# General usage

What?

Captures packet information

Can you filter which packets are captured?

yes, using

boolean expression

TODO

How much data does tcpdump capture of each packet by default?

96 bytes

What does tcpdump capture by default?

Basic info about each packet captured

Where does tcpdump direct output by default?

console

How can you direct output to a file?

-w

Once output has been captured to a file, what can be done with it?

You can replay it, applying various filters to limit the output.

How can you replay a previously captured sniffer session?

use the -r flag

How can you increase the amount of data captured?

-s

# Filtering output

How can capture output be filtered?

By host, port, source or destination address, and protocol

# Interpretting output

Michaels-Air-2:~ grudkowm$ sudo tcpdump -i 1 host 199.15.188.141

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on en0, link-type EN10MB (Ethernet), capture size 65535 bytes

19:02:33.360052 IP michaels-air-2.fios-router.home.57654 > 199.15.188.141.https: Flags [S], seq 2579334557, win 65535, options [mss 1460,nop,wscale 5,nop,nop,TS val 946517816 ecr 0,sackOK,eol], length 0

19:02:33.431114 IP 199.15.188.141.https > michaels-air-2.fios-router.home.57654: Flags [S.], seq 3478617903, ack 2579334558, win 4140, options [mss 1380,nop,wscale 0,nop,nop,TS val 2370844156 ecr 946517816,sackOK,eol], length 0

19:02:33.431190 IP michaels-air-2.fios-router.home.57654 > 199.15.188.141.https: Flags [.], ack 1, win 4104, options [nop,nop,TS val 946517885 ecr 2370844156], length 0

19:02:33.431962 IP michaels-air-2.fios-router.home.57654 > 199.15.188.141.https: Flags [P.], seq 1:228, ack 1, win 4104, options [nop,nop,TS val 946517885 ecr 2370844156], length 227

19:02:33.452880 IP 199.15.188.141.https > michaels-air-2.fios-router.home.57654: Flags [.], seq 1:1369, ack 228, win 4140, options [nop,nop,TS val 2370844178 ecr 946517885], length 1368

19:02:33.452884 IP 199.15.188.141.https > michaels-air-2.fios-router.home.57654: Flags [.], seq 1369:2737, ack 228, win 4140, options [nop,nop,TS val 2370844178 ecr 946517885], length 1368

19:02:33.452956 IP michaels-air-2.fios-router.home.57654 > 199.15.188.141.https: Flags [.], ack 2737, win 4018, options [nop,nop,TS val 946517905 ecr 2370844178], length 0

19:02:33.454432 IP 199.15.188.141.https > michaels-air-2.fios-router.home.57654: Flags [P.], seq 2737:4098, ack 228, win 4140, options [nop,nop,TS val 2370844178 ecr 946517885], length 1361

19:02:33.360052 IP michaels-air-2.fios-router.home.57654 > 199.15.188.141.https: Flags [S], seq 2579334557, win 65535, options [mss 1460,nop,wscale 5,nop,nop,TS val 946517816 ecr 0,sackOK,eol], length 0

PPI output

Michaels-Air-2:~ grudkowm$ sudo tcpdump -i en0 -y PPI

tcpdump: data link type PPI

tcpdump: verbose output suppressed, use -v or -vv for full protocol decode

listening on en0, link-type PPI (Per-Packet Information), capture size 65535 bytes

20:11:58.079753 Assoc Request[|802.11]

20:11:58.079761 Assoc Request[|802.11]

20:11:58.080044 Assoc Request[|802.11]

20:11:58.080049 Assoc Request[|802.11]

20:11:58.102958 Assoc Request[|802.11]

# Common operations

Remove timestamps from output

-t

Display packet in ascii only

tcpdump -A

Display packet body in both hex and ascii

tcpdump -X -i 1

Display packet body in hex only

tcpdump -x -i 1

Exit after receiving N packets

tcpdump -c 4

list network interfaces

sudo tcpdump -D

Only view tcp traffic

tcpdump tcp

Only view udp traffic

tcpdump udp

Only view traffic to port 50

tcpdump port 50

Don’t resolve hostnames

tcpdump -n

Don’t resolve either hostnames or ports

tcpdump -nn

Sniff traffic on given iface

tcpdump -i [iface name / num]

Show link layer types available on an interface

tcpdump -L

Display more info about each captured packet

tcpdump -v

tcpdump -vv

Change datalink type used while capturing packets

tcpdump -y

Print less output

tcpdump -q

# Terms

Data link

Data link type

PKTAP - Packet Tap

RAW - Raw IP

PPI - Per packet info

EN10MB - Ethernet

Link layer

Lowest layer in the TCP/IP protocol suite

Related to the physical medium that a host is connected to

In-band

Communication conducted within the same channel used for other communications

Out-of-band

Communication conducted via a separate channel from other communications

PDU

Protocol data unit

Different depending on the protocol being referred to

in TCP/IP, different layers utilize different PDU’s

# Concepts

promiscuous mode

sniffer captures packets including those not addressed to it

monitor mode

TODO

packet metadata

# Reference

http://ss64.com/nt/

https://www.winpcap.org/windump/docs/manual.htm

http://danielmiessler.com/study/tcpdump/

http://albanianwizard.org/tcpdump-how-to-the-linux-troubleshooter.albanianwizard

<http://science.hamptonu.edu/compsci/docs/iac/packet_sniffing.pdf>

http://albanianwizard.org/how-to-read-tcpdump-output-tcpdump-advanced-use.albanianwizard

http://www.wains.be/pub/networking/tcpdump\_advanced\_filters.txt