北京大学出版社
侯大庆　田舒　编著

Windows NT 网络服务综述

Windows NT 网络服务综述

侯大庆　田　舒 编著

北京大学出版社

新登字(京)159 号

图书在版编目(CIP)数据

Windows NT 网络服务综述/侯大庆,田舒编著. —北京:北京大学出版社,1994.6
ISBN 7-301-02512-2

Ⅰ.W… Ⅱ.①侯… ②田… Ⅲ.窗口软件-概论 Ⅳ.TP 311.25

出 版 者: 北京大学出版社
地　　址: 北京大学校内
邮政编码: 100871
排 印 者: 北京科技期刊出版集团电脑排印中心排版
北京飞达印刷厂印刷
发 行 者: 北京大学出版社
经 销 者: 新华书店
版本记录: 787×1092 毫米 16 开本 12.5 印张 290 千字
1994 年 6 月第一版 1994 年 6 月第一次印刷
印　　数: 0001—3 500 册
定　　价: 25 元

前　言

综观当今的计算机应用领域，网络正在发挥着日益重要的作用。服务器/客户模型来越受到人们的推崇。Microsoft 的 Windows NT 操作系统由于强大的宣传攻势受到众多人士的注目，相信会有很多的用户会转到 Windows NT 及其网络上。根据美国权威 预测机构IT 的估计，Windows NT 到 1995 年将占据客户方操作系统的 70%～80% 的份额，可见 Windows NT 将来必成大器。在 Windows NT 发布刚近半年之际，推出本书可以满足各个层次人士的求知欲望。

Windows NT 是 Microsoft 公司的最新成员，是九十年代最先进的操作系统之一。本书将从几个方面介绍 NT 的网络服务。我们将同时考虑到读者对 Windows NT 网络服务的理解，以及怎样在其上使用网络服务功能等等。使得你通过阅读本书之后，能够正确评估是否选择 Windows NT 网络高级服务器，知道如何使用 NT 网络高级服务器，也能粗略了解最新的操作系统的网络原理和设计方法。如果你能在这几方面有所收获，那么本书的目标也就达到了。

本书共分十一章。

第一章对 Windows NT 操作系统以及 NT 网络概念作一介绍，其中包括用户域、用户组、以及信任关系等名词的介绍。

第二、三章说明如何将 OS/2 上的 LAN Manager 升级到 Windows NT 网络高级服务器。

第四章说明一些可能用到的网络知识。

第五章从用户界面说明 Windows NT 网络的操作和管理。

第六章介绍 Windows NT 网络的远程服务。

第七章介绍了 NT 远程服务软件的安装与使用。

第八章说明如何配置调制解调器。

第九章介绍了 NT 远程服务对 X.25 的支持。

第十章介绍了如何装置 NT 远程服务的中间安全检查装备。

最后一章介绍了如何执行系统维护和故障排除。

作　者

1993 年 11 月

目　录

第一章　NT 简介及网络基本概念

1.1　Windows NT 操作系统介绍

在系统地介绍 Windows NT 的网络服务之前，不讲一下 Windows NT 操作系统的一些特性，似乎令人有不完整的感觉，因而在这一部分我们将概要地把 Windows NT 操作系统里那些有趣的、强大而又巧妙的功能部分介绍给您，我们的目的是使您在没有 Windows NT 的常识情况下，通过读完这一部分后，仍能读懂后续章节的有关内容。

- Windows NT 的产生背景
- Windows NT 的特点
- Windows NT 的结构浏览

1.1.1　Windows NT 的产生背景

构造操作系统是一种复杂的、浩大的而且富有挑战性的工作，姑且不论没有多少计算机工作者能够有幸构造一个实际的操作系统，即便您能实现一个操作系统，也不见得能为大多数人所接受。从这一点讲，Windows NT 的实现者们是幸运的，他们的成果正在被愈来愈多的人们所青睐。当然，这里有他们所付出的艰巨劳动。

1988 年秋天，Microsoft 公司聘请了 David N. Culter（“Dave”）领导开发他们的 Windows NT 操作系统。Dave 是一位著名的小型计算机系统设计师，曾主持设计了很多大型操作系统，其中最著名的是 DEC 公司的分时系统 VMS。Dave 不负所望，Microsoft 于 1993 年 5 月 24 日正式推出了 Windows NT。

Microsoft 研制 Windows NT 是有多方面考虑的。纵观当今计算机领域，硬件技术正在突飞猛进地发展，CISC、RISC 两种体系的计算机竞争日趋激烈，特别是一些有希望的处理器技术的出现，比如在 Intel 的 CISC 技术基础上开发出的多处理器机器，迫切要求有相应的系统软件能使用这些硬件特性。Microsoft 认识到必须开发出一种能够利用这些及其他先进硬件特性的操作系统，一种 90 年代的、可以方便地在不同平台上移植的操作系统。尽管 Microsoft 在 80 年代与 IBM 合作开发了 OS/2，但是这个操作系统有很多缺点：不可移植（用汇编语言写的）、运行于单处理机—— Intel 计算机上，这些缺点促使 Microsoft 决定重新建立一个新颖的，可移植的操作系统—— Windows NT。

1.1.2 Windows NT 的特点

Windows NT 的出现并不是为了替代 DOS 上的 Windows 系列产品，Microsoft 希望它能够在高档的工作站平台及局域网络 LAN 的超级服务器方面占有市场，并且向主干计算机系统(Backbone)上发展。尽管 Windows NT 与 Windows 相比在很多方面看起来无甚改变，如 NT 和 DOS 上的 Windows 都支持图形用户接口 GUI 和 Win32 应用程序接口 API，但是，NT 具有：

- 良好的可移植性
- 可扩充性
- 安全性达到美国政府 C2 级标准。为每个应用程序提供 32 位虚拟地址空间，突破了 DOS 640K 瓶颈限制。
- 支持对称多处理机结构 SMP(Symmetric Multiple Processors)与多线程程序
- 将网络功能集成在操作系统中
- 16 位标准字符集

1.1.2.1 良好的可移植性

可移植性是一个定性而非定量概念，可移植性问题的关键在于软件移植的难度有多大，而不在于软件是否可移植(只要不惜代价，大多数软件最终都是可移植的)。

Windows NT 设计时采用了以下几种技术，从而使它变得容易移植：

用可移植的 C 书写 NT 的主要部分，他们所用的 C 语言中含有异常处理机制，即扩展了 C 语言的功能；Windows 环境的图形部分及部分网络接口用 C++书写；汇编语言只用来书写硬件通信及要求最优速度的部分。这些手段保证了代码级可移植性。

把与具体处理器结构相关的数据结构及对寄存器的操作代码放在一个小模块中，这些模块可为其他处理器的类似模块所取代。这就实现了操作系统其它部分与处理器无关。

使用同一种处理器——如 sun sparc ——生产出来的工作站之间有很多不同之处，为了获得在这些平台之间的移植性，NT 将与特定平台有关的代码放在一个被称为硬件抽象层 HAL(Hardware Abstraction Layer)的动态连接库中，这使高层软件在移植时无需改动。

因为它是 32 位的，所以 Windows NT 易于移植到那些 32 位编址的机器上。

1.1.2.2 良好的可扩充性

Windows NT 借鉴了 Mach 操作系统的微内核技术：构造一个很小的内核，由它提供主要的操作系统服务，而由被称为服务器的应用程序提供其它的操作系统功能，包括完整的 API。服务器可增强成新的服务器，从而使 NT 具有良好的可扩充性。

NT 支持可装载驱动程序，一种新的文件系统、设备及网络可以通过 Windows NT 的 I/O 系统装入相应的文件系统驱动程序、设备驱动程序或传输驱动程序得到实现。NT 还支持 RPC(Remote Procedure Call)机制，这种机制调用远程服务，无需考虑服务在网络上的位置，网络上某个计算机上新增服务立即可为其他计算机使用。

1.1.2.3 C2 级安全性

Windows NT 提供了以下保护特性以使用户避免遭到意外的或恶意的侵袭：

① 美国政府认可的安全性结构。其中包括用户登录、资源配额及对象保护等安全机制，所谓资源配额是指一种限制某一用户可用资源(比如硬盘空间)数量的机制。

② 提供虚拟内存，由虚拟内存管理程序控制每一用户的内存空间，这样每个用户进程都可以运行在一个保护子系统下，一个进程失败，并不影响系统内其它进程正常运转，并且能够防止一个用户非法读出或修改另一个用户的内存数据。

另一个与安全性类似的问题是稳固性，稳固性与安全性合称为操作系统的可靠性。在此我们主要介绍一下 Windows NT 的文件系统稳固性。

Windows NT 支持 FAT、HPFS (High Performance File System)、CD-ROM 及其本身的文件系统 NTFS，NT 可随时装入这些文件系统。NTFS 是 Windows NT 自己的文件系统，它能够管理 1.7 兆 terabytes 的数据，几乎是大得难以想象，而 HPFS 只能管理 7.6GB数据，NTFS 还 允许只可执 (Execute-only)文件、文件的多属性连接(即文件附有一些传统文件没有的属性)及长文件名到短文件名的自动映射。Windows NT 的 NTFS 这些特性使得 Windows NT 服务器能够胜任各种要求的服务器，大得近乎无限制的硬盘空间能够满足超级服务器的要求。

NTFS 能从各种磁盘错误下恢复，其中包括关键盘区的错误。它采用冗余存储及基于事务的方案来保护数据，从而保证了出错后的可恢复性。所谓基于事务的方案是指把一件任务看成不可分割的单位，只有该任务的各部分全部完成，才执行对硬盘的改动，中间任何一步失败都会导致整个任务的失败，对硬盘保证没有影响。

NT 的高级网络服务器支持 1 级和 5 级安全的冗余磁盘阵列 RAID 技术，基于 RAID 技术的磁盘系统提供磁盘阵列、剪取(Striping)及镜象冗余功能，这些都提高了系统的容错能力和从错误恢复的能力。

1.1.2.4 *对称多处理机技术 SMP*

Windows NT 是目前硬件平台可移植性最佳的操作系统，它支持 Intel 系列机及 RISC 系列机，如 MIPS R4000、DEC Alpha 机等；另外 ，Windows NT 可以有效地利用 SMP 技术，充分发挥多处理机系统带来的优越硬件性能。这两点 Windows NT 操作系统具有良好的可伸缩性——不但能在不同硬件平台上运行，而且还支持多处理器机器。下面，我们重点介绍一下 SMP 技术。

对于具有多个处理机的机器，以前的操作系统都以非对称方式 ASMP 使用它们，所谓非对称方式，系操作系统将各个不同的服务分别指定到某一固定的处理机上，比如文件系统服务由甲处理机完成，应用程序由乙处理机执行……，比起单处理机机器，这种做法无疑会提高系统的性能，但是对于具有多个对称处理机的系统，这还不够，这样做还没有完全发挥处理机整体的效益，比如应用程序需要 I/O 服务时，它必须等待文件系统处理机甲完成后，才能继续运行。ASMP 操作系统适合于在具有多个非对称处理机的机器上运行，比如由一个主机带一个或者几个协处理器这种结构的机器。有没有办法使多处理机达到更大的并行度呢？有的，对称多处理机 SMP 技术就满足了这个需要。

对称多处理机要求各个处理机地位是平等的，没有控制和被控制的关系，Windows NT 操作系统 可以在某一处理机上运行，也可以在其它几个处理机上运行，每个处理机既可运行一个进程，也可以运行一线程，总之，目标是使各个处理机充分地运转起来、尽量

避免空闲和等待。对称多处理的目的是使各个处理机以最大的利用率运转起来。各个处理机之间共享内存。线程是一个比进程小一些的概念，可以把线程看成可独立运行的程序单元。一个进程可以分解为若干个线程，这些线程可以并行运行，并且共享同一内存，这样就可以避免了程序运行中一些不必要的等待。图 1-1 说明了上述这些概念及关系。举例来说，有一个进程要完成数据库操作，一部分是与用户交互来读取用户数据，一部分是查询数据库，若查询部分是很耗时的操作，则可以将这两个操作作为线程分别运行在不同的处理机上，显然这样会提高系统的响应速度，避免了这两部分之间不必要的等待。目前的 Windows NT 最多支持 4 个多处理机，委托开发(OEM)的 Windows NT 有可能支持更多。关于对称多处理技术、线程当然还有很多细节需要详细说明，我们这里只是交待了一个大概，如果您需要做深入的了解，可以参考有关的专著。对于本书来说，了解这么多已经足够了。

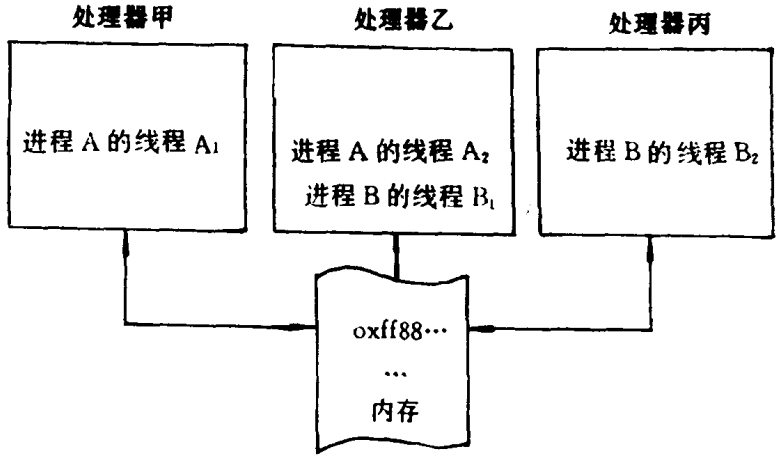

图 1-1

1.1.2.5 内装的网络结构

由于计算机通信的需要，个人计算机网络被广泛的引入到现存的操作系统中，这些网络功能参数是通过在 MS-DOS 、OS/2 和 UNIX 等操作系统上增加具有联网功能的应用程序及驱动程序来实现的，所以有人称 LAN Manager 为“网络操作系统”严格说来并不准确。这些网络软件实现了用户帐号、资源安全性和一些计算机通信机制，如套接字(Socket)、命名管道等。然而，在 Windows NT 中，网络软件不再作为操作系统的一个附加层来运行。而是作为 NT 本身包含的一部分来运行，即将上面所提功能作为操作系统的功能来实现。

NT 内装网络目的是实现同级(OSI 分层)联网，并且不需要用户为联网添加任何附加的服务器。同时，由于把网络功能做到操作系统内部，使得可以利用操作系统的一些功能，比如高速缓存，来优化网络服务性能。

NT 内装网络的另一目的是使不同的联网软件、硬件在利用 NT 时能够方便地加入网中运行，即现存的网络、网络驱动程序和网络服务器(如，Novell Netware、Banyan

VINES 和 SUN NFS) 在 Windows NT 中能够容易地进行交互和交换数据，Windows NT 内装网络软件能够装入和卸出操作系统，因而这个目的可由装入相应的网络驱动程序而得以实现。

Windows NT 还有以下联网目标：

① 与在其他操作系统上运行的 LAN Manager 交互操作；

② 提供存取 LAN Manager 以外其它网络上非 Microsoft 文件系统的功能；

③ 提供构造分布式的、具有较好可靠性的应用程序的工具，如数据库服务程序等。

1.1.2.6 16 位标准字符集

为了使 Windows NT 真正成为一个多国语言、国际化的操作系统，Windows NT 采用了一个称为 Unicode 的统一字符代码集来表示数据，这是一种 16 位编码方式，可表示 65,536 个字符，足以应付各种语言的编码需要。图 1-2 是 Windows NT 国际化的界面。在这里用户可以选择语言(不只是英文)、货币表示方法、日期表示方法等。

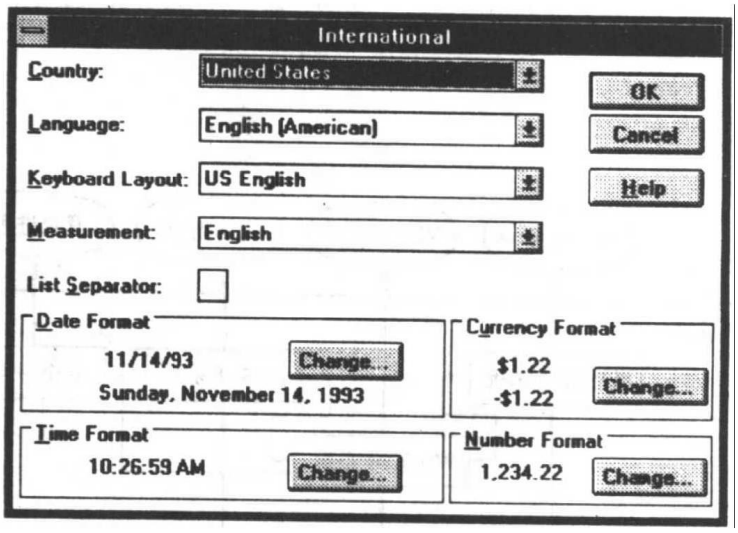

图 1-2

1.1.3 对 Windows NT 结构的简单浏览

对操作系统构造和操作系统理论不感兴趣的读者可以略去这一部分，一般对你使用 Windows NT 没有多少影响。

Windows NT 的基本结构可以分为两部分：系统用户态部分(Windows NT 保护子系统)和系统核心态部分(NT 执行体，内核)。

Windows NT 系统用户态部分包含若干服务器，这些服务器被称为保护子系统(Protected Subsystems)，它们之间可通信，它们也可以与内核通信。

NT 执行体可以支持任意数量的保护子系统(服务器)，服务器把 Windows NT 执行

体的功能提供给其用户及应用程序，并提供程序设计接口。即用户和应用程序可以通过服务器调用 NT 执行体的服务。

每个保护子系统提供一个用户程序可调用的 API，Windows NT 有两类保护子系统：环境子系统和集成子系统。每个环境子系统是一个用户态服务器，为特定的操作系统（如 MS-DOS、Windows、UNIX）提供一个 API，这样，NT 获得运行从多种操作系统平台上来的应用程序的能力。

Windows NT 最重要的环境子系统是 Win32 子系统。这个子系统提供了 32 位的 Windows 应用程序接口 API，由它控制所有来自用户的输入和应用程序的输出。NT 还提供了一个 POSIX 环境子系统、一个 OS/2 环境子系统、一个 16 位 Windows 子系统和一个 MS-DOS 环境子系统。一个应用程序运行时首先由 Win32 子系统判断它属于哪一类操作系统，交由相应的环境子系统来执行，即 DOS 应用程序交由 DOS 环境子系统执行，16 位 Windows 应用程序交由 16 位 Windows 环境子系统执行，等等。这些应程统执行，16 位 Windows 应用程序交由 16 位 Windows 环境子系统执行，等等。这些应用程序的输出及用户输入由 Win32 负责传送和处理。

集成子系统指那些完成重要操作系统功能的服务器，如子系统、网络子系统等。

保护子系统的关系如图 1-3 所示。

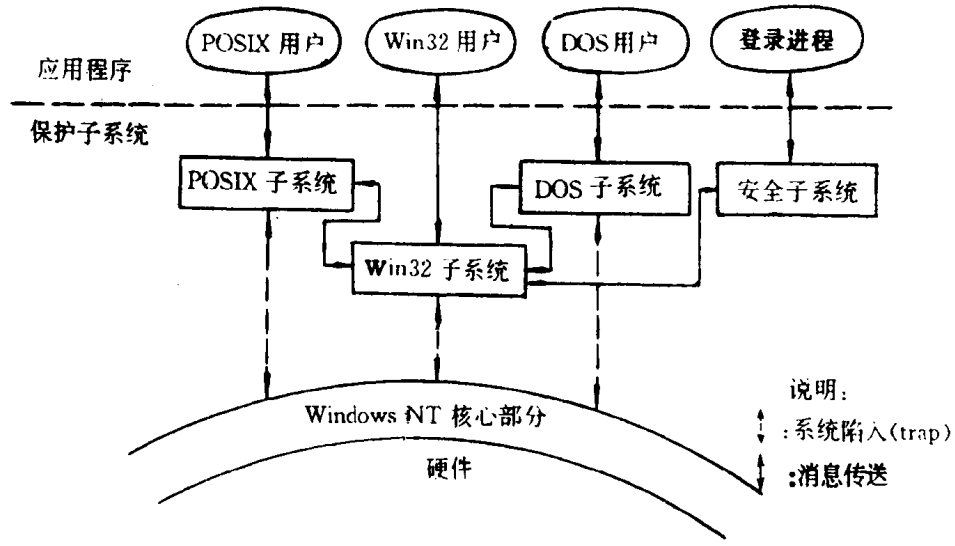

图 1-3

Windows NT 是一个安全性较好的操作系统，系统中每一用户都有一个帐号，每个帐号都有相关的安全信息数据集。系统中有若干登录进程(Logon Process) 负责等待用户输入登录信息，由于用户可从键盘/鼠标登录，也可以从网络连接登录，故设置多个登录进程负责验证相应登录要求的合法性。当它检查到用户试图访问系统时，就向用户索取用户帐

号名及口令。

登录进程把获得的安全信息交给安全子系统，由安全子系统对照安全数据库进行用户登录合法性检查，一旦用户合法，则为该用户生成唯一的一个安全标记 SID，供以后在系统内区别该用户，并把系统的控制权及 SID 交给 Win32 环境子系统，Win32 子系统取得屏幕控制权。Windows NT 启动后的界面看起来与 Windows 3.1 很相似。

NT 的网络子系统是使用可卸出/装入的文件系统驱动程序来实现的，也就是说，网络软件被看成一种文件系统驱动程序，可由文件系统将网络软件装入和卸出 Windows NT 操作系统。Windows NT 通过文件系统驱动程序调用 Windows NT 转发程序，转发程序接收对于远程文件的存取请求，并把它传送给另一名机器上的网络服务器，完成相应的网络服务。如图 1-4 所示。

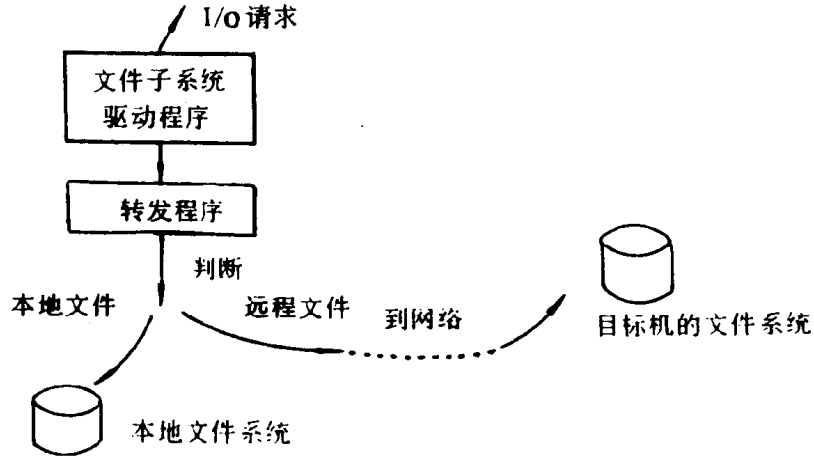

图 1-1

1.2 基本概念介绍

在本书，我们将介绍 Windows NT 高级服务器(Windows NT Advanced Server)中的一些概念，包括：

- 用户域 (Domain)
- 用户组(Group)
- 用户域之间的信任关系(Trust)
- Windows NT 高级服务器的安全机制

注意，在本书中提及 Windows NT 高级服务器时，根据上下文不同，有时指网络服务器软件，有时指运行该软件的机器，请注意区别。

由这几个概念将衍生出以下几个问题：

- 用户域模式(Domain model)
- 混合域内的其它服务器与 NT 服务器之间的互操作(关于混合域的构造，我们以后

将详细说明)

下面,我们将依次介绍这些问题与概念:

1.2.1 用户域

Windows NT 高级服务器在LAN Manager 的域概念基础上建立并扩充而形成自己的用户域概念。LAN Manager 的域概念是这样的:

在LAN Manager 中,一个用户域是一组服务器组成的一个逻辑单元(这些服务器在物理位置上不一定离得很近),属于该域的任何用户都可以只通过一次登录(Logon)而达到访问整个域中所有资源(如服务器应用程序、打印机、文件等)的目的(当然,是在有权限限制的情形下)。在一个域中,有些工作站上运行着域控制器(Domain Controller),由它们负责验证登录用户的合法性。整个域中有一个一致的用户帐号数据库,将该数据库复制到各个域控制器,从而赋予了各域控制器以检查登录合法性的功能(图 1-5)。

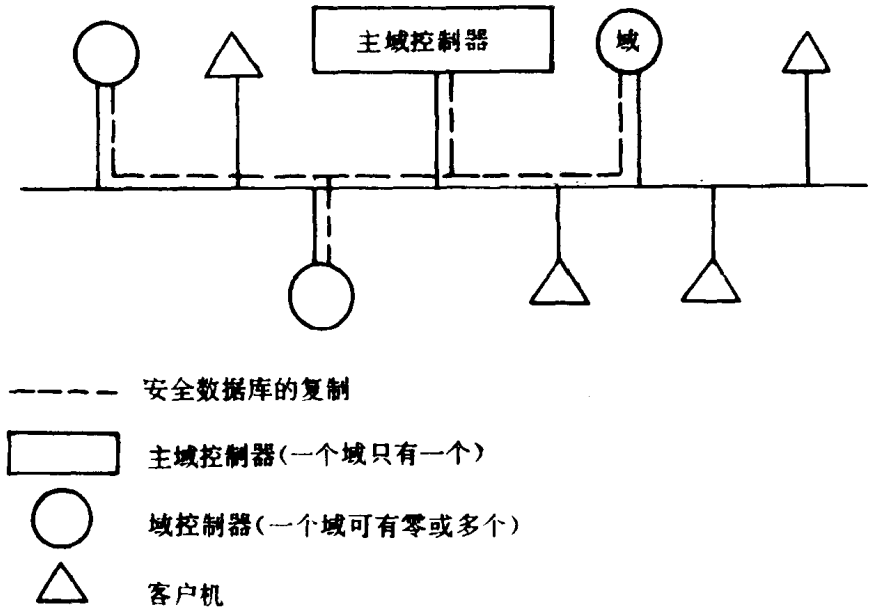

图 1-5

用户域中的每个用户对资源的使用权是不一样的,如果对每个用户的权限分别进行管理,当然是可以的,但是这样将加重管理的负担,影响系统的性能。而LAN Manager 通过把那些可以拥有相同权限的用户合为一个组,对组赋予组权限,从而简化了管理任务。比如,为可以使用网络打印机的用户建一 Printer 组,一个叫 Howard 用户加入该组,便具有了使用打印机的权利。同一用户还可以加入到不同的组中以拥有多种权利,如 Howard 还可以加入 admin 组,这样他便具有了管理系统的权利了。

以上是对LAN Manager 用户域概念的简单描述。Windows NT 高级服务器对LAN Manager 的用户域概念进行了以下扩充和加强:

1. 在整个企业(Enterprise)网络(一般由多个用户域组成)范围内,而不只是在一个