Windows 2000 Server 技术培训和认证丛书

Microsoft Windows 2000 Server 网络管理

徐晓峰 主编
世纪传人研修中心 编著

Microsoft Windows 2000 Server

人民邮电出版社
www.pptph.com.cn

Windows 2000 Server 技术培训和认证丛书

Microsoft Windows 2000 Server 网络管理

徐晓峰　主编

世纪传人研修中心　编著

人民邮电出版社

图书在版编目(CIP)数据

Microsoft Windows 2000 Server 网络管理/徐晓峰主编. -北京:人民邮电出版社,2001.10
(Windows 2000 Server 技术培训和认证丛书)
ISBN 7-115-09634-1
Ⅰ.M... Ⅱ.徐... Ⅲ.服务器-操作系统(软件),WIndows 2000 Server
Ⅳ.TP316.86
中国版本图书馆 CIP 数据核字(2001)第 058659 号

Windows 2000 Server 技术培训和认证丛书

Microsoft Windows 2000 Server 网络管理

◆ 主　　编　徐晓峰
编　　著　世纪传人研修中心
责任编辑　李振广

◆ 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
读者热线:010-67129212　010-67129211(传真)
北京汉魂图文设计有限公司制作
北京顺义振华印刷厂印刷
新华书店总店北京发行所经销

◆ 开本:800×1000　1/16
印张:14
字数:326 千字　　2001 年 10 月第 1 版
印数:1-5 000 册　　2001 年 10 月北京第 1 次印刷

ISBN 7-115-09634-1/TP·2453

定价:22.00 元

内 容 提 要

Windows 2000 Server 是 Microsoft 公司最新的服务器操作系统平台，它提供了文件和打印服务、活动目录服务、路由和远程访问服务、IIS 服务和数字证书服务等功能强大的网络服务。同时 Windows 2000 Server 也是稳定可靠的操作系统平台，可在其基础上安装如 Exchange 2000、SQL Server 2000、Internet Security、Acceleration Server 2000 等 Microsoft 的 2000 系列服务器产品以及其他厂商的软件产品。

本书是 Windows 2000 Server 技术培训和认证丛书的第二本，系统介绍了建立和管理基于 Windows 2000 的网络环境所需要的技术和方法。Windows 2000 网络管理的主要内容包括对 Windows 2000 TCP/IP 网络连接的管理和对 Active Directory 活动目录的管理。

本书适合负责建立和管理 Windows 2000 网络环境的 IT 技术人员和网络管理人员学习使用，也可供对 Windows 2000 的基本使用已有一定基础的电脑爱好者阅读参考。

序　言

提起 Microsoft（微软）公司，不管对计算机了解还是不了解的人似乎都能说上一段。事实上也的确如此，作为世界 500 强之一，并且公司市值曾经排名世界第一的知名企业，尽管大家对它褒贬不一，但它仍然以其无可辩驳的优势成为软件业当之无愧的霸主。

Windows 2000 Server 是 Microsoft 公司最新的服务器操作系统平台。Windows 2000 Server 技术的掌握，以及 Windows 2000 MCSE 认证的获取，将为您的职业发展提供有利的帮助。

北京世纪传人研修中心暨清华微软认证高级技术培训中心(CTEC)一直从事微软高级技术教育在中国的普及与发展，是国内最早开设 Windows 2000 课程的培训机构。在对 Windows2000 Server 进行教授的过程中，通过自身的实践经验与体会，以及同学员的沟通与交流，我们发现现有的教材、辅导资料不能很好地适应大家学习的需要：一来，教材大多为英文，对很多有意愿学习的人来说，这本身就是一种障碍。而英文教材的中文翻译本存在很多知识理解上的偏差；二来，Windows 2000 Server 功能强大，需要掌握的知识点非常多，英文教材中的知识点是完全按照 Windows 2000 Server 的技术特性分类的，存在很强的技术跳跃性，不利于一般读者的学习。

本丛书《Microsoft Windows 2000 Server 网络基础》、《Microsoft Windows 2000 Server 网络管理》、《Microsoft Windows 2000 Server 网络高级应用》正是基于上述问题，通过循序渐进的规划，帮助您逐步掌握构建以 Windows 2000 Server 为核心的网络环境所需要的各方面的知识，是一套知识结构清晰，技术实际应用指导性很强的丛书。

本丛书由徐晓峰负责整体内容的规划和最后修改，胡明亮撰写了本书第 1、2、3、4 章、徐成思撰写了第 5、6 章，徐晓峰撰写了第 7、8 章，牟华撰写了第 9、10 章，李栋撰写了第 11 章，牟华和程文俊撰写了实验部分。

愿本丛书能够为您在对 Windows 2000 Server 技术的掌握上有所帮助。

北京世纪传人研修中心

（中心网址：http://www.atec.com.cn）

目　录

第 1 章　Windows 2000 TCP/IP

1.1　概述

随着 Internet 的不断发展，TCP/IP（TCP：Transmission Control Protocol，传输控制协议；IP：Internet Protocol，因特网协议）作为 Internet 的通用协议其应用也越来越广泛。在 Windows 2000 中提供了具有高性能的 32 位的 TCP/IP 应用，除了 Windows 家族产品中的 TCP/IP 所具备的功能外，又增加了一些新的功能或对原来的功能进行了一定的改进。安装 Windows 2000 系统的计算机可以通过 TCP/IP 协议和其他使用 Windows 系统或是任何支持 TCP/IP 协议系统的计算机连接，借助如文件传输（FTP）和远程登录（Telnet）等工具可以方便地实现网络的传输和管理等工作，由于 TCP/IP 协议的良好结构和性能，组成的网络具有易扩展、易管理和通用性强等特点。

本章将对 TCP/IP 的结构进行比较完整的介绍，包括 TCP/IP 协议组和相关的主要协议。本章还介绍 Windows 2000 TCP/IP 的特性，包括 NDIS 5.0 和其他新的特性。

关于 IP 地址的概念在《Windows 2000 Server 基础》一书中已经有了详细的介绍，所以在本章中不再涉及。

1.2　Windows 2000 TCP/IP 特性

Internet 最初是由美国高级研究计划署资助建立的一个用于军事和研究目的的网络 APPANET，诞生于 1969 年。开始的时候，使用的网络协议是 NCP（网络控制协议），后来改进为 TCP 和 IP 协议，从 NCP 协议到 TCP/IP 协议的转变是 ARPANET 演变为 Internet 的标志之一。TCP/IP 准确地说是一个协议组，包括了网络互联和服务的定义，以及网络的管理工具，最初的目的是为了让不同公司的设备可以互连在一起工作，所以良好的兼容性和广泛的支持从一开始就是 TCP/IP 协议突出的优点。

TCP/IP 协议的优点表现在以下几个方面：

- 良好的容错能力；

- 很好的故障恢复能力；
- 极佳的扩展性；
- 与硬件厂商和网络类型的无关性；
- 较小的数据开销。

考虑到 TCP/IP 的开发背景，作为军用的网络协议良好的容错能力是必不可少的。事实上，即使网络有一部分出现故障或崩溃，TCP/IP 仍可以保证其他部分可以正常工作，基于 TCP/IP 的网络如 Internet 都具有很强的生命力，极难被彻底破坏。由于 TCP/IP 网络这种相对独立的特性，使得排错和增加网络设备都很简单，基本上不会影响到网络的其他部分。另外，TCP/IP 并不是针对某一公司的产品和网络设备开发的，也不局限于特定的操作系统，它可以在不同的设备和不同的网络类型上都工作得很好，这对于一个大型的网络，比如 Internet，或是一个有多个公司提供设备的网络来说是很重要的。

由于 TCP/IP 有如上的优点，更重要的是它已经成为一个事实上的标准，被大部分公司和厂商所支持，TCP/IP 已成为 Internet 的基本协议，也是使用最广泛的网络协议。在 Windows 2000 中，TCP/IP 协议也是唯一默认安装的网络协议，取代了 Windows NT 4.0 中的 NetBEUI 协议和 NWLINK IPX/SPX。

在 Windows 2000 中，支持的主要 TCP/IP 特性有：

- 可以针对多种网络媒介绑定多块网卡；
- 支持逻辑上和物理上的 multihoming；
- 广域的 IP 寻址和路由；
- IGMP v2（Internet Group Management Protocol Version 2，网际分组管理协议第 2 版）支持 IP 的多目广播；
- 检测 IP 地址冲突；
- ICMP（Internet Control Message Protocol，网际消息协议）路由器检测；
- 可以设定多个默认网关；
- 自动检测网关是否可用；
- 在 TCP 传输时自动检测 PMTU（Automatic Path Maximum Transmission Unit）；
- IP 的安全性；
- QoS（服务质量）；
- TCP/IP over ATM services；
- VPN（虚拟专用网络）。

在 Windows 2000 中，支持增强的 TCP/IP 特性有：

- 增加默认窗口的大小；
- 改变 TCP 滑动窗口的大小；

- SACK（Selective Acknowledgments，选择性确认）；
- TCP 快速重传；
- 对 RTT(Round Trip Time，往返时间)的算法进行了改进。

Windows 2000 提供的主要服务有：

- DHCP 服务；
- WINS 服务；
- DNS 服务；
- 远程拨入服务（RAS）；
- 在 VPN 中使用的 PPTP（Point-to-Point Tunneling Protocol，点到点遂道协议）和 L2TP（Layer Two Tunneling Protocol，第二层遂道协议）；
- TCP/IP 网络打印；
- SNMP 协议；
- Winsock2 接口；
- IIS（Internet Information Services，Internet 信息服务）；
- TCP/IP 连接、管理和测试工具。

对于 DNS、WINS 和 DHCP 这三个服务，因为比较重要，也比较复杂，所以我们在后面单独列出章节来介绍，其他主要的协议和服务我们会在本章的后面几节讲述。

前面列举了 Windows 2000 所支持的主要 TCP/IP 特性和服务，在进一步介绍 TCP/IP 协议的工作过程和服务内容之前，我们先从整体上了解一下 Windows 2000 中 TCP/IP 协议的结构，如图 1.1 所示。

在图中列出的只是 Windows 2000 中主要的协议、服务和接口，并不是 TCP/IP For Windows 2000 的全部内容。

其中 TDI 和 NDIS 是两个公用的接口，Winsock 则是与用户应用程序的接口，包括了一组为 Windows 设计的扩展接口，大大方便了程序员开发 Windows 的网络应用程序。事实上，Windows 的很多网络工具都是基于 Winsock 的，如 Ping、FTP 和 Telnet 等。Windows 2000 支持的是 Winsock 的 2.2 版，一般又称为 Winsock2。

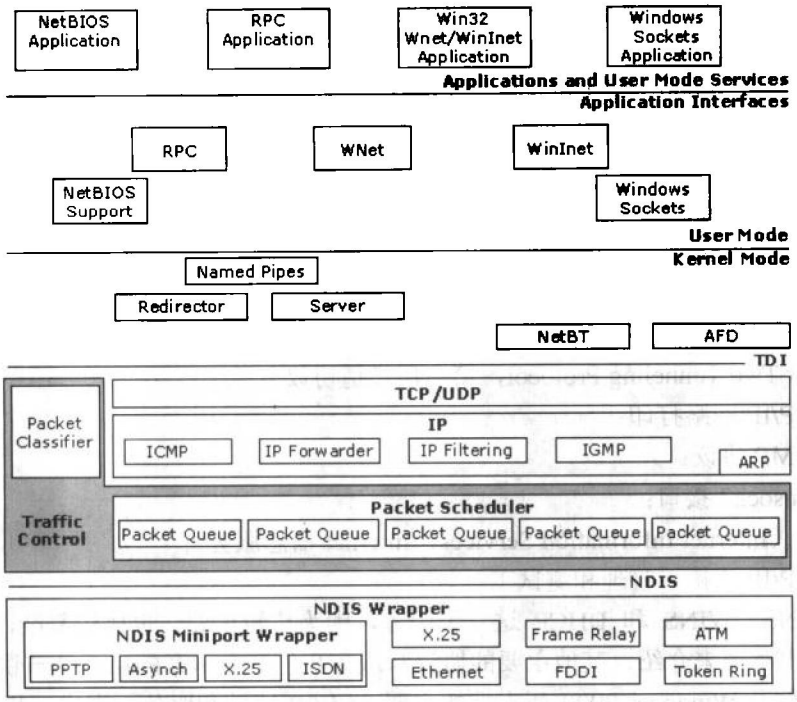

图 1.1 TCP/IP For Windows 2000 结构图

1.3 TCP/IP 协议组结构和主要协议

TCP/IP 协议并不是只有 TCP 和 IP 两个协议，而是由一组协议组成的，只是因为 TCP 和 IP 是其中最有名的两个协议，所以称为 TCP/IP 协议或 TCP/IP 协议组。对一个网络管理人员来说，除了需要了解 TCP/IP 协议的使用之外，还要能够对网络进行规划、优化配置和排错，因此需要更深入地了解 TCP/IP 协议的工作过程。

TCP/IP 协议组的结构如图 1.2 所示。TCP/IP 协议组分为四层，从上向下依次是应用层、传输层、Internet 层和网络接口层，这种分层模型又称为 DARPA 模型。如果将 DARPA 模型与 OSI（开放系统互联）参考模型进行比较可以看出，两个模型虽然层数不同，但在概念上是很相似的，如图 1.3 所示。TCP/IP 结构中的一层对应着 OSI 参考模型中的一层或几层，这可以让我们更容易地理解 TCP/IP 模型中各个层的作用，同时，对 TCP/IP 协议工作过程的分析可以方便地扩展到 OSI 参考模型中。在下文中如果没有特别说明，所使用的

分层都是按照 TCP/IP 协议的分层结构。

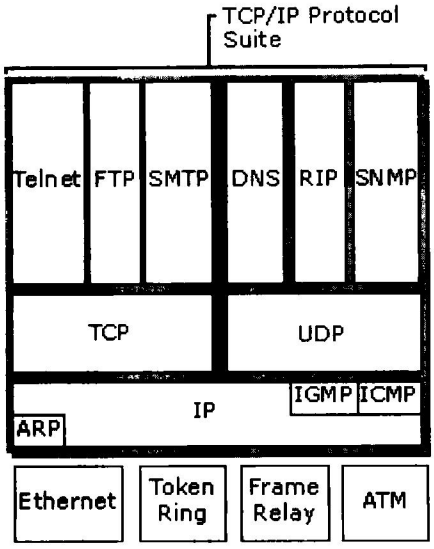

图 1.2 TCP/IP 协议结构

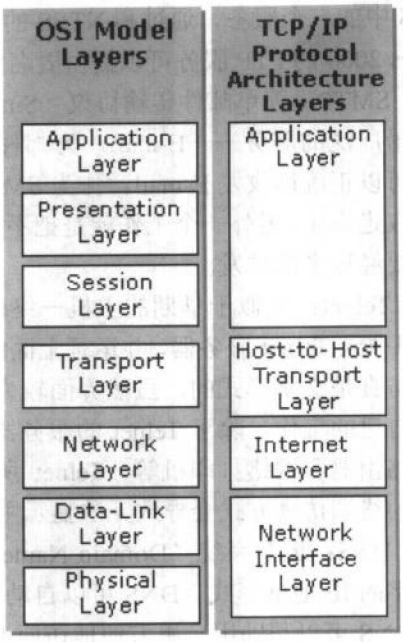

图 1.3 OSI 与 DARPA 的模型关系

1.3.1 应用层

应用层主要的工作是为应用程序提供与下层服务及其他应用程序的通信协议和接口规范。由于用户的要求是多种多样的，为了满足用户不同的需求，应用层包含了大量的各种各样的协议，是内容最为丰富的一层。下面介绍主要的应用层协议。

- HTTP：超文本传输协议（Hyper Text Transport Protocol），是 Internet 上数以亿计的 Web 网页的基础，它规定了 Web 页的传输和描述语言。
- FTP：文件传输协议（File Transfer Protocol），可以在两台主机之间传输文件，两台主机可以使用相同的系统，也可以是不同的系统。需要注意的是，FTP 可以指协议，也是一种服务，还可能是一个程序。使用 FTP 协议传输文件需要一台计算机提供 FTP 服务，提供 FTP 服务的计算机称为 FTP 服务器，其他的计算机作为客户访问。FTP 协议提供了一定的安全认证措施，一般用户需要登录才能使用 FTP 服务。在 Internet 上也有很多匿名

（anonymous）的 FTP 服务器允许匿名访问，一般提供的是一些共享和免费的软件。对 FTP 服务器来说，应该限定匿名用户的权限，以保证服务器的安全。Windows 2000 中 FTP 服务是 IIS 中的一个服务，通过和 NTFS 的权限相结合，提供了极为灵活而又严密的安全性。Windows 2000 的 FTP 服务可以提供匿名的 FTP 服务。

- SMTP：简单邮件传输协议（Simple Message Transfer Protocol），用于提供 Internet 上使用最广泛的服务——E-mail，为邮件的传输格式以及附件格式定义了一系列的标准，使用户可以正确地收发 E-mail。作为 SMTP 服务器，需要接收用户的邮件并暂时保存，直到用户取走为止，另外一个工作就是把不是自己管理的邮件转发出去，用户接收到的 E-mail 通常都要经过多次转发。

- Telnet：类似于早期的主机－终端模式，把客户机模拟成 Telnet 服务器的终端形式，可以登录 Telnet 服务器，并运行上面的程序，或完成执行命令、进行管理的功能。Telnet 的终端仿真是文字形式的，虽然界面较为简单，但是可以让用户几乎可以和在主机登录一样完成自己的工作。除了 Telnet 的服务器之外，一些网络设备也是通过 Telnet 方式来管理的，如路由器和网络打印机等。Telnet 所使用的命令一般与提供服务的系统有关，另外，不正确的终端仿真方式会导致无法显示主机的信息。

- DNS：域名系统（Domain Name System），可以把 Internet 上的便于记忆的名称转换为数字的 IP 地址形式。DNS 可以自动查询出文字地址对应的 IP 地址，把域名转化为 IP 地址。DNS 可以帮助用户更方便地访问 Internet。使用 DNS 的一个好处是可以很方便地找到并记住一些网站，比如美国微软公司的网址是 www.microsoft.com，IBM 公司的网址是 www.ibm.com。在 Windows 2000 中支持 DNS 的动态更新。

- WINS（Windows Internet Name Service）：Microsoft 特有的协议，用于把 NetBIOS 名解析成 IP 地址，功能与 DNS 有相似之处，其区别就是 DNS 协议提供的是域名或者说主机名与 IP 地址之间的解析，WINS 提供的是 NetBIOS 名与 IP 地址之间的解析。WINS 同样提供动态的 NetBIOS 名解析。

- DHCP：动态主机配置协议（Dynamic Host Configuration Protocol），也是 Microsoft 操作系统特有的协议，可以为某一网络中的计算机动态地分配 IP 地址并完成某些指定的配置，可以大大减少网络管理员的工作量，并避免了某些由于用户错误配置 TCP/IP 协议而造成的网络故障。在一个比较大的局域网中或是计算机移动较为频繁的情况下，比如经常有便携机加入网络时采用 DHCP 具有很大的优越性，另外，当计算机的数量多于可以使用的 IP 地址的数量的时候，使用 DHCP 可以提高 IP 地址的使用效率。

- SNMP：简单网络管理协议（Simple Network Management Protocol），可以检测网络运行的各种信息并提供网络的管理功能。通过在网络设备、服务器以及工作站上运行的 SNMP Agents，收集节点上所传输的数据包、流量以及设备或计算机的资源占用情况，汇

总这些信息可以了解整个网络的运行情况，为网络优化和排错提供依据。网络的管理员还可以通过设定 SNMP Agents 的阈值实现报警的功能。

1.3.2 传输层

传输层的工作与 OSI 参考模型的传输层功能类似，都是在端到端的数据传输中保证数据的正确、完整并且顺序正确，也就是提供了可靠的端到端的数据传输。在传输层的以下各层都是不考虑数据传输的可靠性的，从这个角度上来说，传输层保证的是包括它本身以及以下两层的传输可靠性。TCP/IP 协议的传输层协议最主要的是 TCP 协议和 UDP 协议。

- TCP：（Transmission Control Protocol，传输控制协议），主要功能是把应用层需要传递的信息分割成数据包，然后发送出去。在接收方则检验数据包是否正确，如果数据包正确则向发送方发送一个确认的消息，如果不正确则要求重发，另外还要把收到的数据包按照正确的顺序排列起来。为了保证数据可以同步发送和接收，TCP 协议在建立连接的时候采用了三次握手的方式，通信的双方商定数据包的大小和同步标志，然后才开始真正的传输，TCP 协议的传输过程实际上是一种数据流的传输。由于 TCP 协议花费了大量的开销用于建立连接和校验数据包等工作，因此，传输效率相对低一些。

像 TCP 协议这样，在发送数据前建立虚拟网络连接的协议，被称之为面向连接的协议。

- UDP：（User Datagram Protocol，用户数据报协议），UDP 协议同样是把应用层的信息分割成数据包并发送出去，但它与 TCP 不同的是，在接收方 UDP 协议只是校验收到数据包的正确性，并不保证数据包的排列顺序是正确的，也不保证可以接收到所有的数据包，所以，也不会发送收到数据包的确认信息。显然，UDP 不能保证数据传输的可靠性，但是它的一个明显的优点就是占用的网络资源少，并且传输速度较快。所以，当某些应用频繁且传递少量数据或对数据传输的可靠性要求不高时，可以使用 UDP 协议，比如传输 SNMP 服务的数据以及多媒体的视频或音频数据等。如果应用程序本身可以保证数据传输的可靠性，使用 UDP 也是一个好的选择。

像 UDP 协议这样，在传输数据之前不建立虚拟连接的协议，被称之为非面向连接的协议。

1.3.3 Internet 层

Internet 层的工作就是提供具体的数据传输路径，要达到这个目的，除了要为每台计算机规定一个可以识别的地址之外，还要从很多的可以使用的路径中找到最好或者较好的