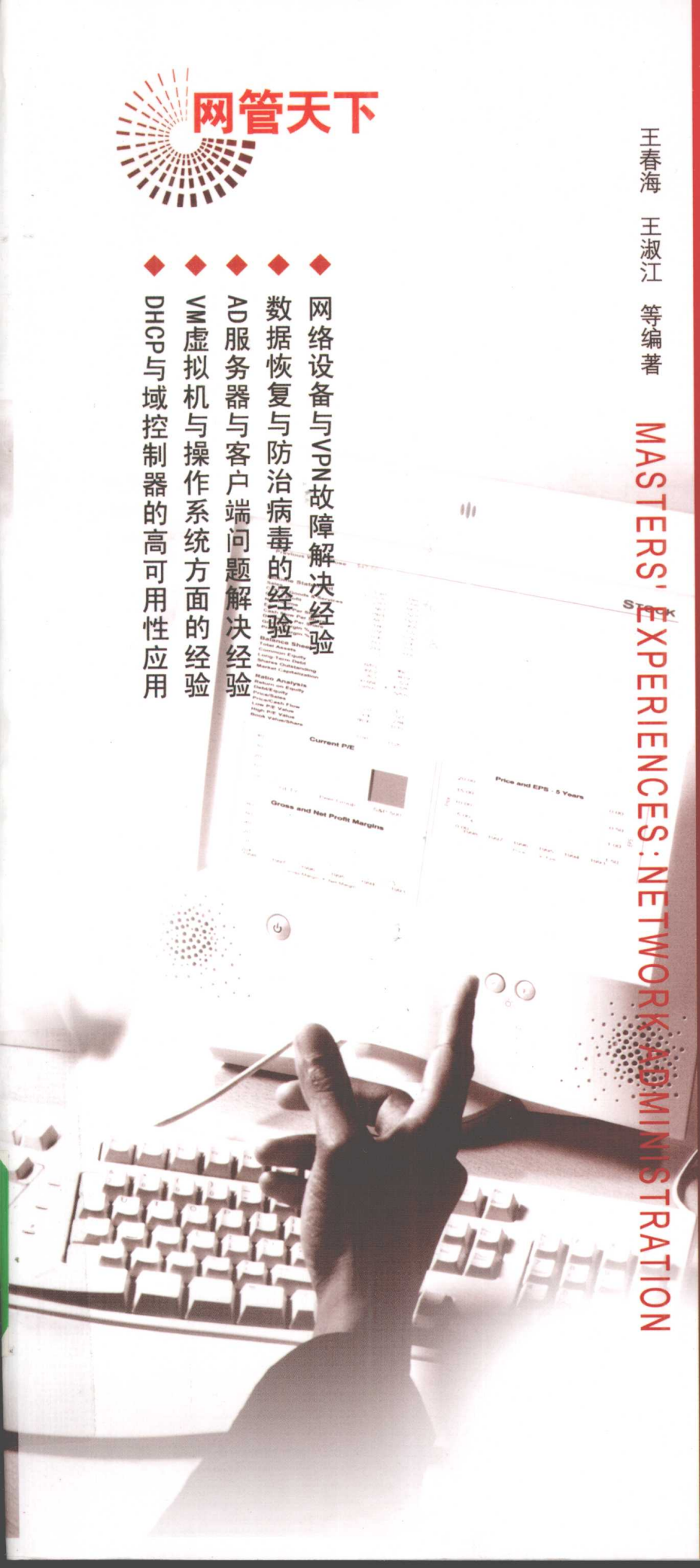
网管天下

网管经验谈

王春海 王淑江 等编著

MASTERS' EXPERIENCES: NETWORK ADMINISTRATION

- 网络设备与VPN故障解决经验
- 数据恢复与防治病毒的经验
- AD服务器与客户端问题解决经验
- VM虚拟机与操作系统方面的经验
- DHCP与域控制器的高可用性应用



電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

网管天下

网管经验谈

王春海　王淑江　等编著

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

内 容 简 介

本书前半部分以实际的网络环境为基础，详细阐述了网络从规划、部署、管理、排故等过程中常用的硬件到软件应用，从服务器到客户端计算机，以及目前炙手可热的虚拟化方面进行了详细地阐述。本书后半部分，着重讲述了网络中重要的高可用性应用，网络防病毒体系，以及网络中对计算机和用户的管理。本书以管理员的日常工作主线为基调，介绍在网络管理中的经验，使读者可以举一反三，触类旁通，增强实际工作能力。

本书语言流畅、通俗易懂、深入浅出、可操作性强，注重读者实战能力的培养和技术水平的提高。适用于网络管理人员，以及对计算机系统维护和网络管理感兴趣的计算机爱好者，并可作为大专院校计算机专业的教材或课后辅导资料。

未经许可，不得以任何方式复制或抄袭本书之部分或全部内容。
版权所有，侵权必究。

图书在版编目(CIP)数据

网管经验谈 / 王春海等编著.—北京：电子工业出版社，2010.1
(网管天下)
ISBN 978-7-121-09880-2

Ⅰ. 网… Ⅱ.王… Ⅲ.计算机网络—管理 Ⅳ.TP393.07

中国版本图书馆 CIP 数据核字（2009）第 207162 号

策划编辑：郭鹏飞
责任编辑：段春荣
印　　刷：北京市天竺颖华印刷厂
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1092　1/16　印张：36.5　字数：934 千字
印　　次：2010 年 1 月第 1 次印刷
定　　价：59.80 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：（010）88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：（010）88258888。

前言

关于《网管天下》丛书

《网管天下》丛书是一套由国内资深网络专家写给网络建设与管理人员的应用实践手册，其目的在于帮助初、中级网络管理员，全方位地解决网络建设与管理中的各种实际问题，包括综合布线设计、实施与测试，网络设计与设备选择、连接与配置，网络服务搭建、配置与监控，网络故障诊断、排除与预防，网络安全设计、配置与监视，网管工具选择、使用与技巧，网络设备、服务和客户管理的自动化等诸多方面；囊括了网络管理中几乎所有的内容，其目的在于将网络理论与实际应用相结合，提高读者分析和解决具体问题的能力，将所学变为所用，将书本知识变为操作技能。

《网管天下》第 1 版已经出版近两年的时间，取得了不错的销售业绩，在同类图书中名列前茅，受到了广大读者朋友的喜爱。《网络管理工具实用详解》一书的版权还输出到了中国台湾，得到了中国台湾出版业同行的认可。不过，在这两年时间里，新的网络设备不断推出、新的网络技术不断成熟、新的管理软件不断升级、新的网络应用也不断丰富，原来图书中的有些内容已经不能适应新设备、新技术、新软件和新应用的需求。因此，在保留图书原有写作风格的基础上，对目录结构做了进一步优化，对过时的内容进行了大幅度的更新，隆重推出了《网管天下》第 2 版。

本丛书具有以下特点。

1. 授之以渔而不是授之于鱼。紧贴网络实际情况，从真实的网络案例入手，为网络管理员提供全面的网络设计、网络组建、网络管理和网络维护等解决方案，以提高读者的分析能力、动手能力和解决实际问题的能力。

2. 实用才是硬道理。为网络管理员提供彻底的、具有建设性的网络设计、网络组建和配置解决方案，真正解决网络建设和网络管理中的实际问题，突出实用性、针对性、技术性、经典性，举案说“法”、举一反三。

3. 理论新、技术新、设备新、案例新。所有的应用案例都发生在最近两年，而且案例中只涉及最主流的、最成熟的设备和技术，以及最新版本的软件，不再讨论那些已被淘汰或面临淘汰的东西，从而力求反映网络的新技术和新潮流。不仅让读者学了就能用，而且还可以拥有三年左右的“保鲜”期。

关于本书

本书以实际网络管理经验为基础，内容涵盖网络管理的多个层面，包括：网络设备、机房管理、服务器、网络安全、操作系统、虚拟化应用、VPN 部署、常用 Windows 内置工具、高可用性应用、网络防病毒系统、以及网络管理的核心——用户和计算机的管理等方面，详细介绍在以上领域经常遇到和需要注意的问题。由于网络管理员所处的环境不同，书中介绍

的经验可能和读者的环境有所不同，也希望读者和编者一起交流经验。

本书由王春海、王淑江等编著，李海宁、田俊乐、陈志成、王延杰、赵卫东、刘淑梅、马倩、杨伏龙、李文俊、王同明、石长征、刘晓辉、白华、郭腾及刘红等也参与了部分章节的编写工作。由于作者水平有限，并且本书涉及的系统与知识点很多，书中难免有不足之处，有关本书的意见反馈和更新消息，可以发邮件到 Redws@163.com 联系作者。对于本书出现的任何问题、意见、建议，也可以与本书编辑（duancr@phei.com.cn）直接联系。

编　者

2009.11

此为试读，需要完整PDF请访问：www.ertongbook.com

目录

CONTENTS

此为试读,需要完整PDF请访问: www.ertongbook.com

第1章 网络方面

计算机网络在我们的日常生活中已经变得越来越普遍。特别是 20 世纪 90 年代以来，随着 Internet 在世界范围的普及，计算机网络逐渐成为人们获取信息、发布信息的重要途径，与此同时，基于计算机网络的应用也越来越多，许多人们生活中的重要环节都可以利用网络方便、快捷地实现。

本章主要介绍了五个方面的经验：网络基础经验、轻松上网经验、路由器故障解决经验、vpn 实用经验，以及网络实验方面经验。

1.1 网络基础经验

本节主要介绍了五个基础性的网络经验，包括机房内网络设备布置经验、解决局域网 IP 冲突经验、网络打印机安装经验、网上邻居疑难问题故障解决经验、局域网互访问题解决经验，另附网络命令全集，以供初级网络管理员查询使用。

1.1.1 机房内网络设备布置经验

要组建一个网络，不仅要从自身的实际需求出发，根据组网经费的多少来务实地规划与设计网络；还要在采购好网络设备和服务器等设备后，对机房、办公地点进行合理的网络布局与布线。对于网管员来说，怎样去进行网络布局与布线这项工作才是致关重要的。

本节所说的网络布局主要是指机房里的网络设备和服务器等设备如何放置，它们又与网络布线如何协调。

1. 网络布局的原则

（1） 实用性。

企业组建的局域网应当根据机房的面积大小、设备的数量多少等情况来决定如何具体实施，根据网络布线的特点来发挥网络布局实用性是非常重要的。

（2） 全面性。

组网过程中，进行网络布局时要考虑周全，尽量让各种设备和布线系统处于合理的位置。

（3） 可靠性。

局域网无论怎样布局，最终目的是要保证其中的所有设备都能可靠稳定地运行，从而使得网络能够正常运转。

（4） 便于维护与升级。

网络的组网不是一成不变的，随着 IT 企业业务不断发展的需求，原先组建的局域网也需要不断地完善和扩充；规划网络布局时就应该考虑到以后的网络维护与升级操作。

2. 网络布局的具体实施要求

规划网络布局首先要规划与设计好机房的设备布局和布线系统，使其合理搭配，然后再全面地考虑网络的布局。

为了确保网络、计算机系统稳定、安全、可靠地运行，保障机房工作人员有良好的工作环境，机房的规划与设计应该做到技术先进、经济合理、安全适用、确保质量，符合国家的有关规定。

（1） 防静电。

静电不仅会使计算机运行出现随机故障，而且还会导致某些元器件、双级性电路等的击穿和毁坏。此外，还会影响操作人员和维护人员的正常工作和身心健康。

（2） 防火、防盗。

机房的设计要重点考虑消防灭火方面的功能。在设计时可以根据消防的防火级别来确定机房的设计方案，机房的火灾报警系统要求在一楼设有值班室或监控点。

机房里应注意防盗设施的安装，具体地可采用防盗门、防盗锁、警卫、自动报警系统等等。

（3） 防雷。

由于机房的通信和供电电缆大多是从室外引入机房，容易遭受雷电的侵袭，因此机房建筑的防雷设计尤其重要。如计算机通信电缆的芯线、电话线等均应加装避雷器。

（4） 保温。

机房里的湿度以保持在 20%~80%的范围为宜，而温度则应保持在 15℃~35℃。安装空调来调节温度是解决此问题的最好办法。

3. 布线系统的规划与设计

有了好的机房，网络设备就有了好的“家”，组建的 IT 网络应当通过布线系统将机房和办公地点互联起来，确保网络的正常运行。如果企业的接入点较多，我们可以采取接入层、汇聚层、交换层三个网络层次的设计，并在此基础上进行布线系统。

对于接入层来说，选择一个合理的接入设备是最关键的，而且我们要根据接入的设备来选择合适的带宽。汇聚层是整个局域网的核心部分，汇聚层网络设备一般支持网络管理功能，方便我们的管理维护和以后的网络升级改造。交换层是整个网络的中间层，连接着汇聚层和网络结点，是决定我们整体网络传输质量的一个很重要的环节。随着百兆位网络设备的普及，我们建议交换层的网络设备首选百兆位。

布线是连接网络接入层、汇聚层、交换层和网络结点的重要环节。在布线时，最好使用专门的通道，不要与电源线、空调线等具有辐射的线路混合布线。

接入层与汇聚层之间的双绞线建议选择超五类屏蔽双绞线，这样可以使网络性能得到最大的提升。汇聚层与交换层之间的双绞线，由于是网络数据传输量最大的一个层次，同样采用超五类屏蔽双绞线。交换层与网络结点之间，我们就可以采用普通的超五类非屏蔽双绞线。

网络设备最好放在结点的中央位置，这样做既可以节约综合布线的成本，又提高了网络的整体性能和网络传输质量。值得注意的是虽然双绞线的传输距离是 100 m，但在 95 m 处才能获得最佳的网络传输质量。在做网络布线时，最好能够设计一个设备间，用来放置网络设备。

4. 网络布局的规划与设计

目前的网络设备大都采用机架式的结构（多为扁平式，或像个抽屉），如交换机、路由器、硬件防火墙等。这些设备之所以用这样一种结构类型，是因为它们都是按照国际机柜标准进行设计的，这样各种设备的平面尺寸就基本统一，可以把它们一起安装在一个大型的立式标准机柜中。这样做的好处非常明显：一方面可以使设备占用最小的空间，另一方面则便于与其他网络设备的连接和管理，同时机房内也会显得整洁、美观。

我们经常接触到的机房里放置有网络机柜、服务器机柜和综合布线柜，从这三个机柜的名字就可以看出它们各自所起的作用。

一般来说，网络设备（如交换机、路由器、防火墙、加密机等）以及网络通信设备（如光端机、调制解调器等）是放置在网络机柜的；服务器机柜的宽度为 19 英寸（1 in=25.4 mm），高度以 U 为单位（1 U=1.75 in=44.45 mm），通常有 1 U，2 U，3 U，4 U 几种标准的服务器。机柜的尺寸也是采用通用的工业标准，通常从 22 U 到 42 U 不等。机柜内按 U 的高度有可拆卸的滑动拖架，用户可以根据自己服务器的标高灵活调节高度，以存放服务器、集线器、磁盘阵列柜等设备。服务器摆放好后，它的所有 I/O 线全部从机柜的后方引出（机架服务器的所有接口也在后方），统一安置在机柜的线槽中，一般贴有标号，以便于管理。

综合布线柜一般配有前后可移动的安装立柱，可以自由设定安装空间，还可按需要配置隔板、风扇、电源插座等附件。配线架通常安装在机柜里，配线架的一面是 RJ45 口，其上标有编号；另一面是跳线接口，上面也标有编号，这些编号和上面的 RJ45 口的编号是一一对应的。每一组跳线都标识有棕、蓝、橙、绿的颜色，双绞线的色线要和这些跳线一一对应，这样进行操作时就不容易接错。配线架不仅仅是为了便于管理线对，而且可以防止串扰，增加线对的隔离空间，提供 360° 的线对隔离。

在机房中，必须放置交换机、功能服务器群和网络打印设备，以及局域网络连接 Internet 所需的各种设备，如路由器、防火墙和网管工作站等。因此机房的网络布局一般至少有三个机柜，综合布线柜和网络机柜应当紧连在一起，便于调线操作，然后再考虑服务器机柜以达到网络设备和布线系统的布局合理。

在网络布局中，每个机柜内最好留点空间，便于以后网络设备、服务器设备的扩充，综合布线柜里除了网络布线外，还有可能布置电话线，所以要在机柜里留下一定空间。

从机柜内部线缆敷设的角度看，机柜配置密度更高，容纳的 IT 设备更多，大量采用冗余配件（如冗余电源、存储阵列等），机柜内设备配置频繁变换，数据线和电缆随时增减。所以，机柜必须提供充足的线缆通道，能从机柜顶部、底部进出线缆。在机柜内部，线缆的敷设必须方便、有序，与设备的线缆接口靠近，以缩短布线距离；减少线缆的空间占用，保证设备安装、调整、维护过程中，不受到布线的干扰，并保证散热气流不会受到线缆的阻挡；同时，在故障情况下，能对设备布线进行快速定位。

供电系统和制冷系统是计算机机房的两个重要部分。在供电系统中，一般采用在线的 UPS 供电方式，蓄电池实际可供使用的容量与蓄电池的放电电流大小、蓄电池的环境工作温度、存储时间的长短和负载的性质（电阻性、电感性、电容性）密切相关。

制冷系统（空调）涉及到机房的整个物理环境，包括空调、地板、机柜及房间布局等诸多方面；因此 UPS 和空调我们也要考虑将它们放置在一个合适的位置。如果机房空间较大，可以将 UPS 和空调都放在机房里；如果空间较小，可以把 UPS（包括蓄电池）放在配电房里。

需要注意的是如果大楼里安装有“中央空调”时，机房里也必须安装独立的空调，因为中央空调不可能24小时都开着，上班的时间可以利用中央空调，下班和星期节假日的时候，如果服务器、网络设备需要正常运行，则必须要开机房里的独立空调。

机柜的扩展性表现在机柜内设备密度的扩展和机柜数量的扩展，因此网络布局时必须将机柜的配风能力（通常称为散热能力）和配电能力考虑在内。一方面，机柜内的设备需要温度、湿度适宜并且风量充足的冷风（冷空气）。这些冷风被机柜内的IT设备吸入，从而为设备内的部件（尤其是CPU）降温。当机柜内设备增加到一定数量时，由地板出风口送出的冷风风量将不能满足所有设备的需求，从而形成部分IT设备配风不足而过热。

解决机柜内设备密度扩展时遇到的这种局部热点问题可以采用调配IT设备位置的方式来解决。例如，把热负荷最大的设备安装在机柜中部位置，以便获得最大的配风风量。另外的解决方法是，在机柜的上部或下部位置安装轴向水平的强排风扇，增强上部或下部的吸入能力（即减小IT设备的入口静压），从而增加配风风量。

另一方面，机柜内的设备需要供电以及与机柜外部进行通信。当机柜内的IT设备数量增加时，这些线缆、连接端子同时成倍增加，从而对机架式电源排插的容量、插口数量都提出了扩展要求。机柜内的布线空间也是需要提前考虑的，因为当机柜内的功率密度提高时，设备后部的线缆将明显增加风阻，所以必须考虑线缆管理及走线空间的问题。

1.1.2 解决局域网IP冲突经验

要想避免IP地址冲突故障现象的发生，首先应该了解制造IP地址冲突的方法，只有这样才能对症下药，采取针对性措施来拒绝IP地址冲突“干扰”局域网的正常运行。

一般来说，在局域网投入运行的初期，网络管理员都会为局域网中的所有工作站分配一个合适的IP地址。不过，在局域网工作站长时间运行后，很可能会出现系统瘫痪或者其他一些故障现象，导致工作站的上网参数发生了丢失。此时工作站用户很可能会自己动手，进入本地工作站系统的TCP/IP属性设置窗口，在其中随意为本地工作站分配一个IP地址，该IP地址由于不是网络管理员事先划分好的那个IP地址，这样一来自然就会形成IP地址的冲突现象。在使用静态IP地址的局域网工作环境中，普通用户可以很容易地打开本地系统的TCP/IP属性设置窗口，并随意修改本地工作站的IP地址，从而造成IP地址使用出现混乱。

为了保护本地工作站的IP地址不被非法用户随意盗用，有一些熟悉网络的朋友往往会采取地址绑定的方法，将网络管理员事先分配给本地工作站的IP地址绑定到对应工作站的网卡设备上。这样一来即使非法用户盗用了本地工作站的IP地址，也不会干扰本地工作站的正常上网访问。可是，对于采取了绑定措施的IP地址来说，非法用户同样也能找到盗用的办法，那就是同时盗用合法工作站的IP地址与网卡设备的MAC地址，然后冒用合法主机的身份进行恶意破坏。

例如，非法用户在盗用了合法工作站的IP地址后，发现盗用后的IP地址不能正常连接到局域网网络中时，他们会认为该IP地址很可能被绑定了。于是非法用户尝试使用MAC地址扫描器之类的工具来查看、盗用合法工作站的网卡MAC地址，在盗取合法工作站的网卡MAC地址后，非法用户再将自己工作站的IP地址修改成合法MAC地址就可以了。修改网卡MAC地址的方法很简单，用户只要依次单击本地工作站系统桌面中的“开始”/“设置”/“网络连接”命令，在弹出的“网络连接列表”窗口中，用鼠标右键单击“本地连接”图标，从弹出的

快捷菜单中执行“属性”命令，打开本地连接属性设置对话框；单击该对话框中的“常规”选项卡，并在对应选项设置页面中单击“配置”按钮，进入本地工作站的目标网卡属性设置对话框；继续单击该设置对话框中的“高级”选项卡，打开如图 1-1 所示的高级选项设置页面，选中该设置页面左侧“属性”列表框中的“Network Address”选项，并将该选项的数值设置成盗用得来的网卡 MAC 地址，最后单击“确定”按钮就可以完成网卡物理地址的修改任务了。

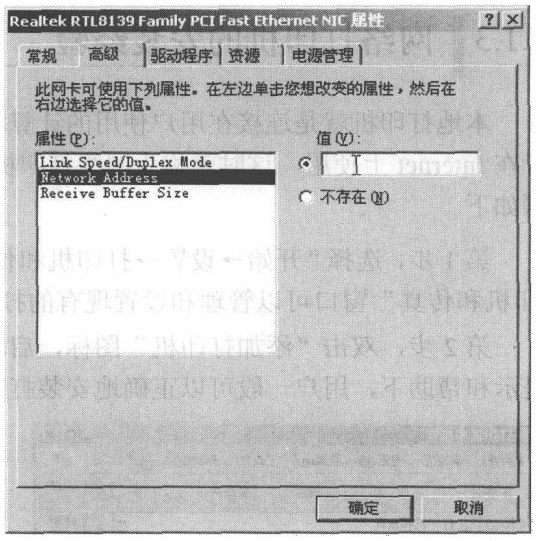


图 1-1　高级选项设置

了解制造 IP 地址冲突的几种方法后，用户就能根据不同的制造方法采取不同的阻止手段了。

在使用静态 IP 地址的局域网工作环境中，网络管理员可以使用 IP-MAC 地址绑定方法，也就是使用静态路由技术的方法来阻止普通工作站用户随意进入 TCP/IP 属性设置窗口，胡乱修改本地系统的 IP 地址。考虑到在相同的局域网网段中，普通工作站的网络寻径不是根据主机的 IP 地址而是根据主机的物理地址来进行的，在不同网段之间通信时才会根据主机的 IP 地址进行网络寻径，所以作为局域网网关的路由器设备上通常保存有 IP-MAC 的动态对应表，这是由 ARP 通信协议自动生成并维护的。我们可以进入局域网路由器的后台管理界面，从中找到配置 ARP 表的设置选项，对静态的 ARP 路由表进行个性化指定，日后局域网路由器设备会自动依照静态的 ARP 表检查通信数据包，要是无法对应，那么就不会进行数据转发操作。使用这种手段，网络管理员能够轻松地阻止非法攻击者在不修改网卡设备 MAC 地址的情况下，冒用合法工作站 IP 地址进行非法网络访问。

为了防止非法用户通过修改网卡 MAC 地址的方法来制造 IP 地址冲突故障现象，我们可以利用局域网交换机的端口绑定功能，来有效化解非法用户通过修改网卡 MAC 地址的方法来适应静态 ARP 表的问题。常见的可管理交换机都支持端口绑定功能，我们可以利用该功能提供的端口地址过滤模式，来实现阻止 IP 地址冲突的目的，因为交换机的端口地址过滤模式会允许每一个交换机的连接端口仅允许具有合法 MAC 地址的工作站访问网络，任何具有不合法 MAC 地址的工作站都将被交换机拒绝访问网络。

在组网规模较大的工作环境中，我们还可以通过划分虚拟子网的方法，来阻止 IP 地址冲突现象的发生。从严格意义上来说，划分虚拟工作子网其实并不属于技术措施，而是管理措施与技术措施结合在一起的手段。将那些具有相同访问行为的 IP 地址统一划分到相同的虚拟工作子网中，并正确设置好相关的路由策略，这样一来我们就能有效拒绝非法攻击者盗用其他工作子网 IP 地址现象的发生。

此外，我们在管理、维护局域网的过程中，尽量少用那些直接针对 IP 地址授权的管理模式，而应该综合运用加密、口令、VPN 连接或其他身份认证机制，建立多层次的严密的安全体系，那样一来就能有效降低 IP 地址冲突所带来的安全威胁了。

1.1.3 网络打印机的安装经验

本地打印机就是连接在用户使用的计算机上的打印机。将其共享后可以在局域网内使用或者在 Internet 上使用，这时就称为网络打印机。要在 Windows 2003 Server 中添加打印机，步骤如下。

第 1 步，选择“开始→设置→打印机和传真”命令，打开“打印机和传真”窗口，利用“打印机和传真”窗口可以管理和设置现有的打印机，也可以添加新的打印机，如图 1-2 所示。

第 2 步，双击“添加打印机”图标，启动“添加打印机向导”。在“添加打印机向导”的提示和帮助下，用户一般可以正确地安装打印机，如图 1-3 所示。

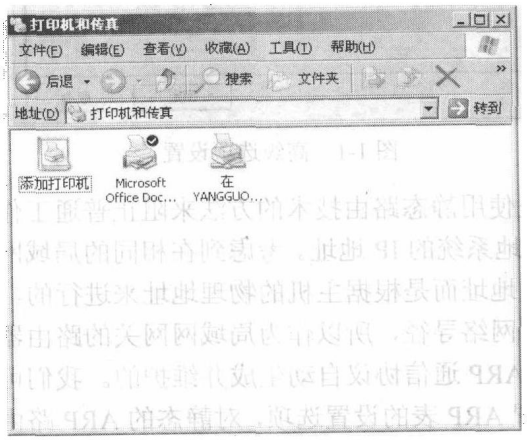


图 1-2 打印机和传真

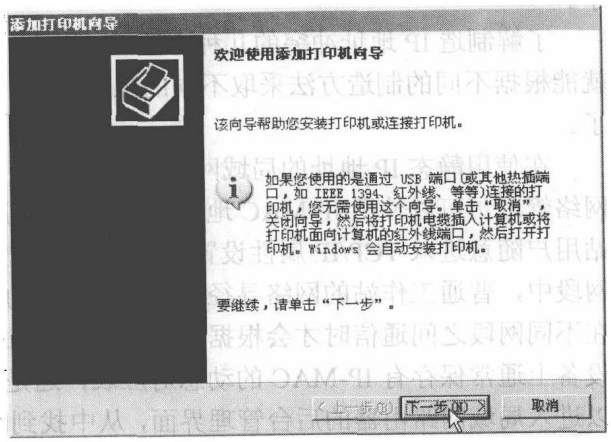


图 1-3 添加打印机向导

第 3 步，单击“下一步”按钮，进入“本地或网络打印机”对话框。在此对话框中，用户可选择添加本地打印机或者是网络打印机。选择“连接到此计算机的本地打印机”单选按钮，即可添加本机打印机，如图 1-4 所示。

第 4 步，单击“下一步”按钮，弹出“选择打印机端口”对话框，选择要添加打印机所在的端口。如果要使用计算机原有的端口，可以选择“使用以下端口”单选按钮。一般情况下，用户的打印机都安装在计算机的 LTP1 打印机端口上，如图 1-5 所示。

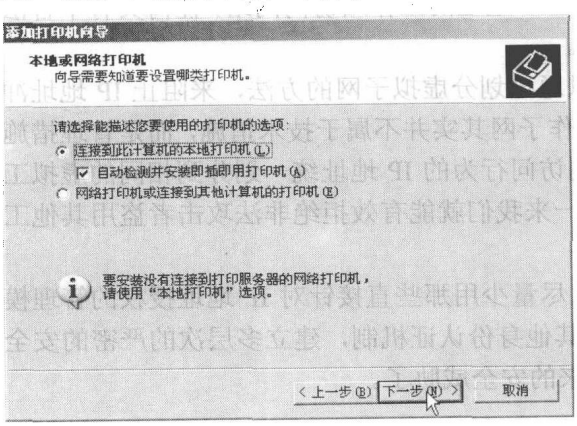


图 1-4 选择打印机类型

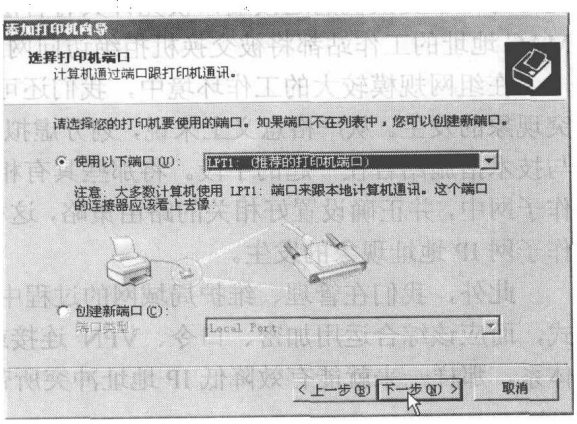


图 1-5 设置打印机端口

此为试读，需要完整PDF请访问：www.ertongbook.com