

# tcpdump Cheat Sheet

## Packet Capturing Options

Switch	Syntax	Description
<b>-i any</b>	tcpdump -i any	Capture from all interfaces
<b>-i eth0</b>	tcpdump -i eth0	Capture from specific interface ( Ex Eth0)
<b>-c</b>	tcpdump -i eth0 -c 10	Capture first 10 packets and exit
<b>-D</b>	tcpdump -D	Show available interfaces
<b>-A</b>	tcpdump -i eth0 -A	Print in ASCII
<b>-w</b>	tcpdump -i eth0 -w tcpdump.txt	To save capture to a file
<b>-r</b>	tcpdump -r tcpdump.txt	Read and analyze saved capture file
<b>-n</b>	tcpdump -n -I eth0	Do not resolve host names
<b>-nn</b>	tcpdump -n -i eth0	Stop Domain name translation and lookups (Host names or port names )
<b>tcp</b>	tcpdump -i eth0 -c 10 -w tcpdump.pcap tcp	Capture TCP packets only
<b>port</b>	tcpdump -i eth0 port 80	Capture traffic from a defined port only
<b>host</b>	tcpdump host 192.168.1.100	Capture packets from specific host
<b>net</b>	tcpdump net 10.1.1.0/16	Capture files from network subnet
<b>src</b>	tcpdump src 10.1.1.100	Capture from a specific source address
<b>dst</b>	tcpdump dst 10.1.1.100	Capture from a specific destination address
<b>&lt;service&gt;</b>	tcpdump http	Filter traffic based on a port number for a service
<b>&lt;port&gt;</b>	tcpdump port 80	Filter traffic based on a service
<b>port range</b>	tcpdump portrange 21-125	Filter based on port range
<b>-S</b>	tcpdump -S http	Display entire packet
<b>ipv6</b>	tcpdump -IPV6	Show only IPV6 packets
<b>-d</b>	tcpdump -d tcpdump.pcap	display human readable form in standard output
<b>-F</b>	tcpdump -F tcpdump.pcap	Use the given file as input for filter
<b>-I</b>	tcpdump -I eth0	set interface as monitor mode
<b>-L</b>	tcpdump -L	Display data link types for the interface
<b>-N</b>	tcpdump -N tcpdump.pcap	not printing domain names
<b>-K</b>	tcpdump -K tcpdump.pcap	Do not verify checksum
<b>-p</b>	tcpdump -p -i eth0	Not capturing in promiscuous mode

## Logical Operators

Operator	Syntax	Example	Description
<b>AND</b>	<b>and, &amp;&amp;</b>	tcpdump -n src 192.168.1.1 and dst port 21	Combine filtering options
<b>OR</b>	<b>or,   </b>	tcpdump dst 10.1.1.1    !icmp	Either of the condition can match
<b>EXCEPT</b>	<b>not, !</b>	tcpdump dst 10.1.1.1 and not icmp	Negation of the condition
<b>LESS</b>	<b>&lt;</b>	tcpdump <32	Shows packets size less than 32
<b>GREATER</b>	<b>&gt;</b>	tcpdump >=32	Shows packets size greater than 32

## Installation Commands

CENT OS and REDHAT	\$ sudo yum install tcpdump
Fedora	\$ dnf install tcpdump
Ubuntu, Debian and Linux Mint	#apt-get install tcpdump

## Display / Output Options

Switch	Description
<b>-q</b>	Quite and less verbose mode display less details
<b>-t</b>	Do not print time stamp details in dump
<b>-v</b>	Little verbose output
<b>-vv</b>	More verbose output
<b>-vvv</b>	Most verbose output
<b>-x</b>	Print data and headers in HEX format
<b>-xx</b>	Print data with link headers in HEX format
<b>-X</b>	Print output in HEX and ASCII format <b>excluding</b> link headers
<b>-XX</b>	Print output in HEX and ASCII format <b>including</b> link headers
<b>-e</b>	Print Link (Ethernet) headers
<b>-S</b>	Print sequence numbers in exact format

## Protocols

**Ether, fddi, icmp ,ip, ip6 , ppp, radio, rarp, slip, tcp , udp, wlan**

## Common Commands with Protocols for Filtering Captures

src/ dst host (host name or IP)	Filter by source or destination IP address or host
ether src/ dst host (ethernet host name or IP)	Ethernet host filtering by source or destination
src/ dst net (subnet mask in CIDR)	Filter by subnet
tcp/udp src/dst port ( port number)	Filter TCP or UDP packets by source or destination port
tcp/udp src/dst port range ( port number range)	Filter TCP or UDP packets by source or destination port range
ether/ip broadcast	Filter for Ethernet or IP broadcasts
ether/ip multicast	Filter for Ethernet or IP multicasts