China-pub.com
下载

China-pub.com
下载

第3章 PPP

Linux下的调制解调器通信功能强大，但也很复杂。调制解调器可以作为标准的终端设备运行，或者作为由内核直接维护的网络连接运行。 Linux中达到网络通信目的的一种方法是点到点协议（Point to Point Protocol，PPP）。PPP可用来提供对TCP/IP（与Internet相关的协议）和IPX（Novell Netware使用的协议）的支持。

本章讨论的PPP与Microsoft Windows所使用的PPP是兼容的。Windows所使用的方法不太安全，但却被广泛地使用。

3.1 PPP客户

在Linux下建立PPP客户连接非常简单。在 XWindow下运行的Control Panel应用程序就可用来建立PPP连接。Shell脚本的方式将在下面讨论，它比 Control Panel方式更为灵活，因为它可以在非X环境中使用，且不需要根访问的权限。基于完整性的考虑，使用 Control Panel的方式将在稍后说明。不管建立 PPP的方法如何，必须配置 /etc/resolv.conf文件以允许系统对Internet主机名进行解析。Linux系统可以依赖于远程DNS服务器达到这个目的，也可以自己运行一个只带缓存的服务器。

3.1.1 脚本方式

为了连接远程PPP服务器，必须将三个文件/bin/network、/bin/network.chat和/etc/ppp/pap-secrets置于Linux系统中。这些文件的内容如下所示：

1. /bin/network文件：

```
#!/bin/sh

exec /usr/sbin/pppd -detach lock modem crtscts \
  defaultroute user USERNAME /dev/ttyS1 57600 \
  connect "/usr/sbin/chat -f /bin/network.chat"
```

2. /bin/network.chat文件：

```
'ABORT' 'BUSY'
'ABORT' 'ERROR'
'ABORT' 'NO CARRIER'
'ABORT' 'NO DIALTONE'
'ABORT' 'Invalid Login'
'ABORT' 'Login incorrect'
''
'ATZ'
'OK'
'ATDT 1234567'
'CONNECT'
''
```

3. /etc/ppp/pap-secrets文件：

China-pub.com
下载


```
# Secrets for authentication using PAP
# client server secret IP addresses
USERNAME    ""                  PASSWORD
```

对它们的配置说明如下：

1) modem所连的串口必须置于/bin/network文件中（例如，替换/dev/ttyS1）。

2) 在/bin/network.chat脚本中，用用户ISP的电话号码替换1234567。

3) 以拨号服务器上的PPP帐户名和口令替换/etc/ppp pap-secrets和/bin/network文件中的USENAME和PASSWORD。

4) 可选操作，在/bin/network.chat文件后放置一行ogin:--ogin: "。这样，本地系统与远程服务器之间的PPP会话开始时，远程服务器会发出“ login: ”消息。若没有收到该消息，则将返回一个消息以激活远程服务器的响应。

5) 运行chmod 755 /bin/network命令，以使得网络脚本可以在Shell中执行。

6) 可选操作，运行chmod u+s /usr/sbin/pppd命令，以将/dev目录中的串行端口设备的权限改为666模式（任何人都可进行读写操作）。这样，系统中的所有用户都可以启动或关闭 PPP。根用户也可以建立一个PPP组，以只允许信任用户管理该接口。

pppd中的demand选项在建立按需PPP连接时十分有用，仅在出现向外网络传输时，它才进行连接初始化，并且有这样的选择，在连接空闲一段时间后就终止连接，同时还可以在不活跃的连接上产生传输后重建连接。在 Red Hat Linux 6.0中，装载的内核包含了支持此选项的pppd（demand选项在5.0版本中可用，但没有任何功能）。下面是使用命令拨号方法时，对/bin/network文件的修正版本。

```
#!/bin/sh

exec /usr/sbin/pppd demand idle 300 192.168.1.2:192.168.1.1\
   -detach lock modem crtscts \
   defaultroute user USERNAME /dev/ttyS1 57600 \
   connect "/usr/sbin/chat -f /bin/network.chat"
```

上面的脚本使用了 demand选项，从而使得连接在一段不活跃的时间后断开。这段时间是由idle选项的参数定义的；该参数以秒为单位，上例中定义为 5min（300s）。

对demand参数而言，最大的限制是分配给设备的 IP地址在建立连接前必须已知。 pppd的手册页指出动态地分配 IP地址可以处理命令拨号安排，但是作者的测试运行并不能证实这个断言。如果由远程PPP服务器分配的IP地址不能一直被占有，那么应该仔细研究一下命令拨号进程diald，因为在这样的安排下它是很灵活的。

关于将Linux附加在ISP上的更多信息可以从ftp://sunsite.unc.edu/pub/Linux/docs/HOWTO/ISP-Hookup.HOWTO中获得。

3.1.2 使用控制面板

为了正确地使用图形化的 PPP控制，必须正确地运行 XWindow环境。在X环境中，打开一个终端窗口，然后键入 control-panel命令以启动控制面板。



图3-1 调制解调器配置图标

在控制面板启动PPP会话之前，应该建立一个对应于真实串行端口设备的符号连接/dev/modem。这可以在Shell下手工完成，也可以通过控制面板

China-pub.com 下载

来完成。点击Modem Configuration图标（如图3-1所示）。

在清单中选择串行端口设备（如图3-2所示），点击“ OK ”。

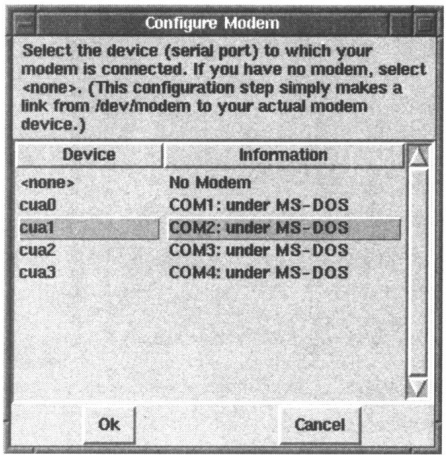


图3-2 调制解调器配置

在控制面板中，点击Network Configuration图标（如图3-3所示）：

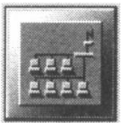


图3-3 网络配置图标

这时将出现网络配置对话框，点击Interfaces按钮，将出现如图3-4所示的窗口。

选择“ Add ”选项，就会显示如图3-5所示的可能的接口类型菜单。选择PPP，再点击“ OK ”。这时创建PPP接口的对话框将随之产生（如图3-6所示）。设置用户自己的ISP以取代相关的选择。

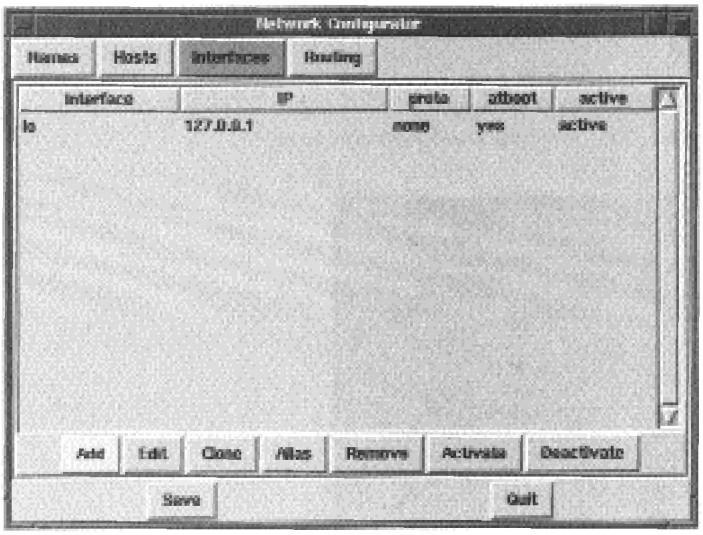


图3-4 网络配置

在所有设置正确后，点击“ Done ”按钮。这时将显示确认对话框（如图3-7所示）。

在设置被保存后， PPP设备被加入到Network Configuration对话框中（如图3-8所示）。点

China-pub.com
下载

击并高亮显示PPP设备，再点击“ Activate ”。

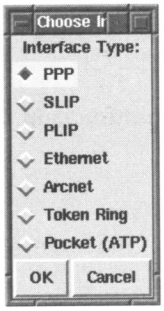


图3-5 接口类型

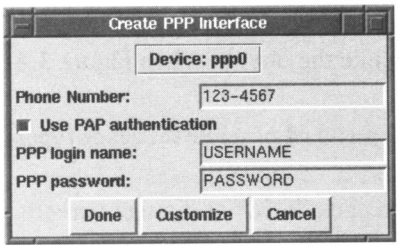


图3-6 PPP接口创建



图3-7 PPP接口确认

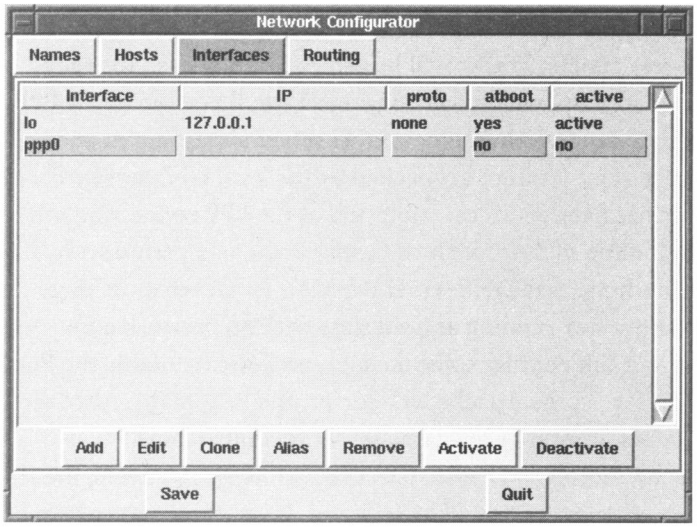


图3-8 PPP接口激活

如果所有设置都正确，那么调制解调器将挂断，并开始拨号。在 Linux-conf工具中也有一个相似的PPP客户控制界面，这里不再讨论。

3.1.3 名字解析

在Internet上，若没有IP地址则没有办法访问相应的主机。不管主机名的结构是什么（如host.foo.com），除非主机名可以被转换为IP地址（如1.2.3.4或其他真实的Internet地址），否则

China-pub.com 下载

主机是不可达的。这种转换并不是靠魔术，而是通过 Internet域名服务器来完成的。少量的名字到IP的转换可以输入到 /etc/hosts文件中，但是对大量主机来说，使用这个文件作为查找表是很不实际的。

对Linux系统的PPP连接而言，有两种选择可以完成 DNS名字解析：一是依赖于 PPP连接的远程DNS服务器，一是运行本地 DNS服务器。每一种方法各有优缺点。

若使用远程DNS服务器，则本地Linux主机的配置很简单；但是对每一台主机进行查找时产生的传输将消耗一部分 PPP连接的带宽。若配置了本地 DNS服务器并加以使用，那么主机名查找将在本地 DNS服务器的cache中存贮下来。这样在主机名第一次被查找后将不再消耗 PPP连接的带宽（除非 DNS服务器授权的远程 cache周期到期）。然而，在没有对 Internet进行网络访问的系统中，引导时运行的只带缓存的名字服务器可能使其他一些驻留程序（尤其是 Postgres SQL服务器、 Apache Web服务器和 Sendmail）发生错误。此外，名字服务器的初始化配置是很麻烦的。

将Linux系统配置成使用远程 DNS服务器的方式，需要知道服务器的 IP地址。通常，最多使用三个服务器。这些地址可以从远程的 ISP或系统管理员处获得。注意， Linux在PPP连接的协商阶段中不能使用 DNS服务（因为安全的原因，不支持 MSDNS）。

当获得远程服务器的地址后， /etc/resolv.conf应被配置成如下形式：

```
search isp.net
nameserver 1.2.3.4
nameserver 5.6.7.8
nameserver 9.10.11.12
```

用户应使用自己的ISP或上层授权机构的名字来取代上述代码中的 isp.net表项。可以忽略第二个和第三个名字服务器表项，但至少应输入一个可操作的服务器。注意，用户应使用正确的IP地址取代上面代码中虚拟的表项地址。

如果使用的是本地的只带缓存的服务器，服务器必须被载入和配置。 DNS服务器和 cache设置可以在安装后的任何时间装载，安装的方法是在安装树的 RedHat/RPMS目录中运行如下的命令：

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

通过/etc/rc.d/init.d/named启动脚本文件，可以在引导时自动配置安装地址来进行软件包的绑定，使之启动。如果与用户希望的不符，可以使用 ntsysv工具来改变引导时的状态。此外，使用该脚本还可以手工启动或终止名字服务。

装载了名字服务器之后，用户应指示 Linux使用名字服务。为了把本地主机指定为主名字服务器，需确保把/etc/resolv.conf文件中的第一个nameserver指令配置成如下形式：

```
nameserver 127.0.0.1
```

如果该文件不存在，则以 644的权限创建该文件。地址 127.0.0.1是全球通用的回送地址，使用上述的方式键入指令。

3.2 PPP服务器

Linux的pppd驻留程序有很灵活的配置选项，而且它可以与多种 IP协议栈通信。然而 pppd只有很少的选项用于控制调制解调器，它不向调制解调器发送初始化字符串，也不响应电话

China-pub.com
下载

响铃。

各种getty实现常用于负责对终端硬件的控制，包括建立调制解调器会话。 mingetty在Red Hat Linux中用于控制VGA控制台登录，但它没有用于管理串口的选项。一些常见的 getty实现有mgetty、agetty和uugetty。但是它们中的大多数都不能参与 PPP网络对话。

使用两个软部件：mgetty和pppd，可以解决这个问题。 mgetty将用于控制串行线并响应调制解调器。如果 mgetty检测到了 PPP会话的启动（这是 mgetty所独有的特征），mgetty将使用 exec ( )系统调用来派生pppd，然后pppd对用户（通过系统的口令数据库或自己的有效用户数据库）进行认证，并在授权后启动网络连接。

3.2.1 配置mgetty

在Red Hat Linux中，mgetty缺省时是不安装的。在缺省安装完成后，应进行明确地装载。这可以通过在Red Hat Linux安装树（本书所附光盘）中的 RedHat/RPMS目录下执行如下的命令执行达到目的：

rpm -Uvh mgetty-1.1.14-8.i386.rpm

上面的命令将安装mgetty二进制文件及相关的配置和文档文件。对大多数常用的 PPP服务器配置而言，应将/etc/mgetty+send-fax/mgetty文件的开始几行修改成如下的形式：

```
speed 115200
modem-type data
rings 1
```

如果用户还需在 mgetty中启动传真传输，则需要对文件使用不同的选项。如果是这样，应从http://www.leo.org/~doering/mgetty/mgetty_toc.html中寻找相关信息的更多文档（需要附加的RPM组件）。

用户应该修改/etc/mgetty+send-fax/login.config文件，使之包含如下的一行：

```
/AutoPPP/- a_ppp /usr/sbin/pppd 115200
```

文件中可能还有另一个被注释掉的 AutoPPP行，该行向 pppd传输更多的参数。因为在/etc/ppp/options中，配置这些选项开关更方便（这样可以保持 ps aux命令的输出列表的清晰），所以在此处将这些选项先注释掉。

mgetty运行时，它将把日志文件放入 /var/log目录中。用户可以考虑不时地手工清除这些文件，或使日志文件自动循环（自动删除老文件）。

3.2.2 /etc/ppp中的选项

在用户安装了mgetty后，运行如下的命令以配置/etc/ppp/pap-secrets文件以允许PAM登录：

```
echo '* * "" *' >> /etc/ppp./pap-secrets
```

此时，应该给每一个提供PPP服务的调制解调器线指定 IP地址。这些IP地址将被记录在文件/etc/ppp/options*中。

用户的/etc/ppp/options文件包含了运行在系统中的所有 pppd会话的控制参数，通常包括如下信息：

```
auth
login
modem
crtscts
```

China-pub.com 下载

```
lock
proxyarp
ms-dns x.x.x.x
ms-dns y.y.y.y
```

pppd手册页中详细介绍了上面所有的选项，下面只是一个概述：

auth：使远程PPP系统进行认证。

login：根据系统口令数据库（/etc/password、/etc/shadow或其他PAM配置使用的文件）进行认证，并将会话记录在wtmp文件中。

proxyarp：配置以太网卡，使之对远程PPP系统的ARP请求作出响应。

ms-dns x.x.x.x：将DNS服务器的IP地址传送到客户端。这只对 Windows客户机起作用，并且在选项文件中最多只能有两个这样的表项。该选项只有在 pppd使用了-DUSE_MS_DNS进行编译时才会工作，但使用该选项将使得客户端的配置非常容易。

每一个支持拔号PPP的串行设备都必须有自己独特的选项文件。如果用户准备在设备文件/dev/ttyS1（DOS COM1:）上附接一个调制解调器，那么文件 /etc/ppp/options.ttyS1将包含定义该调制解调器的参数。例如，位于 IP地址1.2.3.1的PPP服务器将把IP地址1.2.3.4分配给PPP拔号。这种配置需要将文件/etc/ppp/options.ttyS1配置为包含下面的一行：

```
1.2.3.1: 1.2.3.4
```

上面的第一个参数是拔号服务器的 IP地址，第二个参数是分配给串行线的 IP地址。每一个串行线应该有不同的IP地址。

用户应该注意1.2.3.4不是真正的C类Internet地址（是个A类地址）。在这里把它用作C类地址，只是为了使上下文更清晰。特别要强调的是，网络 1.2.3及其产生的主机地址在Internet上都不应使用。

上面列出的proxyarp选项值得用户特别注意。如果不使用 proxyarp，那么串行设备可以向服务器传送数据，但是不能与其他机器进行通信（ proxyarp选项把以太网设备配置为响应 PPP IP地址的ARP响应）。用于本地访问的特定拔号线可能需要将 proxyarp参数从/etc/ppp/options文件中移去，而将其写入接收整个网络访问的线缆所对应的指定设备选项文件中。

除了proxyarp，还要求允许PPP设备和LAN设备交换数据，即必须启动通过网络接口的数据包转发。为了完成这一步，应该对 /etc/sysconfig/network文件进行修改。如果禁止转发（这是缺省的方式），那么文件中会有如下的一行：

```
FORWARD_IPV4=false
```

将这一行改成如下形式，就能启动数据包转发：

```
FORWARD_IPV4=true
```

/etc/sysconfig/network文件中的指令只在系统引导时才被执行。为了不重启系统而启用数据包转发，键入如下命令：

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

如果没有可用的IP地址分配给串行设备，那么可以考虑使用在 192.168.x.x范围内的地址，然后使用免费的TISFireWall ToolKit等代理软件进行地址转换（第4章进行介绍）。通常，在这种情况下不能使用proxyarp。关于IP伪装（在本书防火墙部分讨论）的信息或许对读者很有帮助。

3.2.3 将mgetty加入到/etc/inittab中

每一个串行线可以通过/etc/inittab文件中的一个入口项控制。 ttyS1的入口项可能是如下的

China-pub.com
下载

形式：

```
S1:345:respawn:/sbin/mgetty ttyS1
```

对于参加mgetty/pppd分配系统中的每一个串行设备，还应在文件中加入相应的描述该设备的行。

完成对/etc/inittab文件的修改后，Linux系统必须被重启或者以根用户方式使用 Shell命令init q。所有外部调制解调器上的灯将开始闪烁。

通过键入命令killall mgetty（在非Red Hat系统中使用该命令时应小心），可以在任何时候重新初始化非活跃的调制解调器。

3.2.4 附加日志信息

大多数系统服务向syslog驻留程序发送活跃消息，而 syslog驻留程序将这些信息中的大多数记录在/var/log/messages文件中。邮件系统的日志数据放在 /var/log/maillog文件中。其他日志文件的位置可以通过查看 /etc/syslog.conf文件获得。

将日志信息拷贝到不活跃的虚拟控制台上，以使之可以被实时检测，这相对而言比较简单。要这样做，只需键入如下的命令：

```
echo '*.* /dev/tty9' >> /etc/syslog.conf
```

然后，重启系统或向syslog驻留程序发一个HUP信号（如kill -HUP <pid>）。

如果同时按下CTRL-ALT-F9键，数字号为9的虚拟控制台将变成可见。它应该包括 syslog驻留程序的完整输出。所有 PPP的活动都应该被立即记录到这个屏幕上，同时还要记录其他系统主要服务（如DHCP、DNS、邮件传输工具等）的活动。

为了返回数字号为1的用户登录所使用的虚拟控制台，只需按下 CTRL-ALT-F1键。而返回XWindow系统对话（如果已经运行了），只需按下CTRL-ALT-F7键。