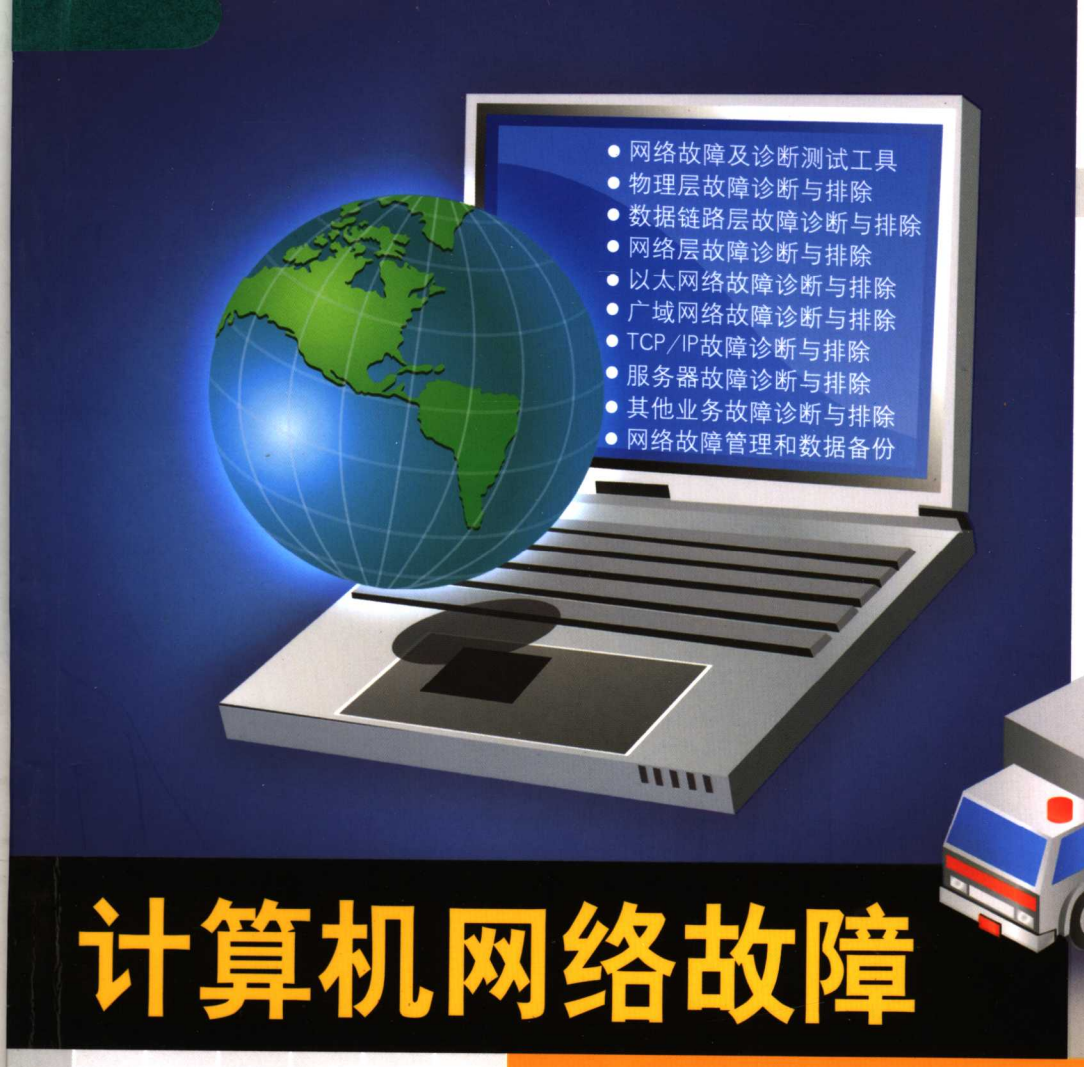

计算机网络故障诊断与排除

潘朝阳　曾劲柏　茆爱军　黎连业　编著

清华大学出版社

计算机网络故障诊断与排除

潘朝阳　曾劲柏
茆爱军　黎连业　编著

清华大学出版社
北　京

内 容 简 介

本书介绍了计算机网络管理过程中所需要的知识。全书由 10 章组成，内容包括网络故障和网络诊断测试工具，物理层故障诊断与排除，数据链路层故障诊断与排除，网络层故障诊断与排除，以太网络故障诊断与排除，广域网络故障诊断与排除，TCP/IP 故障诊断与排除，服务器故障诊断与排除，其他业务故障诊断与排除，以及网络故障管理和数据备份。

本书取材新颖，内容丰富，实用性强，叙述由浅入深、循序渐进，内容系统全面、重点突出，概念清楚易懂，是一本实用性很强的图书。

本书为中科院计算所培训中心计算机网络故障诊断与故障排除课程指定教材，也可供计算机和通信网络管理人员、工程技术人员阅读、参考，还可作为网络管理培训班、高等院校相关专业的教材和教学科研人员的参考书。

图书在版编目(CIP)数据

计算机网络故障诊断与排除/潘朝阳等编著. —北京：清华大学出版社，2007.4

ISBN 978-7-302-14654-4

Ⅰ.计…　Ⅱ.潘…　Ⅲ.①计算机网络—故障诊断 ②计算机网络—故障修复　Ⅳ.TP393.07

中国版本图书馆 CIP 数据核字(2007)第 018895 号

责任编辑：刘金喜
封面设计：久久度文化
版式设计：康　博
责任校对：胡雁翎
责任印制：何　芊
出版发行：清华大学出版社　　**地　　址**：北京清华大学学研大厦 A 座
http://www.tup.com.cn　**邮　　编**：100084
c-service@tup.tsinghua.edu.cn
社 总 机：010-62770175　**邮购热线**：010-62786544
投稿咨询：010-62772015　**客户服务**：010-62776969
印 刷 者：北京季蜂印刷有限公司
装 订 者：北京市密云县京文制本装订厂
经　　销：全国新华书店
开　　本：185×260　**印　张**：18.5　**字　数**：416 千字
版　　次：2007 年 4 月第 1 版　　**印　　次**：2007 年 4 月第1 次印刷
印　　数：1～5000
定　　价：28.00 元

前　言

本书是基于计算机网络管理过程中所需要的知识而展开的。对物理层故障、数据链路层故障、网络层故障、以太网络故障、广域网络故障、TCP/IP 故障、服务器故障、网络故障管理和数据备份等进行了详细的讨论。本书所叙述的内容是全面的，基本上反映了网络故障诊断与故障排除所需要的知识，它是作者多年来网络管理经验和教学经验的总结。

本书内容丰富、实用，是一本非常好的参考书。无论是对网络管理人员还是工程技术人员，都是十分有用的。

全书由 10 章组成，它们是：

第 1 章　网络故障和诊断测试工具；
第 2 章　物理层故障诊断与排除；
第 3 章　数据链路层故障诊断与排除；
第 4 章　网络层故障诊断与排除；
第 5 章　以太网络故障诊断与排除；
第 6 章　广域网络故障诊断与排除；
第 7 章　TCP/IP 故障诊断与排除；
第 8 章　服务器故障诊断与排除；
第 9 章　其他业务故障诊断与排除；
第 10 章　网络故障管理和数据备份。

本书是在潘朝阳同志“网络故障诊断与故障排除”培训教学内容的基础上，并参考了培训班中部分学员交换的技术资料编写的。

本书由潘朝阳、曾劲柏编写，黎连业统稿，茆爱军参加了部分写作工作，李淑春、黎娜和黎萍做了大量的录入校对、插图等工作。

在本书的写作过程中，得到了许多热心朋友、公司的支持和帮助以及同行者的支持，尤其是王兆康、王长富等同志提出了许多有益的建议，中科院计算所培训中心为本书的写作提供了许多方便，王健华校长对书稿得以顺利出稿提供了大力支持，马建跃、张久军同志对本书提出了许多修改意见，借此机会对上述同志一并表示感谢！

本书非常适合网络管理人员、工程技术人员和大学生阅读和参考，同时可供从事计算机、通信、网络等工作的人员阅读和参考，也可以作为各类培训班的教材。

由于水平有限，书中难免有不当之处，敬请读者批评指正。服务邮箱：wkservice@tup.tsinghua.edu.cn。

编著者

目　录

第 1 章　网络故障和网络诊断测试工具

本章重点介绍以下内容：

- 网络故障概述；
- 常用的网络故障测试命令；
- 网络故障管理系统；
- 网络故障诊断；
- 网络故障管理；
- 网络故障的定位；
- 网络诊断工具；
- 网络测试工具。

1.1　网络故障概述

在信息化社会里，各企事业单位对网络的依赖程度越来越高，网络随时都可能发生故障，影响正常工作。所以，必须掌握相应的技术及时排除故障。有些单位如电信、电子商务公司、游戏运营商等使用的网络一旦发生故障，若不能及时排除，会产生很大的损失。这些单位一般会安装网络故障管理软件，通过软件来管理和排除网络的故障。从网络故障本身来说，经常会遇到的故障有：

- 物理层故障；
- 数据链路层故障；
- 网络层故障；
- 以太网络故障；
- 广域网络故障；
- TCP/IP 故障；
- 服务器故障
- 其他业务故障等。

那么，网络发生故障的原因是什么呢？根据有关资料的统计，网络发生故障具体分布为：

- 应用层占 3%；
- 表示层占 7%；
- 会话层占 8%；
- 传输层占 10%；
- 网络层占 12%；
- 数据链路层占 25%；
- 物理层占 35%。

引起网络故障的原因还有以下几种：

(1) 网络管理员差错

网络管理员差错占整个网络故障的 5%以上，主要发生在网络层和传输层，是由于安装没有完全遵守操作指南，或者网络管理员对某个处理过程没有给予足够的重视造成的。

(2) 海量存储问题

数据处理故障的最主要原因是硬盘问题。据有关报道，大约有超过 26%的系统失效都归结到海量存储的介质故障上。

(3) 计算机硬件问题

大约有 25%的故障是由计算机硬件引起的，如显示器、键盘、鼠标、CPU、RAM、硬盘驱动器、网卡、交换机和路由器等。

(4) 软件问题

软件引起的故障也不鲜见，表现为：

- 软件有缺陷，造成系统故障；
- 网络操作系统缺陷，造成系统失效。

(5) 网络问题

网络故障的原因是多方面的，如线缆、连接器件、网卡、网桥、交换机或路由器的模块出现故障。

(6) 使用者发生的差错

使用者没有遵守网络赋予的权限。例如：

- 超权访问系统和服务；
- 侵入其他系统；
- 操作其他用户的数据资料；
- 共享账号；
- 非法复制。

既然有网络故障产生，那么就有网络管理。

网络故障管理一般包括 5 点：

- 对网络进行监测，提前预知故障；
- 发生故障后，找到故障发生的位置；
- 解决故障；

- 记录故障产生的原因，找到解决方法；
- 故障分析预测。

1.2　常用的网络故障测试命令

常用的网络故障测试命令有 ipconfig、ping、tracert、netstat 和 nslookup 等。下面简单说明它们的基本用法。

1. ipconfig 命令

使用 ipconfig 命令可以查看 IP 配置，或配合使用/all 参数查看网络配置情况。

单击“程序”→“运行”，输入 CMD 进入 DOS 命令行窗口，在 DOS 命令行窗口中输入 ipconfig /all，会显示出如图 1-1 所示画面。

```
C:\Documents and Settings\Administrator>ipconfig /all

Windows 2000 IP Configuration

        Host Name . . . . . . . . . . . . : zhangjj
        Primary DNS Suffix  . . . . . . . :
        Node Type . . . . . . . . . . . . : Hybrid
        IP Routing Enabled. . . . . . . . : Yes
        WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter internet连接:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : CNC Enternet P.P.P.o.E
        Physical Address. . . . . . . . . : 44-45-53-54-77-77
        DHCP Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 221.219.16.58
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 221.219.16.58
        DHCP Server . . . . . . . . . . . : 1.1.1.1
        DNS Servers . . . . . . . . . . . : 202.106.46.151
                                            202.106.0.20
        Lease Obtained. . . . . . . . . . : 2005年12月5日 9:47:59
        Lease Expires . . . . . . . . . . : 2038年1月19日 11:14:07
```

图 1-1　输入 ipconfig /all 命令弹出的画面

在图 1-1 中显示出了本机 TCP/IP 配置情况。如果显示出的 IP 地址不在网络的网段中，本机则无法与其他机器通信；如果网关、DNS 配置有误，则本机不能访问外网计算机，也不能上网。

使用/release 和/renew 参数重新从 DHCP 服务器上获取 IP 地址。

2. ping 命令

在 DOS 命令窗口中输入 ping /? ，可以看到 ping 的各个参数如下：

```
C:\Documents and Settings\Administrator>ping /?
```

```
Usage: ping [-t] [-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS]
            [-r count] [-s count] [[-j host-list] | [-k host-list]]
            [-w timeout] destination-list
Options:
    -t              Ping the specified host until stopped
                    To see statistics and continue - type Control-Br
                    To stop - type Control-C
    -a              Resolve addresses to hostnames
    -n count        Number of echo requests to send
    -l size         Send buffer size
    -f              Set Don't Fragment flag in packet
    -i TTL          Time To Live
    -v TOS          Type Of Service
    -r count        Record route for count hops
    -s count        Timestamp for count hops
    -j host-list    Loose source route along host-list
    -k host-list    Strict source route along host-list
    -w timeout      Timeout in milliseconds to wait for each reply
```


1) ping 命令参数介绍

- /t

ping 指定的计算机直到中断。

- /a

将地址解析为计算机名。

```
C:\Documents and Settings\Administrator>ping -a 159.254.188.86
Pinging lily [159.254.188.86] with 32 bytes of data:
```

通过运行 ping -a 159.254.188.86 可以知道 IP 为 159.254.188.86 的计算机名是 lily。

- -n count

发送 count 指定的 echo 数据包数。默认值为 4。

- -l size

发送包含由 size 指定的数据量的 echo 数据包。默认值为 32 字节，最大值是 65 527。

- -f

在数据包中发送“不要分段”标志，数据包就不会被路由上的网关分段。

- -i TTL

将“生存时间”字段设置为 TTL 指定的值。

- -v TOS

将“服务类型”字段设置为 TOS 指定的值。

- -r count

在“记录路由”字段中记录传出和返回数据包的路由。count 可以指定最少 1 台，最多 9 台计算机。

- -s count

指定 count 指定的跃点数的时间戳。

- -j host-list

利用 host-list 指定的计算机列表路由数据包。连续计算机可以被中间网关分隔(路由稀疏源)，IP 允许的最大数量为 9。

- -k host-list

利用 host-list 指定的计算机列表路由数据包。连续计算机不能被中间网关分隔(路由严格源)，IP 允许的最大数量为 9。

- -w timeout

指定超时间隔，单位为毫秒。

2) 使用 ping 命令测试故障的步骤

现在有一台计算机不能访问 Internet 上的 Web 服务器，我们可以使用 ping 命令找出故障的位置。操作步骤如下：

(1) ping 159.0.0.1。

如果 ping 不通，则说明本机 TCP/IP 没有装好。

(2) ping 本机的 IP 地址。

如果 ping 不通，则说明网卡没有装好，或网卡驱动有问题。

(3) ping 本网段的其他设备 IP 地址。

如果 ping 不通，则说明连接本机的线路有问题，或者是交换机的端口有问题，也有可能是交换机本身出了问题。

(4) ping 本网段的网关。

如果 ping 不通，则无法上网，因为没有设备能把数据包转发出去。原因可能是路由器没有配置好或代理服务器出了问题。

(5) ping DNS 服务器。

如果 ping 不通，则说明 DNS 服务器出了问题，或本机的 DNS 服务器设置不正确。

3. tracert 命令

Tracert 命令用来检验数据包是通过什么路径到达目的地的。通过执行 tracert 命令，可以清楚地看到数据走的路径。当 ping 一个较远的主机出现错误时，用 tracert 命令可以方便地查出数据包是在哪里出错的。如果信息包一个路由器也不能穿越，则有可能是计算机的网关设置错了。那么，可以用 ipconfig 命令来查看。

4. winipcfg 命令

winipcfg 命令的功能与 ipconfig 的基本相同，只是 winipcfg 在操作上更加方便，同时能够以 Windows 的图形界面方式显示。当需要查看任何一台机器上 TCP/IP 协议的配置情况时，选择“开始”→“运行”，在出现的对话框中输入 winipcfg，即可出现测试结果。

5. netstat 命令

利用该命令可以显示有关统计信息和当前 TCP/IP 网络连接的情况，用户或网络管理人员可以得到非常详尽的统计结果。当网络中没有安装特殊的网管软件，但要详细地了解网络的整个使用状况时，netstat 命令是非常有用的。

netstat 命令的语法格式是：netstat[-参数 1][-参数 2]……

其中主要参数有：

- -a:

显示所有与该主机建立连接的端口信息。

- -n:

以数字格式显示地址和端口信息。

- -e:

显示以太网的统计信息，该参数一般与 S 参数共同使用。所显示的内容中，Discards 表示不能处理而被废弃的信息包数，Errors 表示坏掉的信息包数。这些数值大时，很可能是集线器、电缆和网卡等硬件发生了故障。另外，网络太拥挤也可能导致这些数值的增大。

- -s:

显示每个协议的统计情况。如果想要统计当前局域网中的详细信息，可通过输入 netstat -e -s 来查看。

6. nslookup 命令

nslookup，命令一般是用来确认 DNS 服务器动作的。nslookup 有多个选择功能，在命令行输入“nslookup <主机名>”并执行，即可显示出目标服务器的主机名和对应的 IP 地址，称之为正向解析。若失败了，可能是执行 nslookup 命令的计算机的 DNS 设置错了，也有可能是所查询的 DNS 服务器停止或工作异常。还有一种情况，虽然返回了应答，但一和该服务器通信就失败。这多数是目标服务器停止工作，但也有可能 DNS 服务器保存了错误的信息。在 DNS 服务器出现问题时，有时可能只能进行正向解析，无法进行逆向解析。此时，只需执行 nslookup 命令，看是否输出目标主机名即可。

1.3 网络故障管理系统

使用 ping 的方法只能针对小型网络，在一些大型网络中一般使用网络故障管理软件，一个网络的故障管理系统不但能反应网络平常运行时的故障情况，更应该能在发生重大网络故障时，快速准确地报告、定位和排除故障。

网络故障管理系统包括：

- Navis NFM 故障管理系统；

- Netcool 故障管理系统。

Navis NFM(Network Fault Management)网络故障管理系统是朗讯科技网络运行系列软件中最著名的产品。其功能强大，能够提供实时故障监测和相关处理，快速定位故障，关联故障，并可提供多厂家、多技术和多业务区的集中管理。另外，“现成的方案”可以快速进行工程实施，并提供本地化的客户和技术支持。

Navis NFM 核心功能包括：

- 告警信息采集、浏览、过滤、分类等。
- 支持信息压缩，可根据信息发生的次数、数值、时间和分组进行压缩。
- 告警门限设置和级别升级（Critical、Major、Minor、Other、Cleared）。
- 自动的告警通知和告警处理功能(寻呼、发送电子邮件、生成工单、网元重新启动等)。
- 多种颜色的故障信息显示和图形化的网络地图显示。
- 支持开放的接口和 API(ASCII、SNMP v1-v3、CORBA、X.25、TL1)。
- 远端登录到网元和网元管理系统。

NFM 可以根据用户的级别，实现分权和分级管理。系统管理员可以为不同的用户设置不同的权限，只定义该用户关心的网元的故障信息的浏览、查找、操作和远程登录等功能。每个用户用自己的账户登录系统后，只能看到权限之内的信息，以及执行被允许的各种操作。同时，NFM 还备有用户使用记录，从而实现对人员使用情况的管理，加强对整个系统的安全保障。

NFM 提供强大的告警抑制功能，可以对非告警类报告提供过滤；根据各种门限进行告警抑制；告警恢复后，NFM 可以自动清除原告警，并将其转入已清除告警中；对告警进行域内、域间的相关性处理等，从而大幅度地减少告警的数量，并有效地减少了分析故障根源所花费的时间。

用户还可以将客户信息和服务相关数据集成到 Navis NFM 数据库，NFM 可实时地显示与故障相关的客户和服务数据信息，产生针对特定客户和服务的故障报告，并在故障影响客户之前对其进行评估。

信息时代的来临，使得计算机网络技术迅速普及和不断发展，作为信息社会的基础设施，无论各级行政机关、科研院所，还是部队、学校、企事业单位都十分重视它的建设和使用。为了更好地发挥计算机网络的作用，更好地利用已有的网络资源，就必须做好网络故障修复工作。一般的网络故障修复对网络管理员来说当然简单，但是专业的、深层次的网络故障只有经过专业训练，并借助专业软件和工具才能诊断，并最终排除。

1.4　网络故障诊断

网络故障诊断是管好、用好网络，使网络发挥最大作用的重要技术工作。

网络故障诊断是从故障现象出发，以网络诊断工具为手段获取诊断信息，确定网络故障点，查找问题的根源，排除故障，恢复网络的正常运行。

网络故障通常有以下几种可能：

- 物理层中物理设备相互连接失败或者硬件和线路本身的问题；
- 数据链路层的网络设备的接口配置问题；
- 网络层网络协议配置或操作错误；
- 传输层的设备性能或通信拥塞问题；
- 网络应用程序错误。

诊断网络故障的过程应该沿着 OSI 7 层模型从物理层开始向上进行。首先检查物理层，然后检查数据链路层，以此类推，确定故障点。

1.4.1 故障诊断步骤

故障诊断的步骤如下：

(1) 确定故障的具体现象，分析造成这种故障现象的原因。例如，主机不响应客户请求服务。可能的故障原因是主机配置问题、接口卡故障或路由器配置命令丢失等。

(2) 收集需要的用于帮助隔离可能故障原因的信息。从网络管理系统、协议分析跟踪、路由器诊断命令的输出报告或软件说明书中收集有用的信息。

(3) 根据收集到的情况考虑可能的故障原因，排除某些故障原因。例如，根据某些资料可以排除硬件故障，把注意力放在软件原因上。

(4) 根据最后的可能故障原因，建立一个诊断计划。开始仅用一个最可能的故障原因进行诊断活动，这样可以容易恢复到故障的原始状态。如果一次同时考虑多个故障原因，试图返回故障原始状态就困难多了。

(5) 执行诊断计划，认真做好每一步的测试和观察，每改变一个参数都要确认其结果。分析结果确定问题是否解决，如果没有解决，继续下去，直到故障现象消失。

1.4.2 故障排除过程

在开始动手排除故障之前，在记事本上将故障现象认真仔细记录下来，观察和记录时一定要注意细节，因为有时正是一些最小的细节使整个问题变得明朗化。

1. 识别故障现象

作为管理员，在排除故障之前，必须确切地知道网络上到底出了什么毛病。知道出了什么问题并能够及时识别，是成功排除故障最重要的步骤。为了与故障现象进行对比，必须知道系统在正常情况下是怎样工作的，反之，是不好对问题和故障进行定位的。

识别故障现象时，应该向操作者询问以下几个问题：

(1) 当被记录的故障现象发生时，正在运行什么进程(即操作者正在对计算机进行什么操作)?

(2) 这个进程以前运行过吗?

(3) 以前这个进程的运行是否成功?

(4) 这个进程最后一次成功运行是什么时候?

(5) 从那时起哪些发生了改变?

带着这些疑问来了解并分析问题才能对症下药来排除故障。

2. 对故障现象详细描述

当处理由操作员报告的问题时，对故障现象的详细描述显得尤为重要。如果仅凭他们的一面之词，有时还很难下结论，这时就需要网管员亲自操作出错的程序，并注意出错信息。例如，在使用 Web 浏览时，无论输入哪个网站都返回“该页无法显示”之类的信息。使用 ping 命令时，无论 ping 哪个 IP 地址都显示超时连接信息等。诸如此类的出错消息会为缩小问题范围提供许多有价值的信息。对此在排除故障前，可以按以下步骤执行：

(1) 收集有关故障现象的信息。

(2) 对问题和故障现象进行详细的描述。

(3) 注意细节。

(4) 把所有的问题都记下来。

(5) 不要匆忙下结论。

3. 列举可能导致错误的原因

作为网络管理员，则应考虑导致无法查看信息的原因可能有哪些，如网卡硬件故障、网络连接故障、网络设备(Hub)故障、TCP/IP 协议设置不当等。这里需要注意的是：不要着急下结论，可以根据出错的可能性把这些原因按优先级别进行排序，一个个先后排除。

4. 缩小搜索范围

对所有列出的可能导致错误的原因逐一进行测试，而且不要根据一次测试，就断定某一区域的网络是运行正常或是不正常。另外，也不要在自己认为已经确定了的第一个错误上停下来，应直到测试完为止。

除了测试之外，网络管理员还要注意：千万不要忘记去看一看网卡、Hub、Modem、路由器面板上的 LED 指示灯。通常情况下 LED 指示灯：

- 绿灯表示连接正常(Modem 需要几个绿灯和红灯都要亮);
- 红灯表示连接故障;
- 不亮表示无连接或线路不通;
- 长亮表示广播风暴;