



第7章 网络故障诊断与维护

- 网络故障诊断概述
- 网络故障的分类
- 网络故障的分层检查
- 网络故障诊断的方法
- 网络故障诊断的工具
- 常见的网络故障及解决方法



网络故障诊断概述

1. 网络故障诊断的目的

- 确定网络的故障点，恢复网络的正常运行。
- 发现网络规划和配置中的瑕疵，改善和优化网络的性能。
- 观察网络的运行状况，及时预测网络通信质量。

2. 网络故障产生的原因

- (1) 物理层问题，由于物理设备相互连接失败或者硬件及线路本身引起的问题。
- (2) 数据链路层问题，包括网络设备接口的配置等问题。
- (3) 网络层问题，由于网络协议配置或操作引起的错误。
- (4) 传输层问题，由于性能或通信拥塞引起超时等问题。
- (5) 应用层问题，包括操作系统、网络应用程序自身中的软件错误。。

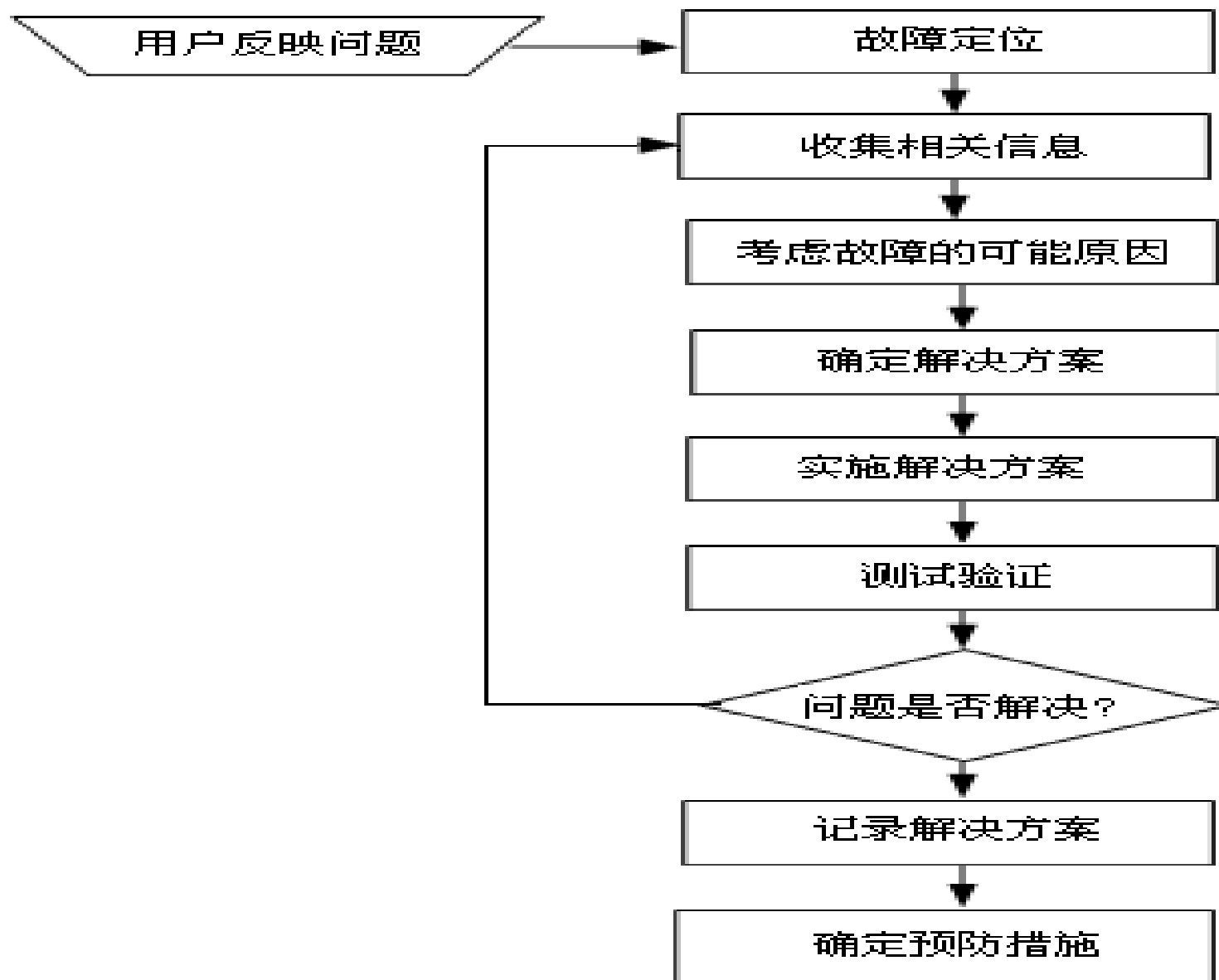


3. 故障排除的方法

- OSI的层次结构为管理员分析和排查故障提供了非常好的组织方式。因而一般使用逐层分析和排查的方法。
- 通常有两种逐层排查的方式
 - 从低层开始排查，适用于物理网络不够成熟稳定的情况，如组建新的网络、重新调整网络线缆、增加新的网络设备；
 - 从高层开始排查，适用于物理网络相对成熟稳定的情况，如硬件设备没有变动。无论哪种方式，最终都能达到目标，只是解决问题的效率有所差别而已。



4. 一般网络故障排除的步骤





第1步：故障的定位

在开始工作之前，应该首先思考下面的问题：

- 周围的用户是否遇到了相同的问题？
- 整个楼宇内其它地方的情况如何？
- 故障出现在所有的应用程序中还是在特定的程序中？
- 更换到另外一台设备后，故障是否仍然存在？



第2步：全面收集相关信息

- 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。
- 收集和了解如下的信息：
 - 以前工作是否正常
 - 观察网络设备的指示灯
 - 故障发生的时间
 - 是否发生了任何改变
 - 不要忽视一些明显的问题
 - 确定正常的工作方式



第3步：考虑分析故障的可能原因

- 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。
- 目标是要建立一张引发故障的事件列表：在故障分析前一步中，应该排除那些不可能引发故障的因素。必要时，还可以回到上一步，收集更多的信息。建立了一张引发故障的事件列表之后，可以调查、排除或确认每一种故障原因



第4步：建立诊断计划

- 在做故障诊断计划时必须考虑：
 - 开始仅用一个可能的故障原因进行诊断活动，来观察这种改变对问题的影响；
 - 要有一种手段可以把所做的改变恢复为原状。
- 在设计某一种解决方案之前考虑的问题：
 - 所确定的原因是否真是故障原因所在。这要经过诊断测试来最后确定。
 - 是否可以对设定的解决方案进行充分的测试，要制定故障的诊断计划。
 - 设定的解决方案应该提出什么样的结果。
 - 所设定的解决方案对于网络的其他部分是如何处理的。
 - 回答这些问题是否需要附加的帮助。



在实施方案前需要完成如下工作：

- 保存全部的网络设备配置文件。
- 对工作站的配置文件进行备份记录。
- 记录配线室的结构，包括设备的位置及其各设备之间的网线的连接（包括设备的端口）等。
- 建立最终的基准，以便对新旧结果进行对比，同时需要在需要恢复时可以作为比较的依据。



第5步：实施解决方案

○实施诊断计划及测试。

在测试过程中，应该设计一些中间环节，以便可以在一些关键点进行测试，而不是对整个解决方案的测试过程结束之后再对结果作出评价。逐步对一些个别进行测试远比对整个解决方案进行测试要简单的多。解决应用问题的一种较好的方法是制定一个逐步执行的计划，以便于能够对中间环节进行测试。



- 确定了故障源，通过测试最后确定了故障发生的原因

- 硬件问题：

- 简单地更换，对损坏部分的维修可以在以后进行。尽可能迅速地恢复网络的所有功能是故障诊断的目的。

- 软件故障：

- 重新安装有问题的软件，删除可能有问题的文件；
- 对软件进行重新的设置。



第6步：测试验证解决方案，即检验故障是否被排除

- 故障是否被排除，要通过操作人员的测试验证。检验故障是否依然存在，这可以确保是否整个故障都已被排除。只是简要地按正常方法操作有关网络设备即可，同时快速地执行其它几种正常操作。要记录相关的信息。有时解决一个地方的问题会引出别处的问题；有时问题是解决了，但也有可能会掩盖其它故障。



第7步：记录解决方案、确定预防措施

- 需要将测试过程中的相关记录以及测试步骤整合成一篇记录文献或文档。
- 通过记录文档可以方便解决类似问题。
- 记录文献或文档应该包括所有与故障相关的信息，如故障的定位、解决方法、操作过程与步骤及测试手段等内容。
- 一个成熟的网络管理机构一般都制定有一整套完整的故障管理日志记录机制。



当完成了故障排除和文献记录等工作之后，就应该着手制定预防措施，以防止同样的故障再次发生。例如，假若故障是由于某种通过网络传播的计算机病毒所引起的，那么就可以通过安装相应的防病毒软件或对防病毒软件及时升级，以及强化软件管理、电子邮件下载等手段或措施来预防相同故障的发生。预防措施是最简单的，也是有效的方法。设计预防措施是一种主动的网络管理方式，而不是一种被动的管理方式。



网络故障的分类

- ◆ 根据网络故障的性质可把网络故障分为物理故障与逻辑故障；
- ◆ 根据引起网络故障的对象来进行划分，可把网络故障分为线路故障、路由器故障、交换机故障、主机故障和软件系统故障等；
- ◆ 按照网络故障覆盖的区域划分，可分为小范围（个别）故障、网段内故障、局域网故障和广域网连接故障。
- ◆ 根据OSI的7层模型来看，又可以归纳为不同层次的网络故障；



1. 按照网络故障的性质分类

(1) 物理故障主要指的是网络设备或网络传输介质引起的故障。网络设备的物理故障包括网络设备损坏、端口老化、电源系统故障或设备运行在恶劣环境下引起的设备故障。网络传输介质的故障主要是指线路损坏、接线水晶头或配线架线序错误、插头松动、线路受到严重电磁干扰、线路或网络模块老化、错接端口等情况。

另一种常见的物理故障就是网络插头误接

(2) 逻辑故障主要是由于网络设备配置错误而造成的网络异常或故障。

- 配置错误可能是路由器端口参数设置有误、路由器路由配置错误以至于路由循环或无法进行远端寻址、路由掩码设置错误，或者是交换机在VLAN划分过程中错误配置了端口参数等；
- 一些重要进程或端口被关闭，以及系统的负载过高；



2. 按照网络故障的对象分类

(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数据流量是否还存在，然后用ping命令检查线路远端的路由器端口能否响应，用tracert命令检查路由器配置是否正确。



2. 按照网络故障的对象分类

(2) 路由器故障。

路由器**CPU**温度过高、**CPU**利用率过高和路由器内存余量太小。可用**MIB**浏览器或网络管理系统实现检测。解决这种故障的方法是对路由器进行升级、扩内存等，或者重新规划网络的拓扑结构。

另一种路由器故障就是自身的配置错误。比如配置的协议类型不对，配置的端口不对等。这种故障比较少见，在使用初期配置好路由器基本上就不会出现了。

(3) 交换机故障。

交换机故障的原因可能是交换网络中出现广播风暴或某端口遭到恶意攻击，也可能是由于发生雷击而烧坏端口等原因引起的。



2. 按照网络故障的对象分类

(4) 主机故障。

主机故障常见的原因就是主机的配置不当（IP地址冲突或主机不在一个网段等）。或者一些服务设置的故障。比如E-Mail服务器设置不当导致不能收发E-Mail，或者域名服务器设置不当将导致不能解析域名。防火墙地址权限设置不当，也会造成网络的连接故障。

还有可能的原因是受到攻击等。

(5) 软件系统故障。

由于网络软件系统（包括网络操作系统、网络协议软件以及网上应用系统）自身存某些缺陷，再加上各类非法软件的危害（如病毒软件、攻击型软件），造成网络故障。



3. 按网络故障覆盖的区域区分

○ 小范围故障

- 一两个用户故障，可能是用户自己的主机配置或是与这些主机连接线路发生故障

○ 网段内故障

- 重点检查该网段的交换机的运行和配置情况是否正常

○ 局域网/广域网故障

- 如果访问内网服务正常，问题应该出在广域网连接设备或线路上
- 如果能访问外网不能访问内网，则问题可能是连接内网服务器的交换机或服务器发生故障
- 如果都不能访问，整个网络的核心设备出现故障。



网络故障的分层检查

1. 物理层故障

网络物理层的故障主要是指网络设备的连接性能故障:

- 线路方面故障
- 端口设置方面的故障
- 集线器故障
- 电源方面的故障
- 网卡故障



线路方面故障

- 线路方面故障主要表现在没有连接电缆；
- 电缆连接方式错误，如集线设备之间的连接线该用交叉线却用了直通线等错误。连接不同的设备使用直通线,如网卡和HUB/交换机,连接相同的设备使用交叉线,如网卡与网卡, HUB/交换机和HUB/交换机；
- 连接电缆不正确，如：双绞线采用标准（EIA568-A标准和EIA568-B）不一致；
- 网线、跳线或信息座故障。



端口设置方面的故障

- 两端设备对应的端口类型不统一，如RS-232端口和V.35端口之间的转换；
- 速率和双工设置不匹配；
- 数据收/发的线路没有接通，如路由器中的端口表现为“down”状态。



集线器故障

- 连接距离过大造成的网络故障
- 必须采用交叉电缆连接的用直通电缆连接
- 端口出现故障

可以观察交换机或集线器的指示灯作为工作正常与否的依据



电源方面的故障

- 掉电
- 超载、欠压等故障



网卡故障

- 网卡参数设置错误
- 在同一网段的网络设备的全双工状态、绑定帧的类型等参数要设置一致，否则，网络速度变慢甚至不通。
- 网卡驱动不正常



2. 数据链路层故障

- (1) 数据链路层数据帧的问题，可能是网卡故障，网卡驱动程序损坏或设置错误引起的。
- (2) 数据链路层地址的设置问题。
- (3) 链路协议的建立问题，在连接端口应该使用同一数据链路层协议封装。
- (4) 同步通信的时钟问题，表现在端口上设置了不正确的时钟。

需要查看路由器的配置，检查连接端口的共享同一数据链路层的封装情况。每对接口要和与其通信的其他设备有相同的封装。通过查看路由器的配置检查其封装，或者使用show命令查看相应接口的封装情况。



3. 网络层故障

- 网络层故障检查主要包括以下几个方面：
 - 路由协议没有加载和网络路由的设置错误。
 - IP地址和子网掩码的错误设置。
 - IP和DNS不正确的绑定。
- 排除网络层故障的基本方法是：

沿着从源到目标的路径，查看路由器路由表，同时检查路由器接口的IP地址。



4. 传输层故障

传输层的主要功能有：提供建立、维护和拆除传输层连接；选择网络层提供合适的服务；提供端到端的错误恢复和流量控制；向会话层提供独立于网络层的传送服务和可靠的透明数据传送。

传输层故障的检查主要包括以下几个方面：

- ❑ 差错检查，如数据包的重发等。
- ❑ 通信拥塞或上层协议在网络层协议上的捆绑方面。



5. 应用层故障

应用层故障检查主要包括以下几个方面：

- 操作系统的系统资源的运行状况
- 应用程序对系统资源的占用和调度
- 管理方面的问题，如安全管理、用户管理等。



网络故障诊断

- 网络管理工具和其它故障诊断工具，包括网络测试及监视工具。
- 查看路由表，是解决网络故障开始的好地方。
- Internet控制信息协议（ICMP）的ping、trace命令和Cisco的show命令、debug命令是获取故障诊断有用信息的网络工具。
- 经验
- 同事
- 制造商的技术支持热线
- 互连网络
- 网络记录



网络故障诊断的方法

- 对比法
- 硬件替代法
- 排除法



对比法

- 使用本系统正常运行或备用的正常设备作为基准,对比故障设备和正常设备之间的区别
- 前提条件:
 - 可以找到与发生故障的设备相近的其他一些设备.
- 优点:
 - 简单易行,对软件排查尤为有利
- 缺点:
 - 用途有限,有些故障无法找到有效的对比基准



操作原则

- 只有在故障设备和正常设备具有相近条件下，才可以采用对比法
- 在对数据进行修改之前应该确保数据的可恢复性
- 在对网络配置进行修改之前应该确保不会对网络中的其他设备造成冲突



硬件替代法

- 用使用正常的设备替换被怀疑存在故障的设备，这种方法主要用于硬件故障的处理。
- 前提条件：
 - 有能够正常工作的其他设备可供选择
- 优点：
 - 简单
- 缺点：
 - 可能会造成网络服务的临时中断



操作原则

- 故障定位所涉及的设备数量不能太多
- 确保可以获得正常工作的设备
- 每次只可以替换一个设备
- 在替换第二个设备之前，必须确保第一个设备的替换能够解决相应的问题



排除法

- 罗列出故障发生的可能性，然后逐步排除。罗列故障可能性时，要尽可能全面，不要有遗漏，排除可能性时要从简到繁
- 优点：
 - 逻辑性强，可以应对各种各样的故障
- 缺点：
 - 对维护人员要求较高，要求维护人员对系统有全面深入的了解



原则

- 对设备更改之前，应该对原来的配置做好记录，以确保可以将设备恢复到原始状态
- 如果需要对用户的数据进行更改，必须事先备份用户数据
- 确保不会影响到其他网络用户的正常工作
- 每次测试仅作一项修改，以便知道该次修改是否有效



网络故障诊断工具

○ 软件工具

- 网络管理系统
- IP连接测试-ping
- 路由追踪-tracert
- 路径测试-pathping
- IP路由表-Route
- 网络诊断工具-netsh diagnostic
- 显示IP地址信息-ipconfig
- 网络协议统计工具-netstat
- 地址解析-ARP
- 监测DNS服务-Nslookup

○ 硬件工具

- 物理层工具：物理线缆测试仪、接地电阻测试仪等。
- 物理层到网络层工具：网络测试仪。
- 物理层到应用层工具：协议分析仪、网络万用表。



PING工具

- `ping`命令可用于确定网络上的一个远程设备从本地系统是否可达，有助于在系统之间调试连通性问题。同时该命令可提供基本的网络性能统计数据，该数据可用于诊断与通信量相关的网络问题。
- 在linux平台和IPv6网络，用`ping6`



ping命令选项

选 项	描 述
-c	仅发送一定数量的报文
-f	用报文对网络泛洪
-i	各个请求之间延迟秒数
-n	显示网络地址
-r	打开记录路由选项
-s	指定各请求发送的字节数



```
[root@rndl7 root]# ping 202.112.18.51
PING 202.112.18.51 (202.112.18.51) 56(84) bytes of data.
64 bytes from 202.112.18.51: icmp_seq=1 ttl=64 time=0.226 ms
64 bytes from 202.112.18.51: icmp_seq=2 ttl=64 time=0.102 ms
64 bytes from 202.112.18.51: icmp_seq=3 ttl=64 time=0.102 ms
64 bytes from 202.112.18.51: icmp_seq=4 ttl=64 time=0.225 ms
64 bytes from 202.112.18.51: icmp_seq=5 ttl=64 time=0.224 ms

--- 202.112.18.51 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 3996ms
rtt min/avg/max/mdev = 0.102/0.175/0.226/0.062 ms
[root@rndl7 root]# ping -c 2 202.112.18.51
PING 202.112.18.51 (202.112.18.51) 56(84) bytes of data.
64 bytes from 202.112.18.51: icmp_seq=1 ttl=64 time=0.143 ms
64 bytes from 202.112.18.51: icmp_seq=2 ttl=64 time=0.142 ms

--- 202.112.18.51 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 999ms
rtt min/avg/max/mdev = 0.142/0.142/0.143/0.011 ms
[root@rndl7 root]# ping -c 2 202.112.18.53
PING 202.112.18.53 (202.112.18.53) 56(84) bytes of data.

--- 202.112.18.53 ping statistics ---
2 packets transmitted, 0 received, 100% packet loss, time 1011ms

[root@rndl7 root]# ping -s 100 202.112.18.52
PING 202.112.18.52 (202.112.18.52) 100(128) bytes of data.
108 bytes from 202.112.18.52: icmp_seq=1 ttl=64 time=0.043 ms
108 bytes from 202.112.18.52: icmp_seq=2 ttl=64 time=0.021 ms
108 bytes from 202.112.18.52: icmp_seq=3 ttl=64 time=0.007 ms
108 bytes from 202.112.18.52: icmp_seq=4 ttl=64 time=0.009 ms
108 bytes from 202.112.18.52: icmp_seq=5 ttl=64 time=0.007 ms
108 bytes from 202.112.18.52: icmp_seq=6 ttl=64 time=0.008 ms
108 bytes from 202.112.18.52: icmp_seq=7 ttl=64 time=0.007 ms
108 bytes from 202.112.18.52: icmp_seq=8 ttl=64 time=0.018 ms

--- 202.112.18.52 ping statistics ---
8 packets transmitted, 8 received, 0% packet loss, time 6993ms
rtt min/avg/max/mdev = 0.007/0.015/0.043/0.011 ms
[root@rndl7 root]#
```



命令提示符

```
C:\Documents and Settings\sldong>ping 2001:251:e00e::41
```

```
Pinging 2001:251:e00e::41 with 32 bytes of data:
```

```
Reply from 2001:251:e00e::41: time=72ms
```

```
Reply from 2001:251:e00e::41: time=70ms
```

```
Reply from 2001:251:e00e::41: time=74ms
```

```
Reply from 2001:251:e00e::41: time=73ms
```

```
Ping statistics for 2001:251:e00e::41:
```

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

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 70ms, Maximum = 74ms, Average = 72ms
```

```
C:\Documents and Settings\sldong>ping 218.192.175.69
```

```
Pinging 218.192.175.69 with 32 bytes of data:
```

```
Reply from 218.192.175.69: bytes=32 time=3ms TTL=64
```

```
Reply from 218.192.175.69: bytes=32 time=1ms TTL=64
```

```
Reply from 218.192.175.69: bytes=32 time=1ms TTL=64
```

```
Reply from 218.192.175.69: bytes=32 time=1ms TTL=64
```

```
Ping statistics for 218.192.175.69:
```

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

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 1ms, Maximum = 3ms, Average = 1ms
```

```
C:\Documents and Settings\sldong>
```



```
218.192.175.66 - default - SSH Secure Shell

File Edit View Window Help

This copy of SSH Secure Shell is a non-commercial version.
This version does not include PKI and PKCS #11 functionality.

Last login: Thu Sep  6 11:24:52 2007 from 202.112.18.92
[root@rndl2 root]# ping 2001:251:e00e::41
ping: unknown host 2001:251:e00e::41
[root@rndl2 root]# ping6 2001:251:e00e::41
PING 2001:251:e00e::41(2001:251:e00e::41) 56 data bytes
64 bytes from 2001:251:e00e::41: icmp_seq=1 ttl=245 time=70.6 ms
64 bytes from 2001:251:e00e::41: icmp_seq=2 ttl=245 time=68.8 ms
64 bytes from 2001:251:e00e::41: icmp_seq=3 ttl=245 time=70.7 ms
64 bytes from 2001:251:e00e::41: icmp_seq=4 ttl=245 time=68.7 ms
64 bytes from 2001:251:e00e::41: icmp_seq=5 ttl=245 time=70.6 ms
64 bytes from 2001:251:e00e::41: icmp_seq=6 ttl=245 time=68.5 ms
64 bytes from 2001:251:e00e::41: icmp_seq=7 ttl=245 time=70.4 ms
64 bytes from 2001:251:e00e::41: icmp_seq=8 ttl=245 time=68.7 ms
64 bytes from 2001:251:e00e::41: icmp_seq=9 ttl=245 time=70.4 ms

--- 2001:251:e00e::41 ping statistics ---
9 packets transmitted, 9 received, 0% packet loss, time 8074ms
rtt min/avg/max/mdev = 68.580/69.755/70.721/0.958 ms
[root@rndl2 root]#

Connected to 218.192.175.66      SSH2 - aes128-cbc - hmac-md5 - 80x24
```



常见的错误信息

(1) unknown host 不知主机名

远程主机的名字不能被命名服务器转换成IP地址。

(2) Network unreachable 网络不能到达

本地系统没有到达远程系统的路由，可以用
`netstat -rn`检查路由表来确定路由配置情况。

(3) No answer 无响应

远程系统没有响应。

(4) Timed out 超时

与远程主机的链接超时，数据包全部丢失。故障原因可能是到路由器的连接问题、路由器不能通过，也可能远程主机已经关机。



一些典型的检测次序及对应可能故障的例子

- (1) ping 127.0.0.1: 检查TCP/IP是否被正确地安装。
- (2) ping本机IP: ping本地计算机的IP地址, 本地计算机对该ping命令作出应答。如果没有应答, 则表示本地配置或安装存在问题。出现此问题时, 局域网用户可断开网络电缆, 然后重新发送该命令。如果网线断开后本命令正确, 则表示另一台计算机可能配置额相同的IP地址。
- (3) ping局域网内其他主机IP: 如果收到回送应答, 表明本地网络中的网卡和传输介质运行正确。但如果没有收到回送应答, 那么表示子网掩码不正确或网卡配置错误, 或电缆线路有问题。
- (4) ping网关IP: 该命令如果应答正确, 表示局域网中的网关路由器正在运行以及能与本地网络上的本地主机通讯。
- (5) ping远程主机IP: 如果收到4个应答, 表示成功地使用了缺省网关。对于拨号上网用户则表示能够成功地访问Internet。
- (6) ping域名: ping域名, 如ping www.sina.com.cn, 通常是通过DNS服务器进行解析。如果这里出现故障, 则表示DNS服务器的IP地址配置不正确或DNS服务器有故障。另外, 利用该命令可以实现域名对IP地址的转换功能。



TRACEROUTE工具

- traceroute命令检测并记录到达一个指定网络目标的路径。
- 该命令对于目标由什么构成没有限制，目标可以是从小主机系统到一个Internet路由器范围的任何种类的设备。唯一的要求是该设备必须支持IP。
- 在linux平台和IPv6网络，用Traceroute6



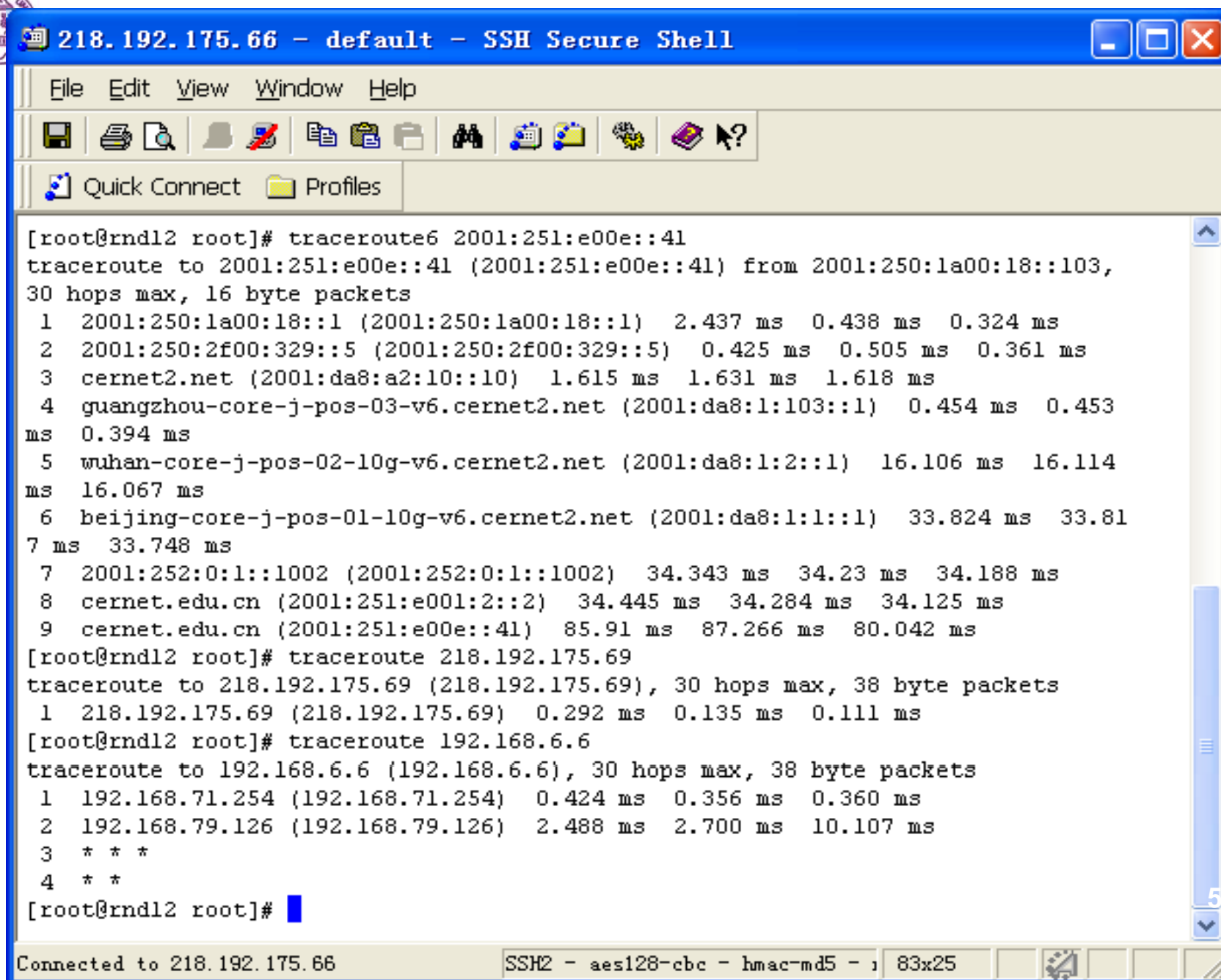
traceroute显示代码

代 码	含 义
*	探测报文没有获得响应
!	接收到的报文中TTL设成了1
!H	目标主机不可达
!N	目标网络不可达
!P	目标协议不可达
!S	源路由选项错误。在实际中，该代码不会出现，并且如果一旦出现，该代码指出产生该错误的路由器的一个程序错误或故障
!F	探测报文需要分段。在实际中，该代码不会出现，并且如果一旦出现，该代码指出产生该错误的路由器的一个程序错误或故障
!X	由于通信被管理性的禁止，该路径被阻塞。换句话说，该路径从软件角度上被关闭或阻塞
!N>	一个ICMP错误代码，N是该错误号



traceroute操作选项

选 项	描 述
-i	指定一个可选接口
-p	设置可选端口来发送探测报文
-g	为松散源路由选择指定一个路由器
-f	设置使用的 TTL 初始值
-s	在发送的探测报文中使用指定地址作为源地。
-q	设置探测询问的数量
-m	设置最大跳步数
-d	启用调试标志 (SO_DEBUG)
-F	指定不分段
-t	设置服务类型 (TOS) 标志
-W	为探测报文设置等待时间
-x	指定不要计算校验和



218.192.175.66 - default - SSH Secure Shell

File Edit View Window Help

Quick Connect Profiles

```
[root@rndl2 root]# traceroute6 2001:251:e00e::41
traceroute to 2001:251:e00e::41 (2001:251:e00e::41) from 2001:250:1a00:18::103,
30 hops max, 16 byte packets
 1  2001:250:1a00:18::1 (2001:250:1a00:18::1)  2.437 ms  0.438 ms  0.324 ms
 2  2001:250:2f00:329::5 (2001:250:2f00:329::5)  0.425 ms  0.505 ms  0.361 ms
 3  cernet2.net (2001:da8:a2:10::10)  1.615 ms  1.631 ms  1.618 ms
 4  guangzhou-core-j-pos-03-v6.cernet2.net (2001:da8:1:103::1)  0.454 ms  0.453
ms  0.394 ms
 5  wuhan-core-j-pos-02-10g-v6.cernet2.net (2001:da8:1:2::1)  16.106 ms  16.114
ms  16.067 ms
 6  beijing-core-j-pos-01-10g-v6.cernet2.net (2001:da8:1:1::1)  33.824 ms  33.81
7 ms  33.748 ms
 7  2001:252:0:1::1002 (2001:252:0:1::1002)  34.343 ms  34.23 ms  34.188 ms
 8  cernet.edu.cn (2001:251:e001:2::2)  34.445 ms  34.284 ms  34.125 ms
 9  cernet.edu.cn (2001:251:e00e::41)  85.91 ms  87.266 ms  80.042 ms
[root@rndl2 root]# traceroute 218.192.175.69
traceroute to 218.192.175.69 (218.192.175.69), 30 hops max, 38 byte packets
 1  218.192.175.69 (218.192.175.69)  0.292 ms  0.135 ms  0.111 ms
[root@rndl2 root]# traceroute 192.168.6.6
traceroute to 192.168.6.6 (192.168.6.6), 30 hops max, 38 byte packets
 1  192.168.71.254 (192.168.71.254)  0.424 ms  0.356 ms  0.360 ms
 2  192.168.79.126 (192.168.79.126)  2.488 ms  2.700 ms  10.107 ms
 3  * * *
 4  * *
[root@rndl2 root]#
```

Connected to 218.192.175.66

SSH2 - aes128-cbc - hmac-md5 - 83x25



TRACERT(WINDOWS)

语法

tracert [-d] [-h MaximumHops] [-j HostList] [-w Timeout] [TargetName]

参数

-d

防止 tracert 试图将中间路由器的 IP 地址解析为它们的名称。这样可加速显示 tracert 的结果。

-h MaximumHops

在搜索目标（目的）的路径中指定跃点的最大数。默认值为 30 个跃点。

TargetName： 指定目标，可以是 IP 地址或主机名。



例子

- 要跟踪名为 corp7.microsoft.com 的主机的路径
 - **tracert corp7.microsoft.com**
- 要跟踪名为 corp7.microsoft.com 的主机的路径并防止将每个 IP 地址解析为它的名称：
 - **tracert -d corp7.microsoft.com**

注: traceroute命令的功能与tracert相同，二者的差别仅仅在于tracert命令是用在Windows平台上，而traceroute命令是用在Unix平台和路由器上



命令提示符

C:\Documents and Settings\sldong>tracert 2001:251:e00e::41

Tracing route to cernet.edu.cn [2001:251:e00e::41]
over a maximum of 30 hops:

1	15 ms	1 ms	1 ms	2001:250:1a00:18::1
2	40 ms	27 ms	27 ms	2001:250:2f00:329::5
3	3 ms	3 ms	2 ms	cernet2.net [2001:da8:a2:10::10]
4	1 ms	3 ms	1 ms	guangzhou-core-j-pos-03-v6.cernet2.net [2001:da8:a2:10::11]
5	17 ms	21 ms	26 ms	wuhan-core-j-pos-02-10g-v6.cernet2.net [2001:da8:a2:12::1]
6	34 ms	37 ms	34 ms	beijing-core-j-pos-01-10g-v6.cernet2.net [2001:da8:a2:11::1]
7	35 ms	35 ms	35 ms	2001:252:0:1::1002
8	35 ms	35 ms	35 ms	cernet.edu.cn [2001:251:e001:2::2]
9	83 ms	70 ms	71 ms	cernet.edu.cn [2001:251:e00e::41]

Trace complete.

C:\Documents and Settings\sldong>tracert 218.192.175.69

Tracing route to 218.192.175.69 over a maximum of 30 hops

1	1 ms	1 ms	1 ms	scut-bgw5.scut.edu.cn [202.112.18.254]
2	19 ms	5 ms	9 ms	192.168.82.5
3	9 ms	14 ms	2 ms	192.168.79.123
4	1 ms	1 ms	1 ms	218.192.175.69

Trace complete.



PATHPING

- 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
- 语法
- **pathping** [-n] [-h *MaximumHops*] [-g *HostList*] [-p *Period*] [-q *NumQueries*] [-w *Timeout*] [-T] [-R] [*TargetName*]



- **-n** 阻止 **pathping** 试图将中间路由器的 IP 地址解析为各自的名称。这有可能加快显示 **pathping** 的结果。
- **-h** *MaximumHops* 在搜索目标（目的）的路径中指定跃点的最大数。默认值为 30 个跃点。
- **-g** *HostList* 指定回显请求消息在 IP 标题中使用“稀疏资源路由”选项（该 IP 标题带有 *HostList* 中指定的中间目标集）。可以由一个或多个具有松散源路由的路由器分隔连续中间的目的地。主机列表中的地址或名称的最大数为 9。*HostList* 是一系列由空格分隔的 IP 地址（带点的十进制符号）。
- **-p** *Period* 指定两个连续的 ping 之间的时间间隔（以毫秒为单位）。默认值为 250 毫秒（1/4 秒）。
- **-q** *NumQueries* 指定发送到路径中每个路由器的回显请求消息数。默认值为 100 个查询。



- **-w Timeout** 指定等待应答的时间（以毫秒为单位）。默认值为 3000 毫秒（3 秒）。
- **-T** 在向路由所经过的每个网络设备发送的回显请求消息上附加一个 2 级优先级标记（例如 802.1p）。这有助于标识不具有 2 级优先级功能的网络设备。此开关用于测试服务质量 (QoS) 的连通性。
- **-R** 确定路由所经过的每个网络设备是否支持“资源预留设置协议” (RSVP)，该协议允许主机计算机为某一数据流保留一定数量的带宽。此开关用于测试服务质量 (QoS) 的连通性。
- **TargetName** 指定目的端，它既可以是 IP 地址，也可以是主机名。
- **/?** 在命令提示符显示帮助。



注意:

- Pathping 参数要区分大小写。
- 为避免网络拥塞，应以足够慢的速度发送 ping 信号。
- 要尽可能地减小突发包丢失所造成的影响，请不要频繁发送 ping 信号。
- 使用 **-p** 参数时，ping 将单独发送到各个中间跃点。因此，向同一跃点发送探测信号的时间间隔为 *period* 乘以跃点数。
- 使用 **-w** 参数时，可以同时发送多个 ping。因此，*Timeout* 参数中指定的时间量不受 *Period* 参数指定的时间间隔的限制。
- 使用 **-T** 参数 在主机计算机上启用 2 级优先级允许数据包同第 2 级优先级标记一起发送，以便 2 级设备可以为数据包指派优先级。不能识别 2 级优先级的旧式设备将丢弃这些貌似变形的数据包。该参数有利于识别正在丢弃这些数据包的网络计算机。



注意:

- 使用 **-R** 参数 对于不存在的会话，RSVP 预约消息将沿路由发送到每个网络设备。如果设备不支持 RSVP，则将返回“网际消息控制协议 (ICMP) 无法达到目标——无法访问协议”的消息。如果设备支持 RSVP，则将返回“RSVP 预留错误”的消息。有些设备可能不会返回以上任何一种消息。如果这样，则会显示超时消息。
- 只有当网际协议 (**TCP/IP**) 协议在 网络连接中安装为网络适配器属性的组件时，该命令才可用。



应用例子

○ D:\>pathping -n corp1

Tracing route to corp1 [10.54.1.196]
over a maximum of 30 hops:

```
0 172.16.87.35
1 172.16.87.218
2 192.168.52.1
3 192.168.80.1
4 10.54.247.14
5 10.54.1.196
```

Computing statistics for 125 seconds...

Source to Here This Node/Link

Hop	RTT	Lost/Sent = Pct	Lost/Sent = Pct	Address
0				172.16.87.35
1	41ms	0/ 100 = 0%	0/ 100 = 0%	172.16.87.218
2	22ms	16/ 100 = 16%	3/ 100 = 3%	192.168.52.1
3	24ms	13/ 100 = 13%	0/ 100 = 0%	192.168.80.1
4	21ms	14/ 100 = 14%	1/ 100 = 1%	10.54.247.14
5	24ms	13/ 100 = 13%	0/ 100 = 0%	10.54.1.196

Trace complete.

显示路径信息。
此路径与
tracert 命令所
显示的路径相同

显示约 90 秒（该时间随
着跃点数的变化而变化）
的繁忙消息

172.16.87.218 与
192.68.52.1 之间的链
接丢失了 13% 的数据
包



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。
- 语法:
- `route [-f] [-p] [Command][Destination] [mask Netmask] [Gateway] [metric Metric]] [if Interface]`
- **-f** 清除所有不是主路由（网掩码为 255.255.255.255 的路由）、环回网络路由（目标为 127.0.0.0，网掩码为 255.255.255.0 的路由）或多播路由（目标为 224.0.0.0，网掩码为 240.0.0.0 的路由）的条目的路由表。如果它与命令之一（例如 **add**、**change** 或 **delete**）结合使用，表会在运行命令之前清除。



ROUTE

- **-p** 与 **add** 命令共同使用时，指定路由被添加到注册表并在启动 TCP/IP 协议的时候初始化 IP 路由表。默认情况下，启动 TCP/IP 协议时不会保存添加的路由。与 **print** 命令一起使用时，则显示永久路由列表。所有其它的命令都忽略此参数。
- **Command** 指定您想运行的命令 (Add/Change/Delete/Print)。
- **Destination** 指定路由的网络目标地址。目标地址可以是一个 IP 网络地址（其中网络地址的主机地址位设置为 0），对于主机路由是 IP 地址，对于默认路由是 0.0.0.0



- **mask subnetmask** 指定与网络目标地址相关联的网掩码（又称之为子网掩码）。
- **Gateway** 指定超过由网络目标和子网掩码定义的可达到的地址集的前一个或下一个跃点 IP 地址。 **metric** *Metric* 为路由指定所需跃点数的整数值（范围是 1 ~ 9999），它用来在路由表里的多个路由中选择与转发包中的目标地址最为匹配的路由。所选的路由具有最少的跃点数。跃点数能够反映跃点的数量、路径的速度、路径可靠性、路径吞吐量以及管理属性。
- **if Interface** 指定目标可以到达的接口的接口索引。使用 **route print** 命令可以显示接口及其对应接口索引的列表。忽略 **if** 参数时，接口由网关地址确定。
- **/?** 在命令提示符显示帮助。



route命令使用示例如下:

- (1) 要显示IP路由表的完整内容, 键入route print
- (2) 要显示IP路由表中以10.开始的路由, 键入route print 10.*
- (3) 要添加默认网关地址为192.168.12.1的默认路由, 键入
route add 0.0.0.0 mask 0.0.0.0 192.168.12.1
- (4) 要添加目标为10.41.0.0, 子网掩码为255.255.0.0, 下一个跃点地址为10.27.0.1, 跃点数为7的路由, 键入route add 10.41.0.0 mask 255.255.0.0 10.27.0.1 metric 7
- (5) 要添加目标为10.41.0.0, 子网掩码为255.255.0.0, 下一个跃点地址为10.27.0.1, 接口索引为0x3的路由, 键入route add 10.41.0.0 mask 255.255.0.0 10.27.0.1 if 0x3



route命令使用示例如下:

(6) 将数据的路由改到另一个路由器, 它采用一条包含3个网段的更直的路径, 则键入

```
route add 209.98.32.33 mask 255.255.255.224  
202.96.123.250 metric 3
```

(7) 要将目标为10.41.0.0, 子网掩码为255.255.0.0的路由的下一个跃点地址由10.27.0.1更改为10.27.0.25, 键入

```
route change 10.41.0.0 mask 255.255.0.0 10.27.0.25
```

(8) 要删除目标为 10.41.0.0, 子网掩码为255.255.0.0的路由, 键入

```
route delete 10.41.0.0 mask 255.255.0.0
```

(9) 要删除IP路由表中以10.开始的所有路由, 键入route delete 10.*

(10) 要将目标为 10.41.0.0, 子网掩码为 255.255.0.0 的路由的下一个跃点地址由 10.27.0.1 更改为 10.27.0.25, 键入:

```
route change 10.41.0.0 mask 255.255.0.0 10.27.0.25
```




NETSH DIAGNOSTIC

- C:\Documents and Settings\dongsl>netsh
netsh>diag
netsh diag>show ip
 - IP 地址
 - 3. [00000011] Intel(R) PRO/Wireless 3945ABG Network Connection
IPAddress = 211.66.86.234
 - 5. [00000015] Microsoft Loopback Adapter
IPAddress = 192.168.100.100
 - netsh diag>show computer
计算机系统 <SLDONG-PC>
netsh diag>show dns
DNS 服务器
 - 3. [00000011] Intel(R) PRO/Wireless 3945ABG Network Connection
DNSServerSearchOrder = 202.112.17.33
202.38.193.33
- netsh diag>



IFCONFIG工具

ifconfig命令是一个接口配置的摘要显示并且可用来配置本地网络接口

该命令可执行下面功能：

- 列出每个已定义的网络接口的配置。
- 启用/禁止任何一个已定义的网络接口。
- 修改网络接口配置参数。
- 创建伪接口。



ifconfig选项及关键字

选 项	描 述
-a	应用到目前安装在该系统上的所有接口
arp	启用在该接口上使用地址解析协议 (ARP)。-arp选项禁止使用ARP
-arp	
promisc	在该接口上启用杂凑 (promiscuous, 也就是, 侦听所有通信) 模式。用 -promisc禁止该模式
-promisc	
allmulti	使所有组播通讯由接口接收。-allmulti选项禁止组播报文重复
-allmulti	
broadcast	当给定参数时, 为该接口设置或清除广播地址。该地址是网络层广播地址
-broadcast	
pointtopoint	为该接口启用一个点到点模式 (point-to-point)。基本假定是: 这是两个设备之间的一个专用链路。如果提供地址参数, 则为链路的另一方设置协议地址。用 -pointtopoint关键字禁止点到点模式
-pointtopoint	
up	使该接口被启动或激活
down	使该接口被关闭或处于不活跃状态
netmask	为该接口设置 IP 网络掩码, 指定的参数可用 255.0.0.0 (十进制点分格式) 形式或 0xff000000 (十六进制) 形式
broadcast	为该接口设置 IP 广播。指定的参数可以使用与 netmask 关键字相同的格式表示
address	为该接口设置 IP 地址。该地址必须是唯一的 IP 地址, 不能已经分配给其他系统



```
[root@rndl7 root]# ifconfig -a
eth0      Link encap:Ethernet  HWaddr 00:0C:F1:DC:73:A9
          inet addr:218.192.175.69  Bcast:218.192.175.71  Mask:255.255.255.248
          inet6 addr: fe80::20c:flff:fedc:73a9/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:11178083 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10463431 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:2551226686 (2433.0 Mb)  TX bytes:1833240910 (1748.3 Mb)
          Interrupt:20 Base address:0xcc00 Memory:feafe000-feafe038

eth1      Link encap:Ethernet  HWaddr 00:0C:F1:DC:73:A7
          inet addr:202.112.18.52  Bcast:202.112.18.255  Mask:255.255.255.0
          inet6 addr: 2001:250:1800:18::103/64 Scope:Global
          inet6 addr: fe80::20c:flff:fedc:73a7/64 Scope:Link
          inet6 addr: 2001:251:4001:18:20c:flff:fedc:73a7/64 Scope:Global
          inet6 addr: 2001:250:1800:18:20c:flff:fedc:73a7/64 Scope:Global
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:9422038 errors:0 dropped:0 overruns:0 frame:0
          TX packets:783899 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:100
          RX bytes:913743605 (871.4 Mb)  TX bytes:274326741 (261.6 Mb)
          Interrupt:18 Base address:0xbc00 Memory:fc9e0000-fca00000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:16436  Metric:1
          RX packets:24230 errors:0 dropped:0 overruns:0 frame:0
          TX packets:24230 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:2443691 (2.3 Mb)  TX bytes:2443691 (2.3 Mb)

sit0      Link encap:IPv6-in-IPv4
          NOARP  MTU:1480  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)
```



IPCONFIG(WINDOWS)

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 IP 地址、子网掩码、默认网关。

语法

```
ipconfig [/all] [/renew [Adapter]] [/release [Adapter]]  
          [/flushdns] [/displaydns] [/registerdns] [/showclassid  
          Adapter] [/setclassid Adapter [ClassID]]
```

参数

/all

显示所有适配器的完整 TCP/IP 配置信息。在没有该参数的情况下 **ipconfig** 只显示 IP 地址、子网掩码和各个适配器的默认网关值。适配器可以代表物理接口（例如安装的网络适配器）或逻辑接口（例如拨号连接）。

/renew [*adapter*]

更新所有适配器（如果未指定适配器），或特定适配器（如果包含了 *Adapter* 参数）的 DHCP 配置。该参数仅在具有配置为自动获取 IP 地址的网卡的计算机上可用。



例子

显示所有适配器的基本 TCP/IP 配置:

ipconfig

显示所有适配器的完整 TCP/IP 配置:

ipconfig /all

更新由 DHCP 分配 IP 地址的配置:

ipconfig /renew

要在排除 DNS 的名称解析故障期间清理 DNS 解析器缓存:

ipconfig /flushdns

要显示名称以 *Local* 开头的所有适配器的 DHCP 类别 ID:

ipconfig /showclassid Local*

要将“本地连接”适配器的 DHCP 类别 ID 设置为 *TEST*:

ipconfig /setclassid "Local Area Connection" TEST



NETSTAT工具

- netstat命令是network status的缩写，提供一些丰富的信息，这些信息是关于目前网络连接、路由选择信息以及其他重要网络相关数据的状态信息，用于严密监测网络,是在UNIX上可用的大多数受欢迎的调试辅助工具之一
- 该工具的功能可被用于完成下面功能：
 - 列出活跃的网络会话。
 - 显示接口信息和统计数据。
 - 显示路由选择表信息。
 - 显示网络数据结构。



- 关键字用来控制哪个数据结构被显示。

netstat关键字

选项	助记符	描述
-i	--interface	显示网络接口参数和统计信息
-g	--groups	显示组播中组成员信息
-M	--masquerade	列出FTP中使用伪装（masquerade）能力的会话
-N	--netlink	显示netlink接口及其活动
-r	--route	显示网络路由选择表
-t	-tcp	显示活跃的TCP连接，-tcp选项使命令持续显示这些连接直到被用户中断



NETSTAT命令选择

netstat命令选择

选项	助记符	描 述
-A	--af	指定一个不同地址族。指定关键字包括 --unix、--ipx、--ax25、--netrom及--ddp
-c	--continue	使得输出持续显示，直到用户中断输出为止
-h	--help	为用户显示命令行简要帮助信息
-n	--numeric	显示数值信息（如：IP地址）来代替试图解析主机、端口或用户名
-p	--program	显示进程名以及列出的网络 socket 标识符
-v	--verbose	显示额外信息



NETSTAT(WINDOWS)

netstat命令可以帮助网络管理员了解网络的整体使用情况。

显示活动的 TCP 连接、计算机侦听的端口、以太网统计信息、IP 路由表、IPv4 统计信息（对于 IP、ICMP、TCP 和 UDP 协议）以及 IPv6 统计信息（对于 IPv6、ICMPv6、通过 IPv6 的 TCP 以及通过 IPv6 的 UDP 协议）。使用时如果不带参数，**netstat** 显示活动的 TCP 连接。

语法

netstat [-a] [-e] [-n] [-o] [-p *Protocol*] [-r] [-s] [*Interval*]

参数

-a

显示所有活动的 TCP 连接以及计算机侦听的 TCP 和 UDP 端口。

-e

显示以太网统计信息，如发送和接收的字节数、数据包数。该参数可以与 **-s** 结合使用。



-n

显示活动的 TCP 连接，不过，只以数字形式表现地址和端口号，却不尝试确定名称。

-o

显示活动的 TCP 连接并包括每个连接的进程 ID (PID)。可以在 Windows 任务管理器中的“进程”选项卡上找到基于 PID 的应用程序。该参数可以与 **-a**、**-n** 和 **-p** 结合使用。

-p *Protocol*

显示 *Protocol* 所指定的协议的连接。在这种情况下，*Protocol* 可以是 **tcp**、**udp**、**tcpv6** 或 **udpv6**。如果该参数与 **-s** 一起使用按协议显示统计信息，则 *Protocol* 可以是 **tcp**、**udp**、**icmp**、**ip**、**tcpv6**、**udpv6**、**icmpv6** 或 **ipv6**。

-s

按协议显示统计信息。默认情况下，显示 TCP、UDP、ICMP 和 IP 协议的统计信息。如果安装了 Windows XP 的 IPv6 协议，就会显示有关 IPv6 上的 TCP、IPv6 上的 UDP、ICMPv6 和 IPv6 协议的统计信息。可以使用 **-p** 参数指定协



- **-r**
 - 显示 IP 路由表的内容。
- *Interval*
 - 每隔 *Interval* 秒重新显示一次选定的信息。按 CTRL+C 停止重新显示统计信息。如果省略该参数，**netstat** 将只打印一次选定的信息。
- */?*
 - 在命令提示符显示帮助。



显示以太网统计信息和所有协议的统计信息:

netstat -e -s

想仅显示 TCP 和 UDP 协议的统计信息:

netstat -s -p tcp udp

要想每 5 秒钟显示一次活动的 TCP 连接和进程 ID:

netstat -o 5

要想以数字形式显示活动的 TCP 连接和进程 ID:

netstat -n -o



ARP工具

- 地址解析协议表（也称为A R P缓存）包含一个本地网络上所有数据链路协议到I P地址映射的完整列表。
- A R P协议是一个动态功能，用来映射数据链路地址（如E t h e r n e t）到I P地址。一个系统无论何时需要发送一个消息时，该系统必须首先知道目标系统的下层（如数据链路层）地址。
- 许多网络工具（如t e l n e t、f t p以及其他一些工具）间接使用A R P表。



- `arp`命令提供查看和修改A R P缓存（A R P表）的能力
- 对于`arp`命令，超级用户可以：
 - 显示A R P缓存。
 - 删除一个A R P表项。
 - 增加一个A R P表项。



重要的arp命令行选项

选 项	关 键 字	描 述
-a	--display	为指定主机显示当前的 ARP表项
-d	--delete	删除一个ARP表项
-f	--file	载入一个包含若干表项的文件置于缓存中
-i	--device	仅显示指定接口的那些表项
-n	--numeric	用数值形式的地址代替主机名来显示
-s	--set	创建一个ARP表项
-v	--verbose	使用冗长模式显示 ARP缓存



ARP (WINDOWS)

语法

arp [-a [*InetAddr*] [-N *IfaceAddr*]] [-g [*InetAddr*] [-N *IfaceAddr*]] [-d *InetAddr* [*IfaceAddr*]] [-s *InetAddr EtherAddr* [*IfaceAddr*]]

参数

- a [*InetAddr*] [-N *IfaceAddr*] : 显示所有接口的当前 ARP 缓存表。要显示指定 IP 地址的 ARP 缓存项，可使用带有 *InetAddr* 参数的 **arp -a**，此处的 *InetAddr* 代表指定的 IP 地址。要显示指定接口的 ARP 缓存表，可使用 -N *IfaceAddr* 参数，此处的 *IfaceAddr* 代表分配给指定接口的 IP 地址。-N 参数区分大小写。
- g [*InetAddr*] [-N *IfaceAddr*] : 与 -a 相同。
- d *InetAddr* [*IfaceAddr*] : 删除指定的 IP 地址项，此处的 *InetAddr* 代表 IP 地址。对于指定的接口，要删除表中的某项，可使用 *IfaceAddr* 参数，此处的 *IfaceAddr* 代表分配给该接口的 IP 地址。要删除所有项，可使用星号 (*) 通配符代替 *InetAddr*。
- s *InetAddr EtherAddr* [*IfaceAddr*] : 向 ARP 缓存添加可将 IP 地址 *InetAddr* 解析成物理地址 *EtherAddr* 的静态项。要向指定接口的表添加静态 ARP 缓存项，可使用 *IfaceAddr* 参数，此处的 *IfaceAddr* 代表分配给该接口的 IP 地址。



例子

- 显示所有接口的 ARP 缓存表：
 - **arp -a**
- 对于指派的 IP 地址为 10.0.0.99 的接口，要显示其 ARP 缓存表：
 - **arp -a -N 10.0.0.99**
- 添加将 IP 地址 10.0.0.80 解析成物理地址 00-AA-00-4F-2A-9C 的静态 ARP 缓存项：
 - **arp -s 10.0.0.80 00-AA-00-4F-2A-9C**



NSLOOKUP工具

- nslookup是一个监测网络中DNS服务器是否能正确实现域名解析的命令行工具。它在 UNIX/Windows NT/2000/XP中均可使用。nslookup必须要安装了TCP/IP的网络环境中才能使用。

命令的一般格式为：

nslookup [IP地址/域名]



例子

```
C:\WINDOWS\system32\cmd.exe

C:\Documents and Settings\sldong>nslookup www.google.com
Server:  orange.gznet.edu.cn
Address:  202.112.17.33

Non-authoritative answer:
Name:      www-china.l.google.com
Addresses:  64.233.189.99, 64.233.189.104, 64.233.189.147
Aliases:   www.google.com, www.l.google.com

C:\Documents and Settings\sldong>
```



例如，现在网络中已经架设好了一台**DNS**服务器，主机名称为**linlin**，它可以把域名**www.company.com**解析为**192.168.0.1**的IP地址

```
C:\> Nslookup www.company.com
```

运行后显示如下结果

```
Server: linlin
```

```
Address: 192.168.0.5
```

```
Name: www.company.com
```

```
Address: 192.168.0.1
```



物理线缆测试仪

- 物理线缆测试仪一般指的是现场测试仪，作用是进行布线故障问题诊断，以便工程师和管理员能够在最短的时间内纠正布线错误、排除故障。
- 线缆测试仪是常用的网络故障诊断工具。电缆测试仪不仅能够测试电缆的连通性、开路、短路、跨接、反接、串绕、以及电缆的长度等各种参数，而且能够用来诊断网络中电缆出现的故障和综合布线的论证测试。



物理线缆测试仪 - MICROSCANNER PRO 数字式超5类电缆分析仪



- 福禄克公司的物理线缆测试仪，可以检测电缆的通断、电缆的连接线序、电缆故障的位置。
- 显著的特色就是将一系列测试结果直观的反映在显示屏上



物理线缆测试仪-国产TPT-8020A测试仪



- 1) 线缆测试
 - (1) 长度测试：。
 - (2) 线序测试：显示线序图；诊断开路、短路、线序错等故障；等。
 - (3) 音频寻线：可产生多达四种不同的音频信号，用于在天花板或配线柜中查找线缆。
 - (4) 端口识别：识别端口和插座类型。
- 2) 网络测试
 - (1) 闪亮端口：帮助确定端口位置
 - (2) Ping测试：支持Ping功能，检测网络丢包等故障。
 - (3) DHCP测试：支持DHCP自动获取或手动设置 IP 地址。
 - (4) 网络扫描：检测设定网段中正在使用的主机数量，并显示IP地址和MAC地址。



网络测试仪

网络测试仪包括了大部分的电缆测试仪的功能。这类仪器可以收集网络的统计资料并用图表形式显示出来。网络测试仪即可以用于被动的工作方式（即出了问题去查找），也可用于主动方式（即网络动态监测）。网络测试仪可以对广播帧、错误帧、帧检测序列FCS、短帧、长帧、冲突帧进行检测。能够对流量进行网络测试，可以检测到诸如噪声、前导帧冲突等。较高级的网络测试仪能够将网络管理、故障诊断以及网络安装调试等众多功能集中在仪器里，可以通过交换机、路由器很容易地观察整个网络的状况。

- 有线网络测试仪
- 无线网络测试仪



安捷伦J6800A 网络分析仪

- 主要可用于安装部署、维护与优化当前数据网络的先进工具。适用于电信运营商的现场安装与维护、企业网络的网络管理与设备制造商研发部门的各类工程技术人员。它既支持集中式的网络故障诊断，又支持分布式网络状况监测，涵盖局域网、广域网、ATM、IP电话、移动（包括3G）等各类应用。
- 可以实现集中式故障定位与分布式监测分析功能。集中式测试具备双端口测试功能，采集网络数据信息，排查间隙性与深层网络问题，全方位管理与监测网络。





无线网络测试仪

- 主要是针对无线路由和AP进行检测，可以排查出无线网络中连接的终端和无线信号强度，进而能有效地管理网络中的节点，增强网络安全
- 该类产品技术还不是很成熟





协议分析仪

- 协议分析仪是能够捕获网络报文的设备，能够找出网络中潜在的问题
- 协议分析仪的主要目的是捕获和解码穿过网络的数据帧，使用户可以清晰地看到数据链路层、网络层和传输层的数据报头，以及每个数据帧中的数据。
- 使用协议分析仪不像网络分析仪提供的信息简单易懂，而是要具备计算机网络的专业知识。
- 常见的几种形式
 - 1) 纯软件的协议分析系统
 - 2) 基于笔记本+数据采集箱的便携式协议分析仪
 - 3) 手持式综合协议分析仪
 - 4) 分布式协议分析仪



分布式协议分析仪-- OPTiVIEW



- OptiView将协议分析、流量分析和网络搜索三大功能集于一身，提供了全新的快速、易用、深层透视、有助于优化WAN、LAN和WLAN性能的网络分析解决方案。包括一个高性能协议分析仪，一个快速电缆测试仪，一个RMONv2探头。



常见的网络故障及其解决方法

工作站故障

1. IP地址冲突

检查冲突主机的操作步骤：

- 更改自己的IP地址
- 使用ping命令，确认非法使用IP地址的主机还在网络上。
- 使用arp -a，确定机器的MAC地址和主机名。知道了主机名，就确定了是谁的IP地址强占了别人的IP地址。



如何预防IP地址冲突呢？

- 捆绑MAC地址和IP地址

在DOS命令提示符下，输入Ipconfig /all命令，查出你的IP地址及对应的MAC地址。用ARP - s 把MAC地址和IP地址捆绑在一起了。

- 加强IP地址的管理

记录好IP地址及MAC地址等信息的记录，记录信息包括：主机名、分配的IP地址、网卡的MAC地址。另外就是要动态监视网络中的IP地址变化。



2.子网掩码设置不正确

在同一个网段中的计算机应该具有相同的子网掩码。如果子网掩码不同，就算位于同一个网段的计算机也是ping不通的。所以，出现同一网段的两台计算机不能互通的故障，除了两台计算机的IP地址设置正确外，还要查看它们的子网掩码是否相同。



3. 没有安装网络协议

- 不同的计算机之间必须使用相同的网络协议才能进行通信。在网络的各层中存在着许多协议，接收方和发送方同层的协议必须一致，否则一方将无法识别另一方发出的信息。网络协议使网络上各种设备能够相互交换信息。常见的协议有：TCP/IP协议、IPX/SPX协议、NetBEUI协议等。
- TCP/IP协议：是互联网协议，如果不安装该协议，网络是不能实现互联，也就无法上网，任何和互联网有关的操作都离不开TCP/IP协议。
- IPX/SPX协议：是Novell开发的专用于NetWare网络中的协议



4. 网关没有设置或设置不正确

- 网关是一个网络通向其他网络的IP地址，要实现这两个网络之间的通信，必须通过网关。如果网络A中的主机发现数据包的目的主机不在本地网络中，就把数据包转发给它自己的网关，再由网关转发给网络B的网关，网络B的网关再转发给网络B的某个主机。所以，只有设置好网关的IP地址，TCP/IP协议才能实现不同网络之间的相互通信。
- 不设置网关或设置不正确，同样是上不了网的。可以通过TCP/IP属性对话框来检查和设置。



5. DNS地址设置不正确

DNS设置不正确，就不能对IP地址进行解析，也就无法使用域名进行访问网络，而只能使用IP地址进行网络访问。

假若在访问一个网站时，在浏览器中的URL地址框中，输入IP地址能够访问某一网站，而输入域名就无法访问，首先检查是否设置了DNS地址，如果DNS地址设置没有问题，则大多是网站的域名服务器出现了问题。



服务器故障及其解决方法

1.服务器常见的故障及其排除方法

- 服务器中的某项服务被停止

由于用户过多，内存占用过大等原因，服务器上的服务被中止，

- 流量问题

由于服务器需要为大量的用户提供大量的服务，流量过大或大量的错误帧的出现，都有可能产生拥塞现象甚至是广播风暴，导致服务器的性能下降甚至死机。

- 系统资源不足

服务器上提供的服务越多，服务器对设置和硬件要求也就越高。若服务器的软、硬件资源不能满足要求，或由于计算机蠕虫等病毒抢占计算机资源，也会造成计算机性能下降或网络故障。



服务器故障及其解决方法

1.服务器常见的故障及其排除方法

○ 服务器软件故障

服务器软件故障是在服务器故障中占有比例最高的部份，约占70%。导致服务器出现软件故障的原因有很多，最常见的是服务器BIOS版本太低、服务器的管理软件或服务器的驱动程序有BUG、应用程序有冲突及人为造成的软件故障。服务器软件设置不当也会可能造成网络故障。如果其端口被其他服务占用，则该服务就不能正常运行，

○ 管理方面的问题

如用户的帐户和安全设置方面的潜在问题，服务权限没有给用户、配置不当或限制某些服务等问题



2. 服务器故障排除的基本原则

- 服务器故障排除的基本原则如下：

- (1) 尽量恢复系统缺省配置

- (2) 从基本到复杂

首先将存在故障的服务器独立运行，待测试正常后再接入网络运行，观察故障现象变化并处理；然后从可以运行的硬件开始逐步到现实系统为止；最后从基本操作系统开始逐步到现实系统为止。

- (3) 交换对比

首先在最大可能相同的条件下，交换操作简单效果明显的部件；其次是交换NOS载体，既交换软件环境；再者是交换硬件，既交换硬件环境；最后是交换整机，既交换整体环境。



- 在服务器故障排除时，需要收集如下一些信息：
- 服务器信息：机器型号(P/N:)、机器序列号(S/N:)、Bios 版本、是否增加其它设备（如网卡，SCSI 卡，内存，CPU等）、硬盘如何配置和安装什么操作系统及版本。
 - 故障信息：在POST（加电自检）时,屏幕显示的异常信息、服务器本身指示灯的状态和报警声，以及操作系统的事件记录文件等信息。
 - 以HP LH6000服务器来说，有红、黄、绿三种指示灯，绿灯常亮表示服务器正常；绿灯亮而黄色闪烁表示服务器有故障，但不是致命的；如果红、黄、绿三灯闪烁就表示服务器有致命故障，服务器停止运行。指示灯只能提示比较笼统的故障。
 - 确定故障类型和故障现象：开机无显示；上电自检阶段故障；安装阶段故障和现象；操作系统加载失败和系统运行阶段故障。



交换机故障

1. 硬件类故障

硬件故障主要指交换机电源、背板、模块、端口等部件的故障，可以分为以下几类：

- (1) 电源故障
- (2) 端口故障
- (3) 模块故障
- (4) 背板故障
- (5) 线缆故障



电源故障

- 由于外部供电不稳定，或者电源线路老化或者雷击等原因导致电源损坏或者风扇停止，从而不能正常工作。
- 解决办法：
 - 首先应该做好外部电源的供应工作，一般通过引入独立的电力线来提供独立的电源
 - 并添加稳压器来避免瞬间高压或低压现象。如果条件允许，可以添加**UPS**来保证交换机的正常供电，
 - 在机房内设置专业的避雷措施，来避免雷电对交换机的伤害。



端口故障

- 这是最常见的硬件故障
- 如果不小心把光纤插头弄脏，可能导致光纤端口污染而不能正常通信。
- 带电插拔接头从理论上讲是可以的，但是也无意中增加了端口的故障发生率。
- 在搬运时不小心，也可能导致端口物理损坏。
- 遇到此类故障，可以在电源关闭后，用酒精棉球清洗端口。如果端口确实被损坏，那就只能更换端口了。



模块故障

- 如果插拔模块时不小心，或者搬运交换机时受到碰撞，或者电源不稳定等情况，都可能导致此类故障的发生。
- 在排除此类故障时，首先确保交换机及模块的电源正常供电，然后检查各个模块是否插在正确的位置上，最后检查连接模块的线缆是否正常。在连接管理模块时，还要考虑它是否采用规定的连接速率，是否有奇偶校验，是否有数据流控制等因素。连接扩展模块时，需要检查是否匹配通信模式。



背板故障

- 如果环境潮湿，电路板受潮短路，或者元器件因高温、雷击等因素而受损都会造成电路板不能正常工作。如果散热性能不好或环境温度太高导致机内温度升高就会使元器件烧坏。
- 在外部电源正常供电的情况下，如果交换机的各个内部模块都不能正常工作，那就可能是背板坏了，唯一的解决办法就是更换背板。



线缆故障

- 接头接插不紧，线缆制作时顺序排列错误或者不规范，线缆连接时应该用交叉线却使用了直连线，光缆中的两根光纤交错连接，错误的线路连接导致网络环路等。



交换机故障

从上面的几种硬件故障来看，机房环境不佳极易导致各种硬件故障，所以在建设机房时，必须先做好防雷接地及供电电源、室内温度、室内湿度、防电磁干扰、防静电等环境的建设，为网络设备的正常工作提供良好的环境。



2. 交换机的软件故障

交换机的软件故障是指系统及其配置上的故障，它可以分为以下几类：

(1) 系统错误：交换机系统是硬件和软件的结合体。在交换机内部有一个可刷新的只读存储器，它保存的是这台交换机所必需的软件系统。由于设计的原因，可能会存在一些漏洞，在条件合适时，会导致交换机满载、丢包、错包等情况的发生。

对于此类问题，需要养成经常浏览设备厂商网站的习惯，如果有新的系统推出或者新的补丁，请及时更新。



2. 交换机的软件故障

(2) 配置不当：由于对交换机的性能等技术指标不熟悉可能会导致配置错误的出现。比如VLAN划分不当导致网络不通，端口被错误地关闭，交换机和网卡的模式配置不匹配等原因。这类故障有时很难发现，如果不能确保配置的正确性，最好先恢复出厂的默认配置，然后再一步一步地配置。

在配置之前先阅读说明书是好的习惯之一。每台交换机都有详细的安装手册、用户手册，深入到每类模块都有详细的讲解。如果还有不清楚之处就需要向供应商的工程师咨询后再做具体配置。



路由器故障

1. 硬故障

常见的硬故障通常表现在硬件上，一般有这么几种：

(1) 系统不能正常加电：表现为当打开路由器的电源开关时，路由器前面板的电源灯不亮，风扇不转。这时要重点检查电源系统，看供电插座是否有电，电压是否在规定的范围内？如果供电正常，应该检查电源线是否完好，接触是否牢靠，必要时可以换一根，如果还不行，可判定问题应该出在路由器的电源上。先检查路由器电源的保险是否完好，若烧了应该更换，若还不行只好送修。



路由器故障

1. 硬故障

(2) 电源和冷却系统的故障

- 当接通电源时，电源指示灯发亮。检查风扇是否正常工作。
- 若电源在启动后很快死机，则可能是环境过热引起的。路由器的工作环境温度应在 $0^{\circ}\text{C} \sim 40^{\circ}\text{C}$ 之间。
- 若路由器无法启动，但电源指示灯发亮，检查电源是否正常。
- 若路由器连续地或间歇地自动重启，可能是处理器或软件的故障，也可能是某条DRAM的安装不正确。



路由器故障

1. 硬故障

(3) 部件损坏：这类情况在硬件故障中是比较常见的一类，这里的部件往往是接口卡。表现为当把有问题部件插到路由器中时，系统其他部分都工作正常，但无法正确识别有问题的部件，这时往往是因为部件本身有问题。还有一种情况，就是部件可以被正确识别，但做完正确配置后，接口就是不能正常工作，这往往是因为存在物理故障。要确认以上这两种情况，最好用相同型号的好的部件替换怀疑有问题的部件，就可以确认问题是否存在了。



9.5.4 路由器故障

1. 硬故障

（4）系统软件损坏：如果路由器开机后总是进入rmon状态，这往往说明系统软件IOS存在问题，不妨将IOS重新写一遍。

（5）其他：这里所要提到的是这样一些情况，有时在对系统软件进行升级时，发现系统无论怎样也不能完成升级。这时不妨检查一下所要升级的软件的大小是否超过了路由器的NVRAM的容量。如果超过了，则无论如何也无法完成升级，这时应该先扩充NVRAM的容量，再升级系统软件。



2. 软故障

(1) 功能无法实现：有些时候，用户要作某些特定的配置(如 NAT)，反复检查后，确认配置正确，可相应的功能就是实现不了。这时先不要怀疑设备有问题，最好先找一找系统软件的版本号，并查找相关的说明，看一看所使用的软件的版本是否支持这个功能。因为路由器的系统软件往往有许多版本，每个版本支持不同的功能。如果当前的软件版本不支持这个功能，那就应该找到相应的软件，先进行升级。

(2) 网络规划存在问题：有些时候，配置似乎没有问题，可路由器就是不能正常工作，或者工作状态不稳定，总出现一些莫名其妙的问题。这时先不要急着反复调试，不妨回过头来看看用户的网络规划，看看是不是有问题。例如是不是有重复使用的网段，网络掩码的计算是否正确等等。

(3) 配置问题：这种问题是最常见的，例如线路两端路由器的参数不匹配或参数错误等等。这种情况只要认真细致地查找，总可以解决。



3. 路由器端口故障及排除

路由器端口包括串口、以太网口、异步通信端口等。端口故障往往是由于网络设备的配置问题而导致的逻辑故障。

(1) 串口故障的诊断与排除

对于串口故障的诊断，一般是用`show interface serial number`串口诊断命令来查看串口链路的状态，通过对这些屏幕显示内容的分析，可以找出串口问题之所在。



(2) 以太网接口故障诊断与排除

以太网接口的典型故障是：带宽的过分利用；碰撞冲突次数频繁；使用不兼容的帧类型。使用`show interface ethernet`命令显示以太网接口的状态，包括该接口的吞吐量、碰撞冲突、信息包丢失和帧类型等有关内容。通过对这些内容的分析，可以找出以太网端口故障的所在地。



(3) 异步通信口故障检测与排除

异步通信口故障一般的外部因素是：

- 拨号链路性能低劣；
- 电话网交换机的连接质量问题；
- 调制解调器的设置；



4.路由协议检测及解决

某些路由器路由设置不正确。可用 `traceroute` 命令察看路由走向，当发现需要检测时，用 `show ip route` 命令查看路由表，其路由表中是否存在所需要的路由。若不存在所需要的路由，可以用 `ip route` 等命令来添加路由。



5. 无法连接网络

- 如果在“网上邻居”中只能看到本机,而看不到同一个网段上的其他计算机,说明网络适配器的安装是正确的,首先确认网线是否插好,相关的网络设备(如HUB,交换机等)是否都工作正常. 检查网线是否正常,使用的是直通线还是交叉线



- 同一个网络是否有同名的情况
- Ping 127.0.0.1， 如果返回正常，说明本地 TCP/IP 安装正常。
- Ping 局域网上其他主机，如果正常，但是仍然无法在网上邻居中看到它，表示对方计算机没有打开“文件和打印机共享”服务



6. 无法实现网内计算机互访

- 实现windows网上邻居互访的基本条件：
 - 双方计算机正常运行，而且设置了网络共享资源
 - 双方计算机添加了“Microsoft网络文件和打印机共享”服务
 - 双方都正确设置了内网IP地址，且必须在一个网段中，所有的计算机都在同一个工作组（或域）
 - 双方计算机都关闭了防火墙，或者防火墙策略中没有设置阻止网上邻居访问的策略



问题1：一台计算机原来采用公网固定IP地址。为了避免被他人盗用，使用“`arp -s ip mac`”命令对MAC地址和IP地址进行了绑定。后来，由于某种原因，又使用“`arp -d ip mac`”命令取消了绑定。然而，奇怪的是，取消绑定后，在其他计算机上仍然不能使用该IP地址，而只能在原来的计算机上使用。需要说明的是，该计算机并不是代理服务器。

问题分析与处理：虽然在TCP/IP网络中，计算机往往需要设置IP地址后才能通讯，然而，实际上计算机之间的通讯并不是通过IP地址，而是借助于网卡的MAC地址。IP地址只是被用于查询欲通讯的目的计算机的MAC地址。

ARP协议是用来向对方的计算机、网络设备通知自己IP对应的MAC地址的。在计算机的ARP缓存中包含一个或多个表，用于存储IP地址及其经过解析的以太网MAC地址。一台计算机与另一台IP地址的计算机通讯后，在ARP缓存中会保留相应的MAC地址。所以，下次和同一个IP地址的计算机通讯，将不再查询MAC地址，而是直接引用缓存中的MAC地址。另外，需要注意的是，通过“-S”参数添加的项属于静态项，不会造成ARP缓存超时。只有终止TCP/IP协议后再启动，这些项才会被删除。所以，即使你取消了绑定，在短时间内其他计算机将仍然认为你采用的是原有IP地址。

在交换式网络中，交换机也维护一张MAC地址表，并根据MAC地址将数据发送至目的计算机。当绑定IP与MAC地址后，只要与交换机通讯过，交换机就会记录下该MAC地址。这样一来，即使后面有人使用了相同的IP地址，将依然不能与网关通讯，更连不通外面了，除非重新启动交换机、清除MAC表，或者MAC地址表超过了指定的老化时间。



问题2：一个局域网是用HUB连接的10Mbps以太网，为什么在传输文件时系统提示只有800KB/S的传输速率，有时候甚至会更少？

问题分析与处理：这是因为速率的计量方式不同引起的。一种是Bit比特位，一种是Byte字节。网络带宽通常以bps(bit/s)作为计量单位，即“Bits-Per-Second(每秒的比特位数量，通常又被译为波特率)”，而许多下载工具软件的计量单位是Byte/S，所以，两者之间相差8倍。

除了计量方式的问题，网络无法达到标准传输速率的主要原因：

- 集线器的限制：假设一个16口的集线器为10Mbps共享带宽，如果所有端口均处于通讯状态，每个端口可获得的传输速率约每秒0.625MB($10\text{ MB} \div 16$)。若欲获得接近理论带宽的传输速率，必须采用交换机作为集线设备。
- 网卡的原因：如果网卡质量不好，发出的数据包经常出现错误，导致数据包经常重发，或收到的数据包错误比较多，也会导致拷贝文件速度降低。
- 网线的原因：如果网线太长，信号衰减比较厉害，或者虽然网线距离近，但网线质量不好，也不能达到理论速度。另外，当网络繁忙时，也达不到理想速度。



问题3：为什么一台计算机可以Ping通IP地址，
但Ping不通域名？

问题分析与处理：TCP/IP协议中的“DNS设置”不正确，先检查其配置。

另外，产生这一问题的原因也可能是域名解析服务器出了问题，可能是自己的域名服务器出故障，也可能是上一级的域名服务器不正常，本级域名服务器ping不到。上级域名服务器不正常。如一时解决不了，可在TCP/IP的配置中换一个DNS服务器即可。



案例1

- 现象： 局域网内所有的服务器和客户端都是用交换机接入的，其中一套计算机不能上网了。
- 检查：
 - 1. 计算机网卡 ,link 指示灯亮但不闪烁-> 有物理链路连接，但没有数据传输
 - 2. ipconfig 查看 IP 地址，没问题
 - 3. ping 本机 IP地址, 正确响应-> 网络配置和网卡没太大问题
 - 4. ping 网关，没有正确响应-> 计算机跳线到交换机端口线路存在问题
 - 5. link 指示灯亮-> 线路没问题
 - 6. 观察交换机端口指示灯link 是绿色的-> 有连接
 - 7. 采用替代法，把该端口的跳线换一个端口，该计算机能ping通网关,换回端口（甚至重启交换机），都不行->原端口故障
 - 8. 用交换机提供的web 方式登陆到交换机，查看该端口状态，无发现冲突、碎片等故障状态,关闭电源，使用酒精棉球清洗，酒精挥发后，在打开交换机，故障排除。



案例2

- 现象：一个学生计算机房，一台教师机，64台学生机，通过三台交换机接入网络，某天突然所有的机都不能上网，而且计算机也变得很慢。前一天正常，之间除了清洁工，没人到过机房
- 检查和分析：
 - 1. 计算机设置错误的可能不大
 - 2. 学生机不可能中毒，教师机查杀病毒，没有发现
 - 3. 计算机网线拔掉，系统运行正常，插上网线，系统又变慢，重启交换机无效
 - 4. 观察交换机状态，所有端口的ACT (ACTIVE)指示灯亮着，但不闪烁。查说明书，说明可能存在环路。
 - 5. 三台交换机启用STP，故障消失-> 果然存在环路
 - 6. 关闭所有计算机，网卡没电-> 相连的交换机端口应该不亮
 - 7. 发现交换机两端口同时亮着 -> 清洁工惹的祸



本章小结

本章介绍了网络故障的诊断与网络维护的相关知识。主要掌握网络故障产生的原因，故障诊断的原理，以及故障排除的步骤等内容。首先介绍了网络故障诊断的目的、故障产生的原因、排除的方法和步骤，然后介绍了网络故障的分类，以及故障分层检查的原理。接着介绍了网络故障诊断的常用软、硬件工具。最后介绍了常见网络故障及排除方法。

分层检查指导故障分别定位于物理层、数据链路层、网络层、传输层和应用层，分段诊断也是常用的方法之一，即把故障定位于某一网段的设备上。



作业

- 故障排除的基本步骤是什么？
- 交换机的故障有哪些？
- 路由器的故障有哪些？
- 网络测试工具有哪些？