Remote Access 24 seven

网络管理技术丛书

高效配置与管理 Remote Access

[美] Paul E. Robichaux 著

魏 伟 陈维军 腾 梅 译

每周7天，

每天24小时

保证网络全天候运转

使你成为

真正的网管专家

美迪亚

NETWORK SYSEX PRESS

電子工業出版社

Publishing House of Electronics Industry

URL:http://www.phei.com.cn

网络管理技术丛书

24 seven Remote Access

高效配置与管理

Remote Access

〔美〕 Paul E. Robichaux 著

魏 伟 陈维军 腾 梅 译

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 提 要

本书向读者介绍怎样设置、维护远程访问解决方案，以及怎样诊断和排除远程访问的故障。全书共分四个部分：第一部分论述远程访问的计划和部署，如协议、硬件、连接等；第二部分论述了怎样用Windows NT进行远程访问；第三部分介绍远程访问的客户机和服务器，如设置Linux PPP服务器/客户机、Windows RAS客户机等；第四部分介绍系统的优化、故障诊断以及灾难恢复。附录部分还介绍了一些远程访问设备的安装与配置。

本书是网络管理专业人员及广大爱好者的案头必备之书。

图书在版编目（CIP）数据

高效配置与管理Remote Access/（美）罗伯考克斯（Robichaux, P. E.）著；魏伟，陈维军，腾梅译. —北京：电子工业出版社，2000. 5

书名原文：Remote Access 24 Seven

ISBN 7-5053-5941-x

Ⅰ. 高… Ⅱ. ①罗… ②魏… ③陈… ④腾… Ⅲ. 远程网络—联接 Ⅳ. TP393.2

中国版本图书馆CIP数据核字（2000）第09946号

书　　名：**高效配置与管理Remote Access**

著 作 者：〔美〕**Paul E. Robichaux**

译　　者：魏伟　陈维军　腾梅

责任编辑：尤韬

印 刷 者：北京天竺颖华印刷厂

装 订 者：三河金马印装有限公司

出版发行：电子工业出版社　URL:http://www.phei.com.cn

北京市海淀区万寿路173信箱　邮编：100036　电话：68279077

北京市海淀区翠微东里甲2号　邮编：100036　电话：68207419

经　　销：各地新华书店

开　　本：787×1092　1/16　印张：17.5　字数：440千字

版　　次：2000年5月第1版　2000年5月第1次印刷

书　　号：ISBN 7-5053-5941-x / TP·3106

定　　价：29.00元

版权贸易合同登记号　图字：01-1999-3376

致　谢

当我告诉人们我写电脑书时，他们许多人认为我只是坐下来，看着我的打印机，等着它打印出已照排好的书页。实际写书过程比这个过程复杂了一点，依照付出总的劳动来说，我的写作只是冰山的一角——是编辑人员，美术设计人员，页面设计人员，索引编排人员以及其他无名英雄，根据我最初的稿件出版了精美的最后作品。

我很幸运能在这个项目上和一组能干博学的成员一起工作：Maureen Adams，我的采集编辑，他使得这个项目很快开始，在我适应Sybex的风格和工作流程时对我尤其耐心。与Maureen一道，Kristine O'Callaghan在协商期间帮助消除了障碍。Susan Berge，Sybex的项目编辑，扮演了交通警察的角色，她穿梭于五个州、三个时区，保证手稿、图形和版样按时、准确。Joshua Konkle作为技术编辑尽职尽责，指出了技术错误，并对怎样改进文稿提出了很好的建议。Walter J. Glenn为此书最后定稿时的技术编辑。最后，编辑Bonnie Bills，清除了偶然的排印错误或过长的句子，使文稿（对于读者和Sybex的生产系统）更加通顺。

本书还得益于两位有贡献的作者的知识和技能：Jim McBee（Exchange Server 5.5 24seven的作者）以及Charles Aulds，我的随叫随到的Linux老师。他们在设计、实现、诊断和支持远程访问网络的专长闪亮于整本书中。其它文稿中的错误都是我的，而不是他们的。

一些主题的专家也对本书做出了贡献。OmniPoint方面的Steve Holden，Live On The Net方面的Michael Lucking，HiWAAY Information Services方面的Mark Derrick和Elizabeth Solano，Newspaper Association of American的BrianBeisel都提供我在每一章用作个案研究的信息。另外，Marc Reich（一位持有证书的灾难恢复计划员）对灾难恢复一章作了全面检查。

一旦所有的写作、编辑、争论结束，出版人员就接手了。项目组长Teresa Trego，校对员Rich Ganis和Marney Carmichael，电子出版专家Adrian Woolhouse，以及插图编辑Tony Jonick与Jerry Williams。

还要感谢 StudioB Productions（我的写作代理机构）的训练有素的专门人员。David和Sherry Rogelberg处理了所有麻烦的琐事，让我可以集中写作一本大书。

我要感谢爱我、支持我的家人：我的妻子Arlene，我的儿子David和Thomas，他们对我不固定的工作时间、我们不时出现的FedEx和UPS驱动器故障以及调制解调器很大的噪音表示了耐心，我要感谢他们。我还要为我们家庭享受的所有幸福而感谢万能的上帝。

译 者 序

当今时代已进入网络时代。随着因特网越来越近的脚步，人们的生活不再局限于使用分离的计算机或局域网。我们更多地依赖于基于因特网的远程访问。作为普通读者，我们需要更多地了解一些远程访问的知识；作为网络的管理人员，更要掌握远程访问的技能。

本书向你介绍了怎样设置、维护现实世界的远程访问解决方案，以及怎样诊断和排除远程访问的故障。作者分四部分进行了详细的讲解。第一部分论述了远程访问的计划和部署，包括远程访问的类型、协议、硬件、连接以及对连接、服务、设备等的计划；第二部分论述了怎样用Windows NT进行远程访问，包括安装与配置远程访问服务，安装与配置路由和远程访问服务，保护NT环境，以及以NT设置VPN；第三部分介绍了远程访问客户机和服务器，包括设置Linux PPP服务器，设置Windows RAS客户机，配置Linux PPP客户机，Mac OS客户机和远程访问，以及NetWare客户机与远程访问；第四部分介绍了系统的优化、故障诊断以及灾难恢复。在附录部分作者还介绍了远程访问设备，如多调制解调器卡、集线器、专用VPN路由器等的安装与配置，并提供了一些远程访问的供应商。

本书由青岛的魏伟、陈维军、滕梅翻译，最后由魏伟和陈维军整理，由魏伟审校。

译者

1999.12.12

前　言

过去，坐在办公室的人们可以使用局域网，而不在办公室（在旅行，生病在家，或在其他什么地方）的人则不能使用——他们不得不等到回到办公大楼才可以利用共享的网络资源来进行工作。这种情况在许多方面是不优化的：那些不得不经常离开办公室的人与他们完成工作所需要的信息隔绝了，而且随着信息在网络服务器上的不断增加，不能访问它的劣势也在不断增加。

现在，远程网络访问已经变成现实。大大小小的公司都意识到了远程访问所提供的好处，对于管理者来说，能够实现可使用的、安全的远程访问解决方案变得越来越重要。本书将教给你一些为你的网络用户确定、计划、安装、维护以及检修远程访问解决方案所必须了解的知识。

本书及其开发过程

在创作这本书以及整个24seven系列丛书时，Sybex非常重视使其与管理者（也就是你）必须知道的知识相结合，如一天24小时，一周7天怎样设置、维护以及检修现实世界的远程访问解决方案。为了做到这一点，我询问了许多有经验的远程访问管理员，问他们：

- 你怎样计划你的远程访问部署？
- 你选择什么硬件和软件？他们令你满意吗？
- 你做对了什么？做错了什么？
- 你愿意与其他的远程访问管理员分享什么？
- 如果再次从零做起，你将回去改变什么？

我的目标是将这些信息进行集中编排，然后以一种任何技术水平的管理者都能理解和使用的方式提供给大家。

在本书每一章的最后，你将找到一个24seven的实例分析，他们介绍了现实世界里一些公司遇到过的通用的问题及其解决办法。一些组织同意列出其真名，也有一些组织的名字已经更改。

谁应该购买这本书？

如果你管理一个局域网，并负责给其增加远程访问的能力，或者负责维护一现有的远程访问的设置，这本书就是专为你写的。或者你也许只想扩展你的知识，知道怎么能够更好地为用户提供服务。

这本书的独特之处在于，在谈论到远程访问的时候，它并不试图讲授局域网的管理。如果你是一个较熟练的NT或者UNIX管理员，那么这本书正是为你写的。如果你还不到该层次，你仍然会发现规划和灾难恢复的资料是有用的，而且随着你水平的提高，其他的技术内容也会逐渐适用你。

这本书是如何组织的

我把这本书分成十四章，然后把这些章节组成四个部分。虽然在谈论相关组件时有章节间的交叉引用，但每一章都是独立的。可根据你的需要和兴趣，以任何顺序阅读这些章节；或者，你也可以从头到尾全部地线性处理。

第一部分　计划和部署

本书的前两章讲述如何根据需要规划远程访问解决方案。第1章介绍可能遇到的硬件、软件和通信协议。本章还讨论了实际通常使用的远程访问客户机和服务器。第2章对容量的规划和估计进行了全面的介绍，使读者了解将需要提供多少线路、端口或座位。

第二部分　用Windows NT进行远程访问

第二部分论及基于Windows NT的远程访问服务器的安装、配置和管理过程。第3章讨论了NT工作站与NT服务器所包含的远程访问服务（RAS）。第4章详细讨论了路由和远程访问服务（RRAS）（RAS的大哥）的安装、配置和管理过程。第5章讲授保护Windows NT远程访问配置的细节（但它并不讲授Windows NT的安全原理——那本身又是一本完整的书）。最后，第6章讨论了用Microsoft的PPTP通信协议建立一个虚拟专用网络（VPN）。

第三部分　远程访问客户机和服务器

第三部分教你怎样在其他操作系统（包括Linux、Windows 95/98以及Mac OS）上设置客户机和服务器。可以利用这些信息来设置最终用户的系统，或者教会他们怎样自己设置。第7章讨论设置Linux PPP服务器。第8章讨论Windows NT与Windows 95/98拨号网络客户。第9章显示配置Linux PPP客户机的细节。第10章则讲述怎样配置Mac OS客户机。这一部分以第11章结束，它解释了怎样在NetWare客户机上配置与使用远程访问。

第四部分　我的网络性能下降且不能恢复

网络故障——这是生活中逃避不了的事实。有时他们并非彻底出现故障，而只是性能降低。在任一情况中，作为负责的管理员，你很可能被请来进行修理，这部分的几个章节将在这方面帮助你。第12章讨论怎么优化远程访问设置，使你现有的设备发挥出最高的性能。第13章全面概述了怎样查找和排除远程访问的故障及其理由，包括对怎么发现与排除RAS、RRAS以及各种各样PPP服务器问题的详细讨论。我希望你认为第14章无用——它详细说明了灾难恢复计划的规划和实现，它将在万一发生自然或人为的灾难时，帮助确保网络可以利用。

附录

我不想在各章中加入硬件配置的细节，使其显得混乱，因此我把这些材料移到了附录中。前三个附录中每一个都陈述了一种不同种类的远程访问的安装、配置和管理过程：附录A讨论了多调制解调器板；附录B讨论了多端口串行卡；附录C讨论了Cisco 1720远程访问路由器。最后，附录D是与远程访问供应和管理有关厂商的一张列表（以及他们的URL）。

补充说明

Sybex没有在本书中附送一张CD-ROM，而是建立了一个与其相应的网站，我们将在本书的使用期间保持更新。这个网页可以在24seven系列网站：http://llwww.24sevenbooks.com上找到。关于其他Sybex的书的信息可在http://www.sybex.com上得到。

第一部分 计划和部署

讨论的主题：

- 远程访问的类型
- 远程访问的协议
- 远程访问的硬件
- 连接你的用户
- 规划通信连接
- 选择提供哪些服务
- 规划设备

第1章 远程访问的概念和协议

在开始规划和部署一个远程访问的解决方案之前，必须理解现存的远程访问的协议与工具。虽然某些类型的服务允许你小规模地开始，然后随着服务的发展而不断改变，而远程访问一般地涉及许多你、你的用户以及你的服务提供商之间的协调。如果在开始之前你就理解你在规划什么，情况会更好。

本章分成四个主要的小节。前三个小节讨论了具体的远程访问的概念，包括远程访问的类型、远程访问的协议和常用的远程访问的硬件。第四节“进行连接”，讨论了使一个远程用户连接到你的网络的实际机制。

远程访问类型

为了本书的目的，我把远程访问定义为通过客户机工作站建立的暂时连接，为客户机工作站（不管其位置）提供网络访问。换言之，我们讨论的是使一客户机临时连接到你的网络并通过它获得访问。远程访问是真正的网络连接，而且正确配置的远程访问连接功能应当完全等同于直接的局域网连接，唯一差别在于数据传输的速度的不同。

由于职员变得更加机动，他们用笔记本电脑、在家或在分公司的办公室工作，所以对公司计算资源的安全远程访问的需求不断增加。最近几年，基本的远程访问解决方案已经扩展，可以支持像安全的数据加密和可靠的远程用户身份验证等特点。这导致了实现这些特点的大量的竞争。

本质上有两种主要类型的远程访问：一种是远程用户直接拨号进入该组织网络，多数人通常用一台模拟调制解调器拨号进入。用户与公司的远程访问服务器直接连接的方案被称

为拨号式远程访问连接。

对于另一种类型的远程访问，用户与不在网络管理员的直接控制下的异地设备建立最初的连接。通常是用一台模拟调制解调器与用户的互联网络服务提供商（ISP）的拨号连接，但是该连接解决方案的范围在快速地扩展。一旦连接到ISP，远程用户就通过Internet与公司的网络建立网络连接，安全由加密保证。这种方案被称为虚拟专用网络（VPN），随着系统管理员意识到它们的潜在利益，它们的用处和重要性不断增加。

这本书我将详细地讨论这两个方案，侧重于保证连接的安全和可靠性的装备和软件协议。这本书主要的讨论集中在对公司的计算机资源的入站访问，但是也将讨论一些出站访问。

拨号式远程访问连接

远程访问中最常见的形式仍然是由客户机直接拨号连接公司的远程访问服务器。在这样的配置中，远程用户的网络访问点是远程网络上的拨号设备。此设备（一般为一台模拟调制解调器，但也可以是数字调制解调器）可以从远程计算机直接访问。远程用户通过公众交换电话网络（PSTN）进行呼叫来开始远程访问连接。产生连接一点儿也不复杂，人们使用他们已经近30年了，并且他们运行的很好。

与网络服务器的拨号式连接

在基于服务器的拨号式配置中，远程用户与直接连接到与LAN相连的服务器计算机的调制解调器建立连接（参见图1.1）。这台服务器电脑通常放置在局域网（LAN）上，以使该远程主机与那些直接连接到局域网的主机对于网络有同样的访问权。在最简单的形式中，这台服务器计算机所要做的只是在一个或多个调制解调器（或在内置卡上或连接在串行口上）上接收发来的呼叫，并运行远程访问服务器软件。因为大多数服务器操作系统（包括Windows NT、Mac OSX服务器、Linux和NetWare）都包含高质量的远程访问软件（这是特别吸引人的选项），从而以最少的额外费用提供第三方远程访问解决方案的许多好处。然而，在现有的服务器上增加远程访问也增加了它的负载，这可能不总是合乎需要的。

图1.1 远程用户通过网络服务器与局域网连接

与专用硬件的拨号式连接

在大多数情况下，专用的远程访问硬件是向远程用户提供网络访问的最容易、最有效的方法。专用的远程访问解决方案容易安装，配置和管理。因为他们是设计来提供单一服务，维护和检修这些设备就非常容易——他们要么工作，要么不工作。

专用硬件在当你需要扩展你能处理的远程用户的数目时，提供相当大的灵活性。然而，专用硬件解决方案比基于服务器的解决方案要昂贵的多，因为专用的远程访问设备自身就是独立的计算机。因此，这种解决方案通常仅仅在向相对大量的连接用户提供远程访问时才是值得的。

专用的远程访问设备用以下三种方式支持拨号线路：

- 使用内置的调制解调器
- 使用多个串行口外接调制解调器或者调制解调器群
- 使用支持通过多通道线路的大量模拟或者综合服务数字网络（ISDN）电话呼叫的集线器（常常叫做多路转换器或缩写为MUXES）

图1.2说明了远程访问集线器的使用，它提供许多内置的调制解调器，他们都可以从设备外部直接访问。本集线器的位置，在Internet防火墙之后，给远程访问客户机提供与直接连接相同的网络访问权。

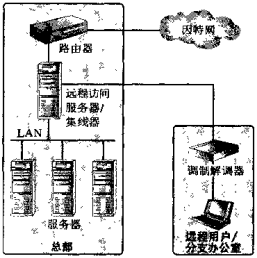

图1.2 远程用户通过专用硬件与局域网连接

虚拟专用网络

传统的远程访问解决方案是利用一束电话线（希望数目足够多，以使每一个用户需要访问时不会遇到占线），让你的用户通过标准的模拟调制解调器拨号进来访问。可是随着你支持线路的数目增多，将会非常昂贵，尤其是如果贵公司必须支付长途电话费来支持真正的远程用户时。Internet的发展使得几乎从世界的任何地方都可以通过本地电话访问任何上网的电脑，因此通过建造自己的VPN，你可以利用Internet来传送访问者和服务器之间的远程访问信息量，这样可以节省一大笔钱。

VPN在技术出版业引起了广泛的注意，但是对于到底什么是VPN很容易混淆不清。最初的定义（也是证明在技术上正确的一个定义）是在公共交换线路上运行的专用网络，这些

公共交换线路通常由电话服务提供商提供，综合使用信息包隧道、身份验证和数据加密协议。例如：如果你是赫兹，你的专用网络通信是通过ARINC的X.25网络传送的，它就是一个VPN。然而，这个术语现在更普遍用于描述通过Internet或某个提供商所管理的网络传送信息量的远程访问连接，这是我们在本书要讨论的一种VPN。因为Internet在安全方面的措施不多，VPN解决方案通常使用功能更强的用户身份验证和数据加密；不同的VPN标准（确实有不同标准）通常使用不同的协议来提供这些能力。

VPN主要可分为三类：

- 基于路由器或防火墙的VPN
- 独立的VPN设备
- 基于网络服务器的VPN

路由器或防火墙VPN

增加VPN服务的逻辑位置是在控制网络访问的设备上。路由器或防火墙控制访问并处理入站和出站的通信，因此大多数的路由器和防火墙供应商在他们的产品上增加了VPN功能。如Cisco 1720访问路由器，它专门设计用于向分支办公室和远程用户提供加强的VPN支持（关于Cisco 1720的更详细的资料请参考附录C）。加强的VPN支持也是Check Point软件技术公司基于软件的FireWall-1防火墙的一项主要功能。在大多数情况下，在现有的路由器或防火墙上增加VPN能力就像安装软件的升级一样简单。因为性能原因，你可能想另外增加硬件，这些硬件经常是用来执行大量占用CPU的数据加密任务。

除了对你现有的硬件是个小的升级之外，在路由器或防火墙上配置VPN服务的另一个优点在于这些设备已经具有对Internet或内部网络的访问，没有必要重新配置你现有的设置或者安装另外的WAN（广域网）连接。

当考虑一个有软件运行在现有的路由器或防火墙之上的VPN解决方案时，要认真考虑其对设备性能的影响。VPN软件需要大量的CPU时间，不应该安装在已经超负载的设备上。

图1.3说明了一个典型的路由器-防火墙VPN的配置。

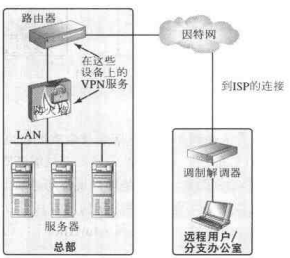

图1.3 典型的路由器—防火墙VPN

独立的VPN设备

正如拨号远程访问服务器一样，VPN也有专用的独立设备。这些装置一般比路由器-防火墙组合提供更高的性能。高端VPN器件能被扩展支持数千个同时的VPN连接，它使用大量的数字信号处理器（DSP）来执行大量占用CPU的数据加密和隧道等任务。专用的VPN设备通常在必须支持大量的高带宽连接时使用，他们通常销售给大中型等公司。

从图1.4可发现当用专用VPN设备时，VPN通信忽略常规的防火墙对未经授权网络访问的保护。

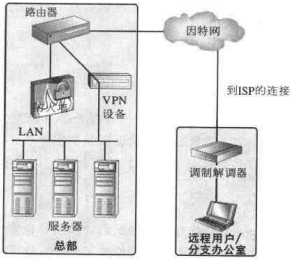

图1.4 专用的VPN设备

基于网络服务器的VPN

最便宜且最易于实现VPN的方法就是在现有的网络服务器上以软件方式运行VPN（参见图1.5）。这常常称为基于软件的VPN，但为了便于区分这类VPN和运行在路由器或防火墙上的相似的软件，在本书中它将被称为基于服务器的VPN。

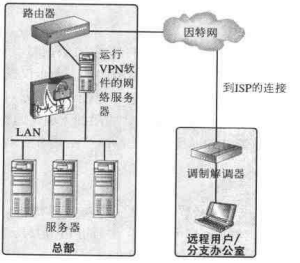

图1.5 基于网络服务器（或基于软件的）VPN

虽然许多独立的厂商提供仅用软件的VPN解决方案，但是大多数的操作系统供应商现在都在操作系统中捆绑VPN软件（服务器和客户机软件）。这实际上不仅仅是一种免费实现VPN的方法，而且它与操作系统的网络和用户身份验证机制的紧密集成使VPN的安装和配置过程变得非常容易。

这类VPN服务的缺点是它大大增加了服务器的系统开销。因此，基于服务器的VPN最好只于VPN连接不频繁或数目很少的情况下。与操作系统捆绑的VPN的另一个缺点是它们通常只执行供应商所选择的协议，并且可能不会充分地支持竞争者产品的客户机连接。如果你想启动一个试验用的VPN实现，而且如果你正在运行基本同系的一套服务器和客户机，这就是最好和最便宜的尝试方法了。

远程访问协议

所有的远程访问服务都依赖于允许客户机和服务器通信的一套核心协议。一些协议提供可选的服务，包括隧道、功能强大的用户验证以及加密。在为网络指定或实现远程访问解决方案以前，你需要理解存在什么协议，他们能做什么，以及哪个最适合你的需要。

访问协议

访问协议（Access protocols）是允许一台远程计算机好像实际连接到一个远程网络一样工作的通信协议。实质上，这些协议把LAN功能扩展到没有使用LAN连接的远程客户机。访问协议对于连接两端的计算机是透明的，它让拨号的主机看起来像在本地连接到公司的网络。

当你为用户设置远程访问时，你的目标可能是向远程用户提供对网络资源的访问，这种访问与他们实际连到LAN时水平一致。远程用户期望能浏览网络，发现和使用像打印机、文件夹、以及文档这样的共享项目，并且使用像数据库引擎和Web服务器这样的网络服务。用户唯一可察觉的差别在于远程访问连接所花的时间要更长些，因为它比LAN连接提供的带宽要窄。

串行线路接口协议

串行线路接口协议（SLIP）是仍在使用的最老的远程访问协议之一。SLIP最初开发用于通过拨号连接UNIX计算机，它的功能是极其有限的。由于仅仅用作高效地对Internet协议（IP）信息包在串行线路上进行组帧，SLIP缺乏对其它网络协议，以及错误修正、用户验证、数据加密和数据压缩的支持。尽管这些局限性严重限制了现代远程访问配置中SLIP的使用，但没有过高的系统开销意味着SLIP通常比它的后继产品具有更高的数据通过量。

点对点的协议

点对点的协议（PPP）被设计来解决SLIP的限制。PPP提供一种复合网络协议的方法，允许不同协议类型同时传输。例如，你可以使用单一的PPP连接传输IPX、AppleTalk以及TCP/IP信息包。PPP也提供SLIP缺少的3个关键的功能：

- 它包含错误探测和数据流控制的内置机制。
- 它为服务器提供一个动态地暂时把一个网络地址分配给进行连接的远程工作站的方法。

• 可选的验证协议能与PPP一同使用来提供对连接用户的身份的高度可靠的验证。

PPP的性能比SLIP的性能稍微慢些，然而，它是目前使用的最主要的远程访问协议，而且所有主要的OS供应商把PPP客户机和服务器作为他们产品的一部分进行发布。

用户验证协议

在联网技术中，验证意味着证实一个连接的用户的身份并且基于这个身份为其授权或拒绝对资源的访问。验证方案基本上分为下列3种类型：

你知道某事的方案是以你对一个口令知道而其它人不知道为基础的。这无疑是用于远程访问的最常用的验证方法。

你拥有某物的方案是以你对智能卡或安全标记这样设备的所有权为基础的。这些设备通常要求一个个人身份号码或口令；否则，偷你标志的某个人可以伪装成你。

你是某个事物的方案取决于能识别一个人的唯一身体特征，如他们的指纹或眼睛视网膜的血管式样。这个生物测定数据对一个特定的人是唯一的并且难以伪造，但是生物测定系统很少用于远程访问，因此我不会进一步讨论他们。

口令验证协议

口令验证协议（Password Authentication Protocol，PAP）为用户提供一个很简单的方法来提交一个口令由远程访问的服务器来验证。对于PAP，口令是以明码交换的——即客户机没有加密地把它的口令发送给服务器，因此一个窃听者能够不费力地获得口令。由于这个原因，只有当完全没有其它的安全验证协议时，才可以使用PAP。一定要知道，在Windows NT的远程访问服务（RAS）中，只要“允许任何包括明文的验证”（Allow any authentication including clear text）的复选框被标记，就允许使用PAP。根据默认值，在大多数基于UNIX的远程访问服务中PAP也被启用。

挑战信号交换验证协议

挑战信号交换验证协议（Challenge-Handshake Authentication Protocol，CHAP）经常被叫作PPP验证协议，因为它是用于确认一个PPP客户机身份的最普通的验证方法。CHAP保证所有由客户机工作站发送到验证服务器的验证信息都加密过。在验证的“挑战”阶段，服务器发送挑战值给客户机；客户机使用单向的功能以用户的口令来加密挑战值。因为服务者知道挑战值和口令，它能核对客户机是否输入正确口令。服务器随机改变挑战密码，因此它仅仅在很短的时期内有效，使对于任何一次的攻击的暴露时间减到最少。CHAP不使用公钥加密，而是依靠一个共享的密钥。

MS-CHAP

Microsoft CHAP（或MS-CHAP）是去除了服务器需要保留口令的明文版本的一个CHAP的变体。MS-CHAP使用RSA信息摘要4（MD4）算法来计算口令和挑战钥匙的散列版本。这个修正允许Windows NT域控制器使用储存的用于远程访问验证的加密的口令。MS-CHAP被认为相当安全，而且它是Windows NT 4支持的最安全的用户验证方法。

说明：服务包3为用于PPP的MD5-CHAP验证器提供有限的支持。安装这个支持的细节在第3章讨论。

Kerberos

Kerberos（读作“KER-ber-ohs”）最初在麻省理工学院作为一个研究项目进行了开发，它有较长的历史，主要用于UNIX。微软决定修补Windows 2000的安全系统，并使它基于Kerberos 5，这给了这个验证方案很大的鼓舞。

Kerberos是票据授权机制，其中用户只有能够提供一个由Kerberos服务器签发的有效“票据”，才被授权访问一个系统或网络资源。这些票据是基于时间的，不更新将会过期。Kerberos服务器处理所有的用户验证、票据的授权、过期和更新等功能。

Kerberos通常是在你登录到你的主服务器以后，用于控制对其它的网络资源的访问，不一定用于初始登录。因为Windows 2000将把Kerberos集成于它的安全模型，很可能微软的市场存在将帮助它从目前相对较小的用户基数扩展出去。这很可能会导致它的使用的增加到对网络资源的访问要求受控访问的任何地方会更多地使用Kerberos。

RADIUS

RADIUS是远程验证拨入用户服务的缩略词（Remote Authentication Dial-In User Service，RADIUS），它为用户验证和确认定义了标准（RADIUS的核心协议由RFC2138所制定，RADIUS记帐由RFC 2139制定）。RADIUS协议围绕一个客户机/服务器模型设计，在此单单一个RADIUS服务器就能为许多其它的系统或服务器提供用户验证。作为RADIUS客户机的远程访问服务器不执行用户验证，而是从网络上其它地方的RADIUS服务器请求这项服务。RADIUS服务器与远程用户使用加密的信息交换来安全地验证用户并通知远程访问服务器是否接受或拒绝连接尝试。

大多数远程访问服务器的主要供应商在他们的产品包含RADIUS客户机支持。当你与一个Internet服务供应商联接时，很可能对你进行验证的不是你所拨号进入的远程访问设备，而是一个有所有有效ISP帐号数据库的RADIUS服务器进行的。把远程访问的控制集中于一个单个的RADIUS服务器大大减少了总体费用，因此越来越多的站点在使用它。

说明： 在第5章中更详细地讨论了RADIUS在NT 4.0中的实现。

TACACS+

TACACS（Terminal Access Controller Access Control System，终端访问控制器访问控制系统的缩略词），像RADIUS一样，是允许网络访问设备使用分离的验证服务器的一个协议。TACACS，最初由Cisco在它的远程访问产品中提供，已经存在很长时间了。TACACS的最初版本（在RFC 1492中记录，日期为1993年7月）大部分已经被叫做TACACS+的增强版本代替了。TACACS+改进了最初的TACACS版本，增加了加密的验证（口令交换）并且分开了验证、授权及记帐的功能——这每一项功能都由其他软件执行。功能的分离也使TACACS不同于RADIUS。在RADIUS中，用户验证通过返回确定用户访问特权的一套属性值来确认，有效地巩固了用户验证和授权的步骤。

许多远程访问服务器的供应商都提供对TACACS+的支持。此协议已经成熟，并且作为IETF的草案标准公布（http://search.ietf.org/internet-drafts/draft-grant-tacacs-02.txt）。著名的基于Windows NT平台的TACACS+服务器有NTTacPlus，由意大利的Master Soft S.n.c of Novara提供（http://msoft.it）。

基于证书的访问控制

国际电信联盟（ITU）出版一系列的标准，统称为X.500系列。X.509标准规定数字证书的格式和结构。如果你曾经使用过一个安全的网页，那么就已经看到了X.509证书在起作用，因为安全网络界面层（Secure Socket Layer，SSL）依靠客户机和服务器的证书来提供它的安全。X.509证书也能用来验证远程访问用户，但它所要求的基础结构不属于本书的讨论范围。

一次性的口令

基于口令的系统有一个主要的弱点：如果口令再次使用的话，那么有人很可能窃取它，并且在你不知道的情况下使用。解决这个问题的一种方法是设计一个每次要求不同口令的验证系统。这些系统叫一次性口令或OTP的系统，它要求用户每次登录时提供一个新口令来验证。

S/Key 由Bellcore设计并提交公共域的一个一次性口令系统。S/Key通过确保在任何时候都没有用户的口令穿过网络而阻止窃听攻击。相反，只使用一次的RSA MD4散列数据由用户的唯一口令形成，并从S/Key验证服务器传递出一个种子。通过算法的多重关口产生一系列的口令，每个仅仅使用一次。在服务器方面，同样序列的口令被产生并存储。当接收到一次性口令时，它根据上一次使用的口令核对来确保它是以正确的顺序接收到的。服务器利用用户的秘密口令产生一次性的口令列表，但是它从不在那个系统存储。S/Key广泛用于UNIX系统，一些供应商也提供用于Windows NT的版本。

SecurID 由Security Dynamics生产的SecurID系统已成为硬件OTP系统事实上的标准。系统使用叫做标志的一台小型手持设备；标志是产生一次性随机生成标志代码的一台很小的计算机。为了验证你自己，你要向试图登录的机器提供你的标志代码，用户名和口令。标志代码在固定的时间间隔生成，并且他们仅仅在其时间间隔期间好用。

这个方案要求用户不仅拥有物理的标志，而且拥有一个有效的用户ID和个人身份号码的组合。这个要求使得SecurID成为一个双因素验证系统，因为它既包含你有的一些东西也包含你知道的一些东西。这确保了验证中的高信任度，但是与常规单因素系统相比它有点不方便。SecurID相对来说是昂贵的，因此，它通常用于网络或系统访问安全极其重要的地方，如在银行和自宫。Secutiy Dynamics销售运行于Windows NT以及几种UNIX版本的SecurID客户机和服务器。

隧道协议

隧道协议（Tunneling protocols）把一个网络协议（有效载荷）与另一个协议（运载工具）捆绑或封装成一体。例如，AppleTalk或IPX信息包能被封装于TCP/IP PPP隧道内。隧道用来在主机之间建立安全的网络连接，他们通常通过不安全的的公共网络，如Internet。有效负载协议是信息包被封装的协议；运载工具协议是用于来回运载封装的信息包的协议。

隧道协议是VPNs的一个基本的要素——VPN信息包作为有效载荷在一个标准TCP/IP连接中传输，使VPN协议对于路由和交换封装信息包的网络设备来说是看不见的。当建立一个VPN连接时，在任一个终端上的设备设定并为所有随后的VPN信息包建立一条隧道，除在这些终点外，VPN好像不存在。这就是为什么它被称为一个“虚拟”网络。