TCPDUMP Cheat Sheet

www.cellstream.com

Command Line Options

-A	Print frame payload in ASCII format	-q	Quick output
-c [count]	Exit after capturing [count] packets	-r [file]	Read packets from [file]
-D	List available interfaces	-s [length]	Capture up to [length] bytes per packet
-e	Print link-level Headers	-S	Print absolute TCP sequence numbers
-F [file]	Use [file] as the filter expression	-v[v[v]]	Print more verbose output
-G [n]	Rotate the dump file every [n] seconds	-w [file]	Write captured packets to [file]
-i [intfc]	Specifies the capture interface	-x	Print the frame payload in HEX
-K	Don't verify TCP checksums	-X	Print the frame payload in HEX & ASCII
-L	List data link types for the interface	-y [type]	Specify the data link [type]
-n	Don't convert addresses to names	-Z [user]	Drop privileges from root to [user]
-p	Don't capture in promiscuous mode		

Capture Filter Primitives

[src|dst] host <host>	Matches a host as the IP source, destination, either
ether [src|dst] host <ehost>	Matches a host as the Ethernet source, destination, either
gateway host <host>	Matches packets that used <host> as a gateway
[src|dst] net <network>/<len>	Matches packets to/from an endpoint residing in <network>
[tcp/udp} [src|dst] port <port>	Matches TCP or UDP packets sent to/from <port>
[tcp/udp} [src|dst] portrange <p1><p2>	Matches TCP or UDP packets to/from port in the range
less <length>	Matches packets less than or equal to a <length>
greater <length>	Matches packets greater than or equal to <length>
(ether|ip) broadcast	Matches an Ethernet or IP v4 broadcast
(ether|ip|ip6) proto <protocol>	Matches an Ethernet, IP v4 or IP v6 protocol packet
(ether|ip|ip6) multicast	Matches an Ethernet, IP v4 or IP v6 multicast
type (mgt|ctl|data) [subtype<subtype>]	Matches 802.11 frames based on type/subtype
vlan [<vlan>]	Matches 802.11Q, optionally with a VLAN ID of <vlan>
mpls [<label>]	Match MPLS packets, optionally with a <label> value
<expr> <relop> <expr>	Matches packets by an arbitrary expression

ICMP Types

icmp-echo icmp-echoreply icmp-ireq
icmp-ireqreply icmp-maskreq icmp-maskreply
icmp-paramprob icmp-redirect icmp-routeradvert
icmp-routersolicit icmp-sourcequench
icmp-timexceed icmp-tstamp icmp-tstampreply
icmp-unreach

Examples

udp dst port not 80 = UDP not bound for port 80
host 10.1.1.1 && host 10.1.1.2 = Traffic between hosts
tcp dst port 80 or 8080 = Packets to either TCP port

Protocols

arp ether fddi icmp ip ip6 link ppp
radio rarp slip tcp tr udp wlan

TCP Flags

tcp-ack tcp-fin tcp-psh tcp-rst tcp-syn tcp-urg

Modifiers

! or not && or and || or or