Windows NT 4与Web站点资源书库

第 4 卷

Windows NT——网络连接

(美)Terry W.Ogletree 著
京京翻译组 译

机 械 工 业 出 版 社
西蒙与舒斯特国际出版公司

本书详细介绍路由选择、远程访问、拨号连网、用户帐号、组、脚本、配置文件等。还介绍了在Windows NT4里如何复制目录、创建登录脚本以及安装和管理网络打印机。

本书涵盖了维护一个高效Windows NT网络所需的全部知识。

本书适合于Windows NT4网络的中、高级用户。

本书版权登记号：图字：01-98-0533

图书在版编目(CIP)数据

Windows NT——网络连接/(美)奥格里特利(Ogletree,T.W.)著；京京翻译组. -北京：机械工业出版社，1998

(Windows NT 4与Web站点资源书库)

书名原文：Windows NT Netorking

ISBN 7-111-06290-6

Ⅰ.W… Ⅱ.①奥… ②京… Ⅲ.计算机网络-连接技术 Ⅳ.TP393

中国版本图书馆CIP数据核字(98)第08198号

出 版 人：马九荣(北京市百万庄大街22号 邮政编码100037)

责任编辑：蒋 克

北京昌平第二印刷厂印刷·新华书店北京发行所发行

1998年5月第1版第1次印刷

787mm × 1092mm1/16 ·17.75印张

印数：0001-7000册

定价：32.00元

目　录

第一部分　域和NT路由选择

第1章　Windows NT域 ……1
1.1　Windows NT域包含有比工作组更多的意义 ……1
1.2　主域控制器 ……4
1.3　备份域控制器 ……6
1.4　什么是委托关系 ……7
1.5　挑选最适合自己需要的一种域模型 ……8
1.6　工作组如何与域打交道 ……9
1.6.1　Windows NT Server客户机和Workstation 客户机 ……10
1.6.2　Windows for Workgroups和Windows 95客户机 ……10
1.6.3　MS-DOS和LAN Manager 2.x ……11
1.6.4　Novell NetWare客户机 ……11
1.6.5　Macintosh客户机 ……12
1.7　总结 ……12
第2章　网络协议及服务 ……14
2.1　网络设备接口规范和传输驱动程序接口 ……16
2.2　NetBIOS接口 ……17
2.3　NetBIOS与TCP／IP（NetBT） ……17
2.3.1　NetBIOS名称 ……17
2.3.2　NetBEUI协议 ……18
2.3.3　什么是NetBEUI帧 ……18
2.3.4　无连接通信与面向连接通信 ……18
2.4　TCP／IP——因特网标准 ……18
2.4.1　用户数据报协议（UDP） ……19
2.4.2　TCP／IP编址 ……20
2.4.3　网络分类 ……20
2.4.4　子网掩码 ……22
2.4.5　因特网域名和InterNIC ……22
2.4.6　地址解析协议（ARP） ……22
2.4.7　因特网控制报文协议（ICMP） ……23
2.4.8　动态主机配置协议（DHCP） ……24
2.4.9　什么是默认网关 ……25
2.4.10　基本TCP／IP工具和诊断工具 ……26
2.5　IPX／SPX的使用 ……27
2.5.1　NWLink IPX／SPX兼容协议堆栈 ……28
2.5.2　Windows NT客户机使用的NetWare客户机软件 ……28
2.5.3　NetWare网关服务 ……28
2.5.4　Windows NT支持的NetWare工具 ……29
2.5.5　NetWare客户机软件 ……29
2.5.6　NetWare目录服务管理器 ……29
2.5.7　数据链路控制 ……29
2.5.8　使用IBM系统网络结构 ……30
2.5.9　Macintosh客户机服务 ……30
2.6　用于因特网访问的点对点协议 ……30
2.7　使用点对点通道协议 ……31
2.7.1　对于虚拟专用网 ……31
2.7.2　对其他协议通道的支持 ……31
2.8　Banyan的VINES网络 ……31
2.9　简单网络管理协议和Windows NT ……32
2.10　DEC的Pathworks网络软件 ……32
2.10.1　DECnet与TCP／IP ……32
2.10.2　基于客户机和服务器的许可协议 ……33
2.11　总结 ……33
第3章　网络名称解析服务 ……35
3.1　什么是B节点、P节点、M节点和H节点 ……35
3.1.1　B节点 ……35
3.1.2　P节点 ……36
3.1.3　M节点 ……36
3.1.4　H节点 ……36

3.1.5 如何标识网络资源 ……37
3.1.6 注册和解析 ……37
3.2 HOSTS和LMHOSTS文件——老式方法 ……37
3.3 域名服务 ……39
3.4 Windows网际命名服务（WINS） ……39
3.4.1 忘记子网——WINS服务器相互间的查寻 ……39
3.4.2 名称注册和名称解析 ……40
3.4.3 WINS服务器 ……40
3.4.4 注册名称到WINS数据库 ……42
3.4.5 在WINS数据库中增加静态的映射名称 ……44
3.4.6 如何查看WINS数据库内的数据 ……45
3.4.7 如何备份和恢复WINS数据库 ……45
3.4.8 如何用JETPACK.EXE压缩WINS或DHCP数据库 ……45
3.5 什么是浏览？ ……46
3.5.1 浏览降低了对广播数据报的需要 ……47
3.5.2 浏览列表 ……47
3.5.3 域主控浏览器 ……47
3.5.4 浏览器的选举 ……48
3.5.5 备份浏览器 ……48
3.5.6 事件日志浏览器报文是什么 ……48
3.6 总结 ……49
第4章 Windows NT下的路由选择 ……50
4.1 网卡、地址和多宿主 ……51
4.1.1 如何为网卡添加五个以上的IP地址 ……51
4.1.2 NetBT每块网卡只支持一个地址 ……52
4.2 用MS Lookback适配器伪造一个网络 ……52
4.3 多协议路由选择 ……52
4.3.1 路由选择信息协议 ……52
4.3.2 BOOTP（引导协议）Relay Agent for DHCP ……54
4.4 路由选择表以及怎样理解ROUTE命令的输出 ……55
4.4.1 ROUTE和TRACERT命令 ……57
4.4.2 NBTSTAT和NETSTAT命令 ……57
4.5 总结 ……58

第二部分 用户及NT网络

第5章 远程访问和拨号网络 ……59
5.1 拨号网络：同世界连接 ……59
5.1.1 设置拨号网络 ……60
5.1.2 如何使用拨号网络 ……63
5.2 应设置拨入还是拨出？ ……64
5.3 连接 ……64
5.3.1 多链路——将两条信道合并到一块儿 ……65
5.3.2 调制解调器 ……66
5.3.3 ISDN ……67
5.3.4 X.25包交换网络（PAD.INF文件） ……67
5.3.5 SLIP／PPP ……68
5.3.6 用RAS访问局域网，并将NT作为因特网网关 ……68
5.3.7 脚本——连接过程的自动化（SWITCH.INF） ……69
5.4 远程访问服务 ……72
5.5 故障诊断日志 ……74
5.5.1 打开DEVICE.LOG和PPP.LOG ……74
5.5.2 用TERMINAL对Modem进行故障诊断 ……75
5.5.3 自动拨号特性 ……76
5.6 因特网信息服务器（IIS） ……76
5.6.1 IIS管理器程序 ……77
5.6.2 在IIS里使用Perl、Java和其他编程语言 ……82
5.7 总结 ……82
第6章 用户帐号和用户组 ……84
6.1 域安全数据库和工作站本地数据库 ……84
6.2 本地和全局用户帐号 ……86
6.3 远程／交互登录 ……87
6.4 域和委托关系的电脑帐号 ……89
6.5 控制本地和全局用户组的访问 ……90
6.5.1 本地和全局用户组有何差异 ……90

6.5.2 将权限授予组，而不是授予个人 …91
6.5.3 在域间导入和导出用户 …92
6.5.4 内建组 …93
6.5.5 内建本地用户组 …94
6.5.6 内建的全局组 …94
6.5.7 内建组的功能 …94
6.5.8 特殊组——作用与位置 …98
6.5.9 创建自己的本地和全局用户组 …99
6.5.10 为组授予权限和资源访问许可 …101
6.6 总结…102
第7章 脚本、配置文件和策略 …104
7.1 登录脚本…104
7.1.1 登录脚本的环境参数 …105
7.1.2 登录脚本的复制 …107
7.2 用户配置文件…107
7.2.1 All Users配置文件 …107
7.2.2 Default User配置文件 …108
7.2.3 如何创建用户配置文件 …109
7.2.4 如何修改默认用户配置文件 …110
7.2.5 System Default配置文件…111
7.2.6 机动用户配置文件 …111
7.2.7 文件夹格式 …112
7.2.8 从前一版本的NT升级配置文件…113
7.2.9 配置文件里的通用与个人程序组 …114
7.2.10 为Windows 95客户机建立用户帐号 …114
7.2.11 使用配置文件时需要登录脚本吗 115
7.2.12 特定用户的哪个配置文件优先 …115
7.3 系统策略…115
7.3.1 什么是系统策略? …115
7.3.2 如何设置系统策略 …116
7.3.3 系统策略模板 …118
7.3.4 为用户、组和电脑定制系统策略 …118
7.3.5 使用系统策略编辑器 …119
7.3.6 用系统策略编辑器编辑注册表 …119
7.4 总结…119
第8章 理解用户权限 …120
8.1 什么是用户权限…122
8.2 什么是用户许可…125
8.3 通过组分配权限是最简便的方法…126
8.4 有些组可以超越个人的用户权限…127
8.5 按职责设计自己的组，然后分配权限 …127
8.6 总结…128
第9章 资源共享和共享安全 …129
9.1 什么是目录服务…129
9.1.1 面向所有网络资源访问的单登录概念 …129
9.1.2 集中式网络及用户管理 …130
9.2 资源共享…131
9.2.1 管理共享 …132
9.2.2 创建用户和服务共享 …133
9.2.3 管理文件共享权限 …136
9.2.4 管理打印共享权限 …136
9.3 什么是文件和目录许可权限…137
9.3.1 FAT不允许权限；要用NTFS …137
9.3.2 NTFS权限 …137
9.3.3 为Windows NT 4.0将老式的HPFS设备转换成NTFS…139
9.3.4 审核用户访问 …140
9.4 总结…143
第10章 目录复制和登录脚本 …144
10.1 导入和导出电脑 …145
10.2 目录复制服务 …146
10.3 配置复制服务 …147
10.4 复制登录脚本 …150
10.5 用电脑名进行广域网连接 …151
10.6 目录复制的故障诊断 …151
10.7 总结 …152
第11章 Windows NT的打印 …153
11.1 打印机、队列和打印设备间有何差异 …154
11.2 在Windows NT里设置一台打印机的步骤 …155
11.3 打印机端口 …156
11.3.1 本地端口 …156

11.3.2 其他端口 ……157
11.3.3 添加LPR端口 ……158
11.3.4 惠普网络端口（DLC） ……158
11.3.5 DEC网络端口 ……159
11.3.6 AppleTalk打印设备端口 ……160
11.4 配置打印机 ……160
11.4.1 在服务器上为不同的硬件平台安装打印机驱动程序 ……161
11.4.2 本地打印机和网络打印机——中断和协议 ……162
11.4.3 设备驱动程序 ……162
11.4.4 如何设置打印机属性 ……162
11.5 访问控制 ……163
11.5.1 使用共享权限 ……163
11.5.2 审核访问 ……164
11.5.3 用一个特殊帐号控制麦金塔客户机的访问 ……165
11.6 如何创建和使用打印机表单 ……166
11.7 真的需要一台专用打印服务器吗？ …167
11.8 如何指定打印作业的延迟时间 ……167
11.9 打印机的优先权级别——谁先打印？ ……168
11.10 如何创建一个打印机池……168
11.11 怎样使用Novell网络的打印机 ……169
11.12 总结……169

第三部分 NT网络管理

第12章 文件系统 ……171
12.1 FAT文件系统综述 ……172
12.2 NTFS快速浏览……175
12.3 NTFS与FAT相比的优点 ……177
12.4 RISC系统必须有一个FAT分区 ……180
12.5 文件／目录权限的安全防护与建立 …180
12.6 FAT和NTFS的长文件名 ……180
12.7 将长文件名转换为8.3格式 ……182
12.8 NTFS文件压缩……182
12.9 NTFS的容错……183
12.9.1 磁盘镜像 ……183
12.9.2 带奇偶校验的磁盘带区 ……183
12.10 总结 ……184
第13章 登录进程 ……185
13.1 交互式及远程登录 ……185
13.2 什么是安全访问记号 ……186
13.3 身份验证过程是如何进行的 ……186
13.4 来自受托域的通过身份验证 ……188
13.5 缓存登录——作用与用法 ……190
13.6 为Windows NT建立自动交互式登录…190
13.7 总结 ……192
第14章 管理工具 ……194
14.1 域用户管理器 ……195
14.1.1 选择欲管理的域或电脑 ……195
14.1.2 向本地数据库或域数据库添加用户 ……196
14.1.3 修改用户属性 ……197
14.1.4 删除或禁止用户帐号 ……197
14.1.5 创建本地和全局组 ……201
14.1.6 添加来自受托域的用户和组 ……203
14.1.7 复制帐号和创建模板 ……204
14.1.8 删除一个用户帐号或组 ……204
14.1.9 设置策略和待审核的安全事件 …205
14.1.10 设置待审核的安全事件 ……208
14.1.11 用域用户管理器管理委托关系 …209
14.2 域服务器管理器 ……210
14.2.1 查看服务器属性 ……210
14.2.2 共享目录 ……212
14.2.3 服务 ……213
14.2.4 发送消息 ……213
14.2.5 用服务器管理器提升BDC ……213
14.2.6 使域内服务器同步 ……214
14.2.7 为域添加新成员 ……214
14.2.8 从域内删除成员 ……215
14.3 磁盘管理器 ……215
14.3.1 创建和删除基本和扩展分区 ……216
14.3.2 创建和扩展卷集 ……216
14.3.3 如何将一个分区标为活动 ……217
14.3.4 立即更改配置 ……217

14.3.5 容错 ……217
14.3.6 工具 ……219
14.4 远程访问管理器 ……219
14.4.1 远程访问服务的启动与中止 ……220
14.4.2 显示已连接的用户 ……221
14.4.3 为用户授予远程访问拨入权限 …222
14.4.4 向用户发送消息 ……222
14.4.5 撤消与用户的连接 ……222
14.5 许可协议管理器 ……222
14.5.1 到底选择每服务器还是每客户许可协议 ……222
14.5.2 “使用”一份许可证是什么意思 ……224
14.5.3 记录和显示许可协议历史 ……225
14.5.4 许可协议组 ……226
14.6 管理向导 ……227
14.6.1 添加用户帐号 ……227
14.6.2 组管理 ……228
14.6.3 管理文件和文件夹访问 ……228
14.6.4 添加打印机 ……229
14.6.5 添加／删除程序 ……229
14.6.6 安装新调制解调器 ……229
14.6.7 网络客户管理器 ……229
14.6.8 许可协议遵守 ……230
14.7 NetWare服务 ……231
14.8 Macintosh服务 ……232
14.8.1 用服务器管理器查看、创建和修改MacFile属性 ……232
14.8.2 启动和结束Macintosh服务 ……235
14.8.3 Macintosh可访问的卷 ……235
14.8.4 Macintosh用户的打印服务 ……235
14.8.5 查看Macintosh用户 ……235
14.9 DOS命令提示行 ……235
14.10 总结 ……237

第四部分 NT网络优化

第15章 性能监视 ……239
15.1 Windows NT性能监视器 ……239
15.1.1 性能监视器综述 ……240
15.1.2 计数器类型 ……241
15.1.3 导出数据，以便其他应用程序使用 ……244
15.1.4 创建折线图和报表 ……245
15.1.5 查看日志文件 ……245
15.1.6 使用警报列表特性 ……246
15.1.7 激活物理和逻辑磁盘性能计数器 ……247
15.2 网络监视 ……247
15.2.1 网络监视代理和工具 ……248
15.2.2 如何创建和使用捕获过滤器 ……249
15.2.3 密码 ……253
15.2.4 支持哪种协议 ……254
15.2.5 捕获数据 ……254
15.2.6 显示过滤器 ……254
15.2.7 查看单个数据帧 ……256
15.3 总结 ……257
第16章 灾难恢复和预防措施 ……258
16.1 备份磁带循环和离站备份磁带 ……259
16.2 通过备份离线保存文件 ……259
16.3 使用NTBACKUP的图形界面 ……260
16.4 使用命令行NTBACKUP ……262
16.4.1 创建备份命令文件 ……263
16.4.2 利用调度服务定时备份 ……264
16.5 如何备份注册表文件 ……265
16.6 随时保留一个离站备份 ……265
16.7 通过网络使用NTBACKUP ……266
16.8 递增与完全备份 ……266
16.9 恢复文件 ……268
16.10 恢复注册表文件 ……269
16.11 随时保留一份更新的ERD ……269
16.11.1 用RDISK创建一张ERD ……269
16.11.2 使用修复进程和ERD ……269
16.12 使用CHKDSK ……270
16.13 事件查看器和事件日志 ……270
16.13.1 选择欲检查的电脑或日志文件 ……270

16.13.2 系统、安全和应用程序日志文件 ……270
16.13.3 事件内容 ……271
16.13.4 归档和清除事件日志文件 ……272
16.13.5 事件日志满时覆盖事件 ……273
16.13.6 更改事件日志的大小 ……274
16.13.7 如何查看归档的事件日志文件 ……274
16.14 总结 ……274

第一部分　域和NT路由选择

第1章　Windows NT域

1.1　Windows NT域包含有比工作组更多的意义

Microsoft Windows for Workgroups是基于一种对等网络模型的操作系统。在这种类型的网络中，每个工作组成员电脑都可直接将自己的资源提供给另一个工作组成员电脑。工作组的每个成员都拥有自己的安全设置数据库，以便控制其它电脑对其资源的访问。

在一个集中式管理的文件服务器网络中(也就是我们通常所说的客户机/服务器模式)，单台或多台电脑扮演着中央资源存储器的作用，而成员则通过访问文件服务器来获取所需的各种网络资源。这种中央服务器能够提供用户级的安全性控制，在这种安全体制下，由服务器验证用户对网络的登录。此外，基于共享的安全控制(既可以拥有用户级安全体制，也可以没有)亦可通过共享名/密码来验证局域网(LAN)的登录。在用户级安全体制之下，可为每个用户只设置一个密码(是否设置多个密码取决于在该网络上安装服务器时采取的设置方式)，但在基于共享的安全体制之下，用户对每个需要访问的共享资源都可能有不同的密码。

在Windows NT中，可同时采取两种安全模型。但首先我们必须要理解这一点：Windows NT包含有两个版本；即Windows NT Server和Windows NT Workstation。

Windows NT Server——在Windows NT Server以前的一个版本叫做Windows NT高级服务器(NTAS)。运行Windows NT Server的电脑既可作为一个客户机使用，也可以作为一台服务器使用。然而，为创建一个NT域，至少必须有一台机器运行Windows NT Server这个版本，从而作为一个主域控制器(PDC)使用。

Windows NT Workstation——这是NT的工作站版本，它能与其他电脑一起建立对等网络，从而成为一个工作组的成员。除此之外，一台Workstation也可以加入网络中一个由NT服务器控制的域。同时，微软已对NT的这个Workstation版本进行了优化设计以利于交互操作。但其联网效率始终没有Server版本的效率高。

除上面讲的那些之外，这两个版本还存在其他一些差别。例如，因为微软在刚开始就将NT Workstation版本设计为一种基于用户的系统，而不是基于网络服务器，因此它有一个限制，即对它的资源进行访问时最多只能建立10个并发网络连接，而在Server版本中就没有这个限制。Windows NT Server允许有更多的并发网络连接，其限制主要取决于运行NT的硬件设备的性能及容量。

NT Workstation还内建有一套不同于Window NT Server的本地及全局用户组(有关用户组方面的详细资料，详参阅第6章“用户帐号及用户组”)。这主要是由于工作站上的用户只能够控制对其各自所属电脑上的资源的访问，而内建的用户组则正是为了适应这种管理功能而设置的。但对Windows NT Server来讲则不一样，当我们将一个NTServer设为PDC(主域控制

器)或BDC(备份域控制器)时，就可以建立另外的组，将具有相同功能的用户划分到不同的组内。通过这些组，能为用户赋予适用于整个域的系统管理功能权限，而这些功能在对Workstation的管理中则用不上。

如果只是简单的看一看，域与工作组好象没有什么分别。两者都是代表网络上一些电脑的集合，相互间共享资源，同时提供相应的安全机制来管理对这些资源的访问。实际上，当我们浏览网络资源、工作组以及域时，这两者看起来确实没有什么分别。在浏览和共享资源时，域和工作组都能为用户提供交互操作，同时对访问权限和某些其他条件限制作出正确的响应。

但是，一个Window NT域与TCP/IP网络上的域又不太一样。在一个TCP/IP网络中，域名是分配给一个特定网络地址的一串文字。这样一来，用户就没有必要记忆那些冗长、晦涩的TCP/IP地址。Windows NT不仅包含了TCP/IP，而且内建有一个域名服务(DNS)，它用于对这些地址进行解释和翻译。但在Windows NT中有一点必须要牢记：域实际是其代表的网络的一个管理单元。用户可以通过很多方法将一个TCP/IP域名改变或者重新映射到另外的地址之上。例如：直接修改HOSTS文件中有关条目，或者改动DNS中的设置等。虽然用户可以改变一台Windows NT Server的网络地址、名称以及域名，但是这三项并非是相互依赖的。如果想改变一个Windows NT域的名称，那么只需要在其他网络成员中修改这个名称即可，而不必修改任何地址。

然而，一旦建立了一个Windows NT域，它就成了对域内的所有用户和电脑进行管理的一个最基本单元，它控制着用户对本域资源的访问，而且一旦采用了委托关系，还可将这种控制应用到别的NT域中。

工作组与域最显著的一个区别还是在二者实施其安全机制的方式上面。在一个工作组中，每台电脑都有自己的安全数据库，并由本机对登录过程进行验证。这些工作组内的电脑可在共享级的基础上为组内的其他电脑提供资源(例如文件及打印共享服务)。为某个共享资源所设置的密码只有一个，它对所有需要访问该资源的计算机都是一样的。如果工作站的管理员授权的话，甚至NT域内的用户都可以直接访问这些共享的资源。

但是，在客户机/服务器模式中，这种安全数据库是存放在Windows NT域一个或多个域控制器中的。这些电脑保存了该域及其成员的安全信息，并由它们对用户的登录进行验证。要建立一个域，就必须要有一个(而且只能有一个)PDC。除此之外，可以有一个或多个BDC、成员服务器以及NT Workstation客户机。

域安全数据库有一个主拷贝，我们将其称之为Windows NT目录数据库(该数据库包含在注册表内)，该数据库存放于PDC上，并且按照一定的时间间隔复制到各BDC上。该PDC目录数据库的变动记录则是存放于一个变动日志文件中的，并会将这些变动复制到各个BDC上。由于每次只传送对该数据库的变动记录，因此在拥有很多用户的网络环境下，就能够明显地减少网络通信量。PDC会定期地给各BDC发送通知，要求它们进行同步处理(在默认设置下，这个时间间隔是每五分钟一次)。各BDC回复PDC自己最后一次接收到的变动记录，这样，PDC就可以只发送自最后一次变动以来新增的变动记录给各BDC。

变动日志的长度有一定的限制，默认设置是大约2000条。这就意味着，如果一个BDC停止服务一段较长的时间之后，就不能够再通过使用变动日志来与PDC目录数据库进行同步处理了，因为有些变动记录已经从变动日志文件中删掉了。在这样的情况下，就必须要复制整

个目录数据库。当然，如果数据量比较大的话，就会花较长的时间才能完成。

注意： NT Server目录数据库最长可以保证到40MB。这是微软推荐的上限，但如果想要它容纳更大量的信息的话，也可以再将其容量上限增大。

可通过直接在注册表中修改参数值，从而变动日志文件的大小。注册表是由几个文件组成的，其中包含了在以前的Windows产品的INI文件中保存的信息。除此之外，注册表还含有其他一些必要的系统信息，例如将在第16章“灾难恢复及日常维护”讲到的系统硬件配置信息等。另外还有一点请大家记住，尽管Windows NT的注册表与Windows for Workgroups的注册表比较相似，但它与Windows 95的注册表却存在相当大的区别。如欲了解这方面的详细情况，请参阅本套丛书第6卷《Windows NT——注册表》。

注意： 如果还没有清楚的概念，或者在没弄清注册表各个项值的含义及相互关系的情况下就直接修改注册表，可能会导致系统不稳定或死机。因此，在准备修改注册表之前，请参考本套丛书第6卷或本卷第16章的内容。

可利用“域服务器管理器”管理工具(详见本书第14章“管理工具”)强制实现PDC目录数据库与BDC目录数据库之间的完全或部分同步。这一点是非常必要的，例如，当新增了一个用户，而用户又需要立即实现对域内各资源的访问，等不及系统自动同步过程的发生。这种情况下就可以应用管理工具来完成。

注意： 在域中新增一个BDC的时候，必须执行一次完全的同步操作，因为在建立该BDC的过程中，系统内根本就没有目录数据库。如正在安装的是一台NT服务器，并将它设为成员服务器而非BDC，那么该电脑就会有一个本地的目录数据库，并有随操作系统所产生的一些默认帐号。

在一个域中，除上述的Windows NT Workstation及服务器成员客户机之外，还可包含Windows 95以及其他一些使用LAN Manager联网软件的客户机。比如微软的MS－DOS和Windows 3.1、UNIX机器以及运行IBM版的LAN Manager软件的OS/2机器。此外，还可以使用NT网关以及Apple和Novell客户端软件，使运行Apple及Novell操作系统的机器也在某种程度上加入到该域中来。但是，在这些类型的客户机上，安全机制的动作方式会有些不同，不过仍然可以通过应用用户权限及资源访问权限的方式来达到建立一个安全的网络环境的目标。

在非控制器的Windows NT客户机(即不作为PDC或BDC的服务器)上，保存着一个本地的安全目录数据库。这样一来，如在该本地目录数据库中创建了一个帐户，那么用户肯定能用这个帐户登录到该工作站或服务器上，从而按照该工作站或成员服务器的管理员赋予的许可权限来访问本地资源。而在一台作为PDC或BDC的NT服务器中，只有面向整个域的目录数据库，因此用户就不能只是登录到该本地的服务器电脑上。也就是说，在PDC或BDC上没有本地的目录数据库。

如除了在本地的目录数据库中有一个帐号之外，在域安全数据库中也有一个同样帐号，那么就可同时登录到该NT域中。

域内成员的单登录进程是Windows NT网络连接中最好的安全特性之一。用户在访问共享

资源或服务器时，不需要记忆各个不同的密码(更糟糕的情况是，由于记不住而不得不将这些不同的密码写在纸上)，管理员可以为每个用户只设定一个单独的用户名和密码，而使用户只用这个密码和帐号就能够访问域内所有的资源。同样，这个机制还可以延伸到整个网络，将运行NT客户软件包的Windows for Workgroup计算机也包容进来。如果使用委托关系(trust relationships)的话，还可以将这种观念扩展至有多个域存在的其他域中，只要遵循NT所允许的各种不同的客户机的某些规则即可。

Windows NT登录信息对话框(参见图1-1)允许用户在密码验证的过程中选择域及本地工作站的名称。在这个对话窗口中只有三个栏目，分别为：用户名、密码以及域。其中，“域”输入框是个下拉式菜单，用户可从中选择该本地NT工作站名称，该工作站所属的域(如果有的话)以及与该工作站所属的域建立有委托关系的其他域的名称。

如果用户在该对话框中选择工作站的名称从而登录到这台本地工作站上，那么就会由该工作站上的本地目录数据库进行登录验证。反之，如果用户在该登录对话框中选择一个Windows NT域进行登录，则该工作站就会与该域的PDC(或BDC，有关详情将在下面的章节中进行阐述)建立一个安全的通讯通道，并将该登录信息以一种加密格式传送给相应的服务器进行验证。这时，在客户机上将会收到由该服务器传回的一个安全标志。该标志中包含了该用户所拥有的访问权限之类的信息。这个安全标志被存放于该工作站的高速缓存中，这样一来，当该用户访问各个域内资源时，就可以毋需再执行这个验证过程。此外，当PDC因为某些意外原因暂时停止服务时，用户对域内资源的访问可以不受到影响。用户可以用缓存在本地电脑内的安全标识继续对原来的资源进行访问。实际上，如果是使用Windows NT(Server或Workstation)来作为客户机，那么该登录信息(加密格式的)以及标志信息都是存放于这些机器的高速缓存中的。

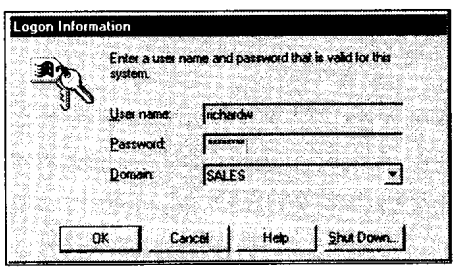

图1-1 从Logon Information对话框中选择一个域或工作站

当我们在网络中浏览其他电脑资源时，工作组和域所采用的方式基本一样。该用户拥有访问权限的电脑和资源将显示在一个浏览列表框中。工作组和域都能够相互接受来自于对方的浏览列表框的更新。如果想要了解有关浏览列表框及资源浏览方面的详细信息，请参阅本书第3章“网络名称解析服务”。如果不将一台Windows NT电脑设置为域控制器或加入到某个域中，那么在默认状态下，这台电脑将自动地成为一个工作组的部分。

1.2 主域控制器

创建一个域的唯一要求就是至少要有一台机被设置成PDC。即使该机器没有联入一个LAN，也可以通过安装Microsoft Loopback Adapter来模拟网络功能。这个适配器是一个软件驱动程序，它能够模拟硬件适配器的动作(仅用于演示目的)。

当然，只有在下面两种情况下才可能用到这种Microsoft Loopback Adapter：一种就是当用户需要一台单独的机器来练习各种域功能的操作及效果；另一种情况则是，用户需要一台单独的NT机器与因特网或远程访问服务(RAS)相连，并且在本机上模拟一个接受RAS交通路由的网络。

Windows NT目录服务

Windows NT目录服务为域提供相应的安全信息，我们将存放这些安全信息的地方称为目录数据库(directory database)，PDC中存放了这个目录数据库的主拷贝。以前我们将这种数据库称之为Security Accounts Management或Systems Accounts Management(SAM)，其中包含有域内所有用户的帐号，这两个名称大家仍然会在微软文档资料和因特网上看到。除了包含有域内所有用户的帐号信息之外，目录数据库中还有两种其他类型的帐号——电脑帐号和组帐号。其中，电脑帐号用于实际验证域内及委托关系的电脑成员(不是用户)，而组帐号则用来保存有关用户组及其成员的信息。除此之外，PDC还能设置域的安全策略，并可作为该域的主浏览器使用。

Windows NT目录数据库最主要的好处在于它提供了一种集中式的用户帐号管理。用户只需用一个用户名和密码在域中进行一次登录，而不必对域中的每台服务器分别进行登录。系统管理员在增加、修改或删除用户时，也只需要在一台机器上进行操作就可以了。

创建PDC时，同时会产生该域的一个唯一的安全性标识符(SID)。每个域电脑成员在加入到这个域中来时都会从该PDC处收到一个唯一的SID。在此有一点需要特别提醒大家注意：系统是通过这个SID来辩认网络中的电脑，而不是通过电脑名称。用户可修改PDC或成员电脑的名称，但不可能修改其SID。构建NT网络时，这一点是必须要弄清楚的。此外，PDC的域SID会加在其他成员服务器和工作站SID的前面，从而可标明该机器所属的域。使用这种SID机制的好处有以下几点：

■在一个域中只有一个PDC。如用户试图创建第二个具有相同域名的PDC，或在一台PDC上重新安装Windows NT Server，并使用同样的域名，那么会产生一个新的SID，系统会将其认为是一个不同的域。用户必须在一台PDC上重新安装Windows NT Server才能将它改成另一个不同的域名。

■用户可在任何时候从一个域中去掉任意一个BDC，但如果不事先将域内一台BDC提升到原PDC的位置上，那么将无法用NT的管理工具从域中将PDC删掉。当管理员决定将原来的PDC重新加入到网络中来时，那个以前由BDC升级而来的PDC会自动降级成一个BDC。

■如果要从域中去掉一个BDC，而且今后想要重新使用这个BDC的电脑名，并打算将该BDC去掉后重新作为该域的一个成员服务器加入进来，那么除了必须按照前面所说的那样重新安装之外，在此之前还需要从该域的目录数据库中将这台BDC机器的电脑帐号先删掉。

■如果想将一台电脑加入到一个域中，必须由在该域的PDC上具有正确的管理授权的管理员级用户才能完成。系统会为这个新成员在PDC的目录数据库中创建一个计算机帐号，并且该域的PDC为其分配一个唯一的SID号。

■如果因为意外情况导致系统找不到PDC，而且没有建立好恢复的安全机制(例如从一个最近的备份或紧急修复磁盘中进行恢复，有关恢复PDC方面的详细情况请参阅本书第16章)，那么这个域就丢掉了。这不是靠简单地重新安装NT并使用相同的域名就能够恢复的。重新安装及设置的域会有不同的SID，其他的域成员将无法识别。如果在网络中为每个域都

设置一个BDC，那么就可以将BDC提升为PDC，并在原来的PDC修复后再将其降为BDC即可。

■用户不能将一台PDC或BDC“降级”为域中的一个成员服务器。除此之外，还不能将一个域中的控制器移走放入另一个域中。如果想要这样做，就必须重头开始重新安装NT操作系统!

尽管这些规则听起来非常严格，我们应该意识到它们是内建于NT中的安全机制的组成部分。“扮演”一个NT域控制器的角色实际上是一项极困难的工作。因为NT网络的客户机并不存储域目录数据库的拷贝，因此可以将这些客户机从一个域随便移到另一个域中，不会有任何问题。用户可以更改PDC的名称，但不能够通过更名而将PDC从一个域移到另一个域中，或将几个域加入到一个单独的域内。SID始终保持不变，从而会防止此类事情发生。

1.3 备份域控制器

如果想为自己的域提供一种安全的结构，那么就可能需要增加一个BDC。同PDC一样，BDC必须是要在Windows NT Server的初始化安装过程中进行设置的。在此有一点必须注意，NT Workstation是不能作为PDC或BDC的。在安装过程中，用户必须选择BDC这个选项，并输入该BDC将要属于的域的名称。如果获得授权(由一个授权的管理员用户或者是有一个为该机器预先建立好的电脑帐号)，那么该BDC会获准加入该域，并将从该域的PDC上下载安全性目录数据库。

因为BDC接收目录数据库的更新记录并将其该数据库存储于本机上，所以当PDC停止服务时，BDC可以进行登录验证。当一个NT域包含有多个子网或一个单独但很大的子网时，这一点就显得非常重要。如果在每个子网中都建一个BDC，将可以分担PDC的用户认证工作，并在该子网中本地执行该功能。

如网络出现意外情况，导致网络超容或PDC服务停止，那么各子网上的BDC将自动担当起域控制器的作用，直到PDC重新恢复服务。这个过程对用户是透明的。

然而，建立一个BDC最重要的原因在于，可以在必要的时候将其提升为PDC。如果PDC丢失或不能恢复，管理员可用“服务器管理器”工具指定一台BDC为新的PDC。因为BDC中储存有与PDC一样的SAM数据库，所以一旦将其提升之后，就能完全担当起PDC的职责。如PDC只是暂时性关闭，可以重新恢复提供服务，那么当前的PDC会自动降级为BDC。在此还要再次强调：工作站不可设为PDC或BDC。如网络中有NT Server作为一个成员服务器(不是PDC或BDC)运行，同样也不能将之提升为PDC或BDC。PDC或BDC的设置都必须在NT的安装过程中进行选择。

除此之外，如果不得不更换PDC电脑上的硬件设备，可以将它作为一台BDC加入到该域中，从当前的PDC处得到一个新的有效的SID，并下载该域的安全性目录数据库，然后再将其提升为PDC。当将一台BDC提升为PDC时，当前的PDC会自动降级为BDC。

请大家记住，只有NT Server才能被设为PDC。用户可使用非NT的LAN Manager 2.x成员作为一个BDC，但这种BDC不能验证任何NT Server和NT Workstation的域登录，它们只能对LAN Manager 2.x客户机或其他非NT客户机提供登录验证。此外，运行于LAN Manager 2.x上的BDC不能被提升为一个Windows NT域的PDC，因为它们只能验证域内那些非NT客户机的登录。LAN Manager域控制器无法交换Windows NT域所使用的全套数据。

1.4 什么是委托关系

在网络中使用域可以对网络资源及各种安全性问题进行集中式管理。然而，在某些情况下，最好还是将用户分成一些更小的组，因为单独一个域可能无法满足管理上的需要。例如，当有一些地理位置相隔很远的LAN时，可以在每一个地方的局域网内设置一个BDC并使用同一个域，或者是根据地理位置的不同设置不同的域。另外一种办法则是，可以根据所进行的业务类型来设立和划分不同的域。

网络中有多个不同的域时，如果想让每个域的用户都可访问到其他域内的资源，那么就必须设置这些域间的委托关系。

委托关系是域之间的安全可靠的连接，这种连接允许一个域内的用户浏览或使用另一个域中的资源，而只需由该用户所在的本地域进行身份验证即可。当一个受托域内的用户访问设定该委托域内的资源时，就会进行通过检查。在这种情况下，委托域将从一个安全的通道中接收受托域发出的一个安全标识，并将该对用户的身份验证结果作为正确的授权予以接受，从而允许受托域内的这个用户访问委托域内的资源。域服务器是通过将其他域存为目录数据库中的一个电脑帐号，就如同将本域中的每个成员存为不同电脑帐号一样，从而实现对委托关系的验证。

在此大家要记住这样一点：来自受托域内的用户不能自动获得委托域资源的访问权。委托域的管理员必须授予该用户(或者包含有该用户的一个用户组)访问授权，就象通常为本域内的用户进行访问授权一样。除此之外，还有一种为受托域中的所有用户进行访问授权的方法，就是为这些用户设立一个本地的组并授权给这个组。实际上，使用用户组来对域资源进行授权是最有效，而且是控制用户权限的效率最高的方法。有关维护内建的局域和全局用户组以及创建新组等方面的详细信息，请参阅本书第6章中的具体讲述。

注意：每个组在目录数据库中还有一个帐号，标识其属于该域。

委托关系既可是单向的，亦可是双向的。在一个单向委托关系中，一个域委托另一个域。在这种情况之下，在受托域中的用户可以访问委托域，但委托域中的用户则不能访问受托域中的资源。如果想将所有的访问授权和许可都控制在一个本地的域内，但同时允许其他域中有一定业务关系而选定的用户访问到本域内某些指定资源，这种情况下应用单向委托关系就能够完全达到要求。

例如，在公司中可设置一个名为Accounting的域，以及另外一些诸如设计、生产的域。因为存储在Accounting域内各成员电脑上的数据都属于机密性质的(老板当然不想公司中每个员工都直接看到工资数据)，可以在Accounting域中创建一个本地的组，并在其中加入来自于其他域或全局组内的用户。然后，就可以对这个本地组进行授权设定，只允许这些用户访问Reports目录或其他一些敏感的数据资源(具体取决于这些资源的许可)。如果想让Accounting域内的用户能够在一台位于另外的域中的打印机上输出报表，这时就有必要应用一种双向的委托关系了。有关用户授权和资源许可方面的详细信息，请参阅本书第8章“理解用户授权”以及第9章“资源共享及共享安全性”。在图1-2中形象地表示了域间几种不同的委托关系。

在双向委托关系中，两个域相互委托。一个域可以与另外一个或多个域建立委托关系(我们称之为多委托域模型——multiple trust domain model)。在这种委托模式之下，每个域的管理员在本域内创建一个本地的用户组，并向前一段所述的那样，将另外的某个域或多个域内

的用户(或组)加入到该本地组中来。

如果要建立和设置委托关系，请使用User Manager for Domains工具(有关该工具的使用方面的资料，请参阅本书第14章中的详细介绍)。

1.5 挑选最适合自己需要的一种域模型

只建一个单独的域能够满足您公司的需要吗？如果用户数比较少，并且对安全性的要求也比较低，那么可以考虑使用工作组就可以了。如果需要集中式安全性以及其他一些由域带来的系统管理上的好处，那么使用一个用户数较少的域就应该可以满足需求。

注意： 一个域目录数据库可以存储大约26000个用户，最多可达到250个用户组。

如果管理的网络比较大，就可能需要设置一个单独的登录域和其他一些资源域，并将这个登录域作为其他资源域的受托域。不同域之间的关系和相互操作可以根据自己的需求设置得简单或复杂。在决定一个域的策略时，还应该考虑到用户的需求、业务的实际状况以及安全性政策等因素。微软公司提供的文档资料中描述了几种域模型，有关这些域模型的内容将在后面的章节中进行讲述。

主控域模型

在这种单独的主控域模型中，所有用户都登录到该主控域中。主控域的目录数据库中包含了该网络中所有用户的记录。除此之外，还有代表该主控域所委托的所有其他域的电脑帐号。所有其他的域及资源域都委托该主控域。但这些域的目录数据库中则不必包含任何代表委托域的电脑帐号。这种电脑帐号使不同的域可以相互识别身份。

在大型组织或单位中，这样的模型可以简化用户帐号及用户组的管理(请参考图1-2)。但是，主控域不能委托资源域，如果这样的话，只要在这些资源域中创建有一个电脑帐号，就会导致该主控域上的安全性信息的改变。如果需要的话，仍然可以通过在各资源域的目录数据库中建立另外的帐号，从而直接登录到该资源域中。但是，这样做可能会搞乱原来的安全政策，用户可以根据自己的特殊情况决定是否这样做。

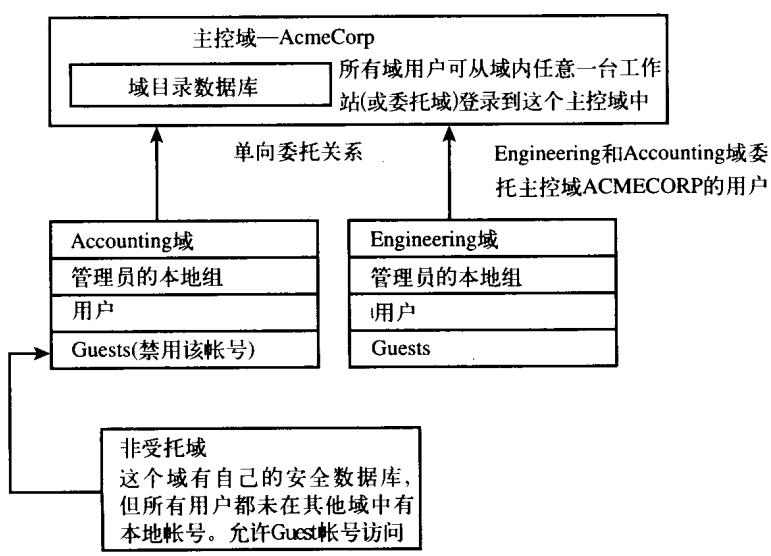

图1-2 主控域模型的委托关系及方向

归纳起来，这种主控域模型可以用来进行集中式的用户管理，同时控制资源的本地或全局访问特性。

一个域委托另一个域后，受托域的Domain Admins全局用户组将被放在委托域目录数据库中的Administrators本地组中。这就使受托域中的管理员可以管理委托域中的资源，因为他们现在也成了该委托域中的管理员。

但是，委托域的管理员可以用Server Manager for Domains来去掉该全局组，从而使委托域中的资源管理能够更加安全。这样做不会影响受托域用户对该域内资源的访问，如果这些用户加入到该域的本地组中的话。这样做的主要目的就是防止避免某些有更高授权的用户修改到委托域中的本地资源及许可。

其他域只能增加用户到委托域认可的全局组中。除非将全局的Domain Admin组保留在委托域的本地Administrator组中，否则只有本地的Administrator组成员才能对资源进行授权或改变资源的许可。

如果您所在的单位非常庞大(也就是说，拥有超过40000个以上的用户)，就可能要用到一种多主控域模型(请参考图1-3)。在这种模型中，有一个或多个域保存用户及组帐号，而所有其他的资源域都委托这些主控域。每个主控域都相互委托(这是一种双向委托关系)，这样用户就可以从网络中任何一台电脑上进行登录，并可以按照本地的许可访问相应的资源。

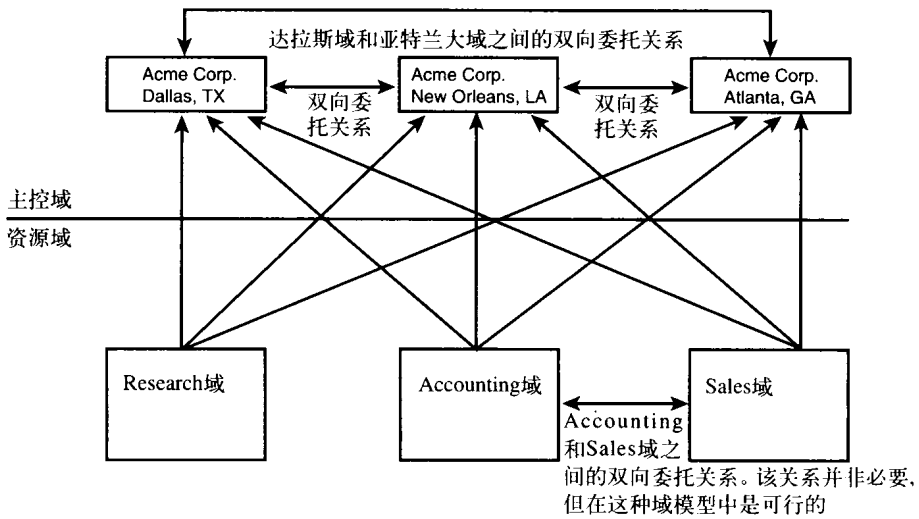

图1-3 带有委托关系方向显示的多主控域

在此请大家注意，使用主控域模型时，每个域至少都要有一个PDC。除此之外，如该单位的网络有子网，那么在每个有委托域的子网的主控域中都应该至少设置一个BDC。以便当网络在运行时，或者当网络连接断掉时作为安全保护机制，担当用户验证的工作。

1.6 工作组如何与域打交道

正如前述的那样，一台NT Server在默认状态并不是一个域成员，而是一个工作组成员。Windows NT工作站不能创建域，但它可加入一个域，亦可创建或加入一个工作组。

在最开始的登录对话框中，必须选择或输入一个用以验证该用户名及密码的域或工作站名称。如该工作站在域中有一个电脑帐号，那么该登录对话框的下拉式菜单中会包含该域的