Using wireless monitor mode in Linux/FreeBSD with Cisco cards

Cisco PCM340/350

The difference between those two cards is the transmit power level. On the PCM340 power is limited to 30mW, whereas the PCM350 can output 100mW. For monitoring applications obviously that doesn't matter a great deal.

When used as a normal wireless client, the firmware will automatically find the best access point based on signal quality and associate with it. This feature extends to monitor mode as well, so it's best to select the SSID name first and then let the card figure out the correct channel. Manually setting the channel doesn't seem to be honored.

Firmware version 4.25.30 seems to work.

Monitor mode in Linux

The driver named *airo* may be used for Cisco cards. For some reason, this driver creates two devices when active, one of them is named ethX as normal and the second one named wifiX. The wifiX device must be used when monitor mode is enabled whereas the ethX device is used when the card is used as a normal wireless client. As far as I can tell there is no benefit to having a separate interface, since the card firmware will not allow frames to be transmitted while in monitor mode.

To enable monitor mode with these cards and start capturing:

```
shell# iwconfig eth0 mode monitor
shell# iwconfig eth0 essid <SSID>
shell# ifconfig wifi0 up
shell# ifconfig eth0 up
shell# tcpdump -n -i wifi0 -s1500 -w <savefile>
```

In the case that your *wireless-tools* support isn't capable of understanding the above "mode monitor" command, you can enable monitor mode by using the following:

```
shell# echo "Mode: y" > /proc/driver/aironet/eth0/Config
```

The link type should then change to IEEE802_11.

Monitor mode in FreeBSD 5.3

The driver named *an* may be used for Cisco cards. If you're running a custom kernel, make sure to include "device an" in your kernel configuration file.

To enable monitor mode with these cards and start capturing:

```
shell# ancontrol -M 1
shell# ifconfig an0 up ssid <SSID>
shell# tcpdump -n -i an0 -s1500 -w <savefile>
```

$Id: monitor-cisco.html,v 1.2 2005/07/28 09:47:55 kos Exp $