China-pub.com
下载

China-pub.com
下载

第2章　配置TCP/IP

从早期版本的UNIX起，传输控制协议/Internet协议（TCP/IP）都是集成到了操作系统之中的，Linux也不例外。事实上，Linux的TCP/IP协议栈已经重新设计过好几遍了。设计当前版本的人认为其速度和可靠性比其对手的任何实现都要好。

可能许多基于TCP/IP的重要网络都受UNIX的影响。如果网络通过某种方式连到了Internet，它就要依赖于根名字服务器（运行的是UNIX）。如果网络使用全球的SMTP邮件系统，就要和各种UNIX系统打交道。如果网络要访问World Wide Web，世界上每两个Web服务器中的一个运行的就是UNIX上的Apache。当然，也可以在其他操作系统上实现这些协议，但UNIX是原创，而且UNIX也是最好的实现。

本章讨论TCP/IP及基本的网络服务。对物理网络介质（通常为以太网）只做简单介绍。如果配置正确的话，系统在安装过程中应该能自动检测到硬件。关于网络线缆方面的知识随处可见，本章只略提一二。

2.1　基本的IP配置

本节试图阐述基本TCP/IP配置的三大部件：IP地址、缺省网关和DNS服务器。

如果主机连到了一个C类IP网络（允许254台主机系统的网络），并且没有连到外部网络和/或Internet上，则只需要一个配置参数（IP地址）。

2.1.1　IP地址

标准IP地址是一个无符号的32位整数，但它们经常被表示成用点分隔的十进制的4个无符号字节。例如IP地址C0A80101将表示成192.168.1.1。TCP/IP网络（或互联网）上的每一台计算机都必须拥有一个独一无二的IP地址。输入IP地址的同时，用户还必须提供网络屏蔽码和广播地址，这些将在稍后介绍。

对于连到需要路由的TCP/IP网络的计算机，一般都需要缺省网关地址。

2.1.2　缺省网关

缺省网关地址即路由器的IP地址，路由器是位于本地网络，并连向其他网络或Internet的网络设备。对于C类IP地址，只有路由器IP地址的最后一个字节与本地网络上其他主机的IP地址不同。要注意的是，路由器经常有一个以上的IP地址。用户只需选择其在本地网络上的那一个IP地址。

如果计算机连到了Internet上（或者连到了另一个执行DNS的TCP/IP网络），则需要最后一个参数。

2.1.3　DNS服务器

域名服务器（Domain Name Server, DNS）是一台能将Internet主机名转换成IP地址的计算

China-pub.com
下载

机。例如，在本书成文之时， www.redhat.com的IP地址为199.183.24.133。DNS服务器提供这种转换——它通过将查询发向分布式的、容错性强的域名系统而达到目的。

在C类IP网络中，网络屏蔽码几乎总是255.255.255.0。网络号是通过将网络上IP地址的最后一个数字变成0（即将IP地址同网络屏蔽码按位逻辑乘）而得到的。如果需要广播地址的话，将网络号的最后一个字节改成255即可（数据将发往本地网络的所有主机——ping广播地址将得到最多254个其他主机的应答）。

例如，假设构建的是一个小型的家庭网络，该网络并不连往Internet（至少大多数时候不连到Internet）。表2-1是IP地址、网络屏蔽码和广播地址的很好选择。

表2-1 基本IP配置

IP地址	192.168.1.1
网络屏蔽码	255.255.255.0
广播地址	192.168.1.255

如果网络中增加了另外一台计算机，可以为其分配IP地址：192.168.1.2，直到192.168.1.254。IP网络上的所有主机必须共享相同的网络号。如果 C类主机192.168.1.5和192.168.100.5直接连接，中间没有网关，它们就不能通信，因为它们不共享相同的网络号。

创建一个包含IP地址和主机名字对的 /etc/hosts文件是一个好主意。这使网络中的主机无需相互记住IP地址。DNS服务器把该功能扩展到大型网络上。

请注意，C类网络号192.168.1.0是用于家庭网络的最佳选择（第4章将进行详细阐述）。

现在，我们假设某个邻居也组建了一个家庭网络，他使用网络号 192.168.2.0。如果在两个家庭之间连上网络线缆，并安装好路由器，则两个网络就可以互相通信。路由器要求两个IP地址，通常选择192.168.1.254和192.168.2.254（254分配给网关，主机1分配给DNS服务器，这也是Red Hat在安装时假设的值）。如果给出明确指示的话， Linux也可以作为一个路由器——在Red Hat Linux中，这种行为由/etc/sysconfig/network文件控制。该文件还包含缺省网关的IP地址。对该文件进行的设置通常在引导时产生作用。第一个网络上的主机可以定义其缺省网关为192.168.1.254，任何不属于本地网络的数据将自动发向远程网络。如果所连接的不止两个本地网，则缺省路由不能用来引导流量，需要更为复杂的路由表。

注意，图2-1和图2-2是netcfg工具的屏幕剪辑。如果安装了网络接口的话，用户可以使用netcfg来编辑网络接口配置。

Linuxconf工具也可用来增加网络设备。在清单 2-1中，配置了一个3Com 509以太网网卡。

清单2-1 使用linuxconf配置以太网接口

```
************ This host basic configuration *************
* You are allowed to control the parameters             *
* which are specific to this host and related           *
* to its main connection to the local network           *
*                                                       *
*                     ********************************
*                     ***********Adaptor 2*************
*                     *[X] Enabled                    **
*Config mode          *(o) Manual ( ) Dhcp ( ) Bootp **
*Primary name + domain *                              **
*Aliases (opt)        *                               **
*IP address           *192.168.1.1                    **
*Netmask (opt)        *255.255.255.0                 ***
*Net device           *eth1                          ***
*Kernel module        *3c509                         ***
*I/O port (opt)       *                               **
```

China-pub.com 下载

```
*Irq (opt)              *                                  ***
*                       ***********Adaptor 3*************
*                       *[ ] Enabled                       **
*                       ***********************************
*       ********         ********        ******          *
*       *Accept*         *Cancel*        *Help*          *
*       ********         ********        ******          *
*************************************************************
```

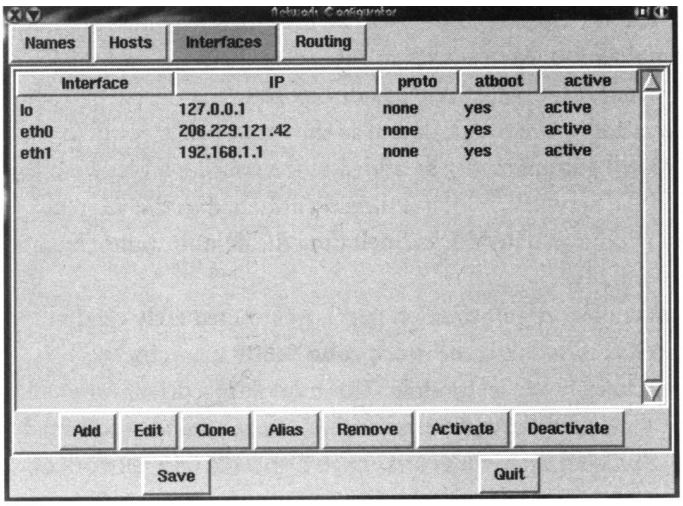


图2-1 netcfg工具

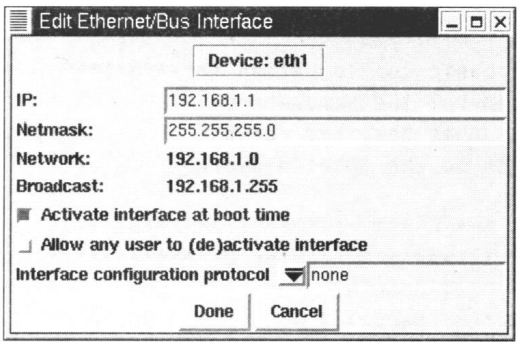


图2-2 使用netcfg配置接口

命令行也可以完成相同的操作，方法是输入下面的命令：

```
# modprobe 3c509.o
eth1: 3c509 at 0x300 tag 1, 10baseT port,
address  00 60 97 a6 b0 e5, IRQ 10.
3c509.c:1.16 (2.2) 2/3/98 becker@cesdis.gsfc.nasa.gov.
# ifconfig eth1 192.168.1.1 netmask 255.255.255.0 \
broadcast 192.168.1.255
eth1: Setting Rx mode to 1 addresses.
```

使用命令行增加设备并不会在系统初始化脚本中增加表项。当 Linux重新引导时，卡的定义将会丢失。用于引导初始化时的卡定义位于 /etc/conf.modules和/etc/sysconfig/network-

China-pub.com
下载

scripts目录中。

当增加上述的网络设备时，到网络的路由自动增加到路由表中，使得主机可以访问直接连到适配器上的网络。访问其他网络（包括缺省路由器）则需要显式增加命令。

上述Shell命令中功能不十分清楚的是 modprobe 3c509.o命令。这个命令装载内核模块。该模块是3Com509网卡的驱动程序。有经验的系统管理员能够挑选出网卡，例如，在网卡中发现有Digital 21040网络芯片时，就会意识到调用 modprobe tulip.o可能可以初始化该块网卡。当然，这些知识是新手所不具备的。要了解网卡内核模块驱动程序的更多信息，可安装 Linux内核源代码，并查看 /usr/src/linux/Documentation/networking目录。有些网络驱动程序模块（尤其是ISA网络适配器的模块，如 NE2000）在正常装载和初始化以前，需要其他一些信息。让系统在安装时检测这些网卡比在安装之后再增加它们通常更为方便。

重复一下，基本的网络配置有三个参数： IP地址、网络屏蔽码和广播地址。网络地址由IP地址和网络屏蔽码自动产生。

其他的扩展配置选项，如网关地址和 DNS服务器在 /etc/sysconfig/network脚本和/etc/resolv.conf文件中说明。这些文件在系统安装时被配置，幸运的是，它们不需要修改。

本节最后要说明的是用于两台计算机通信的 10-BaseT以太网，它是连接小型网络的廉价方式。如果使用的是 10-BaseT的双绞线以太网，则需要一个 hub以连接两台或更多的计算机。两个10-BaseT设备在没有hub的情况下也可以互相通信，条件是使用特殊的线缆（可以从制造商处获得）。这种线缆在两端之间颠倒传输和接收线缆对。表 2-2是RJ-45的连线图（注意， 4、5、7和8针没有使用）。

表2-2 10-BaseT交叉线缆连线图

线 缆 对	本 地 主 机	远 程 主 机
TX	1	3
	2	6
RX	3	1
	6	2

这种交叉线缆明显减少了连接 10-BaseT设备的花费，在低代价安装中十分有用。交叉线也可用来连接多个10-BaseT的hub，连线需要在每个hub上占用一个端口。

2.2 子网

本节讨论对C类IP网络进行子网划分的技术。对 IP网络进行子网划分的方法可以将单个网络转化成多个网络。当需要维持多个网络，但没有多个A类、B类或C类网络时，经常使用这种技术。

除非有特别需要的理由，否则不要对 C类网络进行子网划分，因为这种用法弊大于利。第 4章讨论的IP伪装技术，是一种只用有限的 IP地址将多个主机连到 Internet的方法。要引起注意的是：子网划分要浪费掉两个IP地址，一个用于网络号，另一个用于广播地址，而且路由器可能还需要第三个地址。

表2-3 2的乘幂

$2^0=1$
$2^1=2$
$2^2=4$
$2^3=8$
$2^4=16$
$2^5=32$
$2^6=64$
$2^7=128$

现在假设某公司一个分支机构的系统管理员，他为自己的部门分配了一个 C类IP网络192.168.1。进一步假设这个机构有两个附属的分支办公室。管理员希望自己的 C类网络与另

China-pub.com 下载

外的办公室连网（没有其他的C类网络地址可用）。

我们回忆一下2的乘幂的值（如表2-3所示）。

C类网络的通用网络屏蔽码在分开前的形式显示在表 2-4中，分别有二进制和十进制两种形式。

表2-4 C类网络屏蔽码

255. 11111111.	255. 11111111.	255. 11111111.	0 00000000

网络管理员决定将C类网络的网络屏蔽码扩展两位，如图 2-5所示。

表2-5 用户定义的网络屏蔽码

255. 11111111.	255. 11111111.	255. 11111111	192 11000000

在修改后的网络屏蔽码中，最后字节的左两位被设置成了 1。两位的组合可以规划成 4种不同的情形（00、01、10或11），所以使用这种方法扩展网络屏蔽码，将建立 4个新的网络。我们只需要使用其中的3个，但是第4个只能留着，因为网络只能用 2的乘幂进行划分（除非使用变长子网屏蔽码，但这不是本书讨论的范围）。

采用这种方法扩展子网屏蔽码之后，可以建立 4个网络（如表2-6所示）。

表2-6 对C类网络进行子网划分的结果

网 络	网络屏蔽码	广播地址	起始IP地址	结束IP地址
192.168.1.0	255.255.255.192	192.168.1.63	192.168.1.1	192.168.1.62
192.168.1.64	255.255.255.192	192.168.1.127	192.168.1.65	192.168.1.126
192.168.128	255.255.255.192	192.168.1.191	192.168.1.129	192.168.1.190
192.168.192	255.255.255.192	192.168.1.255	192.168.1.193	192.168.1.254

因为每一个网络需要路由器对流量进行路径选择，所以路由器要消耗每一个网络上的一个IP地址。全部计算起来，消耗的新网络号、广播地址和新的网关地址总计为 12个，所以只有在十分必要时才使用这种技术。

2.3 DNS

域名系统（DNS）是将主机名转换成IP地址的引擎。它是Internet设计中的基石。没有哪个连到Internet上的域能够不用DNS。

一个Red Hat Linux系统除了使用代理以外，不管用何种其他方式连到 Internet，它都至少会安装一个只进行缓存的DNS服务器，以及一个指向127.0.0.1的/etc/resolv.conf文件。如果在ntsysv菜单的软件包列表中选择了 named，那么安装时就会装载这样的缓存服务器。对于 PPP的MODEM用户，短暂的使用者，或限制带宽的使用者尤其如此，因为激活一个缓存服务器将减少DNS通信量。

DNS服务器和只带缓存的设置可以在安装之后的任何时候装载，从安装树的 Red Hat/RPMS目录中发出下面的命令即可：

```
rpm -Uvh bind-8.2-6.i386.rpm
rpm -Uvh caching-nameserver-6.0-2.noarch.rpm
```

China-pub.com
下载

安装Bind软件包之后，系统会通过 /etc/rc.d/init.d/named启动脚本在引导时自动配置。如果不能如愿，可以使用ntsysv工具修改引导状态。

请注意，如果Red Hat Linux通过网络（FTP、NFS或SMB）安装，安装时指定了名字服务器，且在安装结束时保留了这些网络设置，则该服务器的优先级比本地主机上的任何名字服务器要高。要将本地主机指定为主名字服务器，需要确保 /etc/resolv.conf的第一条nameserver指令如下所示：

```
nameserver 127.0.0.1
```

IP地址127.0.0.1是一个特殊的地址，称为回送地址，它总是表示本地主机。

/etc/resolv.conf文件可以用来增加或去除本地的名字服务器。如果本地服务器发生故障，就会丢失通往Internet的连接性。所以，比较好的方法是列出三个名字服务器表项，在主服务器停止响应时，备份服务器开始启动。

设置/etc/resolv.conf文件时一定要小心。若某个用户对该文件没有读权限，则 DNS查询将会失败。

名字服务器一般用于两种方式：

- 被询问它所知道的主机信息（称为授权的）。
- 被询问的主机是非授权的，它需要再询问其他（授权的）名字服务器来获取信息，并进行缓存。

上面讲到的名字服务器的只带缓存设置建立了一个本身不知道任何信息的名字服务器。对每一个主机的信息，该服务器都需要询问其他名字服务器。虽然建立授权的名字服务器是系统管理员的职责，本书推荐自己安装只带缓存的名字服务器；只带缓存的名字服务器是授权的名字服务器的简化版本。

2.3.1 用于向前查看的文件

在创建 DNS记录以前，必须先从 InterNIC处获得一个域。可以首先访问 Web站点http://www.internic.net来达到该目的。要注意一个域在注册之时必须在所请求的域上有两个授权的名字服务器。

现在包含在Red Hat Linux中的通用的whois工具可以用来查询InterNIC数据库（该工具在以前版本中没有）。参见清单2-2。

清单2-2 使用whois

```
# whois redhat.com
[rs.internic.net]

Registrant:
Red Hat Software (REDHAT-DOM)
   4201 Research Commons, Suite 100
   79 T.W. Alexander Dr.
   P.O. Box 13588
   Research Triangle Park, NC 27709
   US

   Domain Name: REDHAT.COM

   Administrative Contact, Technical Contact, Zone Contact:
```

China-pub.com 下载

```
      Network Operations Center  (NOC144-ORG)
noc@REDHAT.COM
      919-572-6500 x235Fax- 919-361-2711
Fax- - 919-361-2711
   Billing Contact:
      Accounts Payable  (AP1279-ORG)  accounts@REDHAT.COM
      (919) 572-6500
Fax- (919) 361-2711

   Record last updated on 23-Jul-97.
   Record created on 26-May-94.
   Database last updated on 16-Dec-98 03:49:10 EST.

   Domain servers in listed order:

   NS.REDHAT.COM          207.175.42.153
   SPEEDY.REDHAT.COM      199.183.24.251

The InterNIC Registration Services database contains ONLY
non-military and non-US Government Domains and contacts.
Other associated whois servers:
   American Registry for Internet Numbers - whois.arin.net
   European IP Address Allocations        - whois.ripe.net
   Asia Pacific IP Address Allocations    - whois.apnic.net
   US Military                            - whois.nic.mil
   US Government                          - whois.nic.gov
```

假设我们得到了域名 acme.com，并且通过 InterNIC进行了注册。要配置主名字服务器，可将清单2-3中的文本存储在/var/named/db.acme文件中。

清单2-3 向前查看

```
@               IN SOA  acme.com.        root.acme.com. (
                        199901010       ; Serial
                        10800           ; Refresh
                        1800            ; Retry
                        3600000         ; Expire
                        86400 )         ; Minimum
                        IN      NS
dns1.other.com.
                        IN      NS
dns2.other2.com.
                        IN      MX      10      acme.com.

localhost               IN      A               127.0.0.1

acme.com.               IN      A               1.2.3.4
www                     IN      A               1.2.3.4

mail                    IN      CNAME           acme.com.
ftp                     IN      CNAME           acme.com.
```

该文件是小的域注册的最简单形式。www.acme.com和acme.com的IP地址都写成了1.2.3.4。域中的其他主机可以列出更多的“ IN A ”记录。

该文件本质上允许 Internet上的任何人连到名为 www.acme.com的主机，它会被解析成

China-pub.com
下载

1.2.3.4。要了解这个解析过程，可以使用UNIX的nslookup命令。

```
nslookup www.acme.com
Server:  localhost
Address:  127.0.0.1

Name:    www.acme.com
Address:  1.2.3.4
```

2.3.2 用于反向查看的文件

要配置进行反向查看的文件，必须得到一个Internet网络号。该网络号通常通过网络服务提供者得到，网络服务提供者从Internet号码分配权威机构（Internet Assigned Numbers Authority, IANA）处得到这些网络号，IANA的结点为http://www.iana.com。

假设用户获得了一个Internet C类网络，则应将清单2-4中的内容拷入文件/var/named/db.1.2.3。

清单2-4 反向查看

```
@               IN SOA  acme.com.    root.acme.com. (
                        199901010 ; Serial
                        10800     ; Refresh
                        1800      ; Retry
                        3600000   ; Expire
                        86400 )   ; Minimum
                        IN NS       dns1.other.com.
                        IN NS       dns2.other2.com.

4                       IN PTR acme.com.
```

术语反向查看（reverse lookup）指的是通过IP地址获取主机名：

```
nslookup 1.2.3.4
Server:  localhost
Address: 127.0.0.1

Name:    www.acme.com
Address: 1.2.3.4
```

如果某个域没有为IP地址定义反向查看（这在使用了该地址时并非一种好的尝试），该IP地址的注册用户可以通过whois得到，如清单2-5所示。

清单2-5 在ARIN服务器上使用whois

```
whois 199.183.24.253@whois.arin.net

[whois.arin.net]
NETCOM On-Line Communication Services, Inc. (NETBLK-
NETCOMCBLK-3)                  NETBLK-NETCOMCBLK-3
                               199.182.0.0 - 199.183.255.255
Red Hat Software (NET-REDHAT) REDHAT  199.183.24.0
```

要挑选出一条记录，使用"!xxx"进行查询，此处的xxx为句柄，在括号中紧跟在名称之后。

ARIN注册服务器只包含Internet相关的网络信息：网络、ASN及相关的POC。要获得相关域的信息，请使用rs.internic.net上的whois服务器；要获取NIPRNET信息，使用nic.mil的Whois服务器。

2.3.3 配置/etc/named.conf文件

一旦建立了主文件，必须以一种方式通知名字服务器使用这些主文件，这可以通过修改

China-pub.com 下载

/etc/named.conf达到目的。修改后的文件显示在清单 2-6中。

清单2-6 named配置文件

```
options {
        directory "/var/named";
};

// no longer a caching only nameserver config

zone "." {
        type hint;
        file "named.ca";
};

zone "0.0.127.in-addr.arpa" {
        type master;
        file "named.local";
};

zone "acme.com" {
        type master;
        file "db.acme";
};

zone "3.2.1.in-addr.arpa" {
        type master;
        file "db.1.2.3";
};
```

修改完named.conf文件后，使用下面的命令重启主名字服务器：

```
/etc/rc.d/init.d/named restart
```

可以配置二级服务器，让其复制服务器中的记录。这样，只需要在一个地方维护这些数据文件，减少了管理工作的负担。当主服务器的文件被修改时，需要增加其文件顶端的序列号，以便调用复制过程（复制过程进行序列号的比较）。通常使用当前日期作为序列号。

二级服务器必须在 named.conf文件中说明主服务器的 IP地址。假设主服务器的 IP地址为 5.6.7.8，则二级服务器上named.conf文件的正常格式显示在清单 2-7中。

清单2-7 二级服务器的named配置文件

```
options {
        directory "/var/named";
};

zone "." {
        type hint;
        file "named.ca";
};

zone "0.0.127.in-addr.arpa" {
        type master;
        file "named.local";
};
```

China-pub.com
下载


```
zone "acme.com" {
        type slave;
        file "db.acme";
        masters {
                5.6.7.8;
        };
};

zone "3.2.1.in-addr.arpa" {
        type slave;
        file "db.1.2.3";
        masters {
                5.6.7.8;
        };
};
```

当二级服务器重新启动时，它自动从主服务器处得到域信息，并建立 /var/named中的db.acme和db.1.2.3文件（它们与主服务器上的源文件并不相同）。

/var/named/named.ca文件（该文件在主服务器和二级服务器上都存在）有时必须重新装载。这样做的原因在于该文件本身。对于只带缓存的名字服务器也是如此。一般应该每六个月检查一下该文件是否被修改。如果计算机升级为新版本的 Red Hat Linux，则named.ca的升级将自动进行。

2.3.4 轮询DNS与簇

Red Hat Linux中的named发布版本支持一种简单方法的服务器负载平衡，几个主机可以分配同样的名字。这样， named将自动在整个IP地址表中循环，对要解析的名字，每次回答一个不同的IP地址。

很明显，这种装载方法将不会均匀分布在所有服务器上。如果一个防火墙的 DNS查询解析到一定的主机上，在一定时间内它可能把上千个客户导向那里，这样就可缓存查询的结果。

这种循环需要配置向前查看文件，可以将如下所示的记录输入 /var/named/db.acme：

```
www     IN      A       1.2.3.4
        IN      A       1.2.3.5
        IN      A       1.2.3.6
        IN      A       1.2.3.7
        IN      A       1.2.3.8
```

第一次询问www.acme.com将得到IP地址1.2.3.4，第二次则为1.2.3.5，第三次为1.2.3.6，等等。

2.4 IP别名和虚拟主机

IP别名（IP Alias）是一种单个以太网接口可以对多个 IP地址响应的机制。这种技术有许多应用背景：如Web站点的虚拟主机以及容错网络服务设计等。

我们假设eth0设备被配置了标准的C类网络地址192.168.1.1。该接口还可通过下面的命令序列（根用户方式运行）进行配置以对 192.168.1.2产生响应：

```
/sbin/ifconfig eth0:0 192.168.1.2
/sbin/route add-host 192.168.1.2 dev eth0:0
```

China-pub.com 下载

如果普通的网络服务（如 Telnet、FTP等）可以运行在第一个接口上，则它们也能运行到第二个接口上。有些服务对 IP别名设置特别敏感，它们对每一个设置了别名的接口将改变其行为（例如Apache）。可以使用下面的命令序列创建其他的接口：

```
/sbin/ifconfig eth0:1 192.168.1.3
/sbin/route add -host 192.168.1.3 dev eth0:1
```

一台计算机可以为另一台计算机提供备份网络服务，前者定期给后者发送 ping报文。如果远程主机不响应了，则前者自动以那台不可操作主机的网络地址执行一个 IP别名服务。这是容错的一种基本形式。

2.5 DHCP

动态主机配置协议（Dynamic Host Configuration Protocol，DHCP）是一种以集中方式为TCP/IP分配IP地址和其他相关参数的方法，它与通常的每台主机记录自己静态信息的方法不同。DHCP服务器应该是一台可操作的、持续连接到网络上的计算机 —— 当客户机需要其服务时，它必须可用。如果一个网络上有很多主机，且网络中有一台主机持续可操作，则可以使用一台DHCP服务器以减少网络管理的工作。协议的服务器部分通过 dhcpd驻留程序实现。该服务器协议与其他操作系统（例如 Microsoft的各种Windows）上的DHCP实现是兼容的，Linux客户机部分由dhcpcd或pump控制。如果在安装 Linux进行TCP/IP配置时选择了 DHCP，它将自动进行配置。安装Linux之后也可使用netcfg实现DHCP。

当Red Hat Linux系统准备好时，DHCP服务器不会自动安装。读者可以在本书所附光盘的RedHat/RPMs目录中以根用户方式运行下面的命令：

```
rpm -Uvh dhcp -2.0b1pl6-6.i386.rpm
touch /etc/dhcpd.leases
```

安装软件包后，系统会在引导时通过 /etc/rc.d/init.d/dhcpd启动脚本进行自动配置。如果用户不喜欢这种启动的方式，可以使用 ntsysv工具修改引导状态。

在Linux上配置DHCP服务器还有一个特殊的问题。必须进行一个路由命令以允许流量发送到255.255.255.255 IP地址上。这个问题在/usr/doc/dhcp-2.0b1pl6/README文件中进行了说明。其完整的命令如下：

```
/sbin/route add -host 255.255.255.255 dev eth0
```

系统每次重启动时都必须运行该命令，所以可以将其放置在某个引导脚本中。最好的位置是/etc/rc.d/init.d/dhcpd文件的启动部分。清单 2-8展示了一个运行系统上启动脚本的一段，它说明了实现DHCP的另一个重要问题及其相关要点。

清单2-8 dhcp启动脚本的修改版本

```
# See how we were called.
case "$1" in
  start)
        # Start daemons.
        echo -n "Starting dhcpd: "
        /sbin/route add -host 255.255.255.255 dev eth1
        daemon /usr/sbin/dhcpd eth1

        /sbin/ipchains -P forward DENY
        /sbin/ipchains -F
```

China-pub.com
下载


```
/sbin/ipchains -A forward -j MASQ \
 -s 192.168.1.0/24 -d 0.0.0.0/0
/sbin/modprobe ip_masq_ftp
echo
touch /var/lock/subsys/dhcpd
;;
```

注意，上述脚本中的route命令使用的不是eth0，而是ethl网络设备。还要注意， ethl作为一个参数传输给了dhcpd命令行。在有多个网络设备的系统中，必须告诉 dhcpd使用哪个设备。

对ipchains和modprobe的调用与DHCP并没有什么关系。它们将本地系统配置成一个伪路由器。拥有192.168.1网络号的网络将把所有待发的报文地址填写成本地 IP地址，并将其发送到缺省网关。这种技术在Internet地址很宝贵时十分有用，我们将在第4章中进行详细讨论。

如果使用的是高级的开发内核，则可能需要使用下面的命令（对于 Red Hat Linux 6.0发布的内核来说并不必要）：

```
echo 1> /proc/sys/net/ipv4/ip_bootp_agent
```

将Linux DHCP服务器联机的最后一步是书写 /etc/dhcpd.conf文件。清单2-9展示了一个示例。

清单2-9 一个示例dhcpd.conf文件

```
subnet 192.168.1.0 netmask 255.255.255.0 {
        range 192.168.1.128 192.168.1.254;
        default-lease-time 600; max-lease-time 7200;
        option subnet-mask 255.255.255.0;
        option broadcast-address 192.168.1.255;
        option routers 192.168.1.1;
        option domain-name-servers 192.168.1.1;
        option domain-name "fake.com";
}
```

该配置用于192.168.1网络。其每一条指令的作用在下面说明：

range 192.168.1.128 192.168.1.254；

该命令设置服务器可分发给客户机的IP地址范围。此处的地址是从128到254。

default-lease-time 600; max-lease-time 7200;

该指令控制客户机保持DHCP服务器分配给它的IP地址的时间，时间以秒为单位。

option subnet-mask 255.255.255.0;

此处说明发送给客户机的实际子网屏蔽码。

option broadcast-address 192.168.1.255;

此处说明发送给客户机的广播地址。

option routers 192.168.1.1;

发送给客户机的路由器的地址在此处说明。注意，这是 DHCP服务器的地址，该DHCP服务器同时又是一个路由器。

option domain-name-servers 192.168.1.1;

发送给客户机的 DNS服务器的地址在此处说明。注意，这是 DHCP服务器的地址，该DHCP服务器同时又是一个DNS服务器。所以， 192.168.1.1必须被配置成某个域的授权的DNS服务器，或者配置成只作缓存的名字服务器。

China-pub.com 下载

```
option domain-name "fake.com";
```

发送给客户机的域名地址在此处说明。

要启动DHCP服务器，可以重新引导系统，或者以根用户方式运行下面的命令：

```
/etc/rc.d/init.d/dhcpd start
```

DHCP还有许多其他的配置参数，如：各计算机可以基于其网卡的介质访问控制（ MAC）地址（MAC地址独一无二地标识厂家生产的以太网卡）从 DHCP服务器处获得特定的设置。

有关DHCP服务操作的其他信息，参见dhcpd、dhcpd.conf和dhcpcd的在线手册页。当需要查看dhcpd的行为时，请查看 /var/log/messages文件，因为DHCP的所有动作都记录在该文件中。

2.6 NFS/NIS

网络文件系统（Network File System, NFS）是由Sun Microsystems公司设计的一种协议，它允许将整个文件系统或单个目录与远程计算机进行方便地共享。如果读者购买了有关 Linux基本NFS操作的书籍，那么将这些书籍丢开吧！ NFS特别容易配置和使用。 NFS服务器是通过/etc/exports文件配置的。最简单的（也是最不安全的）配置是将与其他机器共享的目录列出来：

```
/home
/usr/local/bin
/var
```

Red Hat Linux的NFS服务器通过调用/etc/rc.d/init.d中的portmap和nfs脚本启动。这样，可以将其配置成在引导时运行，也可以通过下面的命令启动 NFS 服务器：

```
/etc/rc.d/init.d/portmap start
/etc/rc.d/init.d/nfs start
```

如果服务器处于活动状态，而又改变了 /etc/exports文件，则可以用下面的命令通知服务器重新读该文件：

```
exportfs -rv
```

服务器被初始化后，客户机就可以使用服务器所输出的目录（在 NFS中称为卷）了，方法是使用下面的mount命令：

```
mount nfs.remotehost.com:/path/to/exported/directory /mnt
```

可以使用IP地址代替主机名。还有一些能够影响性能的选项（如 rsize=8192, wsize=8192等）。更多的信息请查看mount手册页。

如果使用的是主机名，而不是IP地址，则系统必须要能够将远程 NFS服务器的名字转换成一个IP地址。因为DNS故障可能导致NFS出现问题，所以人们经常在 /etc/hosts文件中放置NFS服务器的一个表项，该服务器的文件系统在引导时被安装。了解 /etc/nsswitch.conf和/etc/fstab文件也很有好处，它们对于系统引导时的安装能带来其他的灵活性。

mount命令执行之后，本地主机就可以在本地目录树中看到远程文件系统，并且像本地文件一样处理这些文件。文件加锁可能产生问题；如果一个文件有多人使用，最好不要将它放到一个NFS卷中。

还要注意的是，安装 Internet上的NFS文件系统并不明智。 NFS通常使用 UDP报文，而UDP只适用于局域网络； Internet上的UDP报文很容易丢失，因此导致重传并影响性能。在

China-pub.com
下载

Internet上很适合使用FTP，而带压缩的scp则更为适宜（scp在第4章中讨论）。

请注意，通常限制根用户访问远程文件系统，这是一种称为 root压制（root squash）的机制。根用户通常可以以 nobody的方式在卷上工作。其他任何用户对管理员所做的工作都难以防备，所以不要将 NFS卷输出给不可信任的系统（或者至少将其输出成只读的形式，这些内容将在下面进行简要介绍）。

如前所述，/etc/exports可以让NFS更加安全。如下所示：

```
/home              remotehost.com
/usr/local/bin     anotherhost.com(ro)
/var               thelasthost.com(no_root_squash)
```

该文件仅允许remotehost.com通过NFS访问/home，且root压制有效。/usr/local/bin目录设置成只能从anotherhost.com以只读方式访问，而/var目录完全与thelasthost.com共享；根用户可以在最后一个远程主机上工作，对输出卷具有完全访问权。

NIS则是一个完全不同的系统。网络信息系统（ Network Information System, NIS）是一个在UNIX主机之间共享几个重要文件（一般为 /etc/passwd、/etc/group以及/etc/hosts等）的框架。不幸的是， NIS一直被人们认为比 NFS更加不安全。而且， NIS使用起来很麻烦，因为本地的/etc/passwd文件不再是本地帐户信息的可靠来源。

有几个NIS的替代软件，如NIS+、DCE registry以及Hesiod Bind等。它们也都难以配置和使用。

一种更加简单且更好的解决方案是在文件变更时，使用 scp从专门分配的主服务器拷贝文件到从服务器。改变这些文件的程序（如 chfn、chsh、passwd和chgrp）在从服务器上应该被关闭。