电脑应用
疑难解析与技巧系列

黑客攻防

疑难解析与技巧800例

华师傅资讯 编著

讲解黑客攻防原理让黑客无处遁形

识破黑客的各种攻击伎俩

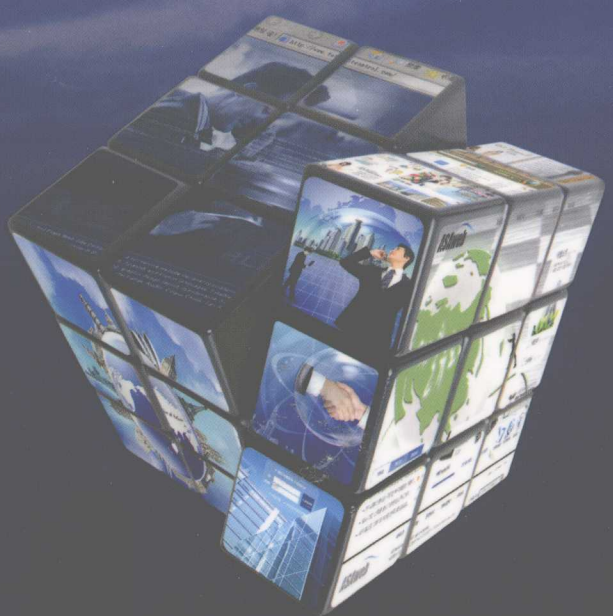
用事实说话

真实地重现黑客攻防实战场面

知己知彼百战不殆

保护网络安全保护个人隐私

放心地享受网络生活



附赠光盘以多媒体教程来帮助学习
附赠光盘中披露黑客攻防常用武器
附赠光盘中收录了其他的实用案例

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

电脑应用
疑难解析与技巧系列

黑客攻防

疑难解析与技巧800例

华师傅资讯 编著

中国铁道出版社
CHINA RAILWAY PUBLISHING HOUSE

内 容 提 要

本书是指导初学者快速掌握黑客攻防操作和应用的入门书籍。书中详细地介绍了初学者必须掌握的基本知识、使用方法和操作步骤，并对初学者在学习过程中经常遇到的问题进行了专家级的指导，以免初学者在起步的过程中走弯路。

本书内容丰富、全面，图文并茂，深入浅出，以图解的方式对每一个入侵步骤都进行了详细的分析，以推测入侵者的入侵目的；对入侵过程中常见的问题进行了必要的说明与解答；并对一些常见的入侵手段进行了比较与分析，以方便读者了解入侵者常用的方式、方法，保障网络安全。本书适合于网络技术爱好者、网络系统管理员阅读，也可作为相关专业学生的参考书。

图书在版编目（CIP）数据

黑客攻防疑难解析与技巧800例/华师傅资讯编著.
北京：中国铁道出版社，2008.6
（电脑应用疑难解析与技巧）
ISBN 978-7-113-08959-7

Ⅰ.黑… Ⅱ.华… Ⅲ.计算机网络－安全技术 Ⅳ.
TP393.08

中国版本图书馆CIP数据核字（2008）第079943号

书　　名：黑客攻防疑难解析与技巧800例
作　　者：华师傅资讯　编著

策划编辑：严晓舟　郑　双
责任编辑：苏　茜　　**编辑部电话：**（010）63583215
封面设计：付　巍　　**封面制作：**白　雪
责任校对：高　爽　　**责任印制：**李　佳

出版发行：中国铁道出版社（北京市宣武区右安门西街8号　　邮政编码：100054）
印　　刷：北京新魏印刷厂
版　　次：2008年9月第1版　　2008年9月第1次印刷
开　　本：787mm×1092mm　1/16　　**印张：**16.5　　**字数：**369千
印　　数：5 000册
书　　号：ISBN 978-7-113-08959-7/TP・2915
定　　价：29.00元（附赠光盘）

前　言

随着计算机网络技术的发展，黑客与网络安全逐渐成为人们关注的热点。怎样认识黑客与防范黑客，保证系统与网络的安全，导致了黑客与反黑客的较量。黑客，或因为“欲望”、“好奇”，或其他原因，经常神出鬼没于黑暗和光明交接的缝隙，利用各种千奇百怪的入侵软件，自由出入于大大小小的公私领域，在用户疏于防范的时候突然现身，叫人防不胜防！如何在网络中生存，成为每个网络使用者必备的基本认识。

在当今这个科技发达的时代，网络在人们的工作、生活和学习中起着重要作用，但目前大多数用户的网络安全知识还很匮乏，在遇到别有用心者的入侵时不知道该如何应对。本书的主要目的就是让读者在尽可能短的时间内，了解黑客入侵原理、常用工具以及攻击方式，并在熟悉基本网络安全知识的前提下，掌握基本的反黑知识、工具和防范技巧，从而揭开黑客的神秘面纱，让广大用户对网络安全高度重视起来，从而采取相关的方法来制定相应的自救措施，“害人之心不要有，防人之心不可无”，也是这个道理。

本书从“攻”、“防”两个不同的角度，通过现实中的入侵实例，并结合作者的心得体会，图文并茂地再现了网络入侵与防御的全过程。本书从内容和层次上可以分为 13 章：第 1 章介绍黑客的入侵命令，培养用户最基本的黑客攻防技能；第 2～3 章讲解针对 Windows 98/Me/NT/2000/XP 操作系统的黑客攻击方式和防范技巧；第 4 章讲解木马的工作原理以及黑客如何利用木马入侵计算机，培养用户封杀木马的技能；第 5 章针对国人最常用的即时聊天工具——QQ 软件，讲解黑客如何盗取号码、QQ 尾巴病毒的发作原理、破解本地加密聊天记录等，分析黑客入侵 QQ 的原理并提出解决办法；第 6～7 章讲解黑客如何入侵系统、邮件、网站及网吧，从而增强用户的防范意识；第 8～10 章讲解如何破解系统、邮箱、程序、文档的密码，从而使用工具进行反入侵；第 11～12 章讲解综合防范技能，封堵黑客可能利用的系统漏洞和端口；第 13 章讲解系统被黑客破坏的情况和如何快速恢复注册表和系统。

本书附带一张精心开发的专业级多媒体教学光盘。它采用了语音讲解、情景式教学、详细的图文对照和真实的情景演示等方式，紧密结合书中的内容对各个知识点进行了深入的讲解，以便于读者快速地对书中的知识点进行消化。同时，本书所涉及的软件全部保存在光盘中，利于读者获取和使用，由于篇幅的缘故，更多的案例不能收录到本书正文中，为此，我们将更多的相关内容和案例附在光盘中，以便于读者随时查阅。

本书由华师傅资讯编著，张燕、吴万军、王利、水淼、张亮、周鹏、李立明、束庆丰、杨杰、朱静、年夫兰、唐国祥、李平、王春燕、尹瑜、刘琢、黄海、冯玉川、吴燕群、潘天、胡平、汪玲、张德友、朱小怀、丁霞共同精心编写而成，由于编者水平有限，书中难免有疏漏和不妥之处，希望广大读者批评指正，联系邮箱：fl05888339@163.com。

本书从保障计算机系统和数据的安全实际需要出发，分析黑客常用的攻击方式和手段，其目的是让更多的读者认识和了解黑客，从而防范黑客，而不是让读者利用黑客技术和手段去攻击别人的计算机系统。因此，最后我们特别声明：利用本书所传授的技术或利用本书光盘中的黑客软件所引起的一切法律和社会后果，由具体行为人负责。

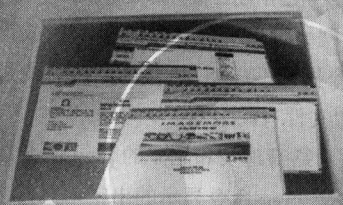
编者

2008 年 5 月

目 录

Chapter 1

剖析黑客入侵命令



黑客世界，风云变幻！黑客王国，谁与争锋！黑客不断敲打着键盘，输入一系列神秘的指令，随着计算机屏幕信息的不断刷新，一个网站可能就这样被黑客入侵了。我们一定很想知道：究竟是什么命令让黑客如虎添翼，有如神助？要揭开黑客的神秘面纱，进入变幻莫测的黑客风云世界，我们先得轻松玩转一些入侵命令。为了了解黑客，我们就从学习各种常用的网络命令开始。

1-1 ping 命令有哪些功能

菜鸟提问：

听说 Windows 系统自带一个功能强大的网络命令：ping。利用 ping 命令可以测试 TCP/IP 协议是否正常工作、测试网络是否畅通。请问 ping 命令有哪些功能？

理论点拨：

ping 是测试网络连接状况以及信息包发送和接收状况非常有用的工具，是网络测试最常用的命令。ping 向目标主机（地址）发送一个数据包，要求目标主机收到后给予答复，从而判断网络的响应时间和本机是否与目标主机（地址）连通。

实战解决：

单击“开始”→“运行”菜单命令，在打开的“运行”对话框中输入 cmd，单击“确定”按钮，可以打开命令提示符窗口，在命令提示符窗口的提示符后输入 ping 命令，按【Enter】键，可以显示 ping 命令的帮助信息，如图 1-1 所示。

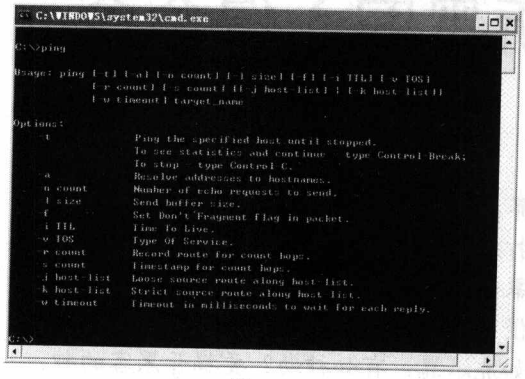


图 1-1

ping 命令有很多功能，在使用 ping 命令时，使用不同的参数，可以进行不同的测试。表 1-1 对 ping 命令的各项参数的功能进行了说明。

表 1-1 ping 命令参数及功能

ping 命令参数	功　能
-t	校验与指定计算机的连接，直到用户中断
-a	将地址解析为计算机名
-n count	发送由 count 指定数量的 ECHO 报文，默认值为 4
-l size	发送包字节的大小，默认值为 32
-f	在包中发送“不分段”标志。该包将不被路由上的网关分段
-i ttl	将“生存时间”字段设置为 ttl 指定的数值
-v tos	将“服务类型”字段设置为 tos 指定的数值
-r count	在“记录路由”字段中记录发出报文和返回报文的路由数量。指定的 count 值最小可以是 1，最大可以是 9
-s count	指定由 count 指定转发次数的时间
-j.host-list	经过由 computer-list 指定的计算机列表的路由报文。中间网关可能分隔连续的计算机（松散的源路由）。允许的最大 IP 地址数目是 9
-k host-list	经过由 computer-list 指定的计算机列表的路由报文。中间网关可能分隔连续的计算机。允许的最大 IP 地址数目是 9
-w timeout	以毫秒为单位指定超时间隔
destination-list	指定要校验连接的远程计算机

当用户不能通过某一应用程序访问远程主机时，可进行如下之一的操作和判断。

（1）如果网络管理员对该远程主机使用 ping 命令进行联机检查，结果成功；接着，在用户端对远程主机执行 ping 命令，结果也成功，则说明网络故障可能是由用户使用的应用程序造成的。

（2）如果网络管理员的 ping 命令执行成功而用户的 ping 命令执行不成功，则故障原因可能是用户端的网络配置文件有问题。

（3）如果网络管理员和用户的 ping 命令都失败了，这时可注意 ping 命令显示的出错信息，这种出错信息通常分为三种情况：

- unknown host（不知名主机）：这种出错信息的意思是该远程主机的名字不能被命名服务器转换成 IP 地址。网络故障可能为命名服务器有故障，或者其名字不正确，或者网络管理员的系统与远程主机之间的通信线路有故障。

- network unreachable（网络不能到达）：这时本地系统没有到达远程系统的路由，可用 netstat-rn 检查路由表来确定路由配置情况。
- no answer（无响应）：远程系统没有响应。这种故障说明本地系统有一条到达远程主机的路由，但却接受不到它发给该远程主机的任何分组报文。这种故障可能是：远程主机没有工作，或者本地或远程主机网络配置不正确，或者本地或远程的路由器没有工作、或者通信线路有故障，或者远程主机存在路由选择问题。

1-2 ping 命令返回信息的含义是什么

菜鸟提问：

当用户在使用 ping 命令时，比如：ping www.163.com，程序就会返回一连串的英文提示信息，这些信息的含义是什么？

理论点拨：

简单地说，ping 就是一个测试程序，按照默认设置，Windows 上运行的 ping 命令发送 4 个 ICMP（网间控制报文协议）回送请求。如果一切正常，每个 32 字节数据，应能得到 4 个回送应答。

实战解决：

在命令提示符窗口的提示符后输入 ping www.163.com，按【Enter】键后，可以显示如图 1-2 所示的信息。

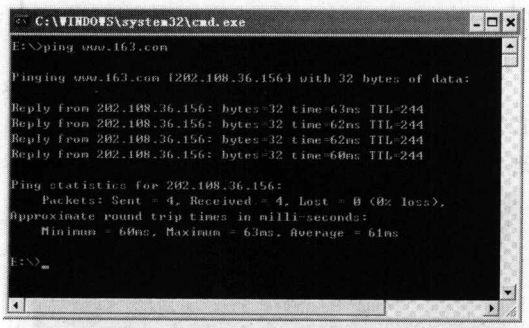


图 1-2

下面我们就来对返回信息一一进行解释：

（1）pinging www.163.com [202.108.36.156] with 32 bytes of data:

正在将 32 字节数据（Windows 默认，但可改变）发送到远程服务器 www.163.com，其后的数字 202.108.36.156 就是该服务器的 IP 地址，所以有时也可用来实现域名与 IP 地址的转换功能。

（2）Reply from 202.108.36.156: bytes=32 time=63ms TTL=244

本地主机已收到回送信息，具体为：32 字节，共用 63ms，TTL 为 244。TTL（Time To Live）是存在时间值。

（3）ping statistics for 202.108.36.156:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milli-seconds:

Minimum = 60ms, Maximum = 63ms, Average = 61ms

对照解释如下：

ping 202.108.36.156 总的信息如下：

数据包个数：发送 4 个数据包（系统默认设置，每次 ping 时向服务器端发送 4 个数据包），共收到 4 个，共丢失 0 个，占总数的 0%。

发送时间总的概括：最快回收时间为 60ms，最慢回收时间为 63ms，平均为 61ms。

1-3 如何判断目标主机的操作系统类型

菜鸟提问：

要入侵远程计算机，首先必须判断计算机的操作系统类型，如何使用 ping 命令判断远程计算机的操作系统类型呢？

理论点拨：

ping 命令能够以毫秒为单位显示发送回请求到回送应答之间的时间量。如果应答时间短，表示数据包不必通过太多的路由器或网络，连接速度会比较快。ping 还能显示 TTL（Time To Live 存在时间）值，可以通过 TTL 值推算一下数据包已经通过了多少个路由器，即源地点 TTL 起始值（就是比返回 TTL 略大的一个 2 的乘方数）减去返回时 TTL 值。例如：返回 TTL 值为 119，那么可以推算数据报离开源地址的 TTL 起始值为 128，所以源地点到目标地点要通过 9 个路由器网段（128-119）；如果返回

TTL 值为 246，TTL 起始值就是 256，源地点到目标地点要通过 10 个路由器网段。所以可以根据 Ping 命令返回的 TTL 值就可以判断远程计算机的操作系统类型。

实战解决：

如果要判断远程计算机 220.170.241.90 的操作系统类型，可以在命令提示符窗口的提示符后运行 ping 220.170.240.90 命令，返回如图 1-3 所示的信息。

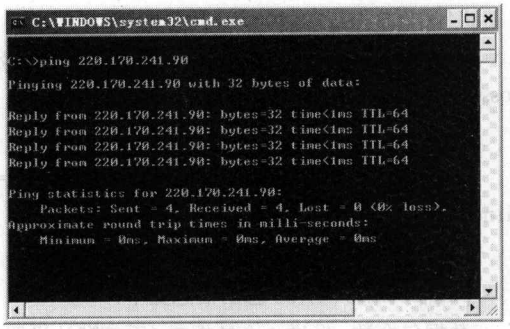


图 1-3

不同的操作系统的主机设置的 TTL 值是不同的，所以利用这个 TTL 值可以帮助识别操作系统类型。一般 Windows 9x/Me 的 ICMP 回显应答的 TTL 值为 32；Windows NT/2000 操作系统 ICMP 回显应答的 TTL 值为 128；Linux Kernel 2.2.x/2.4.x 操作系统的 TTL 值为 64（有的时候使用 ping Windows XP 命令，其 TTL 值是 64 或者 128）；一般 UNIX 及类 UNIX 操作系统的 TTL 值为 255。

根据 TTL 值来判断操作系统类型，有时也不一定正确，因为不排除人为修改 TTL 值而达到欺骗的效果。

1-4 怎样测试网卡是否工作正常

网卡是连网的关键部件，如果网卡损坏或网卡的驱动程序发生错误，则不可能进行连网。在 Windows XP 下，一般通过如下步骤查看网卡驱动是否正常。

第 1 步：在桌面上右击“我的电脑”图标，在弹出的快捷菜单中选择“属性”命令，打开“系统属性”对话框，如图 1-4 所示。

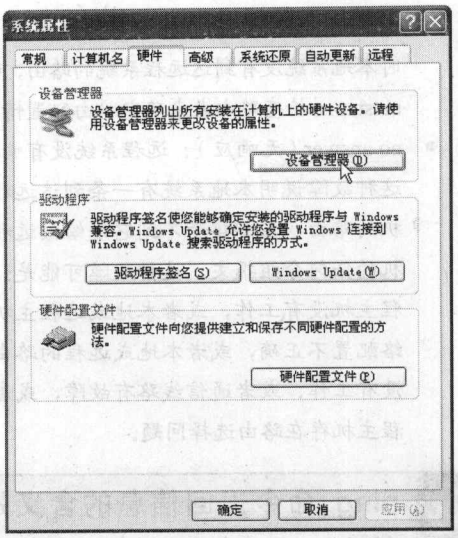


图 1-4

第 2 步：切换到“硬件”选项卡，单击“设备管理器”按钮，即可打开如图 1-5 所示的“设备管理器”窗口，如果在“网络适配器”区域出现红色的叉号或黄色的感叹号，即表示网卡的驱动存在故障，需要重新安装网卡驱动程序。

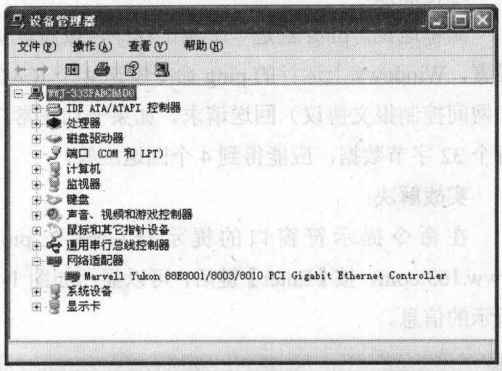


图 1-5

而在命令提示符环境下，可以使用 ping 127.0.0.1 命令快速测试网卡是否正常工作，如果出现如图 1-6 所示的信息即可判断出是网卡故障。

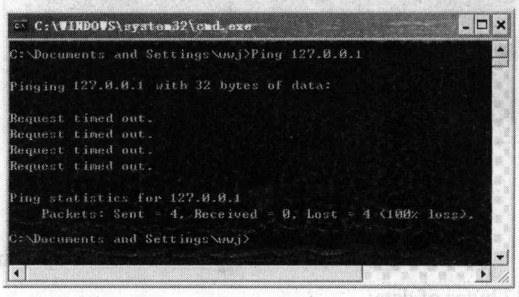


图 1-6

重新安装网卡的驱动程序，使“设备管理器”中的“网络适配器”区域中不存在红色的叉号或黄色的感叹号，再次使用 ping 127.0.0.1 命令测试网卡，出现如图 1-7 所示的信息时，即表示网卡工作正常。

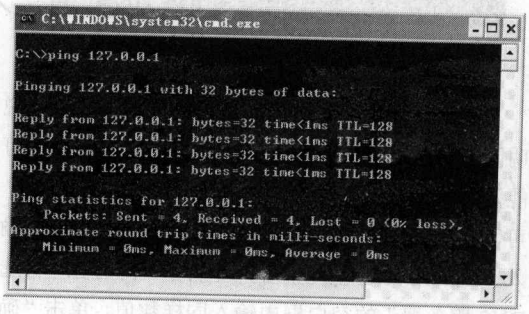


图 1-7

1-5 如何测试网络协议是否工作正常

计算机要正常连接上网络，除了本机正确安装了网卡外，还必须安装 TCP/IP 等协议，在确认网卡正常工作的情况下，可以通过以下步骤查看计算机中已安装的协议。

第 1 步：在桌面上右击“网上邻居”图标，在弹出的快捷菜单中选择“属性”命令，打开“网络连接”窗口，如图 1-8 所示。

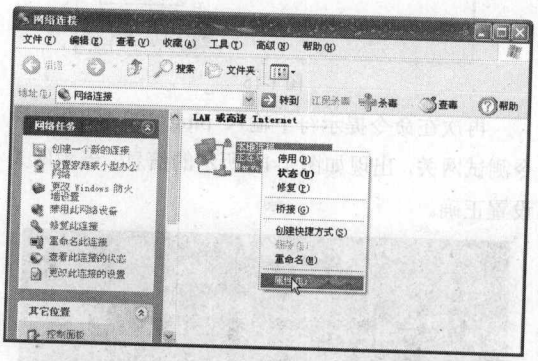


图 1-8

第 2 步：右击“本地连接”图标，在弹出的快捷菜单中选择“属性”命令，打开“本地连接属性”对话框，如图 1-9 所示。

在此对话框中，可以检查是否安装了 TCP/IP 等协议，也可以选中“Internet 协议（TCP/IP）”选项，单击“属性”按钮，在打开的对话框中对协议的属性进行配置。

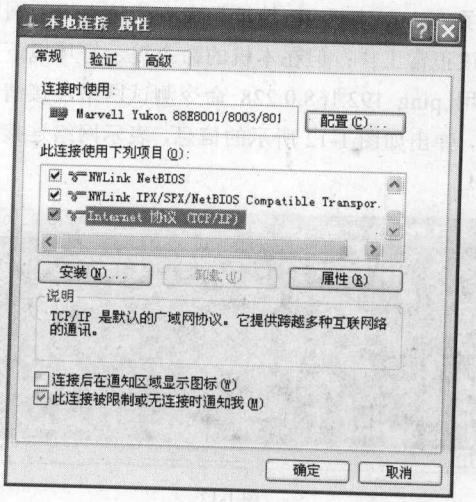


图 1-9

在命令提示符下可以使用“ping 本机 IP 地址”命令快速检测网络协议是否工作正常，出现如图 1-10 所示的界面，表示协议工作正常。

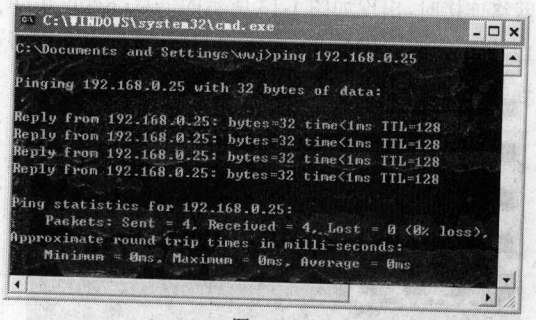


图 1-10

而出现如图 1-11 所示的界面，则表示网络协议不能正常工作，应重新安装或配置网络协议。

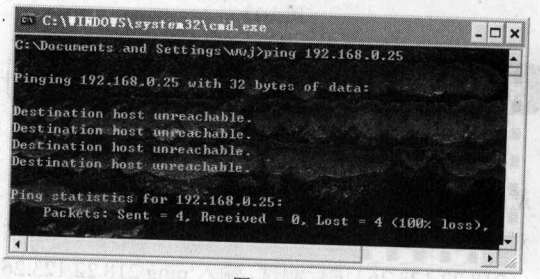


图 1-11

1-6 如何测试网络连接情况

局域网的所有计算机都无法和 IP 为 192.168.0.228 的计算机进行正常通信。事先已经使用了 ping

127.0.0.1 命令，确认本机的网卡正常工作；也使用了“ping 本机 IP 地址”命令确认本机的网络协议正常工作；但在本机的命令提示符环境下，使用 ping 192.168.0.228 命令测试网络连接情况时，弹出如图 1-12 所示的信息，表示网络连接不通。

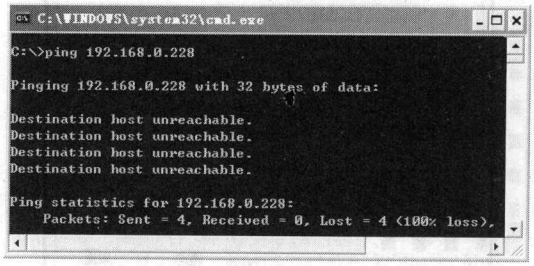


图 1-12

此故障的原因最大的可能是网络之间不通，重新制作网线，并确认网线的水晶头和网卡及路由器正常连接，再一次使用 ping 192.168.0.228 命令测试网络连接时，出现如图 1-13 所示的信息：Reply from 127.0.0.1: bytes=32 time<1ms TTL=128 即表示网络连接正常。

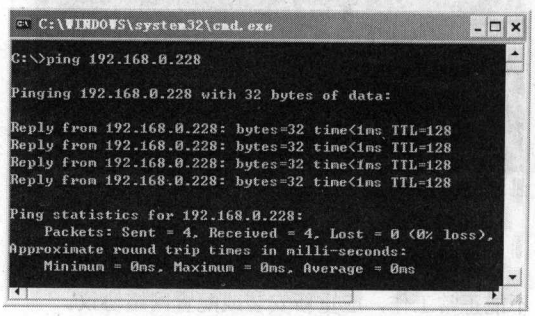


图 1-13

1-7 如何测试网关

计算机能够和局域网中的其他计算机正常通信，但是不能访问互联网，在命令提示符下对某一网站 www.ABCD.com 的 IP 地址（218.22.123.26）进行测试，输入 ping 218.22.123.26 命令并按【Enter】键，出现如图 1-14 所示的结果，说明网络不通。

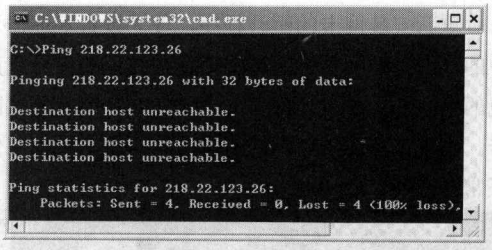


图 1-14

既然计算机能够访问局域网的其他计算机，说明网卡和网络协议正常工作，从故障现象分析，可能是网关配置不当。已知网关地址为 192.168.0.1，可以在“Internet 协议（TCP/IP）属性”对话框中输入正确的网关地址，如图 1-15 所示，同时在“首选 DNS 服务器”的空白框内输入同样数值，单击“确定”按钮。

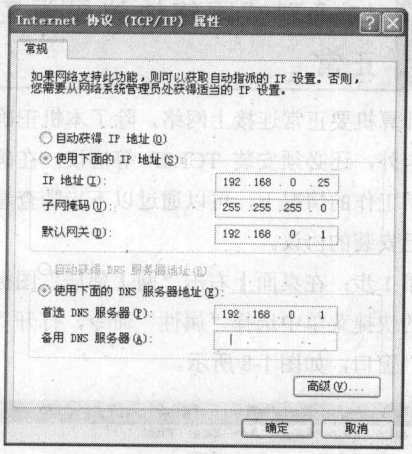


图 1-15

再次在命令提示符下输入 ping 192.168.0.1 命令测试网关，出现如图 1-16 所示的信息，表示网关设置正确。

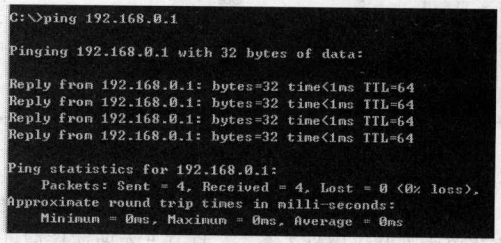


图 1-16

提示 如果无法知道网络的 IP 地址，也可以直接对网址进行测试，输入网址即可，如 Ping www.ABCD.com。