至少有一个 NTFS 格式的分区。

(4)安装了 TCP/IP 协议,并且配置使用了 DNS 服务,即该计算机可以是一台 DNS 服务器,也可以是一台 DNS 客户机。

(5)安装者必须使用具有创建域的权力的用户账户,例如本地管理员账户。

1.3.2 创建森林根域

由于最简单的域森林将只有一个域树,这个域树中只有一个域,即森林根域,而这个域中只有一台计算机,那就是该域的域控制器,因此本节将要创建最简单的域森林中的森林根域。在创建完成后,将会同时完成以下工作。

- 创建了一个新的域森林。
- 创建了该域森林中的第一个域树。
- 创建了该域树中的第一个域,即树根域。
- 创建了该树根域中的第一个域控制器。

在此以创建图 1.3 所示的森林根域 a. com 中的第一台域控制器 server1. a. com 为例来说明创建森林域的方法。

首先在工作组中选择一台独立服务器,或者在域中选择一台成员服务器,并且这台服务器运行的操作系统必须为 Windows Server 2003 标准版、企业版或数据中心版。然后在该服务器上按照下面的操作步骤创建森林根域中的第一台域控制器。

步骤 1:单击“开始”→“运行”,在弹出的命令行对话框中输入“dcpromo. exe”,从