网络安全管理与 Windows 2000

黎 萍　陈建华　编著

人 民 邮 电 出 版 社

需要全本请访问 www.ertongbook.com

图书在版编目（CIP）数据

网络安全管理与 Windows 2000/**黎萍，陈建华编著.北京：人民邮电出版社，**2000.9
ISBN 7-115-08679-6

I.**网**… II.**①黎**…**②陈**… III.**①计算机网络安全技术②窗口软件，**Windows 2000 IV.TP393.08

中国版本图书馆 CIP **数据核字（**2000**）第** 41096 **号**

内 容 提 要

本书从网络管理的角度出发，介绍了网络系统的安全性和 Windows 2000 **的基本知识。作为网络管理员怎样使网络更安全？网络安全需要哪些技术？**Windows 2000 **的安全性如何？如何使用** Windows 2000**？对于这些问题书中均作了较为详细的叙述。**

本书通俗易懂、内容丰富、实用性强。适合网络管理人员、网络研究开发人员、大专院校的师生和计算机联网用户阅读参考，也可作为 Windows 2000 **的培训教材。**

网络安全管理与 Windows 2000

◆ **编　　著　黎　萍　陈建华**
责任编辑　张瑞喜

◆ **人民邮电出版社出版发行　　北京市崇文区夕照寺街** 14 **号**
邮编 100061　**电子函件** 315@pptph.com.cn
网址 http://www.pptph.com.cn
北京汉魂图文设计有限公司制作
北京顺义向阳胶印厂印刷
新华书店总店北京发行所经销

◆ **开本：**787×1092 1/16
印张：20.25
字数：502 **千字**　　2000 **年** 11 **月第** 1 **版**
印数：1 – 0 000 **册**　　2000 **年** 11 **月北京第** 1 **次印刷**

ISBN 7-115-08679-6/TP·1746

定价：30.00 **元**

前　　言

Windows 2000 是 Microsoft 公司最新推出的网络操作系统，这个操作系统基于 Windows NT 技术，也包含了一些 Windows 98 的成分。它充分发挥了先进的 CPU 的处理能力，并采用了操作系统的最新技术。与 Windows 2000 以前的操作系统相比，增加了许多令人激动的新功能。它使用对称的多处理器结构，大大提高了运行效率；使用抢占式多任务管理，提高了系统的响应速度和运行保障能力；使用 Internet 连接向导，使得连接 Web 更加简单和方便；它支持多种网络传输协议，可以方便地与其他网络操作系统连接，共享网络资源；使用完善的安全系统，能可靠地识别和管理用户及保护系统资源。Windows 2000 与 Windows 其他版本的不同点是： Windows 2000 弃用了 Windows NT 4.0 的域（Domain）管理，采用全新的活动目录服务（Active directory service)技术，并给出一系列基于目录的技术和工具。 为了帮助读者更好地掌握 Windows 2000 的使用，我们结合国内用户的实际使用情况，编写了《 网络安全管理与 Windows 2000》一书。

本书为用户、尤其是初学者着想，深入浅出地论述了网络安全管理和 Windows 2000 的各种基本功能和使用方法。全书分为 Windows NT 网络安全概述、Windows NT 网络安全性实施、Windows NT 文件系统（NTFS）的安全性、Windows 2000 的安全性、Windows 2000 网络管理、Windows 2000 的基本操作、Windows 2000 的资源管理系统、Windows 2000 的存储管理与性能优化、用户帐号的管理、Windows 2000 的网络打印管理、中文输入 —— 多语言技术、Windows 2000 中的 Internet Express、使用 Outlook Express 收发电子邮件和阅读新闻等章节。内容丰富、叙述详细并且配有大量插图，读者可以看图操作。

本书的读者对象为：

(1) Windows NT 网络管理人员；

(2) Windows NT 应用开发人员；

(3) 从事网络系统集成的科技人员；

(4) 大学生、研究生和对 Windows 2000 感兴趣的电脑爱好者。

本书在编写过程中得到了许多同志的帮助和支持，黎连业等同志对本稿提出了许多积极的建议，在此对他们表示衷心的感谢。由于作者水平有限，不当和错误之处在所难免，恳请读者批评指正。

黎 萍　陈建华

目　录

第一章　Windows NT 网络安全概述 ····· 1

1.1 **什么是网络安全性** ····· 1
1.2 **网络安全的威胁源** ····· 2
1.3 **建立网络安全保护策略** ····· 3
1.4 **网络安全设计** ····· 5
1.5 **使用容错技术** ····· 7
1.6 Windows NT **网络安全性的具体对象** ····· 9

第二章　Windows NT 网络安全性实施 ····· 19

2.1 **创建** Windows NT **域** ····· 19
2.2 **用户帐户和域的工作方式** ····· 20
2.3 **使用委托关系维护网络安全性** ····· 23
2.4 Windows NT **与用户帐户的安全性** ····· 28

第三章　Windows NT 文件系统（NTFS）的安全性 ····· 32

3.1 **为什么使用** NTFS **文件系统** ····· 32
3.2 **共享许可权与** NTFS **许可权** ····· 32
3.3 NTFS **的安全性** ····· 34
3.4 NTFS **的审核功能** ····· 38

第四章 Windows 2000 的安全性 ····· 39

4.1 Windows 2000 **安全性的特点** ····· 39
4.2 Windows 2000 **的加密文件系统** ····· 41
4.3 Windows 2000 **的安全模型** ····· 43
4.4 Windows 2000 **中安全证书的使用** ····· 43
4.5 Windows 2000 **中的安全级别设置** ····· 46
4.6 Windows 2000 **中的公用密钥体系** ····· 49
4.7 Windows 2000 **系统的安全性管理** ····· 50

第五章　Windows 2000 的网络管理 ····· 54

5.1 Windows 2000 **的最新特色** ····· 54
5.2 Windows 2000 **增强的网络功能** ····· 60
5.2.1 Windows 2000 **中的工作组、域和域树** ····· 60

5.2.2 Windows 2000 动态式目录服务……62
5.2.3 Windows 2000 微软管理控制台（MMC）……67
5.2.4 Windows 2000 其他增强的功能……68
5.3 Windows 2000 的更改和配置管理功能……74
5.3.1 Windows 2000 的更改和配置管理功能的特点……74
5.3.2 Windows 2000 更改和配置技术……74
5.4 从 Windows NT 4.0 升级到 Windows 2000……76
5.4.1 升级到 Windows 2000 的优点……77
5.4.2 Windows 2000 活动目录域模型……78
5.4.3 主域控制器的升级……81
5.4.4 备份域控制器的升级……84
5.4.5 多域模型的升级……85
5.4.6 保证升级的安全性……85

第六章 Windows 2000 的基本操作……87

6.1 启动、登录和退出 Windows 2000……87
6.1.1 启动 Windows 2000……87
6.1.2 登录 Windows 2000……87
6.1.3 退出 Windows 2000……88
6.2 Windows 2000 的桌面……89
6.3 Windows 2000 的窗口……92
6.3.1 窗口的组成……92
6.3.2 窗口的操作……93
6.4 Windows 2000 的对话框……99
6.4.1 对话框的基本组成元素……99
6.4.2 对话框的主要操作……100
6.5 Windows 2000 的菜单……102
6.5.1 几种常见的菜单……102
6.5.2 菜单的基本操作……104
6.6 启动和关闭应用程序……105
6.6.1 启动应用程序……105
6.6.2 关闭应用程序……107
6.6.3 在多个应用程序间切换……108
6.7 文档的管理……108
6.7.1 文档的打开和查找……108
6.7.2 文档的复制、移动和删除……108
6.7.3 文档的保存……109
6.8 设计自己的任务栏和开始菜单……109
6.8.1 设计自己的任务栏……109
6.8.2 设计自己的开始菜单……111

需要全本请访问 www.ertongbook.com

6.9 Windows 2000 的帮助系统 112
6.9.1 使用系统帮助文件 112
6.9.2 获得特定项目的帮助信息 113
6.9.3 从 Internet 上获得帮助 113

第七章 Windows 2000 的资源管理系统 115

7.1 Windows 2000 中的文件和文件夹 115
7.2 使用“我的电脑”管理系统资源 116
7.3 使用“资源管理器”管理系统资源 119
7.4 使用“网上邻居”浏览网络系统资源 121
7.5 管理文件和文件夹 124
7.5.1 创建、打开和保存文件和文件夹 125
7.5.2 文件和文件夹的基本操作 129
7.5.3 创建快捷方式 146
7.5.4 同步文件 151
7.6 回收站的有效利用 153
7.6.1 恢复被误删除的文件或文件夹 153
7.6.2 清空“回收站” 153
7.6.3 设置“回收站”属性 154

第八章 Windows 2000 的存储管理与性能优化 155

8.1 Windows 2000 的文件系统 155
8.2 Windows 2000 的分布式文件系统 159
8.3 Windows 2000 的磁盘管理 162
8.4 Windows 2000 的存储功能 166
8.5 Windows 2000 的远程存储管理 170
8.6 Windows 2000 的系统管理和性能优化 180
8.6.1 使用 Microsoft 管理控制台（MMC） 180
8.6.2 设置系统属性进行性能优化 181

第九章 用户帐号的管理 187

9.1 设置用户帐号 187
9.1.1 用户帐号的类型 187
9.1.2 规划新的用户帐号 188
9.2 管理用户帐号 189
9.2.1 查看本地用户组 189
9.2.2 创建新的用户帐号 190
9.2.3 设置用户工作环境 191
9.2.4 修改用户帐号 195
9.2.5 设置用户任务 197

9.3 设置组……199
9.3.1 什么是组……199
9.3.2 组的类型与特性……199
9.3.3 规划新的分组……201
9.3.4 查看本地组……201
9.3.5 创建新的本地组……202
9.3.6 设置组帐号的属性……204
9.3.7 组的删除和重命名……205
9.4 Windows 2000 的系统安全性管理……205
9.4.1 用户帐号的安全性管理……205
9.4.2 网络系统的安全性管理……208

第十章 Windows 2000 的网络打印管理……209

10.1 Windows 2000 打印概述……209
10.1.1 Windows 2000 的打印特性……209
10.1.2 Windows 2000 中的打印术语……210
10.1.3 Windows 2000“打印机”的连接方式……210
10.1.4 Windows 2000 网络上安装打印设备的要求……212
10.2 在 Windows 2000 下安装网络打印机……212
10.3 连接到网络打印机……215
10.4 配置网络打印机……217
10.5 设置打印机属性……221
10.6 设置打印机使用权限……228
10.7 设置打印服务器属性……230
10.8 Windows 2000 中的 Internet 打印服务……231

第十一章 中文输入——多语言技术……238

11.1 中文输入法的管理……238
11.1.1 安装中文平台……238
11.1.2 中文输入法的删除……240
11.1.3 设置输入法属性……240
11.1.4 设置输入法的热键……241
11.2 中文输入法的使用……242
11.2.1 中文输入法的用户界面……242
11.2.2 选用中文输入法……243
11.2.3 设置输入法功能……243
11.2.4 手工造词……245
11.2.5 在线造词……245
11.2.6 重码选择……246
11.3 使用输入法生成器……246

11.3.1 码表源文件格式……246
11.3.2 创建输入法……247
11.3.3 码表逆转换……249
11.3.4 词条排序……249
11.3.5 批量造词……250
11.4 字体的管理……250
11.4.1 安装新字体……250
11.4.2 删除字体……251
11.4.3 设置字体选项……252
11.5 使用造字程序……255

第十二章 Windows 2000 中的 Internet Explorer 5.0……257

12.1 Windows 2000 中 IE 的最新特色……257
12.2 安装、添加和设置 Internet Explorer 5.0……259
12.3 Internet Explorer5.0 的使用……264
12.3.1 走入 Internet Explorer5.0……264
12.3.2 预订 Web 站点……268
12.3.3 设置频道屏幕保护程序……271
12.3.4 设置和管理活动桌面……272
12.3.5 漫游万维网……275
12.4 自定义 Internet Explorer5.0……279
12.4.1 自定义 Internet Explorer5.0 的起始页……279
12.4.2 规划“收藏”文件夹……279
12.4.3 优化自己的 Web 页……281

第十三章 使用 Outlook Express 收发邮件和阅读新闻……283

13.1 Outlook Express 的主要功能……283
13.2 电子邮件使用基础……284
13.2.1 什么是电子邮件……284
13.2.2 使用电子邮件需要什么条件……285
13.2.3 Internet 电子邮件的功能……285
13.2.4 电子邮件信箱地址……286
13.2.5 电子邮件的运行方式……287
13.2.6 电子邮件格式……288
13.3 Outlook Express 的启动与常用设置……288
13.3.1 启动 Outlook Express……289
13.3.2 Outlook Express 常用设置……289
13.4 使用 Outlook Express 收发邮件……291
13.4.1 查看电子邮件……292
13.4.2 发送电子邮件……293

13.4.3 回复电子邮件……294
13.4.4 使用信纸……294
13.4.5 管理电子邮件……294
13.5 使用 Outlook Express 阅读新闻……296
13.5.1 连接到新闻服务器……297
13.5.2 设置下载新闻组内容……299
13.5.3 防止自动下载新闻组邮件……299
13.5.4 整理新闻组文件……300
13.5.5 阅读新闻……301
13.5.6 Outlook Express 脱机工作方式……301
附录：安装 Windows 2000 的主要过程…… 303

第一章　Windows NT 网络安全概述

随着计算机网络技术的发展和局域网、因特网的广泛应用，网络系统的安全责任越来越重大，网上“黑客”、计算机病毒等问题，使得网络管理人员更加关注于网络安全问题和防火墙技术。

本章重点介绍网络安全性的基本含义、网络安全性与使用 Windows NT 的关系，目的使读者了解 Windows NT 网络安全的基本知识。

1.1　什么是网络安全性

简单说来，网络安全性就是保护用户在网络上的程序、数据及设备免遭别人在非授权情况下使用或访问。

实际上网络安全性的含义还包括若干较为复杂的系统管理方面的问题。也就是说，网络安全的目标不仅是保护网络系统的部件、程序、数据免遭他人非法使用和访问，而且也保护企业的权益不受侵犯。

网络安全计划的主要任务是保护系统的数据、程序、设备和网络部件的安全，使其免遭损坏、偷窃或误用，同时也包括需要时网络能提供安全服务。这种网络安全计划的实施可以通过网络操作系统提供的安全工具、系统设计中的冗余以及提供必要的物理屏障阻止非授权人员访问系统部件等手段来完成。

随着科学技术的发展，现代企业解决问题的办法正在变得针对性越来越明确，同时越来越依赖于分布式计算机网络使群体人员一起协同有效地工作。另外，对于技术上更加复杂的保护方法的要求也越来越高。网络系统越来越复杂，要想达到预期的安全效果的难度也越来越大。

在实施网络安全计划的同时，遇到的一个重要问题即是限制系统的最终用户对系统资源的访问。因为，对网络安全计划的最终目标是允许网络用户为使用网络而访问所需的程序和数据，而不受任何不必要的限制，使得网络用户能以快速有效的方式访问授权访问的资源。

网络安全的具体内容如下：

计算机通信安全的内容远不只是使用用户识别码和口令，它还包含着广泛的规则和惯例。我们认为：网络的安全性是由数据的安全性和通信的安全性两部分组成的。数据的安全性是一组程序和功能，用来阻止对数据进行非授权的访问、转移、修改和破坏；通信的安全性是一种保护措施，要求在通信中采用保密安全性、传输安全性、辐射安全性等措施，并且要求对于通信安全性信息采用物理安全性措施。通过上述各种措施，可以拒绝非授权的人员

在通信中获取有价值的信息。通信安全性的具体定义如下：

(1) 保密安全性：通过提供技术保密系统以及对密码系统的正确使用来实现。

(2) 传输安全性：通过采取措施来保护传输不被除密码分析以外的手段来截获和利用。

(3) 辐射安全性：通过采取措施以拒绝非授权的人员获得有价值的信息来实现，而该信息是从密码设备和电信系统的泄露性辐射截获并分析而得出的。

(4) 物理安全性：通过采取一切必要的物理措施来保护需要保密的设备、材料和文档，使其不被非授权的人员访问和观察。

通信安全性的分层如图 1-1 所示。

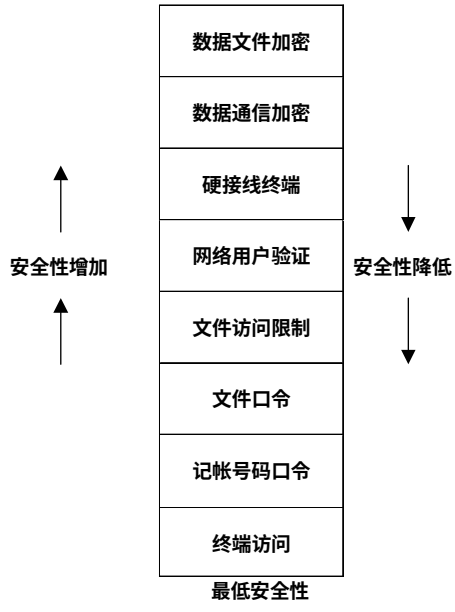


图 1-1　通信安全性的分层

从图 1-1 可知，安全性的技术定义与加密技术有着直接的关系，加密是保护信息最有效的方法。

1.2　网络安全的威胁源

分布式网络系统的安全威胁分为人为威胁源和物理威胁源两种基本类别。

一、人为威胁源

所谓人为威胁源有两种，一种是指计算机黑客闯入用户的网络计算机系统，我们把它称为外部危险；一种来自系统的内部，我们把它称为内部危险。

1. 内部危险

网络内部危险包括下面内容：

(1) 设计安全方案过程中，没有考虑存在于员工和公司之间的关系。

(2) 网络安全需要花费管理人员的精力来维护和实施，造成经费的增大。

需要全本请访问 www.ertongbook.com

(3) 网络安全威胁主要来自企业内部松懈的、甚至完全不存在的安全措施。

(4) 用户对限制访问的安全策略有抵触情绪，不遵守安全标准。

要防止内部危险的发生，必须建立一套网络安全标准，规定与网络有关的资源以及每种资源允许的访问权限。另外，应该让用户了解如何正确使用网络资源，并且要有实施网络安全的措施。

2. 外部危险

网络外部危险包括以下内容：

(1) 窃取机密信息。

(2) 向外部透露敏感信息。

(3) 非法访问网络服务程序和资源。

(4) 干扰网络正常服务。

(5) 故意损害、修改和删除数据。

(6) 窃取或损坏硬件或软件。

二、物理威胁源

网络物理威胁源包括以下内容：

1. 设备故障

设备故障是导致网络数据丢失或无法使用的最常见的原因之一。对网络故障的检测依据是对网络组成部件的监测。轻微故障通常被记录在错误日志中，而严重的设备故障则需要通知网络管理员。如果在网络内配置有适当的冗余系统，就能避免设备故障，降低成本。

2. 物理损害

非法访问网络部件可能导致对系统的物理损害，为防止此类物理损害，需提供足够的安全地域放置主要的网络设备。

3. 无恢复计划

当发生自然或人为灾难时，必须实施恢复计划。人为地对网络安全进行检查有时也会造成对网络的物理损害。这种危险可能来自网络内部也可能来自外部。

物理保护网络部件安全的程序可以不同，用户可以在网站上安装监视器和报警设备，也可以把网络布线室封闭起来。

1.3 建立网络安全保护策略

要建立网络安全保护策略，首先需要考虑网络在哪些方面需要采取安全措施，如图 1-2 所示。

网络安全保护层及其功能如下：

1. 为物理层提供的安全保护

物理障碍层为保护网络安全提供了第一道屏障，目的是防止系统的硬件损失。网络上的硬件是系统的心脏，对硬件常见的危险属于环境性质的危险。如果把设备置于恶劣环境之中，对许多设备的损伤就容易发生。为提供物理层的安全保护，就应该在系统连接外界的中间设

置物理障碍，以保护系统免遭非法用户的进入。对物理层的安全保护设备包括储存装置、文件服务器、驱动系统、网络集成器，以及提供给用户与网络资源连接的通信装置等。

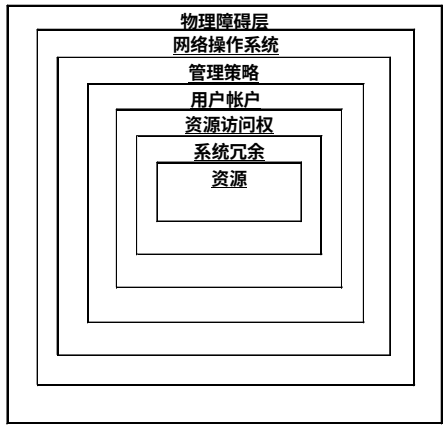


图 1-2　网络安全保护层

2. 为网络操作系统提供的安全保护

网络操作系统为保护网络安全提供了第二层保护。Microsoft 公司为高度安全网络服务器平台提供了一个内在的安全保护。通过网络操作系统这一层次的安全墙，它能为系统拥有或控制所有服务器对象增加审核功能。

3. 用管理策略实施安全保护

管理策略为保护网络安全提供了第三层保护屏障。用管理策略实施安全保护是资源保护的第二阶段，也是设计开始发挥作用的第一阶段。在这一层上的安全模式中，重点要集中考虑服务器管理器、域的用户管理器这样的网络管理实用程序的可访问性问题。

4. 分配用户帐户

分配用户帐户标识为保护网络安全提供了第四种安全保障手段。合法用户在系统上必须拥有系统承认的帐户，完成登录过程，并提供特定帐户的具体口令，才允许访问网络资源。

5. 资源访问权

资源访问权为保护网络安全提供了第五层安全保障。对资源的访问许可权，既可授予个人帐户，也可授予某个帐户 ID 是其成员的组。另外，文件访问权可直接应用于新技术文件系统（NTFS）格式化的磁盘驱动器分区上的文件和目录。文件许可权的优点是可以阻止在文件服务器上登录过程中，使用 Windows 界面的用户访问 Windows NT 上的文件和目录。

6. 系统冗余

系统冗余为保护网络安全提供了第六层保护。网络安全措施不仅能提供安全保障，还应提供快速恢复系统的功能。

服务器或系统连网部件中硬件设备的故障很容易通过给系统设计冗余而得以防止。分布式网络环境中的冗余在网络设计及其服务器部件中是最常见的。例如：把数据镜像到多个海量存储装置上去后，就提供了冗余。

冗余与容错两者之间的差异可以通过启动备份系统所需的时间识别。例如：数据的冗余可以通过把磁盘驱动器上的数据备份到磁带上来完成，也可以通过镜像驱动器来完成。

1.4 网络安全设计

进行网络安全设计常遇到以下安装新网络的安全设计和现有网络的安全设计两种情况。

一、安装新网络的安全设计

为新安装的网络进行网络安全设计有以下几个方面：

1. 设计物理安全保障措施

列出系统中必须保护的物理部件。具体地讲，应该列出构成网络硬件核心的服务器和网络设备清单。如表 1-1 所示。

表 1-1　　网络文件服务器以及保护方法

部件名称	潜在危险源	保护方法
网络文件服务器	暴露环境	提供防热、防冷、防潮湿的保护环境的器材
	电源差	安装不间断电源设备，清理、过滤输入电源
	断电	为设备提供备份并自动停止服务器程序的运行
	非授权访问	把设备部件锁在房间或柜子里
	病毒入侵	停用可拆卸媒体设备
	物理损坏	把设备部件锁在房间里或柜子里
	偷窃	保存一份最新的设备清单、并编上序号

根据表 1-1 所示，对网络中的每一个存储设备、发送设备、信息处理设备一一列表处理。

2. 提供安全的网络操作系统

网络操作系统是网络的心脏。它为企业信息提供了安全保护。在 Windows NT 操作系统中配置了一套强大的安全保护措施。这些保护措施功能如下：

(1) 任意控制访问。

任意控制访问用于指定用户对系统中指明对象的访问。

(2) 利用标识和验证确认帐户。

利用标识和验证确认帐户。要求用户在访问系统中的对象或资源以前，必须在系统中有一个帐户，而该帐户必须通过口令加以验证。

(3) 保护系统安全结构。

保护系统结构安全意味着系统可以保护自己不受系统外部改变代码或数据结构的影响。

(4) 对象重新使用。

对象重新使用明确规定了系统使用的对象在重新返回系统之前，必须清除附带的一切访问授权。

(5) 审核能力。

Windows NT 能够审核对系统中的所有对象的访问。审核功能可记录登录和退出、文件访问、对象删除、访问违章等事件。

3. 定义网络安全策略

在增加新的网络用户之前，用户应该定义网络的管理结构与以 Windows NT 为基础的局域网系统使用的域概念的关系。

如果使用多个域，就需要定义用来减少管理开销的域委托关系。在确定除 Windows NT 提供的缺省用户组外，还需要确定本地用户组和全局用户组，对于每一个新安装的系统，这些用户组是不同的。

4. 定义用户策略和属性

用户帐户策略和属性是决定允许用户如何与系统进行交互操作的关健。Windows NT 中的用户策略可以分成如下三个基本类别：

(1) 帐户策略。

帐户策略具体规定了与用户口令有关的选项。如果口令要更换，可以实施强制用户使用口令以及口令最短长度的安全策略。

(2) 权限策略。

用户权限策略使你能够给某个用户帐户分配不同的权限。例如：备份操作员组有权超越安全规程并备份服务器上的磁盘信息。服务帐户具有在 Windows NT 平台上运行服务程序的能力。

(3) 审核策略。

审核策略具体规定审核在你的系统上登录的层次，可以为用户提供在网络系统上各种有价值的事件记录数据。

可定义的用户其他属性还有：

- 用户更改口令。
- 帐户类型是全局型还是本地型。
- 指定用户主目录。
- 赋值用户配置文件和强制性配置文件。
- 赋值网络登录脚本。
- 分配用户到默认组。

5. 设置资源访问权

所谓资源，就是系统为用户提供的服务，具体说就是文件服务程序。它能让你访问在文件服务器中磁盘驱动器上的目录。此外，网络资源还包括打印机、调制解调器和数据库等。

设置资源访问权的方法如下：

(1) 将一台文件服务器标识为只允许本部门成员访问的主机。

(2) 把要访问的数据所在目录设定共享许可权，只允许拥有许可权的人员访问。

(3) 创建一个本地用户组，只允许这个组的成员有权改动在共享目录内的数据。

(4) 在访问服务器时，必须限制服务器的登录权以保护数据，否则应该使用 NTFS 许可权应用于访问数据所在的目录。

二、现有网络的安全设计

保护现有网络的安全可以按照设计新网络的安全性来考虑。不同之处在于，在设计每一层安全模式时，必须对现有的网络安全性作出评估，可以从物理层开始，逐层往下设计。

改进现有网络的安全性可按以下几项进行评估：

(1) 评估网络设备物理安全层的现状。
(2) 核实 NOS 所提供的安全特性与功能。
(3) 审定现有管理策略和手续。
(4) 检查网络上现有的用户特性和用户策略。
(5) 审查网络上的可用资源以及授予用户的资源访问权限。
(6) 确保存在替换手段，提供网络上的资源连接和管理支持。

三、设计物理安全措施

网络的物理安全措施可以包括许多不同的领域。每个领域必须加以标识，并对其在系统中的完整性作出评估。

使用表 1-2 所示的保护网络的物理结构，可以防止网络资源的损失。

表 1-2　　保护网络的物理结构

安全威胁	资源损失的原因	物理补救措施
设备造成的可用网络资源的损失	环境因素，通风差、高温或过分潮湿引起敏感电子部件损坏	把所有部件置于符合制造厂家环境操作规程要求的地方
	电源不合格引起部件失灵	安装浪涌电流抑制装置、改善线路条件，安装不间断电源设备
	停电引起重要的部件脱机	必要时应安装不间断电源来提供备份电源和自动关机服务程序
	物理损坏引起网络资源损失	把设备锁在房间里和柜子里
	设备被窃引起网络资源损失	保存一份所有设备的最新清单，并给所有设备编上序号
	普通文件、设备故障	为关键部件提供冗余备份系统
	自然灾害或物理灾害导致网络主要部件毁坏	建立灾难恢复计划，详细规定恢复硬件、软件和数据的办法
非授权物理访问网络部件	网络设备物理安全保护不好	锁好所有元器件
	双向访问系统允许 Internet 访问	关闭 IP 路由选择功能，停用有关网卡连接，使用防火墙系统代替双向跟踪
计算机软件病毒	使用线路窃取设备窃取通过网络传输的数据	保护传输线路，使其无法私自访问，对线路上发送的数据实施加密
	网络源感染	使用抗病毒软件
	从软盘等其他媒体传染的病毒	将服务器中存储设备锁住，用商业抗病毒软件来保护系统

1.5　使用容错技术

容错技术也是用来保护网络资源的一种方法，当网络出现故障时，提供物理的冗余系统部件作为备份。

一、保护驱动器介质安全的方法

1. 事务跟踪

保护数据的一种方法是使用 NTFS 卷上的事务跟踪日志。使用事务跟踪日志，系统出现故障时可以把磁盘驱动器上所包含的数据完全返回到故障前的状态。通过事务跟踪日志文件

可以查看到 I／O 写入过程中发生的正常进程。

(1) 启动 I／O 操作，把一个文件存到磁盘上。

(2) Windows NT 系统把 I／O 操作进程信息以及不断进行的改写信息存储到事务日志中。

(3) 系统把取消事务的信息记录在日志文件中。

(4) I／O 操作全部完成，文件得到更新。

2. 驱动器镜像与复式配置

使硬盘更为安全可靠的方法是使用驱动器的镜像和复式配置。驱动器镜像就是在同一服务器中安装两个容量基本相同的硬盘驱动器。当一个驱动器出现故障时，另一个驱动器就可以作为唯一的信息源使用。

复式配置与驱动器镜像的功能相似，不同点是复式配置给每个硬盘驱动器加一个控制器，提供又一个保护措施。

Windows NT 通过硬盘管理程序把同一系统中的分开的物理驱动器合成镜像（或者复式配置）驱动器集，这样的设置既提供了完整的数据，又可以在故障排除前获得系统资源。

3. 使用廉价磁盘的冗余阵列（RAID）系统

使用 RAID 系统是保护存在海量存储装置上信息的标准手段。RAID 系统与镜像或复式配置的差异在于提供数据冗余的方法和所涉及的开销不同。RAID 保护分成以下几种等级：

(1) RAID.0 级——它的功能是把数据分条存入多个硬盘，但当磁盘发生故障时，不能提供数据冗余。

(2) RAID.1 级——它的作用是包括带数据分条的磁盘镜像或复式配置。

(3) RADI.2 级——它的作用是在磁盘的信息位这一级上进行分条。

(4) RADI.3 级——它的作用是在所有物理磁盘上按字节分条写入信息，同时保留一个磁盘用于存放校验和数据。当出现故障时，可用该盘来恢复数据。

(5) RADI.4 级——它的作用与运行方式同 RAID.3 级相同，差异在于数据以块的形式跨磁盘写入，而非按字节写入。纠错数据如 RAID.3 级相同，保存在奇偶校验磁盘上。

(6) RAID.5 级——它的作用与运行方式同 RAID.4 级相同，数据用块的形式跨磁盘写入。RAID.5 级的奇偶数据是写入所有磁盘。

二、网络媒体容错

当出现单路或单向通信中断，网络媒体容错为你提供了一条替换通信信道，当电缆中断时令牌环网可以具备在多站访问装置之间构成回路。光缆分布式数据接口（FDDI）系统使用光缆，并采用两个反向旋转的网环实现冗余配置。

三、电源备份系统

由于计算机网络系统在用电质量、电压的不稳定，使得微机系统和其他网络设备经常出现故障。如果在网络设备上使用浪涌电流抑制装置、线路调节器或不间断电源（UPS）设备，便很容易解决这些问题。根据网络系统设备的不同可以选择以下的电源保护器：

1. 浪涌电流抑制器

浪涌电流抑制器用于保护网络部件不受电源线路上电压过高的影响。这些高压电，可能造成相当大的损失。但浪涌电流抑制器并不能消除进入的交流电，在电压过低或完全停电的情况下又不能提供电源。

需要全本请访问 www.ertongbook.com