TCPDUMP

packetlife.net

Command Line Options

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

Capture Filter Primitives

[src|dst] host <host>	Matches a host as the IP source, destination, or either
ether [src|dst] host <ehost>	Matches a host as the Ethernet source, destination, or either
gateway host <host>	Matches packets which used **host** as a gateway
[src|dst] net <network>/<len>	Matches packets to or 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 a port in the given range
less <length>	Matches packets less than or equal to **length**
greater <length>	Matches packets greater than or equal to **length**
(ether|ip|ip6) proto <protocol>	Matches an Ethernet, IPv4, or IPv6 protocol
(ether|ip) broadcast	Matches Ethernet or IPv4 broadcasts
(ether|ip|ip6) multicast	Matches Ethernet, IPv4, or IPv6 multicasts
type (mgt|ctl|data) [subtype <subtype>]	Matches 802.11 frames based on type and optional subtype
vlan [<vlan>]	Matches 802.1Q frames, optionally with a VLAN ID of **vlan**
mpls [<label>]	Matches MPLS packets, optionally with a label of **label**
<expr> <relop> <expr>	Matches packets by an arbitrary expression

Protocols

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

TCP Flags

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

Modifiers

! or **not**
&& or **and**
|| or **or**

Examples

udp dst port not 53	UDP not bound for port 53
host 10.0.0.1 && host 10.0.0.2	Traffic between these hosts
tcp dst port 80 or 8080	Packets to either TCP port

ICMP Types

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