 与windows系统一样，linux操作系统也会存在很多问题和故障，很多linux新手都害怕故障，面对出现的问题显得无可奈何，更有甚者，由此放弃了linux，其实，我们不应该惧怕问题，学习就是一个发现问题与解决问题的过程，只要掌握了解决问题的基本思路，一切故障都会迎刃而解，当然前提是我们已经具备了解决问题的思路和扎实的知识功底。

**一、处理linux系统故障的思路**作为一名合格的linux系统管理员，一定要有一套清晰、明确的解决故障思路，当问题出现时，才能迅速定位、解决问题，这里给出一个处理问题的一般思路：  
 重视报错提示信息：每个错误的出现，都是给出错误提示信息，一般情况下这个提示基本定位了问题的所在，因此一定要重视这个报错信息，如果对这些错误信息视而不见，问题永远得不到解决。  
 查阅日志文件：有时候报错信息只是给出了问题的表面现象，要想更深入的了解问题，必须查看相应的日志文件，而日志文件又分为系统日志文件（/var/log）和应用的日志文件，结合这两个日志文件，一般就能定位问题所在。  
 分析、定位问题：这个过程是比较复杂的，根据报错信息，结合日志文件，同时还要考虑其它相关情况，最终找到引起问题的原因。  
 解决问题：找到了问题出现的原因，解决问题就是很简单的事情了。  
从这个流程可以看出，解决问题的过程就是分析、查找问题的过程，一旦确定问题产生的原因，故障也就随之解决了。

**二、 忘记linux root密码**  
这个问题出现的几率是很高的，不过，在linux下解决这个问题也很简单，只需重启linux系统，然后引导进入linux的单用户模式（init 1），由于单用户模式是不需要输入登录密码的，因此，可以直接登录系统，修改root密码即可解决问题。  
下面是详细的处理方法，这里我们以Redhat linux为基准，操作步骤如下：  
（1） 重启系统，待linux系统启动到grub引导菜单时，找到当前系统引导选项（可以按方向键展开隐藏的菜单，单处理器只有一个引导项，多处理器有3个或3个以上引导项，一般默认选项就是系统当前引导选项）。  
（2） 通过方向键将光标放到当前系统引导项上，然后按键盘字母“e”，进入编辑状态。  
（3） 然后通过上下键，选中带有kernel指令的一行，继续按键盘字母“e”，编辑该行，在行末尾加个空格，然后添加single，类似与这样：  
kernel  /vmlinuz-2.6.18-8.el5 ro root=LABEL=/ rhgb quiet single  
（4） 修改完成，按回车键，返回到刚才的界面。  
（5） 最后按键盘“b”，系统开始引导。  
这样系统就启动到了单用户模式下，这里的单用户根windows下的安全模式类似，在单用户模式下，只是启动最基本的系统，网络以及应用服务均不启动。单用户模式启动完毕，系统会自动进入到命令行状态下，类似与“sh-3.1#”，然后直接执行passwd，回车，系统会提示输入新的root密码两次，最后会看到修改密码成功的提示，这样就完成了root密码的修改。如果需要正常启动系统，现在只需输入“init 3”，就进入了多用户模式。用root用户重新登录系统，看看设置的新密码是否生效。

**三 linux系统无法启动的解决办法**导致linux无法启动的原因有很多，常见的原因有如下几种：  
 文件系统配置不当，比如/etc/inittab文件、/etc/fstab文件等配置错误或丢失，导致系统错误，无法启动。  
 非法关机，导致root文件系统破坏，也就是linux根分区破坏，系统无法正常启动  
 Linux内核崩溃，从而无法启动  
 系统引导程序出现问题，比如grub丢失或者损坏，导致系统无法引导启动。  
 硬件故障，比如主板、电源、硬盘等出现问题，导致linux无法启动。  
从这些常见的故障可知，导致系统无法启动的主要有两个问题，硬件原因和操作系统原因，对于硬件出现的问题，只需通过更换硬件设备，即可解决，而对于操作系统出现的问题，虽然出现的问题可能千差万别，不过在多数情况下都可以用相对简单统一的一些方法来恢复系统，下面我们就针对上面提出的几个问题，结合Redhat Linux系统环境，给出一些常用的、普遍的解决问题的方法。

1．/etc/fstab文件丢失，导致系统无法启动  
/etc/fstab文件存放了系统中文件系统的相关信息，如果正确的配置了该文件，那么在linux启动时，系统会读取此文件，自动挂载linux的各个分区，如果此文件配置错误，或者丢失，就会导致系统无法启动，具体的故障现象是在检测mount partition时出现：  
starting system logger  
 此后系统启动就停止了。  
针对这个问题，我们的第一思路就是想办法恢复/etc/fstab这个文件的信息，只要恢复了此文件，系统就能自动挂载每个分区，正常启动。可能很多读者首先想到的是将系统切换到单用户模式下，然后手动挂载分区，最后结合系统信息，重建/etc/fstab文件。  
但是这种方法是行不通的，因为fatab文件丢失导致linux无法挂载任何一个分区，即使linux还能切换到单用户下，那么此时的系统也只是一个read-only的文件系统，无法向磁盘写入任何信息。  
我们介绍另外一个方法，就是利用linux rescue修复模式登录系统，进而获取分区和挂载点信息，重构/etc/fstab文件。  
这里以rhel5为例，首先将系统第一章光盘放入光驱，设置BOIS从光驱启动，这样系统就从光驱引导，然后在boot后输入：linux rescue，如图1所示：

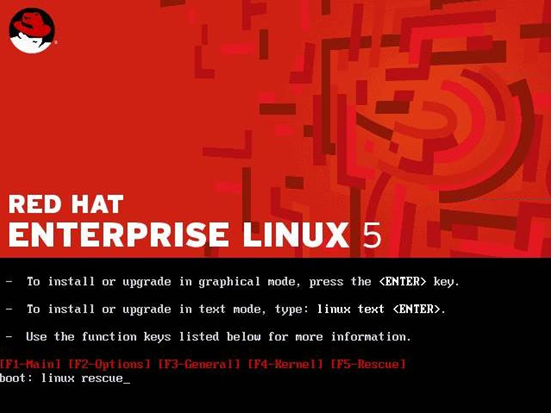
[](http://img1.51cto.com/attachment/201105/131010719.png)

图1设置linux进入修复模式

接着系统自动开始引导，进入图2所示画面：

[](http://img1.51cto.com/attachment/201105/131031494.png)

图2 选择语言

这里是选择模式使用的语言，可以按照自己需要设定，我们这里选择“English“，然后按tab键，选中“ok”，回车进入下一步。  
 下面进入的是键盘选择界面，如图3所示，这里选择默认的“us”即可。

[](http://img1.51cto.com/attachment/201105/131056864.png)

 图3 选择键盘类型

下面进入网络配置界面，如图4所示：

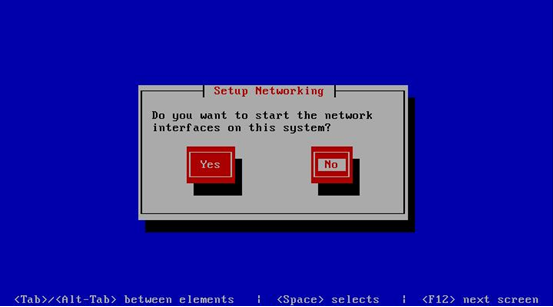
[](http://img1.51cto.com/attachment/201105/131115302.png)

图4 是否启用网络

这里是选择是否启用网络，由于系统已经无法启动，我们已经在linux系统上进行操作了，启用网络与否都无所谓。这里选择不启用。  
下面到了最关键的步骤了，如图5所示，修复模式会自动将系统的所有分区挂载到/mnt/sysimage目录下，选择“Continue”，则修复环境进入到read-write状态下，可以对分区进行读写操作，选择“Read-Only”，修复环境进入到只读模式，由于我们要重建fstab文件到/etc目录下，因此选择“Continue”进入可读写模式下。

[](http://img1.51cto.com/attachment/201105/131151123.png)

图5 选择修复模式的启动方式

下面是一个友情提示界面，如图6所示，由于fstab文件丢失，修复模式找不到任何可挂载的分区，从这里可知，修复模式在这里也读取/etc/fstab文件，回车，进入下一步。

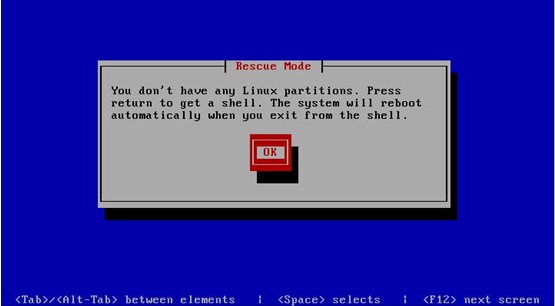
[](http://img1.51cto.com/attachment/201105/131211228.png)

图6 无法挂载系统任何分区

下面就进入了修复环境下，可以进行操作了。如图7所示

[](http://img1.51cto.com/attachment/201105/131232739.png)

图7 修复模式命令行

上面详细演示了如何进入linux的修复模式，其实很多情况下，linux无法启动时，都可以通过这个方式登录系统进行修复和更改操作。  
下面是恢复/etc/fstab文件的详细过程：  
首先查看一下系统分区情况，如下所示

sh-3.1# fdisk -l  
Disk /dev/sda: 42.9 GB, 42949672960 bytes  
255 heads, 63 sectors/track, 5221 cylinders  
Units = cylinders of 16065 \* 512 = 8225280 bytes  
Device Boot      Start       End      Blocks   Id  System  
/dev/sda1   \*     1         25     200781   83  Linux  
/dev/sda2       26        1300    10241437+  83  Linux  
/dev/sda3      1301        1682     3068415   83  Linux  
/dev/sda4      1683        5221    28427017+  5  Extended  
/dev/sda5      1683        1873     1534176   83  Linux  
/dev/sda6      1874        2064     1534176   83  Linux  
/dev/sda7      2065        2255     1534176   83  Linux  
/dev/sda8      2256        2382     1020096   83  Linux  
/dev/sda9      2383        2484     819283+  82  Linux swap / Solaris  
/dev/sda10      2485        5221    21984921  83  Linux

因为分区并没有损坏，通过fdisk命令可以查看到系统分区的完整信息，但是每个分区对应的label name信息我们还不知道，下面通过e2label命令查看每个分区对应的label name：  
sh-3.1# e2label /dev/sda1  
/boot  
sh-3.1# e2label /dev/sda2  
/usr  
sh-3.1# e2label /dev/sda3  
/  
sh-3.1# e2label /dev/sda5  
/var  
sh-3.1# e2label /dev/sda6  
/tmp  
sh-3.1# e2label /dev/sda7  
/home  
sh-3.1# e2label /dev/sda8  
/opt  
sh-3.1# e2label /dev/sda10  
/webdata  
这样，就得到了所有分区的挂载点信息，接下来就可以构造一个fstab文件了。  
小技巧：可以参考其它系统中fstab文件的格式，结合本系统的分区和挂载点信息，构造出自己的fstab文件来。  
由于fstab文件是存放在系统根目录下的，因此需要挂载原来系统的根分区，从上面可知根分区对应的设备名为/dev/sda3，接着在修复模式创建的临时根分区下创建一个挂载点，然后挂载原来系统的根分区。操作过程如下所示：

sh-3.1# pwd  
/  
sh-3.1# mkdir temp  
sh-3.1# mount /dev/sda3  /temp  
sh-3.1# df     
Filesystem           1K-blocks   Used Available Use% Mounted on  
/dev              515644      0    515644  0% /dev  
/tmp/loop0           79872     79872   0 100% /mnt/runtime  
/dev/sda3           2972268    259916   2558932 10% /temp

这样以来，原有根分区的文件全部挂载到了/temp目录下，接着就可以创建我们需要的fatab文件了。

sh-3.1# vi /temp/etc/fstab  
LABEL=/ /        ext3    defaults        1 1  
LABEL=/boot     /boot    ext3    defaults        1 2  
LABEL=/cicro    /cicro     ext3   defaults        1 2  
devpts     /dev/pts    devpts  gid=5,mode=620 0 0  
tmpfs       /dev/shm    tmpfs   defaults        0 0  
LABEL=/home   /home      ext3    defaults        1 2  
LABEL=/opt    /opt      ext3    defaults        1 2  
proc     /proc      proc    defaults        0 0  
sysfs    /sys      sysfs   defaults        0 0  
LABEL=/tmp     /tmp      ext3    defaults        1 2  
LABEL=/usr     /usr      ext3    defaults        1 2  
LABEL=/var  /var      ext3    defaults        1 2  
LABEL=SWAP-sda9   swap    swap    defaults        0 0

配置完毕，保存退出，然后重启系统。  
sh-3.1#reboot

2、root文件系统破坏，导致系统无法启动  
Linux下普遍采用的是ext3文件系统，ext3是一个具有日志记录功能的日志文件系统，可以进行简单的容错和恢复，但是在一个高负荷读写的ext3文件系统下，如果突然发生掉电，就很有可能发生文件系统内部结构不一致，导致文件系统破坏。  
Linux在启动时，会自动去分析和检查系统分区，如果发现文件系统有简单的错误，会自动修复，如果文件系统破坏比较严重，系统无法完成修复时，系统就会自动进入单用户模式下或者出现一个交互界面，提示用户介入手动修复，现象类似下面所示：  
checking root filesystem  
/dev/sdb5 contains a file system with errors, check forced  
/dev/sdb5:  
Unattached inode 68338812  
/dev/sdb5: UNEXPECTED INCONSISTENCY; RUN fsck MANUALLY  
(i.e., without -a or -p options)  
FAILED  
/contains a file system with errors check forced   
an eror occurred during the file system check   
\*\*\*\*dropping you to a shell;the system will reboot   
\*\*\*\*when you leave the shell   
Press enter for maintenance  
(or type Control-D to continue):  
give root password for maintenance  
从这个错误可以看出，系统根分区文件系统出现了问题，系统在启动时无法自动修复，然后进入到了一个交互界面，提示用户进行系统修复。  
这个问题发生的机率很高，引起这个问题的主要原因就是系统突然掉电，引起文件系统结构不一致。一般情况下解决此问题的办法是采用fsck命令，进行强制修复。  
根据上面的错误提示，当按下“Control-D”组合键后系统自动重启，当输入root密码后进入系统修复模式，在修复模式下，可以执行fsck命令，具体操作过程如下：  
[root@localhost /]#umount /dev/sdb5  
[root@localhost /]#fsck .ext3 -y  /dev/sdb5   
e2fsck 1.39 (29-May-2006)  
/ contains a file system with errors, check forced.  
Pass 1: Checking inodes, blocks, and sizes  
Pass 2: Checking directory structure  
Pass 3: Checking directory connectivity  
Pass 4: Checking reference counts  
Inode 6833812 ref count is 2, should be 1.  Fix<y>? yes  
Unattached inode 6833812  
Connect to /lost+found<y>? yes  
Inode 6833812 ref count is 2, should be 1.  Fix<y>? yes  
Pass 5: Checking group summary information  
Block bitmap differences:  -(519--529) -9273  
Fix<y>? yes  
…… ……  
/: \*\*\*\*\* FILE SYSTEM WAS MODIFIED \*\*\*\*\*  
/: 19/128520 files (15.8% non-contiguous), 46034/514048 blocks  
 上面就是fsck修复受损文件系统的过程，fsck详细用法在本书第四章有详细的讲述，这里不在多讲。需要注意的是，在执行fsck的时候，一定要先卸载要修复的分区，然后再执行修复操作，切记！

**三、其它故障的一般解决方案**如果是linux的引导程序出现问题，那么也可以通过光盘引导的方式进入linux修复模式，然后修改对应的引导程序或者重新安装引导程序。  
如果linux内核崩溃或者丢失，同样可以先进入linux rescue下，然后加载root分区，最后重新编译内核。  
如果出现了最坏的情况，文件系统破坏严重，同时内核也崩溃，那么此时重新安装系统反而比较容易，在这种情况下可以先将linux上有用的数据和文件备份转移到其它设备，然后对整个文件系统进行全新安装。  
在这里我们不可能对每个出现的问题，都给出详细的解决方案，问题都是千差万别的，每个问题的处理都不尽相同，本书要传授给大家的是当linux系统出现问题后，解决问题的一般思路和通用策略，熟练掌握了这些技巧，处理任何linux问题都能游刃有余。

**四、 linux下常见网络故障处理**  
linux网络服务功能非常强大，在linux上可以部署Web Server、DNS Server、Mail Server、Db server、Ftp server等等，但是也由此产生了很多网络问题，据统计，在linux系统下产生的故障，有60％来自网络方面，40%来自系统本身，可见熟练解决linux下故障，对于熟练掌握linux有着巨大的帮助。  
解决linux网络问题的顺序应该是首先从Linux操作系统自身的底层网络开始，然后逐步有点及面的向外扩展，网络问题的一般解决流程为：   
 网络硬件传输问题，可以通过检查网线是否正常，网卡、集线器、路由器、交换机等是否正常来确认是否由硬件问题造成网络故障。  
 检查网卡是否能正常工作，可以从网卡是否正常加载、网卡IP设置是否正确、系统路由是否设置正确3个方面进行检查确认。  
 检查DNS是否设定正确，可以从linux的DNS客户端配置文件/etc/resolv.conf，本地主机文件/etc/hosts进行检查确认。  
 服务是否正常打开，可以通过telnet或者netstat命令的方式检测服务是否开启。  
 访问权限是否打开，可以从本机iptables防火墙、linux内核强制访问控制策略selinux两方面入手，进行检查确认。  
 局域网主机之间联机是否正常； 可以通过ping自身IP，ping局域网其它主机IP，ping网关地址来确认局域网是否连接正常。  
接下来，我们就针对上面给出的解决网络问题的一般思路，详细展开讲述。

1. 检查网络硬件传输问题  
检查网络故障，首先要排除的是网络硬件设备是否存在问题，比如网线是否正常，网卡、集线器、路由器、交换机等是否正常，这些是网络正常运行的基本条件，如果发现某些设备出现故障，只需更换硬件即可解决问题。

2．检查网卡是否能正常工作  
（1）检查网卡是否正常加载  
通过lsmod、ifconfig命令可以判断网卡是否正常加载，如果通过ifconfig可以显示网络接口（eth0、eth1等等）的配置信息，表示系统已经认到了网卡驱动程序，检测到了网络设备，网卡加载正常。  
（2）检查网卡IP设置是否正确  
 接下来就要检查网卡的软件设定，比如IP是否配置，配置是否正确，确保IP的配置和局域网其它计算机配置没有冲突。  
（3）检查系统路由表信息是否正确  
 最后就是要检查系统的路由表设置是否正确，如果一个linux系统有两块网卡，同时两块网卡设置的IP不在一个网段，要特别注意系统路由表的设置。  
例如下面这个系统的网络接口信息：  
[root@webserver ~]#  ifconfig  
eth0      Link encap:Ethernet  HWaddr 00:12:3F:FF:65:24    
          inet addr:10.10.1.239  Bcast:10.10.1.255  Mask:255.255.255.0  
          inet6 addr: fe80::212:3fff:feff:6524/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:20632289 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:20223702 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000   
          RX bytes:793608426 (756.8 MiB)  TX bytes:2567481473 (2.3 GiB)  
          Interrupt:201   
eth1      Link encap:Ethernet  HWaddr 00:12:3F:FF:65:25    
          inet addr:192.168.200.30  Bcast:192.168.200.255  Mask:255.255.255.0  
          inet6 addr: fe80::212:3fff:feff:6525/64 Scope:Link  
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1  
          RX packets:15496910 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:8028739 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:1000   
          RX bytes:1048038084 (999.4 MiB)  TX bytes:3195989266 (2.9 GiB)  
          Interrupt:209   
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:508961 errors:0 dropped:0 overruns:0 frame:0  
          TX packets:508961 errors:0 dropped:0 overruns:0 carrier:0  
          collisions:0 txqueuelen:0   
          RX bytes:574086961 (547.4 MiB)  TX bytes:574086961 (547.4 MiB)  
从上面输出可知，本系统有两块网卡，分别配置不同网段的IP地址，假定eth0通过映射的方式对外提供ssh连接服务，而eth1仅供局域网主机之间共享数据使用。  
现在的问题是，外界无法ssh远程登录到此系统，而网卡加载没有问题，网卡IP设置也没问题，接下来看看此系统的路由设置：

[root@webserver ~]#  route  
Kernel IP routing table  
Destination    Gateway    Genmask    Flags Metric Ref    Use Iface  
10.10.1.0       \*    255.255.255.0   U     0  0     0 eth0  
192.168.200.0   \*    255.255.255.0   U     0  0     0 eth1  
default    192.168.200.1   0.0.0.0   UG    0  0     0 eth1  
到这里，问题已经基本排查出来了：从route的输出可知，linux的缺省路由是192.168.200.1，而192.168.200段的IP仅仅供局域网主机之间共享数据使用，没有连接出去的访问权限，因而，外界无法连接到linux系统，也是理所当然的事情了。  
定位了问题，解决方法很简单，删除192段的缺省路由，然后增加10段的缺省路由即可：  
[root@webserver ~]# route delete default  
[root@webserver ~]#route add default gw 10.10.1.254  
此时外界就可以通过ssh服务远程连接到linux系统了。

3．检查DNS解析文件是否设置正确  
在Linux系统中，有两个文件用来指定系统到哪里寻找相关域名解析的库。分别是文件/etc/host.conf和/etc/nsswitch.conf。  
/etc/host.conf文件指定系统如何解析主机名，Linux通过域名解析库来获得主机名对应的IP地址。下面是RedHat Linux安装后缺省的/etc/host.conf内容：  
order hosts,bind  
其中，order指定主机名查询顺序，这里表示首先查找/etc/hosts文件对应的解析，如果没有找到对应的解析，接着就根据/etc/resolve.conf指定的域名服务器进行解析。  
/etc/nsswitch.conf文件是由SUN公司开发的，用于管理系统中多个配置文件查询的顺序，由于nsswich.conf提供了更多的资源控制方式，nsswich.conf文件现在已经基本取代了hosts.conf，虽然LINUX系统中默认这两个文档都存在，但实际上起作用的是nsswitch.conf文件。  
nsswitch.conf文件每行的配置都以一个关键字开头，后跟冒号，紧接着是空白，然后是一系列方法的列表。  
例如这段信息：  
hosts:   files dns  
表示系统首先查询主机库文件，如果没有找到对应的解析，接着会去DNS配置文件指定的DNS服务器进行解析。  
清楚了linux下域名解析的原理和过程，我们就可以根据这两个文件的设定，确定解析的顺序，从而判断出域名解析可能出现的问题。

4．检查服务是否正常打开  
在一个应用出现故障时，必须要检查的就是服务本身，比如服务是否开启，配置是否正确等等，检查服务是否正确打开，分为两步，第一步是查看服务的端口是否打开：  
例如，我们不能用root用户ssh登录到192.168.60.133这台linux服务器，首先检查sshd服务的22端口是否打开：  
[root@localhost init.d]# telnet 192.168.60.133 22  
SSH-2.0-OpenSSH\_4.3  
这个输出表示192.168.60.133的22端口对外开放，或者可以说sshd服务是处于打开状态。如果没有任何输出，可能是服务没有启动，或者服务端口被屏蔽。  
也可以在服务器上通过netstat命令检查22端口是否打开：

[root@localhost xinetd.d]# netstat -ntl  
tcp        0      00.0.0.0:3306   0.0.0.0:\*      LISTEN        
tcp        0      0 :::80        :::\*       LISTEN        
tcp        0      0 :::22      :::\*       LISTEN        
可以看到，22端口在服务器上是打开的，同时，服务器上打开的还有3306、80端口。  
接着进行第二步的检查，既然服务已经打开，可能是sshd服务配置的问题，检查sshd服务端配置文件/etc/ssh/sshd\_config，发现有下面一行信息：  
PermitRootLogin no  
由此可知是ssh服务端配置文件限制了root用户不能登录系统，如果需要root登录系统，只需更改为如下即可：  
PermitRootLogin yes  
到这里为止，我们通过对端口和服务配置文件的层层检查，最终找到了问题的根源。需要说明的是，这里的重点不是讲述如何让root登录linux系统，而是要通过这个例子让读者学会处理类似问题的思路和方法。

5．检查访问权限是否打开  
（1）检查系统防火墙iptables的状态  
当某些服务不能访问时，一定要检查是否被linux本机防火墙iptables屏蔽了，可以通过iptables -L指令查看iptables的配置策略，例如我们不能访问某台linux服务器提供的www服务，通过检查，系统网络、域名解析都正常，并且服务也正常启动，然后检查了服务器的iptables策略配置，信息如下：  
[root@localhost ~]# iptables -L -n  
Chain INPUT (policy DROP)  
target     prot opt source               destination  
Chain FORWARD (policy ACCEPT)  
target     prot opt source               destination  
Chain OUTPUT (policy DROP)  
target     prot opt source               destination  
从上面的输出可知，这个linux服务器仅仅设置了预设策略，而致命的是将INPUT链和OUTPUT链都设置为DROP，也就是所有外部数据不能进入服务器，服务器数据也不能出去，这样的设置相当于没有网络。  
为了能访问这台服务器提供的www服务，增加两条策略即可：  
[root@localhost ~]#iptables -A INPUT -i eth0 -p tcp --dport 80 -j ACCEPT  
[root@localhost ~]#iptables -A OUTPUT -p tcp --sport 80 -m state --state ESTABLISHED -j ACCEPT  
这样以来，internet上的其他人就能访问我们的www服务了。  
（2）检查selinux是否打开  
 在前面的章节，我们已经讲述过selinux的含义和功能，它可以最大限度地保证Linux系统的安全，但是selinux有时也会给linux下软件的运行带来一些问题，这些问题大部分是对selinux不了解造成的，为了迅速定位问题，最简单的方法是先关闭selinux，然后测试软件运行是否正常，这不是个好方法，但是对于判断问题往往是很有用的，selinux是个很好的安全访问控制软件，可是如果你还不能熟练运用selinux访问控制策略的话，还是建议将它暂时关闭，等到对linux有了更深入的认识后，再开启selinux不失为一个明智的策略。

6．检查局域网主机之间联机是否正常  
通过上面5步的检查，linux系统自身的问题已经基本排除，接下来需要扩展到linux主机之外的网络环境，检查网络之间的连通是否存在故障，可以先通过ping命令测试局域网主机之间的连通性，然后ping网关，检测主机到网关的通信是否正常。  
任何网络故障的出现，都是有原因的，只要我们根据上面给出的解决问题流程，逐一排查，99%的问题都能得到很好的解决。