Windows 2000 Server 技术培训和认证丛书

Microsoft Windows 2000 Server 网络高级应用

徐晓峰 主编
世纪传人研修中心 编著

人民邮电出版社
www.pptph.com.cn

Microsoft Windows 2000 Server

Windows 2000 Server 技术培训和认证丛书

Microsoft Windows 2000 Server 网络高级应用

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 网络高级应用/徐晓峰主编;世纪传人研修中心编著.
-北京:人民邮电出版社,2002.1
(Windows 2000 Server 技术培训和认证丛书)
ISBN 7-115-09904-9
Ⅰ.M... Ⅱ.①徐...②世... 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 084986 号

Windows 2000 Server 技术培训和认证丛书

Microsoft Windows 2000 Server 网络高级应用

◆ 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.ptpress.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:13.75
字数:275 千字　　2002 年 1 月第 1 版
印数:1-5 000 册　　2002 年 1 月北京第 1 次印刷
ISBN 7-115-09904-9/TP·2647

定价:21.00 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、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 Microsoft 的 2000 系列服务器产品，如 Exchange 2000、SQL Server 2000、Internet Security、Acceleration Server 2000 以及其他厂商的软件产品。

本书是 Windows 2000 Server 技术培训系列丛书的第三本，主要介绍了用 Windows 2000RRAS 实现用户的远程访问、VPN 和公司网络的远程互联，以及如何在分布式环境中配置 Active Directory，Windows 2000 的网络安全和数字证书的实现五个部分。

本书面向负责规划、建立和管理 Windows 2000 网络环境的 IT 技术人员和网络管理人员，要求读者对 TCP/IP 网络、Windows 2000 和 Active Directory 的知识都已经有了一定的基础。

序　言

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 Windows 2000 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，而曲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《Windows 2000 Server 网络基础》、《Windows 2000 Server 网络管理》、《Windows 2000 Server 网络高级应用》正是基于上述总是，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。

本系列丛书由徐晓峰负责整体内容的规划和最后修改，冯欣撰写了第 1 章到第 8 章，徐晓峰撰写了第 9 章到第 11 章，胡晓亮撰写了第 12 章，冯明亮撰写了第 13 章，周晓旭撰写了第 14 章，程文俊撰写了实验手册。各位作者为本书花费了大量的时间和心血，在此感谢各位作者的辛勤工作。

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　远程访问服务简介

1.1　概述

远程访问允许用户远程连接到公司的内部网络或是 Internet（因特网）。通过安装路由和远程访问服务（Routing and Remote Access Service，RRAS），Windows 2000 Server 为远程访问提供了强大的支持，配置远程访问的主要任务就是配置 RRAS，为远程访问客户创建适当的远程访问连接，并且在远程访问服务器上赋予用户适当的访问权限。

在安装并且配置了路由和远程访问服务后，还需要进行更多的工作。用户既可以为远程访问客户配置 IP 地址，使该客户可以使用 TCP/IP 协议访问公司的网络资源，也可以设置验证和加密的协议，从而增强远程访问连接的安全性。

路由和远程访问服务除了提供远程访问服务外，还提供了多协议 LAN（局域网）到 LAN、LAN 到 WAN（广域网）和网络地址转换（NAT）路由服务。关于路由和远程访问服务所提供的路由服务，将在本书以后的章节中进行介绍。

1.2　远程访问简介

通过 Windows 2000 的远程访问功能，远程访问客户可以连接到远程访问服务器上，并且透明地访问远程访问服务器，我们称之为点对点（Point-to-Point）的远程访问连接；远程访问客户还可以透明地访问与远程访问服务器相连的网络，我们称之为点对局域网（Point-to-LAN）的远程访问连接。所谓透明地访问，即远程访问客户可以从远程拨入访问网络上的资源，好像他们直接地连接在远程访问服务器上，或是直接地连接在公司的网络上。

Windows 2000 的远程访问提供了两种不同类型的远程访问连接。

◆　拨号远程访问

通过远程的拨号，一个远程访问客户可以使用现有的通信设备（如公共服务电话网（PSTN 等），创建到远程访问服务器上的端口的实际连接。一般的情况下，在远程访问客

户机和远程访问服务器两端，可以使用调制解调器或是 ISDN 适配器进行连接。

拨号远程访问允许在远方工作的用户拨入到单位的网络中，对公司的网络资源进行访问，但是如果远程拨入的客户较多，远程访问服务器一端就需要配置较多的拨号线路和适配器。例如，如果 10 个远程客户要通过公共服务电话网拨号到远程访问服务器上，服务器一端就需要准备至少 10 根不同号码的电话线和 10 台调制解调器，这会是一笔较大的开销。此外，如果远程访问客户需要长时间的连接远程访问服务器，长途电话的费用也会是非常昂贵的。

因此，当拨号远程访问的规模扩大时，可以使用虚拟专用网络（Virtual Private Network）的方式进行远程连接。

◆ 虚拟专用网络（Virtual Private Network，VPN）访问

虚拟专用网络使用 Internet（而不是通过拨号）来实现远程访问。一个 VPN 客户使用 Internet 创建一个虚拟的、点对点的连接。虽然 Internet 是公开的，但是 VPN 对传输的数据进行了加密，因此 VPN 对于远程访问客户是安全可行的。

虚拟专用网络是一种虚拟的点对点连接，远程访问服务器无需添加电话线和相应的适配器，因此，可以降低远程访问的成本。此外，在外地的用户可以先通过当地的 Internet 服务供应商与 Internet 相连，然后再连接到远程访问服务器上。这样，就可以节省长途电话的费用。可以看到，使用虚拟专用网络进行远程访问是一种经济、灵活的方法。

注释：

本章主要介绍使用拨号的方法进行远程连接，当然很多主题同样适用于虚拟专用网络。关于虚拟专用网络，本书将会在第 4 章中详细介绍。

1.3 拨号远程访问的组件

一个拨号的远程访问连接由远程访问客户、远程访问服务器、连接类型和数据传输协议构成，如图 1-1 所示。其中数据传输协议又包括远程访问协议和局域网协议。

1.3.1 远程访问客户（Remote Access Clients）

Windows 2000、Windows NT 3.5（以及以后的 NT 系统）、Windows 95、Windows 98、Windows for Workgroups、MS-DOS 和 Microsoft LAN Manager 都可以作为远程访问客户访问 Windows 2000 远程访问服务器。

此外，几乎所有的第三方的点对点协议（Point to Point Protocol）的远程访问客户都可

以访问 Windows 2000 远程访问服务器，其中包括 UNIX 系统和 Apple Macintosh 系统。

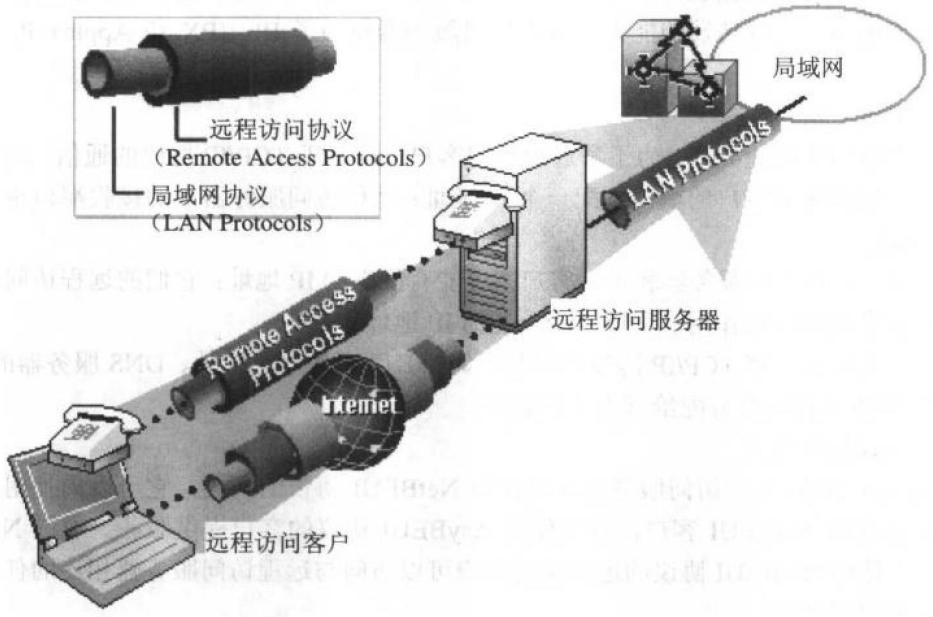

图 1-1　拨号远程访问示意图

1.3.2　远程访问服务器（Remote Access Server，RAS）

Windows 2000 远程访问服务器可以接受拨号客户的远程连接，Windows 2000 远程访问服务器还负责对建立好的远程连接进行管理。Windows 2000 远程访问服务器最重要的功能是在远程访问客户和服务器相连的网络之间转发数据包。

需要说明的是，这里所说的 Windows 2000 远程访问服务器是指运行路由和远程访问服务（RRAS）的 Windows 2000 服务器，并且服务器已经配置好，可以接受远程连接。

Windows 2000 远程访问服务器在远程连接中起着非常重要的作用，它可以为客户提供以下服务。

◆　验证

Windows 2000 远程服务器可以和 Windows 2000 远程访问客户相互协商决定使用何种验证协议，并使用该协议验证远程访问客户的身份。

◆　路由

当远程连接建立后，远程访问客户可以向远程访问服务器和与远程访问服务器相连的

网络发送局域网协议的数据包。当远程访问客户向远程网络发送局域网数据包时，远程访问服务器必须将这些数据包转发给它的接受者。要完成这一功能，远程访问服务器必须有可以根据路由协议进行转发的能力。远程访问服务器充当了 IP、IPX 和 AppleTalk 协议的路由器。

◆ IP 地址分配

当远程访问连接建立后，为了和远程访问客户进行基于 TCP/IP 协议的通信，远程访问服务器会向远程访问客户的端口分配一个 IP 地址；远程访问服务器上的接收端口也会接受一个 IP 地址。

请注意，远程访问服务器和远程客户都可能有静态的 IP 地址；它们的远程访问端口在通信中起到虚拟网卡的作用，可以接受分配的 IP 地址。

另外，其他的一些 TCP/IP 协议的参数，如 WINS 服务器的地址、DNS 服务器的地址、DNS 服务器的名称也会分配给远程访问客户。

◆ NetBIOS 网关

Windows 2000 远程访问服务器可以作为 NetBEUI 协议的网关，它可以向使用了 PPP 远程访问协议的 NetBEUI 客户，或是使用 AsyBEUI 协议的客户提供服务。通过 NetBIOS 网关，一个使用 NetBEUI 协议的远程访问客户可以访问与远程访问服务器相连的任何基于 NetBIOS 的网络资源。

1.3.3 连接类型（Connection Type）

在远程访问客户和远程访问服务器上安装好拨号设备，通过已有的通信体系，就可以实现拨号远程连接。采用何种设备和通信体系取决于用户选择的连接类型。

1. 公共交互电话网（PSTN）

公共交互电话网（PSTN），可以用来进行远程连接，如图 1-2 所示。当我们选用 PSTN 时，在远程访问客户机和远程访问服务器两端都需要安装调制解调器（Modem）。

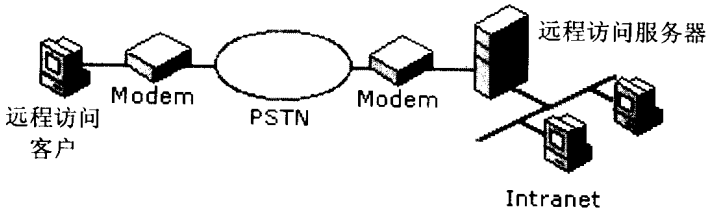

图 1-2 通过 PSTN 远程访问

由于电话网络已经非常普及，因此一般的情况下，用户都可以找到电话，从而进行远程拨号。此外，与其他的拨号方式相比，PSTN 的成本较为便宜。

但是使用 PSTN 也存在着一些缺陷：

◆ PSTN 并不是为数据传输进行设计的，因此 PSTN 的传输速度较低，另外传输的数据不够稳定；

◆ 由于 PSTN 对公众开放，因此在使用时，需要注意远程访问的安全性。

2. 综合服务数据网（ISDN）

综合服务数据网（ISDN）用于替代已有的 PSTN 网络的标准，它提供了一个数字化的网络，可以用于处理语音、数据和其他服务。ISDN 可以使用已有的 PSTN 线路。ISDN 提供了多个通道，每个通道有 64kbit/s 的带宽。例如通常使用的窄带 ISDN（N-ISDN），即有两个 64kbit/s 的信道。

使用 ISDN 进行远程拨号，需要在远程访问客户机和远程访问服务器两端安装 ISDN 适配器如图 1-3 所示。

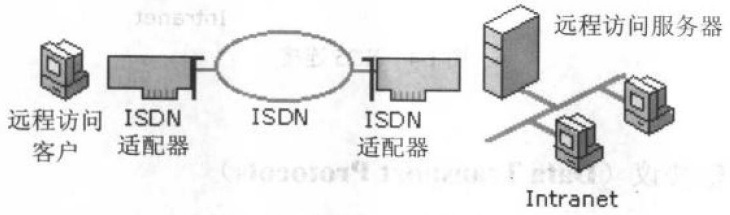

图 1-3　通过 ISDN 远程访问

ISDN 的传输率较高，另外由于是数字化的网络，数据的稳定性也比较好。但是，ISDN 适配器的价格比较高，使用费用也比 PSTN 的费用高很多。

3. X.25

X.25 网络使用包交换协议，可以绕过有噪音的电话线路传输数据。该协议依赖于具有包转送节点的包罗万象的广域网，这些节点可以参与将 X.25 数据包传递到指定的地址。X.25 网络连接如图 1-4 所示。

Windows 2000 远程访问通过两种方式支持 X.25:

◆ 远程访问客户支持使用 X.25 Smart Cards（智能卡），可以直接连接 X.25 数据网，使用 X.25 的协议建立连接，收发数据。远程访问客户也可以使用调制解调器拨入到 X.25 PAD，然后连接到 X.25 的网络。

◆ 远程访问服务器只支持使用 X.25 Smart Cards（智能卡）。

此外，还可以使用 DDN 专线、ATM 等连接方式，它们的数据传输速率都很高，但缺

点是使用的成本较高。

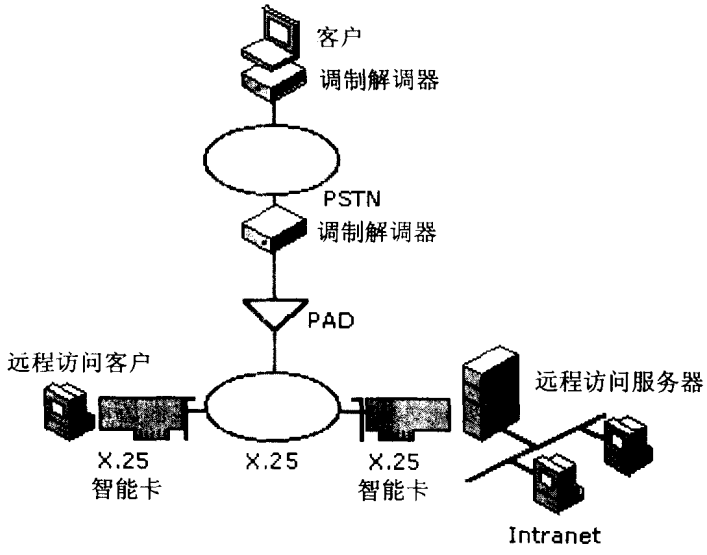

图 1-4　X.25 连接

1.3.4　数据传输协议（Data Transport Protocols）

Windows 2000 远程访问同时使用了远程访问协议和局域网协议，用于远程访问客户机和远程访问服务器之间建立连接，收发数据。远程访问协议用于在广域网（WAN）上传输数据，而局域网协议负责数据在局域网内部的传输。

Windows 2000 使用远程访问协议在远程访问客户机和远程访问服务器的拨号设备之间建立连接，在连接建立后，Windows 2000 使用局域网协议在两台计算机之间通信。当远程访问客户机和远程访问服务器通信时，路由和远程访问服务首先将数据封装在局域网协议中，使数据可以在局域网内传输；在局域网协议中封装好的数据包需要封装在远程访问协议中，使数据包可以在广域网上传输。这样，数据才会传送到远程访问服务器一端。

1. 远程访问协议（Remote Access Protocols）

Windows 2000 的远程访问可以支持以下几种远程访问协议。

（1）SLIP（Serial Line IP）

SLIP 是支持 TCP/IP 的远程访问协议，SLIP 通常和 Telnet 应用程序一起使用，SLIP 不适合大多数的现在的网络程序。

SLIP 存在着一些局限性：

◆ 只支持 PAP，密码明文传输；

◆ 只支持 TCP/IP；

◆ 由于 Windows 2000 的路由和远程访问协议不包括 SLIP Server 组件，因此，运行 SLIP 的 Windows 2000 不能作为远程访问服务器使用。

（2）PPP（Point to Point Protocols）

PPP 是 SLIP 的增强版本，它提供了较好的安全性，支持多种协议，并且有很好的互联性（Interoperability）。PPP 有以下一些优点：

◆ 支持多种验证协议，包括最新的 MS-CHAP V2；

◆ 可以传输几乎所有的主要局域网协议，包括 TCP/IP、IPX 协议、NetBEUI 协议和 AppleTalk 协议；

◆ 可以在拨号远程访问客户机一端使用，也可以在远程访问服务器一端使用；

◆ 运行 PPP 的 Windows 2000 客户机几乎可以连接所有的远程访问服务器。

由于 PPP 协议具有上述优点，因此成为最常用的远程访问协议。

有一种说法是：所有的优点都是 PPP 的，所有的缺点都是 SLIP 的。它概括地说明了 SLIP 和 PPP 的关系。

（3）Microsoft RAS（AsyBEUI）

该协议也被称为异步 NetBEUI 协议或是 AsyBEUI 协议，可以被运行着以前的微软操作系统的远程访问客户使用，例如 Window For Workgroups、MS-DOS 和 LAN Manger 等。

Windows 2000 远程访问服务器可以使用 Microsoft RAS 协议，远程服务器可以作为远程访问客户的 NetBEUI 网关，即允许客户使用各种局域网协议、访问服务器和与服务器相连的网络，其中包括 TCP/IP、NWLINK IPX/SPX 和 NetBEUI。

2．远程访问协议在 Windows 2000 中的使用

远程访问协议在 Windows 2000 中的使用如表 1-1 所示。

表 1-1　　远程访问协议的使用

远程访问协议	远程访问客户	远程访问服务器
PPP	允许	允许
SLIP	允许	
AsyBEUI	允许	允许

此外 Windows 2000 还支持 AppleTalk 远程访问协议（ARAP）。通过使用 AppleTalk 远

程访问协议，Apple Macintosh 的远程访问客户可以访问 Windows 2000 的远程访问服务器。由于 Windows 2000 路由和远程访问服务中不包括 ARAP 的客户端组件，因此，Windows 2000 作为远程访问客户无法连接只安装了 ARAP 的远程访问服务器。

3．局域网协议（LAN Protocols）

路由和远程访问服务支持如下的局域网协议：

- TCP/IP；
- NWLink；
- NetBEUI；
- AppleTalk。

由于路由和远程访问服务支持这些主要的局域网协议，它允许远程访问客户访问和远程访问服务器相连的各种网络，如 UNIX 网络、Netware 网络等。

例如，一个远程访问客户通过 NetBEUI 协议对远程访问服务器进行访问。建立连接后，远程访问服务器可以充当网关的角色，从而允许远程访问客户访问与远程访问服务器相连的 Novell 网络（使用 Nwlink IPX/SPX）或是 UNIX 网络（使用 TCP/IP 协议）。

注释：

远程访问中的远程访问协议和局域网协议的区别在于它们应用的范围不同。远程访问协议应用于广域网的范围，而局域网协议应用于局域网的范围内。

例如，中国北京的一箱西红柿要运送到美国纽约的市场上。首先，西红柿要用卡车运送到机场，再用飞机将这箱西红柿转送到纽约，在飞机到达纽约后，再用卡车将西红柿运往纽约的市场。可以看到，在北京和纽约市内，运输需要使用到卡车，而在北京和纽约之间的运输需要使用到飞机。可以对比卡车和飞机的区别理解远程访问协议和局域网协议的区别。

1.3.5 PPP 协议

PPP 协议是最常用的远程访问协议，它是进行远程访问的核心协议，它可以实现以下的功能。

- 提供多个协议在数据链路层的数据封装。

PPP 可以创建分别包含 IP 包、IPX 包或是 NetBEUI 包的数据帧。

- 建立、维护和结束逻辑链接（Logical Link）。

PPP 协议使用链接控制协议（Link Control Protocol，LCP）来建立 data-link 连接，并设置 data-link 连接的参数。部分的 LCP 协商可以用于验证远程客户的信任状（Credentials）。

- 提供协议参数设置。