资深网管
倾力打造
高薪职业
必经之路

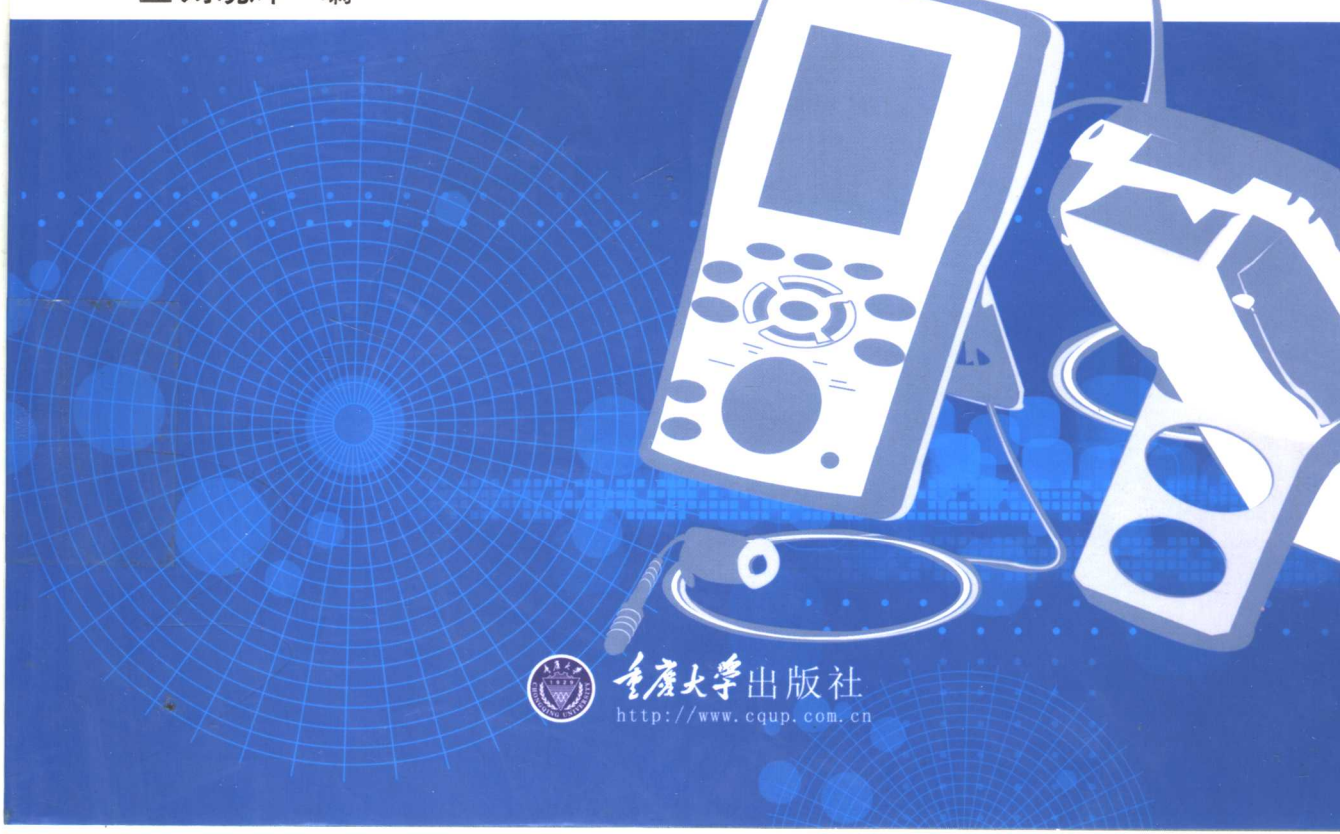
网管从业宝典

故障排除经典案例分册

经典案例分析 全新思路讲解 独特培训方法

／汇集经典常见故障／总结解决问题思路／局域网故障排除经验谈
／全程分析网络故障处理过程／全面演示网管故障处理工具
／网管职业技巧点拨

■ 刘晓辉 编



重庆大学出版社
http://www.cqup.com.cn

网管从业宝典

故障排除经典案例分册

WANGGUAN CONGYE BAODIAN GUZHANG PAICHU JINGDIAN ANLI FENCE

刘晓辉 编

重庆大学出版社

内 容 提 要

本书针对局域网中的故障以及解决方法进行了详细的介绍和说明，主要介绍了 Windows 网络故障诊断工具、网络故障诊断工具、故障诊断经验与技巧、网卡和网络协议故障与排除方法、交换机故障与排除方法等方面的内容，让读者可以轻松掌握相关知识。本书风格活泼，实践内容丰富，适合广大学生、网络爱好者及网络从业人员阅读。

图书在版编目（CIP）数据

网管从业宝典　故障排除经典案例分册 / 刘晓辉编.
重庆：重庆大学出版社，2007.4
ISBN 978-7-5624-4063-5

Ⅰ. 网… Ⅱ. 刘… Ⅲ. 计算机网络－管理 Ⅳ. TP393.07

中国版本图书馆 CIP 数据核字（2007）第 041894 号

网管从业宝典　故障排除经典案例分册

刘晓辉　编

责任编辑：宋　坤　刘颖果　黄　成　　版式设计：王明娟
责任校对：方　正　　责任印制：赵　晟

*

重庆大学出版社出版发行
出版人：张鸽盛
社址：重庆市沙坪坝正街 174 号重庆大学（A 区）内
邮编：400030
电话：(023) 65102378　65105781
传真：(023) 65103686　65105565
网址：http://www.cqup.com.cn
邮箱：fxk@cqup.com.cn（市场营销部）
全国新华书店经销
重庆科情印务有限公司印刷

*

开本：787 × 1092　1/16　　印张：21　字数：430 千
2007 年 4 月第 1 版　　2007 年 4 月第 1 次印刷
ISBN 978-7-5624-4063-5　　定价：32.00 元

FOREWORD

前言

21 世纪是一个名副其实的信息时代，同时也是竞争激烈的时代。随着大学生的不断增多，学生就业成为了社会热点问题。学习一技之长，找到一份称心如意的工作是每个大学生的梦想，而网络管理员则是很多大学生理想中的职业。但网络管理员这一职业对于理论与实践能力要求都非常高，对于那些没有实际工作能力的学生来说，他们很难胜任这样一份工作。

于是，我们便编撰了此书，系统地介绍组建局域网的各种理论、操作和经验，希望能对大家的网络管理工作有所帮助，同时也希望可以帮助读者轻松掌握网络管理员在日常工作中常用的各种知识。

本书引入了学生与老师 2 个角色，采用问答的方式将枯燥的知识和技术串联起来，生动活泼，又不失理论和技术的系统性，由浅入深、由易至难、步步推进，全面而系统地解决了读者的各种问题。

本系列书共分为 4 个分册，涵盖了网络基础知识、网络组建、网络管理与维护和网络故障问答等内容。

本书为故障排除经典案例分册，共分 10 个部分。第 1 部分介绍 Windows 网络故障诊断工具；第 2 部分介绍网络故障诊断工具；第 3 部分介绍故障诊断经验与技巧；第 4 部分介绍了网络链路故障的解决方法；第 5 部分介绍了网卡和网络协议故障的解决方法；第 6 部分介绍了交换机故障的解决方法；第 7 部分介绍了路由器和宽带路由器故障的解决方法；第 8 部分介绍了对等网络故障的解决方法；第 9 部分介绍了无线网络故障的解决方法；第 10 部分介绍了应用网络服务故障的解决方法。

本书作者是长期工作在网络教学和管理第一线的高校教师，既有扎实的理论，又有丰富的实践经验，并出版过十余册有关局域网方面的书籍。相信本书能够为所有准备从事网络管理工作的读者提供一些帮助，缩短大家熟悉工作的时间，并在求职时少走一些弯路。

本书是中小型网络管理人员的必备参考书，同时可作为局域网组建者的指导书，也可作为各类网络培训机构或各大中专院校相关课程的参考书。

第一章 Windows 网络故障诊断工具

第二章 网络故障诊断工具

第五章 网卡和网络协议故障

第六章 交换机故障

第七章 路由器和宽带路由器故障

第八章 对等网络故障

第九章 无线网络故障

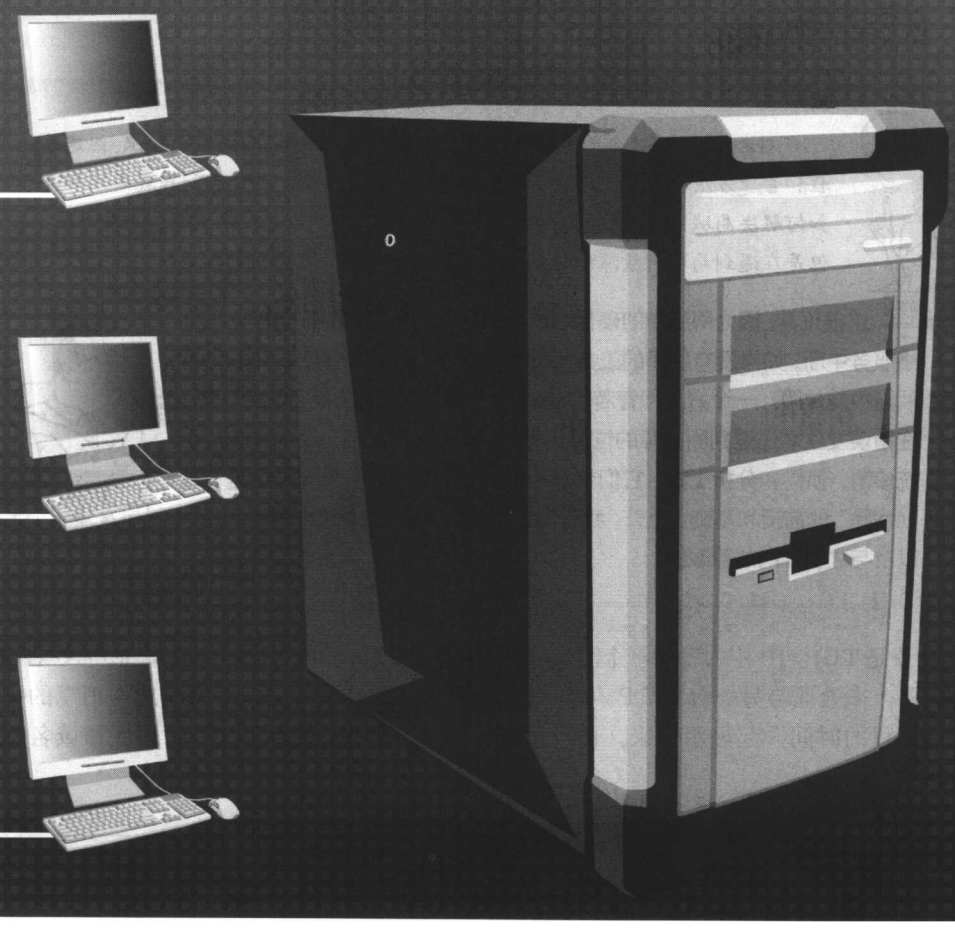
第十章 应用网络服务故障

第一章

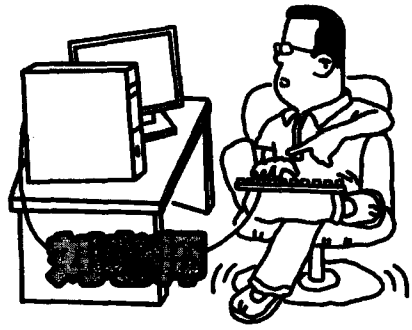
Windows网络故障诊断工具

内容提要：

1 网络链路诊断工具
2 Windows系统诊断工具
3 Wiindows服务诊断工具



网络管理员最怕什么？他们最怕就是网络出现故障。网络故障小则影响某个人或部门的正常工作，大则影响公司的整体运行，甚至会带来不可估量的经济损失。面对如潮的指责声，网络管理员的工作压力陡然提升。在这里，我就向大家介绍一下自己处理网络故障的经验，希望对大家的工作有所帮助。



第一节 网络链路诊断工具

一、IP 连接测试——Ping

刘老师，经过这么长时间的学习和实践，我对于局域网的理论知识、组建过程和管理方法都有了比较深刻的了解。不过，现在我遇到的最大问题就是不知道如何解决局域网中的故障。对于单机故障来说，我可以轻松解决硬件软件故障，但是在遇到局域网故障的时候，我就有些摸不着头脑了。

这很正常，因为网络中的硬件瑕疵、系统Bug、错误操作都可能导致网络服务中断。如果没有优秀的工具和丰富的经验，普通用户很难解决局域网当中的故障。一个好的网管若想在故障发生前敏锐地捕捉到蛛丝马迹，在错误发生后迅速判断故障的位置，搞清导致故障的原因，就必须借助系统诊断、侦错和分析工具。它们就像是听诊器、CT机和病历记录，是“药到病除”的前提和基础。今天，我就向你介绍一些局域网故障的诊断工具以及与之相关的故障案例。

Ping 命令是TCP/IP 中内置的一个测试工具，主要通过发送Internet 控制消息协议（ICMP）回响请求消息，来验证与另一台TCP/IP 计算机的IP 级连接。对应的回响应答消息的接收情况将和往返过程的时间一起显示出来。Ping 是用于检测网络连接性、可到达性和域名解析的主要TCP/IP 命令。

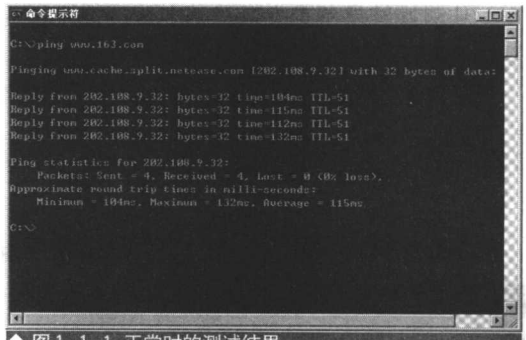
1.应用示例

示例1：正常时和故障时的测试结果。

网络运行正常情况下，在命令提示符窗口中输入如下命令：

ping www.163.com

回车执行，所有发送的包均被成功接收，丢包率为0，如图1-1-1所示。



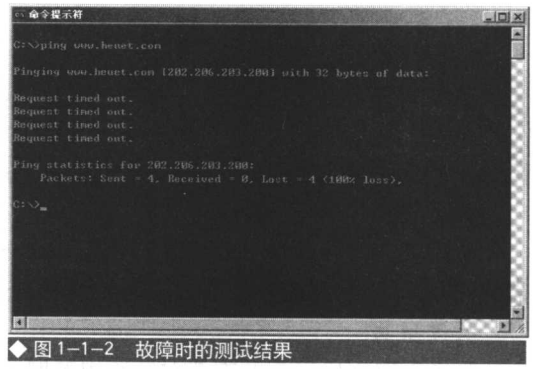
◆ 图1-1-1 正常时的测试结果

正常测试结果中会连续出现类似“Reply from 202.1011.11.22：bytes=32 time=104 ms TTL=51”的语句。其中104 ms表示从发送数据到收到回应经历的时间，如果超出限定时间后仍未收到回应，则视为连接超时，自动继续发送下一个测试数据包，系统默认的超时时间为4 000 ms（4 s）；TTL=51表示对方主机的TTL值为51，根据TTL值一般可以确定该计算机使用哪种操作系统，例如Windows XP/2000系统的主机通常为128，Windows 98系统的主机通常为64，而Unix系统的主机一般为255。

当网络出现故障时往往得不到上述结果。在命令提示符窗口中输入如下命令：

ping www.henuet.com

按回车执行，会显示如图1-1-2所示的结果。表明网络连接不正常，所有发送的测试数据包均未被成功接收，丢包率为100%。



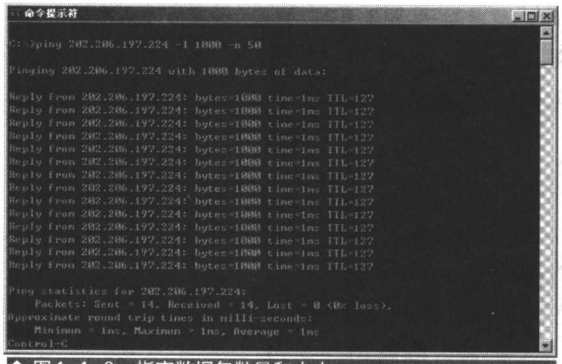
◆ 图1-1-2 故障时的测试结果

示例2：指定测试数据包的数目和数据包的大小。

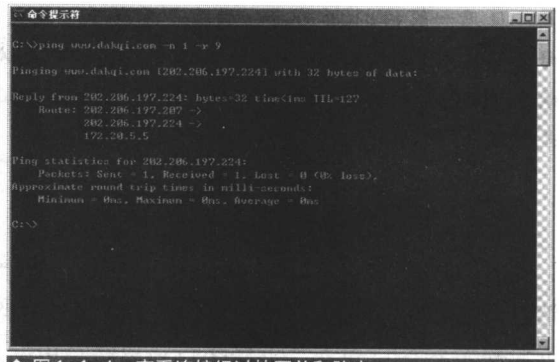
发送指定数量的数据包，最后可以得出丢包的概率，如果丢包率非常高，虽然网络是连通的，但其稳定性会非常差。指定数据包的大小，则是为了测试网络是否能够提供一定的带宽。例如，在命令提示符窗口中输入如下命令：

ping 202.206.196.224 n 50 l 1000

按回车执行，其中发送数据包的数量为50，数据包大小为1 000 bytes，如图1-1-3所示。



◆ 图1-1-3 指定数据包数量和大小



◆ 图1-1-4 查看连接经过的网关和路由

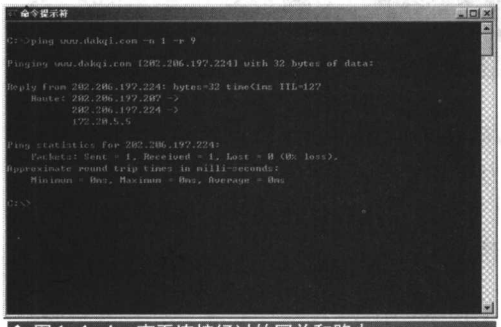
从测试结果不难发现，丢包率为0%。通常情况下，丢包率低于20% 时不会影响到正常网页浏览等应用。

示例3：测试到http://www.dakqi.com的连通性以及所经过的路由器和网关，并只发送一个测试数据包。

在命令提示符窗口中输入如下命令：

ping www.dakqi.com n 1 r 9

按回车执行，可显示所经过的网关和路由器，如图1－1－4所示。



◆ 图1－1－4　查看连接经过的网关和路由

刘老师提醒

由于ping命令行是TCP/IP协议的一个组件，因此应用之前必须正确安装TCP/IP协议。

2.解决故障

故障描述

一次，笔者在配置完一台路由器后执行ping命令，检测链路是否通畅。发现报文都没有ping通，增加报文数，但故障依旧，老刘断定是连通性问题。

故障分析

检查双方的配置命令并查看路由表，却一直没有找到错误所在。可能是连通性问题，这时需要采取逐段检测的方法对链路中的网关进行逐级测试，看问题出在哪一段。

故障解决

笔者采取逐段检测的方法对链路中的网关进行逐级测试，发现都可以ping通，但是响应的时间越来越长，最后一个网关的响应时间在1 800 ms左右。可能是由于超时而导致ping不通，受此启发，笔者将ping命令报文的超时时间改为4 000 ms，这次成功ping通了，显示所有的报文响应时间都在2 200 ms左右。

故障点评

使用一般的ping命令，缺省是发送5个报文的，超时时长是2 000 ms。如果ping不通，最好能够再用带参数－c和－t的ping命令再执行一遍，如ping －c 20 －t 4000 ip－address，即连续发送20个报文，每个报文的超时时长为4 000 ms，这样一般可以判断出到底是连通性问题还是性能问题。

二、路由追踪——Tracert

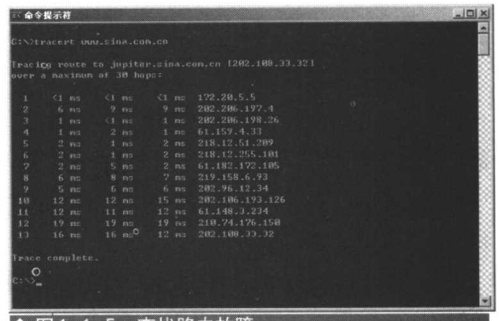
通过递增“生存时间（TTL）”字段的值将“Internet 控制消息协议（ICMP）回响请求”消息发送给目标可确定到达的路径。所显示的路径是源主机与目标主机间的路径中，路由器的近侧路由器接口列表。近侧接口是离路径中发送主机最近的路由器接口。

示例1：追踪到新浪网（http://www.sina.com.cn）的路由。

在命令提示符下输入命令：

tracert www.sina.com.cn

回车，命令成功执行，可以看到从本机到新浪网之间所经过的所有路由，如图1－1－5所示。



◆ 图1－1－5　查找路由故障

三、路径测试——Pathping

示例1：查看本地主机到局域网网关的路径信息。

在命令提示符窗口中输入如下命令：

pathping 172.20.5.5

按回车执行，显示如图1－1－6所示结果。由于本例中没有使用－n参数，所以将本地主机IP地址解析为域名了。

示例2：查看远程主机的路径信息。

由于到远程主机往往要经过多重路由，因此通常需要指定禁止解析成域名，以加快查询速度。在命令提示符窗口中输入如下命令：

pathping www.tom.com　　n

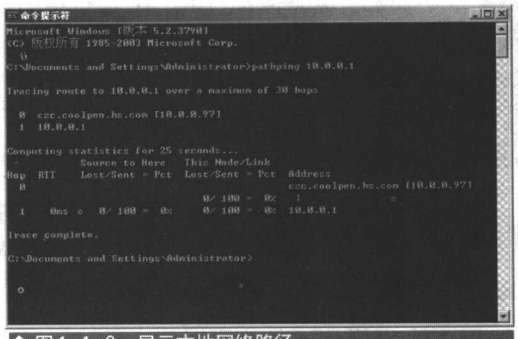
按下回车，执行成功，显示如图1－1－7所示。

刘老师提醒

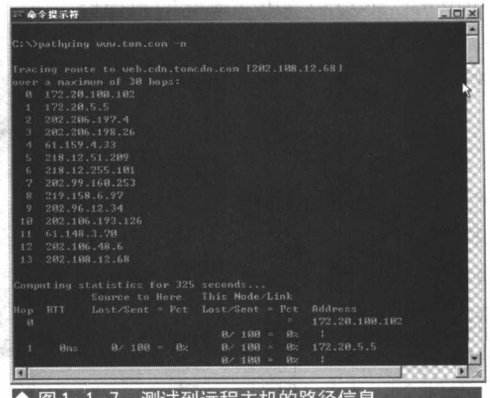
Pathping主要用于提供有关在来源和目标之间的中间跃点处的网络滞后和网络丢失信息。Pathping将多个回响请求消息发送到来源和目标之间的各个路由器一段时间，然后根据各个路由器返回的数据包大小计算其结果。因为pathping显示任何特定路由器或链接的数据包的丢失程度，所以用户可据此确定引起网络问题的路由器或子网。Pathping通过识别路径上的路由器来执行与tracert命令相同的功能。然后，该命令根据指定的时间间隔定期将ping发送到所有路由器，并根据每个路由器的返回数值生成统计结果。

当运行pathping时，将首先显示路径信息。此路径与tracert命令所显示的路径相同。接着，将显示约90 s（该时间随着跃点数的变化而变化）的繁忙消息。在此期间，命令会从先前列出的所有路由器和及其链接之间收集信息。期间结束时将显示测试结果。

从上述结果可以看出所有的路由跃点均无丢失数据包现象，源主机到目标主机的连接是完全正常的。在Address列中所显示的链接丢失速率（以垂直线“|”表示）表明造成路径上转发数据包丢失的链路拥挤状态。



◆ 图1－1－6　显示本地网络路径



◆ 图1－1－7　测试到远程主机的路径信息

四、IP路由表——Route

Route命令主要用于手动配置路由表，如添加或者删除一条路由等，是网络管理工作中应用较多的工具。使用不带参数的route可以显示其帮助信息。

示例1：显示当前路由表中的所有项目。

在命令提示符窗口中输入命令：

Route print

按回车，执行成功，显示如图1-1-8所示结果。由于当前计算机的所有网卡均配置了IP地址，因此所有的这些项目都是自动添加的。

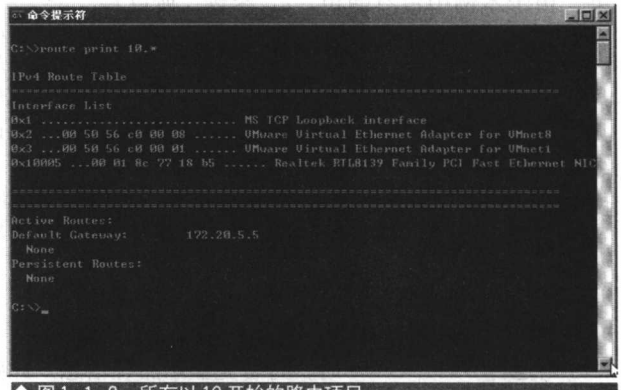
◆ 图1-1-8 当前所有路由项目

示例2：显示IP路由表中以10开始的路由条目。

在命令提示符窗口中输入如下命令：

route print 10.*

按回车，执行成功，显示如图1-1-9所示结果。在route命令中支持通配符应用，删除一系列路由时同样可以使用这种方法。



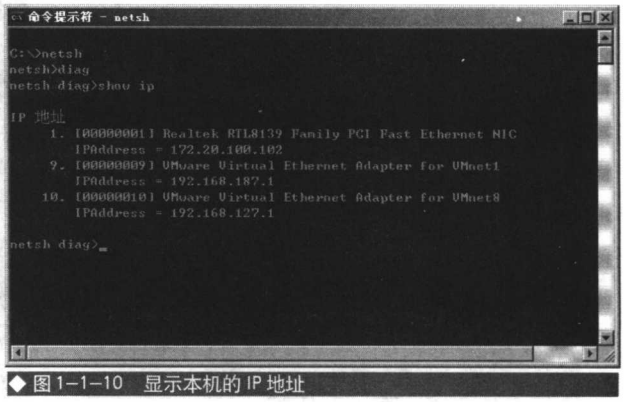
◆ 图1-1-9 所有以10开始的路由项目

五、网络诊断工具——Netsh diagnostic

可以使用Netsh网络诊断命令或诊断环境从命令行管理操作系统和网络服务参数，同时进行相关的疑难解答。Netsh诊断环境的命令提示符是netsh diag>。Netsh diag环境是Windows Server 2003家族的新增内容，因此这些命令将不能在Windows 2000 Server环境下运行。

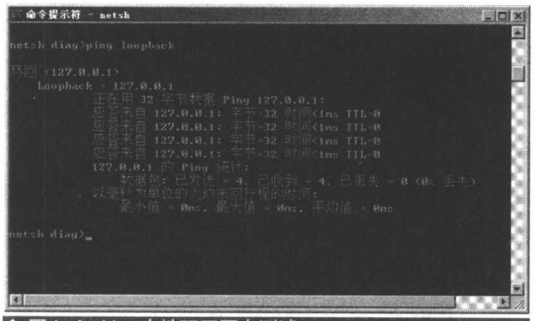
示例1：显示本机所有的IP地址。

首先，在Windows Server 2003的命令提示符窗口中依次输入netsh和diag命令进入netsh diag>环境中，然后输入show ip命令并执行，显示包括本地主机的IP地址和网卡名称，如图1-1-10所示。

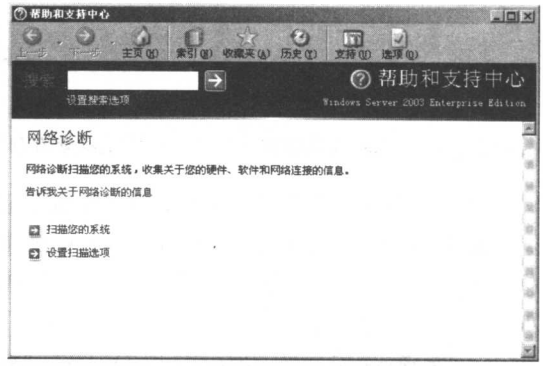


◆ 图1-1-10 显示本机的IP地址

示例2：本地环回网卡测试。



◆ 图1-1-11 本地环回网卡测试



◆ 图1-1-12 诊断网页

在netsh diag>命令行模式下输入ping loopback并执行，如图1-1-11所示。

示例3：启动诊断网页。

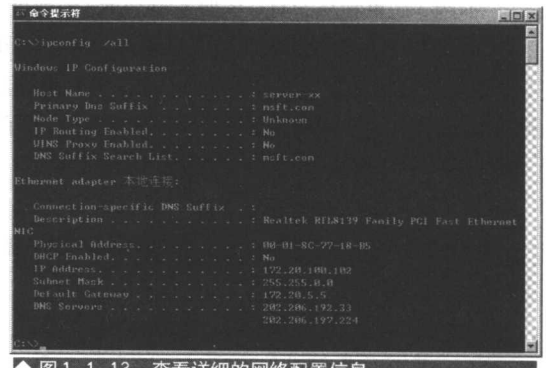
在netsh diag>命令提示符模式下输入gui并执行，即可打开“帮助和支持中心”窗口，网络诊断窗口可以帮助用户扫描当前系统、采集本地硬件、软件以及网络连接的相关信息，如图1-1-12所示。

六、显示IP地址信息——ipconfig

显示所有当前的TCP/IP网络配置值，刷新动态主机配置协议（DHCP）和域名系统（DNS）设置。使用不带参数的ipconfig可以显示所有适配器的IPv6地址或IPv4地址、子网掩码和默认网关。

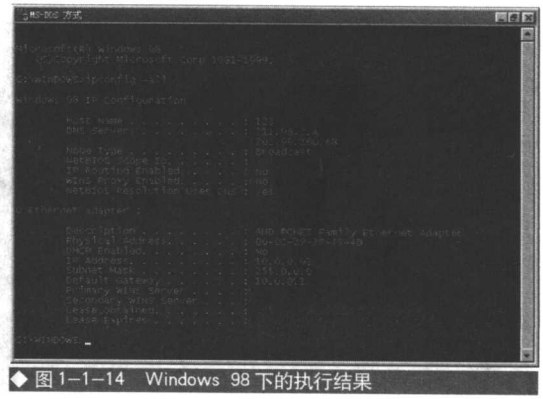
示例1：查看本地计算机的详细网络配置信息。

在命令提示符窗口中输入ipconfig /all并执行，将显示包括所有适配器的IP地址、子网掩码和默认网关，还包括主机的相关配置信息，如主机名、DNS服务器、节点类型、网络适配器的物理地址等，如图1-1-13所示。



◆ 图1-1-13 查看详细的网络配置信息

在Windows 98下执行ipconfig /all命令的结果和Windows XP下略有不同。在Windows 98下的执行结果如图1-1-14所示。



◆ 图1-1-14 Windows 98下的执行结果

示例2：清空DNS缓存。

有的时候有的网站DNS域名没变，但是IP地址变了，这时就需要重新查询DNS服务器，重新建立DNS缓存，否则将连接不到服务器。

在命令提示符下输入命令：

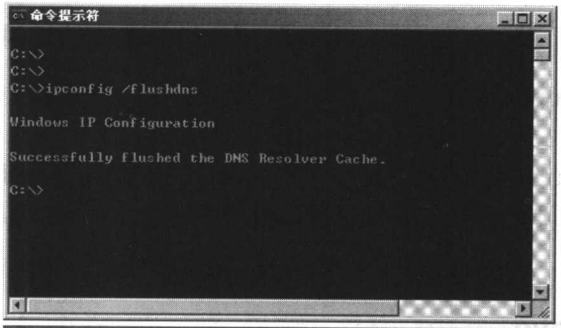
ipconfig /flushdns

刘老师提醒

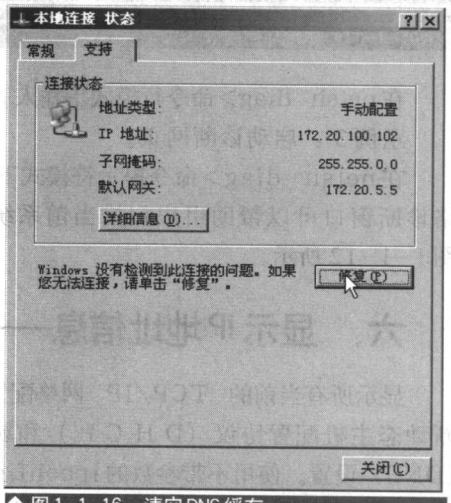
Ipconfig还有一个等价命令——winipcfg，不过winipcfg只能应用于Windows Me、Windows 98和Windows 95系统，并且将以图形界面的方式显示输出结果，同样可以查看到TCP/IP配置的详细信息。

按下回车键，命令成功执行，DNS缓存记录被清空，如图1-1-15所示。

此命令的作用等同于在Windows操作界面下，右键单击托盘区域的“本地连接”小图标，在打开的“本地连接　状态”对话框中选择“支持”选项卡，然后单击“修复”选项，如图1-1-16所示。



◆ 图1-1-15　清空DNS缓存



◆ 图1-1-16　清空DNS缓存

示例3：重新从DHCP服务器获取IP地址。

由于IP地址的租约到期或是手动设置了不正确的IP地址而导致电脑无法上网，这时我们只需让此计算机重新从DHCP服务器获取一下IP地址就行了。

第一步，在命令提示符下输入命令：

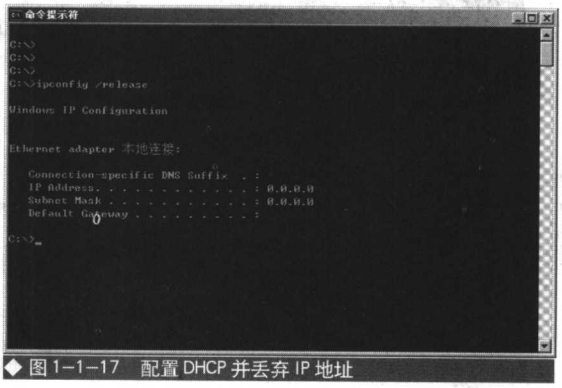
ipconfig /release

回车执行，释放所有适配器或特定适配器的当前DHCP配置并丢弃IP地址配置，如图1-1-17所示。

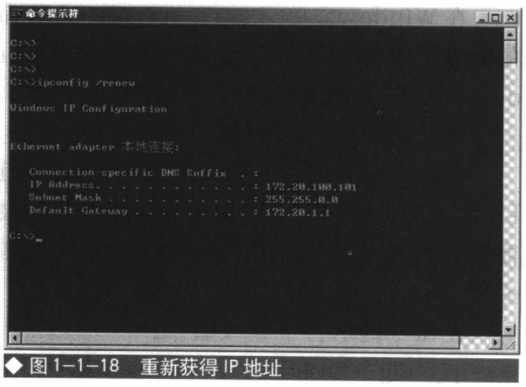
第二步，在命令提示符下输入命令：

ipconfig /renew

按回车执行，重新从DHCP服务器上获取新的IP地址，如图1-1-18所示。



◆ 图1-1-17　配置DHCP并丢弃IP地址



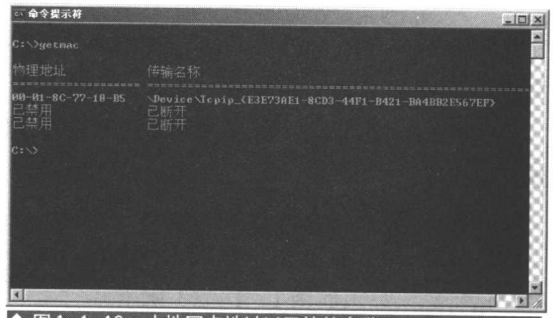
◆ 图1-1-18　重新获得IP地址

七、网卡地址及协议列表工具——GETMAC

Getmac 命令用于返回计算机中所有网卡的媒体访问控制（MAC）地址，以及每个地址的网络协议列表，既可以应用本地计算机，也可以通过网络获取远程主机或者用户计算机的MAC 地址等相关信息。

示例 1 ：获取本机的网卡地址以及协议名称。

在命令提示符窗口中输入getmac 命令并执行，显示如图 1－1－19 所示。



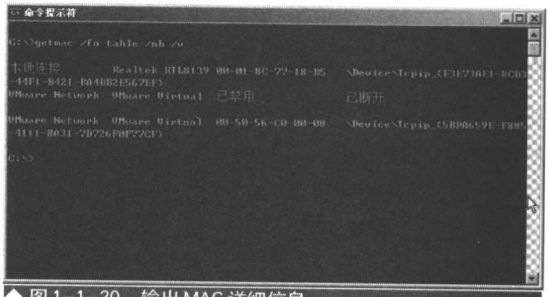
◆ 图 1－1－19　本地网卡地址以及协议名称

示例 2：在本地计算机上以table 的格式输出MAC 的详细信息。

在命令提示符窗口中输入如下命令：

getmac /fo table /nh /v

按回车执行。通过查看得知，本地计算机共有 3 块网卡（每块网卡都具有一个唯一的MAC 地址），其中有一个Vmare 虚拟机网卡被禁用，因此网卡的MAC 地址没有显示，另外一个为Vmare 虚拟机网卡的MAC 地址，如图 1－1－20 所示。



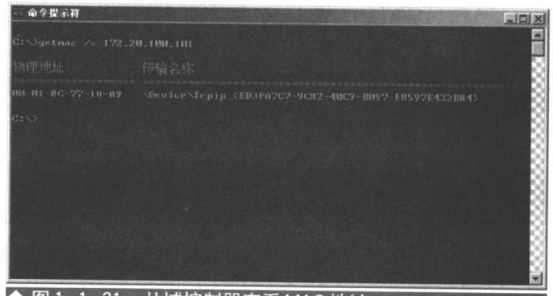
◆ 图 1－1－20　输出 MAC 详细信息

示例 3 ：在域控制器上，查看局域网内IP 地址为172.20.100.101 计算机的网卡MAC 地址。

在命令提示符下输入命令：

getmac /s 172.20.100.101

按回车执行，显示如图 1－1－21 所示。其中目标主机也可以通过计算机名来指定。



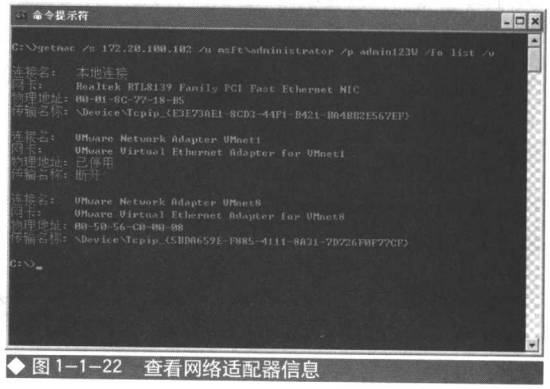
◆ 图 1－1－21　从域控制器查看 MAC 地址

示例 4：查看地址为 172.20.100.102 的远程计算机上域（msft）的用户（Administrator）的网络适配器的详细信息。该示例与上一示例的不同之处在于：上一个示例只能在域控制器上实现，而本例在任何一台联网的计算机上都能实现。

在命令提示符窗口下输入如下命令：

getmac /s 172.20.100.102 /u msft \ administrator /p admin123W /fo list /v

按回车键执行命令，如图 1－1－22 所示。



◆ 图 1－1－22　查看网络适配器信息