Tcpdump Best Practices

List of interfaces on which tcpdump can listen:

[crayon-6622ec77a6214992329551/]
Listen on interface eth0:
[crayon-6622ec77a621c867932641/]
Listen on any available interface :
[crayon-6622ec77a621e800882289/]
Be verbose while capturing packets:
[crayon-6622ec77a6220917247841/]
More verbose while capturing packets:
[crayon-6622ec77a6222726053048/]
Very verbose while capturing packets:
[crayon-6622ec77a6224977930635/]
Verbose and print the data of each packet in both hex and ASCII, excluding the link level header:
[crayon-6622ec77a6226811997266/]
Verbose and print the data of each packet in both hex and ASCII, also including the link level header:
[crayon-6622ec77a6228522069720/]
Less verbose (than the default) while capturing packets:
[crayon-6622ec77a622a070378593/]
Limit the capture to 100 packets:
[crayon-6622ec77a622c289513665/]
Record the packet capture to a file called capture.cap:
[crayon-6622ec77a622e628037331/]
Record the packet capture to a file called capture.cap but display on-screen how many packets have been captured in real-time:
[crayon-6622ec77a6230301639105/]
Display the packets of a file called capture.cap:
[crayon-6622ec77a6232823264607/]
Display the packets using maximum detail of a file called capture.cap:
[crayon-6622ec77a6234407843168/]
Display IP addresses and port numbers instead of domain and service names when capturing packets

[crayon-6622ec77a6236964519283/]
Capture any packets where the destination host is 192.168.5.1. Display IP addresses and port numbers:
[crayon-6622ec77a6238173007355/]
Capture any packets where the source host is 192.168.5.1. Display IP addresses and port numbers:
[crayon-6622ec77a623a147465997/]
Capture any packets where the source or destination host is 192.168.5.1. Display IP addresses and port numbers:
[crayon-6622ec77a623c732118676/]
Capture any packets where the destination network is 192.168.5.0/24. Display IP addresses and port numbers:
[crayon-6622ec77a623e569740828/]
Capture any packets where the source network is 192.168.1.0/24. Display IP addresses and port numbers:
[crayon-6622ec77a623f859233508/]
Capture any packets where the source or destination network is 192.168.5.0/24. Display IP addresses and port numbers:
[crayon-6622ec77a6243220791309/]
Capture any packets where the destination port is 23. Display IP addresses and port numbers:
[crayon-6622ec77a6245741792176/]
Capture any packets where the destination port is is between 1 and 1023 inclusive. Display IP addresses and port numbers:
[crayon-6622ec77a6247346478624/]
Capture only TCP packets where the destination port is is between 1 and 1023 inclusive. Display IP addresses and port numbers:
[crayon-6622ec77a6249274530051/]
Capture only UDP packets where the destination port is is between 1 and 1023 inclusive. Display IP addresses and port numbers:
[crayon-6622ec77a624b032255908/]
Capture any packets with destination IP 192.168.1.1 and destination port 23. Display IP addresses and port numbers:
[crayon-6622ec77a624d810062563/]
Capture any packets with destination IP 192.168.5.1 and destination port 80 or 443. Display IP addresses and port numbers:
[crayon-6622ec77a624f207313113/]
Capture any ICMP packets:

[crayon-6622ec77a6251846017767/]
Capture any ARP packets:
[crayon-6622ec77a6253042767149/]
Capture either ICMP or ARP packets:
[crayon-6622ec77a6255667355284/]
Capture any packets that are broadcast or multicast:
[crayon-6622ec77a6256285289634/]
Capture 500 bytes of data for each packet rather than the default of 68 bytes:
[crayon-6622ec77a6258230567361/]
Capture all bytes of data within the packet:
[crayon-6622ec77a625a549047212/]