Sniffer basics

1. Start with the same setup as you finished with in the prior lab. In this lab, you will be coordinating with a partner group. One group will be generating traffic, while the other group will try to sniff it. A laptop group has to pair with a PC group. The laptop group will do the sniffing, while the PC group will generate traffic.
2. Ensure that the PC's AP is operating on the designated working channel, and that the PC is associated with that AP.
3. Ensure that the ethernet interface of the PC is down using `ifconfig`. Ensure that the wireless link is working, by downloading http://www.iitk.ac.in/
4. Now put the laptop in monitor mode: `iwconfig wlan0 mode monitor`
5. Ensure that the laptop is in the same channel as the PC's designated channel: `iwconfig wlan0 channel <PC's-channel>`
6. Now make the laptop sniff: `tcpdump -n -i wlan0 host <PC's-IP-addr>`
7. While tcpdump is running on the laptop, use the PC to download the web-page: http://www.cse.iitk.ac.in/~bhaskar/temp/netread-papers.txt
8. Observe the packets being captured on the laptop.
9. Can you identify the DNS lookup?
10. Can you identify the TCP 3-way handshake?
11. What are the sizes of the various packets?
12. What are the sequence numbers in the various TCP packets?
13. Now, in the PC, load the web-page http://www.cse.iitk.ac.in/~bhaskar/temp/httpTest.txt
14. Do you see the DNS lookup on the laptop? Why or why not?

Sniffing continuous ping

1. Have the PC ping its AP, and have the laptop sniff this by using: `tcpdump -n -i wlan0`
2. Observe the stream of ping request and reply packets.
3. Now run `tcpdump -e -n -i wlan0`. This will make tcpdump also gather the ethernet headers. You are likely to see a whole set of packets (other groups' packets also).
4. Now redirect the tcpdump output to a file: `tcpdump -e -n -i wlan0 > out.txt`
5. Get the MAC address of the PC's wireless card by typing `ifconfig eth1`.
6. Open the file `out.txt` in an editor (say `vim out.txt`). Are you able to locate the ping request packets sent by the PC? Are you able to see the MAC acknowledgement packets?

Setting up a 802.11 key

1. Now we are going to temporarily enable the ethernet interface of the PC. Type `ifconfig eth0 up`.
2. Setup a security key at the PC's AP. Click on “Radio data encryption (WEP)” in the SSID/channel configuration page. Change the data encryption usage to “Full encryption”. And set the first WEP key to 40-bit,

and use the encryption key given in your configuration sheet.

3. Setup the same key at the PC: `iwconfig eth1 key <your-key>`.
4. Now type `iwconfig` to ensure that the your PC client is associated with your PC's AP. You should see that the encryption is turned on from the output of the `iwconfig` command.
5. Now repeat the sniffing of the ping packets at the laptop using `tcpdump -n -i wlan0`
6. Are you able to sniff any packets at the laptop now? Why or why not?
7. Now use `tcpdump -e -n -i wlan0 > out2.txt`. Look for the MAC address of the PC's wireless interface. Observe the difference from what you had seen in `out.txt`.