13.4 在 Linux 上嗅探无线网络

在 Linux 系统嗅探只需要简单地启用无线网卡的监听模式，然后启动 Wireshark 即可。然而，不同型号的无线网卡启用监听模式的流程各不相同，所以在这里我不能给出明确提示。实际上，有些无线网卡并不要求你启用监听模式。你最好 Google 一下你的网卡型号，确定是否需要启用它，以及如何启用。

在 Linux 系统中，通过内置的无线扩展程序启用监听模式是常用的办法之一。你可以用 iwconfig 命令打开无线扩展程序。如果你在控制台上键入 iwconfig，应该会看到这样的结果：

```
    $ iwconfig
eth0  no wireless extensions
lo0   no wireless extensions
eth1  IEEE 802.11g     ESSID:"Tesla Wireless Network"
      Mode:Managed  Frequency:2.462 GHz  Access Point:00:02:2D:8B:7
      Bit Rate:54 Mb/s  Tx-Power-20 dBm  Sensitivity=8/0
      Retry Limit:7  RTS thr: off  Fragment thr: off
      Power Management: off
      Link Quality=75/100  Signal level=-71 dBm  Noise level=-86 dB
      Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
      Tx excessive retries:0  Invalid misc:0  Missed beacon:2
```

iwconfig 命令的输出显示 eth1 接口可以进行无线配置。这是显然的，因为它显示了与 802.11g 协议有关的数据，反观 eth0 和 lo0，它们只返回了「no wireless extensions」。

这个命令提供了许多无线配置信息，仔细看一下，有无线扩展服务设置 ID（Extended Service Set ID，ESSID）、频率等。我们注意到「eth1」下面一行显示，模式已经被设置为「被管理」，这也就是我们想改动的地方。

要将 eth1 改成监听模式，你必须以 root 用户身份登录。可以直接登录或用切换用户（su）命令，如下所示：

```
    $ su
Password:
```

在你成为 root 用户后，就可以键入命令来配置无线网卡选项了。输入以下命令可以将 eth1 配置成监听模式：

```
    # iwconfig eth1 mode monitor
```

网卡进入监听模式后，再次运行 iwconfig 命令应该能反映出变化。输入以下命令，以确保 eth1 接口可以工作：

```
# iwconfig eth1 up
```

我们也将使用 iwconfig 命令改变监听信道，输入以下命令，改变 eth1 接口的信道为信道 3：

```
# iwconfig eth1 channel 3
```

> 注意
>
> 你可以在捕获数据包的过程中随意修改信道，所以随便改吧，没问题！也可以将 iwconfig 命令脚本化以简化过程。

完成这些配置后，请启动 Wireshark 开始你的数据包捕获之旅！