tcpdump Cheat Sheet

comparitech

Packet Capturing Options

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

Logical Operators

Operator	Syntax	Example	Description
AND	and, &&	tcpdump -n src 192.168.1.1 and dst port 21	Combine filtering options
OR	or, ||	tcpdump dst 10.1.1.1 && !icmp	Either of the condition can match
EXCEPT	not, !	tcpdump dst 10.1.1.1 and not icmp	Negation of the condition
LESS	<	tcpdump <32	Shows packets size less than 32
GREATER	>	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
-q	Quite and less verbose mode display less details
-t	Do not print time stamp details in dump
-v	Little verbose output
-vv	More verbose output
-vvv	Most verbose output
-x	Print data and headers in HEX format
-xx	Print data with link headers in HEX format
-X	Print output in HEX and ASCII format **excluding** link headers
-XX	Print output in HEX and ASCII format **including** link headers
-e	Print Link (Ethernet) headers
-S	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