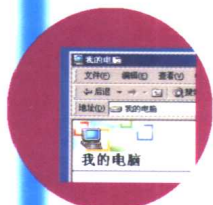
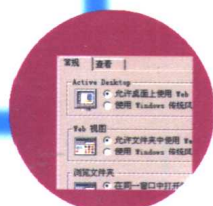




博碩文化



Windows 2000 Server

企业网络建构实务

Active Directory 篇

颜逸品 编著

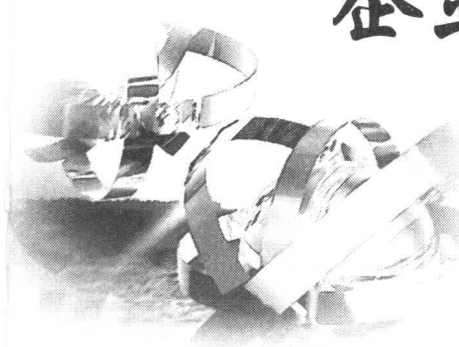


中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE



Windows 2000 Server

企业网络建构实务



~Active Directory 篇

颜逸品 编著

中国铁道出版社

2001·北京

(京)新登字 063 号

北京市版权局著作权合同登记号: 01-2000-3079 号

版 权 声 明

本书中文繁体字版由台湾博硕文化股份有限公司出版, 2000。本书中文简体字版经台湾博硕文化股份有限公司授权由中国铁道出版社出版, 2000。任何单位或个人未经出版者书面允许不得以任何手段复制或抄袭本书内容。

本书贴有博硕文化激光防伪标签, 无标签者不得销售。版权所有, 侵权必究。

图书在版编目(CIP)数据

Windows 2000 Server 企业网络建构实务.Active Directory 篇/颜逸品编著.

—北京: 中国铁道出版社, 2001. 1

ISBN 7-113-04050-0

I. W… II. 颜… III. 内联网-服务器-操作系统(软件), Windows 2000 Server IV. TP393.18

中国版本图书馆 CIP 数据核字(2000)第 88286 号

书 名: Windows 2000 Server 企业网络建构实务——Active Directory 篇

作 者: 颜逸品

出版发行: 中国铁道出版社(100054, 北京市宣武区右安门西街 8 号)

策划编辑: 苏 茜

特邀编辑: 袁秀珍

封面设计: 冯龙彬

印 刷: 北京市燕山印刷厂

开 本: 787×1092 1/16 印张: 26.75 字数: 646 千

版 本: 2001 年 2 月第 1 版 2001 年 2 月第 1 次印刷

印 数: 1~5000 册

书 号: ISBN 7-113-04050-0/TP·504

定 价: 40.00 元

版权所有 盗印必究

凡购买铁道版的图书, 如有缺页、倒页、脱页者, 请与本社计算机图书批销部调换。

出版说明

本书探讨了 Windows 2000 Server 的运作基础，彻底剖析了企业网络建构的需求，尽情发挥了 Active Directory 的强大功能。以 Windows 2000 Server Active Directory 目录系统为基础，一步步引导读者进入 Windows 2000 Server 建构企业网络的殿堂。您可以由本书的说明很快了解目前网络的发展趋势以及建构方法，并且可以根据书中的设置过程建构出您公司的企业网络。

本书程序源代码下载地址：

<http://www.bookposter.com/download.htm>

本书由台湾博硕文化股份有限公司提供版权，中国铁道出版社计算机图书项目中心审选；张巍、高胜、王明、沈放、邓力、罗怡、葛兰、彭涛等同志完成了本书的整稿工作；孟丽花、肖志军、廖康良、陈贤淑等同志完成了本书的排版工作。

中国铁道出版社

2001.2

目 录

第 1 章	Windows 2000 操作系统架构与网络功能概述	1
1-1	操作系统的演化与目的	1
1-2	Windows 2000 操作系统的管理能力以及 Windows 2000 系统的基本运作原理	4
1-2-1	Windows 2000 所采用的开放式系统模式与工业标准	7
1-3	Windows 2000 操作系统的基本组成架构	8
1-3-1	客户/服务器计算架构	9
1-3-2	对象式运作	9
1-3-3	Multitasking 与 Multiprocessing	10
1-3-4	Windows 2000 操作系统的核心模式(Kernel Mode) 与用户模式 (User Mode)	12
1-3-5	Windows 2000 操作系统核心模式以及用户模式的运作	12
1-4	网络架构的基本概念	15
1-4-1	层与层之间的通讯	17
1-4-2	在网络上传送数据与接收数据	20
1-4-3	开放式系统连接模式	21
1-4-4	网络上的除错	30
1-4-5	局域网的架构——IEEE 802 标准的低级通讯协议	31
1-4-6	ANSI FDDI 规格	33
1-4-7	数据传输服务模式	33
1-5	Windows 2000 操作系统的分层网络架构	37
1-5-1	层级边界	37
1-5-2	Windows 2000 操作系统里的网络通讯协议	39
1-5-3	分布式处理以及客户/服务器架构	42
1-5-4	分布式组件对象模式 (DCOM)	43
1-5-5	分布式处理的进程与进程间通讯 (IPC)	52
1-5-6	网络资源的访问	56
1-5-7	工作站的服务	58
1-5-8	服务器的服务	61
1-5-9	功能连接	62
1-5-10	远程访问服务 (RAS)	62

1-5-11	Windows 2000 操作系统网络层级模式	65
1-6	Windows 2000 新类型的网络组织架构	65
1-6-1	在 Windows 2000 Server 操作系统方面	65
1-6-2	在内建的国际互联网 (Internet) 组合方面	67
1-6-3	安全性的改进方面	67
1-6-4	新类型的管理工具	68
1-6-5	在 Windows 2000 Professional 网络功能上的改变	68
第 2 章	Windows 2000 域规划与系统安全	71
2-1	Windows 2000 安全性的模式架构	71
2-1-1	访问控制	74
2-2	审核安全事件	88
2-3	Windows 2000 Server 的域	91
2-3-1	域目录数据库	92
2-3-2	域控制站 (DC)	93
2-3-3	成员服务器	93
2-3-4	信任关系	93
2-3-5	域安全策略	94
2-3-6	计算机帐号以及安全性通讯管道	94
2-3-7	在混合的操作系统环境下的系统安全	95
2-3-8	工作组	95
2-3-9	Windows 95 / Windows 98 客户端计算机	95
2-3-10	LAN Manager 2.x Servers 端以及客户端	96
2-3-11	Novell NetWare 的联机	96
2-4	登录与身份验证程序	96
2-4-1	交互式登录与远程登录	97
2-4-2	NetLogon 服务	101
2-5	规划域	105
2-5-1	依照用户资源使用频率来区分	106
2-5-2	依照域内使用人数来区分	106
2-5-3	依照地理区域来区分	106
2-5-4	从安全性方面考虑——建立安全性域	107
2-5-5	管理与分配	107
2-5-6	在广域网络上的目录数据库数据同步以及远程访问服务	108
2-5-7	系统安全考虑以及 C2 系统安全等级	108
2-6	域规划的评估要点	111
2-6-1	域选择表格	111
2-6-2	位置因素的考虑	111
2-6-3	主要域数量	112

2-6-4	信任域的数量.....	112
2-6-5	域控制站的数目.....	114
2-7	域服务故障排除.....	115
2-7-1	在连接服务器或其共享资源的时候发生的问题.....	115
2-7-2	访问一部计算机上的共享资源所发生的问题.....	116
2-7-3	域控制站验证用户密码失败.....	116
2-7-4	在域名称里的特殊字符.....	116
第 3 章	Windows 2000 浏览计算机目录服务.....	117
3-1	Windows 2000 的浏览目录服务.....	117
3-1-1	识别浏览计算机.....	119
3-1-2	在浏览系统中的计算机成员.....	126
3-2	选择提供浏览服务的服务器.....	133
3-3	浏览计算机公告信息.....	134
3-3-1	客户端计算机的计算机公告.....	136
3-3-2	选择性浏览功能设置计算机的公告.....	136
3-3-3	备份浏览计算机的公告.....	136
3-3-4	设置浏览系统中计算机公告的时间.....	137
3-4	客户端计算机从主要浏览计算机取得浏览清单.....	138
3-5	一个域或工作组下浏览计算机的数量.....	139
3-6	计算机的关机或死机.....	140
3-6-1	客户端计算机死机或关机.....	140
3-6-2	备份浏览计算机的死机或关机.....	140
3-6-3	主要浏览计算机死机或关机.....	141
3-6-4	域主要浏览计算机死机或关机.....	141
3-7	跨越多个工作组以及域的浏览服务.....	141
3-7-1	广域网络的浏览服务.....	143
3-7-2	使用 TCP/IP 协议的浏览计算机服务.....	143
3-8	Windows 95/98 成为主要浏览计算机.....	145
3-9	浏览计算机系统组件.....	145
第 4 章	新类型的域目录服务 Active Directory 的介绍.....	147
4-1	Active Directory 域概述.....	147
4-1-1	弹性的资源查询.....	148
4-1-2	资源的安全性.....	149
4-1-3	目录数据库的备份.....	150
4-1-4	域目录数据的分割.....	151
4-1-5	Active Directory 目录的延伸性.....	151
4-1-6	与 DNS 的组合.....	153

4-1-7 与其它目录服务的兼容性.....	154
4-2 Active Directory 目录服务.....	155
4-3 Active Directory 的架构.....	156
4-3-1 Active Directory 支持的目录服务协议.....	156
4-3-2 动态 DNS.....	157
4-3-3 程序设计界面.....	158
4-4 域结构.....	159
4-4-1 域树以及域目录林.....	160
4-4-2 域目录数据库的复制.....	162
4-4-3 逻辑的域结构与实体网络站点的结构.....	170
4-4-4 组织单位 (OU)	174
4-5 使用全局性目录查询对象资源.....	175
4-5-1 跨越域目录树的搜索.....	176
4-6 Active Directory 客户端计算机.....	176
4-7 Active Directory 域的安装与设置.....	177
4-7-1 安装 Microsoft DNS Server.....	177
4-7-2 激活 Active Directory 安装向导	182
4-8 在您的 Active Directory 域上加入计算机.....	190
4-8-1 加入 Windows NT 4.0 或 Windows 95/98 计算机.....	190
4-8-2 将 Windows 2000 的计算机加入到 Active Directory 里	191
4-8-3 在 Active Directory 域里加入复制域控制站 (备份域控制站)	195
4-8-4 在域目录树里新增一个子域.....	197
4-8-5 在域目录林里新增的域目录树.....	201
4-9 删除 Active Directory 域.....	203

第 5 章 管理 Active Directory 域..... 207

5-1 使用 Active Directory 域和信任关系管理单元工具.....	208
5-1-1 激活 Active Directory 域和信任关系管理单元工具.....	209
5-1-2 加入用户主要名称后缀 (UPN)	209
5-1-3 管理域目录林下的每一个域.....	211
5-1-4 变更域运作模式.....	212
5-2 Active Directory 用户和计算机管理单元.....	215
5-2-1 启动 Active Directory 用户和计算机管理工具.....	216
5-2-2 Active Directory 域里的对象	216
5-2-3 建立组织单位.....	219
5-2-4 建立用户帐号对象.....	221
5-2-5 移动对象.....	230
5-2-6 建立组.....	231

5-2-7	将用户帐号加入到组里.....	234
5-2-8	在 Active Directory 域里发布共享文件夹.....	236
5-2-9	在 Active Directory 域上发布共享网络打印机.....	241
5-2-10	在 Active Directory 域上添加与管理计算机对象.....	245
5-2-11	建立嵌套式组.....	248
5-3	在 Active Directory 域上寻找对象.....	250
5-3-1	条件式的搜索.....	250
5-3-2	筛选式的搜索.....	254
第 6 章	高级 Active Directory 资源对象类型管理.....	257
6-1	Active Directory 架构规划.....	258
6-1-1	定义 Active Directory 类别.....	262
6-1-2	属性的定义.....	273
6-1-3	语法 (数据类型).....	275
6-1-4	架构快取.....	277
6-2	架构的修改.....	278
6-2-1	弹性的单一主要架构变更模式.....	280
6-2-2	建立类别.....	283
6-2-3	类别属性定义.....	288
6-2-4	修改类别对象.....	291
6-2-5	建立属性.....	291
6-2-6	加入辅助性的类别.....	294
6-2-7	架构内容修改后的系统检查.....	295
6-2-8	取得有效的对象识别符 (OID).....	295
6-2-9	更新架构快取数据.....	297
6-2-10	关于修改架构的其它注意事项.....	299
第 7 章	规划与活用 Active Directory 域.....	301
7-1	规划站点(Site)的结构——提升网络效率的法宝.....	301
7-1-1	联机速度的规划.....	303
7-1-2	工作站以及域控制站间的通讯.....	304
7-1-3	站点与域目录数据的复制.....	305
7-1-4	站点.....	308
7-1-5	服务器对象以及 NTDS 设置对象.....	309
7-1-6	联机对象.....	309
7-1-7	网站链接对象.....	310
7-1-8	网站链接桥对象.....	311
7-1-9	Active Directory 站点和服务管理单元.....	311
7-2	规划域结构.....	321

7-2-1	多重域模式.....	321
7-2-2	规划域目录树以及域目录林.....	326
7-2-3	域控制站以及全局编录服务器的设置.....	326
7-2-4	规划委派模式.....	329
7-3	规划 DNS 结构.....	332
7-3-1	新的 DNS 架构规划.....	332
7-3-2	配合旧有的 DNS 设置规划.....	333
7-3-3	使用 WINS.....	334
7-4	Windows NT 域迁移到 Windows 2000 Active Directory 域.....	335
7-4-1	由先前的域模式来规划迁移的程序.....	335
7-4-2	迁移一个域.....	339
7-4-3	将第二列域合并入主要域.....	346
第 8 章 Active Directory 的程序化管理.....		351
8-1	LDAP 数据交换格式.....	351
8-1-1	使用 LDIFDE 将 Active Directory 域对象导出.....	354
8-1-2	使用 LDIFDE 修改 Active Directory 域里的对象.....	356
8-1-3	使用 LDIF 建立新的用户.....	360
8-1-4	使用 LDIF 删除用户帐号.....	362
8-1-5	LDIF 语法.....	363
8-2	使用 ADSI 与 VB Script.....	367
8-2-1	ADSI.....	368
8-2-2	使用 VB Script 导出 Active Directory 域内的对象.....	389
8-2-3	通过 ADSI 修改 Active Directory 域内的对象属性.....	391
8-2-4	通过 ADSI 建立新的用户帐号.....	393
8-2-5	通过 ADSI 删除用户帐号.....	395
8-3	通过 ADSI 完成高级的域管理.....	396
8-3-1	通过 ADSI 修改用户对象的架构.....	396
8-3-2	通过 ADSI 接口显示用户帐号的属性.....	399
8-4	延伸性的用户接口.....	400
8-4-1	通过 ADSI 扩充用户类别的 Display Specifier 对象.....	405
8-4-2	使用 Active Directory 用户和计算机管理单元修改属性.....	411
8-4-3	使用新属性来搜索用户.....	412
8-4-4	通过 Windows 2000 的用户界面使用新属性.....	413



第 1 章

Windows 2000 操作系统架构与 网络功能概述

首先,我们针对 Windows 2000 操作系统的特性以及 Windows 2000 操作系统本身的网络架构做一个了解,以便协助读者建立企业网络的基础。在这一章里,将要为读者说明 Windows 2000 的网络运作架构,以及 Windows 2000 操作系统本身所具备的新架构以及新类型的网络服务。其中包含 Windows 2000 操作系统本身的适用对象、适用环境以及 Windows 2000 系统的基本运作原理的说明。本章还说明了 Windows 2000 操作系统本身基本的组织架构,让您了解整个 Windows 2000 操作系统本身具有的能力,以及如何提供相关的服务。

在 Windows 2000 操作系统的网络服务上,本章更说明了 Windows 2000 操作系统所采用的基本的网络架构,其中包含了 Windows 2000 操作系统内每个网络处理或服务的模块,以及 Windows 2000 操作系统所遵守的工业标准与规格。在本章里,还说明了 Windows 2000 操作系统的分层结构,以及分层结构间的沟通界面的规格;Windows 2000 操作系统所采用的网络通讯协议;Windows 2000 用来建立与服务器间或与工作站间连接的跨网络应用程序分布式处理服务与机制;Windows 2000 操作系统内跨网络资源共享的机制;Windows 2000 工作站与服务器的相关网络服务的说明;以及 Windows 2000 新类型的网络组织。

1-1 操作系统的演化与目的

在早期,一些较大型的运算,不管是需要较多保存运算空间的计算行为,还是需要较快处理能力的微处理运算操作,都会希望在大型主机上运作。但是,大型主机(例如 IBM mainframe 等机器),不论是设备本身系统的安装,还是维护系统运作的成本,都是一般中小企业所负担不起的。另一方面,大型主机必须承担机器死机的风险,一旦大型主机系统死机,终端用户便无法通过大型主机的运算来完成他们的工作,这些,都是以往大型主机高成本,低效率的缺点所在。如图 1-1 所示:

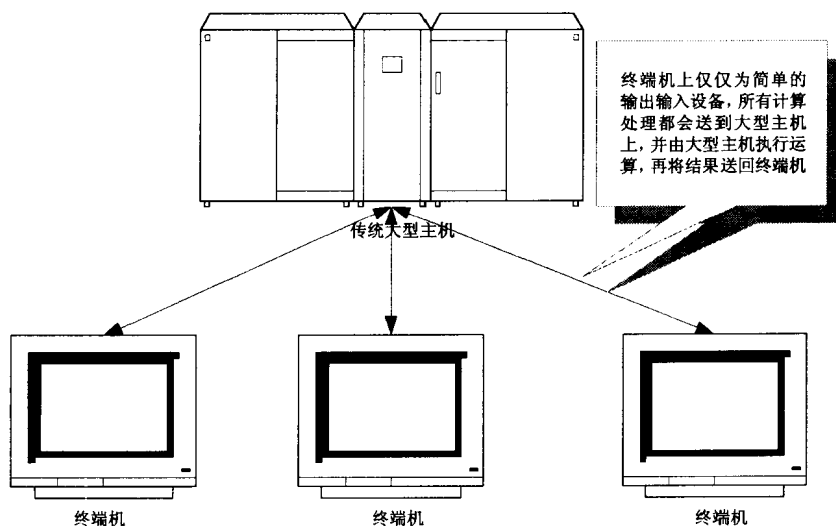


图 1-1 大型主机的运算方式

随着网络技术以及个人计算机的发展, 客户/服务器架构的分布式运算环境, 渐渐地以低管理成本、低设备成本, 以及低维护成本的优点与大型主机连接运作, 慢慢地取代了以往企业计算机数据的处理类型。一般传统的客户/服务器 (Client/server) 架构, 是将许多的服务器分散在各个区域上, 这些服务器通常拥有较好的硬设备以及具备较高速的微处理器, 并配备有较高容量的内存空间。服务器是提供各项服务的基本主机, 其功能类似以往的大型主机, 但是通常特定服务器仅提供某些特定的服务 (例如 Web 服务器只提供全球信息网站的相关服务)。当客户端计算机需要使用该服务器上的服务时, 客户端必须连接上服务器, 才可以使用服务器所提供的相关软件以及硬件的资源。如图 1-2 所示:

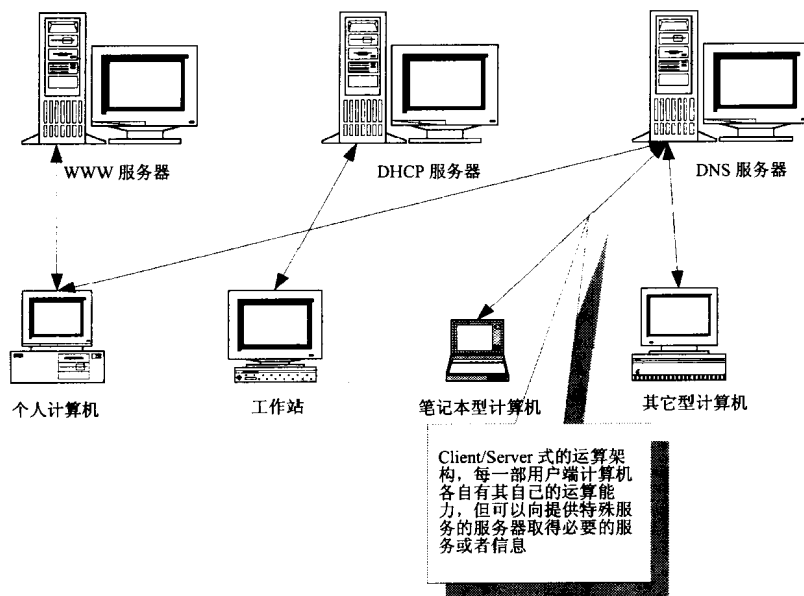


图 1-2 Client/Server 式的运算架构

这种方式虽然改善了以往大型主机高成本以及高风险的负担,但是这种传统式的主从分布式环境下的服务器,就如小型的大型主机一般,若服务器数量到达一定程度,会增加管理这些服务器的困难以及成本。在网络成长的同时(网络成长的意思是指网络上大小服务器以及客户端计算机、网络设备的数量增加时),网络管理的复杂度是成指数类型地增加。不但如此,应用程序的编写,系统的安装,或者服务的提供,都会随着网络的成长不断增加难度。这是由于网络上计算机的操作系统,没有与网络组合在一起的原因。如果将网络上计算机的操作系统与网络本身组合在一起,情况就不一样了。

因为操作系统本身就担任计算机硬件的基本资源分配的角色与工作。如果将网络组合在操作系统内,当用户在使用服务器所共享的资源时,就可以不必知道服务器真正实体提供此服务的详细情况(诸如资源实体保存的地址等)。对于网络系统管理人员来说,更可以利用集中式的管理方式,减少许多个别服务器设置安装的复杂度,减轻网络管理的负担。对于系统开发人员来说,甚至不需要知道网络实体间到底是采用何种通讯协议,或者采用何种实体通讯的模式,便可以组合整个企业里面的分布式系统的运作。这些,通过操作系统以及网络的组合,系统开发或者发展人员只需要知道分布式组件(Distributed COM, DCOM)或者简单的 Script,以及系统所提供的应用程序设计界面(API)即可完成您公司内部网络信息系统以及信息服务的基本架构。与传统式的主从架构(Client/Server)比较,将操作系统与网络组合起来,将是未来的趋势之一,也是 Windows 2000 新系统的特色所在。如图 1-3 所示:

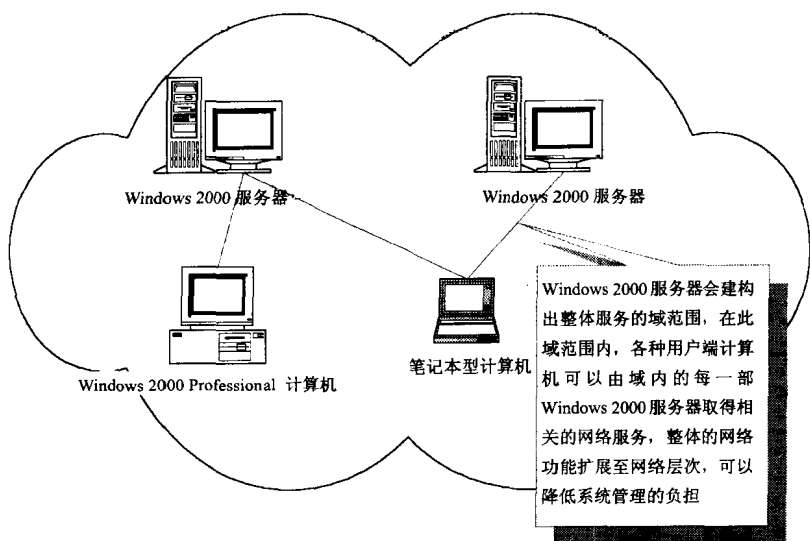


图 1-3 Windows 2000 提供的域以及其它网络服务

我们都知道 Microsoft 在 Windows 95 操作系统以后,就已经将网络功能内建在 Microsoft 以后所发展的操作系统里了,因此,Windows 2000 操作系统也与之前的操作系统一样,拥有完整组合的内建网络能力。除此之外,Windows 2000 操作系统一共提供了四个主要的版本,其中有专门提供给客户端用户使用的 Windows 2000 Professional 操作系统,还有专门提供给企业内部网络建立个别服务器所使用的 Windows 2000 Server、Windows 2000 Advance Server 以及 Windows 2000 Data Center Server 等三种不同层次的服务器操作系统。在这些 Windows 2000 家族操作系统里,组合了许多企业网络内部必须使用到的基本网络服

务,您更可以利用 Windows 2000 家族的操作系统来与其它的操作系统平台做相互的连接与应用,以提高您企业内部网络信息系统以及信息解决方案的组合与问题解决能力。

1-2 Windows 2000 操作系统的管理能力以及 Windows 2000 系统的基本运作原理

微软公司的 Windows 2000 操作系统的设计目的,主要有下列几个方向。首先,我们将微软公司的 Windows 2000 操作系统的管理能力,分成几个主要的部分来进行说明:

第一部分:操作系统的基本能力(管理机器硬件本身的能力)

操作系统的基本功能即是管理机器的硬设备资源,将硬件的资源提供给用户使用。此部分的能力,即是一般操作系统应该有的能力,在 Windows 2000 操作系统里,提供了下列管理机器硬件的能力:

1. Windows 2000 提供了不同微处理器的机器执行环境,Windows 2000 不但提供了 Intel x86 系列微处理器的操作系统版本,同时也提供了 Alpha、MIPS、PPC 等微处理器版本的兼容系统。因此,换句话说 Windows 2000 同时提供了复杂指令系统计算机(CISC) (Intel x86) 微处理器,以及简化指令系统计算机(RISC) (MIPS, DEC, 以及苹果的 PowerPC 等) 微处理器的运作平台。
2. 可以支持单一微处理器,以及超过一个的微处理器(多处理器、并行处理)机器的运作。Windows 2000 操作系统使用了对称式多重处理器的硬件架构支持多重处理器硬件的运作环境。在这里说明一下,对称式与非对称式多重处理器架构的不同点。所谓的对称式多重处理器,是指操作系统核心的处理过程,也就是操作系统的 kernel process,是同时分散在多个处理器上。每个处理器均会处理操作系统核心的处理过程。同时,在每个处理器上,也会同时处理应用程序的处理过程。也就是说,在每个微处理器上同时处理操作系统核心程序以及应用程序处理过程。而非对称式多重处理模式,是采用第一个微处理器作为操作系统核心处理过程的主要微处理器,这个微处理器专门处理操作系统核心的作业程序。而其它的微处理器只处理应用程序的处理过程。这种模式称为非对称式的处理模式。如图 1-4 所示:

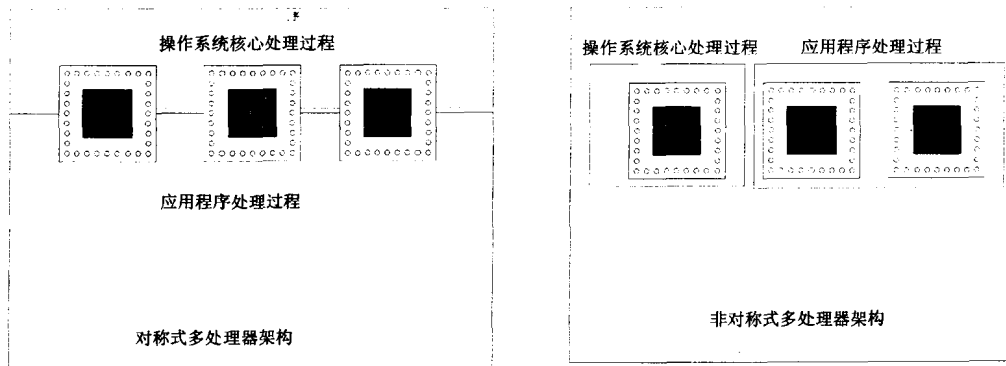


图 1-4 对称式与非对称式多重处理器的运作模式

3. 充分的电源管理以及即插即用装置 (Plug and Play)。在以往的 Windows NT 4.0 操作系统里, 并没有提供完整的即插即用的硬件处理功能, 在 Windows 2000 里, 除了提供了强大的电源管理能力, 并且拥有与 Windows 95/98 相同能力的即插即用功能。Windows 2000 操作系统还可以检测到硬设备, 您也可以以更简单的方式来安装并管理硬设备资源。通过 Windows 2000 的即插即用机制, 系统可以自动动态地识别到硬设备。系统可以动态重新配置硬件的资源 (输入、输出地址, 中断要求等)。也可以自动地加载系统所检测到的适当的硬件驱动程序。并通知应用程序, 告知应用程序设备所发生的事件 (像是设备删除或添加), 还可以锁定支持“高级设置以及电源界面”(ACPI) 的设备的电源管理。
4. Windows 2000 操作系统包含了更强大的保存架构, 以简化保存管理的负担。在 Windows 2000 中, 新的磁盘系统管理员 (Disk Administrator) 可以使用改良过的磁盘分区 (partition) 来定义更强大的空间管理。另外, 配合即插即用以及电源管理功能, Windows 2000 还可以在不用重新开机的情况下 (也就是 Online 的状态) 来更改、删除、移动所有的磁盘分区或者更改 RAID 的设置。通过 Windows 2000 新的目录名称空间, 磁盘驱动器分区的磁盘驱动器代号将不会只限制在 26 个 (因以往的磁盘驱动器分区的磁盘驱动器代号是以 26 个字母所表示, 所以, 以往的操作系统多半仅能衔接上 26 个磁盘分区)。
5. Windows 2000 操作系统支持了大型内存的管理与配置, 让应用程序以及 Windows 2000 本身的系统核心程序的执行效率更佳。在 Windows NT Server 4.0 操作系统中, 能够支持 3GB 的内存配置。在 Windows 2000 Server 操作系统中, 突破了传统 32 位的内存配置限制。Windows 2000 Server 操作系统里, 除了能够正常地执行一般的 32 位应用程序外, 还有一些需要使用较多内存的程序, 像是统计数值程序, 图像处理过程, 或者一些经常使用到 I/O 操作的系统 (例如关系数据库系统) 等的应用程序, 这些应用程序都可以通过 Windows 2000 操作系统本身所提供的 API 来访问 Windows 2000 的内存架构, 获取到最多的内存资源, 并提供最好的系统运作效率。

第二部分: 通讯网络的建立以及管理能力

1. Windows 2000 操作系统支持分布式处理以及内建网络的能力。在 Windows 2000 操作系统里, 支持了许多目前广泛使用的通讯协议以及服务。在通讯协议上, 除了支持国际互联网 (Internet) 上主干协议 TCP/IP 之外, 另外也提供了 NetBEUI、PPTP、L2TP、NetBT、IPX/SPX 等应用协议, 建立了企业内部网络 (Intranet) 以及上下游产业网络 (Extranet) 的基础。另外, Windows 2000 操作系统所提供的网络服务 (Service), 更是包含了目前最广泛使用的所有网络上的服务。例如 Windows 2000 IIS 5.0 除了提供的 WWW 服务器、FTP 服务器、Email (SMTP) 服务器之外, 还提供了 Windows 2000 新类型的网络服务。您可以使用 Windows 2000 Server 操作系统来建立 Index Server, 提供网络以及本机相关文件、信息的搜索服务。您也可以以 Windows 2000 Server 操作系统来建立集中式的认证服务器, 可以协助维护网络上的交易的安全性。此外, 还有许多的服务, 这些, 我们都将在本书后的几个章节里, 替各位读者慢慢的说明。
2. 在操作系统内部实体运作部分, Windows 2000 操作系统遵守了大部分的工业标准, 这些

工业标准兼容了其它作业平台的基础,其中 Windows 2000 系统参考了 RFCs、POSIX、IEEE 等规格。这些 Windows 2000 所遵守的规格是目前网络上或者系统上采用的标准。因此,Windows 2000 更容易与其它操作系统平台建立良好的连接性。另外一方面,系统开发人员也可以通过开放式的标准,利用 Windows 2000 的操作系统平台,更容易建立企业内部的分布式系统,提供您企业更多的解决方案。

3. Windows 2000 操作系统提供了完整的系统安全保护机制,例如原本 Windows NT 系统里的 C2、Functional C2 等级的安全性认可。此外,Windows 2000 系统还附加了许多新类型的网络安全机制的应用,例如 Kerberos 的使用以及编码原理的应用,确保用户重要数据以及系统本身的安全,防止被其它人破坏或者入侵。随着分布式计算环境时代的来临,系统安全的机制显得越来越重要。在本书稍后几章,您可以看到 Windows 2000 关于系统安全的保护措施。

第三部分:系统本身的架构与能力

1. Windows 2000 操作系统提供了延展性的能力,在 Windows 2000 系统内,提供了可修改的界面。在 Windows 2000 设计模块里,您可以不需要进行大幅度修改系统架构,就能够增加各层次的操作系统核心的新功能以及新的服务,比起以往的 Windows NT 系统,更具信息系统的延展性功能。
2. Windows 2000 操作系统的架构本身会保护操作系统避免受到应用程序的破坏。在 Windows 2000 操作系统里,应用程序会在属于自己的 process 里执行,而不会超出他们拥有的地址空间。操作系统的核心(kernel)与应用程序是相互隔离的,这样我们可以使用已经定义好的用户模式(user-mode)应用程序设计界面(application programming interface, APIs),让应用程序与系统核心做沟通。
3. 在 Windows 2000 的核心模式(kernel-mode)里,允许让高效率的子系统执行各种应用。因为在核心模式里,不需要通过线程(thread)或者进程(process)的交换(通过线程的处理,进程的效率能够提升,详细参考数据,读者可以参考一些操作系统原理的相关书籍,因为限于篇幅的关系,在这里笔者就不多加叙述了),这些子系统便能直接与硬件互相影响操作,或者子系统与子系统间的相互沟通与运作。因此,在 Windows 2000 里,特别容易感觉到效率的增进,特别是图形密集的应用程序,其效果更明显。
4. Windows 2000 操作系统与其它系统平台的兼容性。Windows 2000 支持与以往 Microsoft 公司所生产以及其它公司所设计的系统平台的连接性,其中包含 MS-DOS、Windows 3.x、OS/2、POSIX 的应用程序,同时也支持了以往的磁盘分区方式,例如 FAT 文件系统,以及各式各样的设备与网络等。此外,Windows 2000 提供了与 Windows NT 4.0 操作系统或者更早期版本不同的网络管理模块,为了提高企业内部网络或者整体网络效率,建议采用 Windows 2000 的作业环境。也就是说,在企业网络内,采用 Windows 2000 Server 版本的操作系统,提供网络上的服务以及管理,并采用 Windows 2000 Professional 版本操作系统,提供用户客户端的操作系统环境。搭配 Windows 95/98 或者 Windows 3.1 等系统,MS-DOS 操作系统,甚至其它的操作系统平台,像 UNIX、OS/2 等,可以建立整体的企业网络。为了方便与早期的操作系统组合(在这里,早期的操作系统指的是微软公司的在 Windows 2000 之前的操作系统产品,例如 Windows NT 4.0、Windows 95/98 等

等), Windows 2000 操作系统提供了许多让用户选择设置的项目。不过, 因为 Windows 2000 Server 的许多服务必须在纯 Windows 2000 操作系统的环境下才能使用, 因此, 为了能够使用更多网络的服务, 更强的网络安全保护, 我们建议在 Windows 2000 的域环境下, 可以建立纯 Windows 2000 的网络环境 (也就是相关的服务服务器由 Windows 2000 Server 或者由 Windows 2000 Advance Server、Windows 2000 Data Center Server 来建立, 而客户端计算机由 Windows 2000 Professional 计算机来担任, 提供用户访问服务的环境)。这些, 我们将在稍后的各个章节中, 为各位读者做说明。

Windows 2000 将实际经验融合在操作系统里, 这些经验以及想法实际上多半是由许多的计算机工业标准而来, 有些则是由学术界的操作系统理论而来, 所以说, Windows 2000 操作系统不但符合现实计算机工业的标准, 同时也配合操作系统理论、建立效率与功能较佳的作业环境。

1-2-1 Windows 2000 所采用的开放式系统模式与工业标准

刚刚我们提到过 Windows 2000 操作系统遵守了目前主流的工业标准, 而且 Windows 2000 操作系统也以开放式架构的服务以及管理能力来提供建立企业网络的基本功能。现在, 我们先来了解一下关于开放式系统以及工业标准的内容。

所谓的开放系统 (Open System) 是指所设计的系统能与其它的系统或者设备兼容, 而不是只有几个限定的特定制造厂商可以相互应用而已。此外, 还必须能接受第三方厂商 (third party) 所额外提供的硬件或软件。举个例子来说, 在 Windows 2000 操作系统上, 同时能安装 INPRISE 公司 (前 Borland 公司) 的 Delphi 或者 IBM 公司的 SCSI 界面卡, 同时, 也可以通过 ODBC (Open DataBase Connection) 连接上不同平台上的数据库系统。在目前的工业标准的区分里, 主要区分成两大类: 分别是 de jure 的标准以及 de facto 的标准。

De jure 标准: De jure 的标准是建立工业标准的主要部分, 而建立 De jure 标准的组织或者团体, 都是经过世界性评选, 公认在他们研究领域范围内具有权威性的组织或团体。诸如: 美国国家标准协会 (American National Standards Institute, ANSI), 电子电路工程协会 (Institute of Electrical and Electronic Engineers, IEEE), 以及国际标准组织 (International Standards Organization, ISO) 等等。这些都是建立工业标准的组织或团体。这些组织内的成员, 多是由于他们的研究目的领域内非常精通的一些专家, 而且多半与学术研究、工业研究单位相互结合, 因此, 由这些团体所建立起来的工业标准多半非常具有权威性。而 De jure 标准, 即是由这些权威性团体单位所建立的公认标准。举个例子来说, 像 ANSI 美国信息交换标准码 (ANSI American Standard Code for Information Interchange, ASCII) 字符编码标准, IEEE 的 UNIX 便携式操作系统接口 (POSIX) 标准以及局域网络实体网络的标准 (IEEE 802 系列), 以及 ISO 的开放式系统连接 (ISO Open System Interconnection, OSI) 参考模型, 这些都是属于 de jure 的标准。

De facto 标准: De facto 标准则是有点类似“先上车后补票”的状况。通常有些技术在发展的时候, 会遇到无相关标准可以依据和遵守的状况。遇到这种状况, 发展该领域的团体或研究单位会先以他们自己的解决方案来当成暂时使用的依据。但是若这些依据使用久了, 发现绝大部分的工业也都慢慢依照此解决方案来建立他们自己的系统时, 这种解决方案也会