

Cisco Internetworking with Windows NT & 2000

Windows NT 与 Windows 2000 的 Cisco 网络互联

(美) Toby J. Velte Amy Hanson Anthony T. Velte 著
戴 锋 莫海芳 李超峰 译



机械工业出版社
China Machine Press

OSBORNE



Education

Cisco专业技术丛书

Windows NT与Windows 2000的Cisco网络互联

Toby J. Velte

(美) Amy Hanson 著

Anthony T. Velte

戴 锋 莫海芳 李超峰 译



机械工业出版社
China Machine Press

本书介绍了在Windows NT和Windows 2000下的Cisco网络互联技术。内容包括硬件技术（如路由器、交换机、集线器、防火墙等），网络操作系统（如Windows及Cisco IOS），目录服务技术（如AD、DEN）。本书内容丰富，并提供了大量实例及设计蓝图以便读者学习。

本书适合于那些从事Microsoft和Cisco技术集成的业内人士。

Toby J. Velte, Amy Hanson and Anthony T. Velte: Cisco Internetworking with Windows NT and 2000 (ISBN 0-07-212083-5).

Copyright © 2000 by the McGraw-Hill Companies, Inc.

Authorized translation from the English language edition published by McGraw-Hill, Inc.

All rights reserved. For sale in the People's Republic of China.

本书中文简体字版由机械工业出版社和美国麦格劳-希尔国际公司合作出版。未经出版者书面许可，不得以任何方式复制或抄袭本书内容。

版权所有，侵权必究。

本书版权登记号：图字：01-2000-1714

图书在版编目（CIP）数据

Windows NT与Windows 2000的Cisco网络互联/（美）沃尔特（Velte T.），（美）汉森（Hanson A.），（美）沃尔特（Velte A.）著；戴锋等译。-北京：机械工业出版社，2001.11
（Cisco专业技术丛书）

书名原文：Cisco Internetworking with Windows NT and 2000

ISBN 7-111-09328-3

I.W… II.①沃…②汉…③沃…④戴… III.①窗口软件，Windows②计算机网络，Cisco产品的 IV.TP316.86

中国版本图书馆CIP数据核字（2001）第066158号

机械工业出版社（北京市西城区百万庄大街22号 邮政编码 100037）

责任编辑：崔继承

北京昌平奔腾印刷厂印刷 · 新华书店北京发行所发行

2002年1月第1版第1次印刷

787mm×1092mm 1/16 · 32.5印张

印数：0 001-5 000册

定价：50.00元

凡购本书，如有倒页、脱页、缺页，由本社发行部调换

前 言

本书所涉及的各种论题，对于设计、建立和维护使用Cisco和微软产品的那些网络都是很重要的。就网络互联来说，给出整体方法步骤是很重要的，但大多数的书籍都过于集中于技术支持或其他的某一方面，本书则强调网络硬件和服务器软件应该相互协调一致地进行设计、综合以及管理。

网络是复杂的，需要高超的技术和周密的计划。在Internet中70%的主干是由Cisco设备组成的。在这种情况下，全世界的企业网络所安装的基础设施中，Cisco网络硬件所占有的大量份额就不足为怪了。只要认为依赖于请求Internet服务提供商或电信专家们做出某种决断是比较头疼的问题，那么Cisco路由器、交换机和防火墙就将日益成为公司LAN/WAN管理员的选择对象。与此同时，如果Cisco的各种设想成为现实，那么越来越多的Cisco硬件和软件将会出现在管理员的桌面上，因此用户和管理员就需要对Cisco硬件和软件获得更深入的领悟。

管理员和用户都对Windows操作系统比对Cisco更熟悉一些。Windows所建立起来的庞大体系还在不断增长，而它理所当然是全世界最通用的桌面操作系统。这里所指的是Windows 95或98系统而不是指NT系统，但这种趋势将很快发生转变。Windows 9x系统在慢慢衰退，它们将被Windows 2000系统所代替，而当前的NT系统也将转变为Windows 2000。这个交会的趋势是明显的：Windows NT和2000与Cisco网络设备关系更紧密了；而对许多的用户、管理员以及IT决策者来说，这已经是理所当然的事了。

随着IT领域的融合，出现了许多新的挑战。用户和管理员将不得不对Cisco和微软系统都更加熟悉——特别是在它们合作的领域。该书对微软和Cisco的某些技术进行了讨论阐述，并对它们的交叉领域也做了适当论述。深入阅读，你将发现一些有助于掌握你的网络的有用工具。

涵盖内容

该书包含16章和4个附录。这些章被分为四个主要部分。第一部分讨论Cisco与Windows的融合；第二部分阐明建立网络的具体细节；第三部分集中阐述了在建立一个网络之后对它的管理；第四部分简要描述了把其他网络连接到你的网络可以使用的策略。

第一部分 Windows与网络的接触

该书的第一部分介绍了你所需要的背景知识，以便领会到今天Cisco和微软将如何塑造未来的网络。同时这一部分还涉及到一些现代组网技术的基础知识。

第1章“Cisco与Windows的结合”——该章对某些最新新闻做了一定的论述，这些新闻都与微软Windows 2000和Cisco的最近策略有关。它还介绍了你所需要的一些概念，使你能恰当地理解并用好本书所涉及的内容。

第2章“目录驱动网络”——该章描述了目录驱动网络的兴起的历史，同时还介绍了DEN和

基于策略的网络的一些基本概念。

第3章“网络基础”——该章对一些基本的网络问题做了介绍，如OSI模型以及各种各样的协议（以太网、令牌环以及快速以太网），其中还包括路由协议，对这些问题讨论的范围都与Cisco硬件和软件以及微软Windows 2000有关。

第二部分 用Windows 2000建造Cisco网络

这一部分涵盖了用简单和高级软件接口配置网络各组成部分时比较老练的处理方式。它的特色就在于，包含了若干Cisco和微软的工具，帮助你使你的配置工作更容易，同时还提供了一些专家技巧和简捷方法。

第4章“Cisco硬件和网络互联工具”——这一章包含了广泛的多种可用硬件的选择，包括路由器、交换机、集线器、访问服务器以及防火墙，同时着重强调了它们许多特有的特性与功能。该章还详细地介绍了Cisco网际操作系统（IOS），并在最后考察了电缆、接线器以及各种管理和故障检测工具。

第5章“配置路由器和RRAS”——该章论述了路由器的配置与安装。它重点强调了在一个实验室的环境下测试新设备和测试IOS版本更新的过程，并提供了一个简单的你可以使用的配置前核对清单，带你一步一步地通过路由器引导过程。该章还详细地介绍了Cisco ConfigMaker和NetSys Baseline，同样详细讨论了如何在Windows机器上设置TCP/IP、Windows路由列表以及微软的路由与远程访问服务（RRAS）。

第6章“安装交换机与VLAN”——该章讨论了Cisco交换机，包括那些支持高性能桌面连通性、企业工作组集合以及分散建筑物集合的交换机。它细致论述了Cisco基于Web的可视化交换机管理（VSM）软件，同样细致论述了生成树协议（STP）以及交换端口分析器（SPAN）。它还讨论了VLAN配置问题、中继方式以及VLAN管理。

第7章“配置Cisco集线器”——该章涵盖了中继器技术、以太网标准以及IEEE 802.3 10BaseT与100BaseT的规范等方面的基础知识。它还对Cisco的Class II中继器的FastHub系列进行了评析，并提供了布线规范说明。该章同时还提供了一些方案，阐述如何使集线器在网络中能比较经济实惠地进行安装。

第三部分 管理一个Cisco/Windows网络

这一部分集中于那些管理一个Cisco/Windows网络的产品和方法，它包括高级活动目录的设计和管理策略、Cisco设备管理，以及Windows NT和Windows 2000的命名服务，如DNS、WINS和DHCP。

第8章“管理设备”——这一章包含了用于管理和配置Cisco/Windows网络的若干多种应用。其中包括HP OpenView和CiscoWorks2000，以及它们的一些附加组件。同时它还涉及到一些工具，这些工具用来帮助管理交换机、网络（包括ATM网络）以及某些特定的Cisco设备，如CiscoWorks交换网络互联（CWSI）、CiscoView、VLANDirector、TrafficDirector以及ATMDirector。

第9章“管理目录服务”——本章详细深入地研究了Windows 2000目录服务管理。它包括微软管理控制台以及各种各样的工具，这些工具可以用来实现对Windows 2000域更平稳、更快速、

低费用的管理。它还讨论了Windows 2000多主复制技术、在Windows 2000中的IP安全 (IPSec) 配置、系统管理服务器 (SMS)、IntelliMirror技术以及分布式文件系统 (Dfs)。

第10章“网络通信测试”——这一章涵盖了网络流量监控的预防和故障检测两方面，以及用于管理该监控过程的工具。它包括网络分析器的使用，如Windows 2000网络监控工具以及Cisco的TrafficDirector。还包括高级仿真方法和工具，如COMNET预测器，同时仔细描述了你可以实施的不同测试类型，包括单一和双重分析器俘获。另外，它还演示了应用测试与“假定方案”的网络仿真，同时还演练了建立网络的一个拓扑图的过程。

第11章“IP地址与命名服务”——这一章讨论了命名服务，包括DNS和DDNS、NetBIOS NBT命名服务、WINS以及DHCP。文中把这些服务进行了综合，提供了一个全面的解决方案；同时还讨论了一些其他基本解决方案，如Cisco路由器转发广播以及一些容错策略。该章还包含了对命名服务的设计选项，以及对最新Windows 2000和Cisco网络登记管理 (CNR) DNS/DHCP工具的概要描述。

第12章“设计Windows 2000域”——这一章讨论了有关Windows 2000域设计规划的最新知识。其中的主题将为你构造Cisco/Windows网络中的绝大部分工作提供必要的帮助。它仔细描述了一些技术上的步骤，这些步骤都是建立新网络或者把现有网络移植为新的Windows 2000域模式，以及解决现实问题如客户移植和命名空间设计所需要的。在该章中提供的若干例子，适用于小型、中型以及企业级组织的网络设计。最后，还讨论了一些工具，如DirectManage、DirectAdmin、DirectScript以及FastLane的域管理套组 (DM/Suite)。

第四部分 内联网/外联网策略

在你已经具有了建立Cisco/微软网络的基础之后，你就可以开始研究特定的、更高级的连通性解决方案了。

第13章“Web服务”——这一章讨论了一些Cisco提供的基于Web的技术。详细地论述了Cisco的DistributedDirector、LocalDirector以及Web缓存引擎。该章还讨论了Cisco的Web浏览器界面，它允许Cisco IOS命令通过一个Web浏览器来执行。

第14章“安全连接”——这一章论述了Cisco和Windows的硬件和软件安全解决方案。其中详细论述了Cisco IOS访问控制列表、Cisco防火墙IOS以及Cisco PIX防火墙，包括路由器IOS、路由器防火墙IOS以及PIX防火墙上的网络地址转换 (NAT) 的处理。除此之外，Cisco的实时入侵探测系统、NetRanger (现在更名为CiscoSecure入侵探测系统) 也在该章中进行了详细的讨论。

第15章“保证服务质量”——这一章论述了服务质量 (QoS) 实现的过去、现在和未来。其中还包含了微软通过活动目录的LDAP的实现 (包括在Windows 2000中)，还讨论了目录驱动网络 (DEN)、IP QoS以及在Cisco IOS操作系统中的QoS命令。

第16章“认证、授权与计费”——这一章讨论了一些重要的机制，可以用它们来防止对你网络的非授权访问，也可以用来控制合法访问并详细地跟踪访问的是谁、访问什么、从什么地点、在什么时候等信息。该章定义了认证、授权与计费 (AAA) 背后的一些概念，并讨论了CiscoSecure访问控制服务器、NetSonar (现在更名为CiscoSecure扫描器)、TACACS+、RADIUS以及CryptoCard等等。

第五部分 附录

本书附录包含了一些参考，可以帮助你进行路由器配置，理解TCP/IP协议套组，以及获得Cisco和微软的技术认证，还为你提供了获取所需要所有帮助知识的方法和网络资源。

附录A“Cisco路由器基本配置”——该附录中包含了关于配置Cisco路由器的知识与技巧，其中有一个逐步进行简单路由器配置的例子。

附录B“TCP/IP协议集概述”——该附录对TCP/IP协议套组进行了很好的概要说明，并用图解对TCP/IP进行了描述，同时还描述了它是如何适用到网络中的，这些都非常有用。

附录C“认证之路”——本章对于所有微软和Cisco的认证都较为详细地进行了描述，并说明了如何获得资格认证，其中包括了：CCNA、CCDA、CCDP、CCIE、MCP、MCSE以及MCSE+I。

附录D“获取帮助：Cisco和Windows资源”——该附录讲述了一些寻求帮助的方法技巧，解释了到哪里可以找到以及如何使用微软在线帮助、命令行帮助、TechNet、在线支持数据包、咨询服务、Internet站点、新闻组以及Windows NT资源工具箱。其中还介绍了Cisco帮助资源，如Cisco在线连接（CCO）、CCO软件中心、技术帮助工具及Cisco文献光盘。

目 录

前言

第一部分 Windows与网络的接触

第1章 Cisco与Windows的结合	1
1.1 为什么是Cisco和Windows	1
1.1.1 Windows对Cisco的认同	2
1.1.2 Windows对网络的理解	2
1.1.3 Windows 2000的几个版本	3
1.2 Windows 2000的组成	4
1.2.1 NT 4.0的缺陷	4
1.2.2 关键概念	5
1.2.3 Windows 2000下的企业网	8
1.3 一些重要的新特性	9
1.4 Windows2000移植	12
1.5 小结	14
第2章 目录驱动网络	15
2.1 支持QoS的基于策略网络	15
2.2 DEN简史	16
2.2.1 作为法定标准的DEN	16
2.2.2 业内对DEN的认同	17
2.3 DEN规范	17
2.3.1 DEN的定义	18
2.3.2 DEN对网络互联目录采取的 开放式措施	19
2.3.3 LDAP:DEN上层结构机制	21
2.4 DEN信息模式	22
2.4.1 DEN类的继承	23
2.4.2 DEN对象间关系的描述	25
2.5 DEN分层结构	26
2.5.1 基于策略的网络	26
2.5.2 Policy类层次结构	28
2.6 DEN的实现	28

2.7 小结	30
第3章 网络基础	31
3.1 开放式系统互联七层模型	31
3.2 低层协议	32
3.2.1 局域网的拓扑结构	32
3.2.2 吞吐率期望值	36
3.3 高层协议	39
3.3.1 TCP/IP	39
3.3.2 IPX/SPX	40
3.3.3 NetBEUI	41
3.3.4 系统网络体系结构	41
3.3.5 SNMP和MIB	42
3.4 路由协议	42
3.4.1 距离矢量路由	42
3.4.2 链路状态路由选择	43
3.4.3 RIP	43
3.4.4 OSPF	45
3.4.5 Cisco的IGRP/EIGRP	47
3.5 广域网传输概要	48
3.5.1 ISDN	48
3.5.2 帧中继	48
3.5.3 ATM	49
3.5.4 HDLC	50
3.5.5 PPP	50
3.6 网络地址表	50
3.6.1 TCP/IP	50
3.6.2 IPX/SPX	54
3.7 小结	55

第二部分 用Windows 2000建造 Cisco 网络

第4章 Cisco 硬件和网络互联工具	57
---------------------------	----

4.1 Cisco硬件	57	4.8.3 Telnet	90
4.1.1 路由器	57	4.8.4 其他工具	90
4.1.2 交换机	63	4.9 设备管理	91
4.1.3 集线器	65	4.9.1 SNMP	91
4.1.4 语音	66	4.9.2 MIB	91
4.1.5 异步传输模式	66	4.9.3 远程监视器	92
4.2 网络安全与Internet产品	67	4.9.4 管理工具的类型	92
4.2.1 防火墙IOS	67	4.9.5 其他管理协议	92
4.2.2 PIX Firewall	67	4.10 小结	93
4.2.3 NetSonar	68	第5章 配置路由器和RRAS	94
4.2.4 NetRanger	68	5.1 路由器基本原理和安装	94
4.3 远程访问服务器	68	5.1.1 执行前的测试	94
4.3.1 Cisco AS5200/AS5300系列	68	5.1.2 配置前的清单	95
4.3.2 Cisco AS5800	68	5.1.3 安装路由器	95
4.3.3 AccessPath	68	5.1.4 管理访问	96
4.3.4 访问服务器总结	68	5.1.5 TFTP	99
4.4 Cisco IOS	69	5.2 ConfigMaker 2.4	101
4.4.1 IOS版本	69	5.2.1 ConfigMaker功能	102
4.4.2 IOS连通性	70	5.2.2 ConfigMaker支持的设备和	
4.4.3 IOS高级特征	71	协议	105
4.4.4 IOS管理特征	72	5.2.3 安装和配置ConfigMaker	109
4.4.5 IOS可靠性	72	5.3 使用ConfigMaker	109
4.5 电缆、连接设备与接口	72	5.3.1 描述网络设备	109
4.5.1 WAN接口	72	5.3.2 连接设备	109
4.5.2 LAN接口	74	5.3.3 安全性	111
4.5.3 控制台端口和辅助端口	76	5.3.4 从ConfigMaker交付配置	112
4.6 访问设备	79	5.3.5 配置SNMP参数	112
4.6.1 控制台访问	79	5.4 NetSys Baseliner	113
4.6.2 浏览器接口访问	80	5.4.1 产品综述	113
4.6.3 Telnet访问	80	5.4.2 安装NetSys Baseliner	114
4.7 命令行接口	81	5.5 NetSys Baseliner的使用	115
4.7.1 访问级别	81	5.5.1 配置NetSys Baseliner	115
4.7.2 有用的CLI命令	82	5.5.2 NetSys Baseliner视图	117
4.7.3 网络设备配置	86	5.6 Windows网络的IP网络互联	120
4.8 故障检修工具	89	5.6.1 为Windows网络建立IP	120
4.8.1 ping	89	5.6.2 管理路由表	123
4.8.2 traceroute	90	5.6.3 微软的RRAS	125

5.7 小结	129
第6章 安装交换机和VLAN	130
6.1 交换机	130
6.1.1 集线器、网桥和交换机	130
6.1.2 Catalyst 2900 XL系列	132
6.1.3 交换网络的轮廓	134
6.1.4 交换机的预先配置	136
6.2 交换机的设置和安装	138
6.2.1 Cisco IOS版本	138
6.2.2 安装程序/安装过程	139
6.2.3 当不能访问交换机时	141
6.3 专用交换机协议	141
6.3.1 生成树协议	141
6.3.2 Cisco组管理协议	142
6.3.3 Cisco 发现协议	142
6.4 用Cisco Visual Switch Manager来管理	143
6.4.1 CiscoVisual Switch Manager入门	143
6.4.2 使用CiscoVisual Switch Manager	144
6.5 交换机的配置指南	146
6.5.1 系统配置	146
6.5.2 安全性	151
6.6 用Cisco Switch Network View来管理	152
6.6.1 运行Cisco Switch Network View 之前	152
6.6.2 使用Cisco Switch Network View	152
6.7 虚拟LAN	153
6.7.1 VLAN的实现	154
6.7.2 VLAN的配置限制	154
6.7.3 VLAN端口成员关系模式	155
6.8 VLAN干线	156
6.8.1 VLAN内部路由协议	156
6.8.2 VLAN干线协议	158
6.9 VlanDirector	160
6.9.1 VlanDirector产品综述	160
6.9.2 安装VlanDirector	161
6.9.3 使用VlanDirector	162
6.10 小结	165

第7章 配置Cisco 集线器	167
7.1 集线器的说明	167
7.1.1 以太网集线器	167
7.1.2 Class I和II中继器	168
7.1.3 电缆距离	168
7.1.4 电缆规格	170
7.1.5 10BaseT 集线器	170
7.1.6 100BaseT 集线器	170
7.2 基本的集线器安装	171
7.2.1 FastHub 216T	171
7.2.2 安装和配置	173
7.3 把集线器综合到网络中	185
7.3.1 工作组	185
7.3.2 服务器室	186
7.4 小结	187

第三部分 管理一个Cisco/Windows网络

第8章 管理设备	189
8.1 新的管理套件：从字符串到图形 用户界面	189
8.1.1 理解管理套件	189
8.1.2 SNMP和MIB	190
8.2 HP OpenView	192
8.2.1 HP OpenView简介	194
8.2.2 安装和配置	194
8.2.3 使用HP OpenView	196
8.3 Cisco管理树	200
8.4 CiscoWorks	201
8.4.1 准备	201
8.4.2 应用组一览	201
8.4.3 安装CiscoWorks for Windows	203
8.4.4 CiscoView	203
8.4.5 配置生成器	207
8.4.6 使用配置向导	208
8.5 CiscoWorks2000	212
8.5.1 入门	212
8.5.2 Resource Manager Essentials	213

8.5.3 Resource Manager Essentials应用	215	10.5.3 带TrafficDirector启动	254
8.5.4 CiscoWorks Switched Internetwork	218	10.6 应用分析	254
8.6 NTManage	220	10.6.1 单分析器捕获的例子	255
8.6.1 安装和配置NTManage	220	10.6.2 双分析器捕获	257
8.6.2 监视对象	221	10.7 模拟和容量计划	259
8.7 小结	223	10.7.1 模拟你的网络	260
第9章 管理目录服务	224	10.7.2 准备模拟	260
9.1 微软管理控制台	224	10.7.3 两种模拟方法	262
9.1.1 在Windows NT上运行MMC	224	10.7.4 模拟样例	264
9.1.2 在Windows 2000上运行MMC	225	10.8 小结	266
9.1.3 snap-in设计	226	第11章 IP地址和命名服务	267
9.2 使用MMC进行网络管理	226	11.1 命名服务: DNS	267
9.2.1 活动目录任务	227	11.2 命名服务: NetBIOS	270
9.2.2 域复制	231	11.2.1 基于广播的网络	270
9.2.3 IP安全(IPSec)配置	234	11.2.2 工作组及其他	271
9.2.4 安全模板	236	11.3 命名服务: WINS	274
9.3 Windows 2000的新特性	239	11.3.1 名字注册、更新和删除	274
9.3.1 系统管理服务(SMS)2.0	239	11.3.2 节点类型	274
9.3.2 IntelliMirror	239	11.3.3 名字-地址查询	276
9.3.3 分布式文件系统	240	11.3.4 复制	277
9.4 小结	242	11.4 WINS / DHCP的集成DNS	278
第10章 网络通信测试	243	11.5 WINS体系结构	278
10.1 测试你的网络	243	11.6 DHCP 基础	281
10.1.1 测试的好处	243	11.7 集成命名服务	281
10.1.2 测试指令	244	11.7.1 Windows 2000的DNS	282
10.2 网络探测器与分析器的比较	245	11.7.2 动态DNS	283
10.2.1 网络分析器	246	11.8 网络注册管理器	284
10.2.2 网络探测器	247	11.8.1 使用带DDNS的CNR	285
10.3 网络测试标准	248	11.8.2 NCR的DHCP服务器	286
10.3.1 SNMP和MIB	249	11.9 小结	287
10.3.2 RMON	249	第12章 设计Windows 2000域	288
10.3.3 RMON-2	250	12.1 收集信息	288
10.3.4 RMON-3	250	12.1.1 决定商务需求	288
10.4 微软的网络监视器	250	12.1.2 明确约束	289
10.5 Cisco的TrafficDirector	252	12.1.3 了解已经存在的网络的特征	289
10.5.1 TrafficDirector Agent	252	12.2 从基础建立域	290
10.5.2 TrafficDirector的接口	253	12.2.1 计划移植到Windows 2000	291

12.2.2 命名空间设计	292
12.3 域结构的例子	294
12.3.1 小型商务	294
12.3.2 中等规模的商务(集中式的)	296
12.3.3 中等规模的商务(非集中式的)	297
12.3.4 企业商务	299
12.4 Windows 2000移植	301
12.4.1 Windows 9x客户问题	301
12.4.2 NT客户问题	302
12.5 域移植例子	302
12.5.1 减轻移植痛苦	303
12.5.2 转换你的第一个域	303
12.5.3 制作转移	304
12.5.4 单域安装	304
12.5.5 添加一个组织单元	306
12.5.6 到本机模式	308
12.6 第三方移植工具	308
12.6.1 DirectManage	308
12.6.2 FastLane的域管理套件	310
12.7 小结	312

第四部分 内联网/外联网策略

第13章 Web服务	313
13.1 Cisco分布式控制器	313
13.1.1 伸缩性问题的解决	313
13.1.2 Cisco对WWW伸缩性问题的 解决方案	314
13.1.3 分布式控制器的机理	314
13.1.4 分布式控制器度量	315
13.1.5 分布式控制器安全	320
13.1.6 分布式控制器模式	320
13.1.7 分布式控制器特性	322
13.1.8 分布式控制器应用	323
13.2 Cisco本地控制器	323
13.2.1 本地控制器是什么	323
13.2.2 本地控制器的优点	324
13.2.3 本地控制器支持的应用	326

13.3 分布式控制器与本地控制器 配置实例	326
13.3.1 分布式控制器配置实例	327
13.3.2 本地控制器配置实例	329
13.4 Cisco缓存引擎	330
13.4.1 Cisco网络缓存解决方案	331
13.4.2 Cisco缓存引擎如何工作	331
13.4.3 Cisco缓存引擎的其他替代品	332
13.4.4 Cisco缓存引擎系列	332
13.5 Cisco Web浏览器界面	333
13.5.1 配置Cisco Web浏览器界面	333
13.5.2 验证浏览器硬件及其软件	333
13.5.3 访问路由器主页	333
13.5.4 用Cisco Web浏览器界面 发布命令	334
13.6 小结	335
第14章 安全连接	337
14.1 Cisco路由器IOS安全技术	337
14.1.1 访问控制列表	337
14.1.2 网络地址转换	338
14.1.3 虚拟专用网络技术	339
14.1.4 事件登记	340
14.1.5 识别与认证	340
14.1.6 路由认证	341
14.1.7 网络层加密	341
14.1.8 Cisco网络数据加密	341
14.1.9 拒绝服务检测及其预防	346
14.1.10 推荐的安全配置	346
14.2 网络地址转换	347
14.2.1 NAT的可用性	349
14.2.2 NAT功能综述	349
14.2.3 什么时候需要配置NAT, 什么时候不要	350
14.2.4 NAT的配置	351
14.3 虚拟专用网络	352
14.3.1 点对点隧道协议	352
14.3.2 PPTP安装规划	352

14.3.3 PPTP服务器的安装与设置	354
14.3.4 PPTP客户的安装与设置	357
14.3.5 第二层隧道协议	359
14.4 Cisco防火墙IOS功能集	359
14.4.1 Cisco防火墙IOS附加安全措施	360
14.4.2 Cisco防火墙IOS的优点	362
14.4.3 目标市场与定位	362
14.4.4 Cisco防火墙IOS设置	363
14.5 Cisco的PIX防火墙	364
14.5.1 PIX防火墙硬件	364
14.5.2 PIX防火墙软件	366
14.5.3 目标市场及拥有成本	369
14.5.4 安装与设置	369
14.5.5 配置PIX防火墙	370
14.5.6 PIX防火墙高级设置	372
14.5.7 PIX防火墙管理器	373
14.6 CiscoSecure入侵探测系统	374
14.6.1 Sensor	375
14.6.2 Director	375
14.6.3 Post Office	376
14.7 小结	377
第15章 保证服务质量	378
15.1 一体化、多媒体及更多需求	378
15.1.1 QoS的定义	379
15.1.2 为什么仅仅带宽是不够的	379
15.1.3 QoS不是什么新东西	381
15.2 QoS基础	387
15.2.1 QoS的两种类型	387
15.2.2 流与连接	388
15.2.3 无态与有态QoS	389
15.2.4 TCP无法独立支持QoS	390
15.2.5 数据包控制与系统开销	393
15.2.6 QoS拓扑结构因素	394
15.3 Cisco的QoS指令	395
15.3.1 CiscoAssure	396
15.3.2 数据包分类	396
15.3.3 拥塞管理	399
15.3.4 拥塞避免	400
15.3.5 流量整形	400
15.3.6 流信令	404
15.4 未来技术：标志交换	405
15.5 小结	409
第16章 认证、授权与计费	410
16.1 Cisco的认证、授权与计费服务	410
16.2 认证	411
16.2.1 AAA认证方法	412
16.2.2 非AAA认证方法	415
16.3 授权	418
16.3.1 授权类型	418
16.3.2 授权方法	418
16.3.3 授权需求	418
16.4 计费	419
16.4.1 设置	419
16.4.2 计费类型	419
16.5 远程访问拨号上网用户服务	423
16.6 远程访问控制器访问控制系统	424
16.7 CiscoSecure访问控制服务器	425
16.7.1 设置CiscoSecure ACS	426
16.7.2 CryptoCard管理	431
16.7.3 网络访问服务器配置	433
16.8 NetSonar	434
16.8.1 配置NetSonar	434
16.8.2 话路配置	435
16.8.3 NetSonar的使用	437
16.9 小结	440
第五部分 附 录	
附录A Cisco路由器基本配置	441
附录B TCP/IP协议集概述	455
附录C 认证之路	464
附录D 获取帮助：Cisco和Windows资源	474

第五部分 附 录

附录A Cisco路由器基本配置441

附录B TCP/IP协议集概述455

附录C 认证之路464

附录D 获取帮助：Cisco和Windows资源474

第一部分 Windows与网络的接触

第1章 Cisco与Windows的结合

Cisco系统和微软公司近来都倍受公众注目。在各自的开发领域里，微软已经宣称视窗（Windows）系统将推出下一代产品Windows 2000，同时Cisco通过不断的收购也正在迅速地发展。两个公司都已经成为各自行业中的先驱，并在他们各自的竞争中始终处于领先地位。然而对于用户和企业来说，更关注的是比最近的产品发布与公司收购情况影响更大的其他一系列的问题。

过去多年时间里，Cisco和微软发展建立起了重要的相互关系，他们已经协定共同承担即将面临的挑战，使Cisco的产品和网际操作系统（IOS）与微软新的目录服务——活动目录（Active Directory，AD）服务——能够更加协调地共同运行；与此同时，微软也将与Cisco合作使Windows 2000可以更多地识别Cisco网络设备以及处理在某个企业网中可能存在的一些通常发生的情况。

网络中的每个用户都将会感受到这些发展所带来的影响。如果没有网络OS与桌面OS的联合，应用程序与Windows本身要想添加某些特性将是不可能的。第三方应用将被重新进行设计以便使用那些来自网络设备的信息，并直接与这些设备相互作用来改变其服务。在网络与Windows系统之间将建立新的“智能型”应用，其所需的新标准如目录驱动网络（DEN）则已经由Cisco与微软开始联合定义了。毫无疑问，这一协作关系将产生更多有用的东西，但是其中的大部分你想要去实现，就必须懂得Cisco IOS与Windows 2000是如何相互影响的。

该书对Cisco与Windows相互重叠结合的领域进行了论述。本章中，我们将看到这些重叠领域当前的状况，以及它们未来的发展方向，并介绍Windows 2000以及活动目录（AD），然后在以后的章节中再论述DEN概念和Cisco网络基础。

1.1 为什么是Cisco和Windows

1997年5月在拉斯维加斯，微软发表了一项申明，新闻稿题为“微软和Cisco合作建立目录服务标准”，开始的一段做了很好的概括：

微软公司和Cisco系统公司今天发表了一份意向书，Cisco将允许微软活动目录在网络基础结构的管理中使用，并提供更丰富的网络服务。作为该协定的一部分，Cisco和微软将共同开发对活动目录的扩展，结合对网络元素与服务的高级管理。依据该协定开发出来的产品对于网络管理员来说，将使得统一其网络基本结构并促进借助于Cisco IOS软件开发更加丰富的网络服务成为可能。与此同时，也将允许服务提供商简化其服务的传递，并为他们的客户提供若干新的服务。

把网络与桌面操作系统结合起来，这是在用户通信连接更丰富的情况下的自然趋势。信息共享，访问那些在企业通信网与Internet上的本地PC之外所存储的信息，这些将日益成为计算机的真正用处所在。促进这一方向发展的技术应该是容易接受的，但是这需要网络与桌面操作系统的支持——那么就看看Cisco和微软的吧。

Cisco是最受欢迎的网络硬件厂商，拥有大约80%的市场份额。Cisco系统可能没有最快的日吞吐量或者最新的千兆位技术，但是它们有可靠的性能。大型的商业环境和紧急任务环境（如Internet）都使用Cisco设备的原因就在于其可靠、一致相容，而且有一个知道如何配置和维护它的技术熟练的专家组为其提供技术支持。Cisco随着其稳定的增长以及不断地获取新东西，它已经拥有了一个坚实的立足点并提高了其长期生存的能力。Cisco的建立阶段正接近尾声——基于Cisco IOS的技术将是所有商家一个不错的选择。

对于桌面操作系统来说，微软从其开办之日起就已经是领头厂商。近来他们被美国司法部宣判为垄断也不为怪。虽然将被分割，但Windows技术却是无所不在的；而且它还在不断地进行改进（特别是推出9x版本），其普遍存在和推进的势头是不用置疑的。Windows将在很长一段时间内依然存在于我们周围，因此，很明显Windows和Cisco的合作是合理的。其结果不仅会为两个公司带来巨大的经济效益，同时许多小的公司如果能灵活地利用相关的机会同样能够获得巨大的经济效益。每个涉及其中的人，从单一的Internet短线贸易商到成千上万的公司都将受益。

Cisco/Windows的联合所提供的新特性承诺：要易于管理、提高安全性，同时提供史无前例的信息访问方式。就此而言，基于标准的基础结构的价值将是高于一切的。

1.1.1 Windows对Cisco的认同

Cisco除了将其设备和IOS结合到Windows 2000中以外，它早就已经开始努力使其与Windows更加友好。过去几乎所有的Cisco应用程序都被设计为在UNIX系统中运行，随后，这些应用程序（如CiscoSecure、NetSonar等等）就有了转向Windows NT的趋势，Cisco甚至已经开始编写（或求取）一些主要运行在Windows NT上的应用程序（如CiscoWorks2000）。与此同时，Cisco也经常发布一些针对UNIX系统的版本，对许多忠于UNIX可靠性的网络管理员继续提供支持。

Cisco不去疏远其他厂商是很明智的。他们经常发布基于Windows NT的产品并与之共同建立基于Web的工具，这样可以使其他系统的用户仍然可以对这些应用进行管理使用，只要它可以运行浏览器就行。Cisco与Windows有着共同的目的：与Novell互用，同时尽可能地与其他厂商建立贸易关系。

在Windows 2000的介绍中，Windows的注意力远远地扩展到32位Windows应用程序的建立之外。Windows 2000为大量的用户给出了强大的目录服务，为Cisco开辟了一类全新的商机。活动目录将对用户工作站和E-mail服务器依然有效，对Cisco网络设备如路由器、交换机和防火墙也一样有效。这些设备可以对该目录进行读取并写入信息。针对这一性能的应用程序的数量也有着巨大的潜力。

1.1.2 Windows对网络的理解

正如Cisco使其应用与Windows兼容一样，微软必须在活动目录中为Cisco开辟一些空间，它

不得不使Windows OS具有更多的网络意识,但这只是第一步。既然Cisco路由器、交换机以及其他设备将与AD相互交谈,那么微软就必须建立AD智能系统,使其能够知道设备在与之交谈什么,因此在AD中新的信息项是必须的,同时还需要建立一个方案有效地使用这些信息,为用户提供更好的服务与更全面的特性;另外,还必须提供一个可伸缩的、安全的环境,并能够通过开放标准与非微软支持的设备进行通信。对于微软来说,做出这些适应性调节应该是不可能的,他们可能找到限制在一定范围内的网络设备与AD通信所采用的方法。公司用户将不再乐于接受不可伸缩的OS、低安全性以及那些只能使用它们自身组件的应用程序。如果这些需求不能满足,那么用户可能只有寻找其他的网络解决方案了。

本章剩余的部分将分析微软以后的动作,从而保证未来他们的OS还会被用户选择使用。

1.1.3 Windows 2000的几个版本

回顾一下过去,Windows 2000原本的命名是Windows NT 5.0,这个名称可能与包括在其中的丰富特性不太恰当。从NT 4.0到5.0的跨度远比以前任何一次升级的更新都大。毫无疑问,微软最大的工程项目莫过于此;实际上,许多NT代码都被完全重新编写。对于整个OS进行如此大的动作,致使大多数用户要充分认识该版本中潜在的性能都不得不花大量时间。在该书中,我们将集中论述其中所涉及的有关一般网络与特定Cisco产品的一些新特性。注意所有在本书中讨论的Cisco应用都可以在Window NT 4.0上正常运行。在我们直接从Cisco硬件和软件控制使用活动目录之前,我们先来看看微软/Cisco开创的更具前瞻性的一些要素。

微软在1998年10月27日宣称,Windows NT的下一个版本(所谓的NT 5.0)将命名为Windows 2000。NT的重新命名是一个明显的市场转移措施——虽然在Windows 98之后,Windows 9x就将引退,但微软不能抛弃这些用户,而期望他们把注意力转移到NT上。许多用户都习惯把NT与高级、复杂而昂贵的工作站联系起来,而在他们的写字台上或家中却没有任何的商业活动需要NT;另一方面,9x产品系列虽然不是很昂贵,但是与NT比较起来却是比较糟糕的,其可靠性不强,又有较大的局限性,这些都归因于其对DOS的继承性。显然,Windows的未来不在于Windows 9.x。

为了使NT 5.0对9x用户来说感觉更亲切一些,调整其名称使其看来对普通的Windows用户会更熟悉一些,同时对于公司的以及单独的用户来说都期望使用基本类似的操作系统。为此,微软计划发布Windows 2000的四个版本,使公司和家庭用户都能根据自己的需求恰当地选择。但是,即使市场销量不同,这些不同的版本除了其中某一种或两种服务有所不同之外,几乎都是相同的。

让我们分别看看Windows 2000的这四种版本。

1. Windows 2000专业版

Windows 2000专业版是NT工作站的改版,该版本将对家庭和商业用户通用。专业版本是服务器版本的客户版,在标准、单处理器奔腾系统中运行。虽然与服务器非常类似,但在任何给定时间它可以连接的网络用户个数是受到限制的。专业版还是不能运行许多网络驱动的服务,如DNS、活动目录以及DHCP服务器。

2. Windows 2000服务器标准版

该版本是网络的主要部分。Windows 2000服务器标准版是一个文件和打印服务器，可以作为一个带活动目录的域控制器（DC）来运行。它支持所有BackOffice系列的应用，包括事务处理服务器、IIS、Exchange、SQL服务器等等。服务器标准版可以运行DNS、DHCP以及WINS服务。当然，该版本也包含了NT 4.0中NT服务器的特性，它支持四路对称多处理（SMP）以及4GB的物理存储器。

3. Windows 2000高级服务器

一般来说，高级服务器版本是Windows NT 4.0改进版——企业版本。企业版是随着微软群集业务的不断发展而产生的。它允许两个NT 4.0服务器一前一后协同操作，这样如果一个服务器失败，另一个服务器将负责处理剩余工作，而不会有丝毫的停顿。Windows 2000高级服务器设置更进一步地扩展了群集业务，它可以支持8GB的物理存储器和8路SMP。

4. Windows 2000数据处理中心

Windows 2000数据处理中心实际上与高级服务器版本相类似，另外还带有一些附加的可伸缩性能，它可以支持64GB物理存储器以及32路SMP。许多年以前，一个视窗操作系统利用如此高的CPU能力几乎是不可想象的，但是不久的将来，这些服务器组将共同用于高度集中的应用中（例如：科学建模、金融贸易以及用于大型站点Web群集），以及用于主机转移、小型机和基于UNIX的系统中。

1.2 Windows 2000的组成

Windows 2000的意义远不只是一个名称而已。如同前面所描述的，它是微软迄今为止最大的项目，包括了比过去都多得多的新代码。从活动目录到增强的安全性能，微软已经在这新型OS中填充了崭新的管理界面以及特性。本节开始将对在Windows 2000中所处理的Windows NT 4.0中的一些缺陷做一定描述，然后我们将介绍一些了解Windows 2000以及其新特性时所需的一些关键概念。

1.2.1 NT 4.0的缺陷

要较好地评估Windows 2000以及其先进之处，就值得回顾一下Windows NT 4.0所遇到的一些结构上的缺陷，这些缺陷大都集中在可伸缩性能的缺乏上。

Windows 2000中的许多改进都是针对于NT 4.0中对用户的限制与管理问题的。例如，在NT 4.0中，用户信息存储在注册表中的一个平面文件中，这限制了一个域中的用户总数最多可达约40,000，要添加到这么多的用户当然需要相当长的时间，但是，你会看到NT 4.0的其他可伸缩性能问题。

在中型或大型的NT网络中，管理员最关注的问题是有若干人都在负责域的管理工作。首先，一般情况下，在分散网络环境下，管理员在繁忙的网络中查看和操纵用户计费时，很少有应答的时间，在主域控制器（PDC）位于WAN链路另一端的网络中，情况也一样。在这种情况下或者当域包含大量的用户帐号和分组时，许多的管理工具将陷入困境并变得使用起来很不方便。同样在更大型的网络中，管理员不得不把某些任务委托给其他人。但是，由于NT 4.0使用一种全有或全无的安全策略，管理员要么具有某域上的所有权利，要么没有任何权利。因此，势必