Capturing Wireless LAN Packets on Ubuntu with tcpdump and Kismet

By Steven Gordon on Wed, 29/12/2010 - 10:15am

Capturing packets on a wireless LAN interface can be fun because you can see what other nearby laptops and access points are sending. By inspecting individual wireless LAN frames, you can see the detailed operation of the wireless LAN medium access control. I first tried capturing wireless LAN packets in 2002. Then, as it is now, the major difficulty was having drivers for your wireless card that support capturing (i.e. *monitor* or *promiscuous* mode). Then I used Cisco Aironet 350 PCMCIA cards, RedHat Linux and Ethereal (now called Wireshark [3]). Nowadays many more cards are supported, but most features of capturing are usually only possible under Unix-like operating systems (its hard/impossible in Windows).

Here are some instructions for using my Samsung NC10 Ubuntu laptop to capture wireless LAN packets. First using the basic commands of `iwconfig` and `tcpdump`, and then the dedicated software Kismet [4]. Of course capturing other peoples traffic may be illegal/unethical in some situations; don't do it if you are not sure. *Update (22 Mar 2012):* Also I have a screencast below showing the steps on a Lenovo [5] laptop. Either read on or watch the 16 minute video.

1. Capture Wireless LAN Packets with tcpdump

First make sure NetworkManager is not automatically connecting or turning interfaces on/off. Right-click on the network icon in Gnome and de-select *Enable Networking* (i.e. so networking is disabled).

Turn the wireless LAN interface off (on my computer the OS labels the interface `wlan0`):

```
$ sudo ifconfig wlan0 down
```

Now use `iwconfig` to put the interface into monitor mode, check the interface status and then turn the interface on again:

```
$ sudo iwconfig wlan0 mode monitor
$ iwconfig wlan0
wlan0     IEEE 802.11bg  Mode:Monitor  Frequency:2.462 GHz  Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
          Power Management:off

$ sudo ifconfig wlan0 up
```

Update (29 Aug 2013): To set the channel to monitor you should select it *before* you enter monitor mode. That is, while the interface is in managed mode (e.g. connected to an AP), set the channel, e.g.:

```
$ sudo iwconfig wlan0 chan 6
```

Packet capture software can now be used, and the wireless LAN card will capture all packets it can receive, even if they are not direct to your laptop. Here I use tcpdump [6]:

```
$ sudo tcpdump -i wlan0 -n
```

`tcpdump` will print out a single line on standard output for each packet received. *Update (22 Mar 2012):* the `-n` option prevents DNS lookups (e.g to convert an IP to DNS) - without this option it is possible that `tcpdump` will not capture all packets as it will be too slow performing the DNS lookups. To stop the capture press *Ctrl-C*. Note that by default in Ubuntu 12.04 and later `tcpdump` captures 65535 Bytes - effectively the entire packet. If you want to capture only a selection of the packet (e.g. first 64 Bytes to save storage space when capturing over a long period of time) and save to a file try:

```
$ sudo tcpdump -i wlan0 -n -s 64 -w file.cap
```

The file `file.cap` can now be opened in Wireshark [3] for easier viewing.

In monitor mode your wireless interface only receives packets--it cannot transmit (i.e. you have no normal network access via wireless).
to return your wireless card to normal (managed) mode run:

```
$ sudo ifconfig wlan0 down
$ sudo iwconfig wlan0 mode managed
$ sudo ifconfig wlan0 up
$ iwconfig wlan0
wlan0     IEEE 802.11bg  ESSID:"MyWirelessNet"
          Mode:Managed  Frequency:2.462 GHz  Access Point: 00:23:69:12:34:56
          Bit Rate=1 Mb/s   Tx-Power=20 dBm
          Retry  long limit:7   RTS thr:off   Fragment thr:off
```

```
Power Management:off
Link Quality=68/70  Signal level=-42 dBm
Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

The wireless card is now associated with an access point again.

2. Monitor Wireless LAN with Kismet

Another way to monitor wireless LAN activities is to use a dedicated application like Kismet [4] (on Windows similar software includes Netstumbler [7] and Inssider [8]). Kismet puts your wireless card into monitor mode and then provides a basic view of the different APs nearby (as identified by the captured packets).

To install and configure on Ubuntu:

```
$ sudo apt-get install kismet
$ cd /etc/kismet
$ sudo nano kismet.conf
```

You must edit the `kismet.conf` file to configure. Two things must be set (others are optional). First the SUID user should be set to your username:

```
suiduser=sgordon
```

And the source needs to be set to identify your wireless LAN interface (`wlan0` on my computer, as well as the driver and card (`ath5k` is the driver for my atheros based wireless card on my Samsung laptop. Steps for setting up Kismet on a Lenovo Ideapad V470 are described here [9].):

```
#source=none,none,addme
source=ath5k,wlan0,atheros
```

After saving `kismet.conf`, start Kismet:

```
$ sudo kismet
```

If all is well, after a few seconds the Kismet interface will start showing you a list of APs. Press *h* for help and start exploring. To quit press *Q*. Make sure when Kismet exists it puts your wireless LAN interface back into managed mode. Check with `iwconfig`, and if not, do so your self with the above commands.

Interest: PCs and Laptops [10]
Internet Software [11]
Ubuntu Linux [12]
ifconfig [13]
iwconfig [14]
kismet [15]
tcpdump [16]

Topic: Wireless LANs [17]
Content: Bangkok Blog [18]
Howto [19]

Source URL: http://sandilands.info/sgordon/capturing-wireless-lan-with-ubuntu-tcpdump-kismet

Links:
[1] http://sandilands.info/sgordon/capturing-wireless-lan-with-ubuntu-tcpdump-kismet
[2] http://sandilands.info/sgordon/user/2
[3] http://www.wireshark.org/
[4] http://www.kismetwireless.net/
[5] http://sandilands.info/sgordon/wireless-lan-lenovo-ideapad-v470-ubuntu-not-working
[6] http://www.tcpdump.org/
[7] http://www.stumbler.net/
[8] http://www.metageek.net/products/inssider
[9] http://sandilands.info/sgordon/kismet-on-lenovo-ideapad-v470-ubuntu
[10] http://sandilands.info/sgordon/taxonomy/term/166
[11] http://sandilands.info/sgordon/taxonomy/term/162
[12] http://sandilands.info/sgordon/taxonomy/term/302
[13] http://sandilands.info/sgordon/taxonomy/term/305
[14] http://sandilands.info/sgordon/taxonomy/term/307
[15] http://sandilands.info/sgordon/taxonomy/term/308
[16] http://sandilands.info/sgordon/taxonomy/term/309
[17] http://sandilands.info/sgordon/taxonomy/term/1
[18] http://sandilands.info/sgordon/taxonomy/term/236
[19] http://sandilands.info/sgordon/taxonomy/term/212