

## TCPDUMP VS SNOOP Cheat Sheet

### Similarities:

Command Line Option		Command Line Option Explanation
Tcpdump	Snoop	
-i	-d	listen on device
-p	-P	Disable promiscuous mode
-d	-C	Print compiled packet matching code from filter
-c	-c	Count packets before exit
-r	-i	Read the packets from file
-w	-o	Write the raw packets to file
-s	-s	Set capture snap length
-tttt	-t a	Print absolute timestamp
-n	-r	Disable address resolution
-XX	-x 0	When parsing and printing, in addition to printing the headers of each packet, print the data of each packet, including its link level header, in hex and ASCII.

### Differences:

1. You can use tcpdump -D to list the network interfaces available on the system and use -L to identify its data link type. While on SunOS, you can either use ifconfig -a or netstat -i to print the network interfaces information.
2. The frame(link layer header+packet) size can be printed by snoop with the option -S.
3. The -q option is quiet mode for both tcpdump and snoop but serve different functions -
  - tcpdump - print less protocol information
  - snoop - do not display packet count when capturing packets
4. Two important options for snoop are -p which is used to locate packet by number and specify the range with -p first,last. The -x offset,length option is used to locate the byte offset by length . For example -x 15 will jump to IP header directly and print the rest of the packet in hexadecimal & ascii format.
5. The tcpdump -U option is great to use together with -w when writing the packet to the file directly instead of waiting the output buffer is full.
6. It is important to run network sniffer with privilege dropping, tcpdump has this support with -Z option so you don't really need to run it as root.
7. Using tcpdump, certain protocols can be interpreted by the use of -T option. For example tftp, cisco netflow and so forth.
8. tcpdump allows you to save the filter expression in the file and parse it with -F option, this is great for recycle purpose.

Both tcpdump and snoop support filter expression and it's best to parse them after all the command options been defined in command line. For the practical usage of tcpdump vs snoop, check out the link below.

- <http://geek00l.blogspot.com/2007/11/sunos-snoopy-dog.html>