We'll use a set of stations running FreeBSD for our experiments. There is no user other than root on these systems, and there is no password. You can also your own laptops if you wish! (The configurations tools are slightly different then, you'd use ifconfig, iwconfig, wlanconfig...). You can use your own laptop to generate traffic or capture if you wish.

Please contact vorav@colorado.edu to setup an appointment to do the experiment.

1 Useful commands

- ifconfig athX: observe or configure interface athX

  Please read the manpages for ifconfig and our interface ath (man ifconfig, man ath)

  Exemples:

  - ifconfig ath0 10.0.0.1/8 to set the IP address, with a 255.0.0.0 netmask.
  - ifconfig ath0 media DS/2Mbps makes the interface use a PHY rate of 2Mb/s
  - ifconfig ath0 media auto makes the interface set automatically the PHY rate
  - ifconfig ath0 mediaopt hostap turns the station into an access point
- `ifconfig ath0 -mediaopt hostap` turns it back into managed (client) mode
- `ifconfig ath0 mode 11b` makes it only use 802.11b
- `ifconfig ath0 channel 6` makes it operate over channel 6. (Otherwise it is possible to set this by specifying the frequency)
- `ifconfig [-]monitor` to put the interface in (or out of) monitor mode.

Also, you can look at section 31.3 of the FreeBSD Handbook (available online)!

• Type `xinit` to launch an X server. The window manager is really basic. You can refer to `/usr/local/share/doc/wm2/README` for a quick introduction to it.

• `ssh` or `sftp` to upload data over the net, maybe after associating with UCB Wireless

• Thumb drives: the incantation to access to a thumb drive is `mount -t msdosfs /dev/da0[s1] /mnt` (then your files appear in `/mnt`) to unmount it after use: `umount /mnt`

• Wireshark to capture traffic. You can make several capture, save them in `libpcap` format and re-open them later on your own computer.

## 2 Traffic generators

In the directory `/root/ipmt`, you have four tools to generate and receive traffic: `tcpmt`, `tcptarget` for TCP and `udpmt`, `udptarget` for UDP. Try the `-h` option to see what options are available.

`udptarget -p 5000` launches a UDP traffic receiver on port 5000. It will print second by second the goodput of the traffic that it gets.

`tcpmt -p 5000 10.1.1.1` sends TCP packets as fast as possible to 10.1.1.1 on port 5000.

## 3 Procedure

1. Use one laptop as AP, one as a client, the last one will be for capturing traffic.
   
   *Do the necessary configurations.*
2. Capture the beacons from your AP. What information do you see?

3. Capture a few ping frames between your client and your AP. What information is there in the L2 ACKs? How does the sender know it is its own frame that was acknowledged? (The monitor sometimes misses frames, don’t panic! Give a portion of capture where this happened for sure—say why!)

4. Use various modulations on the sender side (e.g. `ifconfig athX media DS/2Mbps`), and see what UDP goodput you get. Plot the throughput against the nominal bit rate. Any comment?

5. Generate concurrent flows sharing the channel, so that packets from the two flows will collide. Extract a portion of the capture where a collision happened.