局域网无敌手丛书

- 局域网故障的分类、局域网故障的诊断方法和故障排除工具
- Windows 98 对等网故障、Windows 2000 / XP / 2003 故障、无盘工作站故障、Internet 常见故障、无线局域网故障

局域网故障排除

许文胜 等编著

上海科学技术出版社

·局域网无敌手丛书·

局域网故障排除

许文胜　等编著

上海科学技术出版社

内容提要

本书采用问答形式，根据“观察分析故障现象—查找故障原因—排除故障”的思路，详细介绍局域网故障的分类、局域网故障诊断的方法、局域网故障排除工具、网络硬件设备故障、Windows 98 对等网故障、Windows 2000/XP/2003 故障、无盘工作站疑难故障、Internet 常见故障和无线局域网典型故障等的排除方法和技巧。

本书适用于中小企业网络管理员、网吧管理人员和学校机房管理员，是立志成为网络管理员的网络新手不可或缺的、必备的常用工具书之一。

图书在版编目(CIP)数据

局域网故障排除/许文胜等编著. —上海：上海科学技术出版社，2004.11

（局域网无敌手丛书）

ISBN 7-5323-7804-7

Ⅰ.局… Ⅱ.许… Ⅲ.局域网络—故障修复

Ⅳ.TP393.107

中国版本图书馆CIP数据核字（2004）第107648号

世纪出版集团
上海科学技术出版社 出版、发行

（上海瑞金二路450号 邮政编码200020）

苏州望电印刷有限公司印刷

新华书店上海发行所经销

开本787×1092 1/16 印张10.5 字数 256000

2004年11月第1版 2004年11月第1次印刷

印数 1—5200

定价：22.00元

前　言

本书系局域网无敌手丛书（共三册）中的第三册。

在本丛书的前两册《局域网基础与实战》和《局域网管理与维护》中已经系统地讲述了局域网组建与管理的相关知识。但在实际使用中我们总会碰到这样或那样的问题，参照前两册的叙述，一些问题可以解决，也有一些问题无法解决。

本书正是针对那些问题，根据笔者多年的实践经验并参照有关著作写成。本书从局域网故障现象和诊断方法入手，全面介绍了引起局域网各种典型故障现象的原因以及故障的排除方法和技巧。本书叙述简捷，针对性强，内容精，容量大。希望能对广大读者有所裨益。

本书分为两大部分，前面的理论部分介绍了局域网故障的分类、局域网故障的诊断方法和故障排除工具；后面的实例部分则采用问答的形式，以一个个实例来分析各种局域网故障的排除。

在写作方面，以理论为线，以实例为面，线面结合，让读者在实例中学习相关的理论知识；在内容上力求实用性、可操作性，让读者在实际工作中少走弯路，快速全面地掌握排除局域网故障的技能；在结构布局上力求结构清晰。

本书由许文胜等编著，参加编写的老师还有黄兰娟、黄丽萍和苏风华等。在本书的写作过程中，还得到了其他很多朋友的帮助，在此一并表示由衷的感谢。

编　者

2004 年 9 月

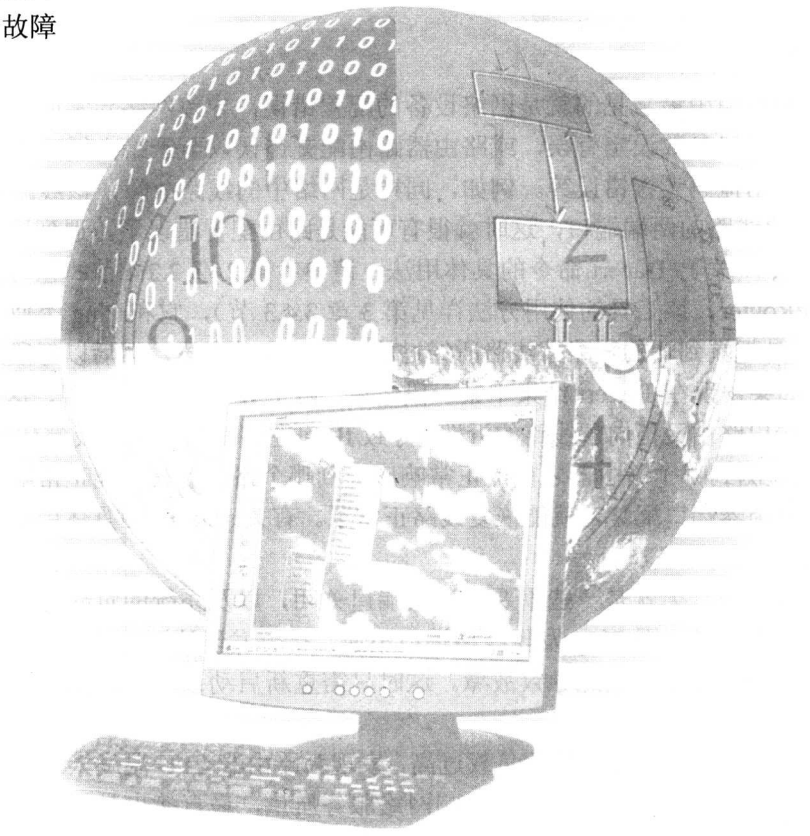
目 录

第1章　局域网故障的分类

根据故障的性质不同，网络故障可分为物理故障与逻辑故障；根据故障对象的不同，网络故障可分为线路故障、路由器故障、主机故障；按照引起故障的不同原因，网络故障可划分为连通性故障、网络协议故障、配置故障和安全故障等。

通过学习本章的内容，读者应该掌握以下知识点。

- 物理故障
- 逻辑故障
- 线路故障
- 路由器故障
- 主机故障
- 连通性故障
- 网络协议故障
- 配置故障
- 安全故障



1.1 按照网络故障的不同性质划分

网络故障按照不同性质，可分为物理故障和逻辑故障两类。

1. 网络物理故障

网络物理故障指的是因设备或线路损坏、插头松动、线路受到严重电磁干扰等情况产生的网络故障。例如，网络管理员发现网络某条线路突然中断，首先用 Ping 命令（关于 Ping 命令的具体用法，请参考第 2 章 2.2 节）检查线路在网管中心这边是否连通。Ping 一般一次只能检测一端到另一端的连通性，而不能一次检测一端到多端的连通性。

如果连续几次 Ping 都出现“Request time out”信息，表明网络不通。这时去检查端口插头是否松动，或者网络插头是否误接；这种情况经常是没有搞清楚网络插头规范或者没有弄清网络拓扑规划的情况下导致的。

另一种情况，例如两个路由器直接连接接口不正确，这时应该将一台路由器的出口连接另一台路由器的入口，或者这台路由器的入口连接另一路由器的出口才行。当然，集线器 Hub、交换机、多路复用器也必须连接正确，否则也会导致网络中断。还有一些网络连接故障很隐蔽，要诊断这种故障没有什么特别好的工具，一般只有依靠经验丰富的网络管理员了。

2. 网络逻辑故障

网络逻辑故障中最常见的就是网络设备的配置错误，导致网络异常或故障。配置错误可能是路由器端口参数设定有误，或路由器路由配置错误以至于路由循环或找不到远端地址，或者是路由掩码设置错误等。例如，同样是网络中的线路故障，该线路没有流量，但又可以 Ping 通线路的两端端口，这时就很有可能是路由配置错误了。遇到这种情况，通常用 Tracert 命令（关于 Tracert 命令的具体用法，请参考第 2 章 2.2.4 节；也可用“路由跟踪程序”TraceRouter，该工具的使用方法详见第 3 章 3.4.3 节），它和 Ping 类似，最大的区别在于 Tracert 是把端到端的线路按线路所经过的路由器分成多段，然后以每段返回响应与延迟来检测。如果发现在 Tracert 结果中某一段之后，两个 IP 地址循环出现，这时，一般就是线路远端把端口路由又指向了线路的近端，导致 IP 包在该线路上来回反复传递。不用担心，Tracert 可以检测到哪个路由器之前能正常响应，到哪个路由器就不能正常响应了。这时只需更改远端路由器端口配置，就能恢复线路正常了。有关 tracert 的具体用法，请参见本书第 2 章的相关内容。

逻辑故障的另一类就是一些重要进程或端口关闭，以及系统的负载过高。例如同样是线路中断，没有流量，用 Ping 发现线路端口不通，检查发现该端口处于 down 的状态，这就说明该端口已经关闭，因此导致故障。这时只需重新启动该端口，就可以恢复线路的连通了。

还有一种常见情况是路由器的负载过高，表现为路由器 CPU 温度太高、CPU 利用率太高，以及内存剩余太少等，如果因此影响网络服务质量，最直接也是最好的办法就是更换路由器，换个好点的。

1.2 按照故障的不同对象划分

网络故障根据故障的不同对象也可以划分为：线路故障、路由器故障、主机故障。

1. 线路故障

线路故障最常见的情况就是线路不通，诊断这种情况首先检查该线路上流量是否还存在，然后用 Ping 检查线路远端的路由器端口能否响应，用 Tracert（跟踪路由）程序检查路由器配置是否正确，找出问题逐个解决。

2. 路由器故障

事实上，线路故障中很多情况都涉及到路由器，因此也可以把一些线路故障归结为路由器故障。检测这种故障，需要利用 MIB 变量浏览器，用它收集路由器的路由表、端口流量数据、计费数据、路由器 CPU 的温度、负载以及路由器的内存余量等数据。通常情况下网络管理系统有专门的管理进程不断地检测路由器的关键数据，并及时给出报警。

注意

路由器 CPU 温度过高十分危险，因为这可能导致路由器的烧毁；而路由器 CPU 利用率过高和路由器内存余量太小都将直接影响到网络服务的质量。解决这种故障，只有对路由器进行升级、扩充内存等，或者重新规划网络拓扑结构。

3. 主机故障

主机故障常见的现象就是主机的配置不当。像主机配置的 IP 地址与网上其他主机冲突，或 IP 地址根本就不在子网范围内，由此导致主机无法连通。主机的另一故障就是安全故障，比如，主机没有控制其上的 finger、RPC、rlogin 等多余服务，而攻击者可以通过这些多余进程的正常服务或 bug 攻击该主机，甚至得到 Administrator 的权限等。

注意

不要轻易地共享本机硬盘，因为这将导致恶意攻击者非法利用该主机的资源。发现主机故障一般比较困难，特别是别人的恶意攻击。一般可以通过监视主机的流量、扫描主机端口和服务来防止可能的漏洞。最后提醒大家不要忘了安装防火墙，因为这是最省事也是最安全的办法。

1.3 按照引起故障的原因划分

根据引起故障的原因，可以将局域网故障分为 4 类：连通性故障、网络协议故障、配置故障和安全故障。

1. 连通性故障

● 常见故障现象

出现连通性故障，通常可以表现出以下一些故障现象：

◆ 工作站无法登录服务器。

◆ 连入 Internet 的局域网中的计算机无法访问 Internet。
◆ 工作站无法通过“网上邻居”看到或者访问局域网中的其他计算机。
◆ 工作站无法使用网络共享资源以及共享打印机。
◆ 在未感染病毒、未受到攻击情况下，局域网中的部分或全部工作站运行速度异常缓慢。

● 常见故障原因

通常上述现象主要由以下几种原因引起：

◆ 网卡未安装，或未安装正确，或与其他设备有冲突。
◆ 网卡本身出现物理故障。
◆ 没有安装或没有正确安装相应的网络协议。
◆ 网线、跳线或插座等连通性设备没有正确安装，或者出现故障。
◆ 集线器没有打开电源，或者出现物理故障，或者相应的通信端口出现故障。
◆ 路由器没有打开电源，或者出现物理故障，或者相应的通信端口出现故障。
◆ 交换机没有打开电源，或者出现物理故障，或者相应的通信端口出现故障。
◆ UPS 电源出现故障。

2. 网络协议故障

（1）常见故障现象

如果局域网中使用的网络协议出现故障，则会呈现出以下一些故障现象：

◆ 网络中的工作站无法登录服务器。
◆ 工作站无法通过网上邻居看到局域网中的其他计算机。
◆ 工作站可以在“网上邻居”中能看到其他计算机，但无法访问。
◆ 工作站在“网上邻居”中找不到任何计算机，也无法访问共享资源。
◆ 连入 Internet 的局域网中的计算机无法访问 Internet。
◆ 局域网中出现工作站重名。

● 常见故障原因

产生网络协议故障的原因主要有以下几种：

◆ 网卡没有安装或者安装错误。
◆ 没有安装所需网络协议（组建局域网首先需要安装 TCP/IP 协议，如果要实现局域网通信，还需安装 NetBEUI 协议）。
◆ 相应的网络协议配置不正确（例如，要安装 TCP/IP 协议会涉及到 4 个参数的设置，也就是 IP 地址、子网掩码、DNS 域名解析服务以及网关，任何一个设置都必须完全正确）。
◆ 在组建局域网时或维护过程中人为修改，造成一个或多个计算机重名。

3. 配置故障

这里主要指的是系统、工具软件中的配置内容。在组建局域网的过程中将涉及到名目繁多的种种配置，如系统相应参数的配置（共享资源的访问权限、用户维护、管理的权限等）、使用工具软件的配置（代理服务器的设置、局域网通信工具的配置等）。切不可由于系统、工具软件的配置简单易行，就轻率为之。配置不当，小则导致某些资源无法使用，

大则导致整个网络瘫痪。因此，系统、软件配置问题需要引起用户的足够重视。当系统或工具软件配置出现问题时，通常会表现出以下一些故障现象：

- ◆ 某些工作站无法和其他部位工作站实现通信。
- ◆ 工作站无法访问任何其他设备。
- ◆ 只能 Ping 通本机。
- ◆ 当局域网连入 Internet 时，用 Ping 命令检测正常，但无法上网浏览。

4. 安全故障

安全故障通常表现为感染病毒、黑客入侵、安全漏洞等几个方面。当局域网连入 Internet 时，出现安全故障的概率大大提高，当然也不排除在局域网内部的“交叉感染”，甚至恶意攻击。

第2章　局域网故障诊断的方法

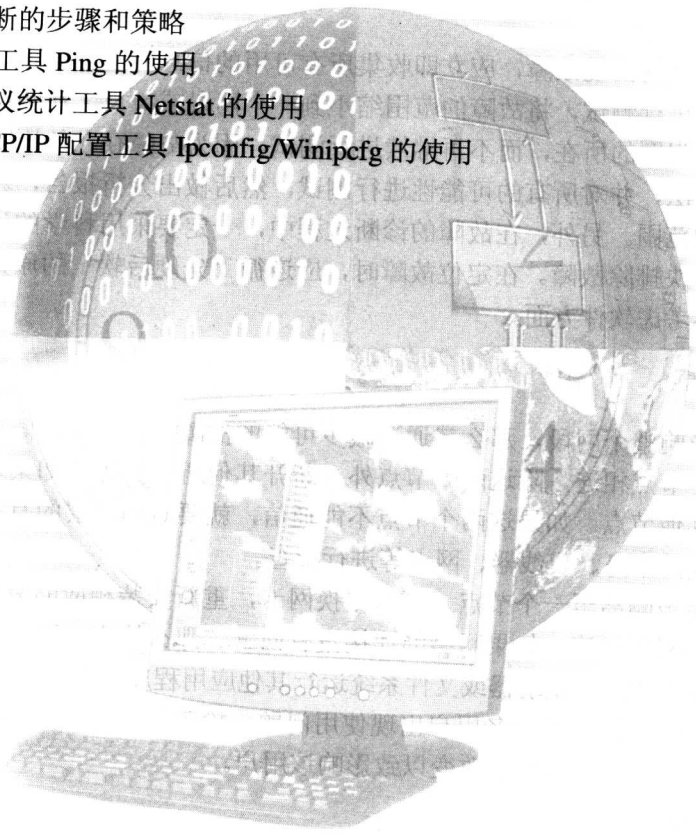
组建好局域网后，还需要保证局域网稳定、正常地运行，这样用户才能放心地利用局域网进行工作。但不可避免地，局域网总会因为这样那样的原因而产生各种各样不同类型的故障，这些故障和问题如果不及时解决，将会影响局域网的正常运行，严重时还会导致系统的瘫痪。所以在局域网出现问题的时候，迅速准确地诊断出故障并加以排除是十分重要的。

局域网的故障可以说是千奇百怪，即使小小的设置不当，也可能造成整个网络的瘫痪，因此诊断、排除故障的方法绝不能一概而论，需要局域网管理者针对具体的故障现象对症下药。故障的诊断与排除的准确与否、速度快慢等，都和用户平时积累的经验息息相关，掌握一些常见的故障诊断、排除方法可以大大提高工作的效率。

本章从故障诊断的步骤和策略入手，以网络测试工具为武器，介绍诊断和排除局域网故障的方法，希望能起到抛砖引玉的作用。

通过学习本章内容，读者应掌握以下知识：

- 故障诊断的步骤和策略
- IP 测试工具 Ping 的使用
- 网络协议统计工具 Netstat 的使用
- 测试 TCP/IP 配置工具 Ipconfig/Winipcfg 的使用



2.1 故障诊断的步骤和策略

局域网故障的诊断应从故障现象出发，确定网络故障范围，查找问题的根源，排除网络故障，快速恢复局域网的正常运行。

建议局域网管理员在排除故障时，能够随时记录各种故障现象以及相应的测试、排除方法，久而久之，就会积累下解决网络故障的“一笔宝贵财富”。

2.1.1 分析故障现象

故障现象是网络故障的表象体现，不同的故障原因一般会产生不同的故障现象。在发生局域网故障时，需要请操作人员对故障现象进行详细的描述。最好能够亲自操作一下，以便仔细分析所出现的问题，并且检查一下在故障发生之前操作人员是否对局域网的配置进行了改动，或执行了一些与网络无关的操作，这些都有可能导致网络故障的产生。

2.1.2 定位故障范围

由于一些本质不同的故障其现象却非常相似，因此仅通过表面现象，往往无法非常准确地将故障归类、定位。

一旦确认局域网出现故障，应立即收集所有可用的信息并进行分析。对所有可能导致错误的原因逐一进行测试，将故障的范围缩小到一个网段或节点。在测试时，不能根据一次的结果就断定问题的所在，而不再继续进行测试。因为故障存在的原因可能不只一处，使用尽可能的方法，并对所有的可能性进行测试，然后做出分析报告，剔除非故障因素，缩小故障发生的范围。另外，在故障的诊断过程中，一定要采用科学的诊断方法，以便提高工作效率，尽快排除故障。在定位故障时，应遵循“先硬后软”的原则，即先确定硬件是否有故障，再考虑软件方面。

2.1.3 隔离故障

如果故障影响整个网段，那么就通过减少可能的故障源来隔离故障，例如，将可能的故障源仅与一个节点相连，除这两个节点外，断开其他所有节点。如果这两个节点能正常通信，再增加其他节点。如果这两个节点不能通信，就要对物理层的有关部分，如双绞线的接头、双绞线的本身、集线器、网卡等进行检查。

如果故障能被隔离至一个节点，可以更换网卡，重新安装相应的驱动程序，或是用一条新的双绞线与网络相连。如果网络的连接没有问题，那么检查一下是否只是某一个应用程序有问题，使用相同的驱动器或文件系统运行其他应用程序，与其他节点比较配置情况，试用该应用程序。如果只是一名用户出现使用问题，检查涉及该节点的网络安全系统。检查是否对网络的安全系统进行了改变以致影响该用户。

2.1.4 排除故障

经过反复的测试，确定了故障源，那么识别故障的类型还是比较容易的。对于网络硬

件设备来说，最方便、快速的措施就是进行更换，对于损坏部分的维修可以以后再进行。

对于软件故障来说，有两种方法可以解决：第一种是重新安装有问题的软件，删除可能有问题的文件，并且要确保拥有全部所需的文件；第二种是对软件进行重新设置，如果问题是单一用户的问题，通常最简单的方法是整个删除该用户，然后从头开始，或是重复必要的步骤，为该用户重新安装原来有问题的软件。相对于无目标地进行检查，执行逻辑有序的这些步骤，重新配置系统可以更快地解决问题。

2.2 网络测试工具

网络管理员诊断和排除局域网故障时就像医生一样，除了望闻问切之外，还需要借助于有关工具进行故障的诊断。这些工具，既有软件工具，也有系统命令，功能各异，各有长处。本节将介绍几种常用的网络测试工具。

2.2.1 IP 测试工具 Ping

Ping 是 Windows 98/NT/2000/XP/2003 中集成的一个专用于 TCP/IP 协议网络中的测试工具，Ping 命令用于查看网络上的主机是否在工作，它是通过向该主机发送 ICMP ECHO_REQUEST 包进行测试而达到目的的。一般凡是使用 TCP/IP 协议的网络，当发生计算机之间无法访问或网络工作不稳定时，都可以试用 Ping 命令来确定问题的所在。

提示

ICMP 是“Internet Control Message Protocol”（Internet 控制消息协议）的缩写。它是 TCP/IP 协议族的一个子协议，用于在 IP 主机、路由器之间传递控制消息，ICMP ECHO_REQUEST 是指 ICMP 回响请求。

Ping 命令把 ICMP ECHO_REQUEST 包发送给指定的计算机，如果 Ping 成功了，则 TCP/IP 把 ICMP ECHO_REQUEST 包发送回来，其返回的结果表示是否能到达主机、向主机发送一个返回数据包需要多长时间。使用 Ping 可以确定 TCP/IP 配置是否正确以及本地计算机与远程计算机是否正在通信。

1. Ping 命令的格式

Ping 命令格式：Ping 目的地址 [-t][-a][-n Count][-1 Size][-f][-i TTL][-v TOS][-r Count][-s Count][｛-j HostList | -k HostList｝][-w Timeout][-R][-S SrcAddr][-4][-6]

其中目的地址是指被测试计算机的 IP 地址或计算机名称。各种参数的含义如下：

- -t：指定在中断前 Ping 可以向目的地持续发送回响请求信息。要中断并显示统计信息，请按 Ctrl+Break 组合键；要中断并退出请按 Ctrl+C 组合键。
- -a：指定对目的地 IP 地址进行反向名称解析。如果解析成功，Ping 将显示相应的主机名。
- -n Count（计数）：指定发送回响请求消息的次数。默认值是 4。
- -1 Size（长度）：指定发送的回响请求消息中“数据”字段的长度（以字节为单位）。默认值为 32。Size 的最大值是 65527。

- -f：指定发送的“回响请求”中其 IP 头中的“不分段”标记被设置为 1（只适用于 IPv4）。“回响请求”消息不能在到目标的途中被路由器分段。该参数可用于解决“路径最大传输单位（PMTU）”的疑难。
- -i TTL：指定回响请求消息的 IP 数据头中的 TTL 段值。其默认值是主机的默认 TTL（生存时间 TTL 是 IP 协议包中的一个值，它告诉网络路由器包在网络中的时间是否太长而应被丢弃）值。TTL 的最大值为 225。
- -v TOS：指定发送的“回响请求”消息中的 IP 标头中的“服务类型（TOS）”字段值（只适用于 IPv4）。默认值是 0。TOS 的值是 0～255 之间的十进制数。
- -r Count：指定 IP 标头中的“记录路由”选项用于记录由“回响请求”消息和相应的“回响回复”消息使用的路径（只适用于 IPv4）。路径中的每个跃点都使用“记录路由”选项中的一项。如果可能，可以指定一个等于或大于来源和目的地之间跃点数的 Count。Count 的最小值必须为 1，最大值为 9。
- -s Count：指定 IP 数据头中的“Internet 时间戳”选项用于记录每个跃点的回响请求消息和相应的回响应答消息的到达时间。Count 的最小值是 1，最大值是 4。对于链接本地目标地址是必需的。
- -j HostList（目录）：指定“回响请求”消息对于 HostList 中指定的中间目标集在 IP 标头中使用“稀疏来源路由”选项（只适用于 IPv4）。使用稀疏来源路由时，相邻的中间目标可以由一个或多个路由器分隔开。HostList 中的地址或名称的最大数为 9，HostList 是一系列由空格分开的 IP 地址（带点的十进制符号）。
- -k HostList：指定“回响请求”消息对于 HostList 中指定的中间目标集在 IP 标头中使用“严格来源路由”选项（只适用于 IPv4）。使用严格来源路由时，下一个中间目的地必须是直接可达的（必须是路由器接口上的邻居）。HostList 中的地址或名称的最大数为 9，HostList 是一系列由空格分开的 IP 地址（带点的十进制符号）。
- -w Timeout（超时）：指定等待回响应答消息响应的时间（以毫秒计），该回响应答消息响应接收到的指定回响请求消息。如果在超时时间内未接收到回响应答消息，将会显示“请求超时”的错误消息。
- -R：指定应跟踪往返路径（只适用于 IPv6）。
- -S SrcAddr（源地址）：指定要使用的源地址（只适用于 IPv6）。
- -4：指定将 IPv4 用于 Ping。不需要用该参数识别带有 IPv4 地址的目标主机，仅需要按名称识别主机。
- -6：指定将 IPv6 用于 Ping。不需要用该参数识别带有 IPv6 地址的目标主机，仅需要按名称识别主机。

用户可以通过在 MS-DOS 提示符下运行“Ping”或“Ping /？”命令来查看 Ping 命令的格式及参数，如图 2-1 所示。

2. Ping 命令的应用

在局域网的维护中，经常使用 Ping 命令来测试一下网络是否通畅。使用 Ping 命令检查局域网上计算机的工作状态的前提条件是：局域网中计算机必须已经安装了 TCP/IP 协议，并且每台计算机已经配置了固定的 IP 地址。应用 Ping 命令的操作步骤如下：

图 2-1　Ping 命令的格式及参数

（1）在 MS-DOS 提示符下，输入 Ping 测试的目标计算机的 IP 地址或主机名，如要测试一台 IP 地址为 192.168.0.2 的客户机与服务器是否已连网，可以在局域网中任意一台计算机中运行 Ping 192.168.0.2。

（2）按回车键，如果客户机上 TCP/IP 协议工作正常，则会以 DOS 屏幕方式显示类似“Reply from IP 地址：bytes=32 time<1ms TTL=64”信息，如图 2-2 所示。

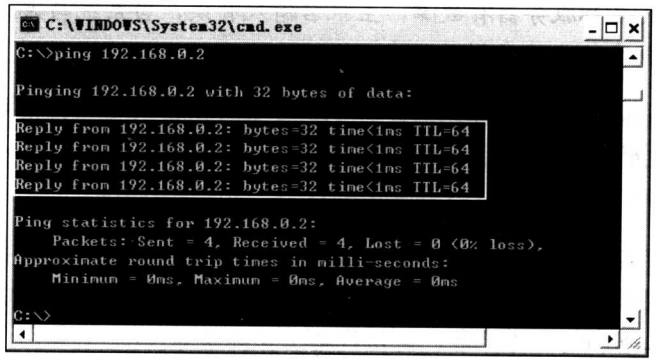


图 2-2　Ping 192.168.0.2 成功信息

（3）如果网络未连接成功，则显示“Request Time out（请求超时）”信息，如图 2-3 所示。

出现以上错误提示的情况时，就要仔细分析一下网络故障出现的原因和可能有问题的网上节点了，可以从以下几个方面来着手检查。

- ◆ 网卡是否安装正确，IP 地址是否被其他用户占用。
- ◆ 检查本机和被测试的计算机的网卡及交换机（集线器）显示灯是否为亮，来判断是否已经连入整个网络中。
- ◆ 是否已经安装了 TCP/IP 协议，TCP/IP 协议的配置是否正常。
- ◆ 检查网卡的 I/O 地址、IRQ 值和 DMA 值，是否与其他设备发生冲突。

如果还是无法解决，建议用户重新安装和配置 TCP/IP 协议。